Integrate Cisco Router

Publication Date: February 7, 2017
Abstract

This guide provides instructions to configure Cisco Router to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and Cisco Router 12.x and 15.x.

Audience

Administrators, who are responsible for monitoring Cisco router devices using EventTracker Manager.
## Table of Contents

Abstract .................................................................................................................................................. 1
Overview................................................................................................................................................ 3
Pre requisites......................................................................................................................................... 3
Configure Cisco Router to send syslog to EventTracker ................................................................. 3
EventTracker Knowledge Pack (KP).................................................................................................... 4
  Categories........................................................................................................................................ 4
  Alerts ................................................................................................................................................ 5
  Reports ............................................................................................................................................. 5
Import Cisco Router Knowledge Pack into EventTracker ............................................................... 9
  Categories........................................................................................................................................ 10
  Alerts ................................................................................................................................................ 11
  Templates ......................................................................................................................................... 12
  Flex Reports .................................................................................................................................... 14
Verify Cisco Router knowledge pack in EventTracker ........................................................................ 15
  Categories........................................................................................................................................ 15
  Alerts ................................................................................................................................................ 15
  Template ......................................................................................................................................... 17
  Flex Reports .................................................................................................................................... 17
Create Dashboards in EventTracker .................................................................................................... 18
  Schedule Reports............................................................................................................................ 18
  Create Dashlets ............................................................................................................................. 20
Sample Dashboards ............................................................................................................................. 24
Overview

Router is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered. Router is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer.

EventTracker compiles and inspects critical events to provide an administrator insight on user behavior, traffic anomalies, link flaps etc.

NOTE: Applicable to the following series of router 800,2600,2800,1900,2900,3900,7200,7500 with IOS 12.x and 15.x

Pre requisites

- EventTracker v7.x or later should be installed.
- Cisco Router devices with software release version IOS 12.4 or higher.

Configure Cisco Router to send syslog to EventTracker

To enable and configure Cisco Routers for Syslog,

1. Enter global configuration mode and type the command `Router# configure terminal`

2. To specify `syslog server`, type the command -

   `Router(config)# logging host`

   It specifies the IP address or host name of EventTracker manager machine.

3. To specify `Severity level`, type the command -

   `Router(config)# logging trap level`

   Informational: 6

4. To specify `facility level`, type the command `Router(config)# logging facility` facility-level.

   The default is local7. Possible values are local0, local1, local2, local3, local4, local5, local6 and local7.
EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker; Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Cisco Router monitoring.

Categories

- **Cisco Router: Access control list** - This category provides information related to access control list.
- **Cisco Router: Access information element** - This category provides information related to access information element.
- **Cisco Router: Accounting services** - This category provides information related to accounting services.
- **Cisco Router: Adapter messages** - This category provides information related to adapter messages.
- **Cisco Router: Adjacency subsystem** - This category provides information related to adjacency subsystem.
- **Cisco Router: Administration** - This category provides information related to administration.
- **Cisco Router: Advance integration module** - This category provides information related to advance integration module.
- **Cisco Router: Advanced interface module** - This category provides information related to advanced interface module.
- **Cisco Router: Airline protocol support** - This category provides information related to airline protocol support.
- **Cisco Router: Alarm interface controller mgmt** - This category provides information related to alarm interface controller management.
- **Cisco Router: Align messages** - This category provides information related to align messages.
- **Cisco Router: Archive configuration** - This category provides information related to archive configuration.
- **Cisco Router: Asynchronous security protocol** - This category provides information related to asynchronous security protocol.
- **Cisco Router: ATM interface processor** - This category provides information related to ATM interface processor.
- **Cisco Router: ATM line card** - This category provides information related to ATM line card.
- **Cisco Router: Attachment circuit** - This category provides information related to attachment circuit.
- **Cisco Router: Authentication failure** - This category provides information related to authentication failure.
- **Cisco Router: Authentication proxy** - This category provides information related to authentication proxy.
• **Cisco Router: Automatic protection switching** - This category provides information related to automatic protection switching.

• **Cisco Router: Cache messages** - This category provides information related to cache messages.

• **Cisco Router: Chassis alarm** - This category provides information related to chassis alarm.

• **Cisco Router: Ethernet devices** - This category provides information related to Ethernet devices.

• **Cisco Router: Hardware device error** - This category provides information related to hardware device error.

• **Cisco Router: HTTP subsystem** - This category provides information related to HTTP subsystem.

• **Cisco Router: Intrusion detection** - This category provides information related to intrusion detection.

• **Cisco Router: Networks** - This category provides information related to networks.

### Alerts

• **Cisco Router: Border Gateway Protocol (BGP) neighbors up or down** - This alert is generated when Border Gateway Protocol (BGP) neighbors up or down event occurs.

• **Cisco Router: Hot Standby Router Protocol (HSRP) state** - This alert is generated when Hot Standby Router Protocol (HSRP) state change occurs.

• **Cisco Router: Interface down or detached** - This alert is generated when interface down or detached event occurs.

• **Cisco Router: Internal software error** - This alert is generated when internal software error occurs.

• **Cisco Router: IP-EIGRP neighbor is up or down** - This alert is generated when IP-EIGRP neighbor is up or down.

• **Cisco Router: Line protocol down** - This alert is generated when line protocol is down.

• **Cisco Router: Runaway processes** - This alert is generated when runaway processes occur.

### Reports

• **Cisco Router -Configuration changed**

This report provides information related to configuration changes which include Device Address, User Name, and Command Issued fields.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>Facility Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/08/2016 05:05:27 PM</td>
<td>CISCO-IOS9</td>
<td>Controller server, changed state to Active due to unknown</td>
<td>CONTROLLER-5-DOWNDETAIL</td>
</tr>
<tr>
<td>12/08/2016 05:05:27 PM</td>
<td>CISCO-IOS9</td>
<td>Dot1x unable to start.</td>
<td>DOT1X-4-PROC_START_ERR</td>
</tr>
</tbody>
</table>

**%FR_VCB-5-UPDOWN: FR VC-Bundle NYKLAXLINK changed state to InActive**
• **Cisco Router - Access denied**
  This report provides information related to connection denial events occurring on router or switch which includes Source address, Source Port, Destination Address, Destination port and Packets Transferred fields.

  Nov 7 12:20:08.139 EST: %SW_DAI-4-ACL_DENY: 1 Invalid ARPs (Res) on Gi1/3, vlan 1502.([001d.e513.8ef1/10.1.1.65/001d.e513.8ef1/10.1.1.65/12:20:07 EST Fri Nov 7 2008])

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Protocol Type</th>
<th>Interface</th>
<th>VLAN Number</th>
<th>Packets Transferred</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2016 04:30:01 PM</td>
<td>CISCO-KX5</td>
<td>102.168.10.112</td>
<td>4206</td>
<td>65.55.127.104</td>
<td>80</td>
<td>ACL_DENY</td>
<td>Gi1/3</td>
<td>100</td>
<td>1 Invalid ARPs (Res)</td>
<td><a href="http://www.websense.com">http://www.websense.com</a></td>
</tr>
<tr>
<td>12/01/2016 04:30:01 PM</td>
<td>CISCO-KX5</td>
<td>170.1.1.2</td>
<td>112</td>
<td>1.1.1.1</td>
<td>80</td>
<td>ACL_DENY</td>
<td>Gi0/1</td>
<td>100</td>
<td>1 Invalid ARPs (Res)</td>
<td><a href="http://www.websense.com">http://www.websense.com</a></td>
</tr>
<tr>
<td>12/01/2016 04:30:01 PM</td>
<td>CISCO-KX5</td>
<td>102.168.10.112</td>
<td>4206</td>
<td>65.55.127.104</td>
<td>80</td>
<td>ACL_DENY</td>
<td>Gi1/3</td>
<td>100</td>
<td>1 Invalid ARPs (Res)</td>
<td><a href="http://www.websense.com">http://www.websense.com</a></td>
</tr>
</tbody>
</table>

• **Cisco Router - Port status change**
  This report provides information related to port status changed from UP to DOWN or vice versa which includes Device Address, Interface Name and Port Status fields.

  00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-OS1</td>
<td>PM-4-ERR_DISABLE</td>
<td>psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state</td>
</tr>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-OS1</td>
<td>PM-4-ERR_DISABLE</td>
<td>psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state</td>
</tr>
</tbody>
</table>

• **Cisco Router - User logon success**
  This report provides information related to user logon success which includes User Name, Source Address and Source Port fields.

  Oct 16 09:32:37.657: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: neteng] [Source: 0.0.0.0] [localport: 0] at 09:32:37 UTC Fri Oct 16 2009

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Local Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2016 05:14:43 PM</td>
<td>David</td>
<td>10.10.2.32</td>
<td>22</td>
</tr>
</tbody>
</table>
• **Cisco Router -User logon failure**
  This report provides information related to user logon failure which includes User Name, Source Address, Source Port and Reason fields.

  **Feb 9 2015 18:34:38.236 MSK: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: rrr] [Source: 10.0.10.169] [localport: 23] [Reason: Login Authentication Failed] at 18:34:38 MSK Mon Feb 9 2015**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>UserName</th>
<th>Source IP Address</th>
<th>Local Port</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2016 05:14:43 PM</td>
<td>David</td>
<td>10.10.2.32</td>
<td>22</td>
<td>Invalid login</td>
</tr>
</tbody>
</table>

• **Cisco Router -Authentication failure**
  This report provides information related to authentication failure that is whenever the user tries to login into one of the Cisco Router.

  **Sep 15 13:09:47.308: %GLBP-4-BADAUTH: Bad authentication received from 149.212.19.162, group**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Client</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 04:09:22 PM</td>
<td>CISCO-IOS8</td>
<td>GLBP-4-UNAVAILABLE</td>
<td>192.23.43.23</td>
<td>Bad authentication received from 192.23.43.23, group 2</td>
</tr>
<tr>
<td>01/03/2017 04:09:22 PM</td>
<td>CISCO-IOS8</td>
<td>CRYPTO-6-UNAVAILABLE</td>
<td>192.23.12.2</td>
<td>Authentication method 192.23.12.2 failed with host accel</td>
</tr>
</tbody>
</table>

• **Cisco Router -Administrative account activity**
  This report provides information related to account activities that is done by the administrator.

  **%AAA-5-USER_LOCKED: User michel locked out on authentication failure**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>UserName</th>
<th>Reason</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/25/2016 07:12:17 PM</td>
<td>CISCO</td>
<td>Smith</td>
<td>locked out on authentication failure</td>
<td>Charles</td>
</tr>
<tr>
<td>11/25/2016 07:12:17 PM</td>
<td>CISCO</td>
<td>Smith</td>
<td>failed attempts reset</td>
<td>Charles</td>
</tr>
<tr>
<td>11/25/2016 07:12:18 PM</td>
<td>CISCO</td>
<td>Smith</td>
<td>unlocked</td>
<td>Charles</td>
</tr>
</tbody>
</table>
• **Cisco Router -VTP management**
  This report provides information related to activities that occur and are related to VTP.

  **%%VTP-2-MODE_OFF_PVLAN_EXIST** Format: VTP Mode changed to off as Private VLAN configuration exists

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 04:40:38 PM</td>
<td>CISCO-IOS2</td>
<td>VTP-4-BAD_STARTUP_VLAN_CONFIG_FILE Format</td>
<td>Failed to configure VLAN from startup-config. Fallback to use VLAN configuration file from non-volatile</td>
</tr>
<tr>
<td>01/03/2017 04:40:38 PM</td>
<td>CISCO-IOS2</td>
<td>SW_VLAN-3-VTP_PROTOCOL_ERROR</td>
<td>VTP protocol internal error: Version 1 device detected on Fa0/23</td>
</tr>
</tbody>
</table>

• **Cisco Router -Router protocol**
  This report provides information about the activities related to Router protocol like IPRT, BGP etc.

  **%%IPRT-3-UNAVAILABLE**: IP Router table creation failure - IISC

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/10/2017 04:04:27 PM</td>
<td>CISCO-IOS2</td>
<td>Failed to send message. 97bhjkl</td>
</tr>
<tr>
<td>01/10/2017 04:04:27 PM</td>
<td>CISCO-IOS2</td>
<td>Failed to allocate private memory</td>
</tr>
<tr>
<td>01/10/2017 04:04:27 PM</td>
<td>CISCO-IOS2</td>
<td>BGP pop shutdown due to no memory condition 789</td>
</tr>
</tbody>
</table>
Import Cisco Router Knowledge Pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility, and then click the Import tab.

![EventTracker Control Panel](image)

Import in the same order as mentioned:

- Templates
- Categories
- Alerts
- Reports as given below:
Categories

1. Click Category option and then click the browse button.

2. Locate All Cisco Router group of Categories.iscat file, and then click the Open button.
3. To import the categories, click the Import button. EventTracker displays success message.

4. Click OK, and then click the Close button.
Alerts

1. Click Category option and then click the browse button.

![Figure 4](image)

2. Locate All Cisco Router group of Alerts.isalt file, and then click the Open button.
3. To import alerts, click the Import button.
   EventTracker displays success message.

![Figure 5](image)

4. Click OK, and then click the Close button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. Select the respective checkbox in the Alert management page, and then click the Activate Now button.
Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  ‘Import’ option.

![Parsing Rule](image)

**Figure 6**

3. Click on **Browse** button.

![Select File](image)

**Figure 7**

4. Locate All Cisco Router group of **Template.ettd** file, and then click the **Open** button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

6. Click on OK button.
Flex Reports

1. Click **Reports** option, and then click the 'browse' button.
2. Locate **All Cisco Router group reports.issch** file, and then click the **Open** button.

![Figure 11 Import Utility](image)

3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

![Figure 12 Import Success](image)

4. Click **OK**, and then click the **Close** button.
Verify Cisco Router knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In the Category Tree, expand Cisco Router group folder to view imported categories.

![Category Management](image)

Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type ‘Cisco Router’, and then click the Go button.
   Alert Management page will display all the imported Cisco Router alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Successfully saved configuration](image)

**Figure 15**

5. Click **OK**, and then click the **Activate now** button.

**NOTE:** Please specify appropriate **systems** in **Alert configuration** for better performance.
Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.

![Parsing Rule]

Figure 16

Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported flex reports, scroll down and click Cisco Router group folder.

Imported reports are displayed in the Reports Configuration pane.
NOTE: Please specify appropriate systems in report wizard for better performance.

Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **Cisco Router** in report groups. Check **Defined** dialog box.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in EventVault explorer** box.

![REPORT WIZARD]

**Figure 21**

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

**Create Dashlets**

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.
3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

4. Click **+** to add a new dashboard.
   Flex Dashboard configuration pane is shown.
4. Fill fitting title and description and click **Save** button.

5. Click 🔄 to configure a new flex dashlet.

   Widget configuration pane is shown.

---

![Widget Configuration](image)

**Figure 25**

6. Locate earlier scheduled report in **Data Source** dropdown.

7. Select **Chart Type** from dropdown.

8. Select extent of data to be displayed in **Duration** dropdown.

9. Select computation type in **Value Field Setting** dropdown.

10. Select evaluation duration in **As Of** dropdown.

11. Select comparable values in **X Axis** with suitable label.

12. Select numeric values in **Y Axis** with suitable label.

13. Select comparable sequence in **Legend**.

14. Click **Test** button to evaluate.

   Evaluated chart is shown.
15. If satisfied, click **Configure** button.

16. Click ‘customize’ 📷 to locate and choose created dashlet.

17. Click 📦 to add dashlet to earlier created dashboard.
Sample Dashboards

1. Cisco Logon Failures Today

Figure 28