Integrate Linux OS

EventTracker v8.x and above

Publication Date: September 27, 2018
Abstract

Linux is, in simplest terms, an operating system. Linux enables applications and the computer operator to access devices on the computer to perform desired functions. The operating system (OS) relays instructions from an application to, for instance, the computer's processor. The processor performs the instructed task, and then sends results back to the application via the operating system.

EventTracker allows you to effectively manage your Linux systems and provides operational efficiencies - reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker's built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Redhat, Suse, CentOS, Fedora operating system.

Audience

Linux OS users, who wish to forward Syslogs to EventTracker Manager and monitor events using EventTracker Enterprise.
# Table of Contents

Abstract ............................................................................................................................................................. 1  
Scope ............................................................................................................................................................. 1  
Audience........................................................................................................................................................... 1  
Introduction.................................................................................................................................................... 3  
Prerequisites.................................................................................................................................................. 3  
Configure rsyslog to forward logs to EventTracker ................................................................. 3  
EventTracker Knowledge Pack ................................................................................................................. 4  
  Flex Reports ............................................................................................................................................... 4  
  Alerts ......................................................................................................................................................... 7  
  Categories ............................................................................................................................................... 7  
Import Linux OS knowledge pack into EventTracker ................................................................. 7  
  Category ............................................................................................................................................... 8  
  Alerts ....................................................................................................................................................... 10  
  Token Templates ................................................................................................................................. 11  
  Knowledge Objects ............................................................................................................................ 11  
  Flex Reports ........................................................................................................................................ 13  
Verify Linux OS knowledge pack in EventTracker ................................................................. 14  
  Categories........................................................................................................................................... 14  
  Alerts ..................................................................................................................................................... 15  
  Token Templates ............................................................................................................................... 15  
  Knowledge Objects.......................................................................................................................... 16  
  Flex Reports ...................................................................................................................................... 16
Introduction

Linux is an operating system. An operating system is software that manages all the hardware resources associated with your desktop or laptop. To put it simply – the operating system manages the communication between your software and your hardware.

Prerequisites

- EventTracker v8.x and later should be installed.
- Linux OS should be installed.

Configure rsyslog to forward logs to EventTracker

To configure the rsyslog to forward logs to a syslog server,

1. Login to the Linux Redhat/CentOS machine as root.
2. Open Terminal window.
3. Open rsyslog.conf in VI Editor. vi /etc/rsyslog.conf
4. Add the below mentioned line in file rsyslog.conf at last.

   ```
   *.* @IP address of EventTracker Enterprise machine: 514
   Example *.* @10.10.10.167:514
   *.*<tab>@<RemoteHost>:<RemotePort> i.e. after *.* it’s a tab, not a regular space
   ```

   **NOTE:** Use ‘@@’ for TCP and ‘@’ for UDP to forward log to Remote host. It would forward the syslog messages to EventTracker Enterprise machine.

5. By default, all audit logs are disabled. For enabling it to append following lines in /etc/rsyslog.conf:

   ```
   # auditd audit.log
   $InputFileName /var/log/audit/audit.log
   $InputFileTag tag_audit_log:
   $InputFileStateFile audit_log
   $InputFileSeverity info
   $InputFileFacility local6
   $InputRunFileMonitor
   ```

6. Save the file using: wq.
7. Add following rules in /etc/audit/audit.rules:

EventTracker

Actionable Security Intelligence
Integrate Linux OS

- `a always,exit -S all -F dir=/boot -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/bin -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/sbin -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/usr/bin -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/usr/local/bin -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/usr/local/sbin -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/usr/sbin -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/lib -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/lib64 -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/usr/lib -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/etc -F perm=aw -k system-objects`
- `a always,exit -S all -F dir=/usr/lib/systemd/ -F perm=aw -k system-objects`
- `auditctl -a exit,always -F arch=b64 -S execve -k root-commands`
- `auditctl -a exit,always -F arch=b32 -S execve -k root-commands`
- `auditctl -a exit,always -F arch=b32 -S execve -k root-commands`

8. To activate the above configuration, restart the syslog service.

```
sudo killall -HUP rsyslog rsyslogd  (On most OS's)
```

On Ubuntu:

```
sudo service rsyslog restart
```

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Linux OS.

Flex Reports

- **Linux-User authentication failed**: This report provides information about the authentication failures by users.

![Figure 1](image-url)
- **Linux-User authentication success**: This report provides information about the successful authentication by users.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>User Name</th>
<th>Src</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/30/2016 02:50:00 PM</td>
<td>PNPL-15-KP/PNPL-15-KP</td>
<td>authentication successful</td>
<td>root</td>
<td>cinderela.booms.local</td>
<td>sshd.auth</td>
</tr>
<tr>
<td>12/30/2016 02:50:42 PM</td>
<td>PNPL-15-KP/PNPL-15-KP</td>
<td>authentication successful</td>
<td>Alex</td>
<td>cinderela.booms.local</td>
<td>gdm-password.auth</td>
</tr>
</tbody>
</table>

  **Figure 2**

- **Linux-SU session failed**: This report provides information related to the failed super user session.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Message</th>
<th>To</th>
<th>By Whom</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>PNPL-15-KP/PNPL-15-KP</td>
<td>FAILED SU</td>
<td>sam</td>
<td>dummy1</td>
<td>pts/0</td>
</tr>
<tr>
<td>PNPL-15-KP/PNPL-15-KP</td>
<td>FAILED SU</td>
<td>root</td>
<td>dummy1</td>
<td>pts/0</td>
</tr>
</tbody>
</table>

  **Figure 3**

- **Linux-Sudo command executed**: This report provides information about the commands executed using super user privileges.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer Name</th>
<th>User Name</th>
<th>Command Executed</th>
<th>Path Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/30/2016 03:21:42 PM</td>
<td>CentOS6-vm</td>
<td>root</td>
<td>sudo /var/logsecure</td>
<td>/root</td>
</tr>
<tr>
<td>12/30/2016 03:21:46 PM</td>
<td>CentOS6-vm</td>
<td>root</td>
<td>sudo /varlog</td>
<td>/root</td>
</tr>
<tr>
<td>12/30/2016 03:21:46 PM</td>
<td>CentOS6-vm</td>
<td>root</td>
<td>sudo /etc</td>
<td>/root</td>
</tr>
<tr>
<td>12/30/2016 03:21:46 PM</td>
<td>CentOS6-vm</td>
<td>root</td>
<td>sudo /var/logsecure</td>
<td>/root</td>
</tr>
</tbody>
</table>

  **Figure 4**

- **Linux-Account operation**: This report provides information about additions, deletions or modifications of account in a Linux server, and includes username, group name, user ID (UID), group ID (GID), user home directory and shell file, and changes that have happened in accounts.
- **Linux-User logon failed**: This report provides information about the logon failures by users.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>UserName</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Type</th>
</tr>
</thead>
</table>

- **Linux-User logon success**: This report provides information about the successful logins by users.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>UserName</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/06/2017 12:48:34 PM</td>
<td>PNPL-15-KP/PNPL-15-KP</td>
<td>Accepted password</td>
<td>Jon</td>
<td>192.168.1.245</td>
<td>56043</td>
<td>ssh2</td>
</tr>
</tbody>
</table>

- **Linux-User connection closed**: This report provides connection related information.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>Closed By</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/30/2016 02:51:10 PM</td>
<td>PNPL-15-KP/PNPL-15-KP</td>
<td>Connection closed</td>
<td>proauth</td>
<td></td>
</tr>
</tbody>
</table>

- **Linux-System shutdown**: This report provides information related to system shutdown done by different hosts.
Integrate Linux OS

Alerts

- **Linux: SU Session Failed** - This alert will be generated when SU session failure occurred on system.
- **Linux: System shutdown** - This alert will be generated when system shutdown happens.

Categories

- **Linux: Audit Details** - This category provides information about the activity related to auditing.
- **Linux: Service or Daemon Status** - This category provides information about the activity related to service or daemon Status.
- **Linux: Sudo User Activity** - This category provides information about the activity related to sudo user activity.
- **Linux: User Account Management** - This category provides information about the activity related to user account management.
- **Linux: User Authentication Failure** - This category provides information about the activity related to user authentication failure.
- **Linux: User Authentication Success** - This category provides information about the activity related to user authentication success.

Import Linux OS knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence:

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

![EventTracker Control Panel](image)

Figure 10

3. Click the **Import** tab.

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate Category/Linux OS.iscat file, and then click the Open button.
3. To import categories, click the Import button. EventTracker displays success message.

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

1. Click **Alert** option, and then click the browse button.

![Export Import Utility](image)

**Figure 13**

2. Locate **Alert_Linux OS.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

![Import alert successfully](image)

**Figure 14**
4. Click **OK**, and then click the **Close** button.

### Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.

2. Move to **Template** and click on import configuration icon on the top right corner.

3. In the popup window browse the file named **Token Template_Linux OS.ettd**.

![Figure 15](image)

4. Now select all the check box and then click on **Import** option.

### Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.

2. Locate the **KO_Linux OS.etko** file.
3. Click the ‘Upload’ option.

Figure 17
4. Now select all the check box and then click on ‘Import’ option.
5. Knowledge objects are now imported successfully.

![File imported successfully]

Figure 18

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

**Flex Reports**

On EventTracker Control Panel,

1. Click Reports option, and select new (*.etcrx) from the option.

![Export Import Utility]

Figure 19

2. Locate the Reports_Linux OS.etcrx file, and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Figure 19](image19.png)

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

![Figure 20](image20.png)

**Verify Linux OS knowledge pack in EventTracker**

**Categories**

1. Logon to **EventTracker Enterprise**.

2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Linux OS** group folder to view the imported categories.

![Category Tree](image)

**Figure 21**

### Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box, enter **Linux OS** and then click the **Search** button.

   EventTracker displays alert of **Linux OS**.

![Alerts](image)

**Figure 22**

### Token Templates

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.
2. On Template tab, click on the Linux OS group folder to view the imported Token Values.

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand Linux OS group folder to view the imported Knowledge objects.

Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Report Configuration.
2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Linux OS** group folder to view the imported Linux OS reports.