EventTracker

Actionable Security Intelligence

# EventTracker Linux Agent

## Install Guide

Publication Date: March 23, 2017

# Abstract

This guide will help the users to install and configure EventTracker Linux agent, and verify the expected functionality of all its components.

# Audience

System administrators, who wish to install the EventTracker Linux agent.

# Table of Contents

Abstract ..... 1
Audience ..... 1
Introduction ..... 3
System Requirements ..... 3
Installation Process of the Linux Agent ..... 3

# Introduction

The EventTracker Agent for Linux offers to install an RPM that offers to forward useful rsyslog messages to a central EventTracker receiver. Now monitoring and accessing data inputs on potentially large number of Linux System from one place is possible.

# System Requirements

- Support **RHEL/CentOS 6.x** and above.

# Installation Process of the Linux Agent

**User can install Linux Agent which has root permission.**

- Get the Tar file based on the operating system Architect version.
- Tar file name - EventTracker-**majorVersion.minorVersion.buildNumber**-1.el6.**operating system Architect version**.tar.gz

Ex:-

1. EventTracker-1.0.9-1.el6.i386.tar.gz (version 1 build 9 for 32 bit operating system)
2. EventTracker-1.0.9-1.el6.x86_64.tar.gz (version 1 build 9 for 64 bit operating system)

- Extract the tar file on Linux system by the command-
  **tar -xzf Filename**
  Ex: - **tar -xzf EventTracker-1.0.9-1.el6.x86_64.tar.gz**

- The extract command will create a folder based on tar file name that will contain 3 files.
  1. setup.sh (script file which helps to install the Linux agent).
  2. public.pem (gpg public key which is used to encrypt ftp password).
  3. EventTracker-**majorVersion.minorVersion.buildNumber**-1.el6.**operating system Architect version.rpm** (rpm package that contains the deployment files).
     rpm file ex-
     a. EventTracker-1.0.9-1.el6.i386.rpm (version 1 build 9 for 32 bit operating system)
     b. EventTracker-1.0.9-1.el6.x86_64.rpm (version 1 build 9 for 64 bit operating system)

- For installing the Linux Agent, the user has to follow the below mentioned steps:
  1. Use linux terminal or any terminal client software to install the EventTracker agent.
  2. Traverse to the directory where the above 3 files are placed.
  3. Change setup.sh file permission mode to 'read, write and execute'.

4. Use command **chmod 777 setup.sh.**
5. Execute setup.sh and it will provide steps from section 1 to 8.
6. The script will request user inputs for EventTracker console host address and will configure the value.
7. If you are not sure about the configuring value then press **Enter** to go ahead with the default value which will be displayed in bracket**[].**
   Ex: Destination port of EventTracker Console [514] – here **514** is default value for EventTracker console port.

## Section 1 of 8:

```
Section 1 of 8: Welcome - RedHat performance package for EventTracker
This collection of scripts is used to configure rsyslog
from this machine to an EventTracker Console.
Pre requisites include
 - rsyslog (5.8.10 or higher)
You will need
 - IP address or DNS name of EventTracker Console
 - Port number to be used at EventTracker Console
 - Internet connection to download and install dependent packages.

Log is written to /tmp/EventTrackerAgent.log
Defaults are chosen, if you are not sure then use the defaults
Press [Enter] to accept default response to any question
Press [Q/q] to quit setup at any time
Press [Enter] to continue
```

## Section 2 of 8: Configure rsyslog

1. The script setup.sh will prompt the user to provide the EventTracker console host address. It should be an IP address or a fully qualified domain name (ex; 192.168.1.104 or louie.toons.local).
2. The script will request the user to provide the EventTracker console port number.
3. If the user configures other than the port 514, then it has to add it in SELinux security policy.

   **Syntax**: - semanage port -a -t processname_port_t -p ProtocolType PortNumber

   **Ex**: - semanage **port -a -t syslogd_port_t -p tcp 515**
   Check whether semanage utility is installed or not. If not installed then, we need to install "policycoreutils-python" package through yum installation.
   command to install "policycoreutils-python"
   **yum install -y policycoreutils-python**

4. The script will also prompt the user to provide the Severity Levels, the value of which will depend on the below displayed table.
5. This section will create **alerts.conf** under **/etc/rsyslog.d** directory.

```
Section 2 of 8: Configure rsyslog
Checking for rsyslog ...
rsyslog version :8.10.0.ad1 found

IP address or Fully qualified domain name of EventTracker Console:
192.168.1.104
192.168.1.104 resolved to : louie.toons.local.

Destination port of EventTracker Console [514]:
514
Message severity:(0-7)[3]:
4
Shutting down system logger:                    [  OK  ]
Starting system logger:                         [  OK  ]
Press [Enter] to continue
```

| Numerical Code | Severity | Description |
|---|---|---|
| 0 | emergency | System is unusable |
| 1 | alert | action must be taken immediately |
| 2 | critical | critical conditions |
| 3 | error | error conditions |
| 4 | warning | warning conditions |
| 5 | notice | normal but significant condition |
| 6 | informational | informational messages |
| 7 | debug | debug-level messages |

## Section 3 of 8: Monitor file changes using rsyslog

1. The script, setup.sh will request the user to enable USB monitor by rsyslog.
2. It will also prompt the user to provide the directory path to be monitored by rsyslog.
3. If the required directory path has been configured then press **n** or **N** to complete.
4. This section will create **custom.conf** under **/etc/rsyslog.d** directory.

```
Section 3 of 8: Monitor file changes using rsyslog
Skip this section ? (y/[n]):

Checking for rsyslog ...
rsyslog version :5.8.10 found
rsyslog version 8.1.14 and above allows you to monitor more than 100 files at a time.

Enable USB monitor ? ([y]/n):

Start USB monitor

Directory to monitor [/var/log] (enter N/n to complete):

Skipping directory : . ...
Skipping directory : .. ...
Skipping directory : audit ...
Skipping directory : ConsoleKit ...
Skipping directory : cups ...
Skipping directory : gdm ...
Skipping directory : httpd ...
Skipping directory : ntpstats ...
Skipping directory : ppp ...
Skipping directory : prelink ...
Skipping directory : sa ...
Skipping directory : samba ...
Skipping directory : sssd ...
Directory added for monitor [/var/log].

Directory to monitor  (enter N/n to complete):
n
Shutting down system logger:                       [  OK  ]
Starting system logger:                            [  OK  ]
Press [Enter] to continue
```

## Section 4 of 8: rpm Installation

1. The script will check for the dependent library. If it is not installed it will download the latest library and install it.
2. It will create 'EventTrackerAdmin' user and will ask for the password.
3. This script will then install the EventTracker rpm.
4. This section will create **EventTracker** directory under **/opt** directory.

```
Section 4 of 8: rpm install (required if performance alert or data upload is desired)
Skip this section ? (y/[n]):

Checking pre-requisites
cronie:[1.4.4] is installed.
binutils:[2.20.51.0.2] is installed.
coreutils:[8.4] is installed.
bind-utils:[9.8.2] is installed.
sysstat:[9.0.4] is installed.
net-tools:[1.60] is installed.
ethtool:[3.5] is installed.
Pre-requisites are all present.

Starting EventTracker scripts install...
Checking for libc ...
glibc installed version:[2.122.12]
Checking for libstdc++ ...
libstdc++ installed version:[4.4.7]
id: EventTrackerAdmin: No such user
A local user "EventTrackerAdmin" is required to run the scripts. Creating...
Enter password for "EventTrackerAdmin":
Re-enter password for confirmation:
Installing the RPM /root/Amit/Build 9/Bin/EventTracker-1.0.9-1.el6.x86_64.rpm
Preparing...                ########################################### [100%]

Start RPM [1.0.9] installation
   1:EventTracker           ########################################### [100%]
EventTracker RPM [1.0.9] installation is complete.

Press [Enter] to continue
```

## Section 5 of 8: Performance Alerts

1. The script will request the user to provide the input for **crond** configuration.
2. It will also prompt the user to provide the thresholds value for system and process alerting.
3. This section will create **ETcrontab** configuration file under **/etc/cron.d** directory.

```
Section 5 of 8: Performance Alerts
This section allows you to define parameters for configuring EventTracker Alerts.
Would you like to skip this section ?(y/[n]):

Please enter the interval(mins) to sample the data [2 mins]:

Stopping crond:                            [  OK  ]
Starting crond:                            [  OK  ]
root: EventTrackerAlert : Test Alert
A test alert has been sent to the EventTracker Console. Was it received?

The following System threshold parameters can be used for alerting:
System wide percentage CPU usage [90]
System wide percentage Memory Usage [90]
System wide percentage Disk Free [10]
Would you like to change these ?(y/[n]):

The following Process threshold parameters can be used for alerting:
Process percentage CPU usage [85]
Process percentage Memory Usage [65]
Would you like to change these ?(y/[n]):

Number of consecutive samples above threshold to trigger an alert:(1-10)[3]:

Number of alerts to suppress in case of continuous alerts (1-10)[3]:

Press [Enter] to continue
```

## Section 6 of 8: Performance data gathering using cron

1. The setup.sh script will request the user to provide input for **crond** configuration.
2. This section will update in **ETcrontab** configuration file that is placed under **/etc/cron.d** directory.

```
Section 6 of 8: Performance data gathering using cron
This section will set up the cron daemon to run performance scripts at the specified interval.
Would you like to skip this section ?(y/[n]):

Interval (mins) to measure performance [2]:

Stopping crond:                            [  OK  ]
Starting crond:                            [  OK  ]
Press [Enter] to continue
```

## FTP configure section

1. The script will request you to provide input for configuring FTP.
2. This section will update in **credentials.txt** file that is placed under **/opt/EventTracker/scripts** directory.
3. It will prompt you to provide the FTP Interval (hours) to transfer the data files.

```
Section 7 of 8: Performance data upload via FTP
This section creates an FTP script that can upload the data files
to FTP server on default port.
Would you like to skip this section ?(y/[n]):

openssl:[1.0.1e] is installed ...
FTP:[0.17] is installed ...

Hostname or IP address of EventTracker Console: [192.168.1.104]:

192.168.1.104 resolved to : louie.toons.local.
FTP username for host '192.168.1.104':
ETAdmin
Enter password for FTP username 'ETAdmin':
Re-enter password for confirmation for FTP username 'ETAdmin':

Interval (hours) to upload files via FTP [1]:

Stopping crond:                            [  OK  ]
Starting crond:                            [  OK  ]
Press [Enter] to continue
```

## Section 8 of 8: Installation summary

1. It will display the Installation Summary where information related to the version, performance alert measurement level, the FTP server that receives the data files and the FTP username are displayed. This is shown in the figure below:

```
Section 8 of 8: Summary
The version of EventTracker Agent installed is : 1.0.9
Scripts owned by user: EventTrackerAdmin
The EventTracker console/manager that receives the syslog message/alerts: 192.168.1.104[louie.toons.local.] on port (514)
USB Monitor : Enabled
Monitor file changes using rsyslog: Enabled
Performance alert measurement interval (mins): 2
Performance data gathering interval (mins): 2
The FTP Server that receives the data files are : 192.168.1.104[louie.toons.local.]
FTP username is: ETAdmin
Interval (hours) to upload files via FTP: 1
EventTracker installation is now complete
Press [Enter] to continue
```