Receive and Forward syslog events through EventTracker Agent

EventTracker v8.2
Abstract

The purpose of this document is to help users to receive syslog messages from various network devices, encrypt them and then forward these syslog messages to EventTracker Manager.

Target Audience

This guide is helpful for users who receive and forward syslog messages through EventTracker agent.
Table of Contents

Abstract .............................................................................................................................................................................. 1
Target Audience ............................................................................................................................................................ 1
Pre-requisite ................................................................................................................................................................. 3
Process to be followed after applying the Update ET82U16-018 and ET82UA16-018 ........................................... 3
To verify whether the configured port is listening and receiving the syslog messages in the Agent Machine... 6
To verify whether the syslog messages are being received in the EventTracker Manager Console............... 7
Pre-requisite

- The user should have licensed LogFile Monitor feature.
- User should apply the Update: ET82U16-018 and ET82UA16-018.

Process to be followed after applying the Update ET82U16-018 and ET82UA16-018

- Open the EventTracker Control Panel.
- Double-click on EventTracker Agent Configuration.
- Select Logfile Monitor tab and then check the Logfile Monitor option.
How to Receive and Forward syslog events through EventTracker Agent

- Select **Add File Name** option.
- Select Logfile type as **“syslog”**.

This is shown in the figure below:

![Figure 2](image)

- Select the **Protocol** from the dropdown list, i.e. **UDP/TCP**.
- Enter the valid **Port** number, which is not used by other processes and then click **OK**.

![Figure 3](image)

- The port gets added in the **EventTracker Configuration** window.
Click **Save** and then **Close** the window.

The `ETAconfig.ini` logfile detail includes `Syslog_Rx` which gets created under Logfile Monitor activity, with the added field names. This is shown below:
EventTracker Agent will receive the syslog message on the configured port and will forward syslog message to the EventTracker Manager. The syslog message will be received on the port to which the agent is reporting.

To verify whether the configured port is listening and receiving the syslog messages in the Agent Machine

- Open the "etalog.txt" kept in the Install directory Agent folder.
- Verify whether the syslog receiver is getting created for the configured port, i.e. '514'.
How to- Receive and Forward syslog events through EventTracker Agent

For addition logging,

1. Create a file named ‘etamoduleconfig.ini’ in the format shown below:

```ini
[Syslog Rx]
File_Name = Syslog_Rx.txt
File_Backup_Copy = 1
File_Size_MB = 10
debug = 4
[End]
```

2. Copy the ‘etamoduleconfig.ini’ file in the Install directory Agent folder and then restart the agent service.

3. The ‘Syslog_Rx.txt’ log file gets created, which will have the details of the syslog messages received. Refer to the figure shown below:

![Syslog_Rx.txt](image)

To verify whether the syslog messages are being received in the EventTracker Manager Console

- Open EventTracker web-> Admin-> System Manager.
  The systems will be listed under the Default Group.
How to Receive and Forward syslog events through EventTracker Agent

![Figure 9](image)

- The user can also perform a log search and get the results as shown below:

![Figure 10](image)