A guide to configure agents for log collection in EventLog Analyzer
Introduction

EventLog Analyzer, a comprehensive SIEM solution, is capable of collecting Windows event logs by using both,

- Agent-less log collection method
- Agent-based log collection method

There is no clear "better option" for log collection. Rather, the mode of log collection is dictated by the requirements of the organization. This guide discusses the architecture and configuration of agents for log collection.

We recommend you to choose the mode of log collection based on your IT infrastructure, policies, and requirements. Contact our support team eventlog-support@manageengine.com for better guidance on choosing the log collection mode.

Agent-based Log Collection

Agent-based log collection is especially useful for easy collection of logs across WAN and through firewalls. One factor that forces the deployment of agents for log collection is unavailability of an established network connection. Agents are also helpful in log collection from devices residing in the restricted zones of your network such as DMZs. Further, agent-based log collection reduces the CPU utilization of the server and thereby provides more control over the EPS (Events per second) rate.

When can you go for agent-based log collection?

With EventLog Analyzer, you can opt for the agent-based log collection method under the below circumstances.

1. When your organization's IT security policy doesn't allow access for WMI/DCOM communication ports in Windows devices (A Windows device could be a server, workstation or domain controller).

2. When there isn't an established network connection between the server where EventLog Analyzer is installed and the device from which the log data is to be collected.

3. When you are looking to balance the overhead load across your network.

4. For easy log collection across WANs and through firewalls.

5. For monitoring the critical changes on files and folders through File Integrity Monitoring feature.
Architecture

This section illustrates the architecture of the agent-based log collection deployment.

The agent should be installed on the desired Windows device in order to remotely collect log data from it, and then send the collected log data to the EventLog Analyzer server. Whereas, in the case of agent-less log collection, the agent resides within the EventLog Analyzer server itself, rather than being present on the Windows device.

To deploy the agent on a specific device, execute the ‘EventLogAgent.msi’ file located in lib\native directory in the installation folder.

How does the agent work?

- The agent accesses the WMI infrastructure of the device internally and obtains the log data directly through WMI querying.

- Once the log data is collected, the agent does the pre-processing which includes log filtering as well as field extraction at the source, before zipping the log file and sending the log data to the EventLog Analyzer server securely through the HTTP protocol.

- Since the log data has already been processed at this point, the server only needs to index the logs to generate the reports and alerts in real-time.
Steps to configure agent-based log collection

With EventLog Analyzer, the process of configuring and managing agents for log collection is very simple. EventLog Analyzer collects the log data through the agent-less mode by default. Even in the agent-based log collection mode, whenever agent is uninstalled, EventLog Analyzer automatically switches to the agent-less mode, to ensure seamless log collection and processing.

Installation Steps

The installation procedure is elaborated below:

1. Navigate to the Admin Settings in the Settings tab, and click on Install Agent link.

2. Enter the device name(s) for which the agent is to be installed. If the device has not yet been added to EventLog Analyzer, it will automatically be added while installing the agent. You can enter multiple devices by separating them with a comma, or alternatively use the Pick Devices link to add multiple devices easily. The Domain Name, which is an optional field, gets automatically populated if you use the Pick Devices option.

   **Note:** Note that an agent can collect logs from up to 25 Windows devices. You can however, freely add or remove devices from an agent.

3. Enter the device’s administrator credentials.

4. Click Verify Login and then click the Install button.

EventLog Analyzer will automatically detect the agents installed on the devices, and obtain the log data in real-time.

**Note:**
The agent(s) can also be installed via GPO with the EventLogAgent.msi file and InstallEventLog.vbs script.

The files are available in the following path:
- `InstallEventLogAgent.vbs` - `<Installation Directory>\ManageEngine\EventLog Analyzer\tools\scripts`
- `EventLogAgent.msi` - `C:\ManageEngine\EventLog\lib\native`

If the agent installation fails due to reasons such as a problem in network connectivity, you can manually install the agent. In this case, you will be prompted in the Agent Administration page to download the MSI file which can be directly installed on the device.

When configuring a device for file integrity monitoring, the agent will be automatically installed in that device.
Agent Administration

The installed agents can easily be managed using the Agent Administration link in the Admin Settings section.

In this page, you can view the devices added to an agent, the status of the agent service, with the option to Start, Stop, and Restart it.

You can also edit or delete the agent, and Add/Remove devices to be monitored by the agent.

Note: Agent Administration cannot be done remotely unless there is an established network connectivity between the agent and EventLog Analyzer server.

Secure log collection

EventLog Analyzer ensures that log collection via agents from your sources is secure. This is achieved by encrypting the data using DES algorithm as well as supporting transport layer security (TLS version 1.2) for communication between the agents and the EventLog Analyzer server.

About EventLog Analyzer

EventLog Analyzer is a comprehensive log management and IT compliance tool for SIEM. The solution provides detailed insights into your log data with audit reports and alert profiles to help mitigate threats and secure your network.

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.