ManageEngine
EventLog Analyzer

A guide to configure agents for log collection in EventLog Analyzer

www.eventloganalyzer.com

Introduction

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

- Agent-less log collection method and
- 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

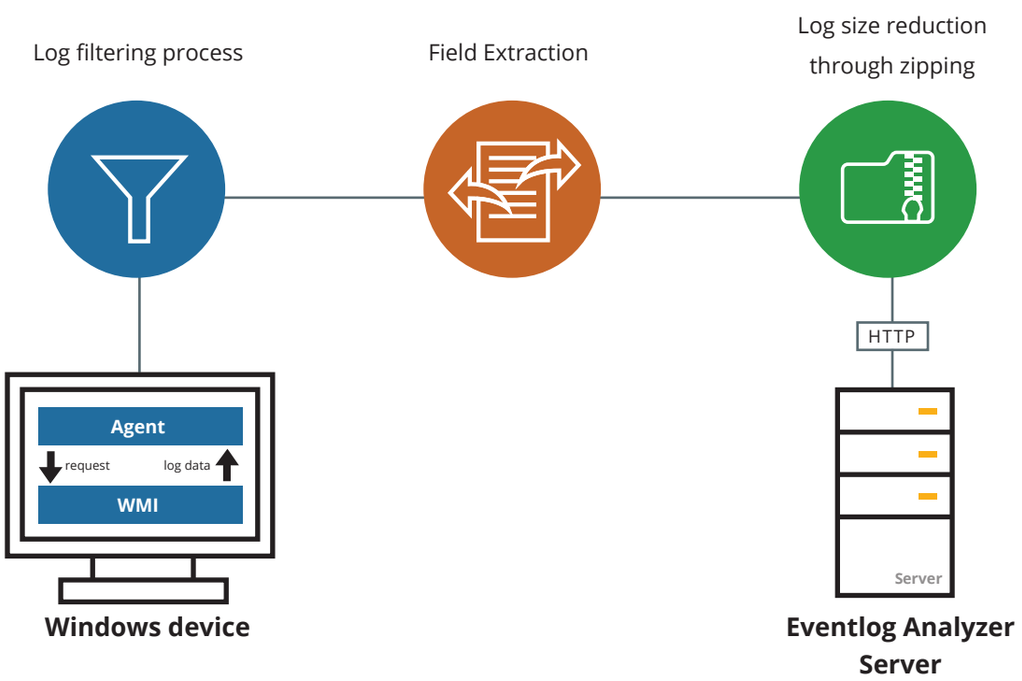
This section illustrates the architecture of the agent-based log collection deployment.

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.



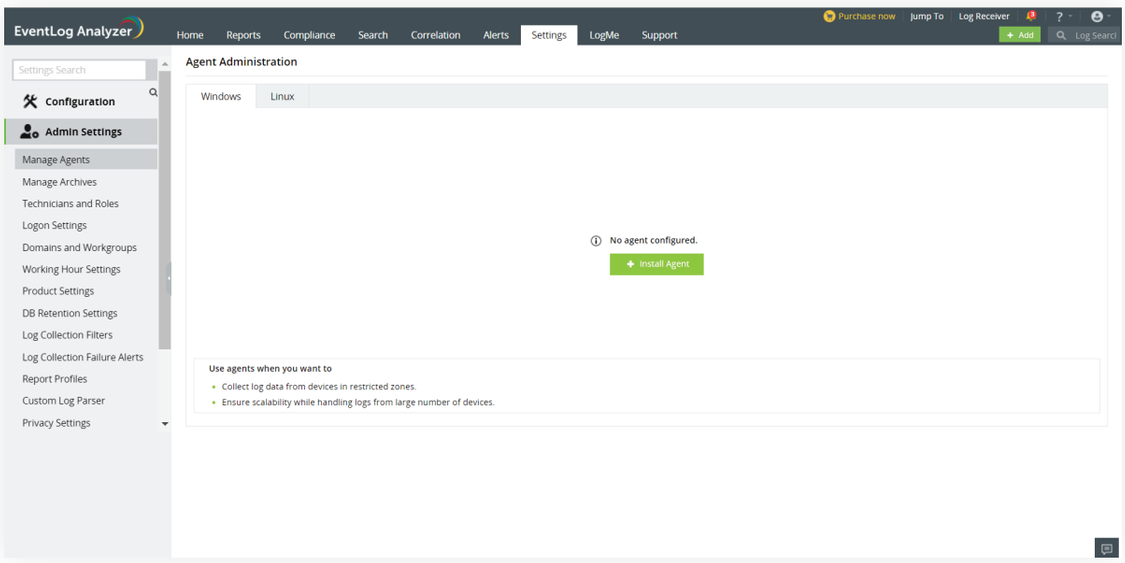
Steps to configure agent-based log collection

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

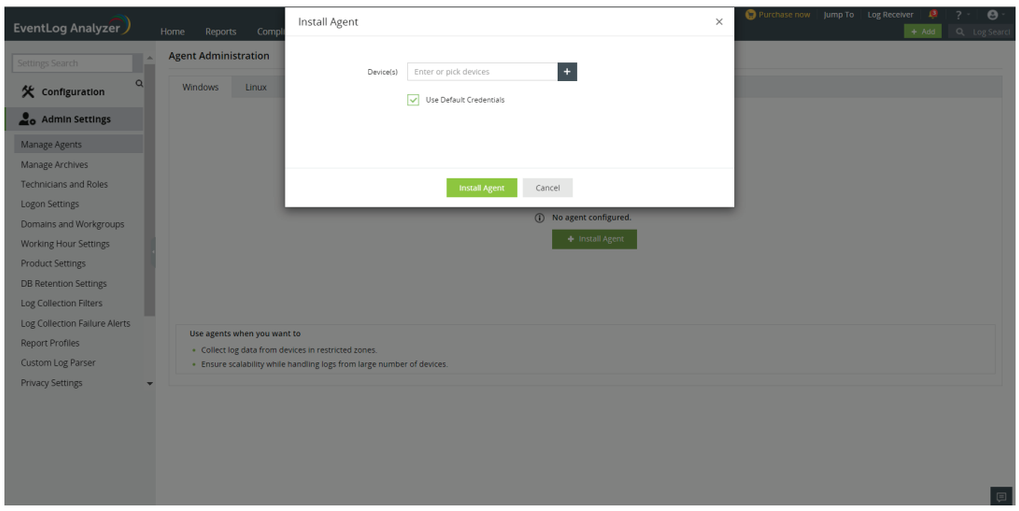
To install the EventLog Analyzer agent, follow the steps given below.

- In the **Settings** tab, navigate to **Admin Settings --> Manage Agents.**
- Click **+ Install Agent** and then the **+** icon corresponding to Device(s).

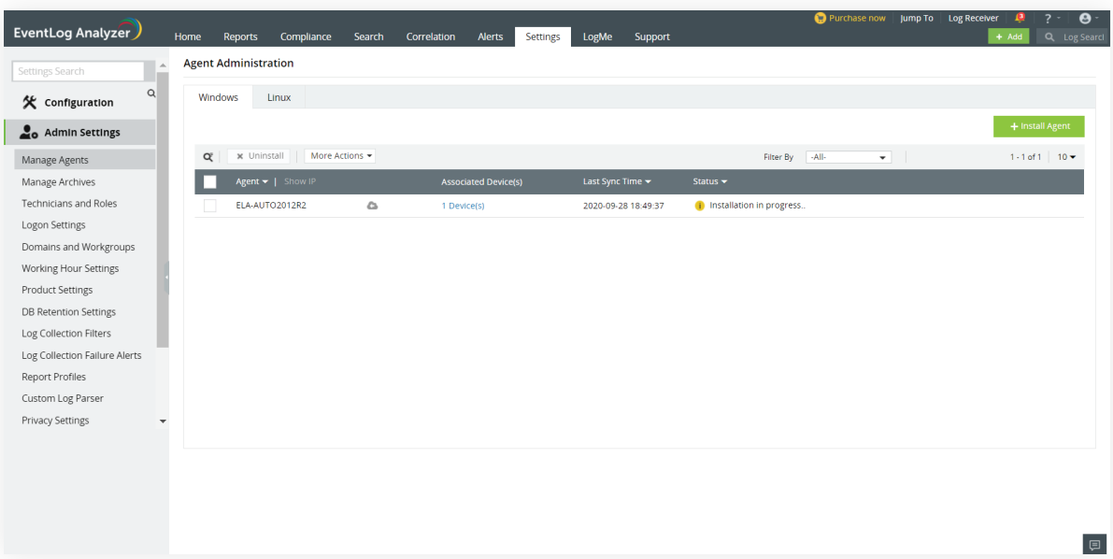


- Select the devices on which you want to install the agent.
- Enter the login name and password to access the device(s). This account should have admin privileges to install the agent successfully. Or you can also choose the **Use Default Credentials** option.

Note: If multiple devices are selected, ensure that the credentials are valid for all the devices.

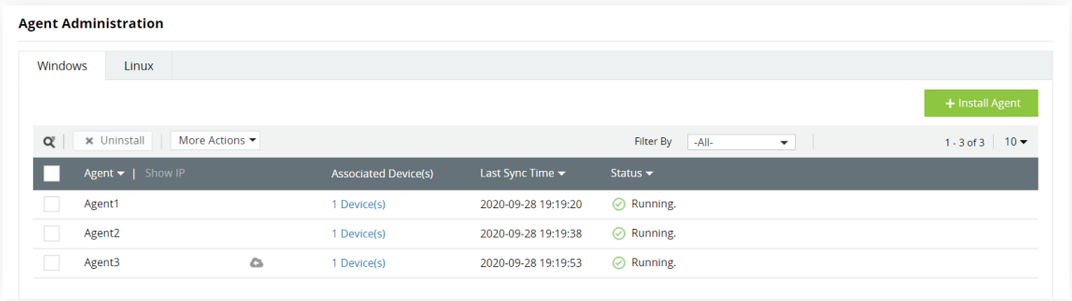


- Use the **Verify Credential** link to validate the credentials entered.
- Finally, click **Install Agent** to initiate agent installation.



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 the log collection from your sources via the agents is secure.

The encryption standards given below are followed by EventLog Analyzer agents of version 4.1 and above which comes bundled with EventLog Analyzer servers of version 12120 and above.

- Confidential data like unique IDs and keys, that are transferred between agents and servers during the initial registration process of the agent, is encrypted with AES algorithm in ECB mode along with integrity checksum SHA256. The keys are further secured using RSA algorithm.
- All other communication between agent and server is encrypted with AES algorithm in ECB mode [SHA256 digest], along with session keys.
- Zip files are password protected, with a different password for each agent, along with SHA 256 integrity checksum.

In EventLog Analyzer agents version 4.0 and below, all communication between agents and servers is encrypted with DES algorithm.

Transport Layer Security version 1.2 is supported in all versions of Eventlog Analyzer.