Vajra Endpoint Detection and Response tool Deployment Guide

Version 1.1
June 2023

Getting Started

The Vajra Endpoint Detection and Response tool leverages the osquery tool that provides endpoint visibility and monitoring. It focuses on osquery-based agent management and offers the following features :

- Detailed visibility into endpoint activities
- Live queries to get real time information
- Alerting capabilities based on security critical events
- Query configuration and management

About this document

This document prescribes how to deploy the Vajra Endpoint Detection and Response tool.

Provisioning the client

The Vajra client that is the part of Endpoint Detection and Response tool, leverages osquery, a multi-platform operating system monitoring and instrumentation framework. Here are the features of Vajra client offers :

- Light weight
- Real time queries

Typically deploying osquery and running it across multiple nodes can be a complicated task, because of its large configuration surface and options. To simplify the deployment of Vajra client, the platform is shipped with a preconfigured package that offers necessary configuration and simplifies client provisioning.

Before you begin

Before you begin make sure the endpoints meet the following system requirements.

- Support 64 bit architecture on Windows 8,10,11 and Linux (Ubuntu, RHEL, CentOS, RPM)
- Do not have installed osquery agent on linux
- Do not have host-based firewalls or other security tools that might interfere with a

remote installation
- Allow outbound TCP traffic on port 1234

Installing the client

On Windows

1. To download the installation script click on [Vajra client]
2. Download the file vajrainstall.ps1
3. Run Powershell as Administrator
4. Run the command

   “`PowerShell.exe -ExecutionPolicy Bypass -File .vajrainstall.ps1`”

5. To uninstall the Vajra client use flag “`-uninstall`”

   Ex : “`PowerShell.exe -ExecutionPolicy Bypass -File .vajrainstall.ps1 -uninstall`”

6. Copy ssl certificate file from server `/path/to/vajra-fleet/ssl/myCA.pem` to client `C:/Program Files/osquery/certs/cert.pem`
7. Change server address where Vajra client should send logs. Add server’s IP/domain in file `C:/Program Files/osquery/osquery.flags`.
8. Replace `<server_ip>` with server’s IP/domain `--tls_hostname=<server_ip>:1234`

   Ex : `--tls_hostname=s3.ieor.iitb.ac.in:1234`

9. Open `Windows>services` find `osqueryd` then `restart`.
10. Now login to the server dashboard using any browser. Go to <server_ip> in the browser and login with the credentials.
11. Going to Nodes page and clicking on 👁 icon go to more details. Give the following configurations to the node in the right hand side configuration panel.
12. Check on `process_open_sockets, listening_ports, logged_in_users, processes, win_process_events, win_socket_events, win_file_events, win_config, chrome_extensions, file` then click on submit
13. You are ready to go

On Linux

1. To download the installation script click on [Vajra client]

2. Download the file vajrainstall.sh
3. Change the file permission to executable “`chmod +x vajrainstall`”
4. Run the command

   “`./vajrainstall`”

5. To uninstall the Vajra client use flag “`-uninstall`”

   Ex : “`vajrainstall -uninstall`”

6. Copy ssl certificate file from server `/path/to/vajra-fleet/ssl/myCA.pem` to client `/etc/osquery/cert.pem`
7. Change server address where Vajra client should send logs. Add server’s IP/domain in file `/etc/osquery/osquery.flags`.
8. Replace `<server_ip>` with server’s IP/domain `--tls_hostname=<server_ip>:1234`

   Ex : `--tls_hostname=s3.ieor.iitb.ac.in:1234`

9. Now restart Vajra client service by running the command on terminal

   ```
   sudo systemctl restart vajra.service
   ```

10. Now login to the server dashboard using any browser. Go to <server_ip> in the browser and login with the credentials.
11. Going to Nodes page and clicking on 👁 icon go to more details. Give the following configurations to the node in the right hand side configuration panel.
12. Check on `process_open_pipes, process_open_files, process_open_sockets, listening_ports, logged_in_users, cpu_time, memory_info, processes, bpf_process_events, bpf_socket_events, bpf_file_events, chrome_extensions, file` then click on submit
13. You are ready to go

Verify the client installation

After you deploy the EclecticIQ Endpoint Response client, complete these steps to verify the installation. When the EclecticIQ Endpoint Response client is installed successfully, the following services and processes start.

Operating System	**Services**

Windows	Osqueryd service vast service vastnw service plgx_win_extension.ext.exe process
Linux	vajra.service

Note : Installation is not successful if any of these services fail to start.

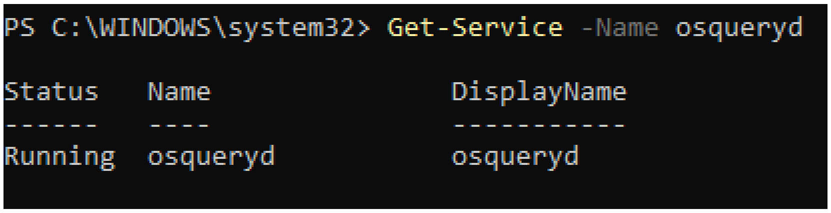
On Windows

Follow these steps to check if the required processes are running.

1. Open the powershell with Administrative privileges
2. Run the following command

   ```
   Get-Service -Name osqueryd
   ```

Review the output to verify the status of Vajra Endpoint Tool.



```
PS C:\WINDOWS\system32> Get-Service -Name osqueryd

Status   Name               DisplayName
------   ----               -----------
Running  osqueryd           osqueryd
```

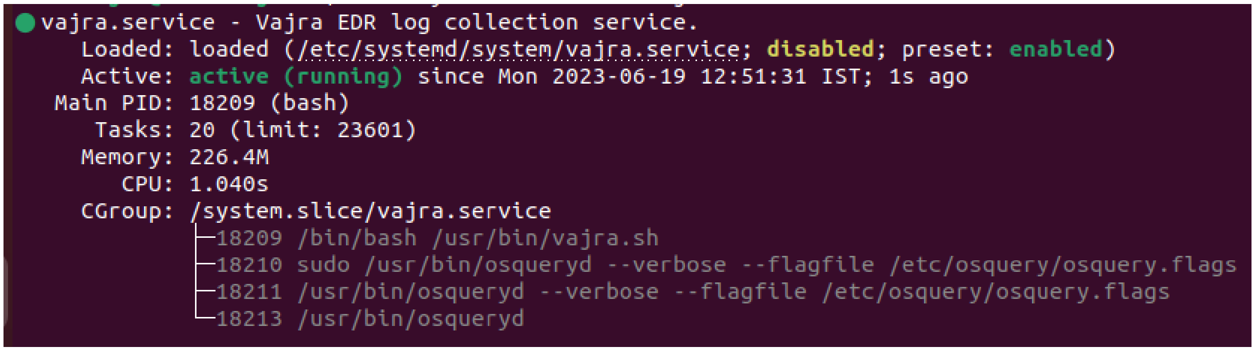
On Linux

Follow these steps to check if the required processes are running.

1. Open the terminal
2. Run the following command

   ```
   systemctl status vajra.service
   ```

Review the output to verify the status of Vajra Endpoint Tool.



```
● vajra.service - Vajra EDR log collection service.
     Loaded: loaded (/etc/systemd/system/vajra.service; disabled; preset: enabled)
     Active: active (running) since Mon 2023-06-19 12:51:31 IST; 1s ago
   Main PID: 18209 (bash)
      Tasks: 20 (limit: 23601)
     Memory: 226.4M
        CPU: 1.040s
     CGroup: /system.slice/vajra.service
             ├─18209 /bin/bash /usr/bin/vajra.sh
             ├─18210 sudo /usr/bin/osqueryd --verbose --flagfile /etc/osquery/osquery.flags
             ├─18211 /usr/bin/osqueryd --verbose --flagfile /etc/osquery/osquery.flags
             └─18213 /usr/bin/osqueryd
```

Uninstall the client installation

On Windows

Complete these steps to uninstall the EclecticIQ ER client.

1. Open a command window with administrative privileges.
2. Close any open instances of the osqueryd, vast, and vastnw services.
3. Close installation directory `"C:\Program Files\plgx_osquery"` if opened in Explorer view or command prompt.
4. Close Event Viewer.
5. Using the command prompt, navigate to the directory where the Vajra client was downloaded.
   This is not the installation directory.
6. Run the uninstall command.
   Here is the syntax to execute the command :

   “`PowerShell.exe -ExecutionPolicy Bypass -File .vajrainstall.ps1 -uninstall`”

On Linux

Complete these steps to uninstall the EclecticIQ ER client.

1. Open a Terminal with root privileges.
2. Using the command prompt, navigate to the directory where the Vajra client was downloaded.

This is not the installation directory.

3. Run the uninstall command.

   Here is the syntax to execute the command :

   ```
   “./vajrainstall -uninstall”
   ```