Troubleshooting the XDR Collector

https://campus.barracuda.com/doc/110560280/

The following are issues that may happen when working with the XDR Collector.

Can I use the Install Command in Multiple Environments?

No. The install command is unique for each account and should only be run on systems within that account's network.

Why is the Install Slow? (PowerShell)

PowerShell downloads can be slow on some systems.

To avoid this, if the system can download the agent zip file from a browser, you can paste the URL from the install command into a browser: https://skout-csd-assets-public-dev.s3.amazonaws.com/xdr-agent/xdr-agent-8.4.2-windows-x86_64.zip

Then, run the rest of the commands from the download directory in order to complete the install.

```
cd .\Downloads\
Expand-Archive .\xdr-agent-8.12.0-windows-x86_64.zip -DestinationPath .
cd xdr-agent-8.12.0-windows-x86_64
.\elastic-agent.exe install --url=https://example.com:443 --enrollment-token=12345
```

Why is the XDR Collector not Communicating?

Ensure the XDR Collector can communicate to the following endpoints/ports.

Logstash	a96190b49bd294a5fbb3725ff20aab78-c7f64fe7557a87d2.elb.us-east-1.amazonaws.com:5044
Management Server	b5e9a5096e0a4f7782cc444c8edbbd5e.fleet.us-east-1.aws.found.io:443
Update Server	artifacts.elastic.co:443

How do I Confirm the Necessary Ports are Open?

To confirm a port is open on Windows

1. On the appropriate system, run Powershell as an administrator.
2. Run any of the following commands:
   ```
   Test-NetConnection a96190b49bd294a5fbb3725ff20aab78-c7f64fe7557a87d2.elb.us-east-1.amazonaws.com -Port 5044
   Test-NetConnection b5e9a5096e0a4f7782cc444c8edbbd5e.fleet.us-east-1.aws.found.io -Port 443
   Test-NetConnection artifacts.elastic.co -Port 443
   ```

> The following is an example success response for `Test-NetConnection artifacts.elastic.co -Port 443`:
>
> ```
> ComputerName     : artifacts.elastic.co
> RemoteAddress    : 34.120.127.130
> RemotePort       : 443
> InterfaceAlias   : Ethernet
> SourceAddress    : 10.6.0.34
> TcpTestSucceeded : True
> ```

To confirm a port is open on Linux

1. On the appropriate system, open a terminal.
2. Run the following command:
   `sudo lsof -i:<000>`, where `<000>` is the port number

How do I Check the Status of the XDR Collector?

To check the status of the XDR Collector on Windows

1. On the appropriate system, open a terminal.
2. cd to the folder where the XDR Collector is installed.
3. Run the following command:
   ```
   .\elastic-agent.exe status
   ```

To check the status of the XDR Collector on Linux

1. On the appropriate system, open a terminal.
2. Run the following command:
   `elastic-agent status`

A healthy status returns the following, or similar:

```
PS C:\Program Files\Elastic\Agent> .\elastic-agent.exe status

┌─fleet

│  └─status: (HEALTHY) Connected

└─elastic-agent
     └─status: (HEALTHY) Running
```

How do I Edit a Config File in Linux?

If you’re having trouble editing a config file in Linux, you can use a text editor such as Nano: https://linuxize.com/post/how-to-use-nano-text-editor/

Barracuda IDS for Windows Issues

Is Suricata Writing Entries in the Log File?

To verify that Suricata is generating new entries in the log file, run the following command in the directory where you installed Suricata (By default, the install folder is \Program Files\Suricata\):

```
Get-Content .\log\eve.json -Wait -Tail 10
```

Why is Suricata/XDR Collector being blocked by my antivirus/endpoint protection software?

Ensure that you have added the executable for both Suricata and XDR Collector to the Allow List in all antivirus and endpoint protection software (except in SentinelOne).

- Suricata: "C:\Program Files\Suricata\suricata.exe"
- XDR Collector: "C:\Program Files\Elastic\Agent\elastic-agent.exe"

What should I do if there are More than 23 Source Ports in the Switch Mirroring Session?

If the number of source ports in the switch mirroring session is greater than or equal to 24, then it is recommended to increase the cache memory of Suricata from the default value of 1MB to 8MB.

What should I do if the IP Address of the Host's Secondary Interface changes?

When using Barracuda IDS for Windows, if the IP address of the host's secondary interface is changed, you will need to stop and delete the Suricata service, then re-install Suricata.

1. To delete the service, run the following command as Administrator:
   `sc.exe delete Suricata`
2. To reinstall Suricata, follow the **To install Suricata** procedure Setting up the XDR Collector for Barracuda IDS for Windows, from Step 2 on. You don't need to repeat Step 1.

Barracuda IDS for Linux Issues

How do I Edit the Host Machine's Secondary Interface in the Configuration File?

1. To open the suricata.yaml configuration file in Nano, open a terminal on the appropriate system and run the following command:
   `sudo nano /etc/suricata/suricata.yaml`.
2. To search for `af-packet`, press CTRL+W.
3. Next to `interface:`, press the spacebar, then enter the secondary network interface.
   > **Example** For example, if the secondary network interface is eth0, the code should read:
   > ```
   > af-packet:
   >   - interface: eth0
   > ```
4. To save the file, press **CTRL** + **O**.
5. To exit, press **CTRL** + **X**.