Setting up the Barracuda XDR Collector for Barracuda IDS for Linux

https://campus.barracuda.com/doc/30234/

This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating Barracuda IDS.

The XDR Collector runs as a service in your environment. While the minimum specifications are listed below, the required resources depend on the number of active integrations and the amount of data being processed.

Minimum requirements

To set up the XDR Collector, the minimum requirements are the following:

Minimum requirements	
CPU	2vCPU
Disk Size	10GB SSD
Memory	1GB
Network interface cards (NICs)	2

For Barracuda IDS/Suricata, the host must have 2 Network Interface Cards. One to monitor span traffic and one for host traffic.

Operating System

- Ubuntu 22.04 (Recommended)
- For other versions, see the Elastic Agent 8.12.x row in the Elastic Agent table on this page.

Required Endpoint/Port Communication

The XDR Collector must be able to communicate to the following endpoints/ports:

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

Dedicated Host Requirements

Barracuda IDS/Suricata requires that the collector run in a dedicated host.

Setting up the XDR Collector for Linux for Barracuda IDS

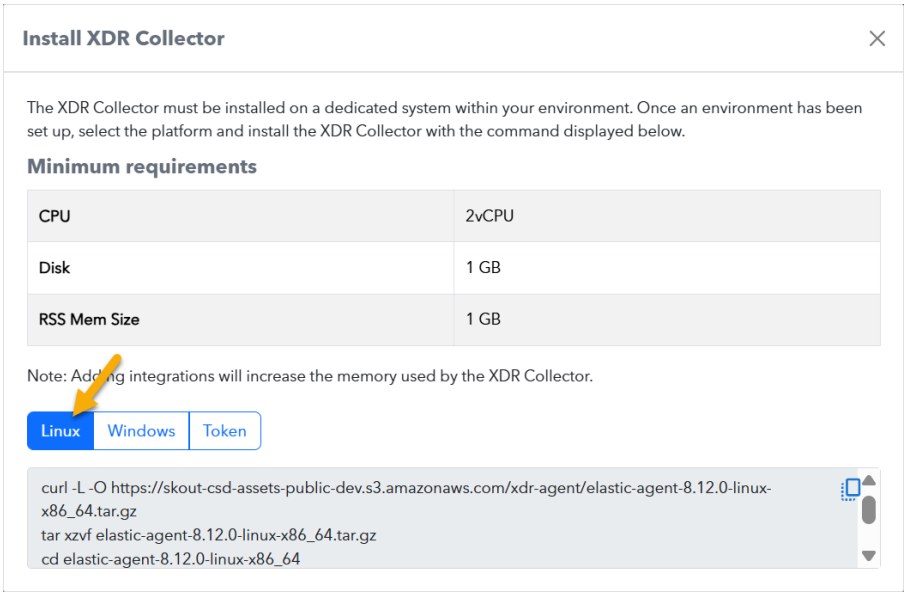
To set up the XDR Collector for Linux, perform the following procedures:

- To install the XDR Collector
- To set up switch port mirroring
- To edit the Suricata configuration

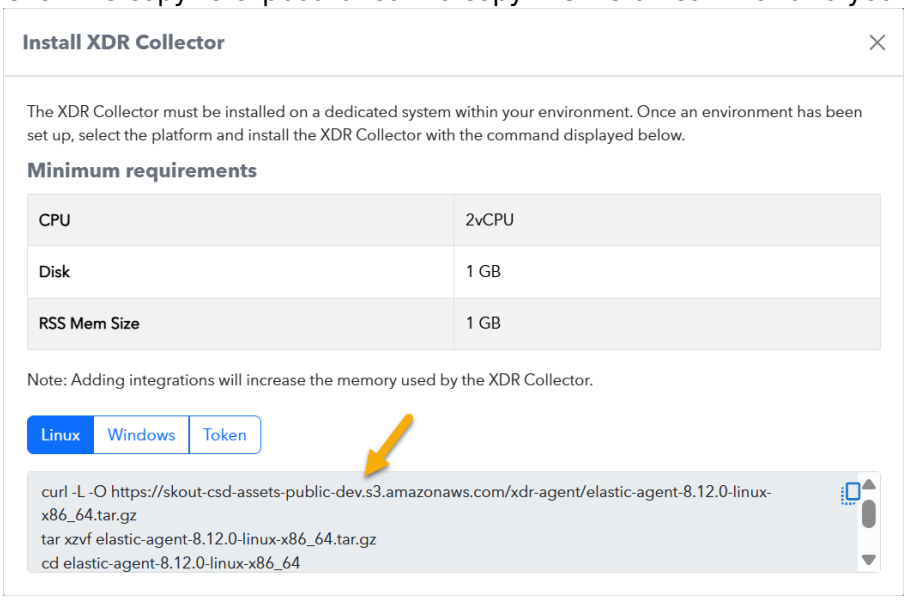
To install the XDR Collector

> The install command is unique to the current selected account and should only be run on systems within that environment.

1. In Barracuda XDR Dashboard, click **Infrastructure** > **Collectors**.
2. In the **Policies** table, next to the on-prem policy, click **Action** > **Install**.
3. Click **Linux**.



4. Click the copy to clipboard icon to copy the install command to your clipboard.



5. Open a terminal on the appropriate system, paste the command, and run it.

To set up switch port mirroring

Click a link for specific configurations for the following:

- Configuring Port Mirroring on VMWare
- Configuring Port Mirroring on Hyper-V

1. Connect the secondary Ethernet interface on the XDR Collector's host machine to the mirrored port on the switch.
2. Configure the switch to mirror traffic in both directions on all other ports on the switch.

Checking the Status of the Barracuda XDR Elastic Collector

To check the status of the XDR Collector, open a terminal and run the following command:
`elastic-agent status`

Installing Suricata

These instructions are also available at Installing Suricata on Linux for the XDR Collector .

To install Suricata, follow the procedure for your environment (below):

- To install Suricata on Ubuntu/Debian
- To install Suricata on RHEL/CentOS/Rocky/Alma/Fedora

To install Suricata on Ubuntu/Debian

1. To run the install script, copy and run the following commands:
   ```
   sudo mkdir -p "/usr/local/bin/suricata"
   sudo bash -c 'curl -L
   "https://skout-csd-assets-public.s3.amazonaws.com/suricata/linux/suricat
   a-scripts.tar.gz" | tar -xz -C "/usr/local/bin/suricata"'
   sudo find "/usr/local/bin/suricata" -type f -exec chmod +x {} \;
   cd /usr/local/bin/suricata
   sudo ./install.sh
   ```
2. Follow the prompts through the configuration.

To install Suricata on RHEL/CentOS/Rocky/Alma/Fedora

1. To run the install script, copy and run the following commands:
   ```
   sudo dnf update -y
   sudo dnf install suricata
   sudo suricata-update
   ```
2. Enable the Suricata service by running the following:
   ```
   sudo systemctl enable suricata.service --sudo bash -c 'curl -L
   "https://skout-csd-assets-public-dev.s3.us-east-1.amazonaws.com/suricata
   /linux/7.0.7/default/suricata-xdr-update.tnow
   ```
3. Copy and run the following commands to download the configuration file:
   ```
   sudo mkdir -p "/usr/local/bin/suricata"
   sudo bash -c ‘curl -L
   “https://skout-csd-assets-public.s3.us-east-1.amazonaws.com/suricata/lin
   ux/7.0.7/default/suricata-xdr-update.tar.gz” | tar -xz -C
   ```

```
sudo mv /usr/local/bin/suricata/suricata.yaml
/etc/suricata/suricata.yaml
sudo mv /usr/local/bin/suricata/disable.conf /etc/suricata/disable.conf
```

4. Set the HOME_NET and interface values in the configuration file:
   - 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`
   - To search for HOME_NET, press CTRL+W.
   - Next to HOME_NET:, modify the subnet(s) of your internal networks in cidr format.
   - For example, if the subnet to be monitored is 192.168.0.0/16, the configuration should read: HOME_NET: "[192.168.0.0/16]"
   - To search for af-packet, press CTRL+W.
   - Next to interface:, press the spacebar, then enter the secondary network interface. For example, if the secondary network interface is eth1, the configuration should read:
     ```
     af-packet:
     - interface: eth1
     ```
5. To create the log cleanup and suricata-update cron jobs, from the terminal open crontab with nano, do the following:
   - Type sudo EDITOR=nano `crontab -e`
   - Add a cronjob that runs hourly and delete log files older than 3 hours, and a cronjob that runs daily to update the rules:
     ```
     0 * * * * find /var/log/suricata/ -name "*.json" -mmin +180 -delete
     0 2 * * * suricata-update
     ```
   - To save the file, press CTRL + O.
   - To exit, press CTRL + X.
6. Restart the Suricata service:
   `sudo systemctl restart suricata.service`

Suricata should now be running in the background. To verify that Suricata is generating new entries in the log file, run the following command:
`ls -t /var/log/suricata/*.json | head -n 1 | xargs tail -f`

To trigger a manual alert for threat simulation

In order to trigger a test alert, run the following command from any system within your network:
`curl http://testmynids.org/uid/index.html`

To uninstall Suricata

To uninstall Suricata, follow the procedure for your environment (below):

- To uninstall Suricata on Ubuntu/Debian
- To uninstall Suricata on RHEL/CentOS/Rocky/Alma/Fedora

To uninstall Suricata on Ubuntu/Debian

1. Run the following commands:
   ```
   cd /usr/local/bin/suricata
   sudo ./uninstall.sh
   ```

To uninstall Suricata on RHEL/CentOS/Rocky/Alma/Fedora

1. Run the following command:
   ```
   sudo dnf remove suricata
   ```
2. To remove the log cleanup and suricata-update cron jobs, from the terminal open crontab with nano:
   - Type sudo EDITOR=nano crontab -e
   - Remove the following entries:
     ```
     0 * * * * find /var/log/suricata/ -name "*.json" -mmin +180 -delete
     0 2 * * * suricata-update
     ```
3. To save the file, press CTRL + O.
4. To exit, press CTRL + X.

Figures