

Setting up the Barracuda XDR Collector for Barracuda IDS for Linux

https://campus.barracuda.com/doc/104369320/

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.

Install the XDR Collector on each server you want to monitor.

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.

IP Address requirements

Two private static IP addresses are required, one for each Ethernet interface.



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
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 configure a static IP address
- To install the XDR Collector
- To set up switch port mirroring
- To edit the Suricata configuration

To configure a static IP address

• Configure a static IP address for each Ethernet interface. See <u>Configuring a Static IP in Ubuntu</u>.

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.

Barracuda XDR



ne XDR Collector must be installed on a dedicate et up, select the platform and install the XDR Coll	d system within your environment. Once an environment has been ector with the command displayed below.
linimum requirements	
CPU	2vCPU
Disk	1 GB
RSS Mem Size	1 GB
ote: Addir Constraints will increase the memory	ry used by the XDR Collector.

4. Copy the command at the bottom of the dialog box.

Install XDR Collector			
The XDR Collector must be installed on a dedicated system set up, select the platform and install the XDR Collector with Minimum requirements	within your environment. Once an environment has been the command displayed below.		
CPU	2vCPU		
Disk	1 GB		
RSS Mem Size	1 GB		
Note: Adding integrations will increase the memory used b	y the XDR Collector.		
Linux Windows			
curl -L -O https://skout-csd-assets-public-dev.s3.amazona x86_64.tar.gz tar xxvf elastic-agent-8.12.0-linux-x86_64.tar.gz cd elastic-agent-8.12.0-linux-x86_64	ws.com/xdr-agent/elastic-agent-8.12.0-linux-		

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

To set up switch port mirroring

- 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

To install Suricata

- If using Ubuntu, add the Suricata repository: sudo add-apt-repository ppa:oisf/suricata-stable
- 2. Update and install Suricata.
 - For **Ubuntu/Debian**, run the following:



```
sudo apt-get update
        sudo apt-get install suricata
      • For RHEL/CentOS/Rocky/Alma/Fedora, run the following:
        sudo dnf update -y
        sudo dnf install suricata
           For RHEL/CentOS/Rocky releases, the EPEL repository must be enabled
3. Enable the Suricata service by running the following:
  sudo systemctl enable suricata.service -- now
4. Set the host machine's secondary interface in the configuration file, by doing the following:
      • 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 af-packet, press CTRL+W.
      • 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
      • To save the file, press CTRL + O.
      • To exit, press CTRL + X.
5. To add the log rotate configuration, do the following:
      • Search for eve-log, press CTRL+W.
      • Add the filename and rotate-interval settings.
          The final format looks like the following.
           - eve-log:
                  enabled: yes
                  filetype: regular
          #regular|syslog|unix dgram|unix stream|redis
                  filename: eve-%Y-%m-%d-%H:%M:%S.json
                  rotate-interval: 30m
6. To update the stats interval configuration, do the following:

    Search for stats, press CTRL+W.

      • Change the interval setting. The final format will look like this:
           stats:
             enabled: yes
             # The interval field (in seconds) controls at what interval
             # the loggers are invoked.
             interval: 86400
7. To create the log cleanup cron job, from the terminal open crontab with nano, do the following:

    Type sudo EDITOR=nano crontab -e

      • Add a cronjob which will run hourly and delete log files older than 90 minutes:
        0 * * * * find /var/log/suricata/ -name "*.json" -mmin +90 -delete
      • To save the file, press CTRL + O.
      • To exit, press CTRL + X.
8. Restart the Suricata service by doing the following:
```

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 in the same directory where you installed Suricata:

sudo tail -f /var/log/suricata/eve.json

Barracuda XDR



Figures

- 1. InstallXDRCollectorDialog1.png
- 2. InstallXDRCollectorDialog2.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.