Setting up the XDR Collector for Barracuda IDS for Windows

https://campus.barracuda.com/doc/104380077/

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 card (NICs)	2

Operating System

- Windows Server 2016 and higher
- Windows 10 and higher

Windows Server 2022 is recommended.

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

Setting up the XDR Collector

To set up the XDR Collector, you must do the following procedures:

- To configure a static IP address
- To install the XDR Collector
- To set up switch port mirroring
- To install Suricata
- To create the log cleanup scheduled task

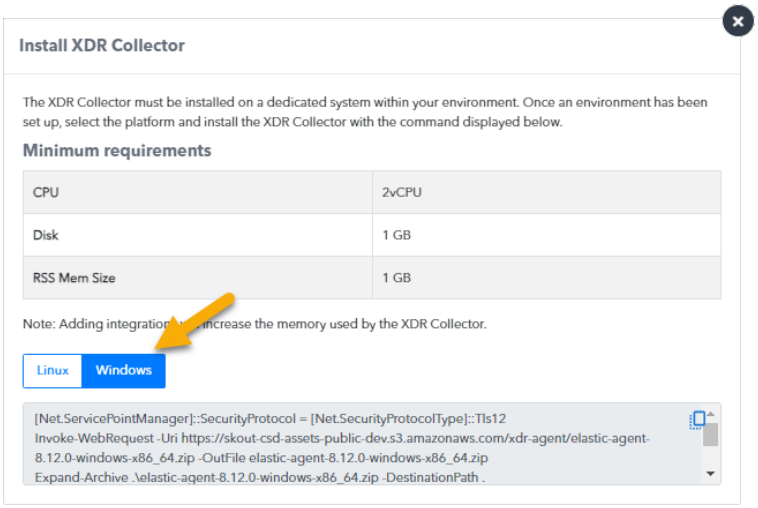
To configure a Static IP Address

Configure a static IP address for each Ethernet interface. See the documentation for your specific version of Windows.

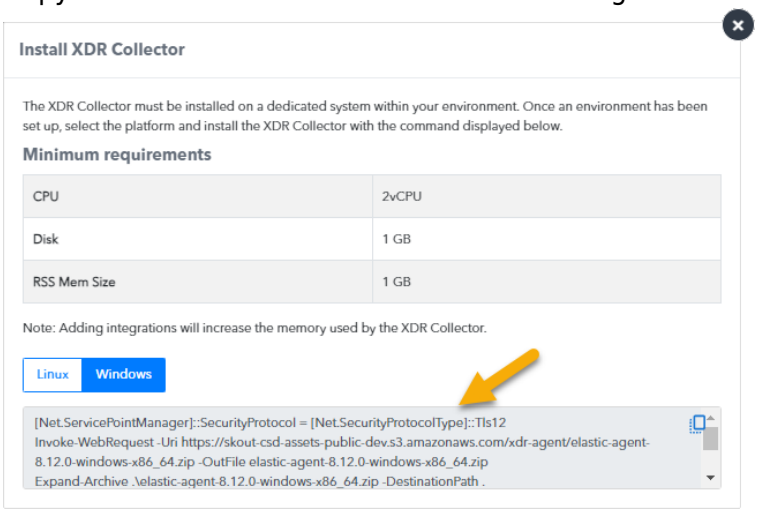
To install the XDR Collector

> The install command is unique for each account and should only be run on systems within that account's network.

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



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



5. On the appropriate system, run Powershell as an administrator, paste the command, and run it.

It may take up to 30 minutes for the install to complete.

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.

To install Suricata

1. Download and install NPCAP (https://npcap.com/#download)
   NPCAP allows Windows software to capture raw network traffic.
2. Download and install Suricata from https://suricata.io/download/

3. As Administrator, open PowerShell and navigate to the Suricata installation directory (C:\Program Files\Suricata)
4. Open suricata.yaml in a text editor and change the stats interval to 86400.

   The file will look like the following:

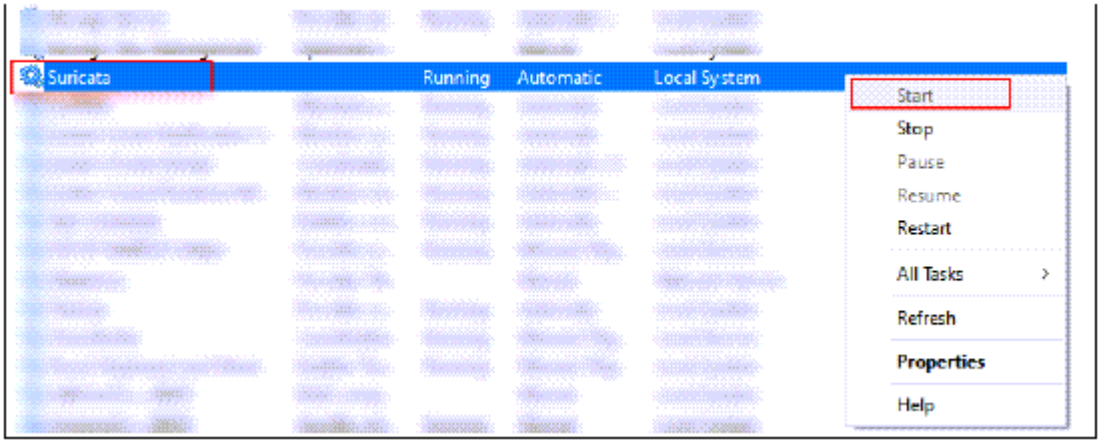
```
stats :
   enabled : yes
   # The interval field (in seconds) controls at what interval
   # the loggers are invoked.
   interval : 86400
```

5. Add the filename and rotate-interval under outputs eve-log.

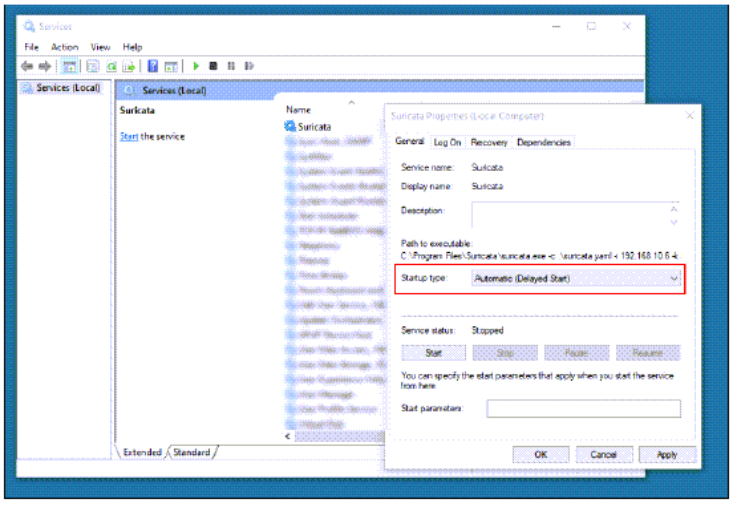
   The file will look like the following:

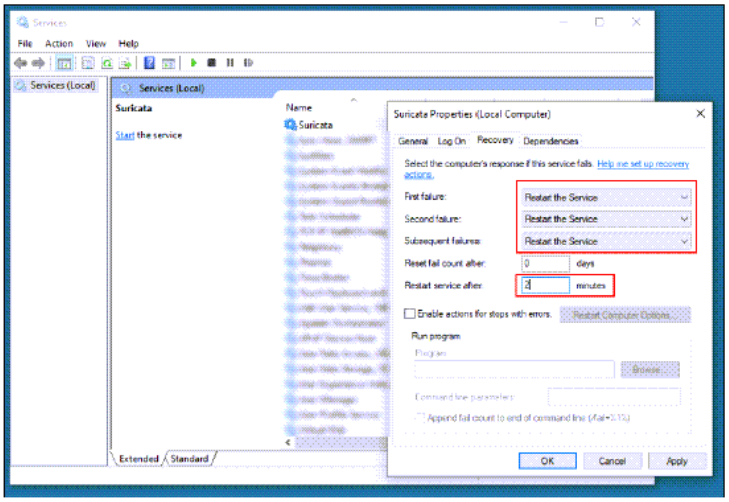
```
- eve-log :
   enabled : yes
   filetype : regular
   filename : eve-%Y-%m-%d-%H%M%S.json
   rotate-interval : 60m
```

6. Save the file.
7. Install the Suricata service with the following option:
   `.\suricata.exe -c .\suricata.yaml -i <X.X.X.X> --service-install`
   Where <X.X.X.X> is the IP address of the host machine's port connected to the switch port-mirroring destination port.
8. While keeping the PowerShell terminal active, open the services.msc interface and start the Suricata service



9. In services.msc, set the Suricata service properties startup type to "**Automatic (Delayed Start)**" and the recovery options to "**Restart the Service**" after 2 minutes.





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 directory where you installed Suricata

(By default, the installation directory is C:\Program Files\Suricata\):

```
Get-Content Get-ChildItem -Path "C:\Program Files\Suricata\log" -Filter
"*.json" | Sort-Object LastWriteTime -Descending | Select-Object -First
1 | Get-Content -Tail 10 -Wait
```

To create the log cleanup scheduled task

This script removes log files older than 30 minutes and creates a scheduled task to execute log removal every 90 minutes.

1. Download the PowerShell script and move it to `C:\Program Files\Suricata\ .`
2. Open PowerShell as an Administrator and run the following:
   `& "C:\Program Files\Suricata\suricata-log-rotate.ps1"`

To delete the scheduled task and cancel the script. run the following:

```
Unregister-ScheduledTask -TaskName "SuricataLogRotateTask" -
Confirm:$false
```

Important Notes

- 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.
- Add 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"
- Do not upgrade either Suricata or the XDR Collector without confirmation from XDR support as this may result in configuration discrepancies. Barracuda XDR Collector upgrades are managed by Barracuda Networks.
- If the IP address of the host's secondary interface is changed, stop and delete the Suricata service, then repeat step 2. To delete the service, run the following command as Administrator:
  `sc.exe delete Suricata`

Figures