

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.

Barracuda XDR



ne XDR Collector must be installed on a c et up, select the platform and install the X	edicated system within your environment. Once an environment has been DR Collector with the command displayed below.
linimum requirements	
CPU	2vCPU
Disk	1 GB
RSS Mem Size	1 GB
tinux Windows	memory used by the XDR Collector.
[Net.ServicePointManager]::SecurityProt Invoke-WebRequest -Uri https://skout.cs	ocol = [Net.SecurityProtocolType]::Tls12

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

nstall XDR Collector	
The XDR Collector must be installed on a dedicated system set up, select the platform and install the XDR Collector wit Minimum requirements	n within your environment. Once an environment has been h 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.
[Net.ServicePointManager]::SecurityProtocol = [Net.Secu Invoke-WebRequest -Uri https://skout.csd-assets-public- 8.12.0-windows-x86_64.zip -OutFile elastic-agent-8.12.0 Expand-Archive .\elastic-agent-8.12.0-windows-x86_64.z	rityProtocolType]::TIs12 dev.s3.amazonaws.com/xdr-agent/elastic-agent- windows-x86_64.zip ip -DestinationPath .

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 (<u>https://npcap.com/#download</u>) 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 portmirroring destination port.

8. While keeping the PowerShell terminal active, open the services.msc interface and start the Suricata service



	an a		and the state		
🚳 Suricata		Running	Automatic	Local System	
sector of the se	and the second second	1	1. Sec. 1. Sec. 1.		Start
					Stop
					Pause
an an ar					Resume
					Restart
anne anne anne anne anne anne anne anne					All Tasks >
A LONG					Refresh
					Properties
alle i alle					Help

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.

Q. Services				- 🗆 X
File Action View	Help			
🗢 🔿 📅 🔯 j	a 🔒 🛛 📷 🕨 🗰 🛤 🕬			
Services (Local)	Ci Services (Local)			n proprovoko konstruktura k
	Suricata	Name	Suricata Pronomes di cocar Cr	meeter) ×
	Start the service	🔕 Suricata		
		and the second sec	General Log On Recovery	Dependencies
		Average in specific strengther	Service name: Suricata	
		Summer Scotter Reading	Display name: Suricata	
		See conserve	Description	Ô
		TOTAL SAMPLES AND	Path to even table	
		Nacos	C/VProgram Files/Suncata/s	inicataliene -c. \suricata yarrii -i 192.168.10.5 4:
		Times (Briang)	Startup type: Automat	c (Delayed Start)
		and the former and		
		Constant Constanting	Second status - Discussi	
		ANY BUDDING	Service status - Stupped	
		and the second states	3/34	ROOM INTERPOSE SUCREMENTE
		Second Statements (2005)	You can specify the start par from here.	aneters that apply when you start the service
		Case Profile Service	Stat parameters	
	Extended Standard	• 2000000000000000000000000000000000000		OK Cancel Apply
Services File Action View	Help			- D X
🔕 Services (Local)	(), Services (Local)			
	Suricata	Name	Suricate Properties (Local ((arrested)
	Start the service	🕰 Suricata	Sencere Properties (cocer o	
		a and an and a second sec	General Log On Fecover	V Dependencies
			Select the computer's response	inse if this service fails. Help me set up recovery
		a states dependentes de proj	First failure:	Restart the Service
		Seale Vertexitedae	Second failure:	Restat the Service V
		and a subsection of the	Subsequent failures	Restat the Service V
		Angenes,	Subsequent failures: Reset fail count after	Restart the Service
		 And an application application Appendix Application Application Application 	Subsequent failures: Reset fail count alter: Restat service after	Restart the Service
		 All in application application Application Application Application Application Application Application Application 	Subsequent failurea: Reset fail count after: Restart service after:	Restart the Service v 0 Geys 2 mmutes
		 State and approximate approximate approximate approximate approx	Subsequent failures: Reset fail count after: Restart service after: Enable actions for stops	Restart the Service V 0 deyn 2 minutes with errors Restart Computer Options
		 All an application Magniture; Magniture; Sourchinate; Non-Anatos; Magniture; Non-Anatos; Magniture; Sourchinate; 	Subsequent failures: Reset fail count alter: Restart service after Enable actions for stops Run program	Restat the Service 0 dept 1 minutes wd1 errors Bastart Computer Databast
		 Alto an Agginetic reage Altophicale; Altophicale;	Subsequent failures: Reset fail count after Restart service after Ensible ections for stops Run program Program	Peter the Service v den den den den den den den de
		 Mich de l'auguste de la segure de la segure	Subsequent failures: Reset fail count after Restart service after Ensible ections for stops Run program Program	Petter the Service v den den den den den den den den den de
		 Marcine and Annual Consequences Marriere Marriere	Subsequent failures Reset fail count after: Restart service after: Bristart service after: Bristele ectors for stops Run program Program Program Common Size paramoles Common Size paramoles	Pestart the Service v Generation Generation Methods M
		 Markov Standards Annales Marrison Marrison	Subsequent failures Resettal count after: Restat service after Bradle actions for stops Rup program Dicipies Contrand fore paramete	Peckat the Service v 0 den (1) mmuten wfb: errors. Restart Clanolizer Options. v Stanner. v Stanner.
		 And an installation regardless of the second second	Subsequent fielumes Reset fail count affect Restat service affect Brable actions for stops Fun program Program Connand fice paramete Connand fice paramete Program Connand fice paramete	Restor the Service V 0 den 3 minutes wB1 errors Bissistic Canadian Colonian arror Bissistic Canadian Colonian

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 <u>PowerShell script</u> 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

Barracuda XDR



Figures

- 1. WindowsInstallXDRCollector1.png
- 2. WindowsInstallXDRCollector2.png
- 3. Pic 1.png
- 4. Pic 2.png
- 5. Pic 3.png
- 6. Pic 4.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.