



**Integration Guide** 

# Integrate Amazon Route 53 with Netsurion Open XDR

**Publication Date** July 18, 2023



# Abstract

This guide provides instructions to configure and integrate Amazon Route 53 with Netsurion Open XDR to retrieve its logs and forward them to Netsurion Open XDR.

#### Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

# Scope

The configuration details in this guide are consistent with AWS CloudTrail and Netsurion Open XDR 9.3 or later.

# Audience

This guide is for the administrators responsible for configuring and monitoring Amazon Route 53 in Netsurion Open XDR.



# Table of Contents

| 1 | Ove  | erview   | 4 |
|---|------|--|---|
| 2 | Pre  | requisites                                       | 4 |
| 3 | Syst | tem Extraction                                   | 4 |
| 4 | Inte | egrating Route 53 with Netsurion Open XDR        | 4 |
| 5 | Dat  | a Source Integration (DSI) in Netsurion Open XDR | 7 |
| 5 | 5.1  | Reports  | 7 |
| 5 | 5.2  | Dashboards                                       | 7 |
| 5 | 5.3  | Saved Searches                                   | 7 |



# 1 Overview

Route 53 is a DNS service in AWS that connects the internet traffic to appropriate servers hosting the requested web application.

Netsurion Open XDR manages logs retrieved from Amazon Route 53. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Amazon Route 53.

## 2 Prerequisites

Root level access to the <u>AWS</u> console.

# 3 System Extraction

Perform the following process for system extraction.

- 1. In Netsurion Open XDR, hover over the Admin menu and click Manager.
- In the Manager interface, go to syslog/ Virtual Collection Point > syslog, hover over the Gear icon located adjacent to it, and then click Extract device id for extracting the system name.
  - Extract the system name using the below regex:

Fill in the following details, (for CloudTrail logs)

- a. Regular expression: (?is)Organisation:(?P<computer>.\*?),
- b. Token Name: Computer-Route53
- 3. After providing the regex details, click the Update button to save the extraction logic details.

# 4 Integrating Route 53 with Netsurion Open XDR

Before forwarding the logs, it is required to enable DNS query logging.

1. Log in to AWS Management console and go to <u>Route 53</u>.

| Dashboard   | Route 53 Dashboard Inte  |   |  |  |
|---|--|---|--|--|
| Hosted zones<br>Health checks<br>IP-based routing<br>CIDR collections | DVS management Availability monitoring and the first synamic and t | g Domain registration were resources, and A domain is the name, such as example.com, that your users use access your application. Register domain |  |  |
| Traffic policies<br>Policy records                                    | Register domain  | More resources 🕑  |  |  |
| Domains<br>Registered domains<br>Pending requests                     | Field and register an available domain, or transfer your existing domains to Boots 51.  Inter a domain name  | Documentation<br>API inference  |  |  |
| esolver<br>PCs  | ter tand and je belown dog un nig is to downer on year our rate our rate our rate our rate our our source angle 20 downer model was night owner our year our owner owner owner our owner owner owner owner owner owne   | FAQs Forum - DHS and health checks  |  |  |
| utbound endpoints<br>eles<br>wery logging                             | Notifications         C           Q. Pad embrations         < 1 >  | rorum - Domain name registration<br>Request a limit increase  |  |  |
| NS Firewall   | Resource Status Last update v  | Service health  |  |  |
| ale groups<br>ornain lists  | No notifications to display  | To view the current status of Route 55, see the AWS Service Health Dashboard 🗷  |  |  |
| plication Recovery Controller 🖸                                       |  |   |  |  |
| alteb to add company  |  |   |  |  |

- 2. In the Route 53 navigation pane, click the **Resolver** drop-down, and then click **Query logging**.
- 3. In the Query logging pane, click Configure query logging.



#### Note

Choose an existing log group or create a new log group.

| Dashboard                     | (i) You are sign | ned in to the fol | lowing Regi  | on: us-east-1 (M | N. Virgin | iia)             |    |                 |           |   |                |      |                             |
|-------------------------------|------------------|-------------------|--------------|------------------|-----------|------------------|----|-----------------|-----------|---|----------------|------|-----------------------------|
| Hosted zones<br>Health checks | To change y      | our Region, use t | the Region s | elector in the u | pper-rig  | nt corner.       |    |                 |           |   |                |      |                             |
| ID-based couting              | Ouery logging    | a configurati     | ons (1) ter  | 0                |           |                  |    |                 |           | Ε | C View details | Dele | Configure query logging     |
| IDR collections               | Q Search         |                   |              |                  |           |                  |    |                 |           |   |                |      | (1)                         |
| Traffic flow                  |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| raffic policies               | Name             | ▲ ID              | 4            | Status           | 4         | Destination type | Δ. | Destination ARN | VPC count | 4 | Sharing status | 4    | Creation time (UTC)         |
| olicy records                 |                  |                   |              | @ Created        |           | CloudWatch Loos  |    |                 | 0         |   | Not shared     |      | 2021-07-30706-38:13 4341047 |
| omains                        |                  |                   |              | 0                |           |                  |    |                 |           |   |                |      |                             |
| egistered domains             |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| ending requests               |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| solver                        |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| G                             |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| oound endpoints               |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| tbound endpoints              |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
|                               |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| es                            |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| es<br>ery logging             |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |
| ery logging<br>IS Firewall    |                  |                   |              |                  |           |                  |    |                 |           |   |                |      |                             |

- 4. In the Configure query logging window, the configuration name for Query logging.
- 5. In the Query logs destination, choose CloudWatch Logs log group.

| Query logging configuration  | name  |  |
|--|---|--|
| Name<br>A friendly name lets you find a Resolver quer  | y logging configuration in the dashboard.   |  |
| MyConfiguration  |   |  |
| The name can have up to 64 characters. Valio   | d characters: A-Z, a-z, 0-9, space, _ (underscore) a  | and - (hyphen)   |
| Resolver can save logs in CloudWatch Logs, i   | n an S3 bucket, or in Kinesis Data Streams.   |  |
| Resolver can save logs in CloudWatch Logs, i<br>Destination for query logs<br>Choose where you want Resolver to publish  | n an S3 bucket, or in Kinesis Data Streams.<br>query logs. Standard storage charges apply.  |  |
| Resolver can save logs in CloudWatch Logs, i<br>Destination for query logs<br>Choose where you want Resolver to publish o<br>CloudWatch Logs log group<br>You can analyze logs with Logs<br>Insights and create metrics and<br>alarms.   | n an S3 bucket, or in Kinesis Data Streams.<br>query logs. Standard storage charges apply.<br>S3 bucket<br>An S3 bucket is economical for<br>long-term log archiving. Latency<br>is typically higher.   | <ul> <li>Kinesis Data Firehose<br/>delivery stream<br/>You can stream logs in real time<br/>to Elasticsearch, Redshift, or<br/>other applications.</li> </ul>                      |
| Resolver can save logs in CloudWatch Logs, i<br>Destination for query logs<br>Choose where you want Resolver to publish of<br>CloudWatch Logs log group<br>You can analyze logs with Logs<br>Insights and create metrics and<br>alarms.<br>CloudWatch Logs log groups<br>You can either choose a CloudWatch Logs log<br>logging configuration. | n an S3 bucket, or in Kinesis Data Streams.<br>query logs. Standard storage charges apply.<br>S3 bucket<br>An S3 bucket is economical for<br>long-term log archiving. Latency<br>is typically higher.<br>g group that was created by the current account, | Kinesis Data Firehose<br>delivery stream<br>You can stream logs in real time<br>to Elasticsearch, Redshift, or<br>other applications. or choose to create a log group for this que |



|  | Add VPC                     |        |        |            |           |   |           |   |   |       |   |
|--|-----------------------------|--------|--------|------------|-----------|---|-----------|---|---|-------|---|
| <b>Q</b> Search                              |                             |        |        |            |           |   |           | < | 1 | >     | 0 |
| VPC ID                                       | VPC                         | name ⊽ | Status | ▽          | IPV4 CIDR | V | IPV6 CIDR | ▽ |   | Owner |   |
|  |                             |        | Ν      | lo VPCs    |           |   |           |   |   |       |   |
|  |                             |        | No VP  | Cs to disp | olay      |   |           |   |   |       |   |
|  |                             |        | A      | dd VPC     |           |   |           |   |   |       |   |
|  |                             |        |        |            |           |   |           |   |   |       |   |
|  |                             |        |        |            |           |   |           |   |   |       |   |
|  |                             |        |        |            |           |   |           |   |   |       |   |
| Tags - option                                | al Info                     |        |        |            |           |   |           |   |   |       |   |
| Tags - optione                               | al Info                     |        |        |            |           |   |           |   |   |       |   |
| Tags - optiona                               | al Info                     | ource. |        |            |           |   |           |   |   |       |   |
| Tags - optiona<br>No tags associa<br>Add tag | al Info<br>ted with the res | ource. |        |            |           |   |           |   |   |       |   |

6. If you receive alert for permissions, perform one of the following processes.

#### Note

The alert for permission occurs in the case if you have not configured the query logging with the new console in the beginning.

- **a.** Click **Grant permissions** to grant Route 53 with WRITE logs permissions to your CloudWatch logs groups. The alert disappears and you shall proceed with the next step. (OR)
- b. If you have 10 resource policies already, then you will not be able to create any more. Henceforth, select any of your existing resource policies and click Edit. Editing will give Route 53 permissions to WRITE logs to your log groups and click Save. By performing this process, the alert disappears, and you shall continue to the next step.
- 7. Choose **Permissions**[optional] if you require to see a table that shows whether the resource policy matches the CloudWatch log group, and whether the Route 53 has the permission to publish logs to CloudWatch.
- 8. After providing the necessary details, click Configure query logging.

#### Note

After enabling the Query logging on Route 53, integrate CloudWatch with Netsurion Open XDR using the NetsurionAWSIntegrator lambda function.

**9.** After configuring the query logging, configure AWS CloudTrail to forward logs to Netsurion Open XDR.

#### Note

Refer to the <u>How To Configure AWS CloudTrail</u> guide to configure AWS CloudTrail to forward logs to Netsurion Open XDR.



# 5 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received in Netsurion Open XDR, configure the DSI in the Netsurion Open XDR.

The DSI package contains the following files for Amazon Route 53.

- Categories\_Amazon Route 53.iscat
- Reports\_Amazon Route 53.etcrx
- KO\_Amazon Route 53.etko
- Dashboards\_Amazon Route 53.etwd
- Templates\_Amazon Route 53.ettd

#### Note

Refer the <u>How To Configure DSI</u> guide for the procedures to configure the above DSIs in Netsurion Open XDR.

### 5.1 Reports

| Name                                   | Description  |
|--|--|
| Amazon Route 53 - DNS query activities | Provides details about activities related to DNS queries in Amazon Route 53. |

### 5.2 Dashboards

| Name   | Description   |
|--|---|
| Amazon Route 53 - DNS queries by geolocation of client   | Displays the DNS queries of clients based on the geolocation.             |
| Amazon Route 53 - DNS queries by geolocation of resolver | Displays the DNS queries based on the resolver according to its location. |
| Amazon Route 53 - DNS queries domain by resolver IP      | Displays the DNS query domain based on the resolver IP address.           |
| Amazon Route 53 - DNS queries by volume                  | Displays the DNS queries by volume irrespective of the log type.          |
| Amazon Route 53 - DNS queries by response types          | Displays the DNS queries based on the response types.                     |
| Amazon Route 53 - DNS queries by query types             | Displays the DNS queries based on the query types.                        |

### 5.3 Saved Searches

| Name                                   | Description  |
|--|--|
| Amazon Route 53 - DNS query activities | Provides details about activities related to DNS queries in Amazon Route 53. |



### **About Netsurion**

Netsurion<sup>®</sup> delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at <u>www.netsurion.com</u>.

### **Contact Us**

#### **Corporate Headquarters**

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

#### **Contact Numbers**

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

| Managed XDR Enterprise Customers | SOC@Netsurion.com              |
|----------------------------------|--------------------------------|
| Managed XDR Enterprise MSPs      | SOC-MSP@Netsurion.com          |
| Managed XDR Essentials           | Essentials@Netsurion.com       |
| Software-Only Customers          | Software-Support@Netsurion.com |

https://www.netsurion.com/support