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 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 AWS console.

3 System Extraction

Perform the following process for system extraction.

1. In **Netsurion Open XDR**, hover over the **Admin** menu and click **Manager.**
2. 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)

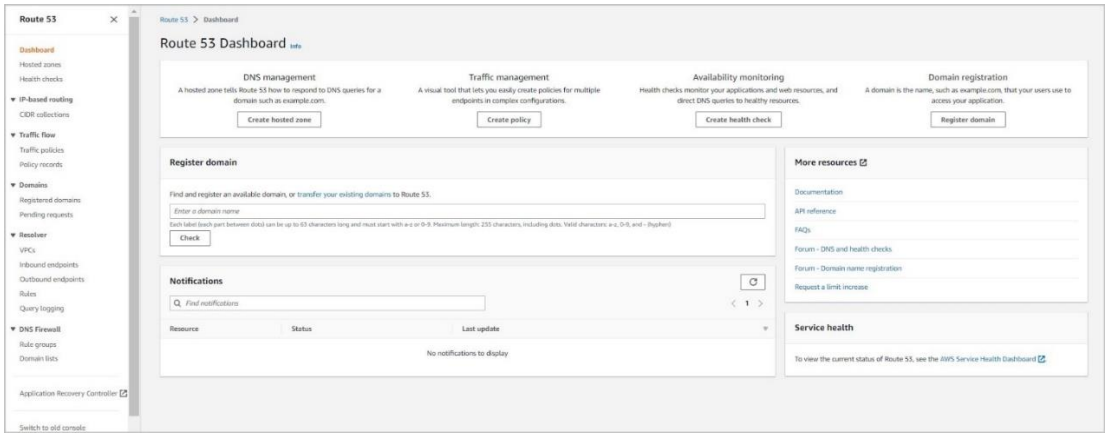
     a. **Regular expression :** `(?is)Organisation:(?P<computer>.*?),`

     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.

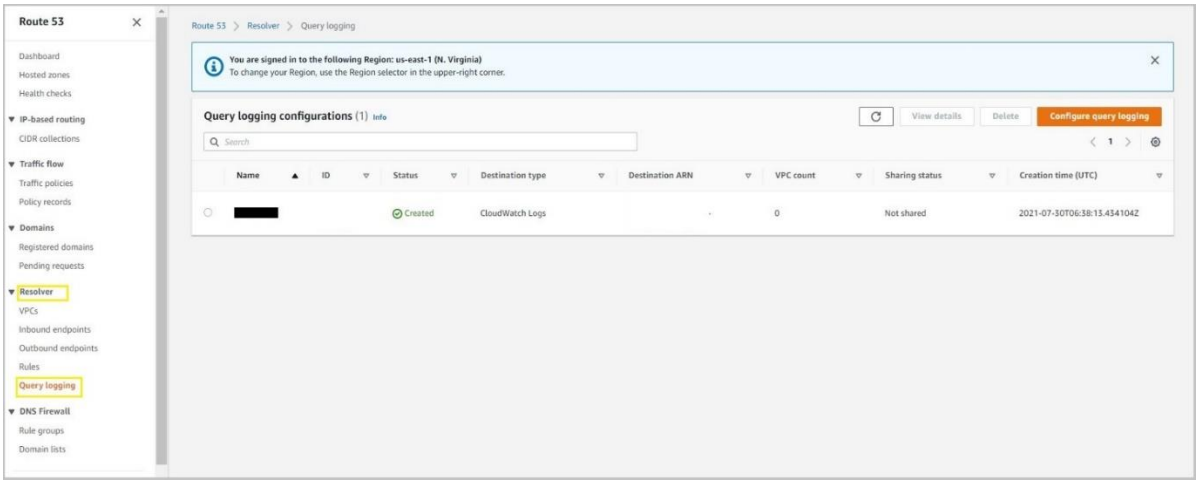
1. Log in to AWS Management console and go to Route 53.



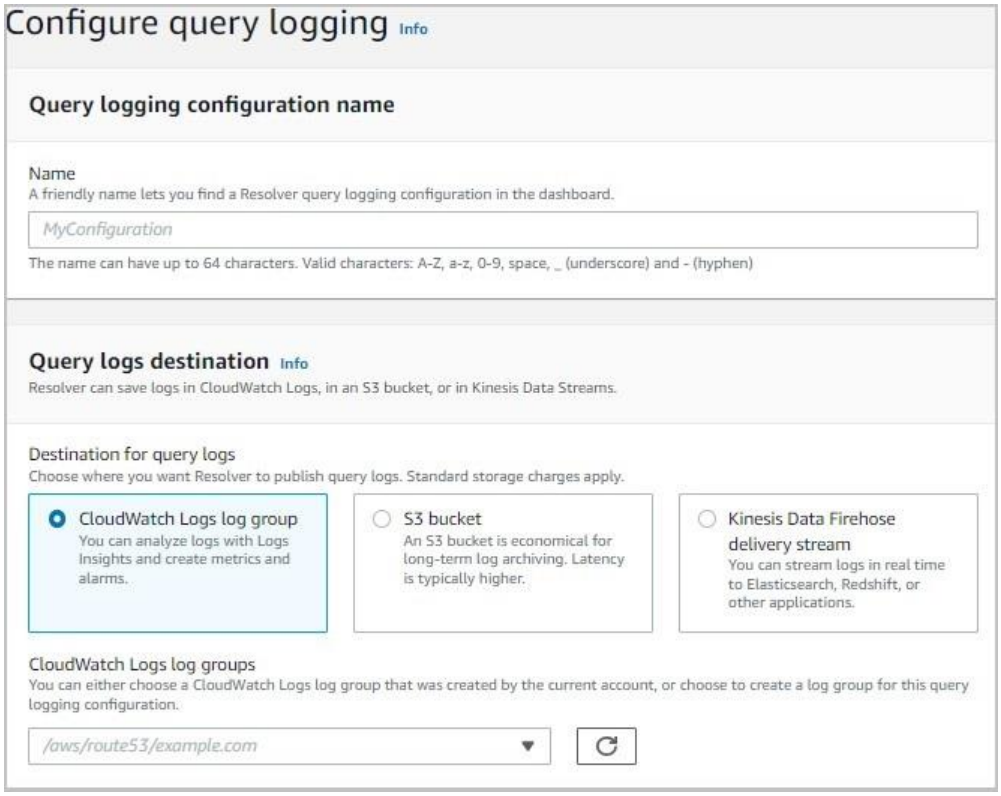
2. In the Route 53 navigation pane, click the **Resolver** drop-down, and then click **Query logging**.
3. In the **Query logging** pane, click **Configure query logging**.

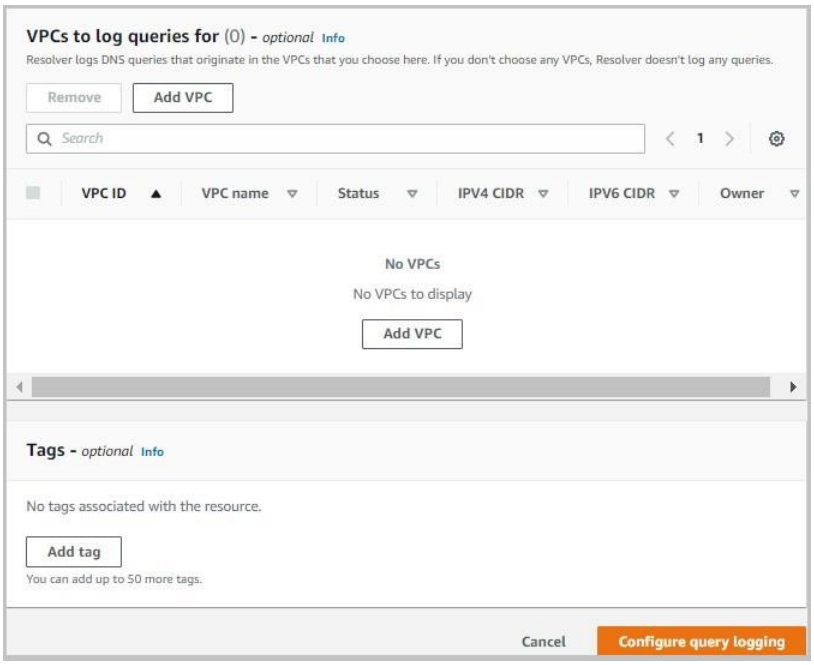
Note

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



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





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 How To Configure AWS CloudTrail 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 How To Configure DSI 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® 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 www.netsurion.com.

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