NetWitness® Platform XDR

Amazon VPC Flow Logs Event Source Log Configuration Guide

NETWITNESS
Platform XDR

Amazon VPC Flow Logs

Event Source Product Information:

Vendor: Amazon

Event Source: Amazon VPC

Versions: all

NetWitness Product Information:

Supported On:
NetWitness Platform XDR 11.5 and later

Event Source Log Parser: cef

Note: The CEF parser parses this event source as **device.type=amazonvpc**.

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Note: This plugin will be deprecated soon. Customers using NetWitness Platform version 11.5 or later can use either the Amazon cloudwatch plugin or S3 Universal Connector to capture vpc flow logs.

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

November, 2022

Contents

To configure Amazon VPC, you must complete these tasks:

I. Configure the Amazon VPC event source

II. Set Up Amazon VPC Event Source in NetWitness Platform XDR

Configure the Amazon VPC Event Source

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

You can customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS Cloud as an extension of your corporate data center.

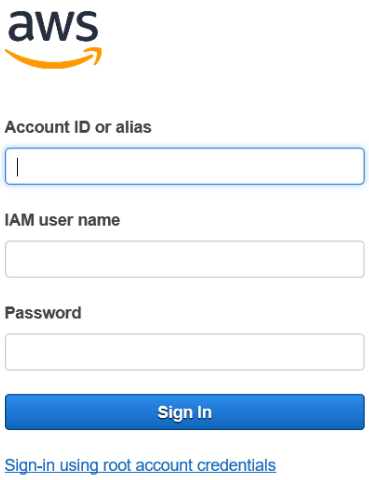
Note: The Amazon VPC plugin is meant for collecting the VPC flow logs provided by AWS. The AWS VPC flow logs are sent to CloudWatch in JSON format, as detailed in the AWS documentation here: https://aws.amazon.com/vpc/

Enable the VPC Service

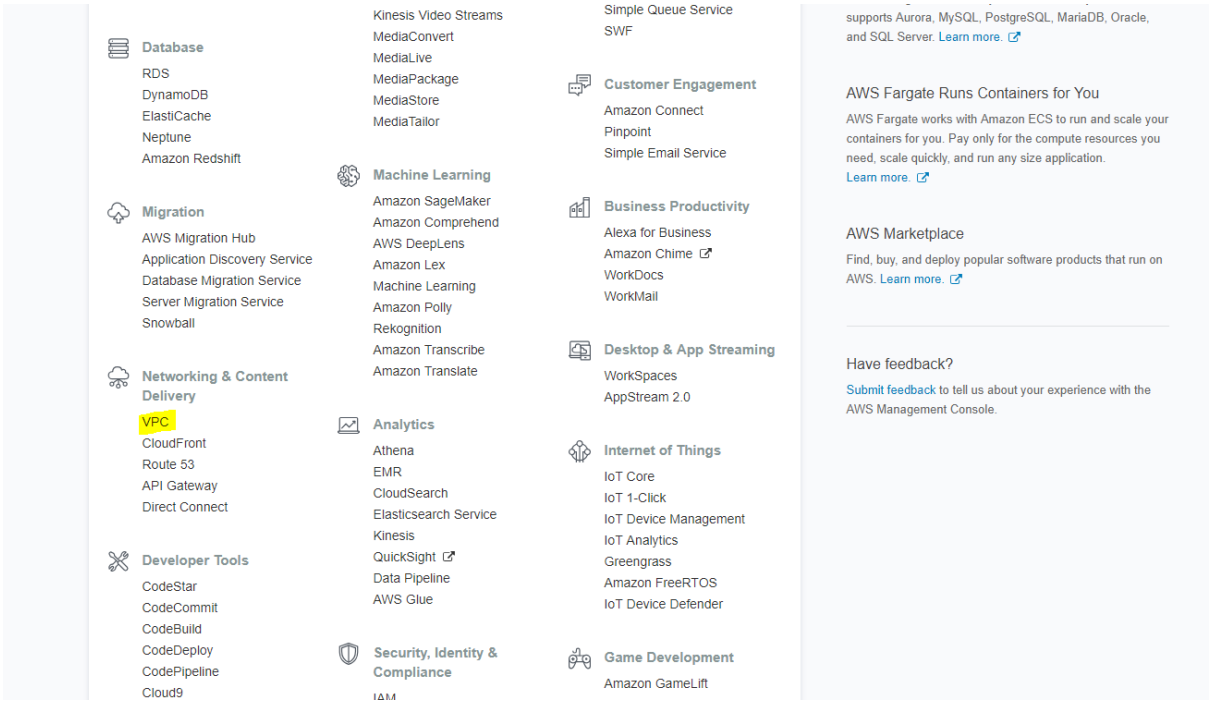
To use VPC Flow Logs, they must be enabled. Use the following procedure to enable VPC.

To enable Amazon VPC:

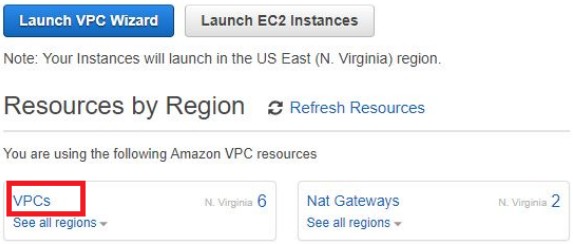
1. Login to AWS using your AWS credentials.



2. After you log in, select the VPC service from the **Networking & Content Delivery** menu.



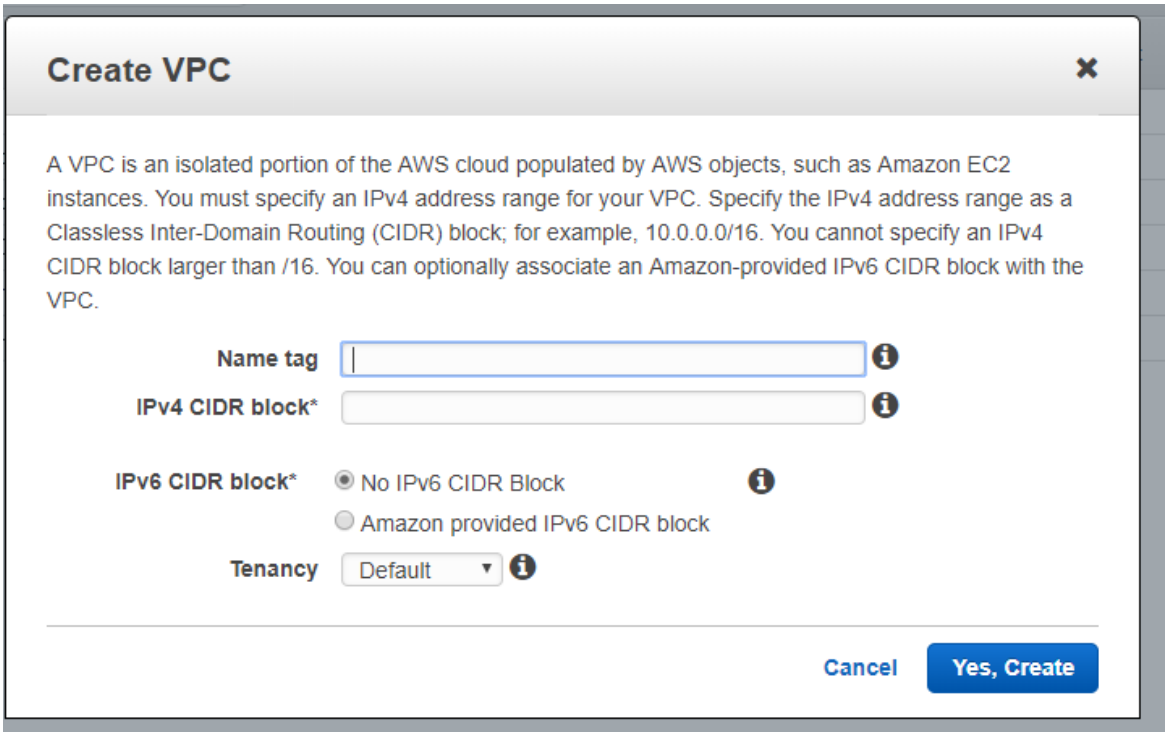
3. Create a new VPC.
   a. In the **Resources by Region** area, click **VPCs**.



   b. Click **Create VPC**.

   The Create VPC window is displayed.

   c. In the Create VPC window, specify the **Name tag** (for example Vpc_test), and provide a valid IP address and subnet in the **IPv4 CIDR block** field.



   d. Click **Yes, Create**.

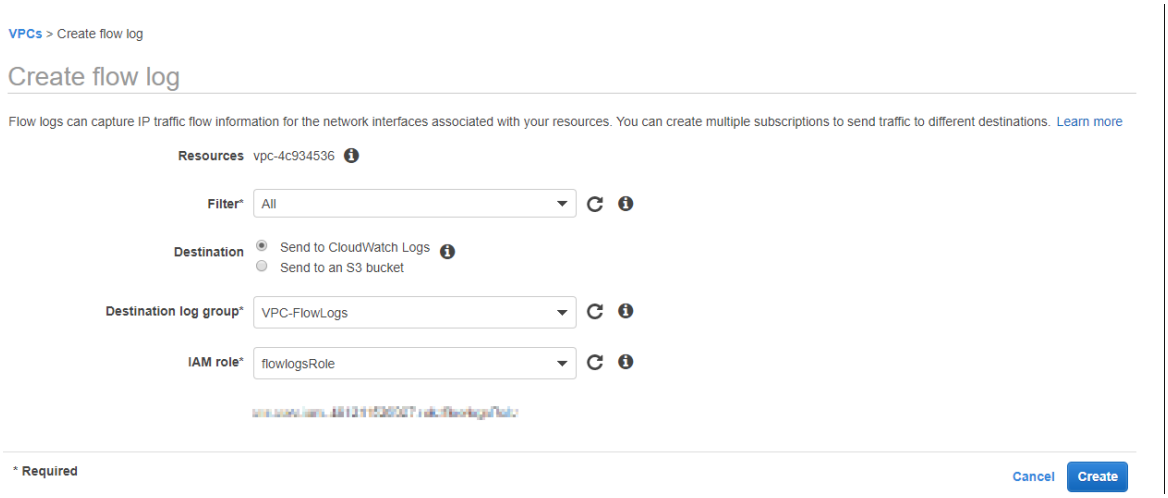
A new VPC is created and appears in the list as shown here:

4. Enable flow logs for the VPC we just created.
   a. Select the VPC that you created.
   b. At the bottom of the window, select the **Flow Logs** tab and click **Create flow log**.

   c. Fill in the details for your flow logs.
      - In **Filter**, select either **Accept**, **Reject** or **All**.
      - For **Destination**, select **Send to CloudWatch Logs**, since we are redirecting the VPC logs to the cloud watch.
      - For **Destination log group**, select **VPC-FlowLogs**.

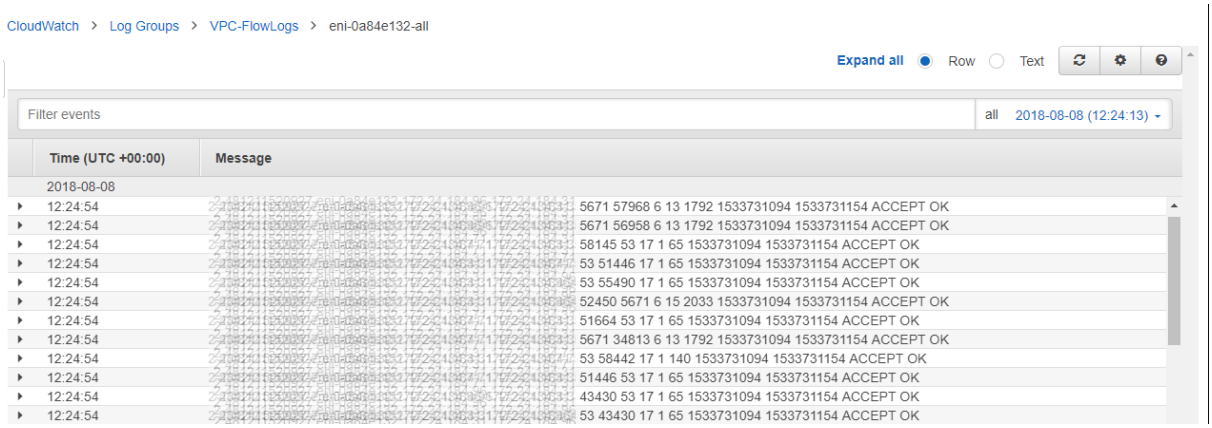
      Note: If this destination log group does not exist, create it as described in Create Log Group if Necessary.

   d. Select **IAM** role as **Flow-Logs-Role** and click **Create**. For details, see Create a Flow Logs Role.



Your new flow logs are created. Note that it may take some time to generate the flow logs.

To check the flow logs, navigate to the CloudWatch service. Click on **Logs**, and in **Filter**, you can search the Flow Logs Group you have created. Click on the Flow Log Group and you can see Multiple Log Streams. Each log stream contains the VPC Flow logs. Click on any Log Stream to see the Flow logs. Sample Flow logs are as shown here:



5. Note the Log Group name and your region name. You pass the region name to the NetWitness Platform XDR to fetch the logs.

Create a Flow Logs Role

This section describes how to create a Flow Logs role if you do not already have one.

To create a Flow Logs role:

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Roles, Create role**.
3. Choose **EC2** as the service to use this role. For Use case, choose **EC2**. Choose **Next: Permissions**.

4. On the Attach permissions policies page, choose **Next: Tags** and optionally add tags. Choose **Next: Review**.
5. Enter a name for your role (for example, Flow-Logs-Role) and optionally provide a description. **Choose Create role**.
6. Select the name of your role. For Permissions, choose **Add inline policy, JSON**.
7. Copy the policy given below for Publishing Flow Logs to CloudWatch Logs and paste it in the window.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Action": [
         "logs:CreateLogGroup",
         "logs:CreateLogStream",
         "logs:PutLogEvents",
         "logs:DescribeLogGroups",
         "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
     }
  ]
}
```

8. Choose **Review policy**.
9. Enter a name for your policy, and choose **Create policy**.
10. Select the name of your role. For Trust relationships, choose **Edit trust relationship**. In the existing policy document, change the service from **ec2.amazonaws.com** to **vpc-flow-logs.amazonaws.com**. Choose **Update Trust Policy**.
11. On the Summary page, note the ARN for your role. You need this ARN when you create your flow log.

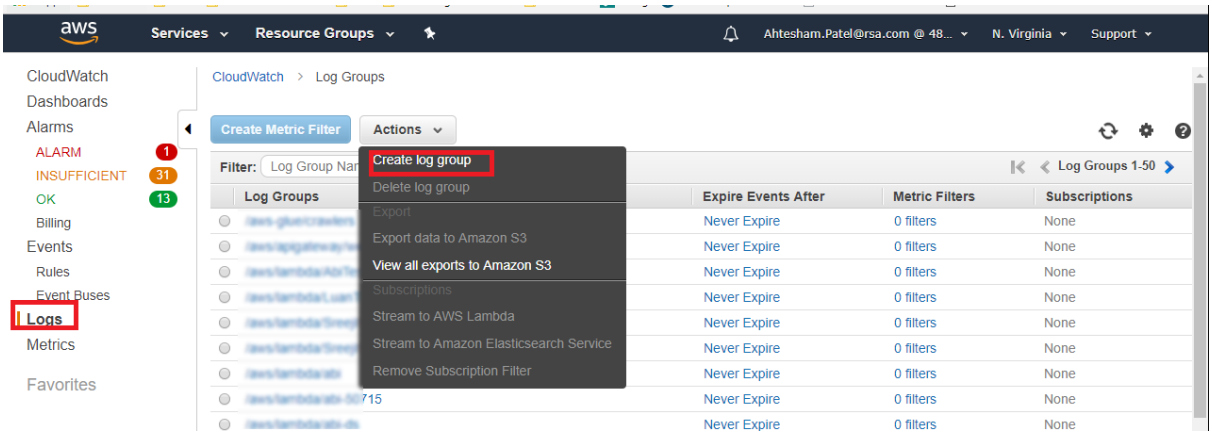
Users must also have permissions to use the **iam:PassRole** action for the IAM role that is associated with the flow log:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Action": ["iam:PassRole"],
        "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    } ]
}
```

Create Log Group if Necessary

If the VPC-FlowLogs Destination log group does not exist, you must create it. Navigate to the CloudWatch service and create a new Log group.

1. Click on **CloudWatch Service** under Management tools and click the **Logs** tab.
2. Click **Actions**, then click **Create log group**.
3. Enter a name for the Flow Log group and click **Create log group**.



Your new Flow Group has been created.

Set Up the Amazon VPC Event Source in NetWitness Platform XDR

In [[[Undefined variable SAVariables.ProductSuiteName]]], perform the following tasks:

I. Deploy the **amazonvpc** package and CEF parser from Live

II. Configure SELinux mode to Enforcing Mode

III. Configure the event source.

Deploy Amazon VPC Files from Live

Amazon VPC requires resources available in Live in order to collect logs.

To deploy the cef parser from Live:

1. In the NetWitness Platform XDR menu, select **CONFIGURE**.

   The **Live Content** tab is displayed.

2. Browse Live Content for the **Common Event Format (cef)** parser, using **Log Device** as the **Resource Type**.

3. Select the **cef** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.

4. You also need to deploy the Amazon VPC package. Browse Live for Amazon VPC content, typing "Amazon VPC" into the Keywords text box, then click **Search**.

5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

   Note: If a remote VLC is being used, you must deploy the package on both the remote VLC and the destination Log Decoder.

6. Restart the **nwlogcollector** service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Services Management Guide*.

Configure SELinux mode to Enforcing mode on the Remote VLC/LC

Run the script `update_selinux_policy.sh`, which is provided in the package, as a root user, after you deploy the package to the Log Decoder.

To enable the Enforcing mode for the SELinux, run the script on the remote Virtual Log Collector (VLC) or Log Collector:

```
sh
/etc/netwitness/ng/logcollection/content/collection/cmdscript/amazo
nvpc/update_selinux_policy.sh
```

Note: You only need to run this script once, during the initial configuration. Also, you do not need to run the script in NetWitness version 11.2 and later.

Configure the Event Source

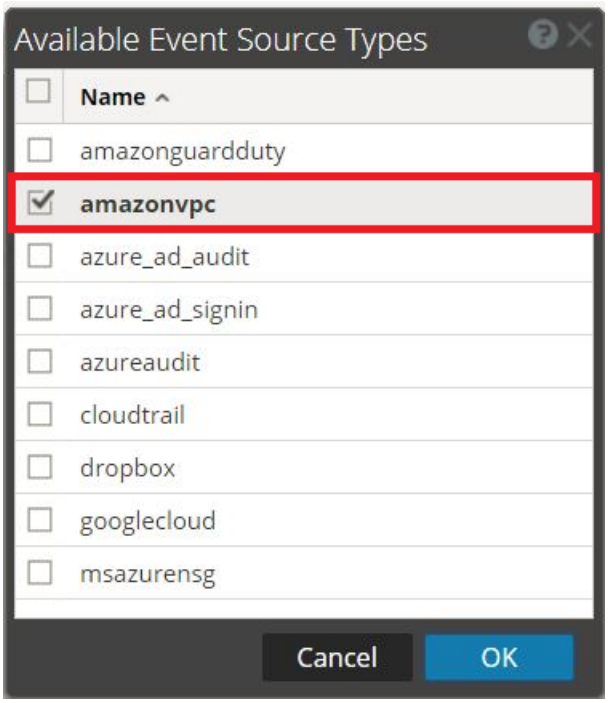
This section contains details on setting up the event source in [[[Undefined variable SAVariables.ProductSuiteName]]]. In addition to the procedure, the Amazon VPC Collection Configuration Parameters are described, as well as how to collect Amazon VPC Flow Events in NetWitness Platform XDR.

To configure the Amazon VPC Event Source:

1. In the NetWitness Platform XDR menu, select **Admin> Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

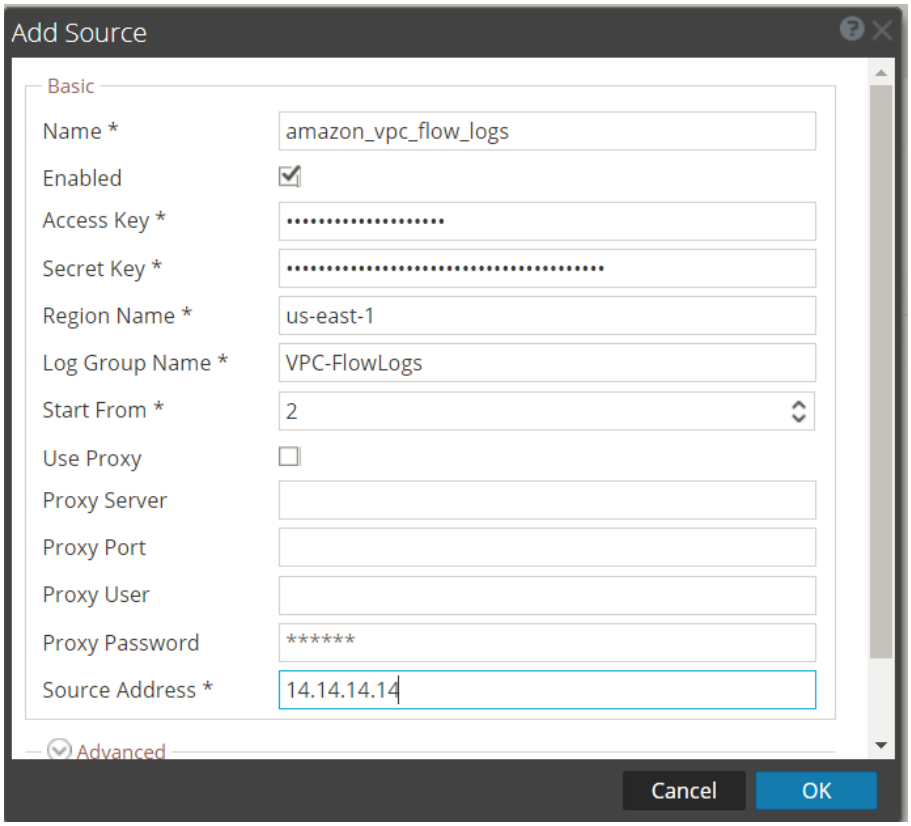


5. Select **amazonvpc** from the list, and click **OK**.

The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.



7. Define parameter values, as described in Amazon VPC Collection Configuration Parameters.
8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform XDR displays an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

Amazon VPC Collection Configuration Parameters

The following tables describe the configuration parameters for the Amazon VPC integration with [[[Undefined variable SAVariables.ProductSuiteName]]]. Fields marked with an asterisk (*) are required.

Basic Parameters

For these parameters, note the following:

- The IAM user, whose credentials are being used as **Access Key** and **Secret Key**, needs to have a minimum of programmatic access with **CloudWatchLogsReadOnlyAccess** policy attached, in order to pull the logs.
- Avoid using special characters in the **Proxy User** and **Proxy Password** sections.

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
Access Key *	Access key for the AWS account.
Secret Key *	Secret key for the AWS account.
Log Group Name *	Provide the Log Group Name that you entered when you configured the VPC Flow logs.
Start From *	Specifies the number of days prior to the current time, from which log collection should start.
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	A custom value chosen to represent the IP address for the Amazon VPC Flow Logs Event Source in the customer environment. The value of this parameter is captured by the **device.ip** meta key.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Parameter	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify **180**, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enabled	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.