NetWitness® Platform

S3 Universal Connector Event Source Log Configuration Guide

NETWITNESS
Platform

S3 Universal Connector

Event Source Product Information:

Vendor: AWS

Event Source: S3

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: aws, aws_cloudtrail, cisco_umbrella, aws_waf, aws_windows, opswat, jamf, cloudflarerbi, appfabric

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

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.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November 2024

Contents

Supported Events	Parser Required	Configuration Steps
Cloudtrail	aws_cloudtrail	CloudTrail
VPC Flow Logs	aws	VPC Flow Logs
AWS WAF Logs	aws_waf	AWS Web Application Firewall Logs
AWS Directory Service	aws_windows	AWS Managed Microsoft AD (AWS Directory Services)
Windows Logs	aws_windows	Windows Logs
CiscoUmbrella	cisco_umbrella	CiscoUmbrella
Opswat MetaAccess Cloud	opswat	Opswat MetaAccess Cloud
Jamf Protect	jamf	Jamf Protect
Application Load Balancer (ALB) access logs	aws	Access Logs from Application Load Balancer
Cloudflare Remote Browser Isolation (RBI)	cloudflarerbi	Cloudflare RBI
AWS AppFabric	appfabric	AWS AppFabric
Amazon CloudFront	aws	Amazon CloudFront

Introduction

Most of the AWS services have an option to send their logs to a S3 bucket. This plugin acts as a universal connector to collect logs from any S3 bucket into NetWitness. Currently we support capture and parsing of the below log sources stored in s3 bucket.

CloudTrail

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides the event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.

For more information see AWS CloudTrail.

VPC Flow Logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Flow logs can help you with a number of tasks, such as:

- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces

Link: Logging IP traffic using VPC Flow Logs.

AWS Web Application Firewall Logs

You can enable logging to get detailed information about traffic that is analyzed by your web ACL. Information that is contained in the logs includes the time that AWS WAF received the request from your AWS resource, detailed information about the request, and the action for the rule that each request matched.

Link:Logging AWS WAF web ACL traffic.

AWS Managed Microsoft AD (AWS Directory Services)

Parser Used: aws_windows

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as AWS Managed Microsoft AD, is powered by Windows Server 2012 R2.

With AWS Managed Microsoft AD, you can run directory-aware workloads in the AWS Cloud, including Microsoft SharePoint and custom .NET and SQL Server-based applications. You can also configure a trust relationship between AWS Managed Microsoft AD in the AWS Cloud and your existing on-premises Microsoft Active Directory, providing users and groups with access to resources in either domain, using single sign-on (SSO).

You can use the AWS Directory Service console or APIs to forward domain controller security event logs to Amazon CloudWatch Logs. This helps you meet your security monitoring, audit, and log retention policy requirements by providing transparency of the security events in your directory.

CloudWatch Logs can also forward these events to other AWS accounts, AWS services, or third party applications. This makes it easier for you to centrally monitor and configure alerts to detect and respond proactively to unusual activities in near real-time.

Link: Enable log forwarding

To use S3 Universal Connector to capture these logs they need to be sent to the S3 bucket. The below link provides the steps to send logs from a CloudWatch Log Group to the S3 bucket via a Kinesis Firehose Service.

Link: Subscription filters with Amazon Kinesis Data Firehose.

Note: When creating the Firehose Service add **aws/directoryservice/** as a custom prefix as shown in the screenshot below and select gzip as the compression.

Windows Logs

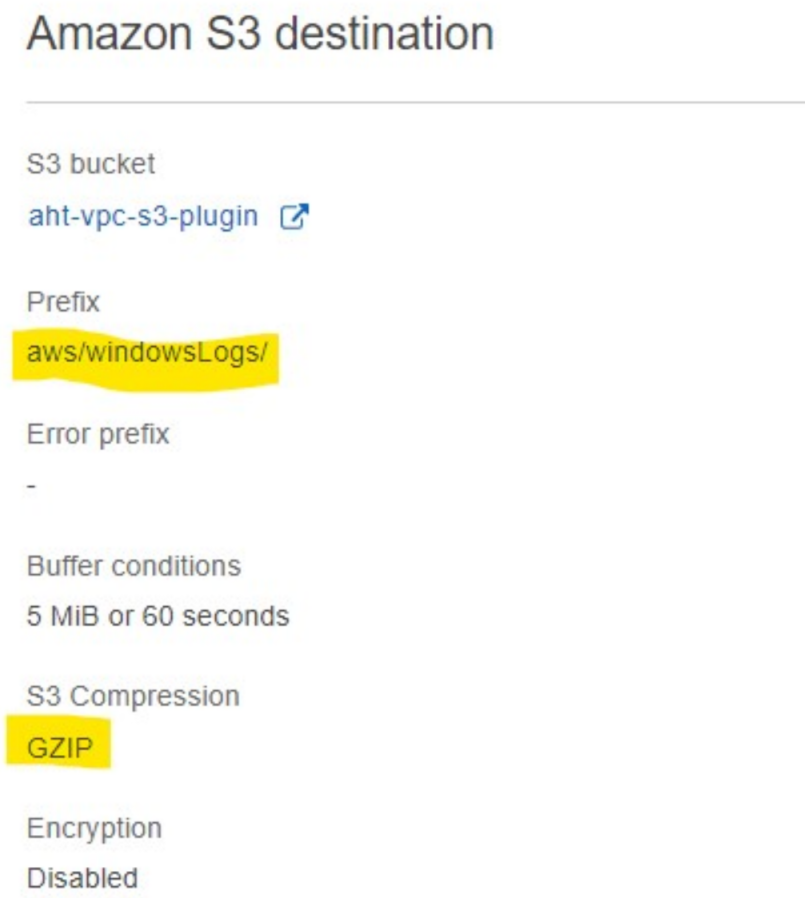
This plugin supports the collection of Windows Logs (System, Application, and Security) sent to the S3 bucket via the Kinesis Agent for Windows.

Amazon Kinesis Agent for Microsoft Windows (Kinesis Agent for Windows) is a configurable and extensible agent. It runs on fleets of Windows desktop computers and servers, either on-premises or in the AWS Cloud. Kinesis Agent for Windows efficiently and reliably gathers, parses, transforms, and streams logs, events, and metrics to various AWS services, including Kinesis Data Streams, Kinesis Data Firehose, Amazon CloudWatch, and CloudWatch Logs.

Kinesis Agent for Windows Documentation: https://docs.aws.amazon.com/kinesis-agent-windows/latest/userguide/what-is-kinesis-agent-windows.html.

Note: When configuring the "KinesisFirehose" sink specify the "Format" as "xml".

Note: When creating the Firehose Service add **aws/windowsLogs/** as a custom prefix as shown in the screenshot below and select gzip as the compression.



CiscoUmbrella

Cisco Umbrella uses the infrastructure of the Internet to block malicious destinations before a connection is established. Cisco Umbrella delivers security from the cloud by observing your internet traffic, and blocking malicious destinations, then logs the activities. Cisco Umbrella logs provide an option to export logs to your company-managed Amazon S3 bucket. We provide support for dnslogs, iplogs, and proxylogs stored in your S3 bucket.

This plugin can be used to collect ciscoumbrella from a customer managed S3 bucket and not from a cisco managed s3 bucket.

Link: Manage Your Logs.

Opswat MetaAccess Cloud

Security teams face challenges with increasing work from home scenarios. They lack visibility and control over devices accessing their network. Adding to the complexity is the myriad point products generally needed to gain this visibility and control. OPSWAT Meta Access is one solution that gives secure network access and deep endpoint compliance to your organization. For more information, see The MetaAccess Platform.

Netwitness Platform supports admin, device, webhook, and device_report JSON events from Opswat MetaAccess using s3universal plugin. All these events can be collected using Opswat MetaAccess API integration with Netwitness Platform as well, see OPSWAT MetaAccess Cloud Event Source Log Configuration Guide.

Jamf Protect

Apple builds one of the most secure out-of-the-box platforms in the information technology domain. Apple's macOS and iOS are best among the market competitors in the OS domain. Jamf Protect enhances Apple's built-in security features by increasing visibility, preventions, controls and remediation capabilities. For more information, see Jamf Protect.

In NetWitness Platform , we collect logs with the help of Jamf Protect using either the Jamf Protect GraphQL API or the AWS S3 bucket storage facility.

The Jamf Protect plugin forwards all the events to either Jamf Protect GraphQL API and AWS S3 storage depending on your configuration. The information in the following table helps you to select the NetWitness plugin collection method to collect particular event type. If you want to use the Jamf Protect GraphQL API integration with Netwitness, see Jamf Protect Event Source Log Configuration Guide.

Jamf Protect Event Types	Jamf Protect GraphQL API	AWS S3 Bucket Forwarding
Alerts	Allowed	Allowed
Audit	Allowed	Not Allowed
Computer List	Allowed	Not Allowed
Telemetry	Not Allowed	Allowed

Access Logs from Application Load Balancer

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Access logs is an optional feature of Elastic Load Balancing that is disabled by default. To enable access logs, see Enable access logs for your Application Load Balancer.

This plugin can be used to collect the Access logs from Application Load Balancer.

Cloudflare RBI

Detailed logs that contain metadata are generated by Cloduflare RBI. These logs are helpful for debugging, identifying configuration adjustments, and creating analytics, especially when combined with logs from other sources, such as your application server.

Note: When pushing Cloudflare RBI logs to s3 bucket, add the string `cloudflare-rbi` as a prefix to the s3 bucket path.

AWS AppFabric

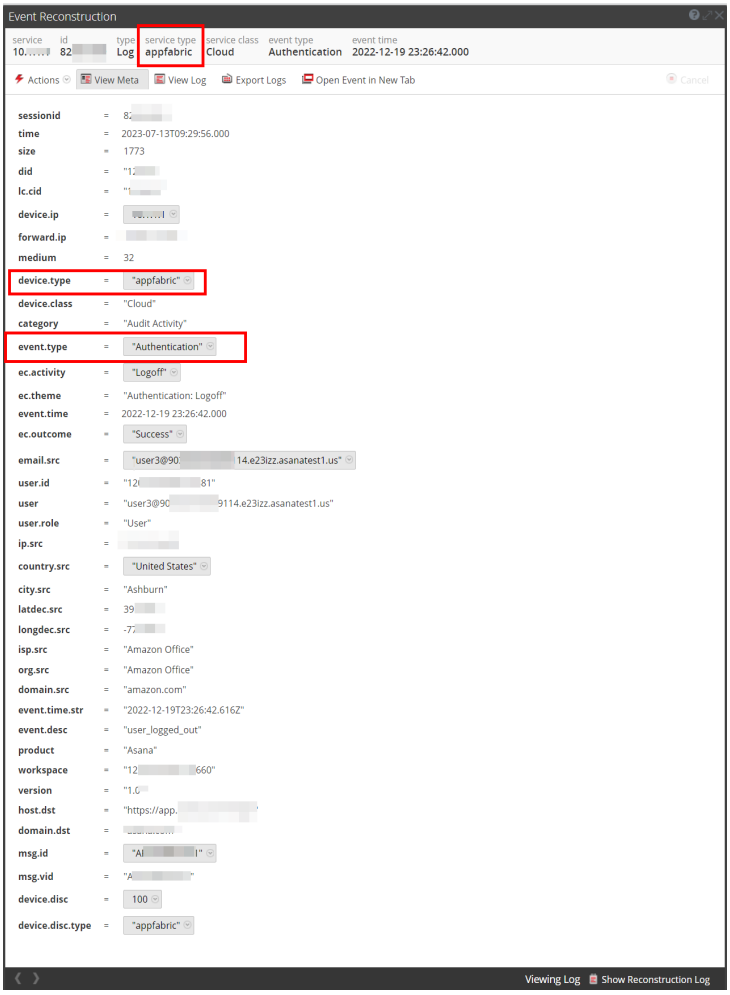
AWS AppFabric quickly connects software as a service (SaaS) applications across your organization. IT and security teams can then easily manage and secure applications using a standard schema. AppFabric automatically normalizes application data for administrators and security analysts to monitor common security policies and user access.

The Open Cybersecurity Schema Framework (OCSF) is an open-source project, delivering an extensible framework for developing schemas, along with a vendor-agnostic core security schema. AppFabric normalizes the SaaS application audit logs into Open Cybersecurity Schema Framework (OCSF), or raw data is made available in two data formats, JSON or Apache Parquet. AppFabric only normalizes usage data for applications authorized in the AWS Management Console.

The normalized logs from authorized SaaS application will be normalized to OCSF format by AppFabric and delivered to the S3 bucket owned by the customer. The Netwitness S3 Universal Connector will pull the AppFabric logs from S3 bucket to Netwitness. The file format supported by S3 Universal Connector are JSON or Apache Parquet.

The collected events are parsed by the appfabric log parser and meta is generated by NetWitness Platform as shown below.

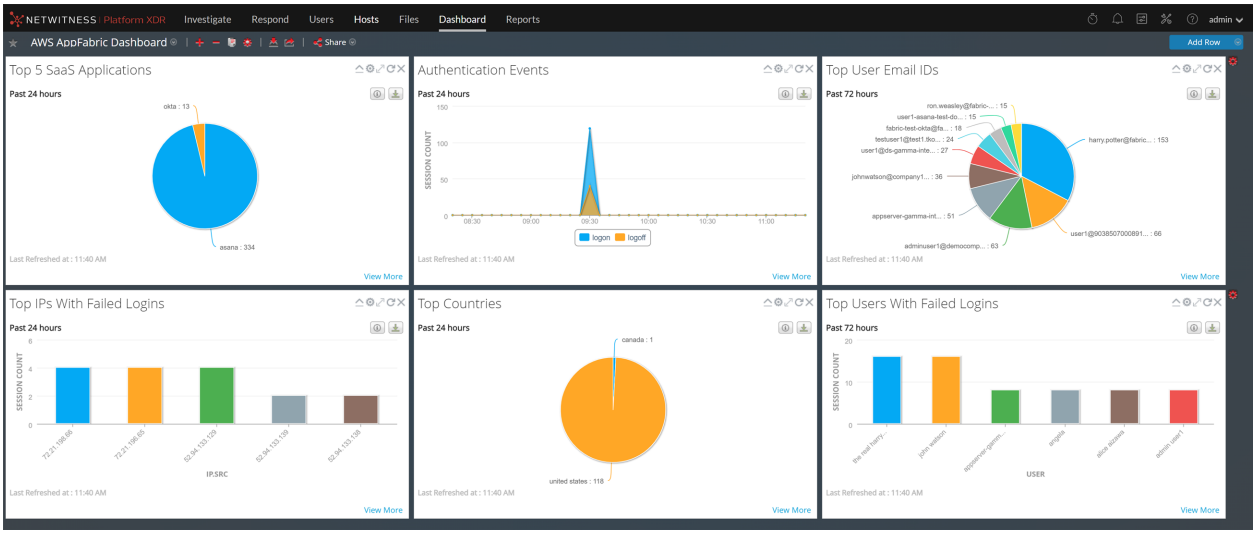
NetWitness Investigation Meta View for AppFabric - Authentication Event



AWS AppFabric Dashboard on NetWitness

As a launch partner for AWS AppFabric, NetWitness empowers customers to use this simplified, standardized method of securing new and existing AWS apps. The dashboard provides insight into the AWS AppFabric data such as Top 5 SaaS applications or Authentication events collected from AppFabric to NetWitness Platform .

- **Top 5 SaaS Applications:** Displays the top 5 SaaS applications integrated with AWS AppFabric.
- **Authentication Events:** Displays the activity names count of authentication events such as Logon, Logoff, Authentication ticket, Service ticket, and so on.
- **Top User Email IDs:** Displays the user email address count of SaaS Applications.
- **Top IPs With Failed Login:** Displays the top 5 Failed login count by IP addresses.
- **Top Countries:** Displays the list of countries from where the events are generated.
- **Top Users With Failed Login:** Displays the top 5 Failed login count by Users.

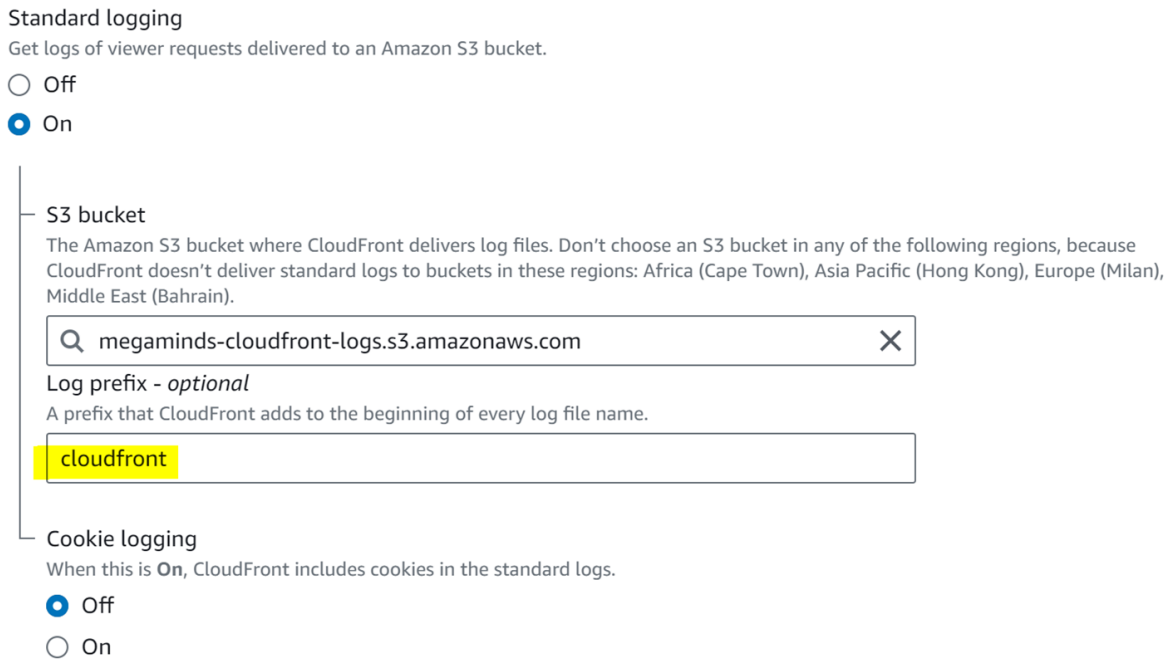


Amazon CloudFront

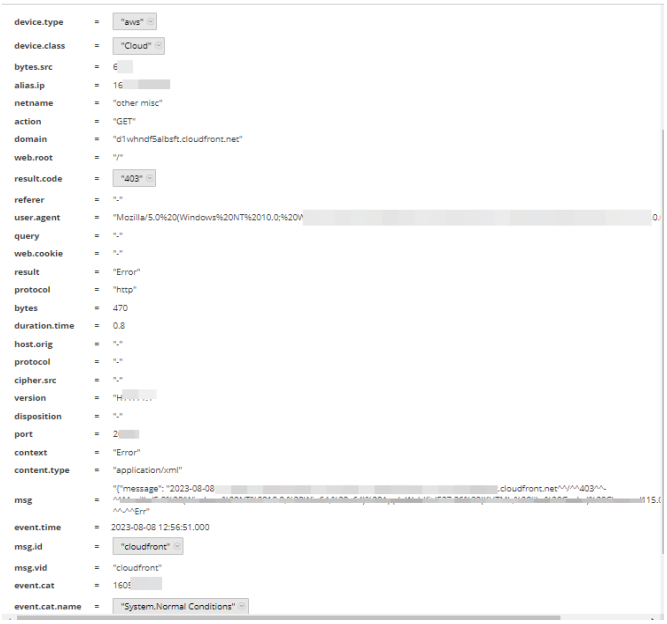
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations.

To log the requests that come to Cloudfront distribution we need to enable Standard logging in the distribution. CloudFront standard logs provide detailed records about every request that's made to a distribution. These logs are useful for many scenarios, including security and access audits.

CloudFront standard logs are delivered to the Amazon S3 bucket of your choice. When you enable Standard logging for a distribution, you should specify the log prefix as ***cloudfront*** and the Amazon S3 bucket that you want CloudFront to store log files as shown below.



NetWitness Investigation Meta View for CloudFront



To provide permissions required to configure standard logging and to access your log files, see Configuring and using standard logs (access logs).

Refer Standard log file format for more information on CloudFront Standard log fields.

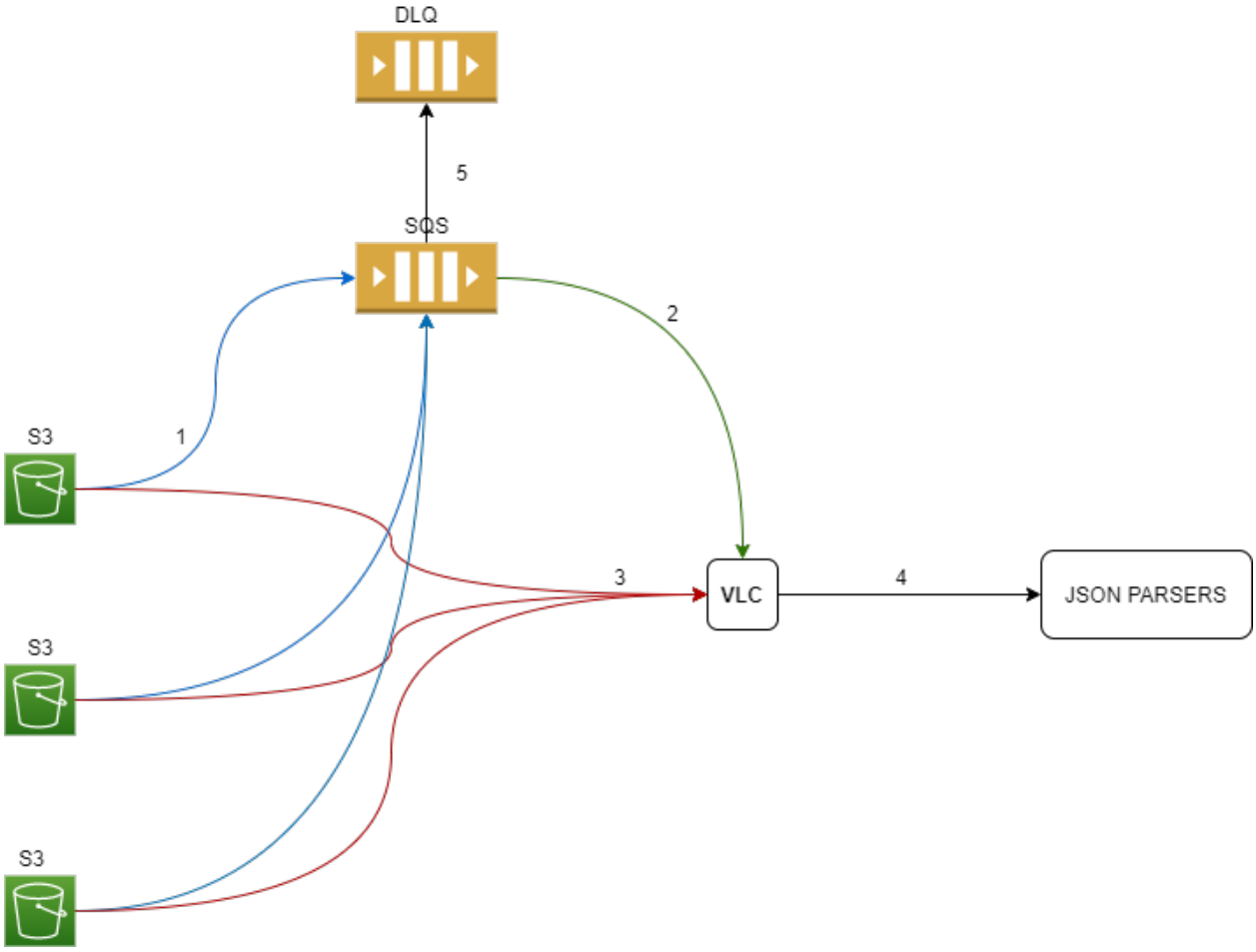
For more information on configuration steps:

Steps	Link
Steps to route amazon VPC logs to S3	Publish flow logs to Amazon S3
Steps to route Cloudtrail logs to S3	Amazon S3 bucket policy for CloudTrail
Steps to route CiscoUmbrella logs to S3	Enable Logging to Your Own S3 Bucket
Steps to route Windows logs to S3	Tutorial: Stream JSON Log Files to Amazon S3 Using Kinesis Agent for Windows
Steps to route Opswat MetaAccess logs to S3	SIEM Integration
Steps to route Jamf Protect logs to S3	Data Forwarding to a Third Party Storage Solution **IMPORTANT:** When you configure Amazon S3 Forwarding on Jamf Protect, you should input **Prefix** as ***jamf*** to successfully complete the configuration. • Telemetry • Unified Logging.
Steps to route Cloudflare RBI logs to S3	Enable Logpush to Amazon S3 **IMPORTANT:** When pushing Cloudflare RBI logs to s3 bucket, add the string `cloudflare-rbi` as a prefix to the s3 bucket path.
Steps to route AppFabric logs to S3	Getting started with AWS AppFabric
Steps to route CloudFront Access logs to S3	Configuring and using standard logs (access logs) **IMPORTANT:** While configuring the Standard logging for CloudFront distribution, provide the Log prefix as `cloudfront`, only then the Netwitness S3 Universal Connector will collect the cloudfront access logs.
Steps to route AWS WAF Logs	Logging AWS WAF web ACL traffic

Note: If the log type you are looking to collect is not supported, NetWitness recommends you to raise a customer support request, Getting Help with NetWitness Platform to get help.

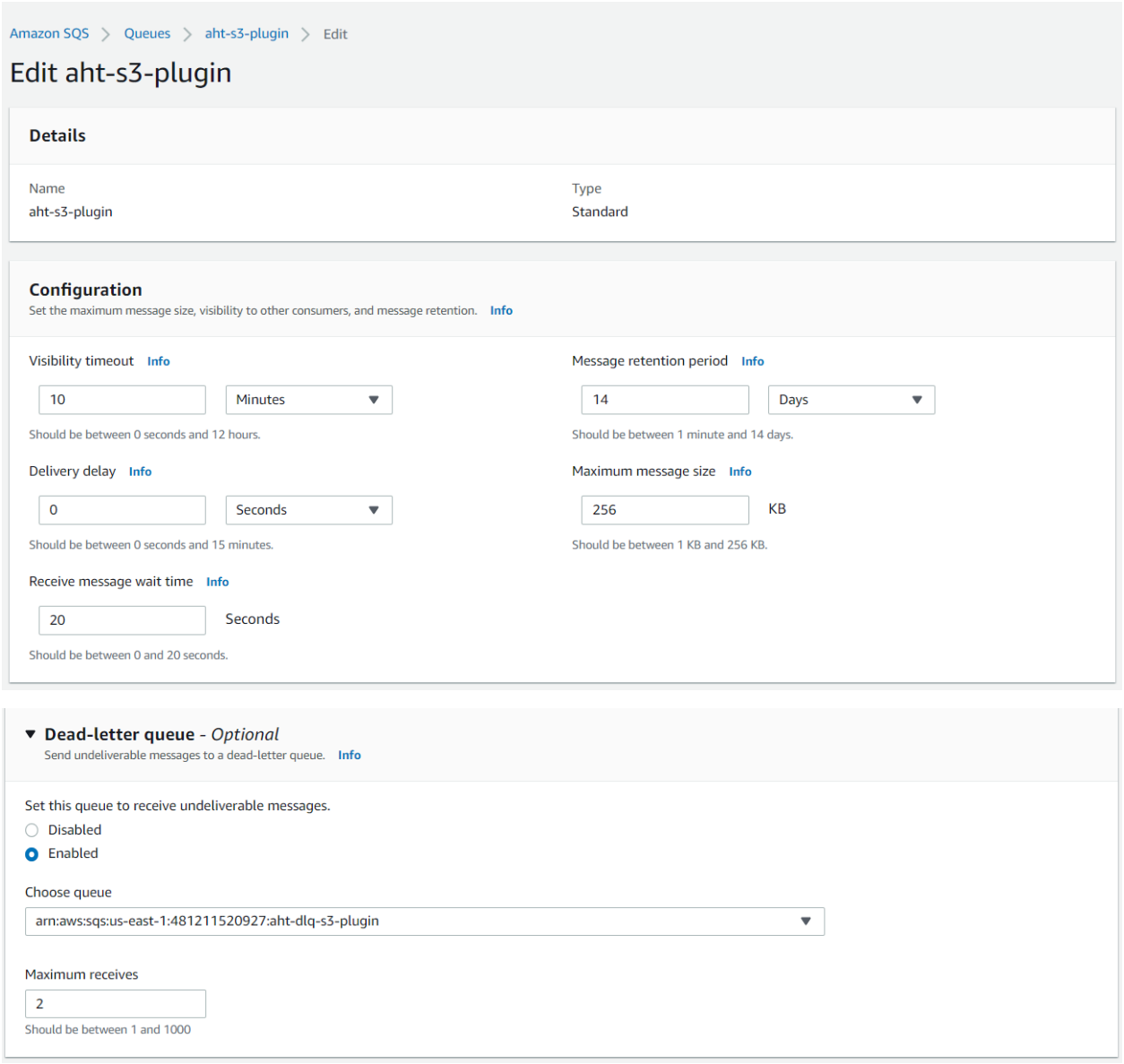
Configuration Steps at AWS Side

The customer needs to setup an event notification to be sent to SQS Queue for any PUT action on the S3 bucket(s). This SQS queue is periodically polled for new messages and when a message is received the corresponding object is read from the required bucket.



1. Create a SQS queue to act as a DLQ.
2. Create SQS queue in the same region as the S3 Bucket(s). A single SQS queue can be used for multiple buckets.

For steps to create SQS Queue, refer- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-create-queue.html.



3. The SQS access policy needs to allow SendMessage action to the Bucket(s) with logs. It also needs to allow “sqs:DeleteMessage", "sqs:ReceiveMessage” action to the IAM user being used by the plugin instance to collect logs. Attached below is an example Access Policy

   {

   "Version": "2012-10-17",

   "Id": "event-notification",

   "Statement": [

   {

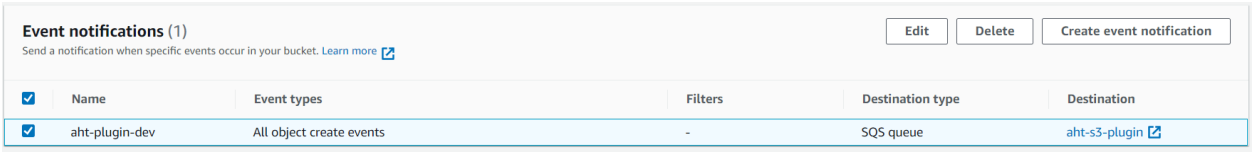
   "Sid": "cloudtrail-notification",

   "Effect": "Allow",

```
"Principal": {
"AWS": "*"
},
"Action": "SQS:SendMessage",
"Resource": "arn:aws:sqs:us-east-1:481xxxxxxx27:aht-s3-plugin ",
"Condition": {
"StringEquals": {
"aws:SourceAccount": "481xxxxxxx27"
},
"ArnLike": {
"aws:SourceArn": "arn:aws:s3:::vlc-ct "
}
}
},
{
"Sid": "Stmt1608120119529",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::481xxxxxxx27:user/plugin_user "
},
"Action": [
"sqs:DeleteMessage",
"sqs:ReceiveMessage"
],
"Resource": "arn:aws:sqs:us-east-1:481xxxxxxx27:aht-s3-plugin "
}
]
}
```


Note: This is just an example access policy for the purpose of demonstration. Customer would need to fine tune it based on their organization's security constraints.

4. Setup the S3 Bucket(s) to trigger event notification to the above created SQS queue.



Refer AWS guide to setup event notification-
https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html.

Note: S3universal connector supports only SSE-S3 encryption on the s3 bucket.

Note: Add filters in the event notification of s3 bucket to send only the notification for specific objects.
For example, to send only Cloudtrail logs notification (avoiding Cloudtrail Insight/Digest) to SQS, the folowing filter can be used: AWSLogs/<account-id>/CloudTrail/.

Setup the S3 universal plugin in NetWitness Platform

In NetWitness Platform, perform the following tasks.

- Deploy S3 Universal Files from Live
- Configure S3 Universal Plugin in NetWitness Platform

Deploy S3 Universal Files from Live

S3 universal plugin requires resources available in Live in order to collect logs.

To deploy s3universal content from Live:

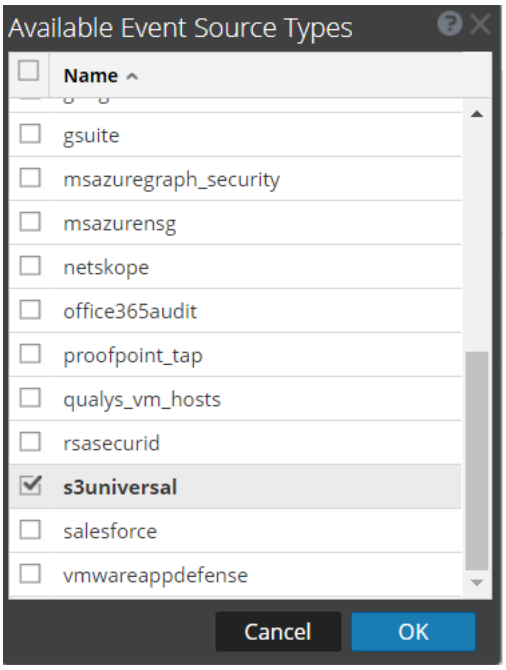
1. In the NetWitness Platform menu, select **Configure** > **Live Content**. Browse Live for S3 Universal plugin by typing **s3universal** into the Keywords text box and click **Search**.
2. Select the item returned from the Search.
3. Click **Deploy** to deploy the S3 Universal to the appropriate Log Collectors using the Deployment Wizard.
4. Deploy the appropriate parsers used by this plugin – aws, aws_cloudtrail, cisco_umbrella, aws_waf.

   Note: If the number of messages in the queue is very high, create multiple instance of the S3universal plugin to ingest the messages at a higher rate.

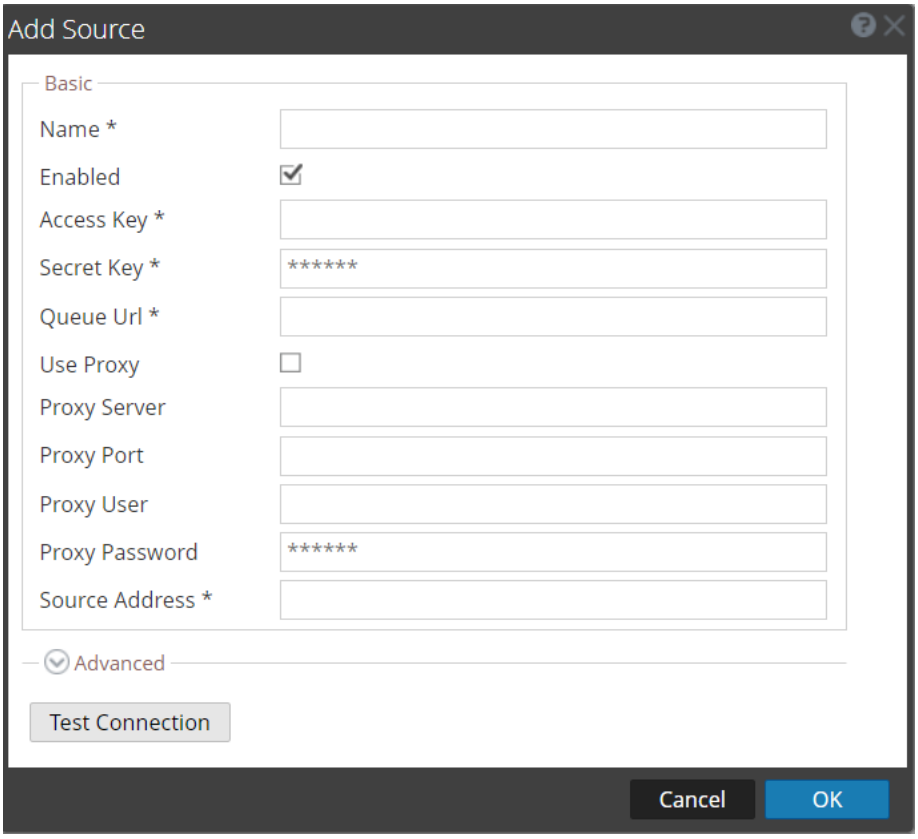
For more details, see the Add or Update Supported Event Source Log Parsers topic on NetWitness Link.

Configure S3 Universal Plugin in NetWitness Platform

1. In NetWitness Platform menu, select **Admin** > **Services**.
2. In the **Services** grid, select a Log Collector and from the **Actions (** **)** menu, choose **View** > **Config** > **Event Sources**.
3. In the **Event Sources** tab, select **plugins** 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 tool bar, click +,
   The **Available Event Source Types** dialog is displayed.



5. Select **s3universal** 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 **Source** panel tool bar. The **Add Source** dialog is displayed.



7. Define the parameter values as described in S3 Universal 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 based on message shown 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 displays a Request Timed Out error.

Note: Test Connection works only if the plugin can connect to the SQS queue and pull messages. The connection to S3 Bucket(s) is not tested. Start the plugin instance and observe /var/log/messages for absence of errors to confirm if the end to end collection is working correctly.

9. If the test is successful, click **OK**.
   The new event source is displayed in the **Sources** panel.
10. Repeat steps 4 - 9 to add another instance of **S3Universal plugin** type.

S3 Universal Collection Configuration Parameters

This section describes the S3 Universal Plugin configuration parameters.

Note: Items that are followed by an asterisk (*) required.

Basic Parameters

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 checkbox to enable the event source configuration to start a collection. The checkbox is selected by default.
Access Key*	AWS IAM Access Key belonging to a user which has "**sqs:ReceiveMessage**" and "**sqs:DeleteMessage**" access to SQS queue being used. It should also have "**s3:GetObjec**t" permission for the S3 buckets being used.
Secret Key*	Secret Key corresponding to the above access Key.
Queue Url*	URL for the SQS queue being used for event notification.
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).

Name	Description
Source Address	IP address that is to be given to S3Universal plugin instance. (Logs from this event source will be collected with this device IP)
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Click **Advanced** to view and edit the advanced parameters, if necessary.

Name	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, the collector waits for that cycle to finish. If you have many 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	The maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600. We recommend setting this value to 1800 to reduce the no of API calls.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	The 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.

Name	Description
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. **Caution**: 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.
HTTPS Proxy	If Proxy server is configured, enable or disable based on the proxy traffic allowed. By default HTTPS Protocol is enabled for the Proxy connection. If the only HTTP traffic allowed via proxy, then uncheck this parameter.
SSL Enable	Uncheck to disable certificate verification

Getting Help with NetWitness Platform

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 the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- 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 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 feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.