LOGZILLA DOCUMENTATION

Aws Cloudwatch Vpc Flow

LogZilla App Store application: Aws Cloudwatch Vpc Flow

LogZilla App Store · Generated April 29, 2026 · logzilla.ai/docs/logzilla-appstore/aws-cloudwatch-vpc-flow

Overview

Amazon Web Services (AWS) CloudWatch is a monitoring and observability service for use with AWS services. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events. CloudWatch can be used to detect anomalous behavior, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep applications running smoothly.

AWS VPC Flow Logs is a feature to capture information about the IP traffic going to and from network interfaces in a VPC.

App Function

The AWS CloudWatch VPC Flow app parses AWS VPC Flow logs received via AWS CloudWatch and creates user tags corresponding to many of the data elements present in each log message.

Vendor Documentation

- Amazon CloudWatch (https://aws.amazon.com/cloudwatch/)
- VPC Flow Logs (https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/)
- Logging IP Traffic Using VPC Flow Logs (https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html)
- Flow Log Record Examples (https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html)

Device Configuration

VPC Flow Logs are forwarded to LogZilla using AWS Kinesis Data Firehose. For complete setup instructions, see the LogZilla documentation: AWS CloudWatch Kinesis Setup (https://www.logzilla.ai/docs/receiving-data/aws-cloudwatch-kinesis-setup).

Summary:

Enable VPC Flow Logs in the AWS Console for the desired VPC
Configure CloudWatch Logs as the destination
Create a Kinesis Data Firehose delivery stream with LogZilla's `/firehose` endpoint as the HTTP destination
Create a CloudWatch subscription filter to forward logs to the Firehose delivery stream

Incoming Log Format

VPC Flow Logs are received from Amazon CloudWatch by means of a CloudWatch web hook. CloudWatch conveys the log messages to LogZilla by sending them to LogZilla's HTTP port as JSON messages. LogZilla then parses the CloudWatch log format

and extracts the specific flow log information.

The flow log information is a fixed-order sequence of space-separated data elements. There are no field keys or names, the meaning must be derived from the data ordering.

Event Classes

The app categorizes events into the following Event Classes:

Event Class	Description	Action
`network`	Normal traffic flows	ACCEPT
`security`	Blocked traffic (potential threats)	REJECT

Parsed Metadata Fields

The app extracts the following user tags from VPC Flow log messages:

Tag Name	Description
`Action`	Flow action (ACCEPT/REJECT)
`Availability Zone`	AWS availability zone ID
`DstIP`	Destination IP address
`DstPort`	Destination port/service
`Flow Direction`	Traffic direction
`Instance ID`	EC2 instance identifier
`Interface ID`	Network interface ID
`Log Status`	Logging status
`Protocol`	Network protocol name
`Region`	AWS region

Tag Name	Description
SrcIP	Source IP address
TCP Flags	TCP flags
Type	Traffic type (IPv4/IPv6/EFA)
VPC ID	VPC identifier
MitreId	MITRE ATT&CK technique (for blocked admin protocols)
MITRE Tactic	MITRE ATT&CK tactic category

MITRE ATT&CK Mapping

Event	MITRE Technique	Tactic
SSH/RDP/Telnet blocked	T1110 (Brute Force)	Credential Access

Log Examples

Incoming SSH Connection Accepted (format 1)

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21
20641 22 6 20 4249 1418530010 1418530070 ACCEPT OK
```

Incoming SSH Connection Accepted (format 2)

```
123456789010 ACCEPT apse2-az3 4249 172.31.16.21 22 1418530070
ingress eni-1235b8ca123456789 eni-0c0d52089ed3b20ba OK 20 -
4.3.2.1 - 1.2.3.4 6 us-east-1 172.31.16.139 20641 1418530010 - -
subnet-vf0-88683c 18 8 IPv4 5 vpc-12345
```

Dashboards

The AWS VPC Flow app includes the following dashboards:

- **AWS VPC Flow: Network** - Accepted traffic flows, protocols, ports, regions
- **AWS VPC Flow: Security** - Rejected traffic, blocked sources, MITRE mapping

Triggers

Trigger	Description	Actionable
AWS VPC: MITRE ATT&CK Threat Detected	Any MITRE-mapped threat	Yes
AWS VPC: SSH Blocked	Blocked SSH connection attempts	Yes
AWS VPC: RDP Blocked	Blocked RDP connection attempts	Yes
AWS VPC: Telnet Blocked	Blocked Telnet connection attempts	Yes
AWS VPC: SMB Blocked	Blocked SMB/NetBIOS (ransomware indicator)	Yes
AWS VPC: Database Access Blocked	Blocked database port access	Yes
AWS VPC: Traffic Rejected	Any rejected traffic	No