**VPC Flow Logs**

## Service Overview

*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 or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.*

## Use cases / Considerations

*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*

*Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without any risk of impact to network performance.*

## Governance

*Not required*

## Cautions

*To use flow logs, you need to be aware of the following limitations:*

* *You cannot enable flow logs for network interfaces that are in the EC2-Classic platform. This includes EC2-Classic instances that have been linked to a VPC through ClassicLink.*
* *You can't enable flow logs for VPCs that are peered with your VPC unless the peer VPC is in your account.*
* *After you've created a flow log, you cannot change its configuration or the flow log record format. For example, you can't associate a different IAM role with the flow log, or add or remove fields in the flow log record. Instead, you can delete the flow log and create a new one with the required configuration.*
* *If your network interface has multiple IPv4 addresses and traffic is sent to a secondary private IPv4 address, the flow log displays the primary private IPv4 address in the dstaddr field. To capture the original destination IP address, create a flow log with the pkt-dstaddr field.*
* *If traffic is sent to a network interface and the destination is not any of the network interface's IP addresses, the flow log displays the primary private IPv4 address in the dstaddr field. To capture the original destination IP address, create a flow log with the pkt-dstaddr field.*
* *If traffic is sent from a network interface and the source is not any of the network interface's IP addresses, the flow log displays the primary private IPv4 address in the srcaddr field. To capture the original source IP address, create a flow log with the pkt-srcaddr field.*
* *If traffic is sent to or sent by a network interface, the srcaddr and dstaddr fields in the flow log always display the primary private IPv4 address, regardless of the packet source or destination. To capture the packet source or destination, create a flow log with the pkt-srcaddr and pkt-dstaddr fields.*
* *When your network interface is attached to a* [*Nitro-based instance*](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#ec2-nitro-instances)*, the aggregation interval is always 1 minute or less, regardless of the specified maximum aggregation interval.*

*Flow logs do not capture all IP traffic. The following types of traffic are not logged:*

* *Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.*
* *Traffic generated by a Windows instance for Amazon Windows license activation.*
* *Traffic to and from 169.254.169.254 for instance metadata.*
* *Traffic to and from 169.254.169.123 for the Amazon Time Sync Service.*
* *DHCP traffic.*
* *Traffic to the reserved IP address for the default VPC router.*
* *Traffic between an endpoint network interface and a Network Load Balancer network interface.*

## Pricing considerations

*Data ingestion and archival charges for vended logs apply when you publish flow logs to CloudWatch Logs or to Amazon S3. For more information and examples, see* [*Amazon CloudWatch Pricing*](https://aws.amazon.com/cloudwatch/pricing)*.*

## More details

*Publishing flow logs to CloudWatch Logs* [*https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html*](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html)

*Publishing flow logs to Amazon S3* [*https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-s3.html*](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-s3.html)

*Troubleshooting VPC Flow Logs* [*https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-troubleshooting.html*](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-troubleshooting.html)