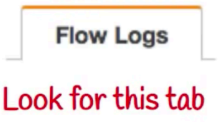
VPC Flow Logs

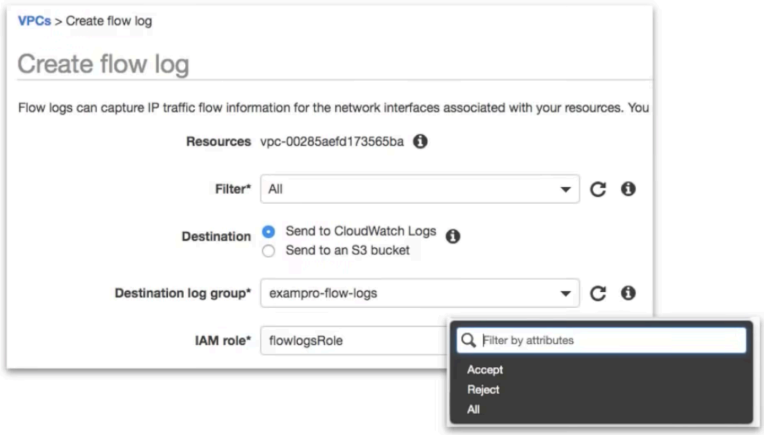
VPC Flow Logs allow you to capture **IP traffic information** in-and-out of Network Interfaces within your VPC.

Flow Logs can be created for.

1. **VPC**
2. **Subnets**
3. **Network Interface**



Look for this tab



All log data is **stored** using Amazon **CloudWatch Logs**.

After a Flow Log is created it can be viewed in detail within CloudWatch Logs

VPC Flow Logs

<version> <account-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-status>

```
2 123456789010 eni-abc123de 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010 1418530070 ACCEPT OK
```

version The VPC Flow Logs version.
account-id The AWS account ID for the flow log.
interface-id The ID of the network interface for which the traffic is recorded.
srcaddr The source **IPv4 or IPv6 address**. The IPv4 address of the network interface is always its private IPv4 address.
dstaddr The destination **IPv4 or IPv6 address**. The IPv4 address of the network interface is always its private IPv4 address.
srcport The source port of the traffic.
dstport The destination port of the traffic.
protocol The IANA protocol number of the traffic. For more information, see Assigned Internet Protocol Numbers.
packets The number of packets transferred during the capture window.
bytes The number of bytes transferred during the capture window.
start The time, in Unix seconds, of the start of the capture window.
end The time, in Unix seconds, of the end of the capture window.
action The action associated with the traffic:
- ACCEPT: The recorded traffic was permitted by the security groups or network ACLs.
- REJECT: The recorded traffic was not permitted by the security groups or network ACLs.

log-status The logging status of the flow log:
- OK: Data is logging normally to the chosen destinations.
- NODATA: There was no network traffic to or from the network interface during the capture window.
- SKIPDATA: Some flow log records were skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.

VPC Flow Logs *CheatSheet*

- **VPC Flow Logs** monitor the in-and-out traffic of your Network Interfaces within your VPC
- You can turn on Flow Logs at the VPC, Subnet or Network Interface level
- VPC Flow Logs **cannot be tagged** like other AWS resources
- You **cannot change the configuration** of a flow log **after it's created**.
- You **cannot enable** flow logs for VPCs which are peered with your VPC **unless it is in the same account**
- VPC Flow Logs can be delivered to an **S3** or **CloudWatch Logs**
- VPC Flow Logs contains the source and destination **IP addresses** (not hostnames)
- Some instance traffic is **not monitored:**
    - Instance traffic generated by contacting the AWS DNS servers
    - Windows license activation traffic from instances
    - Traffic to and from the instance metadata address (169.254.169.254)
    - DHCP Traffic
    - Any traffic to the reserved IP address of the default VPC router