**VPC Flow Logs**

**What is it?**

* VPC Flow Logs is a feature that enables you to configure information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you’ve created a flow log, you can view and retrieve its data in Amazon CloudWatch logs.
* Flow logs can be created at 3 levels;
  + VPC
  + Subnet
  + Network Interface level

**VPC Flow Logs Exam Tips:**

* You cannot enable flow logs for your VPCs that are peered with your VPC unless the peer VPC is in your account.
* You cannot tag a flow log.
* After you’ve created a flow log, you cannot change its configuration; for example, you can’t associate a different IAM role with the flow log.
* Not all IP traffic is monitored;
  + 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.
  + DHCP traffic.
  + Traffic to the reserved IP address for the default VPC router.