**CloudWatch Queries**

**VPC Flow Logs**

**Top 10 byte transfers by source and destination IP addresses**

stats sum(bytes) as bytesTransferred by srcAddr, dstAddr | sort bytesTransferred desc | limit 10

**Top 20 source IP addresses with highest number of rejected requests**

filter action="REJECT" | stats count(\*) as numRejections by srcAddr | sort numRejections desc | limit 20

**Find the top 15 packet transfers across hosts**

stats sum(packets) as packetsTransferred by srcAddr, dstAddr | sort packetsTransferred desc | limit 15

**Find the IP addresses where flow records were skipped during the capture window**

filter logStatus="SKIPDATA" | stats count(\*) by bin(1h) as t | sort t

**Average, min, and max byte transfers by source and destination IP addresses**

stats avg(bytes), min(bytes), max(bytes) by srcAddr, dstAddr

**IP addresses using UDP transfer protocol**

filter protocol=17 | stats count(\*) by srcAddr