**AWS ELB Resume Points**

Here are some resume points related to AWS Elastic Load Balancing (ELB) with different load balancer types:

# Classic Load Balancer (CLB):

* Experienced in designing and configuring CLBs to distribute traffic across multiple EC2 instances, improving application availability and fault tolerance.
* Proficient in setting up CLB listeners and configuring load balancing policies, such as round robin, least connections, or session stickiness, to optimize traffic distribution.
* Skilled in troubleshooting and resolving CLB-related issues, such as SSL certificate mismatches, backend instance connectivity problems, or load balancer health check failures.
* Demonstrated expertise in configuring CLB cross-zone load balancing to evenly distribute traffic across multiple Availability Zones, ensuring high availability and reducing latency.
* Experienced in integrating CLBs with Auto Scaling Groups (ASGs) to automatically scale the number of instances based on traffic demand and ensure optimal application performance.
* Proficient in implementing CLB cross-zone load balancing to evenly distribute traffic across multiple Availability Zones, ensuring high availability and reduced latency.
* Skilled in configuring SSL termination on CLBs to offload SSL/TLS encryption and decryption from backend instances, improving performance and reducing the load on application servers.
* Experienced in troubleshooting CLB-related SSL certificate issues, such as certificate expirations, invalid certificate chains, or misconfigurations.
* Demonstrated expertise in using CLB access logs and integrating with Amazon S3

or Amazon Athena for log analysis and monitoring of application traffic patterns.

* Proficient in implementing CLB session stickiness to maintain session persistence for applications that require stateful connections.
* Proficient in troubleshooting CLB-related issues in real-time, such as instances failing health checks, load balancer not distributing traffic correctly, or SSL certificate errors.
* Experienced in analyzing CLB access logs and CloudWatch metrics to identify performance bottlenecks, anomalies, or abnormal traffic patterns, and taking proactive measures to resolve them.
* Skilled in diagnosing and resolving network connectivity issues between CLB and backend instances, investigating security group rules, subnet configurations, or VPC routing problems.
* Demonstrated expertise in troubleshooting SSL/TLS handshake failures or certificate-related errors, ensuring secure and uninterrupted communication between clients and the CLB.
* Proficient in collaborating with AWS Support or using third-party monitoring tools to analyze and troubleshoot CLB issues, applying quick and effective solutions to minimize impact on applications and end users.

# Application Load Balancer (ALB):

* Proficient in designing and configuring ALBs to route traffic at the application layer, enabling advanced load balancing features such as path-based routing, host-based routing, or redirect rules.
* Experienced in implementing ALB target groups and configuring health checks to ensure the availability and proper functioning of backend instances.
* Skilled in utilizing ALB features like content-based routing, SSL/TLS termination, or WebSocket support to enhance application delivery and security.
* Demonstrated expertise in troubleshooting ALB-related issues, such as incorrect target group configurations, routing conflicts, or backend instance registration problems.
* Proficient in utilizing ALB access logs and integrating with AWS CloudWatch metrics to monitor and analyze application traffic, performance, and request patterns.
* Experienced in configuring ALB content-based routing to route traffic based on request attributes, such as URL path, host headers, or query parameters, enabling advanced application routing and microservices architecture support.
* Proficient in utilizing ALB features like advanced request routing rules, including redirect and rewrite rules, to optimize URL handling and application behavior.
* Skilled in integrating ALBs with AWS WAF (Web Application Firewall) to protect applications against common web exploits and security threats.
* Demonstrated expertise in implementing ALB target group stickiness to maintain session affinity for applications that require persistence at the application layer.
* Experienced in troubleshooting ALB-related HTTP errors, such as 502 Bad Gateway or 504 Gateway Timeout, and resolving backend connectivity issues or misconfigurations.
* Experienced in real-time troubleshooting of ALB-related issues, such as routing misconfigurations, target group failures, or backend instance connectivity problems.
* Proficient in analyzing ALB access logs, CloudWatch metrics, and target group health checks to identify and resolve issues related to HTTP errors, request routing, or unhealthy instances.
* Skilled in diagnosing and resolving issues with ALB listener configurations, ensuring proper load balancing, SSL/TLS termination, or WebSocket support.
* Demonstrated expertise in troubleshooting ALB-related security issues, such as AWS WAF rule violations, cross-site scripting (XSS) attacks, or SQL injection attempts.
* Proficient in using real-time monitoring and logging tools, such as AWS X-Ray or AWS CloudTrail, to trace and diagnose ALB-related issues across distributed systems or microservices architectures.

# Network Load Balancer (NLB):

* Experienced in configuring NLBs to handle high network traffic loads with

ultra-low latency, distributing traffic across multiple targets at the TCP and UDP transport layer.

* Proficient in implementing NLB listeners and target groups, defining port mappings and health checks for routing traffic to backend instances.
* Skilled in utilizing NLB features such as static IP addresses, Elastic Network Interfaces (ENIs), or preserving source IP addresses for seamless integration with applications that require client IP visibility.
* Demonstrated expertise in troubleshooting NLB-related issues, such as network connectivity problems, incorrect target group configurations, or improper health check settings.
* Experienced in integrating NLBs with AWS services like Auto Scaling, ECS, or EKS to dynamically scale and manage the backend instances based on network traffic demand.
* Proficient in configuring NLB target group attributes, such as health checks, timeouts, or deregistration delays, to ensure high availability and fault tolerance of backend instances.
* Experienced in implementing NLB source IP preservation to maintain the source IP address of the client when forwarding traffic to backend instances, facilitating network-level logging and IP-based security controls.
* Skilled in utilizing NLB features like UDP load balancing or TCP listener timeouts to optimize the handling of specific network protocols and connection behaviors.
* Demonstrated expertise in troubleshooting NLB-related network connectivity issues, such as routing misconfigurations, security group rules, or network ACL restrictions.
* Proficient in utilizing NLB access logs and integrating with Amazon Kinesis or AWS Lambda for real-time analysis and monitoring of network traffic patterns.
* Proficient in real-time troubleshooting of NLB-related network connectivity issues, such as routing misconfigurations, security group rules, or network ACL restrictions.
* Experienced in analyzing NLB access logs, CloudWatch metrics, and target group health checks to identify and resolve issues related to high latency, network timeouts, or backend instance failures.
* Skilled in diagnosing and resolving issues with NLB listener configurations, ensuring proper load balancing, UDP or TCP handling, or source IP preservation.
* Demonstrated expertise in troubleshooting NLB-related network performance issues, investigating packet loss, jitter, or throughput problems, and implementing

optimization measures.

* Proficient in leveraging real-time network monitoring tools, such as VPC Flow Logs or third-party network diagnostic tools, to troubleshoot NLB issues and ensure optimal network performance.

# Gateway Load Balancer (GLB):

* Proficient in designing and implementing GLBs to provide scalable and highly available access to virtual network appliances, such as firewalls, intrusion detection systems, or NAT gateways.
* Experienced in configuring GLB endpoints, route tables, and health checks to ensure proper traffic distribution and availability of the virtual network appliances.
* Skilled in troubleshooting GLB-related issues, such as incorrect routing configurations, connectivity problems between GLB and backend appliances, or issues with health checks.
* Demonstrated expertise in integrating GLBs with other AWS services, such as VPC peering, Transit Gateway, or AWS PrivateLink, to establish secure and efficient network communication.
* Experienced in configuring GLB endpoints for integrating virtual network appliances, such as firewalls or NAT gateways, into the network traffic flow, enhancing network security and routing capabilities.
* Proficient in implementing GLB route tables and policies to direct traffic between different network destinations based on defined rules and conditions.
* Skilled in troubleshooting GLB-related issues with virtual network appliance connectivity, routing configurations, or performance bottlenecks.
* Demonstrated expertise in integrating GLBs with Transit Gateway to enable secure and scalable interconnection of multiple VPCs or on-premises networks.
* Proficient in leveraging GLBs for AWS PrivateLink implementations, providing private connectivity to AWS services without traversing the public internet.
* Experienced in real-time troubleshooting of GLB-related issues with virtual network appliance connectivity, routing configurations, or performance bottlenecks.
* Proficient in analyzing GLB access logs, CloudWatch metrics, and diagnostic outputs from virtual network appliances to identify and resolve issues related to

packet drops, high latency, or misconfigurations.

* Skilled in diagnosing and resolving issues with GLB endpoint configurations, ensuring proper traffic routing, policy enforcement, or network segmentation.
* Demonstrated expertise in troubleshooting GLB-related issues in AWS PrivateLink or Transit Gateway setups, investigating routing conflicts, security group configurations, or DNS resolution problems.
* Proficient in collaborating with network administrators, application developers, or AWS Support to diagnose and resolve complex GLB-related issues that span multiple layers of the networking stack.