**AWS VPC Resume Points**

Here are some resume points related to AWS VPC (Virtual Private Cloud):

* Proficient in designing and implementing AWS VPC architectures, including subnetting, routing, security groups, and network access control lists (ACLs).
* Experienced in configuring VPC peering connections and VPN connections to establish secure network connectivity between VPCs and on-premises environments.
* Skilled in implementing VPC endpoint services, such as AWS PrivateLink, to securely access AWS services without traversing the internet.
* Demonstrated expertise in designing and implementing high-availability VPC architectures using multi-Availability Zone (AZ) deployments and load balancers.
* Proficient in implementing VPC security best practices, including network segmentation, secure communication protocols, and access controls to protect resources within the VPC.
* Experienced in implementing VPC flow logs and utilizing CloudWatch Logs and other monitoring tools to monitor network traffic and troubleshoot connectivity issues.
* Skilled in implementing network address translation (NAT) gateways or NAT instances for instances within private subnets to access the internet.
* Demonstrated expertise in implementing VPC endpoints for AWS services like S3, DynamoDB, or Kinesis to securely access these services without internet gateways.
* Proficient in implementing VPC security architectures, including bastion hosts, network access control, and security group rules, to protect VPC resources from unauthorized access.
* Experienced in troubleshooting VPC connectivity issues, such as misconfigured routes, security group conflicts, or routing table misconfigurations.
* Proficient in implementing VPC peering between different AWS accounts to

establish private and secure communication between VPCs in a multi-account environment.

* Experienced in utilizing VPC endpoint policies to control access and permissions for resources accessed through VPC endpoints.
* Skilled in implementing VPC traffic mirroring to capture and analyze network traffic for monitoring, security analysis, or compliance purposes.
* Demonstrated expertise in implementing VPC Transit Gateway to simplify network connectivity and routing between multiple VPCs, VPNs, and on-premises networks.
* Proficient in implementing VPC ingress and egress filtering using network ACLs and security groups to enforce fine-grained network access control.
* Experienced in configuring VPC peering connection or VPN connection options like transit VPC, Direct Connect, or AWS VPN CloudHub for scalable and secure network connectivity.
* Skilled in implementing VPC endpoints for AWS services like Amazon SNS, Amazon SQS, or Amazon API Gateway to securely access these services from within the VPC.
* Demonstrated expertise in utilizing VPC flow logs and network monitoring tools to analyze network traffic patterns, identify anomalies, and troubleshoot connectivity issues.
* Proficient in implementing VPC endpoint policies and AWS Identity and Access Management (IAM) policies to enforce granular access controls and permissions for resources accessed through VPC endpoints.
* Experienced in implementing VPC peering or VPN connection failover solutions using AWS Route 53 DNS failover or Elastic IP address reassignment for enhanced availability and reliability.
* Proficient in identifying and resolving VPC connectivity issues, such as instances unable to communicate with each other or access the internet, by analyzing route tables, security group rules, and network ACL configurations.
* Experienced in diagnosing and resolving VPC peering connectivity issues, including misconfigured route tables, incompatible IP address ranges, or missing peering connection authorizations.
* Skilled in troubleshooting VPN connectivity issues, such as authentication

failures, tunnel disruptions, or routing conflicts, by analyzing VPN configuration settings and logs.

* Demonstrated expertise in troubleshooting VPC security group rules and network ACL configurations to allow or restrict traffic flow based on desired network access policies.
* Proficient in diagnosing and resolving network performance issues within VPC, such as high latency or packet loss, by analyzing network flow logs and utilizing network monitoring tools.
* Experienced in troubleshooting VPC endpoint connectivity issues, including endpoint policy misconfigurations, DNS resolution problems, or incompatible service endpoint configurations.
* Skilled in identifying and resolving VPC route propagation issues, such as misconfigured route tables or missing route table associations, to ensure proper network routing within the VPC.
* Demonstrated expertise in troubleshooting VPC peering connection issues, such as asymmetric routing or security group conflicts, by analyzing VPC peering connection status and configurations.
* Proficient in analyzing VPC flow logs and utilizing CloudWatch metrics to troubleshoot network traffic issues, identify anomalies, and investigate security incidents.
* Experienced in collaborating with AWS Support, utilizing AWS Trusted Advisor, or utilizing third-party network diagnostic tools to investigate and troubleshoot complex VPC-related issues.
* Proficient in troubleshooting VPC internet connectivity issues, such as misconfigured internet gateways, incorrect route table settings, or issues with Network Address Translation (NAT) gateways.
* Experienced in diagnosing and resolving VPC DNS resolution issues, including misconfigured DNS settings, DNS resolution failures, or domain name resolution conflicts.
* Skilled in troubleshooting VPC security-related issues, such as unauthorized access attempts, security group misconfigurations, or compromised instances within the VPC.
* Demonstrated expertise in troubleshooting VPC connectivity issues with external

resources, such as on-premises networks, AWS Direct Connect, or third-party VPN connections.

* Proficient in analyzing VPC flow logs and utilizing CloudTrail logs to investigate and troubleshoot security incidents, unauthorized access attempts, or unusual network traffic patterns.
* Experienced in diagnosing and resolving VPC routing issues, including incorrect route table entries, route propagation problems, or routing table conflicts between VPCs or subnets.
* Skilled in troubleshooting VPC Elastic IP (EIP) address issues, such as incorrect EIP associations, EIP blacklisting, or issues with Elastic Network Interfaces (ENIs).
* Demonstrated expertise in troubleshooting VPC network performance issues, such as high latency, network congestion, or bandwidth limitations, by analyzing network metrics and performance data.
* Proficient in diagnosing and resolving VPC peering connection issues, such as stale or inactive peering connections, peering connection limits, or compatibility issues between VPCs.
* Experienced in utilizing VPC flow logs and network packet capture tools to capture and analyze network traffic for troubleshooting complex network issues or performance bottlenecks.