**AWS EKS Resume Points**

Here are some resume points related to AWS Elastic Kubernetes Service (EKS):

* Proficient in deploying and managing Kubernetes clusters using AWS EKS, ensuring high availability, scalability, and fault tolerance.
* Experienced in designing and implementing EKS architecture, including node group configurations, networking, security, and integration with other AWS services.
* Skilled in deploying containerized applications on EKS clusters using tools like Kubernetes manifests or Helm charts, ensuring proper resource allocation and configuration.
* Demonstrated expertise in leveraging EKS managed node groups or self-managed nodes to scale cluster capacity based on application demands and optimize cost.
* Proficient in configuring and managing EKS networking components, including VPC, subnets, security groups, and load balancers, to ensure secure and efficient communication within the cluster.
* Experienced in implementing EKS security best practices, such as IAM roles for service accounts (IRSA), AWS Secrets Manager integration, and pod security policies, to enhance cluster security.
* Skilled in utilizing EKS features like Cluster Autoscaler, Horizontal Pod Autoscaler (HPA), and Pod Disruption Budgets (PDB) to achieve efficient resource utilization and application performance.
* Demonstrated expertise in integrating EKS clusters with container registry services like AWS Elastic Container Registry (ECR) or third-party solutions for seamless image deployment.
* Proficient in implementing EKS cluster upgrades and managing Kubernetes version compatibility to leverage the latest features and security patches.
* Experienced in troubleshooting EKS cluster issues, including container deployment failures, network connectivity problems, performance bottlenecks,

and application scaling challenges.

* Proficient in configuring and managing EKS cluster networking, including VPC peering, subnet routing, and ingress/egress traffic control, to ensure secure and efficient communication within the cluster.
* Experienced in implementing EKS cluster autoscaling using AWS Auto Scaling groups or Kubernetes cluster autoscaler to dynamically adjust the cluster size based on resource utilization and application demands.
* Skilled in utilizing EKS managed node groups and Spot Instances to optimize cost while maintaining cluster capacity and availability.
* Demonstrated expertise in implementing EKS cluster logging and monitoring using tools like Amazon CloudWatch, Fluent Bit, or third-party solutions to gain visibility into cluster performance and troubleshoot issues.
* Proficient in configuring EKS cluster access and authentication using IAM roles, AWS Security Token Service (STS), or external identity providers to ensure secure access control for cluster users.
* Experienced in deploying and managing EKS Fargate, a serverless compute engine for Kubernetes, to run containerized applications without managing the underlying infrastructure.
* Skilled in integrating EKS clusters with AWS services like AWS App Mesh or AWS Identity and Access Management (IAM) for enhanced service mesh capabilities and fine-grained access control.
* Demonstrated expertise in utilizing Kubernetes Operators or AWS Controllers for EKS to manage and automate the lifecycle of AWS resources and third-party applications within the cluster.
* Proficient in implementing EKS cluster upgrades and conducting rolling updates to ensure minimal disruption and maintain application availability.
* Experienced in troubleshooting EKS cluster issues, including pod scheduling failures, container runtime errors, networking misconfigurations, or performance bottlenecks, utilizing Kubernetes and AWS-native tools for diagnosis and resolution.
* Proficient in analyzing EKS cluster logs, including container logs, system logs, and control plane logs, to identify and troubleshoot issues related to application errors, network connectivity, or resource utilization.
* Experienced in diagnosing and resolving EKS pod scheduling failures, including issues with resource requests/limits, node affinity/anti-affinity, or pod readiness checks.
* Skilled in troubleshooting EKS container runtime errors, such as image pull failures, container crashes, or resource contention, using tools like kubectl, describe commands, or container-specific diagnostics.
* Demonstrated expertise in investigating and resolving EKS network connectivity issues, including pod-to-pod communication, service discovery, or external access problems, by analyzing network configurations, security groups, or load balancer settings.
* Proficient in diagnosing and resolving EKS cluster performance bottlenecks, such as high CPU/memory utilization, slow response times, or scaling inefficiencies, by analyzing metrics, logs, and resource utilization.
* Experienced in troubleshooting EKS storage-related issues, including persistent volume (PV) provisioning failures, file system errors, or data corruption, by analyzing storage configurations, access permissions, or storage class settings.
* Skilled in identifying and mitigating EKS security vulnerabilities, such as container image vulnerabilities, misconfigured access controls, or unauthorized pod deployments, by leveraging EKS security features and best practices.
* Demonstrated expertise in investigating and resolving EKS cluster scaling issues, including improper pod autoscaling behavior, incorrect cluster auto scaling configurations, or insufficient cluster capacity for application demands.
* Proficient in troubleshooting EKS control plane issues, such as API server errors, etcd database problems, or certificate expiration, using AWS CloudWatch logs, EKS diagnostic commands, or AWS Support resources.
* Experienced in collaborating with development teams, system administrators, or AWS Support to troubleshoot complex EKS issues, leveraging log analysis, monitoring tools, and Kubernetes-specific debugging techniques.
* Proficient in analyzing EKS cluster metrics and utilizing AWS CloudWatch alarms to proactively identify and troubleshoot issues related to resource utilization, performance degradation, or capacity constraints.
* Experienced in troubleshooting EKS pod evictions and rescheduling events, including issues with resource contention, node failures, or pod anti-affinity

configurations.

* Skilled in diagnosing and resolving EKS ingress and load balancer issues, such as misconfigured routing rules, SSL certificate mismatches, or target group registration problems.
* Demonstrated expertise in troubleshooting EKS cluster upgrades, including issues with version compatibility, control plane health checks, or etcd database migrations.
* Proficient in analyzing EKS cluster events and auditing logs to identify unauthorized access attempts, security breaches, or abnormal behavior within the cluster.
* Experienced in troubleshooting EKS authentication and authorization issues, including problems with IAM roles, RBAC configurations, or Kubernetes service accounts.
* Skilled in investigating and resolving EKS pod image pull failures, such as authentication errors, image registry availability, or network connectivity issues.
* Demonstrated expertise in troubleshooting EKS pod crashes and restart loops, including issues with application dependencies, resource limits, or container runtime configurations.
* Proficient in diagnosing and resolving EKS persistent volume (PV) and persistent volume claim (PVC) issues, such as storage provisioning failures, mounting errors, or access permission problems.
* Experienced in collaborating with AWS Support or engaging with the Kubernetes community to troubleshoot complex EKS issues, leveraging documentation, forums, and expert advice.