CASSIDY
CONSULTING GROUP

Platform Engineer

Description: Cassidy Consulting Group is seeking a Platform Engineer. This is a W-2 job opportunity. Please visit our website to learn more about Cassidy Consulting Group – https://www.cassidyconsulting.us.

Position Description:
This position is for a Platform Engineer supporting the Army Edge Computing Capability (AECC) project that ALTESS is fielding for the US Army. The AECC solution is a containerized, Kubernetes-based, multitenant hosting environment for hosting Army enterprise and tactical applications. AECC is utilizing Kubernetes and potentially Red Hat OpenShift to implement a cloud-native, software-defined infrastructure across multiple global sites. ALTESS provides value-added common and managed services built on top of the Kubernetes foundation, which hosted Army applications will require. ALTESS is a managed service provider (MSP) and hosting services provider for Army applications. ALTESS is a Product Lead office under Capability Program Executive (CPE) Enterprise Software and Services (CPE ES2).

Position Responsibilities:
- Work with Government engineers to develop and maintain the AECC Kubernetes-based architecture.
- Develop, deploy, and maintain Infrastructure as Code (IaC) for the deployment and sustainment of the Kubernetes platform in the AECC.
- As applications are hosted on the AECC solution, utilize IaC for the provisioning of customer namespaces and containerized workloads.
- Provide daily administration of the Kubernetes platform, including patching and upgrading of all Kubernetes components (e.g., control plane, worker nodes, CNI plugins, CSI drivers, and CRI runtimes).
- Configure and manage Container Network Interface (CNI) plugins (e.g., Calico, Cilium, OpenShift SDN) to ensure secure and efficient networking for Kubernetes workloads.
- Deploy and manage Container Storage Interface (CSI) drivers to enable dynamic provisioning of persistent storage for containerized workloads (e.g., OpenShift Data Foundation, Ceph).
- Monitor utilization of all container orchestration resources and notify the AECC Lead when additional resources will be required.
- Harden the Kubernetes platform per cloud-native best practices and the required government cybersecurity controls.
- Troubleshoot and perform root cause analysis of any hosting platform issues, including Kubernetes networking, containerized workloads, persistent storage, and runtime issues.
- Develop and maintain system, infrastructure, and process documentation (e.g., system diagrams, network topology, Kubernetes configurations, CSI driver configurations, CRI runtime configurations, standard operating procedures).
- Provide on-call support for triage and resolution of after-hours production incidents.
- Make recommendations for improvements to security, scalability, manageability, and performance across a wide variety of containerized network, storage, and compute services.
- Build, configure, and administer Kubernetes clusters.
- Implement and manage container registries (e.g., Docker Hub, Harbor, Red Hat Quay) for secure image storage and distribution.
- Deploy and manage persistent storage solutions for containerized workloads (e.g., OpenShift Data Foundation, Ceph, NFS).

Required Skills:
- Senior-level experience with Kubernetes-based platforms, such as Red Hat OpenShift, Rancher, or vanilla Kubernetes.
- Experience with Container Storage Interface (CSI) drivers for dynamic provisioning of persistent storage (e.g., OpenShift Data Foundation, Ceph, AWS EBS, Azure Disks).

- Strong Infrastructure as Code (IaC) using tools like Helm, Kustomize, or Terraform, and GitOps experience using ArgoCD, or Flux.
- Strong troubleshooting skills across the entire technology stack – Kubernetes networking, storage, server, and containerized applications.
- Familiarity with persistent storage solutions for Kubernetes workloads (e.g., OpenShift Data Foundation, Ceph, NFS).
- Experience with monitoring and observability tools for Kubernetes (e.g., Prometheus, Grafana, Elasticsearch, Fluentd, Kibana).

Desired Skills:
- Strong knowledge of Kubernetes networking concepts, including Container Network Interface (CNI) plugins (e.g., Calico, Cilium, OpenShift SDN), service discovery, ingress controllers, network policies, and DNS management.
- Proficiency in building, configuring, and administering Kubernetes clusters in enterprise environments.
- Experience with container orchestration tools and technologies (e.g., Docker, Podman, Kubernetes).
- Experience with container registries and image management (e.g., Docker Hub, Harbor, Red Hat Quay).
- Strong automation and Infrastructure as Code (IaC) skills using tools like Ansible, Terraform, Python, Pulumi.
- Working knowledge of DoD Security Technical Implementation Guides (STIG) and the Information Assurance Vulnerability Management (IAVM) process, and/or industry hardening best practices and processes.
- Familiarity with DevSecOps practices, including CI/CD pipeline integration for containerized workloads.

Education & Experience: Bachelor's degree or higher in IT-related field

Required Certifications:
- Security+ or equivalent DoD 8570.01-M IA Tech Level II certification.
- Must have (or obtain within 6 months of hire) a Computing Environment certification in a related field:
  - Certified Kubernetes Administrator (CKA).
  - Red Hat Certified Specialist in OpenShift Administration.
  - Certified Kubernetes Security Specialist (CKS).
  - Other equivalent Kubernetes or container-related certifications.

Security Clearance: DoD Secret Clearance

Location: Radford, VA (hybrid/telework onsite as needed)

Cassidy Consulting Group is an Equal Employment Opportunity employer. Cassidy Consulting Group prohibits discrimination against employees and qualified applicants for employment on the basis of race, color, religion, sex (including pregnancy), age, disability, marital status, national origin, veteran status, or any other classification protected by applicable discrimination laws.