Cloud Engineer, OCI

Concept Plus is a mission-focused technology solutions provider that transforms IT concepts into impactful solutions for federal agencies. Headquartered in Fairfax, VA, we bring the agility, responsiveness, and customer intimacy of a small business combined with the quality and infrastructure of a larger firm.

Recognized as an award-winning Oracle partner, we have delivered innovative solutions across Defense, Intelligence, Civilian, Health IT, and Tribal sectors. Our highly certified experts build systems that drive efficiency, accelerate modernization, and ensure mission outcomes with certainty.

We offer competitive pay, comprehensive health, dental, and vision insurance, paid life insurance, paid time off, 11 paid holidays, performance bonuses, tuition reimbursement, unlimited training, and the opportunity to thrive in a collaborative, flexible, and innovative environment.

For more information, visit www.conceptplus.com.

About the role

Concept Plus LLC is seeking an Oracle OCI Cloud Engineer to provision, administer, and sustain Oracle Cloud Infrastructure (OCI) environments in support of an Oracle eBusiness, OCI hosted common services program. In this role, you will be responsible for the day-to-day administration, configuration, monitoring, and optimization of OCI resources including Compute, Networking, Storage, IAM, and related services within the Cloud One-provisioned OCI tenancy. You will work within an Integrated Team Structure alongside cloud architects, DevSecOps engineers, database administrators, and cybersecurity personnel to ensure the scalability, availability, and security of common services. This role requires 3 to 5 years of hands-on OCI administration experience and an active Oracle Cloud Infrastructure certification. An active Secret clearance and DoD 8140/8570 IAT-II or higher certification are required to start.

What you'll do

- Provision, configure, and administer OCI resources including Compute instances, Virtual Cloud Networks (VCN), subnets, security lists, route tables, gateways, block and object storage, and Identity and Access Management (IAM) policies and compartments
- Monitor OCI environment health, performance, and capacity utilization using OCI Monitoring, Logging, and Observability services; respond to alerts and resolve infrastructure issues in alignment with 24/7/365 operational support requirements
- Support environment migrations to OCI, including lift-and-shift of existing workloads, resource rightsizing, and post-migration validation
- Implement and maintain OCI security controls including compartment isolation, security zones, Cloud Guard, Vault-managed secrets, and network security group (NSG) policies in compliance with DoD RMF and Cloud One authorization requirements
- Execute patching and maintenance activities for OCI-hosted infrastructure, including compute patching, OS-level updates, and OCI platform service upgrades, per approved change management procedures

- Support backup, restore, and disaster recovery operations, including OCI Object Storage lifecycle policies, cross-region replication configurations, and DR/COOP failover testing
- Collaborate with the DevSecOps Lead to implement and maintain IaC (Terraform) templates for repeatable, compliant OCI environment provisioning
- Document OCI configurations, runbooks, and standard operating procedures (SOPs) to support operational continuity and knowledge transfer
- Support the Technical Lead in implementing OCI architecture decisions, including the migration from legacy Oracle products to OCI-native equivalents (e.g., OCI GoldenGate Microservice, OCI IAM SSO Asserter, OCI Analytics Cloud)
- Participate in Integrated Team ceremonies including sprint planning, standups, and retrospectives; contribute to backlog refinement for infrastructure-related work items
- Assist the Cybersecurity Lead/ISSO with continuous monitoring, vulnerability scanning remediation, and ATO evidence collection for OCI-hosted resources
- Support service management and onboarding processes, including provisioning new mission partner environments and managing access controls per DESMF-aligned procedures
- Monitor and respond to OCI service quota limits, cost anomalies, and tenancy governance requirements in coordination with DISA and Cloud One administrators

Qualifications

- US Citizen
- Bachelor's degree in Information Technology, Computer Science, Systems Engineering, or related technical field; equivalent work experience considered
- 3–5 years of hands-on Oracle Cloud Infrastructure (OCI) administration experience, including Compute, Networking, Storage, IAM, and Monitoring
- Active Oracle Cloud Infrastructure certification required at time of hire (e.g., OCI Foundations Associate, OCI Cloud Operations Professional, OCI Architect Associate, or equivalent)
- Demonstrated experience provisioning and managing OCI tenancies, compartments, VCNs, and IAM policies
- Experience with OCI security services including Cloud Guard, Security Zones, OCI Vault, and network security groups
- Experience supporting backup/restore, capacity management, and patching activities in a cloud-hosted environment
- Familiarity with DoD RMF, ATO processes, and cloud security compliance requirements
- Active DoD Secret clearance required to start; must be maintainable for the duration of the program
- Active DoD 8140/8570 IAT-II or higher certification required at time of hire (qualifying certifications include CompTIA Security+ CE, CompTIA CySA+, GSEC, SSCP, GICSP, CND, or any IAT-III equivalent such as CASP+ CE, CISSP, CISA, CCNP Security, GCED, or GCIH)

- # Preferred Qualifications

- Active Top Secret (TS) security clearance; candidates holding an active TS clearance will be given strong preference as the program's operational scope and data sensitivity may require TS access
- Experience administering Linux (RHEL, Oracle Linux, or equivalent) server environments, including OS configuration, hardening, scripting, and performance tuning
- Experience with Microsoft Windows Server administration, including Active Directory, Group Policy, and Windows-based workload management
- Hands-on experience with container technologies including Docker and Kubernetes (K8s), including image management, container runtime administration, and cluster operations
- Oracle Database Administration (DBA) experience, including database provisioning, patching, backup/recovery (RMAN), and performance monitoring on OCI or on-premises environments
- Familiarity with Oracle Fusion Middleware components (WebLogic Server, Oracle SOA Suite, Oracle HTTP Server) and associated installation, configuration, and patching procedures · Experience implementing and managing DR/COOP architectures using Oracle GoldenGate (classic or Microservice) for near real-time data replication and Oracle Active Data Guard for standby database synchronization, failover, and switchover operations
- Experience with OCI DevOps services, OCI Container Engine for Kubernetes (OKE), OCI Artifact Registry, or OCI Resource Manager (Terraform-as-a-service) · Experience operating within a DISA-managed or Cloud One cloud environment, including familiarity with IL4/IL5 authorization boundaries and tenancy governance processes
- Familiarity with ITIL service management practices and DESMF-aligned operations procedures
- Prior experience supporting AFLCMC, BES Directorate, or a DoD ERP program of record
- Additional OCI certifications (e.g., OCI Architect Professional, OCI Security Professional, or OCI Database Professional) are a strong plus

Concept Plus is an Equal Opportunity Employer. As such, we will give your application full consideration without regard to your race, color, religion, sex, age, national origin, disability, veteran status, sexual orientation, gender identity, or any other classification protected by federal, state, or local law.