Multi-Cloud SysOps · FinOps · Observability

Cloud Operations & Platform Engineering

AWS · Azure · Linux & Windows · Datadog · FinOps

Client Engagement Portfolio · April 2026 · Confidential

2	11+	FinOps	Datadog
Cloud Platforms	Core Responsibilities	Cost Champion	Observability Lead

This portfolio covers multi-cloud operations engineering across AWS and Azure — spanning production infrastructure management, cross-platform system administration, FinOps cost optimisation, patch lifecycle ownership, backup and DR compliance, security hardening, and enterprise-grade observability with Datadog and cloud-native monitoring tools.

1 PRODUCTION ENVIRONMENT MANAGEMENT — AWS & AZURE

- ■Manage and support production environments across AWS and Azure, ensuring high availability and performance SLAs
- ■Perform Linux (RHEL, Ubuntu) and Windows Server administration: disk management, services, and user access
- ■Execute deep-dive troubleshooting using log analysis, strace, perf, OS-level debugging, and cloud-native diagnostics
- ■Proactively identify and remediate performance bottlenecks before they reach end-user impact thresholds
- ■Maintain operational runbooks, incident playbooks, and post-mortem documentation for all production environments

EC2 / Azure VMs	Linux / Windows Server	Log Analysis	strace / perf	Runbooks	Incident Response

2 FINOPS — CLOUD COST OPTIMISATION & GOVERNANCE

- ■Champion FinOps culture across engineering and stakeholder teams, driving cost-awareness in architecture decisions
- ■Actively monitor cloud spend and implement rightsizing for EC2, Azure VMs, and underutilised managed services
- ■Manage Reserved Instances, Savings Plans (AWS), and Azure Reserved VM Instances to optimise committed spend
- ■Identify and eliminate zombie resources: unattached EBS/disks, idle load balancers, orphaned snapshots, and stale IPs
- ■Utilise AWS Cost Explorer and Azure Cost Management to generate reports and actionable insights for leadership
- ■Implement tagging standards, budget alerts, and cost anomaly detection across all accounts and subscriptions

★ FinOps Core Discipline

AWS Cost Explorer	Azure Cost Mgmt	Reserved Instances	Savings Plans	Rightsizing	Tagging Governance

3 PATCH MANAGEMENT — CROSS-PLATFORM FLEET LIFECYCLE

- ■Own the end-to-end patch lifecycle for heterogeneous fleets across AWS (Linux/Windows) and Azure environments
- ■Utilise AWS Systems Manager (SSM) Patch Manager for automated patching, compliance reporting, and maintenance windows
- ■Manage Azure Automation Update Management for scheduled patching across Azure VMs and Arc-connected machines
- ■Define patch baselines, approval rules, and exception handling for critical production workloads
- ■Track patch compliance dashboards and generate audit-ready reports for security and governance stakeholders

AWS SSM Patch Mgr	Azure Update Mgmt	Patch Baselines	Maintenance Windows	Compliance Reports	Azure Arc

4 BACKUP, DISASTER RECOVERY & COMPLIANCE

- Implement and verify backup strategies using AWS Backup for EC2, RDS, EFS, and DynamoDB workloads
- Manage Azure Recovery Services Vaults for VM, SQL, and file share backup with geo-redundant retention
- Define and validate RTO/RPO targets through scheduled DR drills and point-in-time restore testing
- Ensure disaster recovery compliance through automated backup reports and vault audit trails
- Manage cross-region and cross-account backup policies to meet data residency and compliance requirements

AWS Backup	Azure Recovery Vault	RTO / RPO	DR Drills	Cross-Region Backup	Compliance Reports

5 SECURITY HARDENING & ACCESS GOVERNANCE

- Enforce security best practices across AWS and Azure by managing Security Groups, NSGs, and IAM/RBAC roles
- Apply least-privilege access principles to all service accounts, users, and application identities
- Conduct periodic IAM access reviews, unused credential cleanup, and permission boundary enforcement
- Configure AWS Config Rules and Azure Policy for continuous compliance posture monitoring
- Manage secrets rotation via AWS Secrets Manager, Azure Key Vault, and environment-level access controls
- Investigate and respond to security findings from AWS Security Hub, Azure Defender, and GuardDuty

Security Groups / NSGs	IAM / RBAC	Least Privilege	AWS Config	Azure Policy	Key Vault / Secrets Mgr

6 DATADOG — OBSERVABILITY PLATFORM ENGINEERING

- Lead implementation and tuning of Datadog across multi-cloud environments as the primary observability platform
- Create custom Datadog dashboards for infrastructure, application, and business-level metric visibility
- Design monitors and alert policies with precise thresholds, reducing noise and increasing signal-to-alert ratio
- Configure composite monitors, anomaly detection, and forecast alerts for proactive issue identification
- Manage Datadog Agent deployment, integrations (AWS, Azure, Kubernetes, databases), and log pipelines
- Build SLO/SLA tracking widgets and error-budget dashboards for reliability engineering alignment

Datadog Dashboards	Monitors & Alerts	Anomaly Detection	Datadog Agent	SLO Tracking	Log Pipelines

7 CLOUD-NATIVE MONITORING — CLOUDWATCH & AZURE MONITOR

- Configure and maintain AWS CloudWatch: metric namespaces, log groups, dashboards, and composite alarms
- Deploy Azure Monitor with diagnostic settings, Log Analytics workspaces, and action groups for alert routing
- Establish baseline metric collection for CPU, memory, disk, network, and application health across all platforms
- Implement CloudWatch Contributor Insights and Anomaly Detection for intelligent threshold management
- Correlate multi-cloud observability data to provide unified operational visibility across AWS and Azure

AWS CloudWatch	Azure Monitor	Log Analytics	Composite Alarms	Baseline Metrics	Anomaly Detection

Across all seven domains, operations are delivered with an automation-first, security-by-design mindset — combining cloud-native tooling, FinOps discipline, and enterprise observability to maintain high-performing, cost-efficient, and resilient production environments on both AWS and Azure.