Quentin Myers

Email: quentinmyers52@gmail.com

Phone Number: 706-981-8447

Summary:

 DevOps engineer with a heavy focus on managing and monitoring AWS cloud environments, managing multiple AWS accounts and setting up access controls and guardrails for users, setting up and configuring comprehensive end to end monitoring of cloud environments with tools like Prometheus, DataDog, Splunk, AWS X-ray. I maintain the platform through Terraform, write extensive code for Lambda functions in AWS in Python, and have managed multiple different containerized environments (ECS, EKS)

Professional Experience:

**AWS Platform Engineer | June 2021 - Present | *BlackSpade Financial Solutions | Atlanta, GA***

* Spearheaded a long term effort to work towards cost optimization strategies for a large scale trade processing application that processes millions of financial transactions per day.
* Fed CloudTrail logs into ElasticSearch cluster, indexed all of the incoming tokens generated for our multi-tenant EKS clusters, performed verification to make sure that each pod was assigned the proper IAM roles associated with the token that belong to their respective namespace
* Worked with Terraform to deploy any lasting changes to our infrastructure across DEV, STAGING, and PROD environments.
	+ Used separate CI/CD deployment pipelines for running terraform plan/apply/destroy for both prod and non-prod environments
	+ Wrote modules for adding new features like lambdas, autoscaling groups, ECS clusters, S3 buckets, etc..
	+ Would implement and test new features through management console in DEV environment, then after the successful logs were produced would add in the appropriate terraform modules to have the changes backed up in IAC
* Wrote Jenkinsfiles for developers to build and release changes for their application code.
* Scripted Ansible playbooks to bootstrap our EC2 instances after Terraform Apply stage to get them prepared to start running their respective services
* Wrote bash scripts to automate common tasks like grabbing a list of IPs from a list of hosts running in our cloud environment
* Edited and worked with various Dockerfiles used by the developers to package up their application and ship off the images to Nexus
* Created the initial solution to cut down on the cost of running our ECS clusters by 2 thirds of the original cost per day across the sum of all our environments:
	+ Hosted meetings with the architecture and cloud security team to approve the rollout strategy
	+ Helped design the proof of concept and wrote almost all of the python logic in the Lambdas for dynamically scaling our clusters up and down at various points throughout the day
	+ Used boto3 library along with client libraries for ASGs, ECS clusters, SSM parameter store, S3 buckets, and EC2 instances
	+ Made large significant improvements to the python code for the scaling logic as well as adding in a number of features such as being able to accept payloads from the java spring boot microservices and do some internal logic to make decisions as to which scaling strategy to implement with our clusters
* Created all the Splunk alerts and DataDog alerts for our cloud environment.
	+ Synched up the splunk alerts with email and PagerDuty along MIR3 schedules to notify different team leads depending on the time of day (12 hr rotation between US and India team lead with some overlap)
	+ Backed up all the splunk and alerts in gitlab and excel spreadsheets to have a hard copy of documentation for all of our alerts
	+ Created health check monitors, synthetic monitors, and API based alerts for useful metrics across our cloud environment such as 4xx errors on S3 buckets or average of CPU Utilization across our ECS clusters
	+ Created splunk queries to send email reports at the beginning and end of every day for the clusters, all the services running on them, as well as whether or not their desired task count matched up to the actual task counts they were meant to have at that specific time.
* Developed, documented and executed test plans and test cases with Software engineers, Product managers and QA engineers in an Agile team environment.
* Performing new functionality, regression manual testing and Selenium.
* Conduced automated security scanning of pipelines with tools: Kiuwan and Synk.
* Created Power Query imports to transform and clean data, to create a data model using power BI Desktop.

**DevSecOps Engineer | March 2013 - March 2021 | *United States Air Force | Atlanta, GA***

* Configured and set up Prometheus for scraping various metrics at different intervals on various Kubernetes pods running as a sidecar container, and outputting the metrics of CPU, RAM, Disk Space to Grafana dashboards.
* Deployed DataDog agent to run on our various VMs and setup monitors, dashboards, and alerts for our service endpoints and for S3 buckets, EKS clusters, RDS instances, and DynamoDB tables
* Performed security and privacy assessments and audits for SOC frameworks.
* Used Terraform to deploy to hybrid cloud environments
* Setup disaster recovery and automatic DNS failover using Route53 failover strategies between our primary and backup region.
* Managed multiple AWS accounts using AWS Organizations and managed the user accounts of various developers through AWS Control Tower.
* Implemented Guardrails, Service Control Policies, and AWS Config rules to place fine-grain access controls on what resources each dev is able to touch.
* Managed and updated IAM roles and policies
* Managed dynamic inventories with Ansible to automatically get updated IP addresses of new hosts without having to manually add them to hosts file
* Used Terraform to deploy to hybrid cloud environments
* Setup disaster recovery and automatic DNS failover using Route53 failover strategies between our primary and backup region.
* Worked with AWS WAF and Shield in the central Firewall Manager dashboard. Setup whitelists and blacklists in WAF along with rules
* Used AWS IAM analyzer to audit our IAM policies
* Used AWS Certificates Manager as well as AWS Secrets manager to store certs, passwords, environment variables
* Used AWS X-Ray for tracing request flows through Java Spring boot applications running on our EC2 instances, helping us understand the flow of data and interactions.
* Came up with various cost savings strategies by using AWS Cost Explorer to identify areas for potential savings and writing automation scripts to scan through our environment and clean up certain unused resources.
* Setup user pools and MFA for Single Sign On with AWS Cognito
* Setup CI/CD pipelines from scratch for our developers using Jenkins webhook, building projects using tools like Maven or NPM, using tools like SonarQube to do code coverage
* Maintained the capability to provide timely and accurate cyber intelligence support within a 24/7 operation.
* Managed, monitor servers and network applications in conjunction with support team (Tools: Netsparker, Nessus).
* Identified potential IDS threats and managed resolution of security violations.
* Updated military personnel data system (PDS)
* Created Jenkins pipelines to automate build, test and deployment stages for various military related applications.
* Maintained Jenkins server configurations, ensuring high availability and performance, while managing plugin updates and security patches.
* Designed, implemented and managed CI/CD pipelines using Jenkins, enabling reliable software releases.

**Systems Engineer | April 2008 - February 2013 | *Volkswagen | Herndon, VA***

* Install, configure, and maintain physical servers, storage devices, and networking equipment within the company's data centers.
* Monitor the health and performance of on-premise infrastructure, using tools like monitoring software, hardware diagnostics, and log analysis.
* Conduct regular hardware and software updates, including firmware upgrades, security patches, and OS updates, to ensure systems are up-to-date and secure.
* Collaborate with network engineers to manage local area networks (LANs), wide area networks (WANs), and virtual private networks (VPNs).
* Maintain and troubleshoot backup and disaster recovery solutions to ensure data integrity and business continuity.
* Create and manage user accounts, permissions, and access controls for on-premise systems and applications.
* Implement and manage virtualization technologies like VMware or Hyper-V to optimize resource utilization and enable efficient provisioning of virtual machines.
* Collaborate with security teams to implement and enforce security policies, firewalls, intrusion detection systems, and access controls.
* Assist in capacity planning and resource allocation, ensuring that on-premise infrastructure can handle growing workloads.
* Support software development teams by provisioning development and testing environments and providing technical assistance.
* Troubleshoot hardware, software, and network issues as they arise, diagnosing and resolving problems to minimize downtime.
* Document on-premise infrastructure configurations, procedures, and troubleshooting steps for internal reference.
* Collaborate with cross-functional teams to evaluate new technologies, hardware, and software for potential adoption.
* Maintain a comprehensive inventory of hardware, software licenses, and other IT assets within the on-premise environment.
* Provide on-call support for critical infrastructure components, responding to incidents and emergencies in a timely manner.
* Ensure compliance with industry regulations and best practices related to on-premise infrastructure management.

Education:

Monad University , Uttar Pradesh, India

Bachelors, Computer Science

ITT Technical Institute , Canton-Michigan
 Associates, Computer and Electronics Engineering