Rajesh V

**571-771-4111** | [rajv.aws@gmail.com](mailto:rajv.aws@gmail.com)

A hexagon with text on it

Description automatically generatedA picture containing text, sign, stop, outdoor

Description automatically generated

**SUMMARY**

* **10+** years of overall experience in IT.
* **7+** years of experience working as **AWS Cloud Security Engineer, AWS IAM Engineer, AWS Infrastructure Engineer.**
* **AWS Certified Security Specialty** and **AWS Certified Solutions Architect Associate.**
* Worked on Enterprise Users **Single Sign On** through browser and through services with third party application hosted in enterprise or cloud using **Active Directory Federation Services**.
* Designed, Configured, and managed public/private cloud infrastructures utilizing **Amazon** **Web Services (AWS) including EC2, Auto-Scaling, AWS Config, Shield, WAF, ANF, Audit Manager, Cognito, Elastic Load Balancer, S3, Cloud Front, RDS, VPC, Route53, Cloud Watch, Cloud Formation, Cloud Front, IAM, Lambda, EBS, RDS, SNS, SQS.**
* Experience with creating Organization Units (**OU**s), IAM roles, IAM groups and writing **SCP**s and **Permission boundaries**.
* In-depth knowledge of Cloud Computing Strategies (**IaaS, PaaS, SaaS**) & building, deploying in and maintaining the cloud environment.
* Good experience with Authentication, Authorization, Vulnerability Assessment and Scan.
* Strong knowledge of AWS **Lambda**, Amazon Simple Queue Service (Amazon **SQS**), Amazon Simple Notification Service (Amazon **SNS**), and Amazon Simple Workflow Service (**SWF**)
* Good experience on **Terraform** Enterprise and AWS Cloud Formation.
* Build a serverless application using step functions, **API gateway, Lambda.**
* Strong knowledge with Web Services, **API Internet Gateway,** **Transit Gateway** and application integration development and design.
* In-Depth Knowledge with IAM principals (**Users, Groups, Roles, Policies**), Provided **Delegation** of Access between accounts using STS Assume Role Tokens Following hub and Spoke Model.
* Configured and supported **SAML** 2.0 with various partners to create **SSO/FEDERATION** between our **Identity Provider** Landing page and **Service Provider's** Applications.
* Experience with integrating **OKTA** and worked on Multifactor Authentication using **OKTA**.
* Has experience in bash and python scripting with focus on DevOps tools, **CI/CD** and **AWS Cloud Architecture** and **Azure** Infrastructure Deployment.
* Created and wrote shell scripts **Bash, Ruby, Python and PowerShell** for automating tasks.
* Administered tasks like taking backups, expanding file system disk space, creating NFS mounts.
* Experience with Subversion Control, Build, Configuration Management tools like **GIT**, **MAVEN**, **CHEF**, **DOCKER**, **ANSIBLE**, **Kubernetes, EKS** and Integration & Monitoring tools like **Splunk,** **JENKINS** on Linux, and Windows Environment.
* Experience with **GraphQL** APIs and **AppSync** and connect to DynamoDB.
* Experience with **Azure** in **infrastructure support, systems architecture, Integration, automation** and middleware planning, implementation, performance, and support across distributed and mainframe platforms.
* Working with **Route 53, DNS failover** and setting up Latency based routing, weighted routing policies. Worked with scripting Automation for **JavaScript, Linux/Unix, Python, Perl, Bash, Ruby.**
* Experience with Tools like **Jira**, **Confluence, Slack**, Federation Services like Identity provider and Service provider for Single sign on with **SAML** 2.0 Authentication.

**Core Competencies**

**Amazon Web Services | IAM | Azure| ADFS | Identity Federation | SAML Authentication | Docker | Ansible | Python | JSON | JavaScript | Cloud Infrastructure Management | TCP/IP Protocols | Big Data Services | Automation Tools**

**Professional Experience**

**Senior Cloud Security Engineer | Kroger - Remote July*’2022 – Present***

* Implemented serverless architecture using **API Gateway**, Lambda and Dynamo DB and deployed AWS Lambda code from S3 buckets.
* Used **API Gateway** to establish communication from Jira server hosted in On Premise to trigger **AWS lambda functions** deployed in AWS cloud and automated creation of IAM Roles.
* Designed the **Federation** Architecture with **Hub and Spoke** model using the SAML authentication for Single Sign On (**SSO**).
* Used **AWS Inspector** and **Guard Duty** to perform Port scanning and perform recommended patches accordingly. Also provides **DLP (Data Loss Prevention)** Solutions to Enterprise.
* Integrated third party **SIEM** tools like **JupiterOne** and **Threat Stack** tools with AWS to provide 24/7 monitoring and alerting and as part of this integration used **SQS** to send the notifications from **cloud trail** and then to the SIEM tools.
* Performing vulnerability scanning and identifying the root cause of the vulnerabilities.
* Created and managed **AWS** **IAM** roles through automation using **Terraform** to integrate into infrastructure.
* Worked on **Organization Units, Permission boundaries, SCPs** to guardrail the accounts.
* Configure **AWS Multi Factor Authentication** in **IAM** to implement 2 step authentication of user’s access using Authenticators and AWS Virtual MFA.
* Included **Security Groups, NACL’s, Internet Gateways,** and **Elastic IPs** to ensure safety for organization in AWS public cloud.
* Enabled **AWS Shield, WAF** and **Network Firewall** to safeguard the applications security from DDoS attacks.
* Configured, managed, and ensured database security and integrity.
* Implemented and maintained database backup and recovery procedures.
* Enabled and utilized **AWS Trusted Advisor** to inspect accounts and provide reporting and remediation recommendations.
* Used **AWS Cognito** for data synchronization and allow users to sign in.
* Automated Security Baselines for **S3** buckets such as setting up bucket **ACLs**, Enabling Public Block Access and using bucket policies to provide **least privilege**.
* Managing CDN on Amazon **CloudFront** to improve site performance.
* Utilized Amazon **Route53 to** manage **DNS** zones and also assign public DNS names to Elastic Load Balancers (**ELB**) Ips.
* Worked on converting existing AWS Infrastructure to Serverless architecture and deploy via **Terraform** and AWS **Cloud Formation** templates.
* Identify internal and external threats or vulnerabilities and remediate security.
* Supported management through risk identification, control testing and process improvement procedures.
* Implemented company policies, technical procedures, and standards for preserving the integrity and security of data, reports and access.
* Managing, provisioning, Application Deployment & Multi-Tier Orchestration using **Ansible** automation.
* Utilized Amazon **Firewall Manager Service** to protect resources across the accounts.
* Used **AWS Audit Manager** to performance audits on industry frameworks SOC2, HIPAA, NIST.
* Created scripts in **Python** which integrated with Amazon API to control instance operations.
* Deployed **Domain Controller** Servers in Dev, Test and prod through automation using **Ansible** playbooks.
* Developed**Security Patterns** and controls For AWS to enforce (**Automate**) Security on the AWS Services that Enterprise Uses. This Security Patterns are compliance of **NIST 800-53, CIS Benchmarks (Center for Internet Security)** and custom standards and AWS Best practices.
* Created Active Directory (**AD**) groups as part of the **Federation** for the **Single Sign On** (SSO) using **SAML** Authentication between the Identity provider and Service Provider (AWS).
* Audit and review the user Policy’s in all Enterprise AWS Accounts to provide the **Least- Privilege** via Roles and Policy’s.
* Worked with Incident Response Team to develop an incident plan for Authentication response Failure. Provisioned Identities using **IAM** solution **OKTA** for Enterprise**.**
* Identifies regulatory changes that will affect information security policy, standards and procedures and recommends appropriate changes.
* Develops and implements security standards, procedures, and guidelines for multiple platforms and diverse systems environments (e.g., corporate, distributed and client server systems).
* Reported findings and advise on remediation efforts.
* Assisted in preparing business application owners prior to external audits.
* Conducted security audits to identify vulnerabilities.

**ENVIRONMENT:** AWS IAM, Inspector, Guard Duty, AD, Shield, Security Hub, Trusted Advisor, EC2, S3, CloudWatch, WAF, ANF, Firewall Manager, Cloud Front, VPC, Lambda, SNS, SQS, API Gateways, Terraform, Ansible, Ansible Tower, Splunk, Jira, Confluence, Slack, Federation Identities, Python.

**Cloud Security Engineer | Amazon Web Services - Remote Apr*’2021 – June 2022***

* Responsible for creating, configuring, and utilizing **AWS VPC** to host clients computing services, virtual networking devices, databases (**RDS**) environment and security configuration.
* Responsible for configuring and spin-up of AWS compute, storage, and messaging services like **EC2, S3, EBS,** and **SNS**
* Articulated audit findings, risks, and detailed recommendations to upper management.
* Monitored use of data files and regulated access to protect secure information.
* Performed risk analysis to identify appropriate security countermeasures.
* Configured multi-account architecture, identity and access management, governance, data security, network design, and logging within provisioned AWS Landing zones.
* Provisioned AWS Landing zones to create a customized baseline of AWS accounts, networks, and security policies.
* Worked on **EC2, VPC, S3, IAM, Volume** and **snapshot, RDS, SNS, CloudWatch, CloudTrail**, and other services.
* Automated **Lambda Functions** using Python that can Fetch AWS Services, Actions from AWS Web pages and Create **Policy templates** to use as part of the **Pipeline**.
* Experience writing **SCPs**, **Permission Boundaries** to enforce **least-privilege** on **IAM** accounts.
* Designed and configured Intrusion Prevention Systems and passive Intrusion Detection Systems in AWS leveraging **AWS Guard Duty**.
* Perform vulnerability assessments and security audits, produce reports of findings, and worked with engineers to implement remedial measures.
* Enabled **AWS Shield** and **AWS Network Firewall** to safeguard the applications security from DDoS attacks.
* Focused on building VPCs from scratch and using AWS **CloudFormation**, creating private and public subnets, security groups, network access lists, configuring internet gateways, OpenVPN, creating **AMI**, understanding of user access management/role-based access/multi factor authentication, API access and, configuration of auto scaling group (ASG) and elastic load balancer (**ELB**) for scaling services.
* Worked with engineers and development teams to ensure that architecture solutions are compliant with security frameworks, such as NIST, ISO 27001/27002, PCI, etc.
* Assisted with design and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, **WAF**, **security groups** and **NACL**s.
* Performed configuration, troubleshooting, and ongoing management of various cloud technologies in the customer’s environment.
* Built infrastructure, networks, and systems for scalability, resiliency, availability, and recovery though infrastructure-as-code.
* Designed and implemented monitoring and protection capabilities to help identify and protect against DoS attacks, MITM, EC2 instance compromise, secret compromise, etc.
* Performed information security **incident response and incident handling** based on risk categorization and in accordance with established procedures (Detection, Triage, Incident analysis, Remediation and Reporting).
* Ensure governance and compliance to published Information Security policies and standards.
* Led root cause analysis, debugging, support, and postmortem analysis for security incidents and service interruptions.
* Created automated workflow to address security related incidents.
* Report findings and advise on remediation efforts.

**ENVIRONMENT:** Incident response, Security assessments and audits, AMI, ELB, AWS IAM, Inspector, Guard Duty, Active Directory, Shield, Security Hub, Trusted Advisor, EC2, S3, CloudWatch, WAF, ANF, Firewall Manager, Cloud Front, VPC, Lambda, SNS, SQS, API Gateways, Federation Identities, Python

**Cloud Security Engineer | ECS Corporate Services- Chantilly, VA *Jan’2018 – Mar’2021***

* Streamline the Process of Access Management, Threat Detection, Remediation Pipeline, Automation Detection.
* Extensive Experience working with Jira for creating Projects, Workflows and User access Management.
* Maintain and support PaaS and **API Gateway** infrastructure and associated tools.
* Used **IAM Access Analyzer** for access management and to identify the resources with elevated privileges.
* Experience working with **SCPs**, **Permission boundaries** to delegate **IAM** roles and users.
* Automated Communication channels through notifications services like **SNS** and **SES**.
* Used Simple Email Service **(SES)** as part of building automation pipelines to notify security team whenever there is a bucket uploaded without a Block public access enabled/ Bucket given public access or data uploaded to S3 buckets is unencrypted.
* Installed **CloudWatch** agent on EC2 servers and used **SNS** service to notify Slack channel for server downtime or utilization increases more the 80 percent CPU.
* Created automated pipelines in AWS **CodePipeline** to deploy **Docker** containers in AWS **ECS** using services like **CloudFormation, CodeBuild, CodeDeploy** and **S3.**
* Design AWS **Cloud Formation** templates to create custom sized VPC, subnets NAT to ensure successful deployment of web applications and database templates.
* Perform troubleshooting and monitoring of the servers on AWS using **Splunk**.
* Manage and monitor multiple user accounts within the firm and providing remediations on accounts that deem to vulnerability threat.
* Understanding of the **NIST** Cybersecurity Framework (CSF)
* Experience working with different security and monitoring tools like **Jupiter One, Threat Stack, StrongDM** to automate and remediate security vulnerabilities to Cloud Infrastructure.
* Experience in performing and/or participating in technical assessments in direct support of a major compliance effort (e.g. **SOC1, SOC 2, HITRUST, HIPAA, PCI, or ISO**)
* Working with different scripting languages like **Python, Groovy script** and **Terraform** for automation.
* Writing **UNIX shell scripts** to automate the jobs and schedule **cron** jobs for job automations.
* Used AWS **Config** to Analyze the Cloud infrastructure and build Auto Remediation for configuration drifts that are out of compliance.
* Experience using AWS **AppSync** to develop **GraphQL** APIs by connecting to data sources like **DynamoDB.**
* Good experience with DevOps tools like **Git, Ansible, Kubernetes.**
* Working experience in AWS with **EKS** by using **CloudFormation.**
* Exercised implementing Tagging resources in AWS Accounts and used these tags for **auditing**, cost exploration and security remediate actions.
* Created AWS Multi Factor Authentication (**MFA**) for instance SSH logon and worked with teams to lockdown **security groups**.
* Developed Automation Pipeline in AWS to Remediate Security incidents using different AWS services like AWS lambda, cloud watch, cloud trail and scripting like python and groovy script.
* Experience in configuring of Network architecture on AWS with **VPC, Subnets, Internet Gateways, NAT, Route Tables.**
* Used **AWS Macie** to Analyze **PHI/PII** data in S3 buckets and write custom quires to enable visibility into the resources that have access to the privileged buckets.
* Applied Industry Standards like **CIS** **Benchmarks**, **NIST, HIPAA and OWASP Top 10** to Implement **security** in AWS Cloud
* Used **Amazon Detective** for security investigation and analysis, used this service mostly to identify **un-authorized access**, abnormal behavior like too Many requests from same API, console/API access from unexpected location, API call during midnights.
* Provided support and resolve issues for the end clients by being in support rotation.

**AWS Infrastructure Engineer | Anthem – Richmond, Virginia *May’ 2016 – Dec’ 2017***

* Automated Pipeline of **Role Creation** that are used as Service Roles for **Cross-Account access.**
* Automated **Lambda Functions** using Python that can Fetch AWS Services, Actions from AWS Web pages and Create **Policy templates** to use as part of the **Pipeline**.
* Created **Step Functions** as part of Role Automation to Read JIRA Input and Fetch **Pre-Generated Policies** from S3 bucket.
* Created JIRA Page that is used a Frontend page for requesting **Role Creation**. This Page helps users to raise tickets and initiate the role Creation Pipeline once Ticket is submitted.
* Automated fetching of **IAM policies** and JIRA Input from user using **Lambda functions** and **Step Functions**.
* On-boarding new users with **MFA** and access policy.
* Deployed application which is containerized using Docker onto a **Kubernetes** cluster which is managed by **EKS**.
* Implemented **Service Control Polices** to enforce **Least Privilege** on Identities and **Control Tower** is used to automate Creation of **Landing Zone** and **Child Accounts**.
* Automated **CI/CD** pipeline using **Code Commit**, Code Build, Code Deploy and **Code Pipeline**. This pipeline will initiate Creation of Role when users submits role JIRA Ticket.
* Created **MySQL** Database tables that are used as JIRA Backend to fetch the AWS Services, App ID’s, and AWS Account Numbers.
* Created Role’s using the Pre-Generated **IAM Policy Templates** based on the JIRA Input.
* Configured **Cloud Watch** to monitor the Role creation and alerts whenever a new role is created.
* Used **Divvy Cloud** and **Splunk** to achieve Compliance and Industry Standards. Followed **NIST 800-53**, **HIPAA** and **Hi Trust** Compliance.
* Used **AWS Config** to implement Custom and Pre-defined Rules to Achieve **Data Privacy** and **Remediate** on Critical issues that are observed.
* Created **Cloud Formation Stack’s** Based on JIRA Input and Pre-Generated Policies that are used for Role creation and This Stacks will be used for Future Role Provision Comparison.
* Used **Guard Duty** and **AWS Inspector** to Scan the infrastructure and Recommend on Findings on Infrastructure Network.

**ENVIRONMENT:** EC2, S3, IAM, Step Functions, Lambda Functions, MySQL, Code Commit, Code Deploy, Code Pipeline, Python, Java.

**Software Developer | VisionTek – Hyderabad, India *Jun 2014 – Aug 2015***

* Design and development of WINDOWS applications using **C# 4.0, AngularJS, .NET MVC 4.0, ADO.NET, XML, AJAX, LINQ** and **SQLServer2012.**
* Worked on a Windows 98 PDA retailer app which is used to get product details when a barcode is scanned by the PDA.
* Worked on complete **Agile Scrum methodology** and User Interface web development in accordance with requirement.
* Designed and developed web pages using **HTML, XHTML, CSS, and jQuery, AngularJS**.
* Worked with business system analysts to understand the requirements to ensure that right set of UI modules been built.
* Maintaining the dynamic and secure websites and web-based applications, including widgets, and templates.
* Built the Responsive Web pages using Bootstrap and Media queries to support various kinds of devices.
* Designed the front-end applications, user interactive (UI) web pages using web technologies likeHTML5 and CSS3.
* Worked on CSS Background, CSS Positioning, CSS Text, CSS Border, Pseudo classes, Pseudo elements etc.
* Made enhancements to existing CSS and DIV tags, made upgrades using Twitter Bootstrap model.
* Used advanced level of jQuery, AJAX, AngularJS, Bootstrap, and CSS layouts.
* Implemented Presentation layer using CSS Framework, AngularJS, Wire-framing, and HTML5.
* Developed data formatted web applications and deploy the script using client-side scripting using.
* Developed **Single Page Application (SPA)** using Angular JS Framework.
* Developed Web Application to replace the existing and legacy Website using Angular JS Framework.
* Develop, install, and configure the applications in the PDA.

**Technologies used**: XHTML, HTML5, CSS3, JavaScript, jQuery, AngularJS, .Net, C#, ASP.Net, ADO.Net, JSON, AJAX, Bootstrap, SQL Server, MySQL, Agile Methodology.

**Web Developer | FonkR Solutions (Hyderabad, India) *JUNE 2012 – JUNE 2014***

* + Design and development of web application using **JavaScript, jQuery, HTML, CSS** and **SQL Server 2010/2008**
  + Responsible for testing, troubleshooting the technical issues and fixing the bugs.
  + Work with the business analysts to analyze the requirements.
  + Involvement in complete software development lifecycle of the project.
  + Write TSQL queries and create indexes on SQL tables.
* Interact with the client for requirements gathering, enhancing the product and provide necessary assistance during the user acceptance testing.
* Developed programs to port the xml data to the database to make the website XML driven.
* Story board design and multiple role web authentication.
* Worked with CSS Selectors, classes, pseudo classes, and Inheritance and cascade concepts.
* Used CSS to embed the online videos for product introduction.
* Implemented Caching, Session State, and Cookie Management, view state, POST and GET techniques.
* Profound Knowledge in Document Object Model (DOM) and DOM functions.
* Worked with several jQuery plugins to make Rich Internet Applications to look intuitive.
* Built dynamic e-mails by using HTML, XHTML, CSS and JavaScript.
* Used AJAX, JSON along with jQuery to request data and response processing.
* Usage of Dependency Injection, DOM manipulation, Directive and Module design.
* Involved in peer-to-peer code reviews and functional testing.

**Technologies used**: HTML, CSS, JavaScript, jQuery, AJAX, DOM, XHTML, Twitter Bootstrap, SQL Server, MySQL.

**Certifications**

* **AWS Certified Solutions Architect – Associate**
* **AWS Certified Security - Specialty**

**Educational Qualifications**

* **Master’s** in **Computer Information Systems and Security** from **Monmouth University, New Jersey** with **3.81 GPA.**
* **Bachelor’s** in **Computer Science and Engineering** from **JNTU, India**.