**Rick Agube**

Houston, TX 77487
60642, Chicago, IL  (713) 592-2658 - rickagube@gmail.com

**Professional Summary**

Ambitious Cloud Engineer with 8+ years of firsthand IT experience provisioning solutions in cloud-native, on-premises, and hybrid cloud environments architected frameworks. Diligent and meticulous professional commended for best practices, quickly learning new procedures and technologies, and sharing knowledge with junior associates.

**Skills**

|  |  |
| --- | --- |
| * Firewalls & Log Analysis, SIEM, etc.Orchestration Services ECS, Docker Containers, Elastic Beanstalk – Amazon Web Services (EC2, EBS, S3, IAM, AMI, VPC, VPC Peering, NACL, Security Groups, Route53, Auto Scaling, ELB, SNS, CloudWatch and Cloud Formation). Palo Alto Prisma Cloud, Dome9, Experience with Infrastructure Orchestration and Configuration
* Programming and markup language skills – C#, Python, Java, Javascript, SQL, JSON, and YAML.
 | * Database Querying Languages; PostgreSQL, MySQL, SQL server, NOSQL/DynamoDB. Jenkins, Puppet, Chef, Terraform, Ansible. AWS Inspector, AWS Shield, Macie, Guard Duty, AWS Secret Manager, Cloud Passage, Qualys, Nessus, OpenVAS, Symantec DLP. (IDS/IPS) SIEM (AlienVault). Migration, AWS DMS, AWS Direct Connect, AWS Snowball, CloudEndure, and Data Sync.
* Excellent knowledge of Information Systems Audit with Governance, Risk and Compliance (GRC).
 |

**Certifications**

**AWS Certified Cloud Practitioner - (Certified)**

**AWS Certified Solutions Architect Associate - (Certified)**

**AWS Certified DevOps Engineer Professional - (Certified**

**Certified Information Security Manager - (Certified)**

**Certified Web Application Security Professional - (Certified)**

**Certified SAFe Scrum Master - (Certified)**

**Project Management Professional - (Certified)**

**AWS Certified Developer Associate (In-Progress)**

**AWS Certified Security Specialty (In-Progress)**

**Work History**

|  |  |
| --- | --- |
| 06/2018 to 05/2021 | Sr. Cloud Architect/DevOps Engineer Walgreens – Houston, Texas* Developed and documented technical designs, ETL architecture and frameworks for secure integration and implementation of new cloud infrastructure and applications, to improve performance, manage costs and drive efficiencies.
* Experience in deploying and monitoring applications on various platforms using Elastic Beanstalk, setting up the life cycle policies to back the data from AWS S3 to AWS Glacier.
* Worked on infrastructure with Docker containerization.Strong Knowledge creating ANT/ MAVEN with Puppet build script for Deployment.
* Expertise in Docker containerized environment, hosting web servers on containers, building docker images using Docker file.Provisioned AWS Landing Zones to create a customized baseline of AWS accounts, networks, and security policies.
* Configured multi-account architecture, identity and access management, governance, data security, network design, and logging within provisioned AWS Landing Zones.
* Performed regular Vulnerability Threat Assessments with Dome9, and Nessus; Compliance tests and monitoring with Barracuda Cloud Guardian, AWS Config and AWS Detective, Network Security using Palo Alto VM-Series, and Aviatrix SNP, integrated with SIEM resources like AWS GuardDuty, Splunk and QRadar.
* Utilized CloudWatch, CloudTrail, SQS, Redis and ElasticSearch for message queueing and log aggregation, used Splunk for real-time log analysis, distributed alerts with SNS topics, and stored the reports in AWS S3 buckets.
* Oversaw cloud infrastructure design and developed detailed architecture models for the customers to host Test, Development, and Production environments.
* Planned for system and application migrations to the cloud, adhering to the customers' technical and business requirements.
* Deployed Docker Engines in Virtualized Platforms for containerization of multiple apps.
* Strong understanding of information processing principles and practices.
* In-depth technical knowledge of networks, storage systems and computing platforms including Amazon AWS, .NET, Windows, and CI/CD pipelines.
* As a last line of defense against a compromised account, I ensured all IAM users have multi-factor authentication activated for their individual accounts and limited the number of IAM users with administrative privileges.
* Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key.
* Optimized cost of cloud solutions with Auto Scaling and reduced MTTR by automating the use of secure, scalable, cost-effective, highly available, and fault tolerant resources, thus mitigating risk tolerance.
* Spun up VPCs from scratch or used templates to provision solutions with Identity and Access Management (IAM), Service Control Policies (SCP) to create user profiles, groups, policies, federated identities, and roles, to ensure least privilege and mitigate risks.
* Built CI/CD Pipelines for DevOps customers with the use of Vagrant for server management or Fargate for serverless environments, Git repos, automation with Jenkins (hosted on AWS EC2), and ran Docker containers in ECS while reducing the TTD.
 |

|  |  |
| --- | --- |
| 04/2016 to 06/2018 | AWS Cloud Solutions Architect  Bank of America – Atlanta, Georgia* Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key.
* Turned on Redshift audit logging in order to support auditing and post-incident forensic investigations for a given database.
* Encrypted data stored in EBS as an added layer of security.
* Encrypted Amazon RDS as an added layer of security.
* Enabled required ssl parameter in all Redshift clusters to minimize the risk of man-in-the-middle attack.
* Restricted access to RDS instances to decrease the risk of malicious activities such as brute force attacks, SQL injections, or DoS attacks.Encrypted highly sensitive data such as protected health information (PHI) or personally identifiable information (PII) using customer-controlled keys.
* Granted the fewest privileges possible for application users.
* Involved IT security teams throughout the application development lifecycle.
* Inventoried and categorized all existing custom applications deployed in AWS.
* Assisted with designed and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups and NACL
* Recommended and managed transmission protection requirements for all environments (systems, applications, containers, etc.) such as VPC peering best practices, SSL certificate management, key pairs, etc.
* Created functional design specifications, Azure reference architectures, and assist with other project deliverables as needed.Provided recommendations with respect to cloud migrations and prepare technical implementation roadmaps for Azure adoption.
* Designed state-of-the-art technical solutions on Azure that address customers requirements for scalability, reliability, security, and performance and leverage existing investments in Azure/MS platforms.
* Configuration and deployment experience in two of the following: Azure PaaS technologies, Azure apps technologies such as AzureSQL, Azure Tables, Cache, SQL Server DW, Azure AD etc., Azure IaaS Technologies such as VMs, Virtual networks, Express Routes, Standard/Premium storage etc.
* Firm grasp on cloud security, leveraging Windows operating systems, Active Directory, AD integration.
* Well versed in designing and building Azure solutions that include high availability, multi-region and multi-set architectures using virtual networks, availability sets and affinity groups.
* Familiar with infrastructure as code, specifically Terraform and Azure Resource Manager.
 |

|  |  |
| --- | --- |
| 02/2013 to 04/2016 | **Consultant; Cloud Security Engineer**  **Allstate** – Remote  * Designed and implemented system security and data assurance.Hands-on experience writing Production-ready automation code to implement solutions with Puppet, Ansible, CloudFormation or similar - e.g.: Chef, Terraform.
* Experience in building applications of various architecture styles like Micro-services architecture consisting of Restful web services and Docker container-based deployments.
* Configured Docker container for branching purposes.
* Strong interpersonal, organizational, and communication skills with the ability to work effectively across internal and external organizations and virtual teams.
* Proven experience in systems and cloud network design and development.
* Deployed Docker Engines in Virtualized Platforms for containerization of multiple apps.
* Reviewed/Monitored entire environment and execute initiatives to reduce failures, defects, and improve overall performance.
* Provided incident management support on escalated trouble tickets when necessary.
* Deployed hundreds of Amazon Workspaces and App Stream 2.0 for end users.
* Conducted education/training sessions for Azure cloud services and offering guidance in infrastructure movement techniques including bulk application transfers into the Azure cloud platform.
* Hands-on experience writing Production-ready automation code to implement solutions with Puppet, Ansible, Cloud-Formation, Terraform.
* Designed production, staging, QA and development Cloud Infrastructures.
* Experience with building, delivering, and managing hybrid Cloud IaaS environments in Azure cloud platform.
* Creating solutions using PaaS with cloud platforms such as Azure.
* Experienced in Azure and AWS cloud migration.
* Managed AWS-provided portal account access credentials and privileges.
* Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key.
* Consistently built VPCs from scratch, creating private and public sub-nets, creating security groups and network access lists, configuring internet gateways,
* Assisted with designed and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups and NACL.
* Strong understanding of information processing principles and practices.
* In-depth technical knowledge of networks, storage systems and computing platforms including Amazon AWS, .NET, Windows, and CI/CD pipelines.
* As a last line of defense against a compromised account, I ensured all IAM users have multi-factor authentication activated for their individual accounts and limited the number of IAM users with administrative privileges.
* Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key.
* Turned on Redshift audit logging in order to support auditing and post-incident forensic investigations for a given database.
* Encrypted data stored in EBS as an added layer of security.
* Encrypted Amazon RDS as an added layer of security.
* Recommended and managed transmission protection requirements for all environments (systems, applications, containers, etc.) such as VPC peering best practices, SSL certificate management, key pairs..
* Created and executed a strategy to build mindshare and broad use of AWS within a wide range of customers and partners.
* Work with onboarding internal clients.
* Solution design for client opportunities in one or more AWS Competencies or general cloud managed services.
* Create a lift and shift process model clearly defining the individual steps of the lift and shift process.
* Designed and implemented monitoring and protection capabilities to help identify and protect against DoS attacks, MITM, EC2 instance compromise, secret compromise, etc.
* Created incident response processes, procedures and maintained security documentation.
* Worked with the client to ensure that the respective business, application, data and technology perspectives are in line with the organization's technology and governance strategies, policies and standards.
* Established and maintained disaster recovery procedures for current and new technologies.
* Reviewed and identified vulnerabilities while creating and analyzing metrics on the state of the system.
* Demonstrated experience working with senior management on highly sensitive projects that require the utmost discretion and maintaining strict confidentiality on all data, records, and tasks as required.
* Conducted assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise and local policy; assessed the level of risk; developed and recommended appropriate mitigation countermeasures in operational and non-operational situations.
* Performed assessments of systems and networks within the network environment and enclave, identified where those systems/networks deviate from acceptable configurations, enclave policy, or local policy.
* Measured effectiveness of defense-in-depth architecture against known vulnerabilities.
 |

**Education**

|  |  |
| --- | --- |
|  | **Bachelor of Science: Cloud System Administration** In-View - 2021***Western Governors University – Online*** |

|  |  |
| --- | --- |
|  | Master of Science: Mechanical Engineering 2011Prairie A&M University – Prairie View, TX |

**Professional Memberships**

Information Systems Audit and Control Association (ISACA)