



Summary

Team-oriented Cloud engineer with 5 years of experience in system and network administration, managing server infrastructures and datacenter operations across multiple platforms (Unix, Linux, Windows). Expert-level knowledge of Amazon EC2, S3, Simple DB, RDS, Elastic Load Balancing, SQS, VPC, Site-to-Site VPN, and other services in the AWS cloud infrastructure. Configured AWS IAM and Security Group in Public and Private Subnets in VPC. Architected, Designed, and Developed the Backup and Archiving, Disaster Recovery in AWS Cloud. Strong perseverance and diligence towards attaining challenging goals and possess good communication skills and quick learning ability.

Technical Skills

Skills	Sub Category
Cloud Environment	EC2, Elastic Beanstalk, S3, EFS, S3 Glacier, AWS Backup, RDS, Dynamo DB, ElastiCache, VPC, CloudFront, Route 53, Direct Connect, AWS Organization, CloudWatch, CloudFormation, CloudTrail, Config, System Manager, IAM, Inspector, Certificate Manager, Key Management Service, WAF & Shield, Security Hub, AWS Marketplace, SNS, SQS, Workspaces, AWS Application Migration Service (MGN), VM Import/Export, AWS Launch Wizard for SAP.
Migration Tool	CloudEndure Migration, AWS Application Migration Service (MGN), VM Import/Export.
Disaster Recovery & Backup Tools	CloudEndure Disaster Recovery, Nimesa Tool, Commvault
Cloud Platform	Amazon Web Services (AWS)
Containers	Docker, Kubernetes (Pursuing)
Scripting	YAML, Shell Scripting, Python
Infra as Code	Ansible
DevOps Tools	Jenkins Pipelines, Sonar-Qube, Maven, Nexus, Jira, Git-Hub, Tomcat, Nginx, Nagios, Jfrog.

Certifications & Licenses:

Course Name: AWS Certified Solution Architect – Associate
Validation Link: <https://aws.amazon.com/verification>
Validation No: 40PCRXYZDGJF1QHKP

Udemy Courses:

Course Name: AWS Cloud Migration for IT Professionals
Certificate no: UC-1decd0a2-cab9-4f62-437-59bd3312a499
Certificate url: ude.my/UC-1decd0a2-cab9-4f62-437-59bd3312a499

Course Name: Amazon Connect AWS Contact Center VOIP
Certificate no: UC-5d734290-29a3-4805-b444-682dbfe480ee
Certificate url: ude.my/UC-5d734290-29a3-4805-b444-682dbfe480ee

Course Name: Learn Backup & Restore with CommVault
Certificate no: UC-fc2c71a2-3eed-4a17-8788-4cbba55fbcd5
Certificate url: ude.my/UC-fc2c71a2-3eed-4a17-8788-4cbba55fbcd5

Course Name: Implement AWS Landing Zone using AWS Control Tower
Certificate no: UC-24900076-d7b7-4c27-9ed0-7a35eead1d8a
Certificate url: ude.my/UC-24900076-d7b7-4c27-9ed0-7a35eead1d8a

Tools

Ticketing Tool: JIRA, Incident tracking and project management, service now
Monitoring Tool: Site 24/7, service now

Experience

Minfy Technologies Pvt Ltd
Designation: Sr. Cloud Engineer
Duration: 2021 Feb – Till Date

Responsibilities

- Involved in designing and deploying a multitude application utilizing almost all of the AWS stack (Including EC2, Route53, S3, RDS, Dynamo DB, SNS, SQS, IAM) focusing on high-availability, fault tolerance, and auto-scaling.
- Increasing EBS backed volume storage capacity when the root volume is full using AWS EBS Volume feature.
- Managing the EC2 backups (AMI, Snapshots) using the AWS Backup Service or Lambda function trigger with CloudWatch Event Rules.
- Manage and maintain Commvault backup and recovery systems, including installing, configuring, and upgrading Commvault software and agents, setting up policies, schedules, and retention rules, monitoring backups, and resolving any issues that arise.
- Troubleshoot and resolve backup and recovery issues by analyzing logs, diagnosing problems, and working with other teams to resolve issues.
- Build and configure Virtual Private Cloud (VPC), Private and Public Subnets, Security Groups, Route Table, and blocking suspicious IP's using ACL.
- Good understanding of ELB, security groups, NACL, NAT, firewall and Route 53.
- Configuring and deploying the AWS Transit Gateway for the connectivity between multi-AWS Accounts.
- Manages the AWS environment, including deployment of SAP HA applications using the Amazon Web Services Launch Wizard.
- Configured and managed the AWS Launch Wizard for SAP service, including creating, updating, and deleting deployment configurations. Provisioning and managing AWS resources such as EC2 instances, EBS volumes, and S3 buckets, including the underlying AWS infrastructure.
- Configuring and Managing Site to Site VPN for connecting on premise servers with AWS network.
- Using AWS Application Migration Service (MGN), install the AWS replication agent on the source server and launch the test instances.
- Performing acceptance tests on the servers. After the Test instance is tested successfully, finalize the Test and delete the Test instance. Stop all operational services on the source server and launch a Cutover instance.
- Using VM Import/Export from virtualization environment to AWS environment. Exporting EC2/AMI to OVA, VHD, VMDK templates to S3.
- Recognize CloudEndure Disaster Recovery lifecycle phases and key concepts. Configure CloudEndure Disaster Recovery to replicate workloads to AWS and recover on AWS in the event of a disaster.
- CloudEndure Disaster Troubleshoot issues in order to achieve successful implementation throughout the disaster recovery lifecycle. Adopt best practices for successful setup, operation, and recovery.
- Managing Nimesa, creating a backup policy and schedule the backup jobs. And also creating crossing account / region backup jobs.
- Using Nimesa, flexible restores, data can be recovered from a single file in an EBS volume to complete EC2 instance.
- Scheduling downtimes of the servers for patching, memory upgrades and various admin activities in coordination with Appropriate teams.
- Responsible for troubleshooting Mount points, NFS, SMB, FTP Servers.
- Created S3 backups using versioning enable and moved objects to Amazon Glacier for archiving purpose.
- Created S3 buckets in the AWS environment to store files, which are required to serve static content delivery. Also Providing S3 bucket access to Cross accounts, copying files from one bucket to another in bulk as per the request.
- Creation of roles, users, groups using IAM service in AWS and implemented MFA to provide additional security to AWS account and its resources.

- Created load balancers (ELB) and used Route53 with failover and latency options for high availability and fault tolerance.
- Experience with monitoring tools such as Cloud Watch.
- Working within SLA to take ownership, escalate to resolve.

Capgemini - Third Party Payroll

Designation: Associate Cloud Engineer

Duration: March 2019 – Feb 2021

Responsibilities

- Expertise with AWS Cloud Technologies such as VPC, EC2, ELB, EBS, Auto Scaling, CloudWatch, CloudTrail, S3, IAM, RDS, SNS, Elastic Beanstalk, Route53, Trusted Advisor, ACM.
- Worked on Multiple AWS instances set the security groups, Elastic Load Balancer (ELB) and AMIs, Auto-scaling to design cost effective, fault tolerant and highly available systems.
- Worked with IAM service creating new IAM users & groups, defining roles and policies and Identity providers.
- Build Customized AWS IAM policies to restrict access to various AWS resources based on user requirements (developers, BI teams, DB teams, Redshift teams etc).
- Used AWS command line interface (CLI) and management console to interact with AWS resources.
- Experience involving configuring S3 versioning and lifecycle policies to backup files and archive files in Glacier.
- Deployed a server less portal with web layer hosted as a static website on S3.
- Restored RDS instances using database snapshots.
- Created NAT gateways and instances to allow communication from the private instances to the internet through bastion hosts.
- Experience in AWS Networking – VPC, NACL's, Security groups, etc.,
- Enabling automated backups and Multi-AZ to improve database performance on RDS.
- Setting up databases in AWS using RDS, storage using S3 buckets and configuring instance backups to S3 bucket.
- Worked on Multiple AWS instances set the security groups, Elastic Load Balancer (ELB) and AMIs, Auto-scaling to design cost effective, fault tolerant and highly available systems.
- Created AWS Multi-Factor Authentication (MFA) for instance RDP/SSH logon, worked with teams to lock down security groups.
- Responsible for deploying SSL Certs across AWS ELB.
- Experience on creating and Resizing Linux Partitions with LVM.
- Monitoring AWS services EC2, S3, and RDS etc., using Cloud watch.
- In case of an event, going through Cloud Trail logs and utilizing what went wrong.
- Deploying, managing, and operating scalable, highly available, and fault tolerant systems on AWS.
- Creating new alarms using SNS topic.
- Submitting a Trusted Adviser reports to customers and suggestions to reduce most.
- Maintenance and scheduling backup jobs using Crontab.
- Store the different Databases Credentials/ Encrypted keys in Secret Manager.
- Coordinating with Windows team, Application team, DBA team and Backup team to resolve server issue and giving suggestion.

Education Profile:

- **B. Tech** from **Jawaharlal Nehru Technological University**, Kakinada in **2014**.

Declaration:

I hereby declare that the above information furnished by me is true and correct to the best of my knowledge

Place: Hyderabad

Sandani Shaik