AWS Q&A for Various Activities

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Category | Question Description | AWS Answer |
| 1 | AWS account structure setup | How should the AWS account structure be organized for a multi-account setup? | Use AWS Organizations to manage multiple accounts. Implement service control policies (SCPs) for governance. |
| 2 | AWS account structure setup | What best practices should be followed when creating IAM roles and users for different accounts? | Use least privilege principle, create separate IAM roles for different permissions, and enable MFA for root account. |
| 3 | Network architecture deployment | How can we ensure high availability in AWS network architecture? | Deploy resources across multiple Availability Zones (AZs) and use services like Amazon Route 53 for failover routing. |
| 4 | Network architecture deployment | What is the best way to connect an on-premises network to AWS securely? | Use AWS Direct Connect or a VPN connection to securely link your on-premises network to AWS. |
| 5 | Core security controls implementation | How can we enforce encryption in transit and at rest in AWS? | Use AWS Key Management Service (KMS) for data encryption at rest, and ensure encryption in transit using SSL/TLS. |
| 6 | Core security controls implementation | How can we control network access to resources within VPCs? | Use security groups, network access control lists (NACLs), and VPC flow logs to control access. |
| 7 | CI/CD pipeline configuration | How can we automate application deployment using CI/CD in AWS? | Use AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy for automating build, test, and deployment processes. |
| 8 | CI/CD pipeline configuration | How can we ensure that our CI/CD pipeline is secure and can be audited? | Implement AWS Identity and Access Management (IAM) for fine-grained permissions, and enable CloudTrail for auditing. |
| 9 | Monitoring and logging setup | How can we monitor AWS resources for performance and health? | Use Amazon CloudWatch for monitoring metrics, logs, and alarms. Utilize AWS CloudTrail for auditing API activity. |
| 10 | Monitoring and logging setup | How can we log and store API requests for security and compliance? | Use Amazon API Gateway with CloudWatch logging enabled to capture API request and response data. |
| 11 | Development environment provisioning | How can we provision a scalable development environment in AWS? | Use Amazon EC2 instances, AWS Cloud9 for cloud-based IDE, and leverage AWS Elastic Beanstalk for application deployment. |
| 12 | Development environment provisioning | How can we ensure that development environments are consistent across different developers? | Use Amazon EC2 with Docker containers or Amazon ECS for containerized environments. Leverage Infrastructure as Code (IaC) tools like AWS CloudFormation or Terraform. |