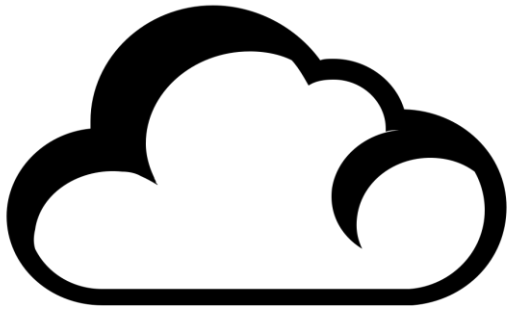
AMAZON WEB SERVICES:
ARCHITECT ASSOCIATE CERTIFICATION



BIG PICTURE QUESTIONS

HOW DO YOU PROTECT THE INTEGRITY OF YOUR INSTANCES?

BY MANAGING FAILURE

Use Load Balancers

Monitor Resource Health

Multiple Availability Zones

Automatically respond to Notifications

HOW ARE YOU PROTECTING YOUR DATA AT REST?

AVAILABLE ENCRYPTION CHOICES

S3 has built-in encryption

RDS encryption

EBS encrypted volumes

Client side encryption

HOW ARE YOU MANAGING USERS

BY ENFORCING PROTECTION

Role-based access using security groups

Clearly defined users, groups, and roles

Design using VPCs

Always use minimum privileges

WHERE WILL YOU PLACE YOUR WORKLOAD IN AWS?

MAKING WORKLOAD CONSIDERATIONS

Select region matching your compliance needs

Choose availability zones for application failover

HOW DO APPLICATIONS RESPOND TO COMPONENT FAILURES?

Monitoring Performance

- CloudWatch logs – collect alerts and alarms from service metrics
- Use Elasticsearch to query CloudWatch logs
- Use Simple Notification Service (SNS) linked to CloudWatch logs
- Trusted Advisor for utilization and security issues
- Alerts you when perceived issues are found

HOW DO I DEFINE MY COMPLIANCE NEEDS?

Finding Out What I Have

- Everything can be enumerated through API calls
- CLI tools – aws ec2 describe-instances
- AWS Config – Config rules to evaluate changes and react
  - Receiving alerts when changes occur
  - Rolling back changes when they occur
- Inspector – set rules for EC2 fleet using tags; alert or revert changes

Security Compliance Tools

- Trusted advisor - Alerts possible issues as they occur
- CloudWatch logs – Alerts based on metrics
- VPC flow logs – Network traffic
- S3 logs – Data plane control
- ELB logs – Traffic and health control
- CloudTrail – Control plane tracking of infrastructure change via API calls

COMPLIANCE WORK

What do I have?

How am I monitoring performance?

Who controls monitoring?

How is it secure?

Is it compliant?

How do changes / updates occur?

HOW DO I CONTROL ACCESS?

Controlling Access to Resources

- Identity and Access (IAM)
  - Authentication and authorization
- Use tags for authorization
- Integrate your enterprise identity system using SAML or AD for authentication
- Then use IAM for authorization

HOW DO I ACCESS AWS AUDITS?

Security Compliance Baseline

- Third party audits provide a 360 degree viewpoint
  - PCI audit twice a year
  - FedRAMP and ISO 27001 audits
  - Overlap between the disciplines is good for customers
- Customers have access to these audit reports and audit materials after signing an Non Disclosure Agreement with AWS

WHAT LOGS ARE AVAILABLE?

CAPTURING LOGS

CloudTrail

CloudWatch logs

ELB logs

VPC flow logs

S3 bucket logs

Operating system logs

PLANNING ACCESS CONTROL

CREATING IAM USERS

Unique Credentials

Unique Privileges

Grant Least Privileges

Credential Rotation

PERMISSIONS

- Always manage permissions through groups
- Easier to:
  - Assign the same permission to multiple users
  - Reassign permissions as responsibilities change
- One change updates multiple users

Manage Restrictions

- Restrict access further with conditions:
- Access FROM a specific IP address
- Database creation using a specific engine
- Create only specific EC2 instances

Setup Auditing

- Provides visibility into your users activity
- View CloudTrail to analyze logs of API calls
- Enable and Log calls to S3 bucket

Enforce Strong Passwords

- Configure a strong password policy
  - Password expiration?
  - Password strength?
  - Reuse policy?
- Password policy does not apply to Root user

Credential Rotation

- Use Credential Reports to identify credentials that should be rotated, or deleted
- IAM console displays when password was last used
- Rotate security credentials on a fixed schedule
- IAM roles for EC2 instances rotate credentials automatically

Enable Multi-Factor Authentication

- For all IAM users
- For the Root User
- Require a one-time code during authentication
  - Virtual MFA
  - Hardware device
  - SMS code for IAM users

Sharing Access

- Use IAM roles to share access
- Analyze and implement based on use case:
  - Cross account access
  - Account delegation
  - Federation

IAM Roles

- Assign IAM Roles to Amazon EC2 instances
- Access keys stored on EC2 instances
- Automatic key rotation by AWS
- Assigns least privilege to the application

Root Account

- Reduce or restrict the root account
- Remove the potential for misuse of credentials

Managing Setup and Change

- Designing shared services:
  - Account creation and IAM provisioning
  - Federation endpoints
  - Core networking security
  - Golden images and associated IAM roles
  - Auditing services
  - Incident response

PLANNING NETWORKS

Planning Your Network Architecture

- How many VPCs?
- What are your present and future needs?
- Public or Public / Private ?
- Private/HW VPN or Private/SW VPN ?
- What external connection type is needed?

Planning CIDR blocks

- How many IP addresses are needed for public subnet?
- How many IP addresses are needed for private subnet?
- Do we need connectivity with a external data center?
- Does your CIDR range overlap with your on-premise data center?

Isolation

- Separate VPCs for production, staging, and development?
- Create one Amazon VPC with separate subnets?
- Create subnets for production, staging, and development?
- Deploy VPCs using CloudFormation?

VPC Security

- Use a virtual appliance firewall you know
- Add intrusion prevention virtual appliance to your VPC
- Encrypt Root and any additional EBS volumes
- Use Flow Logs to monitor the VPC environment
- Install antivirus software on EC2 instances hosted in VPC’s
- Deploy security groups and NACLs

Check VPC Soft Limits

- Understand hard and soft limits for your VPCs
- Limitations are in effect for security groups route tables and subnets, etc.
- Ensure your long term design will not be affected by the limitations
- Request increases in soft limits if limitations will affect your long-term design at the start

IAM and VPCs

- Ensure IAM policies are attached only to groups or roles
- Design with the least access principal

Security Design

- Security groups at the EC2 instance level
- Use security groups for white listing
- Use NACLs for blacklisting
- Create different security groups for different tiers of your infrastructure (Web, App, DB)
- Avoid errors: Standardize security group naming conventions
- Enable VPC flow logging in all VPCs

Public Subnets

- Only ELB or security solutions in public subnets
- Design a DMZ in a Public Subnet
  - Force all incoming traffic into DMZ
  - Trunk all outgoing traffic from DMZ to Public subnet where Load Balancer resides

Secure Internet Gateway Usage

- Don’t add IGW to main routing table
- Minimize use of IGW through custom route tables
- Minimize subnet size utilizing NAT or Internet facing proxy services

VPC Peering

- Peering allows easy interconnection
- Enterprise running multiple VPCs in single region with interconnected applications
- Enterprises with different AWS accounts for different departments
- Peering with cloud brokers allowing monitoring and management of AWS resources
- Review that routing tables for VPC peering are designed for “least access”

SECURING ACCESS

Monitor Load Balancing with CloudWatch

- Monitor the following ELB metrics:
  - Latency
  - Request count
  - Healthy hosts
  - Unhealthy hosts
  - Backend response (4xx- 5xx)
  - Elastic load-balancing response (2xx- 4xx)

Perform SSL Termination at the ELB

- Enable SSL termination at the ELB
- Saves time, CPU processing time for your instances

Cross Zone Load Balancing

- Instances placed into multiple availability zones?
  - Enable cross zone load-balancing
  - Providing application availability and resiliency

Health Checks

- Health checks for Instances
- Health checks for ELB
- Health checks for Route 53
- ELB outage – requests are routed away from the unhealthy ELB
- Instance failure – solved by auto scaling groups and ELB integration
- Route 53 health checks results are published to all DNS Servers

Protect your Web Applications

- Place application behind a load balancer (ELB)
  - ELB only accepts well-formed TCP connections
  - SYN floods or UDP reflection attacks are not accepted
  - ELB detection of attacks prompts scaling to absorb the additional traffic
- AWS WAF to create additional mitigation strategy rules
  - Block known IP addresses with rules / actions
  - Create rules with conditions that block

PLANNING S3 STORAGE

S3 Versioning

- New version created from each object upload
- Retrieve “deleted objects”
- Protect from accidental deletion
- Create lifecycle rule for versioned objects

- Not enabled by default
- Versioning can only be suspended after enabled

MFA Bucket Protection

- A valid MFA code required for permanently deleting an object version (MFA Delete)

Lifecycle Policies

- Control data costs
  - Transition – Standard to Amazon Glacier; after defined time
  - Expiration: Delete objects after defined time

Versioning and Lifecycle Policies

- Versioning = Recycle bin
- Lifecycle policies = Data automation

Cross–region Replication

- Replicate all deleted objects to destination bucket in separate region
  - Both source and destination buckets need to enable versioning
  - Uploads into source bucket will then be replicated
- For Compliance: Records are stored in different region
- Separate Security: Remote replicas managed by separate AWS accounts
- Faster access: Lower latency

IAM Roles

- Use IAM roles for S3 control
  - Central permission management
  - IAM policies for users, groups, and roles

Bucket Policies

- Directly attached to the S3 bucket
  - Access control in the S3 environment
  - S3 ACLs can control individual objects within each bucket

SECURING CONTENT

End-to-End HTTPS

- CloudFront supports HTTPS traffic:
  - From browser to Edge locations
  - From Edge locations to origin
- Redirect all HTTP traffic to HTTPS traffic
  - Define in CloudFront distribution
- SSL certificate provided by CloudFront or custom SLL certificate

Use Amazon S3 for Static Objects

- Free data transfer from S3 to CloudFront
- Decrease the load on your web servers
- S3 is highly available and scalable

Control Access to S3 Content

- Enable Origin Access Identity (OAI)
- “Special” user that only has access to your specific S3 content
- Stops direct S3 access
- Content can be only accessed via CloudFront when OAI is enabled

Route 53 ALIAS Records

- Route 53 queries CloudFront distributions
- All DNS queries using ALIAS records are free!
- Create ALIAS record for your zone apex
- CloudFront will directly translate your ALIAS record into the CloudFront IP address with no additional charge

Custom Error Pages

- Set a low error caching minimum TTL
- After the TTL has expired CloudFront will check and see if the requested resource is now available
- Create custom error pages to improve customer experience
- Deliver error pages from S3 and not your origin server

CloudFront Access Logs

- Create CloudFront logs
- Must be manually turned on
- Provide analytics into your content and usage

CloudFront Reports

- Cache statistics
- Popular objects
- Top referrers
- Viewer reports
  - Locations
  - Browsers
  - Operating systems

AUDITING AND MONITORING

What are your Compliance Rules?

- State, province, country rules
- Does your industry operate abiding by specific compliance rules ?
- What additional internal compliance rules do you follow ?

CLOUDTRAIL WITH CLOUDWATCH

- All activity based on APIs, and resources can be monitored
- Alarms and notifications alert abnormal account activity
- CloudTrail logs can be stored forever in S3 bucket

RESTRICT ACCESS TO CLOUDTRAIL LOGS

- Restrict access to CloudTrail logs with IAM or bucker policies
- Decrease the risk of unauthorized log access
- S3 Lifecycle policy on bucket holding your CloudTrail logs
- Archive log contents in Glacier matching data retention policies

ENABLE LOG FILE VALIDATION

- After delivery to S3 bucket, changes made to logs can be identified
- Integrity of log files remains intact

ENCRYPT CLOUDTRAIL LOGS

- Define decryption permissions for accessing CloudTrail logs
- Ensure access control matches your compliance requirements

ENABLE CLOUDTRAIL IN ALL REGIONS

- Enable CloudTrail in all regions, even in regions where you don’t currently operate
- Be alerted when unexpected activity occurs in unused regions
- Activity could indicate security issues

LOG GLOBAL API CALLS

- Some essential services are global, not bound by region: IAM, CloudFront, Route 53, or WAF
- Enable global events in one trail
- Disable global events from all other trails