

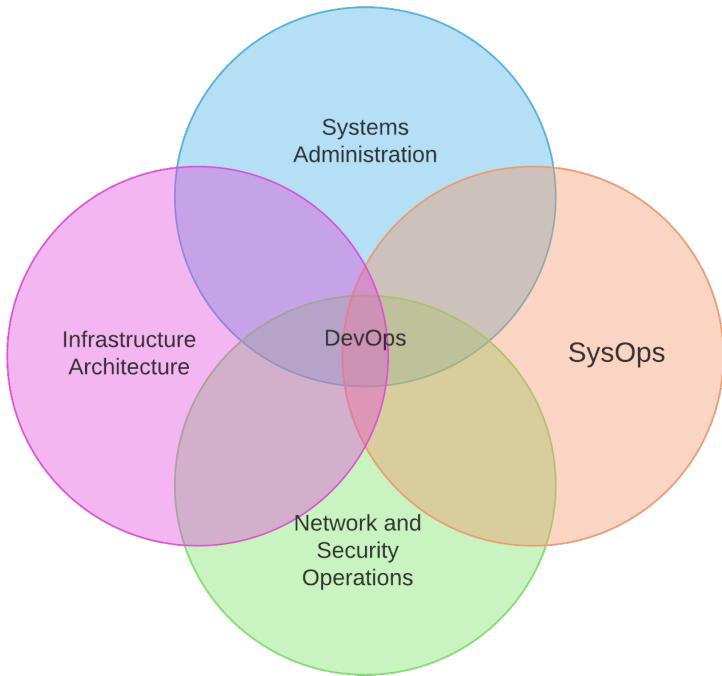


AWS Certified SysOps Administrator (Associate)
Crash Course

Introduction

What is SYSOPS?

SYStems OPerationS



Course Prerequisites

- Solid AWS service fundamentals
- Previous AWS operations experience
 - CLI
 - Console
- Command-line proficiency

Course Scope

In Scope

- Operations
- Limits
- Trade-offs
- Service scope
- Deployment choices
- Sample questions

Out of Scope

- Service definition
- Fundamentals
- Global PoP
- Architecture

Exam Dashboard

Where is the exam dashboard?

<https://aws.amazon.com/certification/certified-sysops-admin-associate/>

Exam Dashboard

Job Description Analogy

It validates an examinee's ability to:

- Deploy, manage, and operate scalable, highly available, and fault-tolerant systems on AWS
- Implement and control the flow of data to and from AWS
- Select the appropriate AWS service based on compute, data, or security requirements
- Identify appropriate use of AWS operational best practices
- Estimate AWS usage costs and identify operational cost control mechanisms
- Migrate on-premises workloads to AWS

Exam Dashboard

Job Description Analogy

Recommended AWS knowledge:

- Minimum of 1 year hands-on experience with AWS
- Experience managing/operating systems on AWS
- Understanding of the AWS tenets – architecting for the cloud
- Hands-on experience with the AWS CLI and SDKs/API tools
- Understanding of network technologies as they relate to AWS
- Understanding of security concepts with hands-on experience in implementing security controls and compliance requirements

Exam Dashboard

Job Description Analogy

Recommended general IT knowledge:

- 1-2 years of experience as a systems administrator in a systems operations role
- Understanding of virtualization technology
- Monitoring and auditing systems experience
- Knowledge of networking concepts (e.g., DNS, TCP/IP, and firewalls)
- Ability to translate architectural requirements

Exam Blueprint

Where is the current exam guide?

https://d1.awsstatic.com/training-and-certification/docs-sysops-associate/AWS_Certified_SysOps_Associate-Exam_Guide_EN_1.4.pdf

Yes, this guide does get updated periodically, hence the version.
Always check for new versions!

Exam Blueprint

Question Domains

Domain	% of Examination
Domain 1: Monitoring and Reporting	22%
Domain 2: High Availability	8%
Domain 3: Deployment and Provisioning	14%
Domain 4: Storage and Data Management	12%
Domain 5: Security and Compliance	18%
Domain 6: Networking	14%
Domain 7: Automation and Optimization	12%
TOTAL	100%

Exam Blueprint

Explanation of question domains

Domain 1: Monitoring and Reporting

- 1.1 Create and maintain metrics and alarms utilizing AWS monitoring services
- 1.2 Recognize and differentiate performance and availability metrics
- 1.3 Perform the steps necessary to remediate based on performance and availability metrics

Domain 2: High Availability

- 2.1 Implement scalability and elasticity based on use case
- 2.2 Recognize and differentiate highly available and resilient environments on AWS

Domain 3: Deployment and Provisioning

- 3.1 Identify and execute steps required to provision cloud resources
- 3.2 Identify and remediate deployment issues

Domain 4: Storage and Data Management

- 4.1 Create and manage data retention
- 4.2 Identify and implement data protection, encryption, and capacity planning needs

Domain 5: Security and Compliance

- 5.1 Implement and manage security policies on AWS
- 5.2 Implement access controls when using AWS
- 5.3 Differentiate between the roles and responsibility within the shared responsibility model

Domain 6: Networking

- 6.1 Apply AWS networking features
- 6.2 Implement connectivity services of AWS
- 6.3 Gather and interpret relevant information for network troubleshooting

Domain 7: Automation and Optimization

- 7.1 Use AWS services and features to manage and assess resource utilization
- 7.2 Employ cost-optimization strategies for efficient resource utilization
- 7.3 Automate manual or repeatable process to minimize management overhead



Too Long; Didn't Read

- Sysops requires understanding of architecture
- Fewer services to learn than Solutions Architect Associate (SAA) certification
- Architecture answers “what” and “why”, Sysops answers “how” and “when”
- Focus on monitoring and automation of tasks

Concepts

Deploy, manage, and operate scalable, highly available, and fault tolerant systems on AWS

Operations

- Deploy
- Manage
- Operate

Architecture

- Scalable
- Highly available
- Fault tolerant

Concepts

Implement and control the flow of data to and from AWS

- Network ingress and egress
- Import and export
- Content delivery
- Synchronous vs asynchronous
- Managed services

Concepts

Select the appropriate AWS service based on compute, data, or security requirements

- Learn the Well-Architected Framework
 - Security
 - Reliability
 - Performance Efficiency
 - Cost Optimization
 - ***Operational Excellence***

Concepts

Identify appropriate use of AWS operational best practices

- Recognizing available options for operational tasks
- Understanding tradeoffs for each option

Concepts

Estimate AWS usage costs and identify operational cost control mechanisms

- Learn service costs
- Stay current
- Cost Optimization Pillar

Concepts

Migrate on-premises workloads to AWS

- **Architecture** skills to plan
- **Operations** skills to execute, maintain and respond



AWS Certified SysOps Administrator (Associate)
Crash Course

AWS Knowledge

TL; DR

- Experience similar to a candidate requirements for a job description
- Command line interface is rich with subtle options
 - Know what they are and when to use them
- Focus on solutions using automation
- CLI and SDK have similar functionality
 - Benefits and drawbacks of each

Candidate Overview

Minimum of one year hands-on experience with AWS

- Hands-on experience is priceless
- Time spent is less important than immersion

Candidate Overview

Experience managing/operating systems on AWS

- Create a personal account
- Use the Free Tier
- Experiment with CLI and SDK
- Experiment with boto (CLI written in Python)

Candidate Overview

Understanding of network technologies as they relate to AWS

- Build a VPC from scratch
- Create infrastructure that uses ELB
- Create infrastructure that uses CloudFront

Candidate Overview

Understanding of security concepts with hands-on experience in implementing security controls and compliance requirements

- Security as part of architecture, not afterthought
- Know how to monitor compliance

Candidate Overview

*Understanding of the AWS tenets –
architecting for the cloud*

7 Tenets (Legacy)

1. Design for failure and nothing will fail
2. Implement elasticity
3. Leverage different storage options
4. Build security in every layer
5. Think parallel
6. Loose coupling sets you free
7. Don't fear constraints

10 Design Principles (Current)

1. Scalability
2. Disposable Resources
3. Automation
4. Loose Coupling
5. Services, not Servers
6. Databases
7. Removing Single Points of Failure
8. Optimizing for Cost
9. Caching
10. Security

Candidate Overview

Service Scope

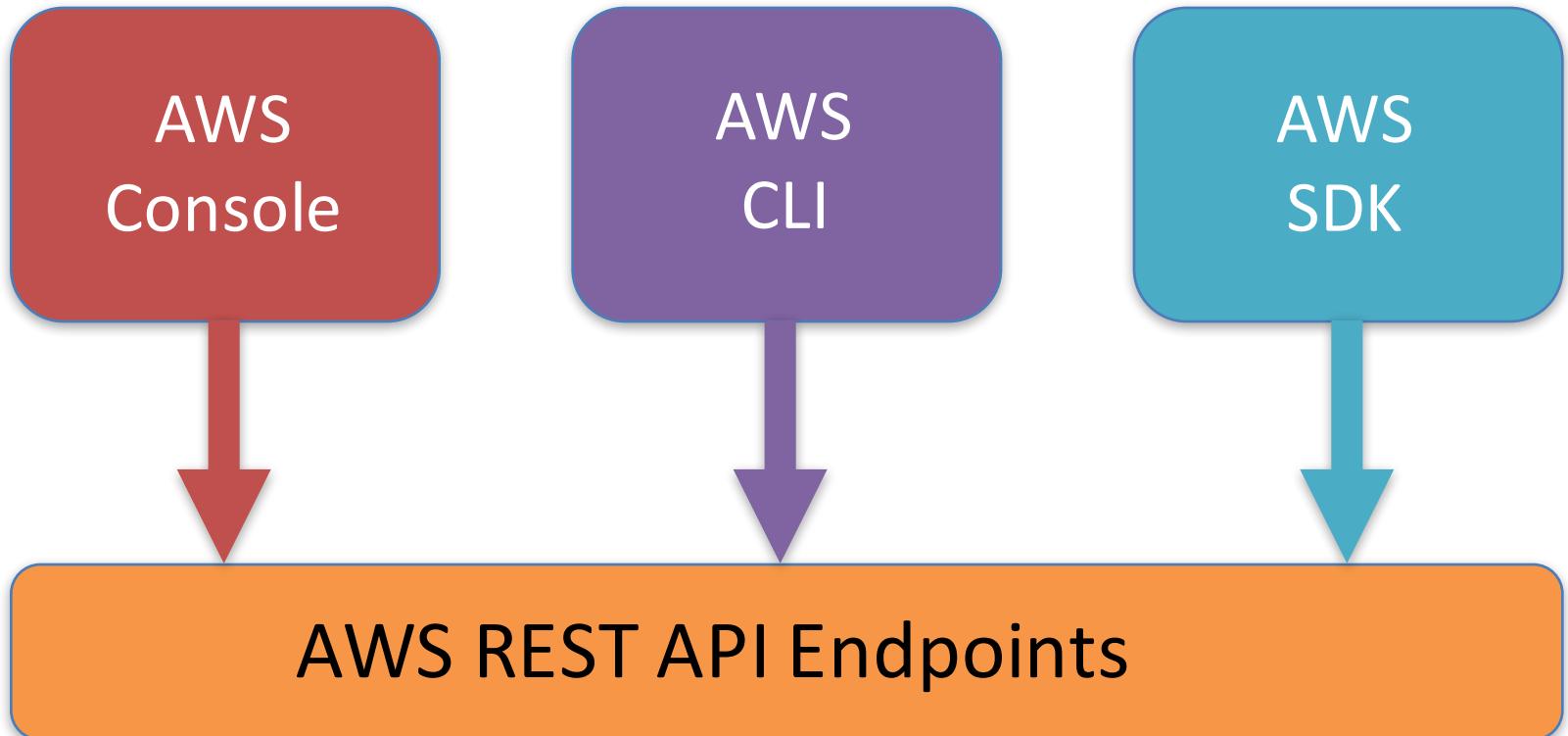
- AZ
 - IAAS
- Region
 - PAAS/SAAS
- Global
 - No management of infrastructure
 - DNS/CDN

Candidate Overview

Service Manageability

- Unmanaged
 - Less HA/FT
 - Building blocks
- Managed
 - Range from PAAS to SAAS
 - Less overhead

AWS CLI & SDK



AWS CLI

- Install
- Configure
- Command Format
- Advanced Commands – Query
- Advanced Commands – Filter

AWS CLI Linux & MacOS Install

Python module install

```
pip install awscli --upgrade --user
```

Standalone installer

```
curl "https://s3.amazonaws.com/aws-cli/awscli-bundle.zip" -o awscli-bundle.zip
```

```
unzip awscli-bundle.zip
```

```
./awscli-bundle/install -b ~/bin/aws
```

AWS CLI Windows Install

Python module install (same as Linux and MacOS)

```
pip install awscli --upgrade --user
```

Standalone MSI installer

64-bit: <https://s3.amazonaws.com/aws-cli/AWSCLI64.msi>

32-bit: <https://s3.amazonaws.com/aws-cli/AWSCLI32.msi>

AWS CLI Configuration

`aws configure [--profile profile-name]`

AWS Access Key ID [None]:

AWS Secret Access Key [None]:

Default region name [None]:

Default output format [None]:

`aws configure get <config option>`

`aws configure set <config option>`

`aws configure list`

AWS CLI Configuration Advanced

IAM Role in .aws/config using a named profile

Same AWS account

[profile *securityadmin*]

role_arn = arn:aws:iam::123456789012:role/*securityadmin*

source_profile = default

AWS CLI Configuration Advanced

IAM Role in .aws/config using a named profile

Cross-account access

With MFA

[profile otheraccount]

role_arn = arn:aws:iam::234567890123:role/otheraccount

source_profile = default

mfa_serial = arn:aws:iam::123456789012:mfa/chadsmith

external_id = 456789

AWS CLI Command Help

`aws <service> <action> help`

- Context-sensitive
- Paginated
- Examples

AWS CLI Command Format

--profile

great for assuming roles

--region

specify the region of the resource acted upon

--output

json for schema and structured output

text to remove formatting

table for human readable format

--endpoint-url

can help avoid latency issues

AWS CLI Command Format

--generate-cli-skeleton

- works with --cli-input-json

- used for many actions

- output includes all possible options

- provides more structure than cli options

- great for operations and automation

AWS CLI Queries

--query

- restrict output to specific properties

- requires JSON schema for specific API method

- JMESPath query expressions supported

- use for chaining commands together

- use for setting variables in scripts

AWS CLI Filters

--filter

- restrict output to specific objects

- reduces the response set, which can save time

- different for every API operation

- contextual help for documentation

AWS CLI Example

```
aws ec2 describe-instances --output text \  
  --query 'Reservations[*].Instances[?not_null(Tags[?Key ==  
    `Name`.Value]).[join(``,Tags[?Key==`Name`.Value],InstanceId,PublicDnsNam  
e,PrivateDnsName]' \  
  --filter Name=group-name,Values=secgroupprefix* \  
          Name=instance-state-  
          name,Values=running
```

Options

JSON schema

JMESQuery

unique filter

AWS CLI Example

```
aws ec2 describe-instances --output text \  
--query 'Reservations[*].Instances[?not_null(Tags[?Key ==  
'Name'].Value)].[join(` `,Tags[?Key==`Name`.Value]),InstanceId,PublicDnsNam  
e,PrivateDnsName]' \  
--filter Name=group-name,Values=secgroupprefix* \  
Name=instance-state-  
name,Values=running
```

Options

JSON schema

JMESQuery

unique filter

AWS CLI Example

```
aws ec2 describe-instances --output text \  
--query 'Reservations[*].Instances[?not_null(Tags[?Key ==  
'Name'].Value)].[join(` `,Tags[?Key==`Name`.Value]),InstanceId,PublicDnsNa  
me,PrivateDnsName]' \  
--filter Name=group-name,Values=secgroupprefix* \  
Name=instance-state-  
name,Values=running
```

Options

JSON schema

JMESQuery

unique filter

AWS CLI Example

```
aws ec2 describe-instances --output text \  
  --query 'Reservations[*].Instances[?not_null(Tags[?Key ==  
    `Name`].Value)].[join(`,`,Tags[?Key==`Name`].Value),InstanceId,PublicDnsNam  
e,PrivateDnsName]' \  
  --filter Name=group-name,Values=secgroupprefix* \  
    Name=instance-state-  
    name,Values=running
```

Options

JSON schema

JMESQuery

unique filter

AWS CLI Example

```
aws ec2 describe-instances --output text \  
  --query 'Reservations[*].Instances[?not_null(Tags[?Key ==  
    `Name`.Value]).[join(``,Tags[?Key==`Name`.Value],InstanceId,PublicDnsNam  
e,PrivateDnsName]']' \  
  --filter Name=group-name,Values=secgroupprefix* \  
        Name=instance-state-  
        name,Values=running
```

Options

JSON schema

JMESQuery

unique filter

AWS SDK Options

Android

C++

Go

iOS

IoT SDK

Java

Mobile SDK

.Net

Node.js

PHP

Python

Ruby

Always check documentation!

CLI vs SDK for operations

CLI

- Text
- Easy

SDK

- Objects
- Portable

CLI vs SDK Bash

```
#!/bin/bash
region=$1
vols=`aws ec2 describe-volumes --region $region --filters \
Name=status,Values=available \
--query Volumes[].VolumeId | tr -s '\t' '\n'`

for i in $vols; do
    aws ec2 delete-volume --region $region --volume-id $i --dry-run
done
```

CLI vs SDK Python

```
#!/usr/bin/python
import boto3, sys
region = sys.argv[1]
ec2 = boto3.resource("ec2", region_name=region)
available_volumes = ec2.volumes.filter(
    Filters=[{'Name': 'status', 'Values': ['available']}])
for volume in available_volumes:
    volume.delete(DryRun=True)
```

CLI vs SDK Python (Lambda)

```
import boto3

def lambda_handler(event, context):
    regionid = event['region']
    ec2 = boto3.resource("ec2", region_name=regionid)
    available_volumes = ec2.volumes.filter(
        Filters=[{'Name': 'status', 'Values': ['available']}]
    )
    for volume in available_volumes:
        volume.delete(DryRun=True)
```

Question Breakdown

Which command can you run to understand syntax and task-specific options for creating an EBS volume?

- A. aws efs help
- B. aws ec2 ebs create help
- C. aws ec2 create-volume help
- D. aws ebs create-volume help

Breakdown – Key Terms

Which **command** can you run to understand **syntax** and task-specific **options** for **creating an EBS volume**?

- A. aws efs help
- B. aws ec2 ebs create help
- C. aws ec2 create-volume help
- D. aws ebs create-volume help

Breakdown – Answer Selection

Which command can you run to get help options for creating an EBS volume?

EFS is a different service, not related to EBS

- A. **aws efs help**
- B. aws ec2 ebs create help
- C. aws ec2 create-volume help
- D. aws ebs create-volume help

Breakdown – Answer Selection

Which command is correct for creating EBS volumes? (Select three options)

First two terms correct but ebs isn't a task

- A. aws efs help
- B. **aws ec2 ebs create help**
- C. aws ec2 create-volume help
- D. aws ebs create-volume help

Breakdown – Answer Selection

Which command would you run to create an EBS volume? What are the options for creating an EBS volume?

This looks right! EBS actions are under EC2 in the CLI

- A. aws efs help
- B. aws ec2 ebs create help
- C. **aws ec2 create-volume help**
- D. aws ebs create-volume help

Breakdown – Answer Selection

Which command can you run to get help options for creating an EBS volume?

EBS isn't a service

- A. aws efs help
- B. aws ec2 ebs create help
- C. aws ec2 create-volume help
- D. **aws ebs create-volume help**

Breakdown – Answer Selection

Which command can be used to get help options for **create-volume**?

Answer: C

- A. aws efs help
- B. aws ec2 ebs create help
- C. aws ec2 create-volume help
- D. aws ebs create-volume help

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button on a media player.

AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 1 - Monitoring and Reporting

Monitoring and Reporting

- 22% of the exam content
- **Create** and **maintain metrics** and **alarms** utilizing AWS **monitoring services**
- **Recognize** and **differentiate** performance and availability **metrics**
- Perform the steps necessary to **remediate** based on performance and availability **metrics**

TL; DR

- CloudWatch metrics can be viewed in different ways
- Learn the common metrics for covered services
- Know which services have status checks
- Know the integration points between monitoring services and automated remediation

CloudWatch Entry Points

CloudWatch Console

The screenshot shows the AWS CloudWatch Metrics Summary page. The left sidebar lists various CloudWatch services: Dashboards, Alarms, Events, Rules, Logs, Metrics, and Favorites. Under Alarms, there are three items: INSUFFICIENT (2), OK (1), and Billing (0). The main content area starts with the Metric Summary section, which states that Amazon CloudWatch monitors operational and performance metrics for AWS resources and applications. It mentions 53 CloudWatch metrics available in the US East (N. Virginia) region. Below this is the Alarm Summary section, which indicates 2 alarms in the INSUFFICIENT state. A 'Create Alarm' button is available. Two alarms are listed: 'FailedConsoleLoginAlarm' and 'UnusedRegionsAlarm'. Each alarm has a status indicator (orange circle), a name, a description, and a line chart. The 'Service Health' section shows the Amazon CloudWatch Service is operating normally.

Metric Summary

Amazon CloudWatch monitors operational and performance metrics for your AWS cloud resources and applications. You currently have 53 CloudWatch metrics available in the US East (N. Virginia) region.

Browse Metrics X

Alarm Summary

You have 2 alarms in INSUFFICIENT DATA state in US East (N. Virginia) region. Create Alarm

Learn more

FailedConsoleLoginAlarm FailedConsoleLogin >= 3 for 2 dat...

Time	Value
4/10 01:00	3
4/10 02:00	3
4/10 03:00	3

UnusedRegionsAlarm UnusedRegions >= 1 for 1 datapoi...

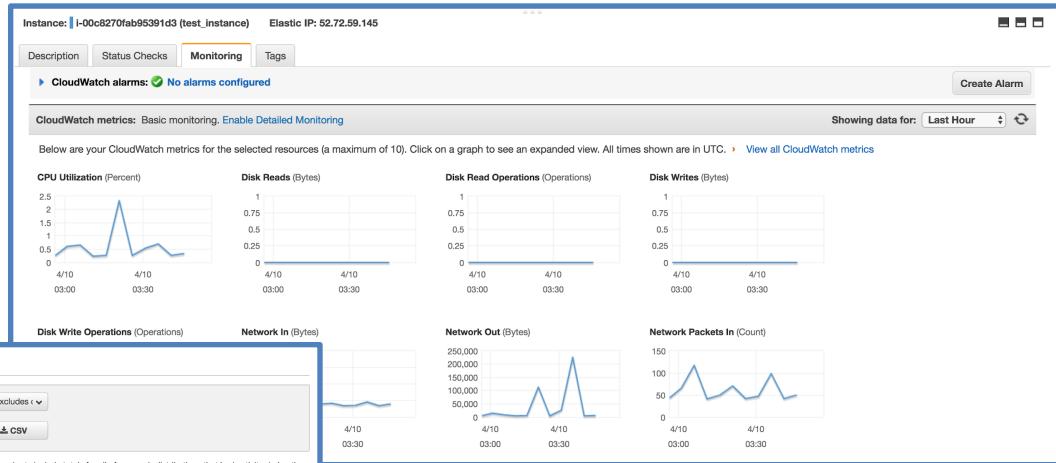
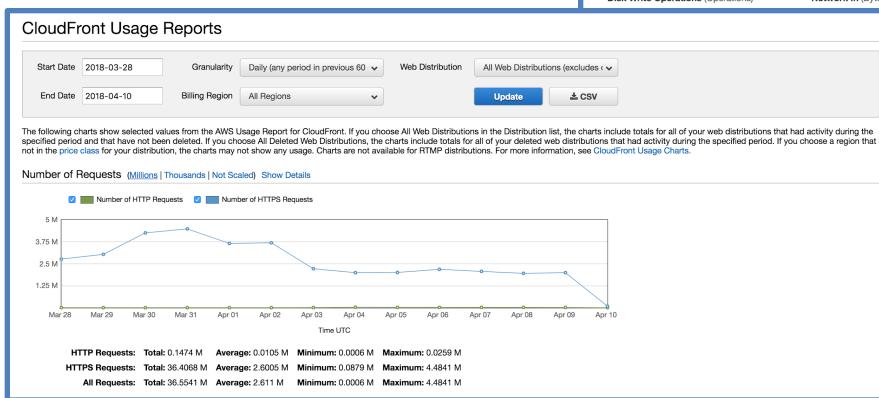
Time	Value
4/10 01:00	1
4/10 02:00	1
4/10 03:00	1

Service Health

Current Status	Details
✓ Amazon CloudWatch Service	Service is operating normally View complete service health details

CloudWatch Entry Points

Resource Dashboards



CloudWatch Entry Points

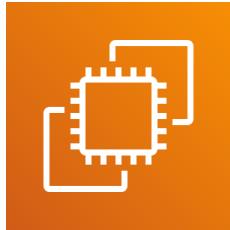
CLI

```
current_cpu=`aws cloudwatch --region $region get-metric-statistics \
--namespace AWS/EC2 --metric-name CPUUtilization \
--start-time $onehourago --end-time $now \
--period 3600 --statistics Average --dimensions Name=InstanceId,Value=$iid \
--query Datapoints[].Average --output text`
```

CloudWatch Metrics

- Performance Metrics
- Determination whether resource is performing as expected
- Can be used to trigger passive or active responses

CloudWatch Metric Highlights



CPUCreditBalance
CPUUtilization
NetworkIn
NetworkOut

EC2

CloudWatch Metric Highlights



EBS

- VolumIdleTime
- VolumeQueueLength
- VolumeReadBytes
- VolumeReadOps
- VolumeWriteBytes
- VolumeWriteOps

CloudWatch Metric Highlights



Classic LB

BackendConnectionErrors
HTTPCode_Backend_2XX, 3XX, 4XX, 5XX
HTTPCode_ELB_4XX,5XX
RequestCount
SpilloverCount
SurgeQueueLength
UnHealthyHostCount

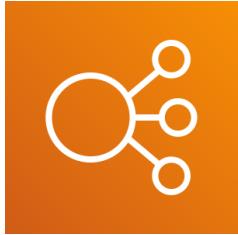
CloudWatch Metric Highlights



Application LB

ActiveConnectionCount
ConsumedLCUs
HealthyHostCount
HTTPCode_ELB_4XX_Count,5XX_Count
HTTPCode_Target_2XX_Count,3XX_Count
HTTPCode_Target_4XX_Count,5XX_Count
NewConnectionCount
RejectedConnectionCount
RequestCount
RequestCountPerTarget
RuleEvaluations
TargetConnectionErrorCount
TargetResponseTime
UnHealthyHostCount

CloudWatch Metric Highlights



Network LB

- ActiveFlowCount
- ConsumedLCUs
- HealthyHostCount
- NewFlowCount
- TCP_Client_Reset_Count
- TCP_ELB_Reset_Count
- TCP_Target_Reset_Count
- UnHealthyHostCount

CloudWatch Metric Highlights



RDS (Non-Aurora)

CPUUtilization
DatabaseConnections
FreeStorageSpace
ReadIOPS
WriteIOPS

CloudWatch Metric Highlights



RDS (Aurora)

ActiveTransactions
BlockedTransactions
CommitThroughput
DeleteThroughput
InsertLatency
(Lots of Latency/Throughput)

CloudWatch Metric Highlights



ConsumedReadCapacityUnits
ConsumedWriteCapacityUnits
ReadThrottleEvents
WriteThrottleEvents

DynamoDB

CloudWatch Custom Metrics

- Required for anything generated inside the OS
 - Shared Responsibility Model coming later
- Can be pushed from on-prem resources
- Good for application metrics

OS memory usage	database
queries/second	
OS disk space usage	nginx
connections	active
JVM heap space usage	MongoDB
lag	secondary
message queue depth	

CloudWatch Alarms

OK = Not always OK

ALARM = not always actionable

INSUFFICIENT_DATA = not always a problem

More than just < , = or >

High Resolution Alarms

Percentile Alarms

Low Data Samples

CloudWatch Alarm Actions

EC2 – Stop, Reboot, Terminate, Recover

Autoscaling – Execute Scaling Policy

SNS – Notifications

Email

SMS

HTTP/HTTPS

SNS - Trigger

Lambda function



CloudWatch Alarm Actions

EC2 – Stop, Reboot, Terminate, Recover

Autoscaling – Execute Scaling Policy

SNS – Notifications

Email

SMS

HTTP/HTTPS

SNS - Trigger

Lambda function

Remediate
is
ACTIVE

CloudWatch Events

Doesn't require metrics

More like a transaction log

Events -> Rules -> Targets



Lambda



SSM Run Command



Kinesis Firehose

And more!

CloudWatch Logs

Action	Details
Aggregate	Multiple sources
Store	Durable and reliable
Access	Console, CLI, SDK
Monitor	Metric filters

CloudWatch Logs

- No single point of failure
- Integration with AWS Ecosystem
- Aggregation point for custom logs (requires agent)
 - EC2
 - On premises

CloudWatch Logs Agent

Single command install

Requires configuration file

Great for OS and application logs

Automate install

- AMI
- EC2 user-data
- Configuration management software
- EC2 Run-command

Access Logs

S3

ELB

Cloudfront/WAF

Stored in S3

API Gateway

Stored in
CloudWatch
Logs

Log Monitoring and Storage

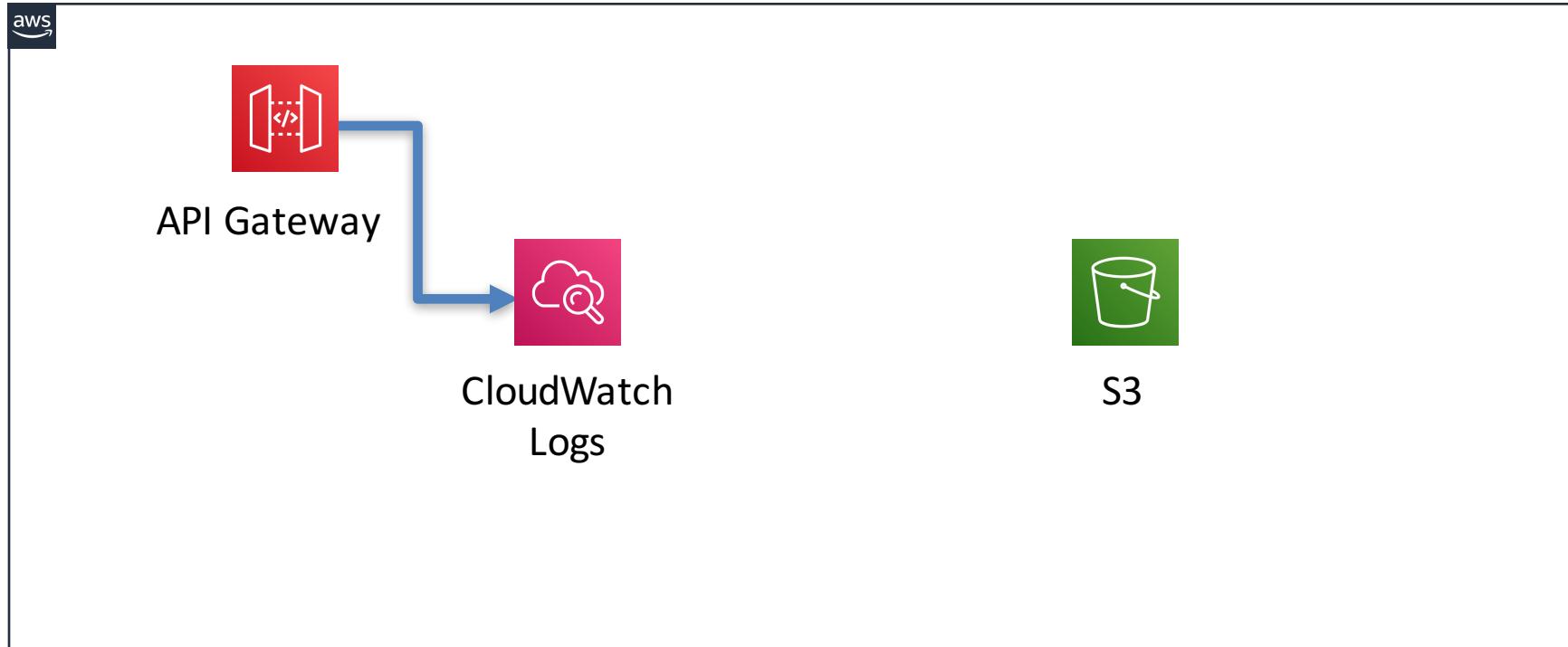


CloudWatch
Logs

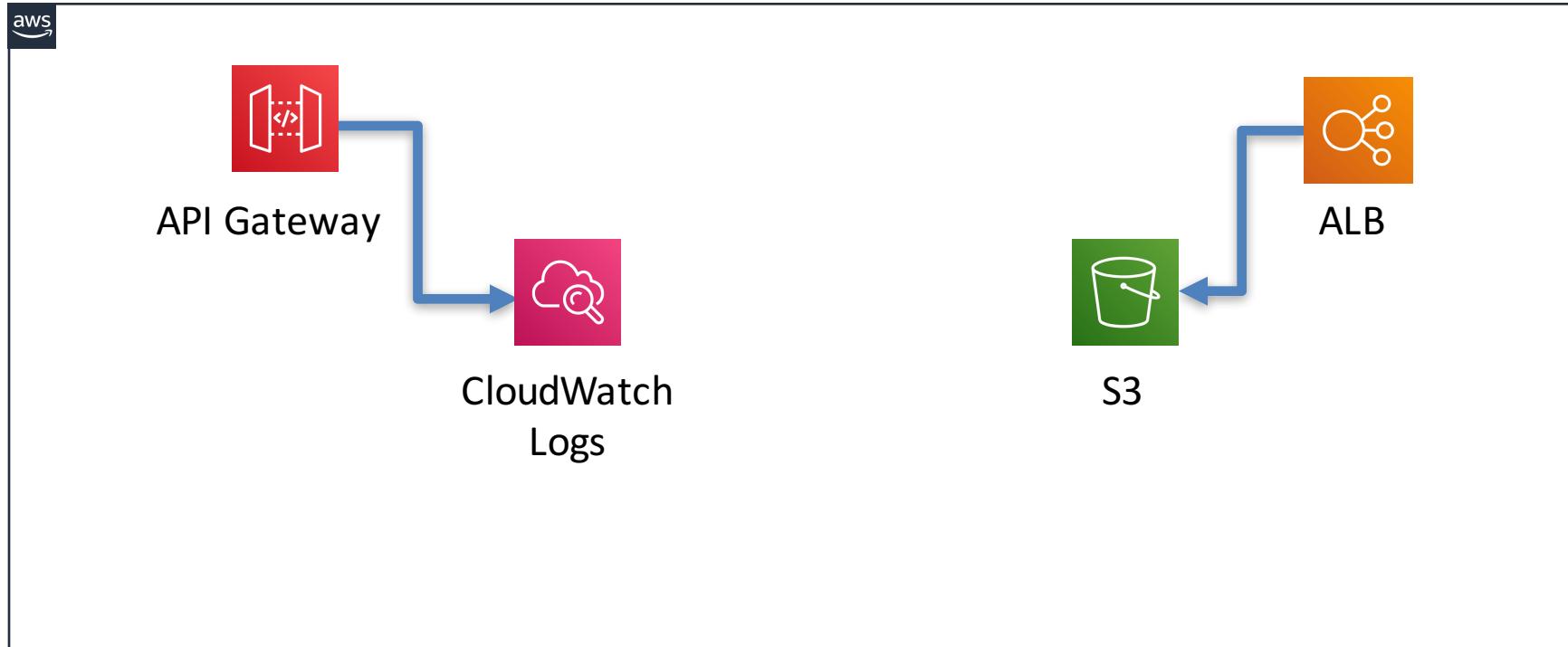


S3

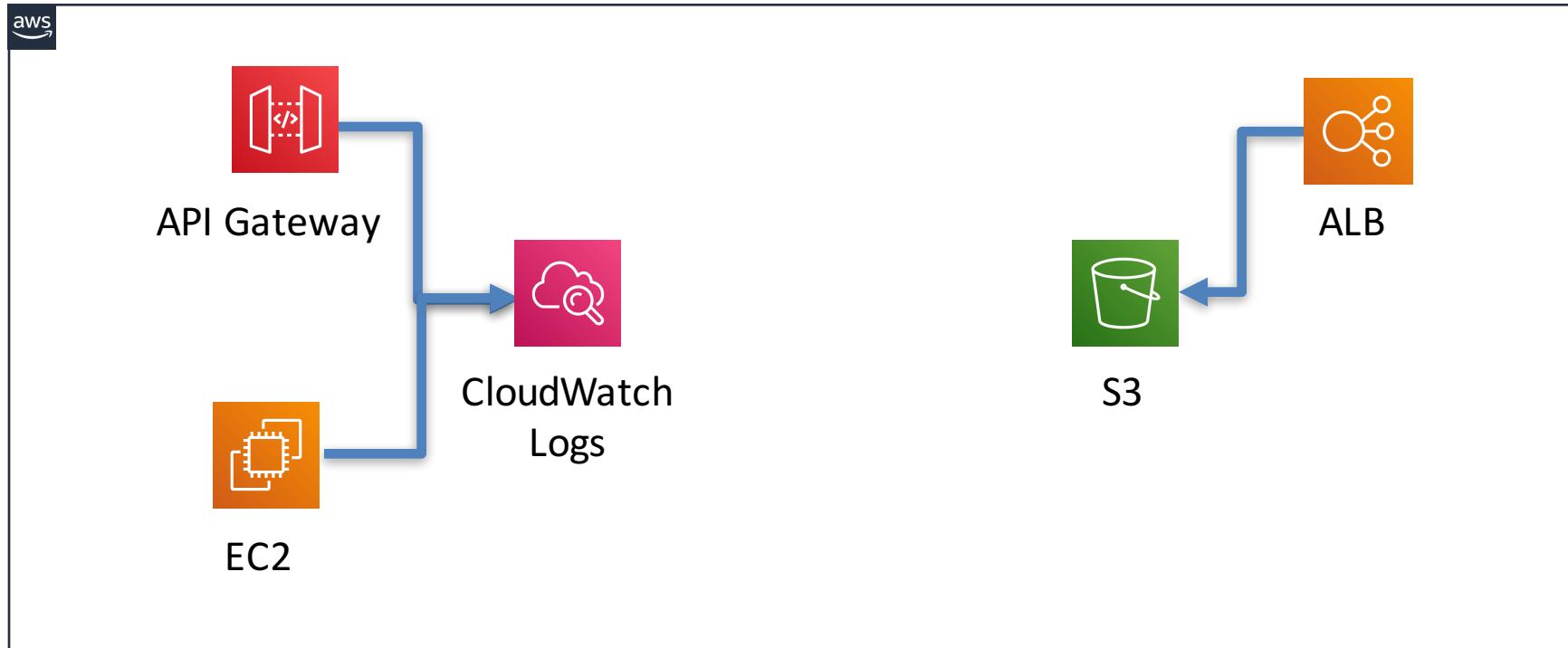
Log Monitoring and Storage



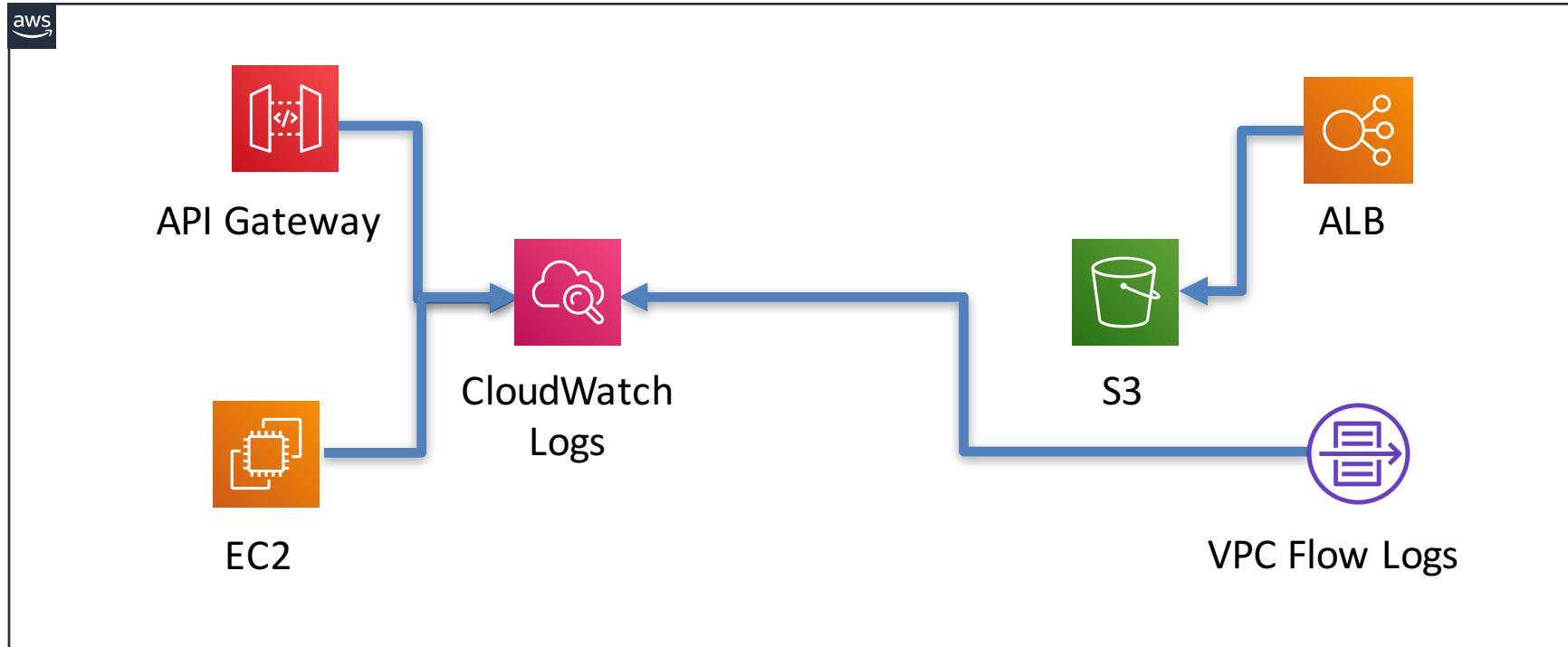
Log Monitoring and Storage



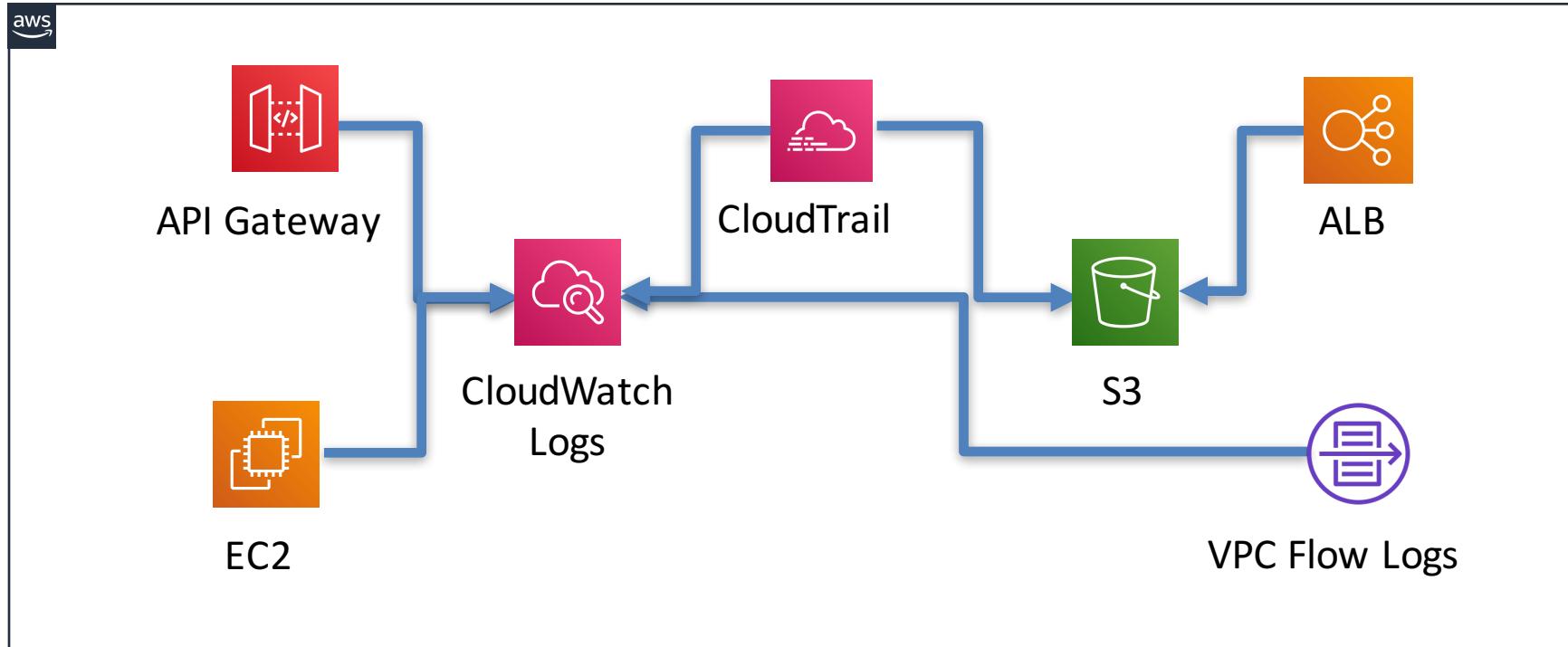
Log Monitoring and Storage



Log Monitoring and Storage



Log Monitoring and Storage



Log Monitoring and Storage

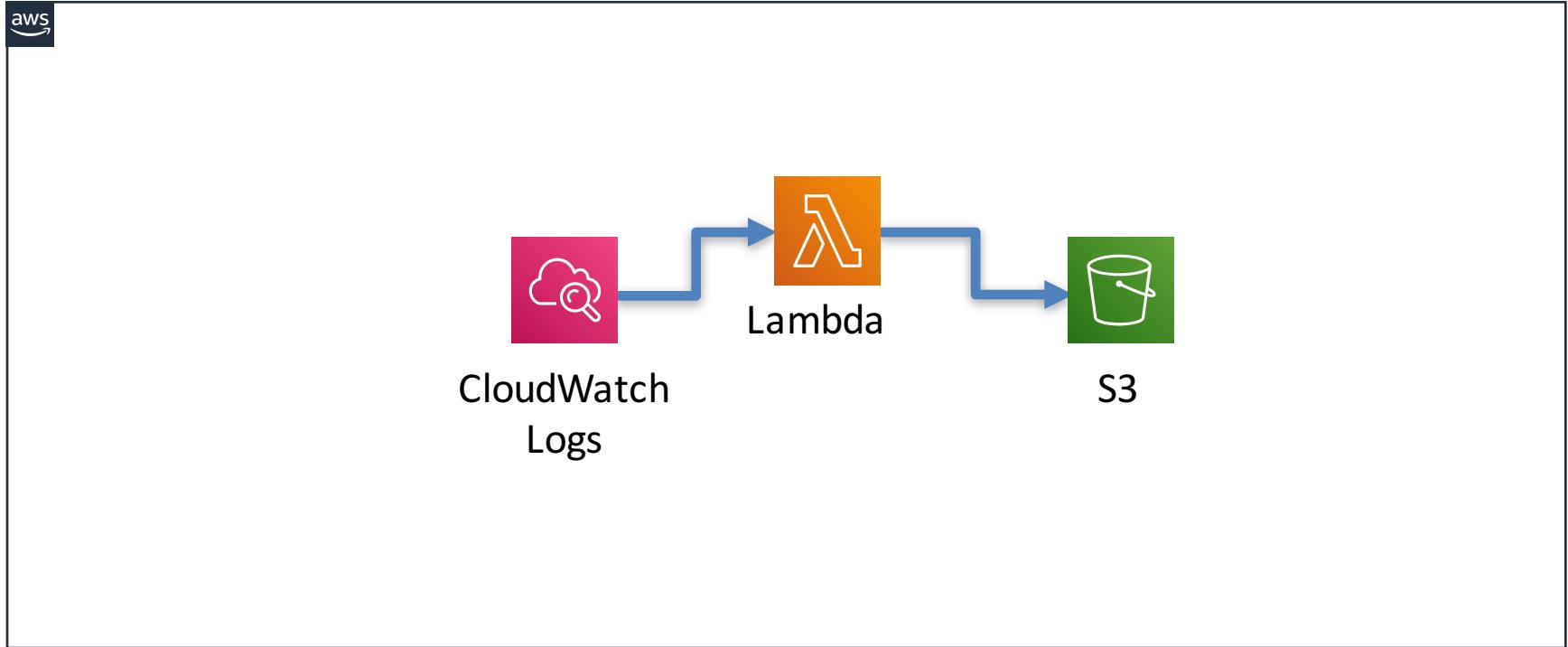


CloudWatch
Logs



S3

Log Monitoring and Storage



Status Checks

- Availability Metrics
- Determination whether resource is accessible
- Can indicate failures at infrastructure tier

EC2 Status Checks

- System Status Checks
 - Network connectivity
 - Physical host power
 - Physical host OS issues
 - Physical host H/W issues
- Instance Status Checks
 - Network configuration issue
 - OS configuration issue
 - OOM
 - Corrupt volume
 - Kernel issue

EBS Volume Status Check

- ok
- warning
- impaired
- insufficient-data

EBS Volume Perf Status Check

- ok
 - Normal volume performance
- warning
 - Degraded or Severely Degraded volume performance
- impaired
 - Stalled or Not Available
- insufficient-data

RDS Status Checks

- Available
- **Backing-up**
- Configuring-enhanced-monitoring
- Creating
- Deleting
- **Failed**
- Inaccessible-encryption-credentials
- Incompatible-credentials

RDS Status Checks cont'd

- Incompatible-network
- **Incompatible-option-group**
- **Incompatible-parameters**
- Incompatible-restore
- Maintenance
- Modifying
- **Rebooting**
- Renaming

RDS Status Checks cont'd

- Resetting-master-credentials
- Restore-error
- Starting
- Stopping
- Stopped
- **Storage-full**
- Storage-optimization
- **Upgrading**

RedShift Cluster Status

- Available
- Creating
- Deleting
- Final-snapshot
- **Hardware-failure**
- Incompatible-hsm
- Incompatible-network
- **Incompatible-parameters**

RedShift Cluster Status cont'd

- Incompatible-restore
- **Modifying**
- Rebooting
- Renaming
- **Resizing**
- Rotating-keys
- Storage-full
- Updating-hsm

Remediate After Monitoring

Learn ways to optimize network performance

Know how to recognize bottlenecks

Maximize VPC Network Performance

- Single AZ
- Placement group
- Enhanced networking
- Jumbo frames
- Keep traffic inside VPC
- VGW vs Direct Connect

Identify Bottlenecks

- Undersized NAT instance
- Undersized RDS instance
- Undersized EC2 instance
- Old EC2 instance type
- Underprovisioned EBS volume
- Latency from cross-AZ traffic
- Serving static assets from EC2
- Aggregating S3 requests from single instance

Question Breakdown

Your company runs RabbitMQ on EC2, and wants to push custom metrics from the application into CloudWatch. Instances are launched into an IAM Role with appropriate permissions to accomplish this. There is a security requirement to track CloudWatch API calls to ensure an audit trail. How can this requirement be met?

- A. Install the CloudWatch Logs Agent on the EC2 instances.
- B. Enable detailed monitoring on the EC2 instances.
- C. Create a CloudWatch Alarm on each RabbitMQ custom metric.
- D. Enable AWS CloudTrail in the same region as the EC2 instances.

Breakdown – Key Terms

Your company runs RabbitMQ on **EC2**, and wants to push **custom metrics** from the application into CloudWatch. Instances are launched into an IAM Role with appropriate permissions to accomplish this. There is a security requirement to **track CloudWatch API** calls to ensure an **audit trail**. How can this requirement be met?

- A. Install the CloudWatch Logs Agent on the EC2 instances.
- B. Enable detailed monitoring on the EC2 instances.
- C. Create a CloudWatch Alarm on each RabbitMQ custom metric.
- D. Enable AWS CloudTrail in the same region as the EC2 instances.

Breakdown – Answer Selection

Your company wants to monitor the application logs with application requirements. How can this requirement be met?

Enables CloudWatch Logs integration, but doesn't meet requirement.

- A. **Install the Cloudwatch Logs Agent on the EC2 instances.**
- B. Enable detailed monitoring on the EC2 instances.
- C. Create a CloudWatch Alarm on each RabbitMQ custom metric.
- D. Enable AWS CloudTrail in the same region as the EC2 instances.

Breakdown – Answer Selection

Your company has an application that needs to be monitored with application metrics. You have requirements to change the polling period for CloudWatch Metrics from 1 minute to 10 minutes. How can you do this?

Just changes polling period for CloudWatch Metrics from 1 minute to 10 minutes.

- A. Install the CloudWatch Logs Agent on the EC2 instances.
- B. **Enable detailed monitoring on the EC2 instances.**
- C. Create a CloudWatch Alarm on each RabbitMQ custom metric.
- D. Enable AWS CloudTrail in the same region as the EC2 instances.

Breakdown – Answer Selection

Your company wants to monitor the application logs with application requirements. This request

Enables alerts and actions but no audit trail

- A. Install the CloudWatch Logs Agent on the EC2 instances.
- B. Enable detailed monitoring on the EC2 instances.
- C. **Create a CloudWatch Alarm on each RabbitMQ custom metric.**
- D. Enable AWS CloudTrail in the same region as the EC2 instances.

Breakdown – Answer Selection

Your company has an application that needs to be audited with appropriate logs. You have requirements to audit the logs and meet this requirement.

CloudTrail logs enable audit trail and meets requirement

- A. Install the CloudWatch Logs Agent on the EC2 instances.
- B. Enable detailed monitoring on the EC2 instances.
- C. Create a CloudWatch Alarm on each RabbitMQ custom metric.
- D. **Enable AWS CloudTrail in the same region as the EC2 instances.**

Breakdown – Answer Selection

Your company has an application deployed to Amazon EC2 instances. The application generates custom metrics that you want to monitor. You have created a CloudWatch Metrics stream and a CloudWatch Metrics role.

Answer: D

- A. Install the CloudWatch Logs Agent on the EC2 instances.
- B. Enable detailed monitoring on the EC2 instances.
- C. Create a CloudWatch Alarm on each RabbitMQ custom metric.
- D. Enable AWS CloudTrail in the same region as the EC2 instances.

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button on a media player.

AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 2 - High Availability

High Availability

- 8% of exam content
- Implement **scalability** and **elasticity** based on use case
- **Recognize** and **differentiate highly available** and **resilient** environments on AWS

TL; DR

- Learn common deployment patterns for HA
- Just in time provisioning
- Trend toward temporary resources
- Trend toward managed services
- Trend toward regional scope over AZ scope
- Multi-regional deployments increase availability *and* cost
- Focus on details over strategy
- How does HA affect operations?

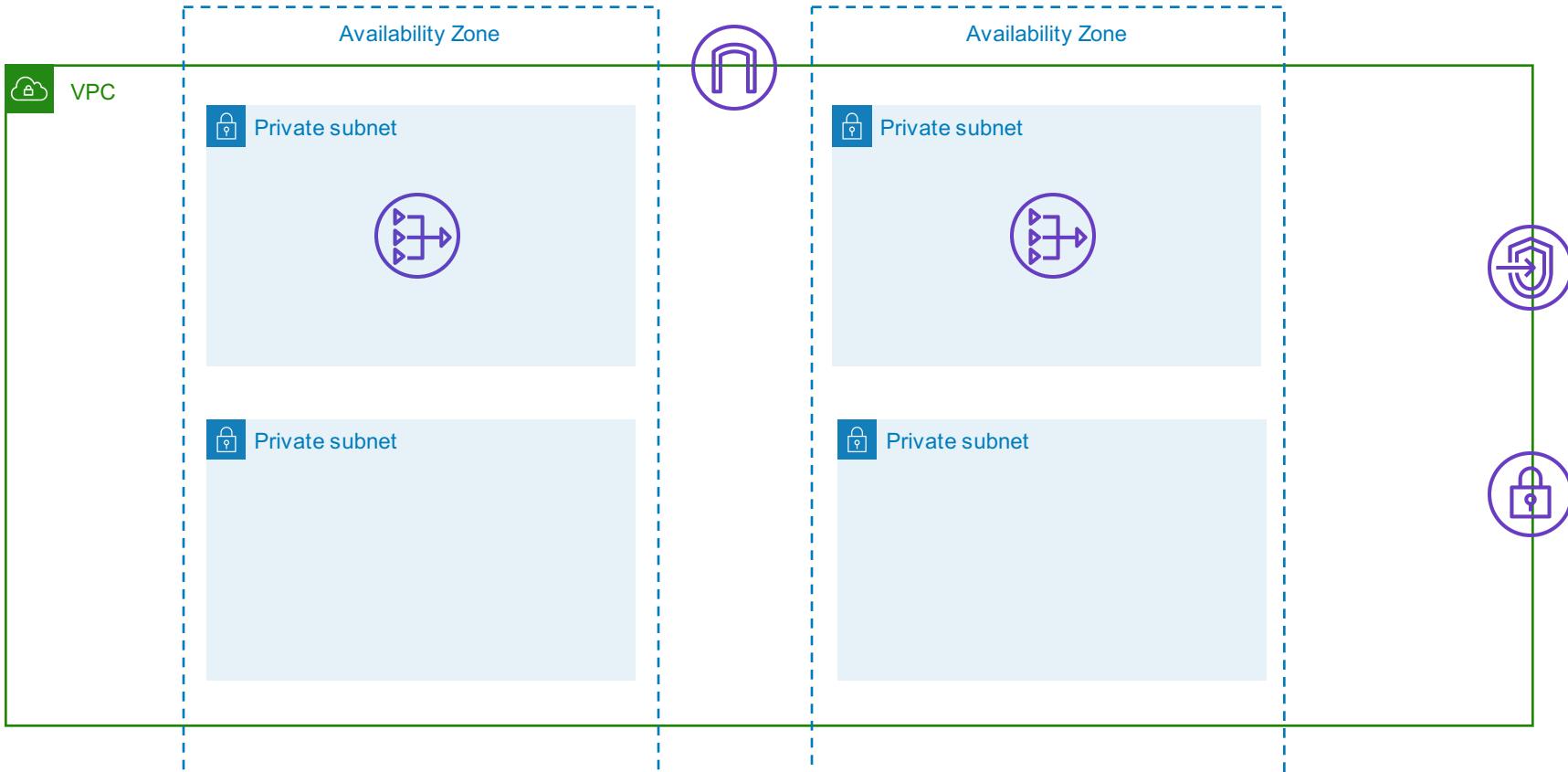
Terms

Fault Tolerance - The system will continue to function **without degradation in performance** despite the complete failure of any component of the architecture.

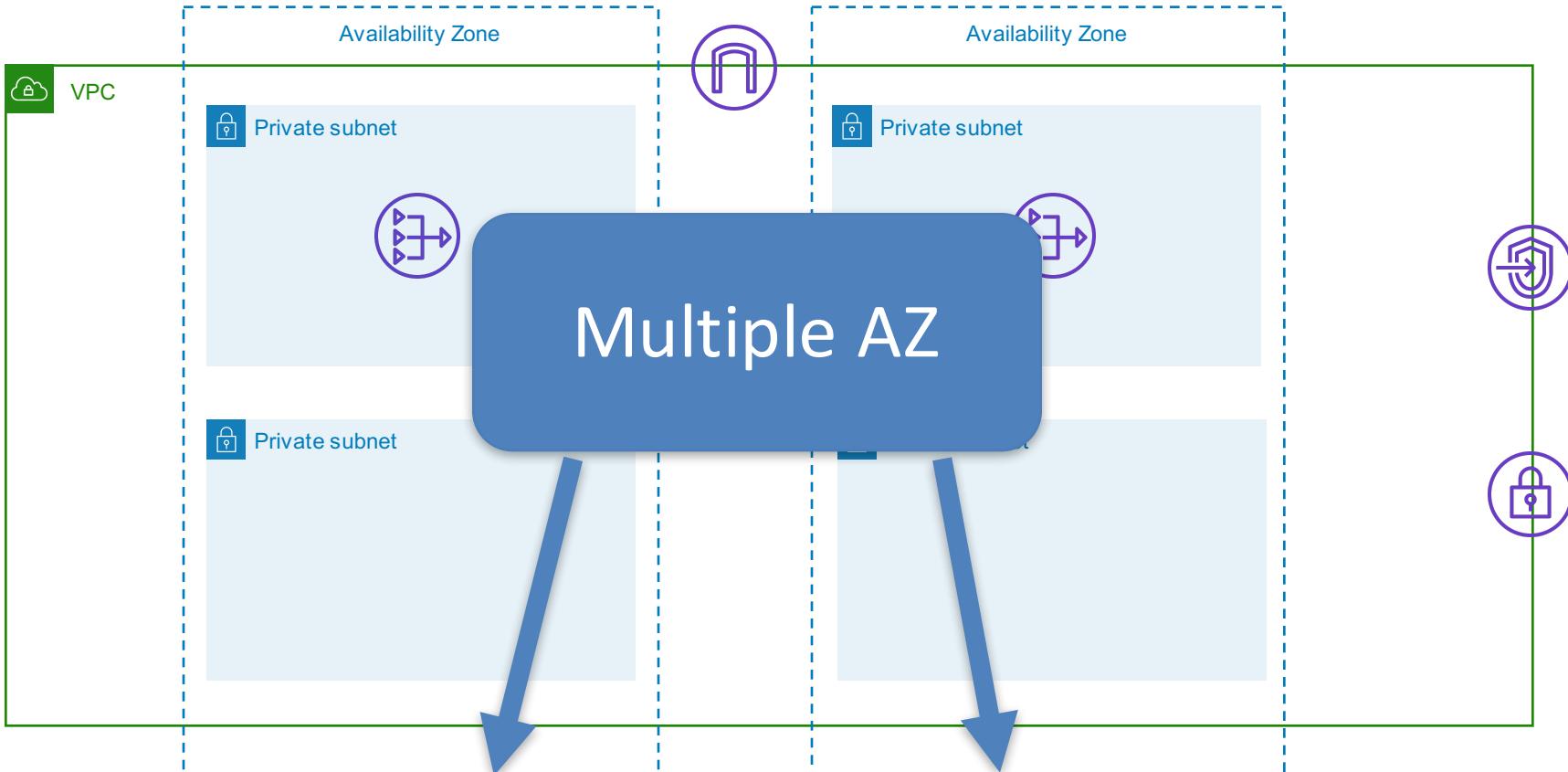
High Availability - The system will continue to function despite the complete failure of any component of the architecture.

Fault tolerant services are ALSO highly available, but the reverse is not necessarily true

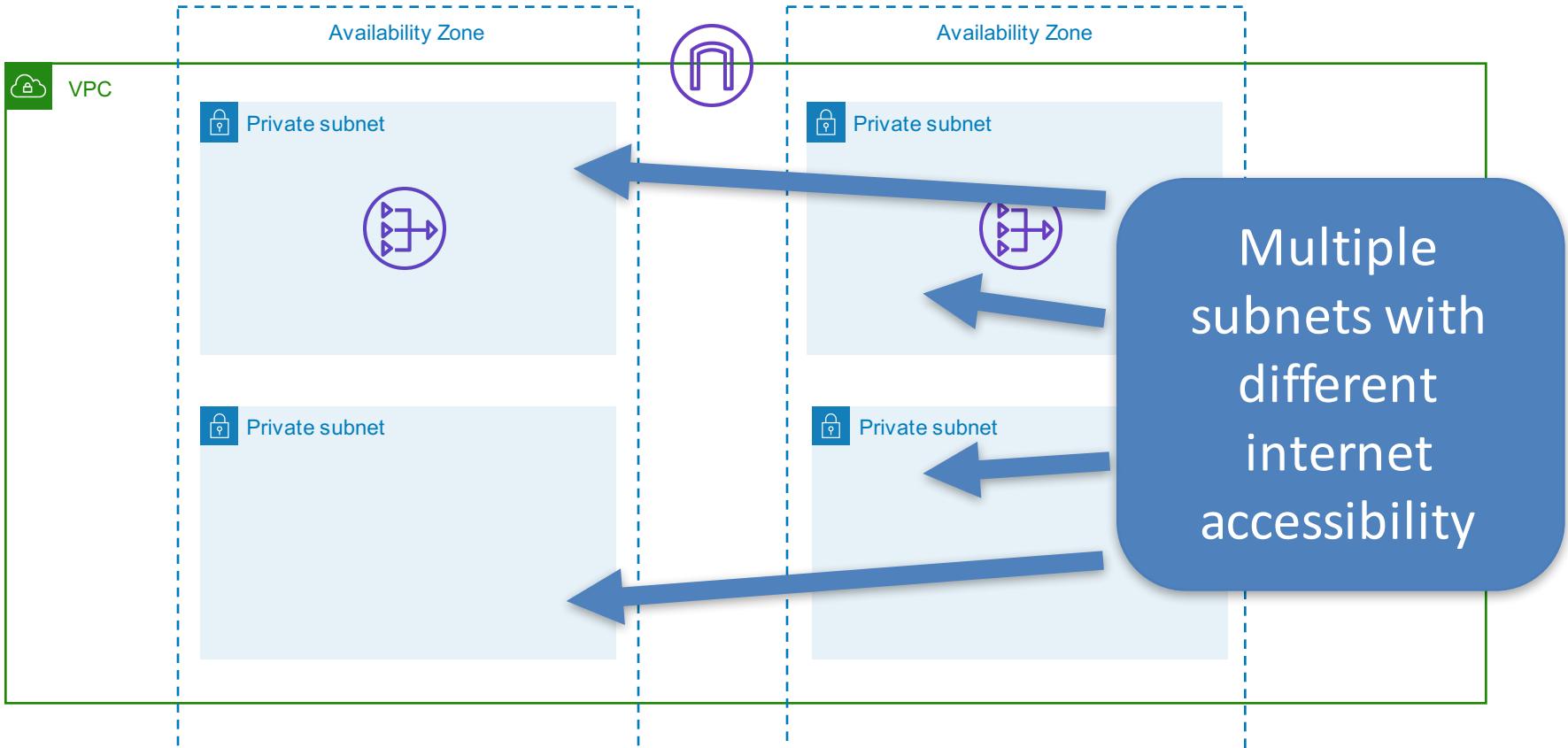
VPC



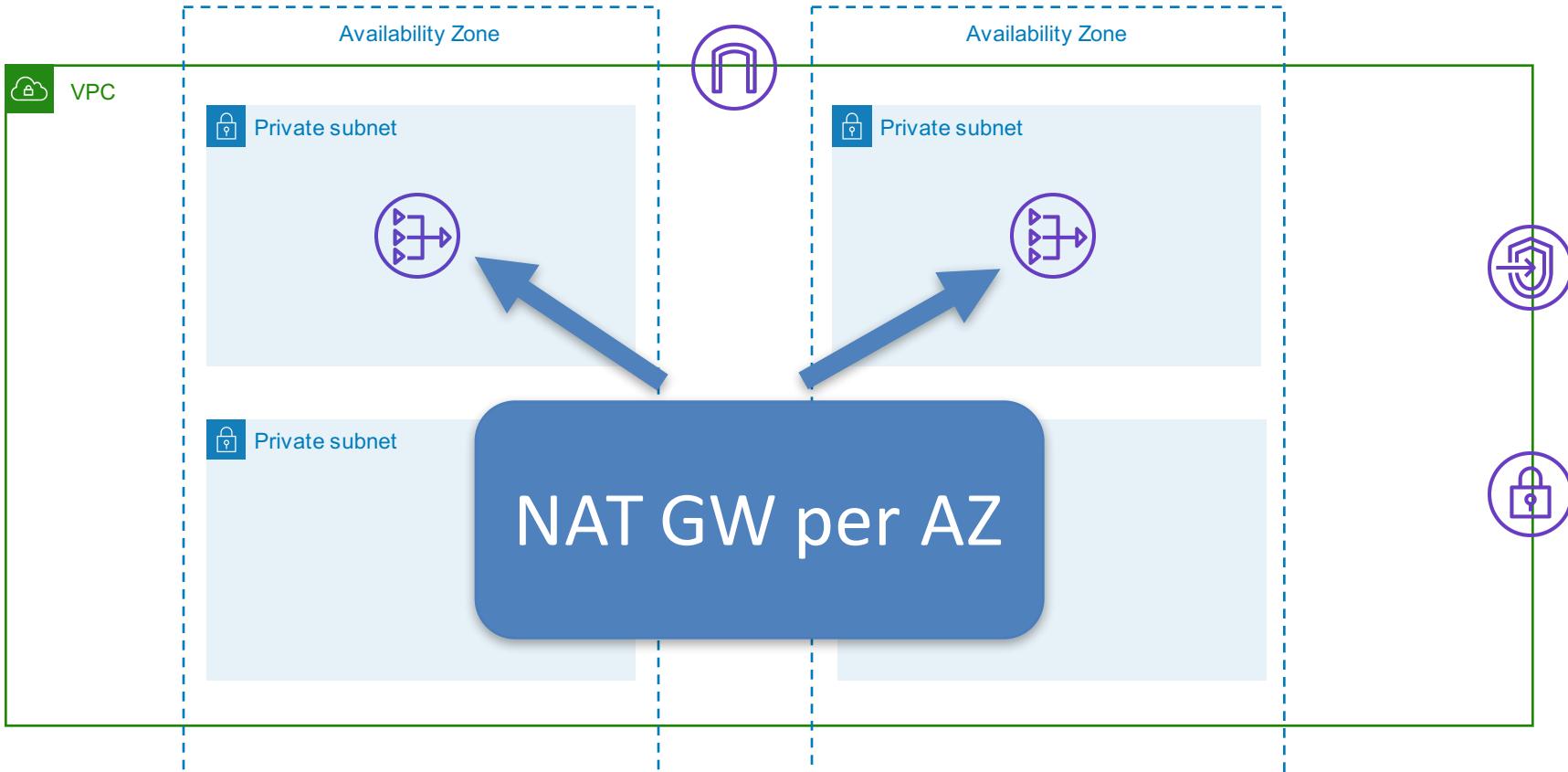
VPC



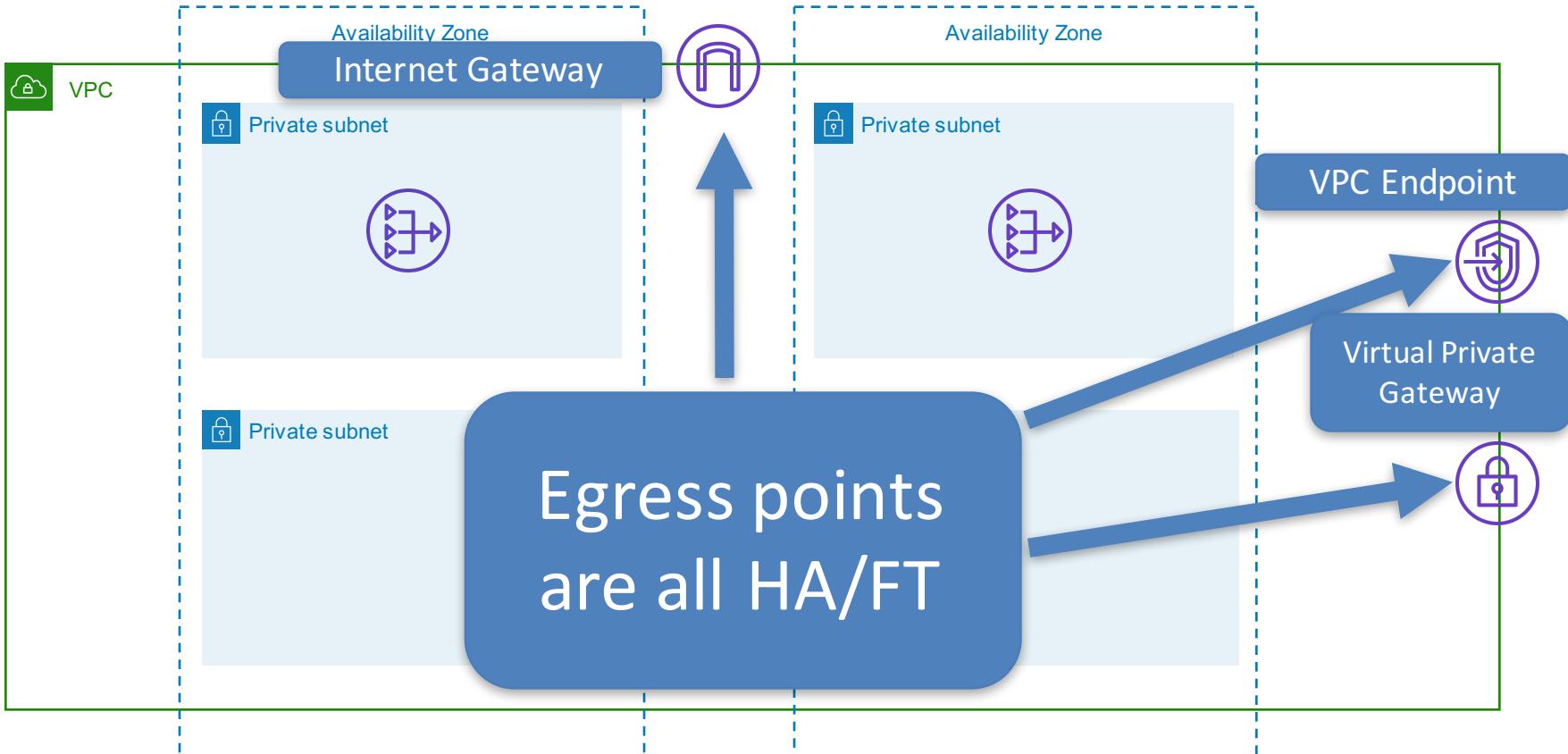
VPC



VPC



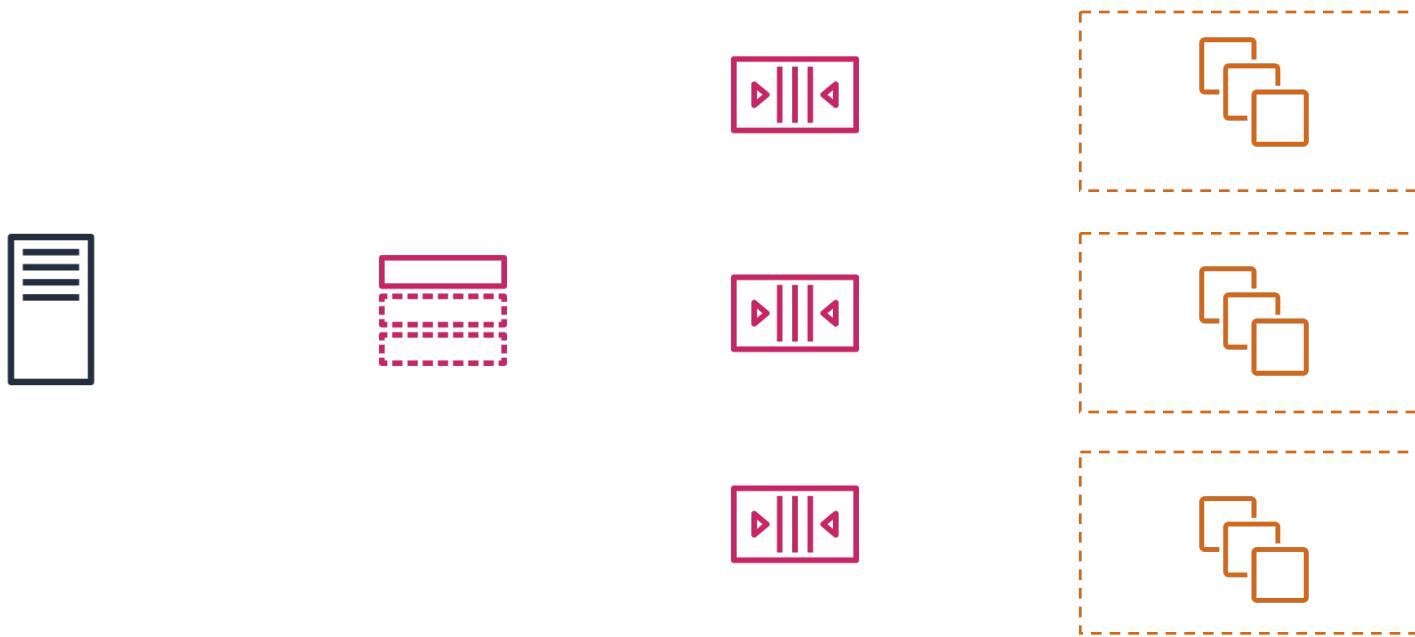
VPC



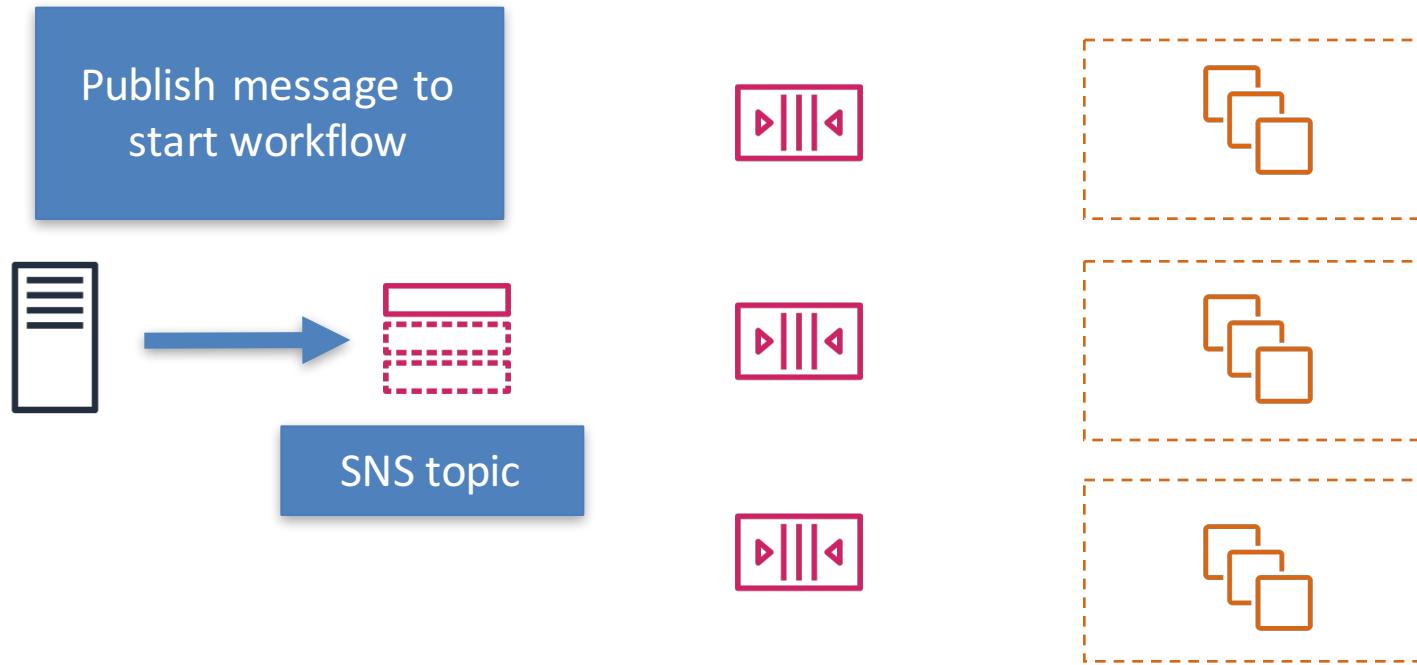
Inherently HA, scalable and elastic Classic

- Layer 4 or 7
- Supports EC2 Classic
- ALB
 - Layer 7
 - Path-based routing
- NLB
 - Layer 4
 - Static IP entry point

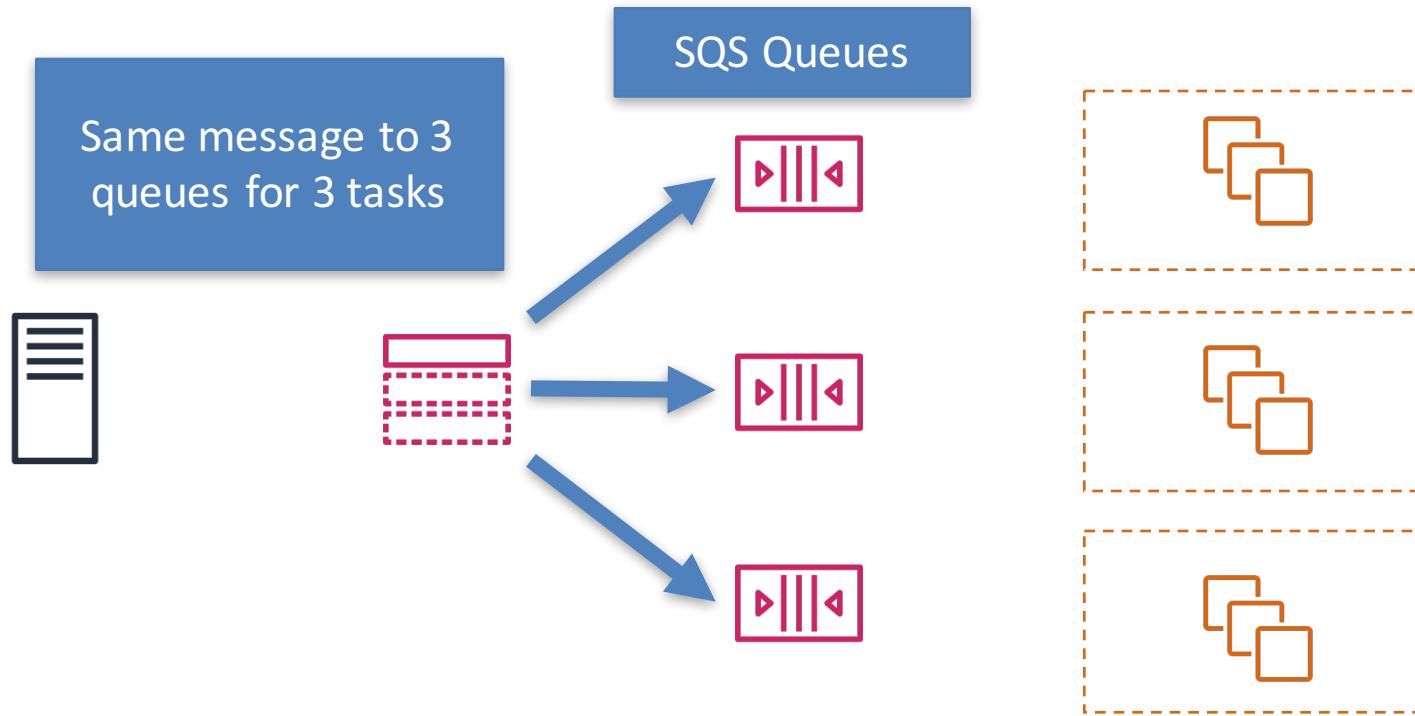
Decoupling with SNS and SQS



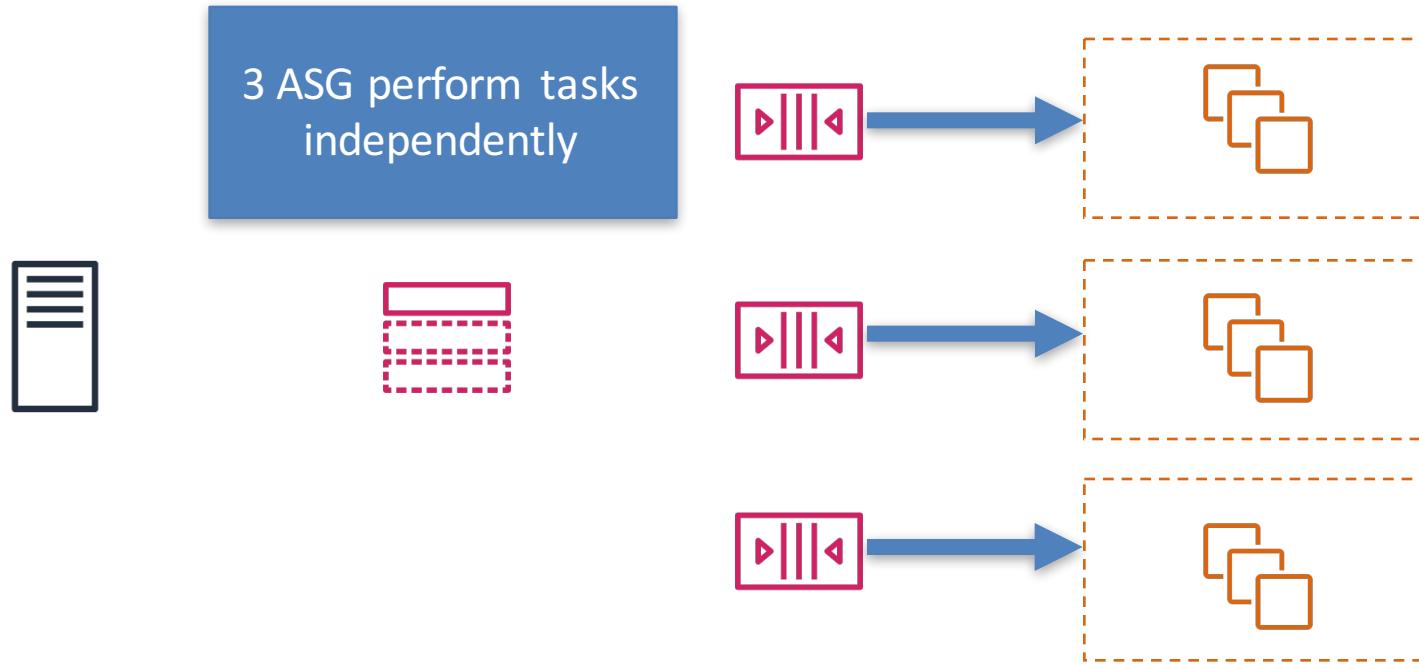
Decoupling with SNS and SQS



Decoupling with SNS and SQS



Decoupling with SNS and SQS



Auto Scaling

Flagship service

- Achieve several best practices at once
 - **Highly available**
 - Cost optimized
 - Temporary resources
- Regional service scope
- Read **ALL** docs on Auto Scaling operations
- Learn Auto Scaling scenarios

Auto Scaling Basics

Launch Template

WHAT to launch
EC2 instance type
Security Group
IAM Role
Pricing model

Auto Scaling Group

WHERE to launch
LIMITATIONS of launch
VPC subnets
ELB association

Auto Scaling Policy

WHEN to launch
Based on metrics
CloudWatch Alarm

Scheduled Actions

WHEN to launch
Based on calendar
Coexist with policies

Auto Scaling Operations

- Manage Auto Scaling policies and step scaling
- Monitor ASG min and max instances
- Roll out updated launch configuration
- Manual tasks for lifecycle hooks
- Manage cooldown periods

Auto Scaling Scenarios

- Stateless web applications
- Unpredictable traffic
- Steady-state groups
- Message queue consumption applications

Auto Scaling Anti-Scenarios

- Applications with session stickiness
- Monolithic applications (singleton instance)
- Applications with fixed IP addresses
- Applications with many manual deploy steps
- Applications with short, large, random traffic spikes

Route53 Basics

- Register domains and serve DNS records
- 100% uptime SLA
- Several routing options
- Health checks
- Failover options
- Integration points with AWS resources

Route53 for HA

- Direct traffic to multiple regions for resiliency
 - Latency-based routing
 - Weighted round robin
- Health checks to avoid degraded endpoints
- ALIAS records
 - Pointer to AWS resources
 - Avoid using IP addresses as SPoF

EC2 Autorecovery

- Alternative to Auto Scaling for steady state
- Maintain instance ID
- Migration to new hardware during reboot
- Recover on demand or use a CloudWatch alarm
- Restrictions on valid instance types

Assumes most operational overhead of DB servers

- OS installation/configuration
 - Database software installation/configuration
 - Backups
 - Patches/updates
 - Failover
 - Replication
- = **Reduced risk**
- = **Higher availability**

RDS Operations

No service interruption

- Snapshots (daily automated or manual)
- Storage upsize
- Add Read Replica

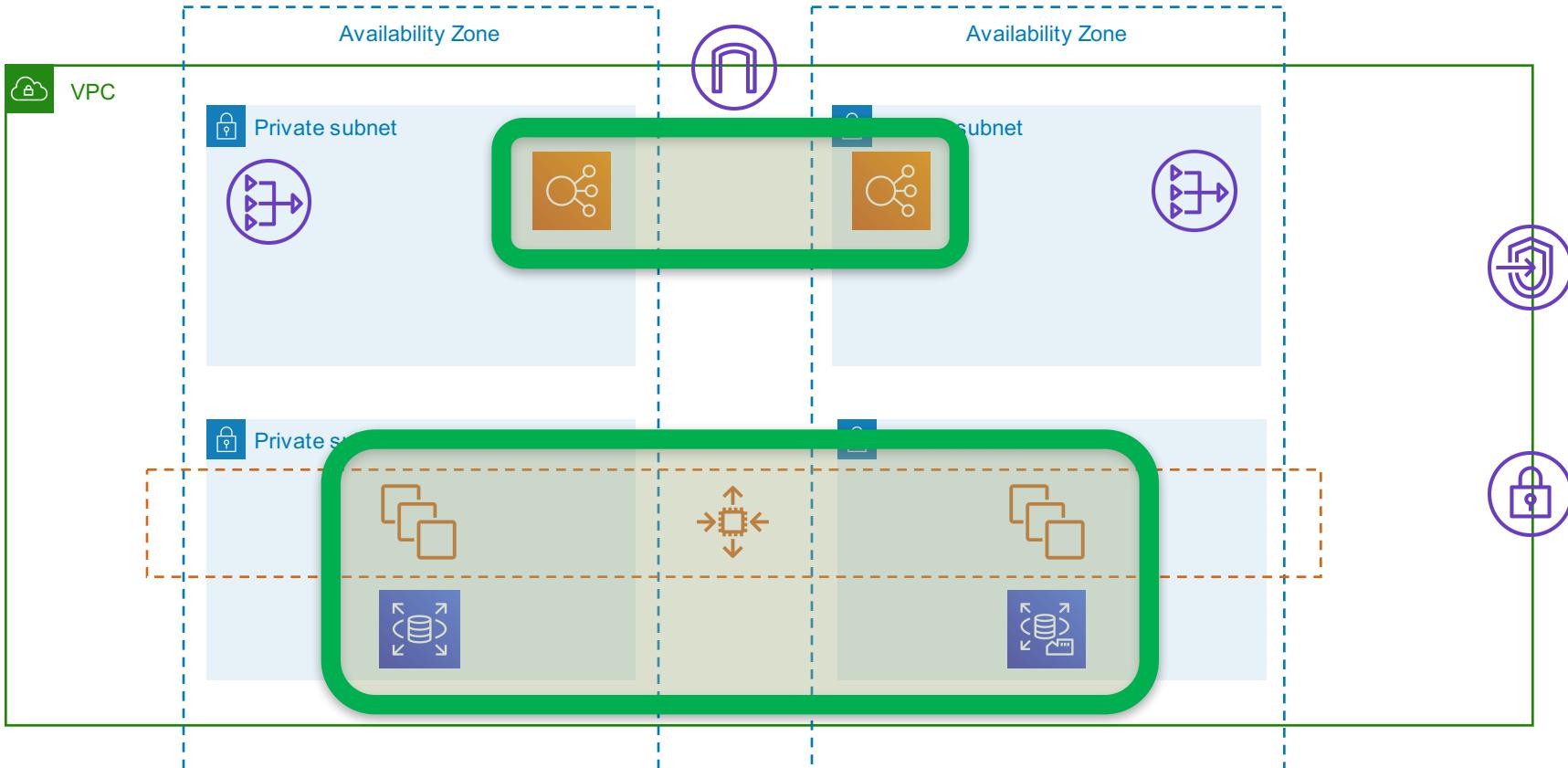
Service interruption

- Configuring Multi-AZ deployment
- Multi-AZ failover
- DB Engine update
- Parameter update

Elastic Beanstalk

- Assumes operational overhead of managing environments, including updates and rollback
- Region-scoped service that supports multiple AZ
- Can be configured with **no single points of failure**
- Platform deploys choices of the following:
 - Elastic Load Balancer
 - EC2
 - Auto Scaling
 - RDS

Elastic Beanstalk Context



Elastic Beanstalk Further Reading

- Supported web server software
- Supported languages
- Application cloning workflow
- Application deployment options
- Deployment rollback options

Understanding Tradeoffs

- Scalability
- Elasticity
- Cost
- Performance

Question Breakdown

Your organization has an S3 bucket named `company_critical_files` used to store file backups from an important source. You've been asked to evaluate the availability of this bucket, and make recommendations to improve the availability. What solution would you recommend?

- A. Create an S3 bucket in a different region than `company_critical_files`.
Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on `company_critical_files`.

Breakdown – Key Terms

Your organization has an **S3 bucket** named company_critical_files used to store file backups from an important source. You've been asked to **evaluate the availability** of this bucket, and make recommendations to **improve the availability**. What solution would you recommend?

- A. Create an S3 bucket in a different region than company_critical_files. Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on company_critical_files.

Breakdown – Answer Selection

Your organization needs to store files. The available storage is limited.

Replication to a second region increases availability

- A. Create an S3 bucket in a different region than company_critical_files. Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on company_critical_files.

Breakdown – Answer Selection

Your organization needs to store files with high availability.

Disabling deletes doesn't change availability

- A. Create an S3 bucket in a different region than company_critical_files. Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on company_critical_files.

Breakdown – Answer Selection

Your organization needs to store files with 4 9s of availability.

Doesn't address the requirement

- A. Create an S3 bucket in a different region than company_critical_files. Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on company_critical_files.

Breakdown – Answer Selection

Your organization needs to store files. The availability of the files is critical. You need to evaluate the cost of downtime and determine how long the system can be down before it affects the business.

Versioning helps prevent accidental deletion, no effect on availability

- A. Create an S3 bucket in a different region than company_critical_files. Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on company_critical_files.

Breakdown – Answer Selection

Your organization needs to store files with 4 9s of availability.

Answer: A

- A. Create an S3 bucket in a different region than company_critical_files. Enable versioning on both buckets, then enable cross-region replication to the new bucket.
- B. Use a bucket policy to disable deletes on the bucket.
- C. No changes. 4 9s of availability is enough.
- D. Enable versioning on company_critical_files.

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button on a media player.

AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 3 - Deployment and Provisioning

Deployment and Provisioning

- 14% of exam content
- **Identify** and **execute** steps required to **provision cloud resources**
- **Identify** and **remediate** deployment **issues**

TL; DR

- Know how to deploy individual resources
- Understand how to deploy groups of resources
- Deployment choices are not mutually exclusive
- Learn limitations of Infrastructure As Code options
- Identify tools for troubleshooting issues

Provision Cloud Resources

Manual Provisioning

- Console – can't be automated
- CLI – can be converted to automation
- SDK – can be converted to automation
- API – can be automated, CLI/SDK easier?

Provisioning EC2 with AMIs

Spectrum from fully-baked to base image and everything in between

- Know how to design for speed (fully-baked)
- Know how to design for flexibility (base image)
- Bootstrapping building blocks
 - User-data
 - Cloudformation cfn-update
 - Configuration management software

Provision and Automate

Service Name	Infrastructure Deploy	Infrastructure Change	Code Deploy
CloudFormation	✓	✓	(sorta)
OpsWorks	✓	✓	✓
Elastic Beanstalk	✓	✓	✓
SSM Run-Command			✓
ECS/EKS	✓	✓	✓
CodeDeploy			✓
3 rd Party	(depends)	(depends)	(depends)

Provision and Automate

Service Name	Infrastructure Deploy	Infrastructure Change	Code Deploy
CloudFormation	✓		
OpsWorks	✓		
Elastic Beanstalk	✓		
SSM Run-Command			
ECS/EKS	✓		
CodeDeploy			
3 rd Party	(depends)		

Supports Container Deployments!

CloudFormation Basics

Flagship service

- Infrastructure as Code (JSON, YAML)
- Integrated with most of AWS
- Exceptions are documented
- Deploy infrastructure and changes
- Does NOT operate on data

CloudFormation Template

Description

Metadata

Parameters

Mappings

Conditions

Transform

Resources – only required section

Output

CloudFormation Template

Description

Metadata

Parameters

Mappings

Conditions

Transform

Resources

Output

Focus here!

CloudFormation Study Hints

1. How can your template be used in multiple regions?
2. What happens when the template creation fails?
3. What happens when the template update fails?
4. Which designs require explicit dependencies?
5. Which resources are replaced upon stack update?
6. Which resources are retained upon stack delete?
7. What are change sets and why are they important?

OpsWorks Basics

Configuration Management + IAC

- Chef Automate
- Puppet Enterprise
- Stacks consist of layers
 - EC2
 - Elastic Load Balancing
 - RDS
 - ECS
 - Custom

OpsWorks Key Concepts

- Good for Chef/Puppet shops (hybrid environments)
- Integrated with Auto Scaling
- Focuses on resources similar to on-prem networks
- Managed service = highly available
- Many integration points with AWS ecosystem

Elastic Beanstalk Basics

Covered earlier

Elastic Beanstalk Key Concepts

- Manages platform
 - ELB
 - Auto Scaling
 - RDS
- Used for resource create, update, and delete actions
- Still requires OS management
- Does not address backups
- Does not address multi-regional deployment

SSM Run Command Basics

- Runs manual or scheduled tasks
- Works in hybrid environments
- Parallelized
- Track results and errors
- Easier to troubleshoot in bulk than manual operations
- Requires agent
- Requires access to SSM service API endpoint

ECS Basics

- Deploy containers without managing infrastructure
- Supports Docker and Windows containers
- Choice of deployment via EC2 or Fargate
- Supports existing VPC infrastructure

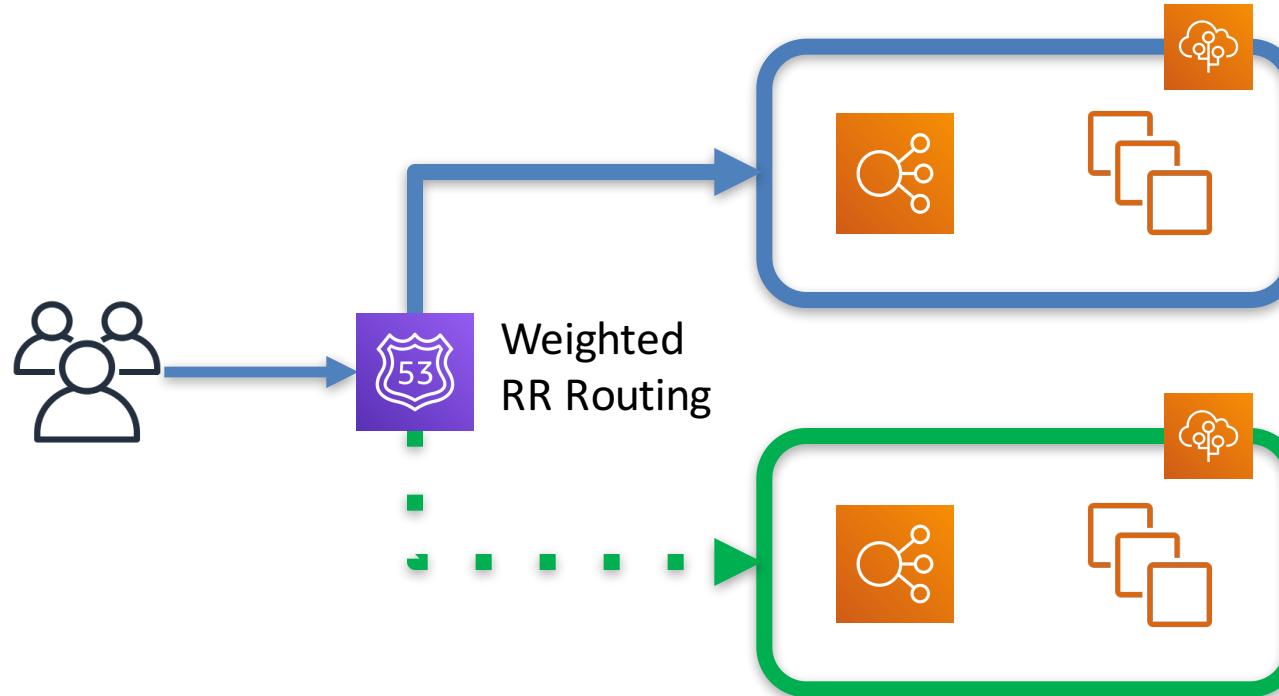
EKS Basics

- Similar to ECS, but uses Kubernetes
- Deploy Docker containers without managing infrastructure
- Choice of deployment via EC2 or Fargate
- Supports existing VPC infrastructure
- Hybrid infrastructure support

CodeDeploy Basics

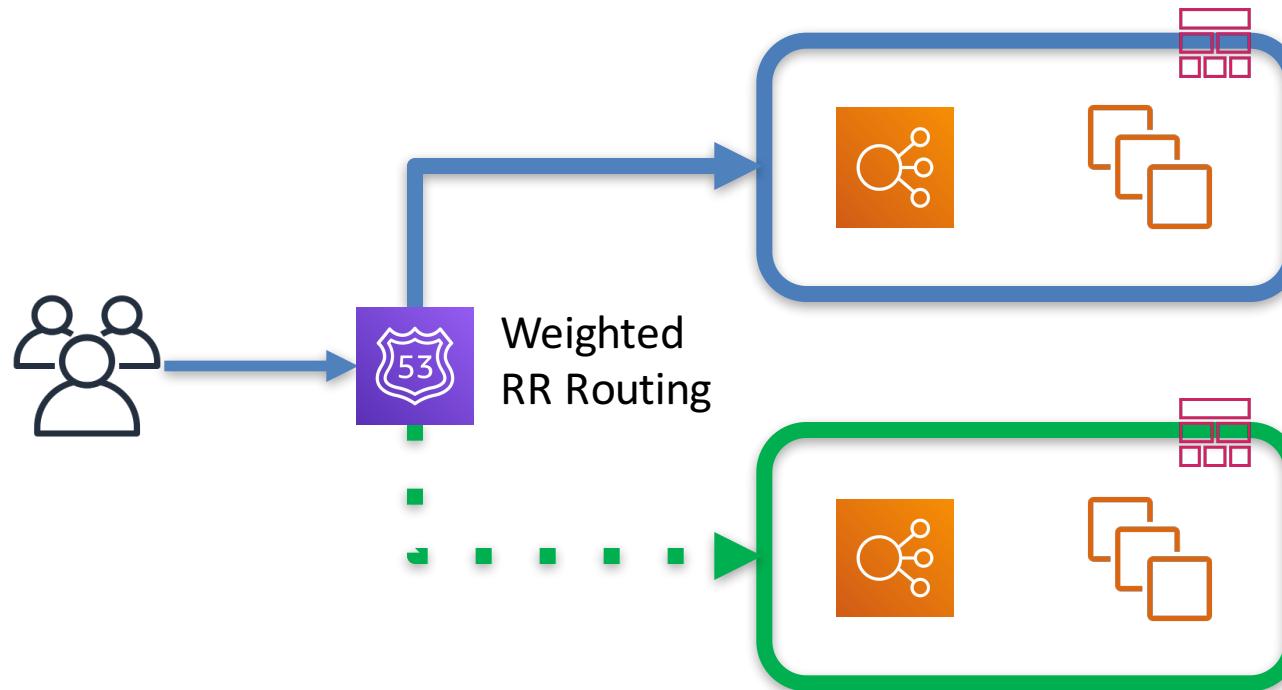
- Deploy to EC2, Lambda, or on-premises
- File and command-based framework
- Rolling updates
- Blue/green deployments
- Stop and rollback
- Does NOT provision network or compute infrastructure

Blue-Green Deployment



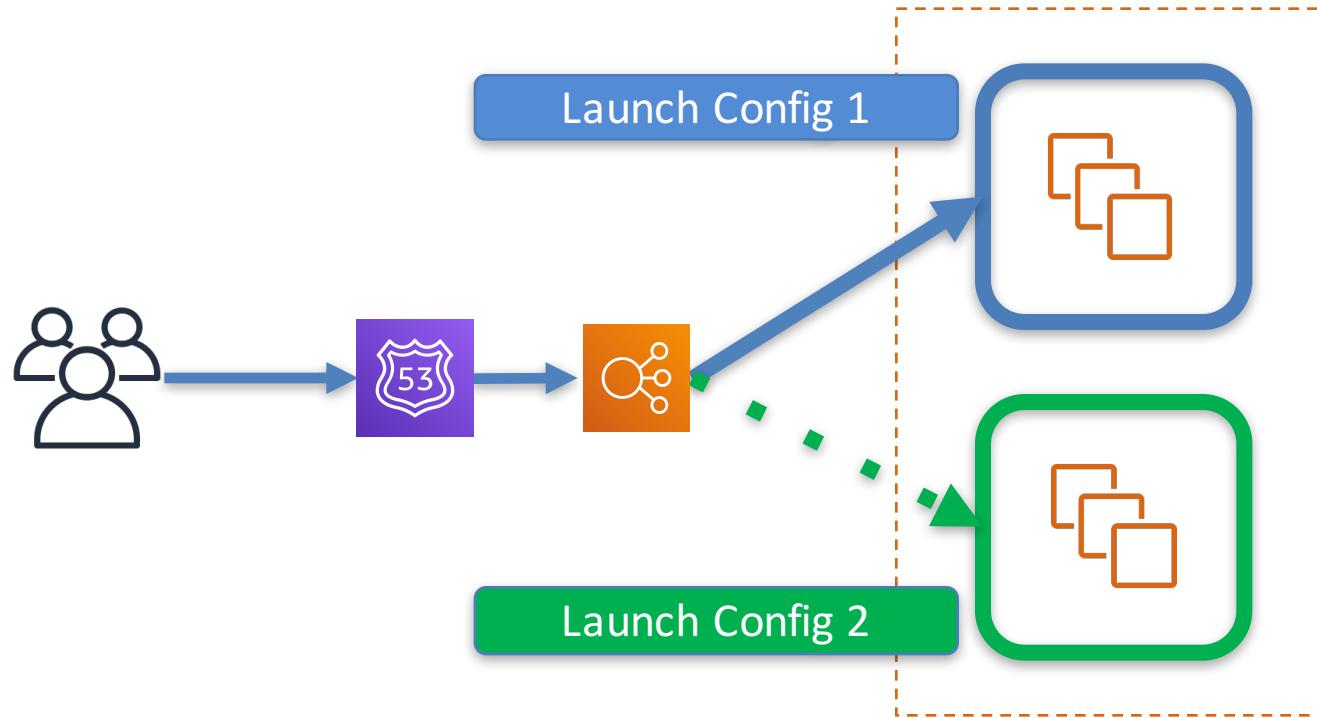
Elastic Beanstalk

Blue-Green Deployment



CloudFormation

Blue-Green Deployment



Auto Scaling

Blue-Green Deployment

How many other possibilities?

- ECS
- OpsWorks
- CodeDeploy
- Multiple options for Elastic Beanstalk
- Multiple options for CloudFormation
- Multiple options for Autoscaling
- And others!

Question Breakdown

Your R&D team wants to deploy a new application using Docker containers. Which services can be used to deploy and manage the containers? (pick three)

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk

Breakdown – Key Terms

Your R&D team wants to deploy a new application using **Docker** containers. Which **services** can be used to **deploy and manage the containers**? (pick three)

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk

Breakdown – Answer Selection

Your Response: EC2 is the Swiss army knife of AWS, and supports containers

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk

Breakdown – Answer Selection

Your Response
contains the correct answer.
Lambda is entirely serverless, with no control over infrastructure

- A. EC2
- B. AWS Lambda**
- C. Elastic MapReduce
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk

Breakdown – Answer Selection

Your RS contains
the co

EMR is a managed Hadoop
framework, not Docker

- A. EC2
- B. AWS Lambda
- C. **Elastic MapReduce**
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk

Breakdown – Answer Selection

Your Runnings Docker
contains manage
the containers of ECS

Containers are the primary function of ECS

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service**
- E. AWS Systems Manager
- F. Elastic Beanstalk

Breakdown – Answer Selection

Your RDS instance contains the command to run Docker

SSM is for inventory, patches, parameters, and updates

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service
- E. **AWS Systems Manager**
- F. Elastic Beanstalk

Breakdown – Answer Selection

Your Response
contains the correct answer.
Elastic Beanstalk supports Docker as a choice for deployment

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk**

Breakdown – Answer Selection

Your RDS instance contains the code

Answers: ADF

- A. EC2
- B. AWS Lambda
- C. Elastic MapReduce
- D. Elastic Container Service
- E. AWS Systems Manager
- F. Elastic Beanstalk



AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 4 – Storage and Data Management

Data Management

- 12% of exam content
- Create and **manage data retention**
- Identify and **implement data protection, encryption, and capacity planning** needs

TL; DR

- Learn differences between automated and manual backups
- Learn how to copy backups between regions
- Understand impact of encryption on backups
- Identify which backups impact availability
- Know which services enforce compliance
- Learn the four DR scenarios
- Recognize limits of storage services for capacity planning purposes

Backups – EC2

- EBS snapshots
 - Increase durability
 - Option to share across accounts
 - Option to copy to different region
 - May require volume quiesce (service interruption)
- Ephemeral volumes
 - No native backup functionality
 - Can do file level sync to S3 or EBS

Backups - RDS

- No interruption of service
- Daily snapshot
 - Can only restore
 - Deleted if DB instance terminated
- Manual snapshot
 - Share across accounts
 - Copy to different region
 - Retained after DB instance termination

Backups - Redshift

- No interruption of service
- Automated snapshot
 - Taken after 8 hours or 5Gb/node data change
 - Can be automatically copied to different region
- Manual snapshot
 - Can be automatically copied to different region
 - Can be shared across accounts
 - Retained after cluster termination

Backups – DynamoDB

- No interruption of service
- Point-in-time recovery (PITR)
 - 35 day retention
- On-demand backup
 - Automatically encrypted

Backups – S3

- Bucket versioning
 - Increases cost
 - Lifecycle policies for versions
- Cross-region replication
 - Even across accounts
- CLI-based copy or sync

Backups – Onsite VMs

- VM Import/Export
- AWS Connector for vCenter (VMware)
- Mileage may vary
- Launching from AMI and bootstrapping may be cleaner

Backups – Storage Gateway

- File gateway
 - S3 buckets available as NFS mounts
 - Run on-premises or in EC2
 - No need for explicit backups
- Volume gateway
 - Cached mode – data written to S3, cached locally
 - No need for explicit backups
 - Stored mode – async backup to S3
 - May need file level backups
- Tape gateway
 - Backed up automatically to S3

AWS Backup

- EFS
- Storage Gateway
- DynamoDB
- RDS
- EBS

Manage Backups

- CLI
- SSM Run Command
- Lambda functions
- Data Pipeline
- 3rd party backup software

DR Processes

Learn the 4 DR scenarios

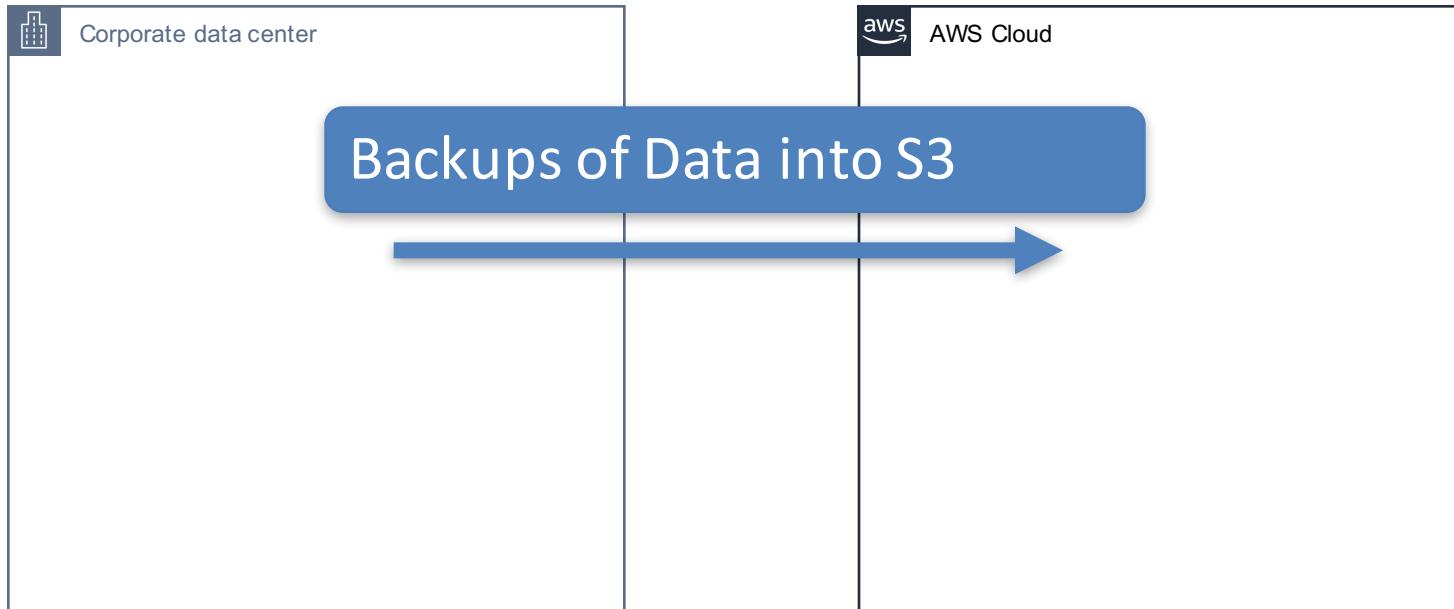
- Backup and restore
- Pilot light
- Warm standby
- Multi-site solution

<https://d1.awsstatic.com/whitepapers/aws-disaster-recovery.pdf>

pages 9-18

DR Scenarios - Highlights

Backup and restore - preparation



DR Scenarios - Highlights

Backup and restore - preparation



Corporate data center



AWS Cloud

Create AMIs
and network
infrastructure

DR Scenarios - Highlights

Backup and restore - execution



Corporate data center



AWS Cloud

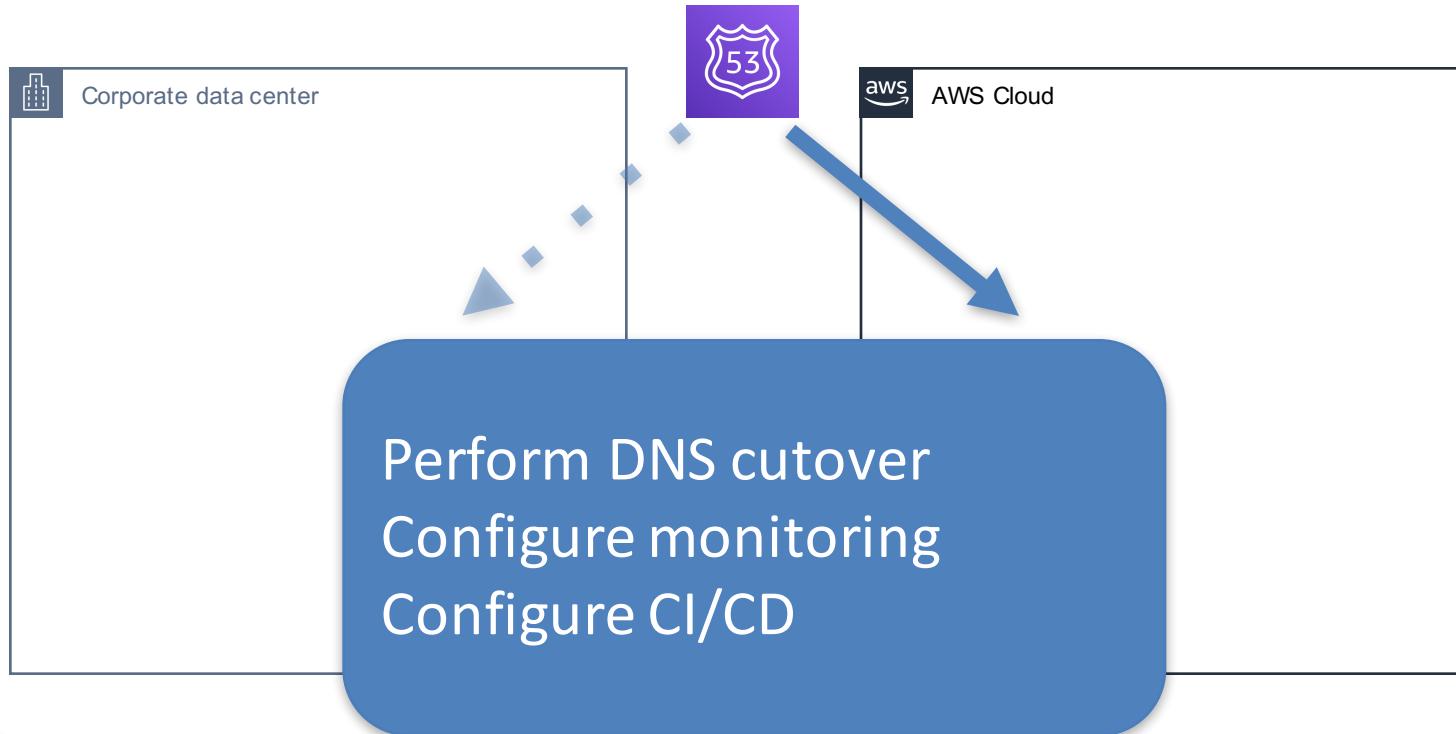
Create ELB
Launch EC2/RDS
Restore data



Pearson

DR Scenarios - Highlights

Backup and restore - execution



DR Scenarios - Highlights

Backup and restore strategic summary

Consideration	Score
RTO	4
RPO	4
Cost	1
Time to implement	1
Complexity to manage	1

1 is best, 4 is worst

DR Scenarios - Highlights

Pilot light - preparation



Corporate data center

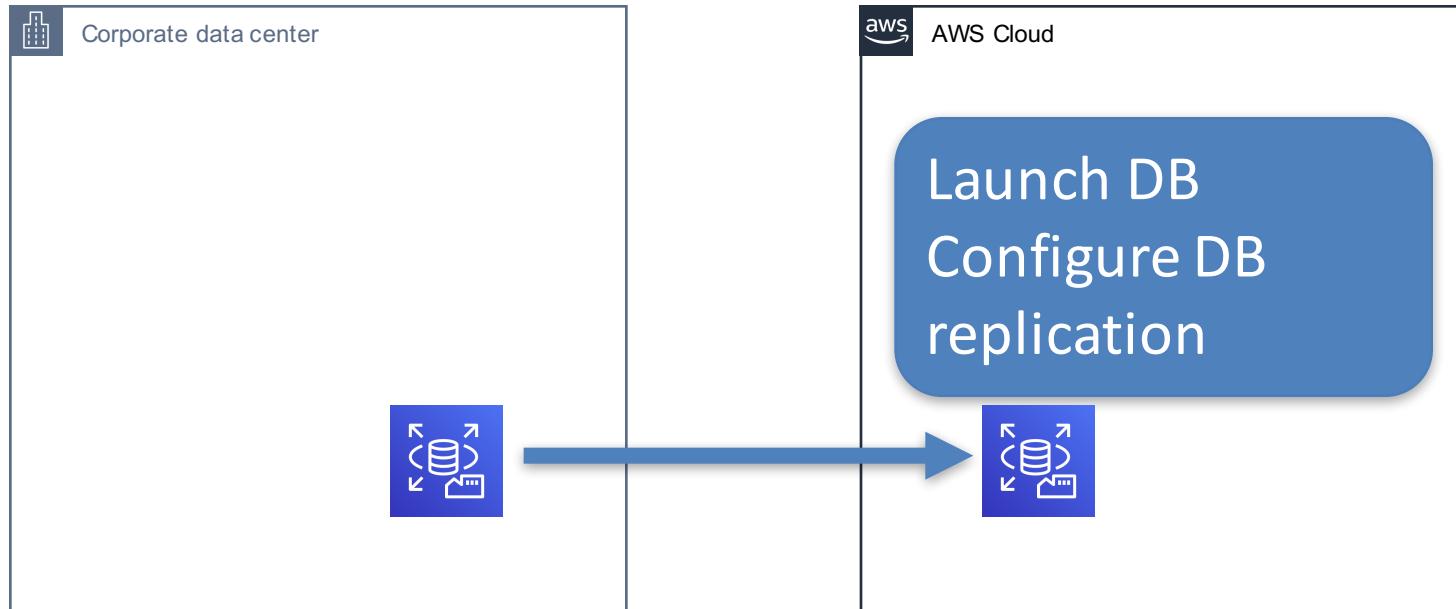


AWS Cloud

Create AMIs
and network
Infrastructure
Create ELB

DR Scenarios - Highlights

Pilot light - preparation



DR Scenarios - Highlights

Pilot light - execution



Corporate data center

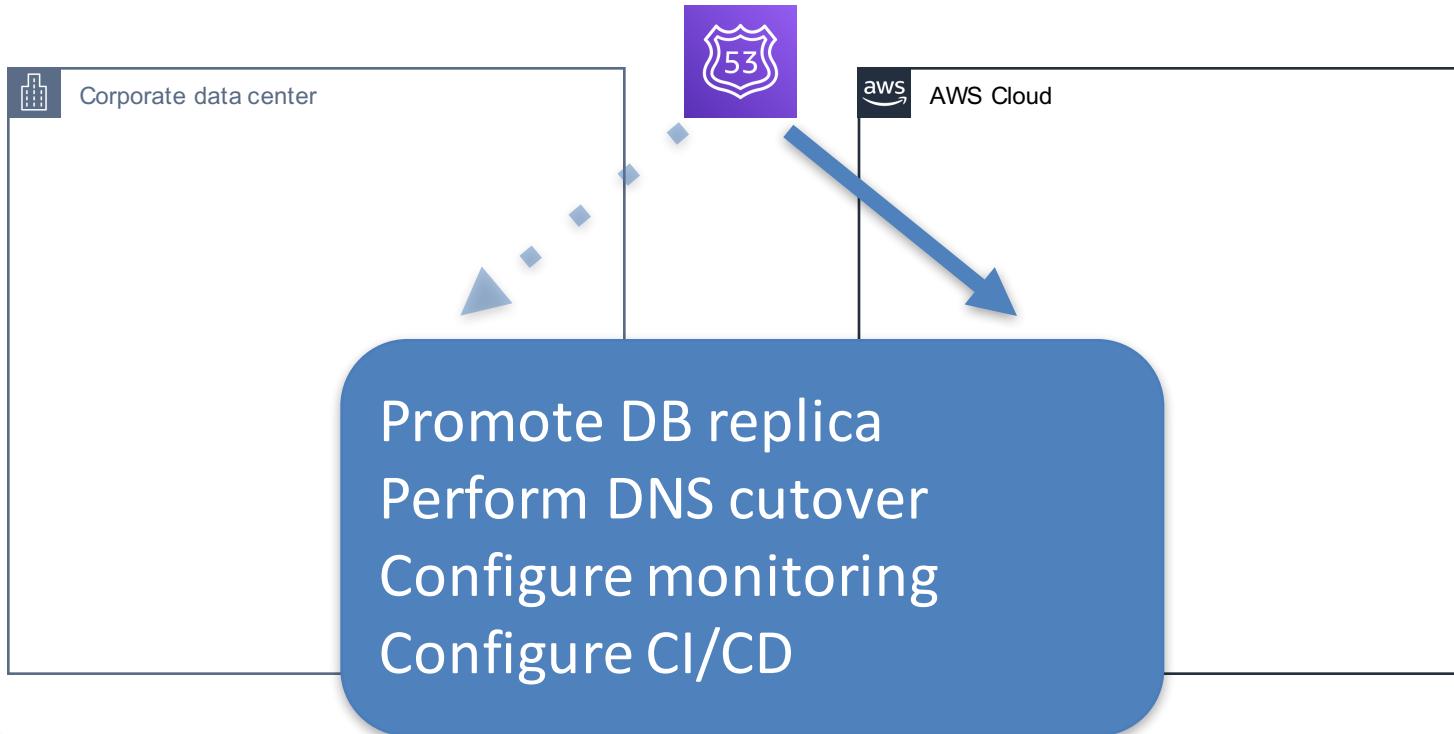


AWS Cloud

Provision EC2
Scale DB

DR Scenarios - Highlights

Pilot light - execution



DR Scenarios - Highlights

Pilot light strategic summary

Consideration	Score
RTO	3
RPO	3
Cost	2
Time to implement	2
Complexity to manage	2

1 is best, 4 is worst

DR Scenarios - Highlights

Warm standby - preparation



Corporate data center

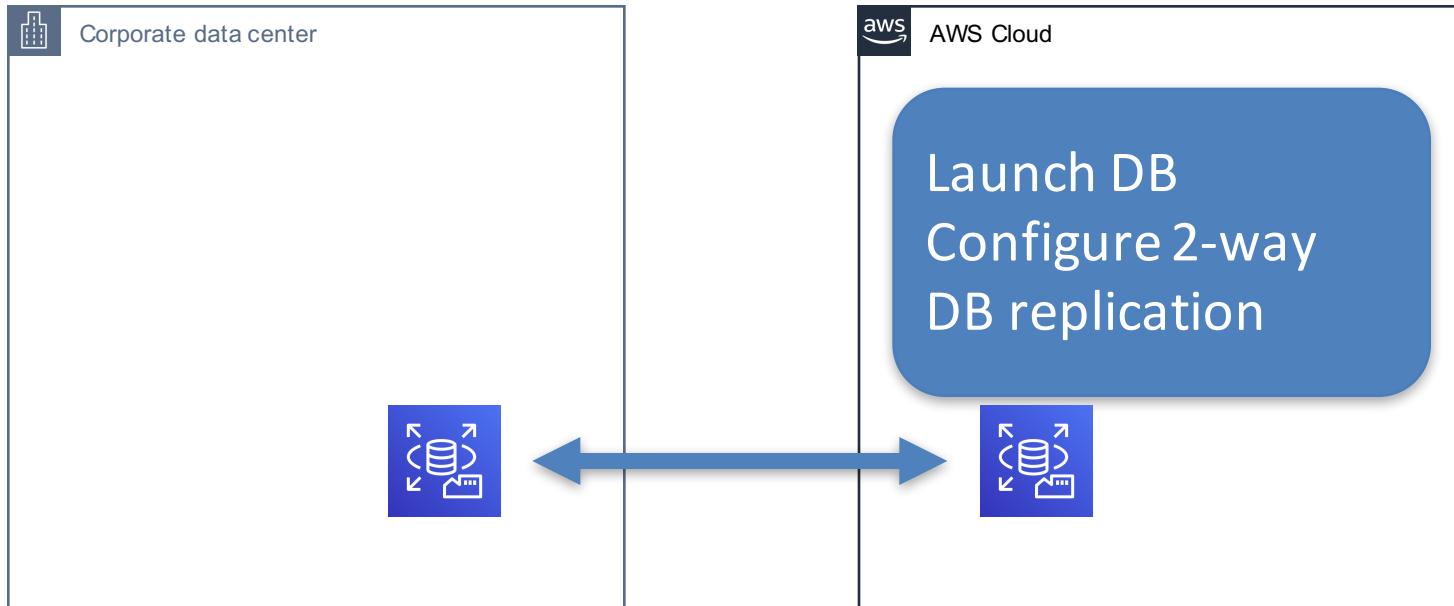


AWS Cloud

Create AMIs
and network
Infrastructure
Create ELB

DR Scenarios - Highlights

Warm standby - preparation



DR Scenarios - Highlights

Warm standby - preparation



Corporate data center

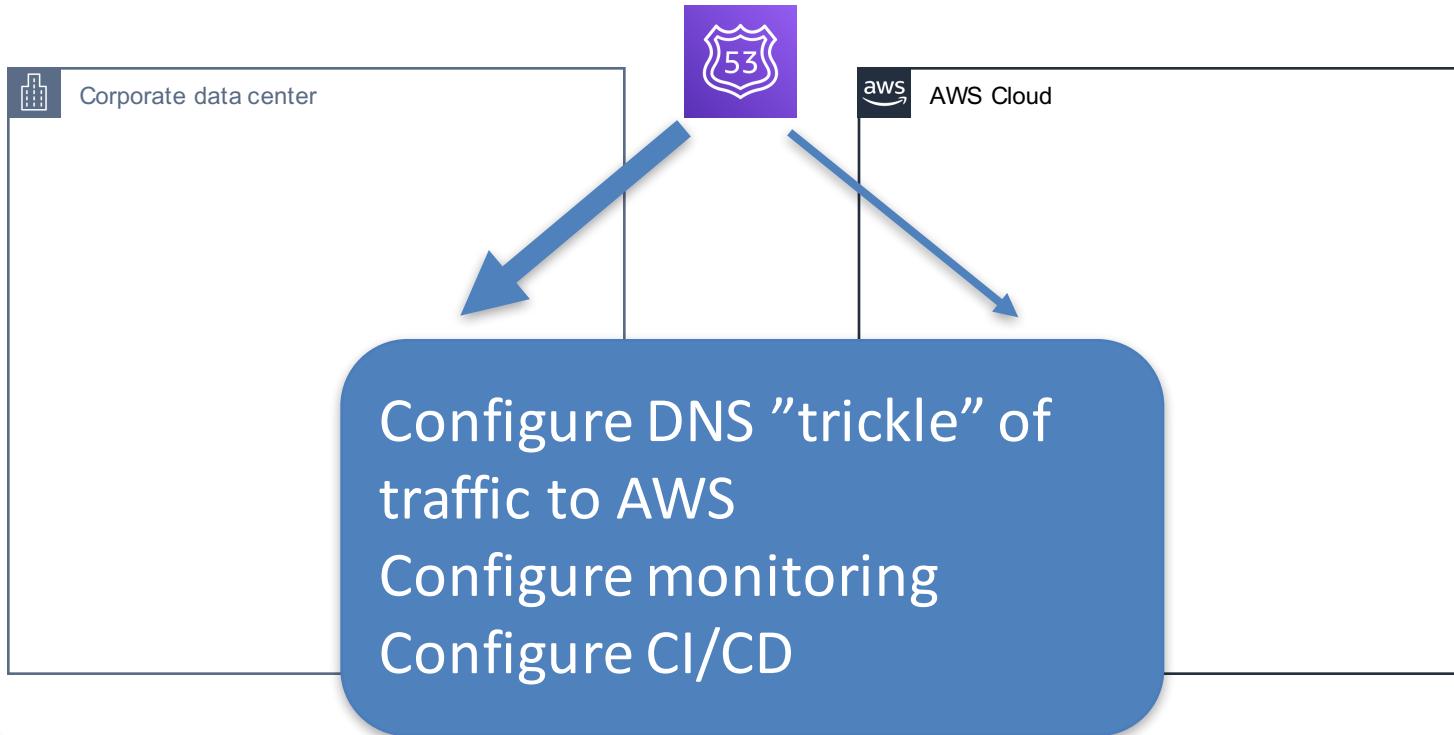


AWS Cloud

Provision EC2

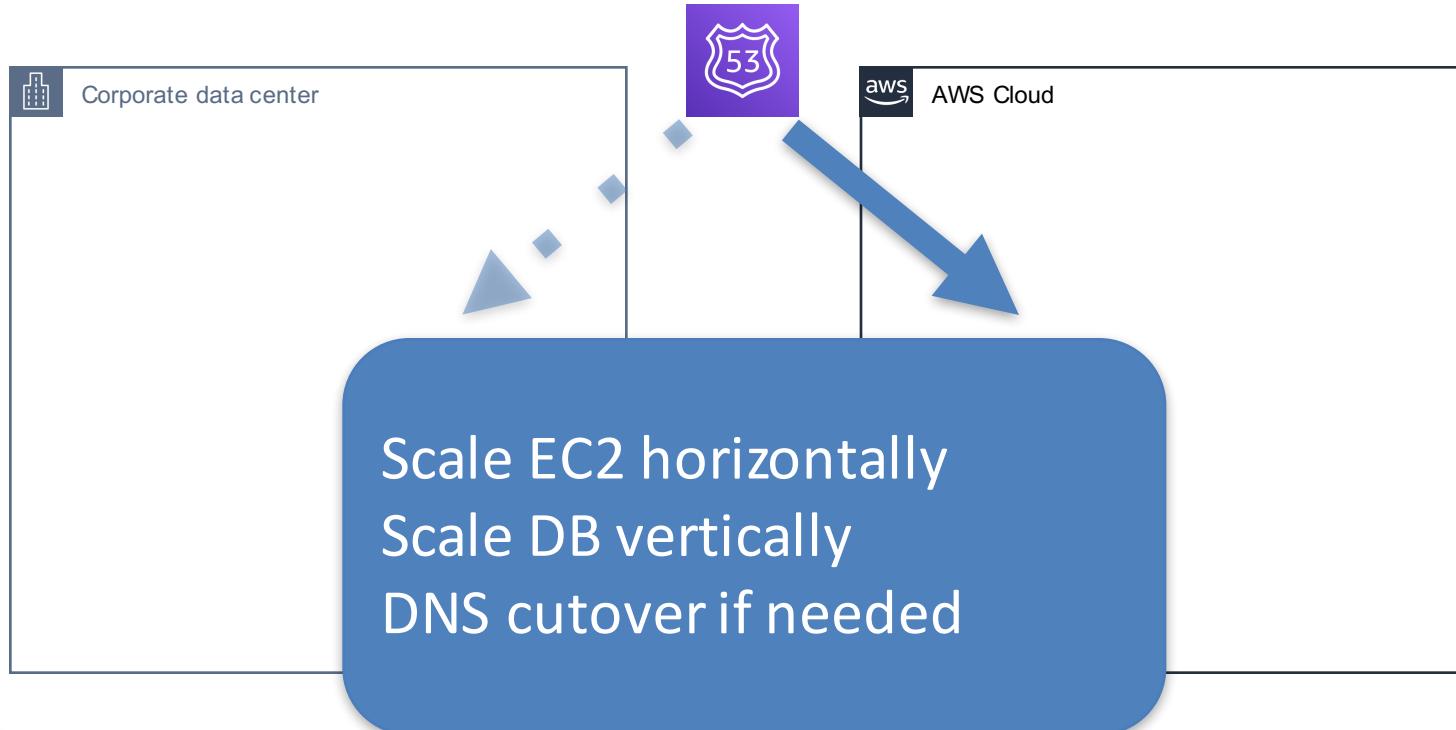
DR Scenarios - Highlights

Warm standby - preparation



DR Scenarios - Highlights

Warm standby - execution



DR Scenarios - Highlights

Warm standby strategic summary

Consideration	Score
RTO	2
RPO	2
Cost	3
Time to implement	3
Complexity to manage	3

1 is best, 4 is worst

DR Scenarios - Highlights

Multi site - preparation



Corporate data center

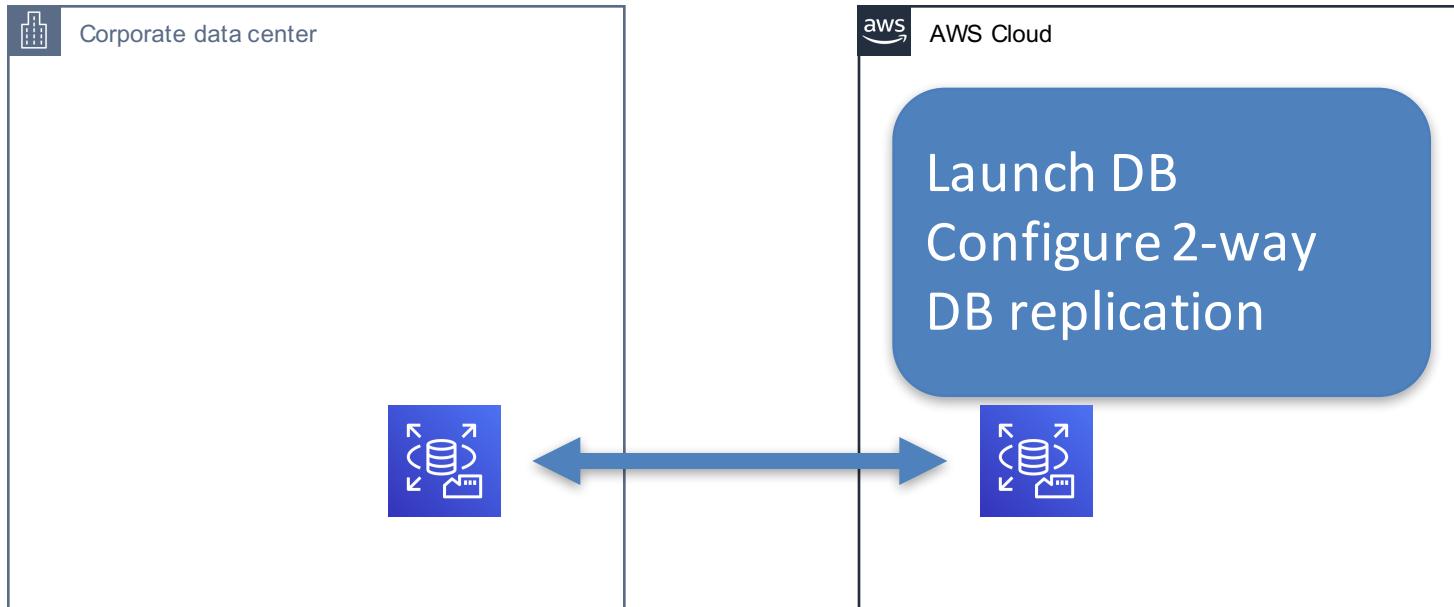


AWS Cloud

Create AMIs
and network
Infrastructure
Create ELB

DR Scenarios - Highlights

Multi site - preparation



DR Scenarios - Highlights

Multi site - preparation



Corporate data center

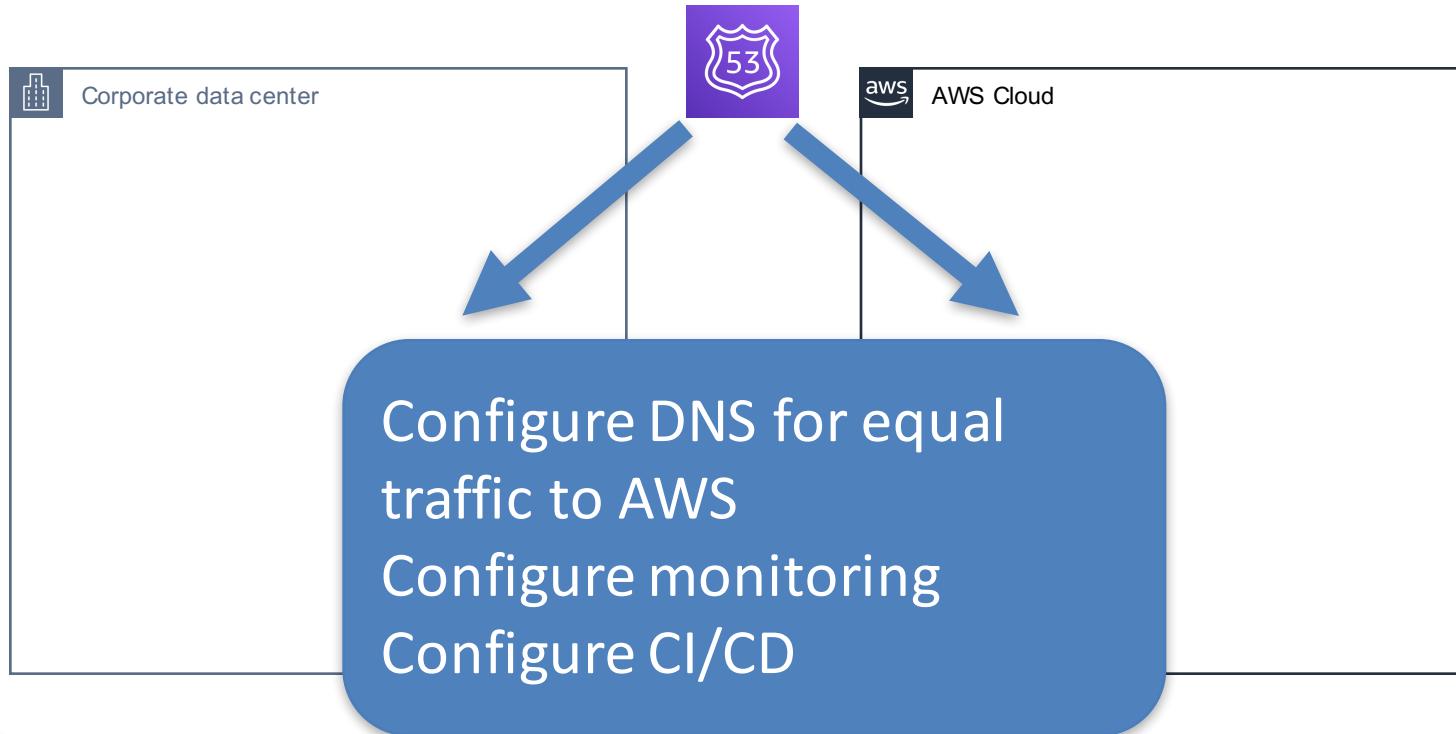


AWS Cloud

Provision EC2

DR Scenarios - Highlights

Multi site - preparation



DR Scenarios - Highlights

Multi site - execution



DR Scenarios - Highlights

Multi site strategic summary

Consideration	Score
RTO	1
RPO	1
Cost	4
Time to implement	4
Complexity to manage	4

1 is best, 4 is worst

Enforcing Compliance

Config Rules

- Passive
- Configuration change or periodic triggers
- Evaluate changes through AWS Config
- Apply built-in rules or custom (Lambda function)
- View Compliance Dashboard for results

Enforcing Compliance

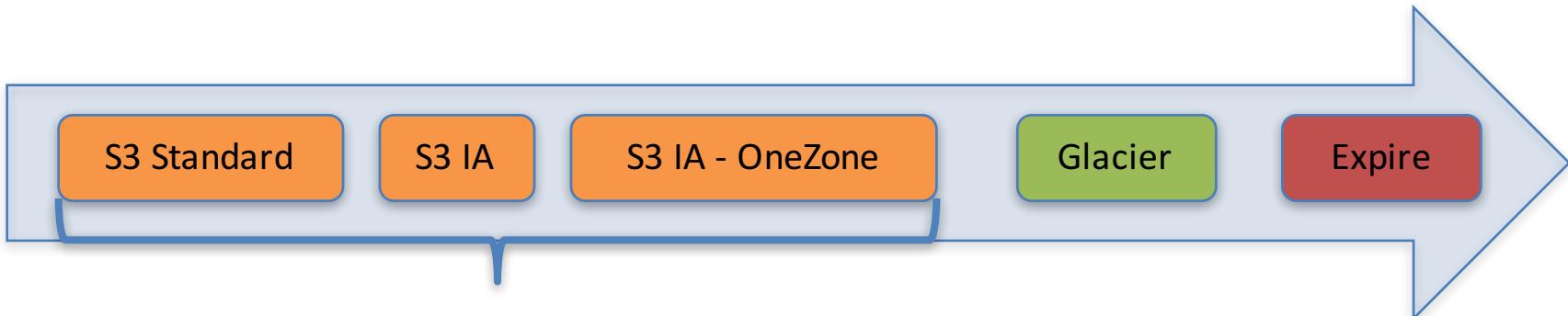
Service Catalog

- Active
- CloudFormation templates as products
- Constraints act upon provisioning
- Users access Service Catalog, not individual services

Enforcing Compliance

S3 Lifecycle Policies

- Active
- Rules apply according to object age
- One-way flow of transition/expiration
- Rules can apply to prefixes or full bucket
- Does not require rule for every storage class



S3

Enforcing Compliance

Glacier Vault Lock

- Active
- Use for delete denial (for example)
- 24 hours to verify lock
- Can never be changed once locked

Data Integrity

Data integrity In-transit

- All AWS API endpoints support SSL
- SSL termination for ELB, CloudFront, API Gateway
- SSL/TLS endpoints for RDS, DynamoDB, RedShift
- VGW/VPN or Direct Connect

Key Terms: SSL, TLS, VPN

Data Integrity

Data integrity at rest strategies

- Access control
- Server-side encryption
 - AWS provided keys
 - KMS or CloudHSM provided keys
 - Customer provided keys
- Client-side encryption

Data Integrity

Data integrity at rest options

- EBS volume encryption
- RDS storage-level encryption
- RDS Transparent Database Encryption (TDE)
 - SQL Server
 - Oracle
- S3 SSE/CSE
- SQS SSE
- DynamoDB SSE (now default)
- RedShift DB Encryption

Data Integrity Operations

Potential operational impact of encryption at rest

- Backups
- Cross region copies
- Cross account sharing
- Performance

Data Integrity Operations

Restrictions on encryption

- Learn resources which must be encrypted at provisioning
- Learn how to remove encryption (not always simple)

Question Breakdown

Your application requires access to images stored in S3. The frequency of access will be no more than 4 times per year, and the image originals have already been placed in Glacier. Which S3 storage class would be the most cost-effective for application access?

- A. S3 Standard
- B. S3 Infrequent Access
- C. S3 One Zone-Infrequent Access
- D. Reduced Redundancy Storage

Breakdown – Key Terms

Your application requires access to images **stored in S3**. The **frequency of access** will be no more than **4 times per year**, and the image **originals** have already been **archived in Glacier**. Which **S3 storage class** would be the most **cost-effective** for application access?

- A. S3 Standard
- B. S3 Infrequent Access
- C. S3 One Zone-Infrequent Access
- D. Reduced Redundancy Storage

Breakdown – Answer Selection

Your application frequently processes image data stored in S3.

Standard is the most expensive S3 storage class

- A. **S3 Standard**
- B. S3 Infrequent Access
- C. S3 One Zone-Infrequent Access
- D. Reduced Redundancy Storage

Breakdown – Answer Selection

Your application has frequent access to image data stored in S3.

S3-IA is a good option, not going to eliminate yet

- A. S3 Standard
- B. S3 Infrequent Access
- C. S3 One Zone-Infrequent Access
- D. Reduced Redundancy Storage

Breakdown – Answer Selection

Your application has infrequent access to a large image collection stored in S3.

Z-IA is a good option also, and is cheaper than S3-IA, eliminating B as a choice

- A. S3 Standard
- B. **S3 Infrequent Access**
- C. **S3 One Zone-Infrequent Access**
- D. Reduced Redundancy Storage

Breakdown – Answer Selection

Your application frequently reads image data from storage.

RRS was a legacy option for cheaper storage but due to price decreases on Standard and S3-IA, no longer relevant

- A. S3 Standard
- B. S3 Infrequent Access
- C. S3 One Zone-Infrequent Access
- D. **Reduced Redundancy Storage**

Breakdown – Answer

Your application frequently processes image data and the storage

All other choices eliminated

Answer: C

- A. S3 Standard
- B. S3 Infrequent Access
- C. S3 One Zone-Infrequent Access
- D. Reduced Redundancy Storage

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button on a media player.

AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 5 – Security and Compliance

Security

- 18% of exam content
- Implement and manage security policies on AWS
- Implement access controls when using AWS
- Differentiate between roles and responsibility within the shared security model

TL; DR

- Protect your data using multiple strategies
- There are both active and passive options
- Shared responsibility model defines strategy for services and features
- Multiple choices for encryption and access control

Anatomy of an IAM Policy

Version	Action
Id	NotAction
Statement	Resource
Sid	NotResource
Effect	Condition
Principal	
NotPrincipal	

IAM Policy Study Focus

Version

Id

Statement

Sid

Effect

Principal

NotPrincipal

Action

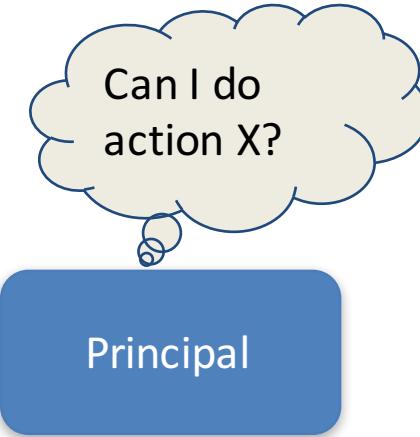
NotAction

Resource

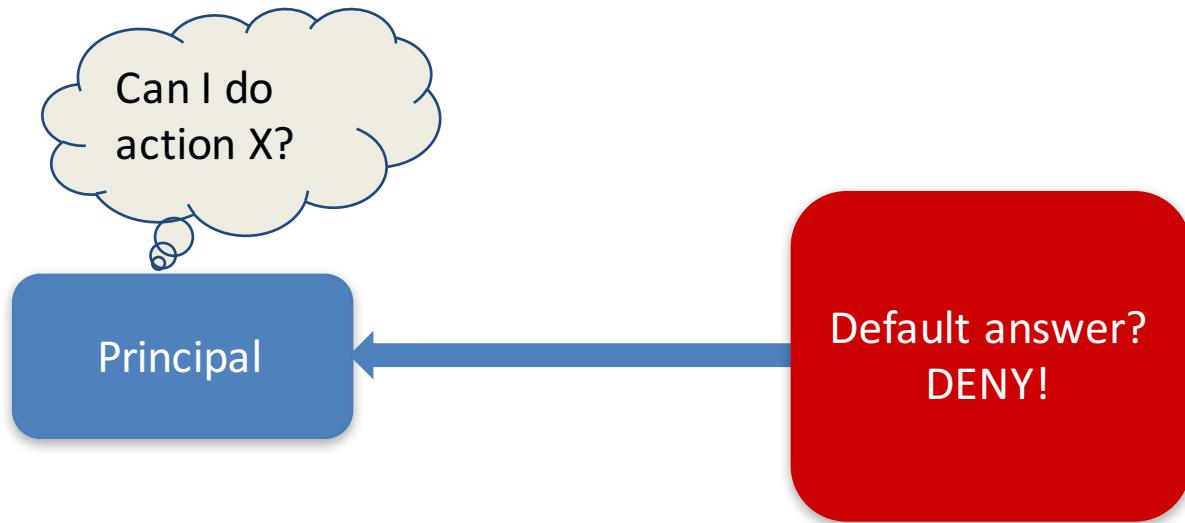
NotResource

Condition

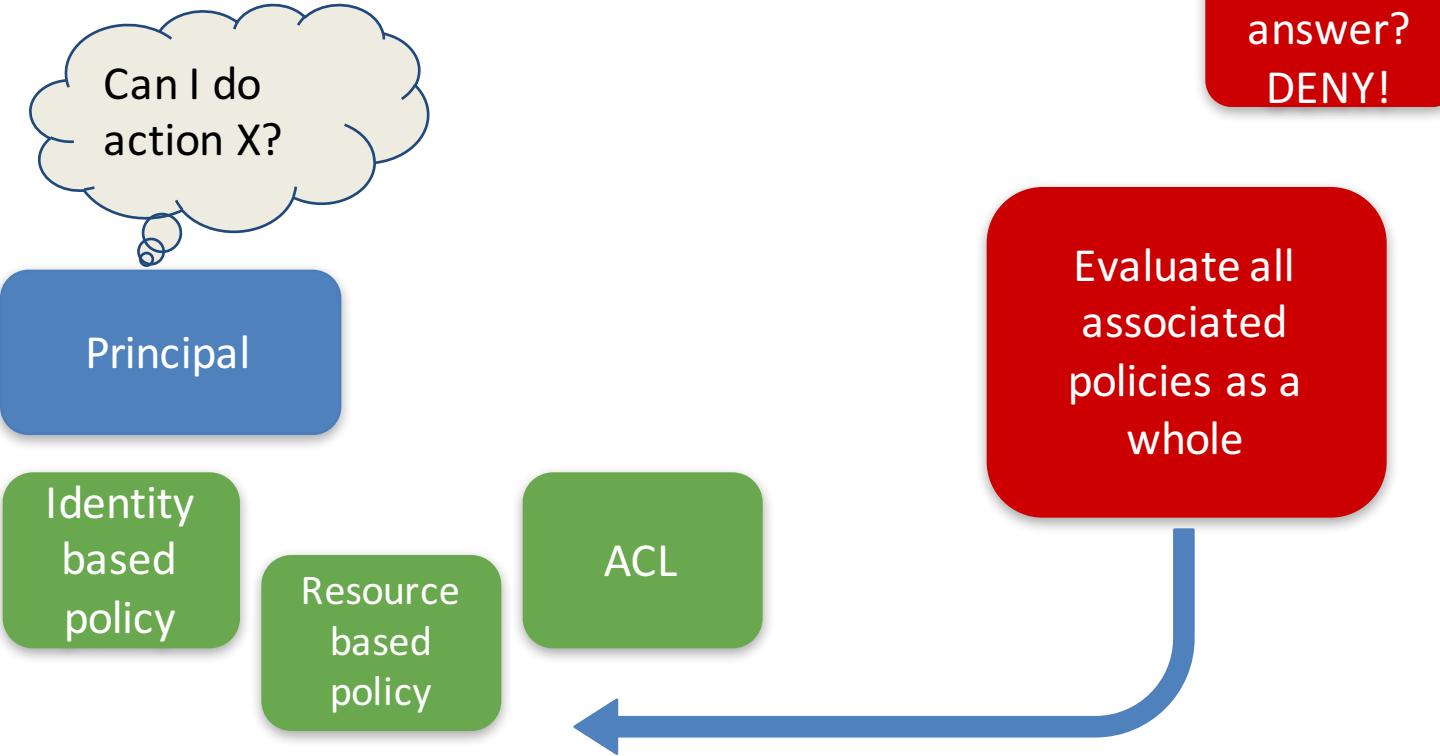
IAM Policy Evaluation



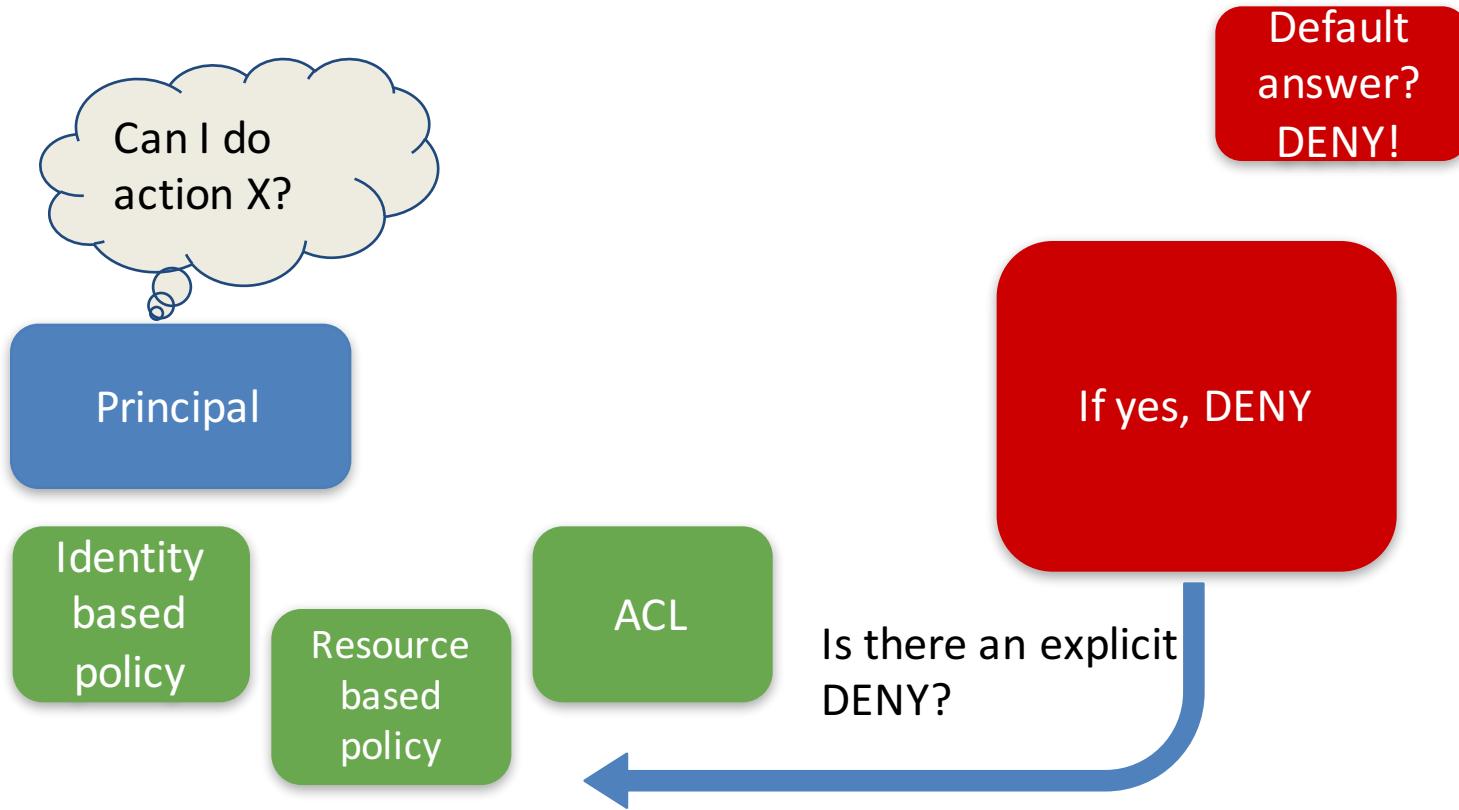
IAM Policy Evaluation



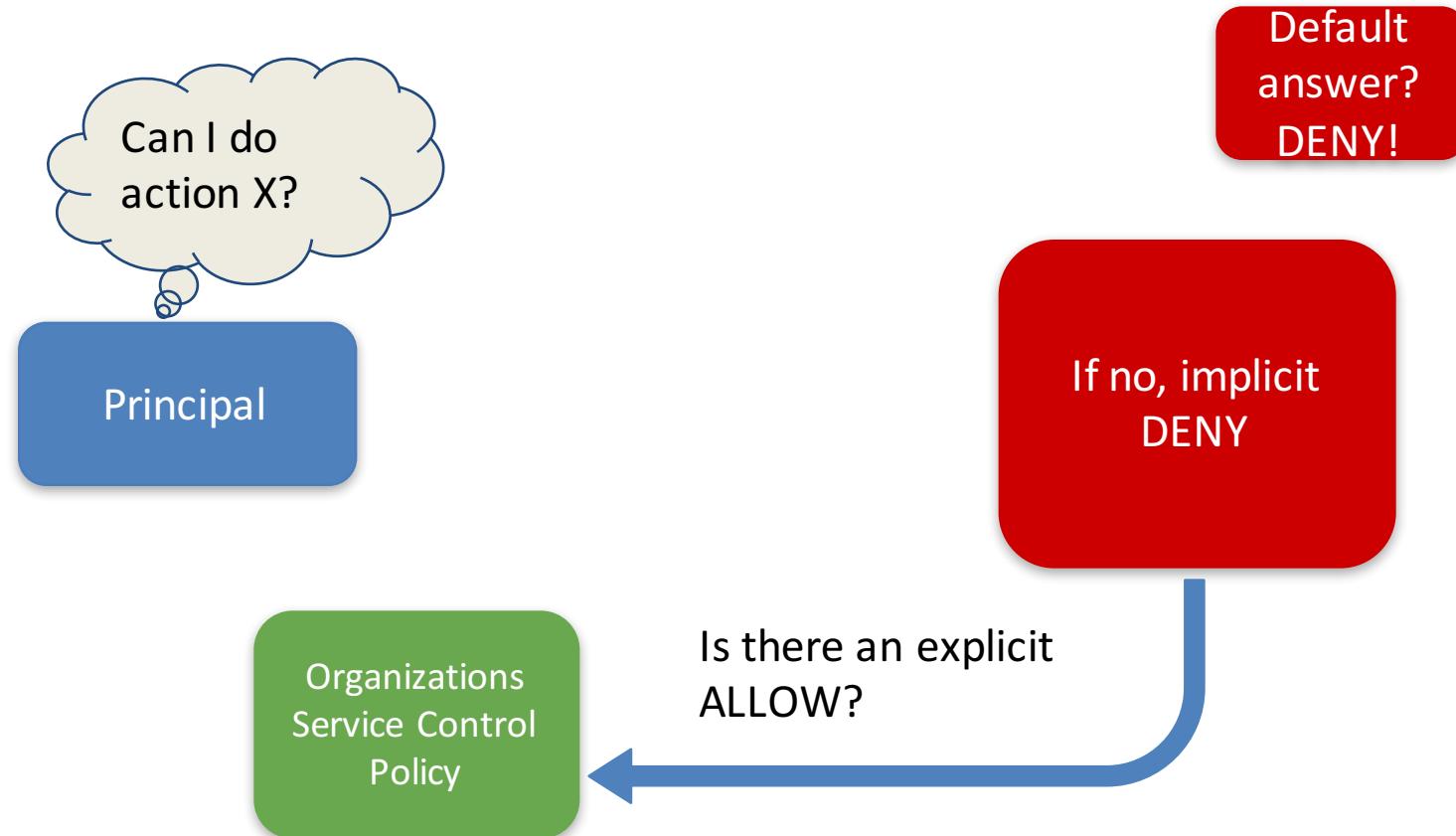
IAM Policy Evaluation



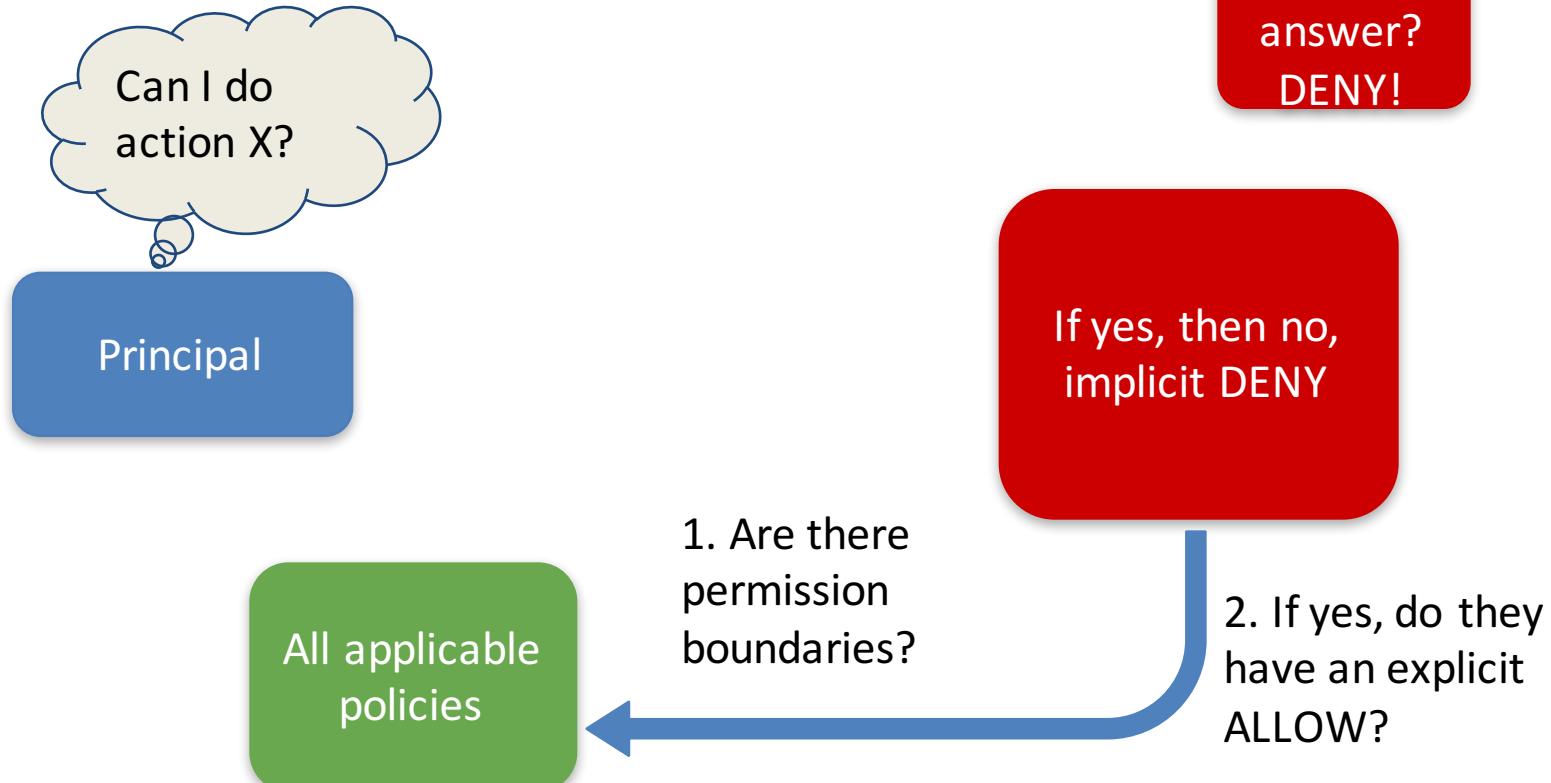
IAM Policy Evaluation



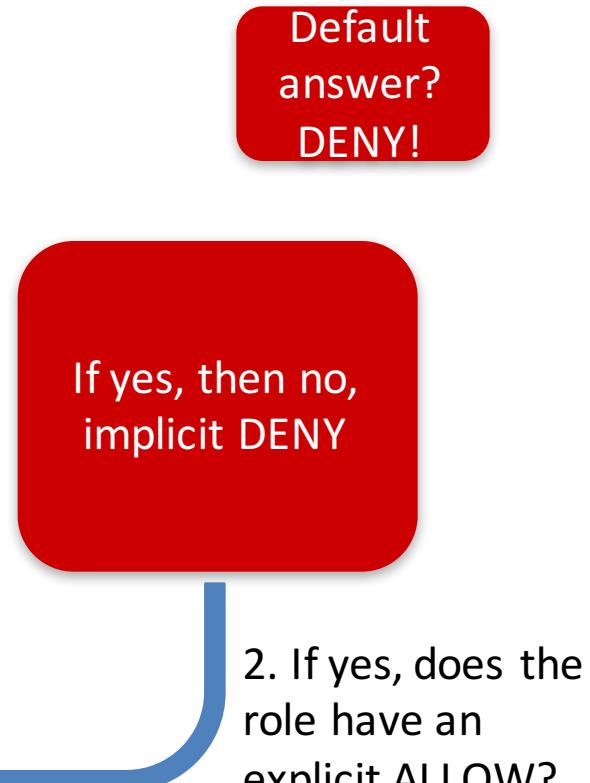
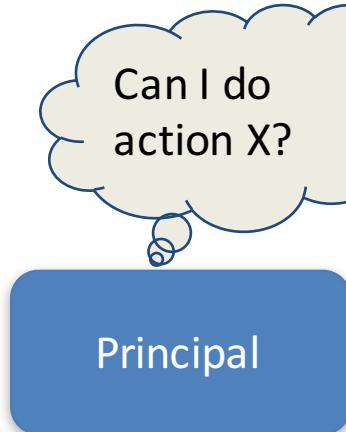
IAM Policy Evaluation



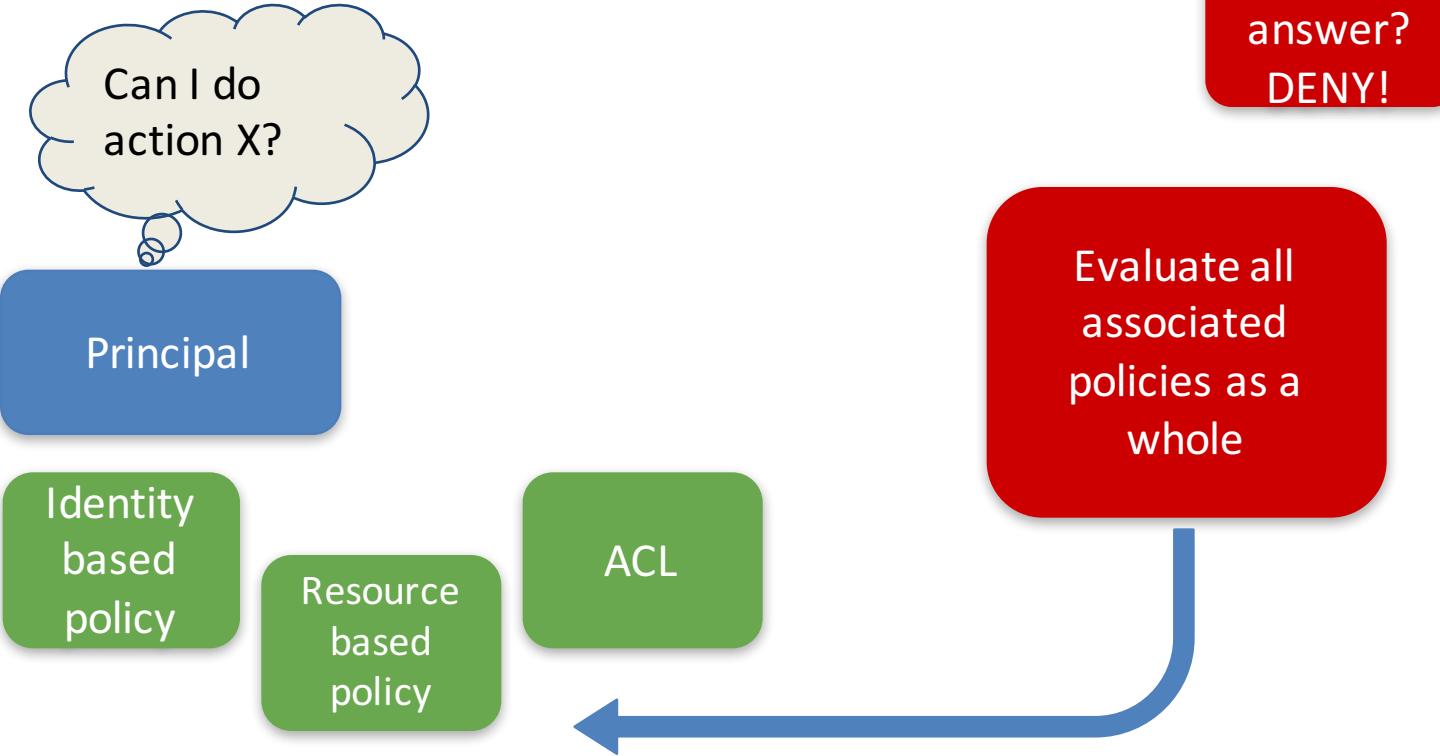
IAM Policy Evaluation



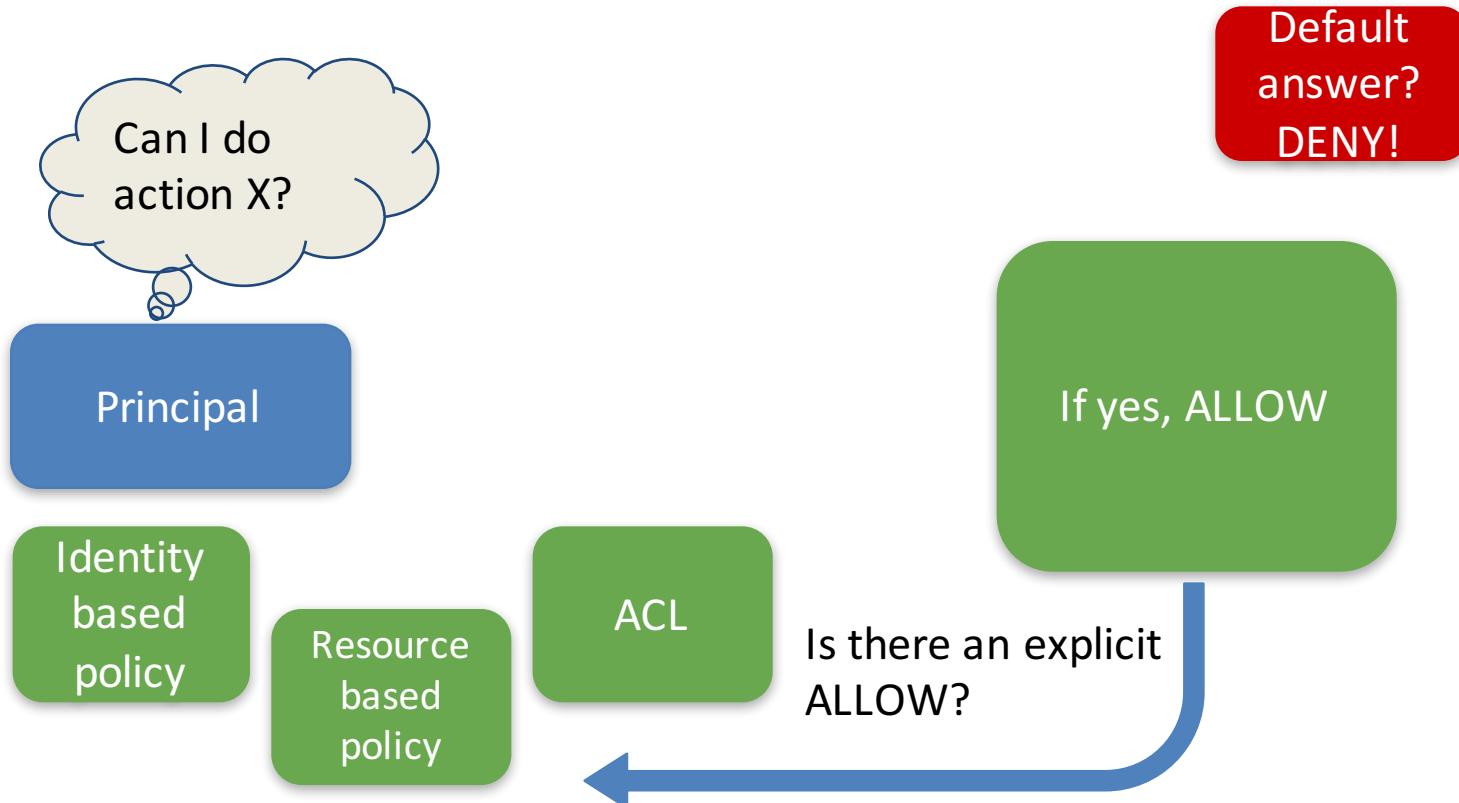
IAM Policy Evaluation



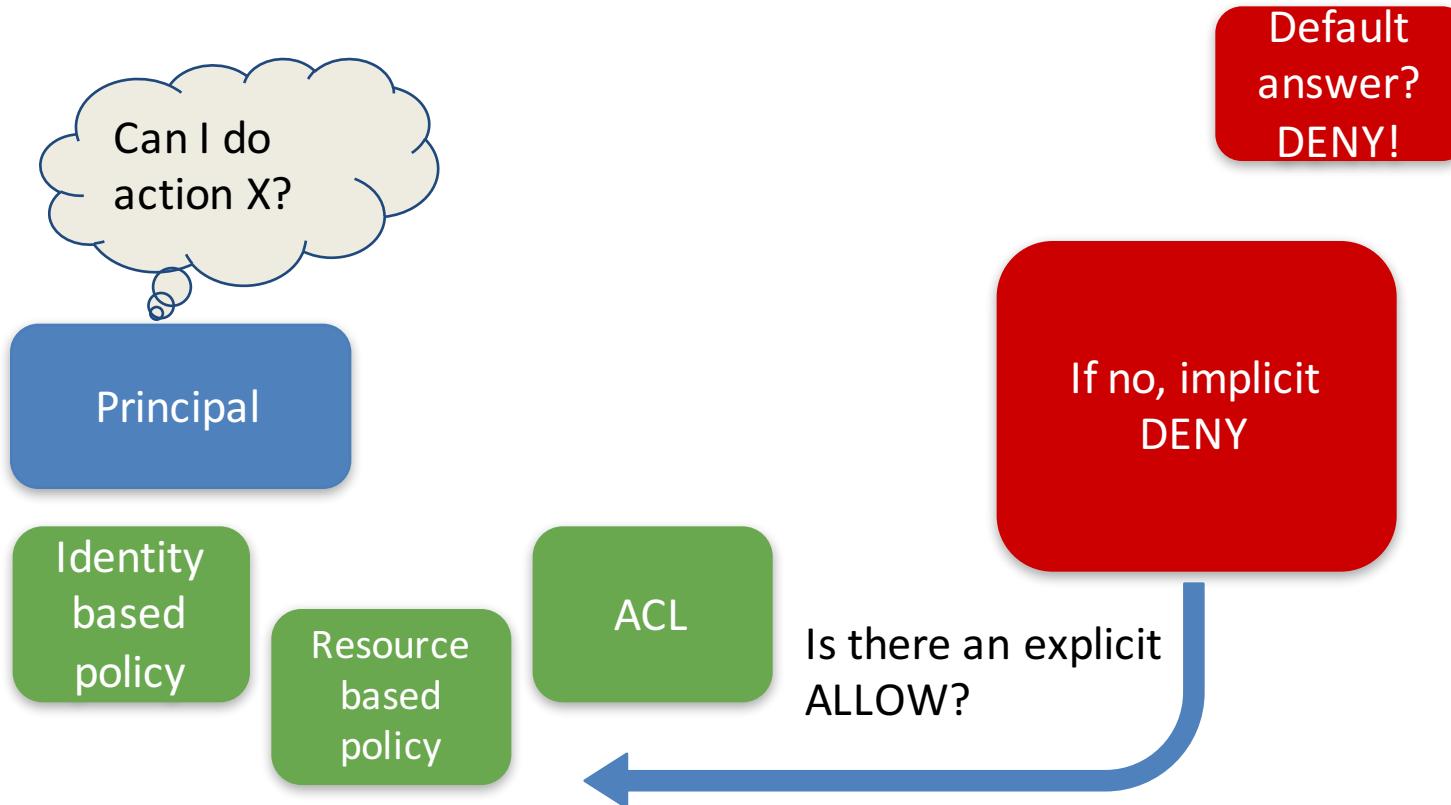
IAM Policy Evaluation



IAM Policy Evaluation



IAM Policy Evaluation



IAM Policy Tips

- Learn where to use “not”
 - NotAction, NotIpAddress, NotResource, etc
- Combine statements
 - Policy length limited to 6144 characters
- Edit policies in console to auto-validate JSON
- Learn all condition types and appropriate use

IAM Policy Example Part 1

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": "s3>ListAllMyBuckets",  
        "Resource": "arn:aws:s3:::*",  
        "Condition": {  
            "StringLike": {  
                "s3:prefix": [  
                    "s3bucketname"]}}}  
    ],  
}
```

Ability to list
the bucket
itself

IAM Policy Example Part 2

```
{  
    "Effect": "Allow",  
    "Action": [  
        "s3>ListBucket",  
        "s3>PutObject",  
        "s3>GetObject",  
        "s3>GetObjectVersion"],  
    "Resource": [  
        "arn:aws:s3::: s3bucketname/*",  
        "arn:aws:s3::: s3bucketname"]},
```

Allow
operations
within the
bucket

IAM Policy Example Part 3

```
{  
    "Effect": "Deny",  
    "NotAction": ["s3:*"],  
    "NotResource": [  
        "arn:aws:s3::: s3bucketname/*",  
        "arn:aws:s3::: s3bucketname"]}]}
```

Deny access to ALL other S3 buckets

Managing IAM Policies

- Creation/validation can be achieved in console
- Test policies with Policy Simulator
- Versioning
 - Not for inline policies
 - Limited to 5 versions per policy document
 - Learn how to roll back
- Edit using new version
- Delete policies with care

Reduce IAM Policy Scope

- Best Practice: Least privilege access
- Familiarize yourself with Access Advisors
 - IAM User
 - IAM Group
 - IAM Role
 - IAM Policy
- Audit usage and create more restrictive policies

Resource Level Permissions

- Applies to several services
 - S3/Glacier
 - SNS
 - SQS
 - KMS
 - etc
- Also uses JSON but applied to resource, not IAM entity

Ensure Access Controls

- Cloudtrail
- Config Rules – covered earlier
- Service Catalog – covered earlier
- Glacier Vault Lock – covered earlier
- Macie
- GuardDuty

CloudTrail

- Enabled by default in all regions
- Audit trail of service API usage
- Enable integration with CloudWatch Logs
- Can consolidate into single S3 bucket from multiple accounts
- CloudTrail logs use SSE by default
- Can enable log file integrity validation
- S3 Bucket and lifecycle policies for log protection

Macie

- Discover, classify and protect sensitive data in S3
- Uses machine learning
- Understands scope of PCI, HIPAA, etc
- Generates alerts which can lead to actions
- Can specify which S3 buckets to protect
- Monitors subset of CloudTrail logs
- Passive service

GuardDuty

- Managed threat detection on your AWS resources
 - Unusual API calls
 - Unusual system deployments
- Can detect compromised EC2 instances
- Can detect brute force attacks
- Can be configured as an active service
 - Disable API keys
- Tip: Integrate with CW Events!

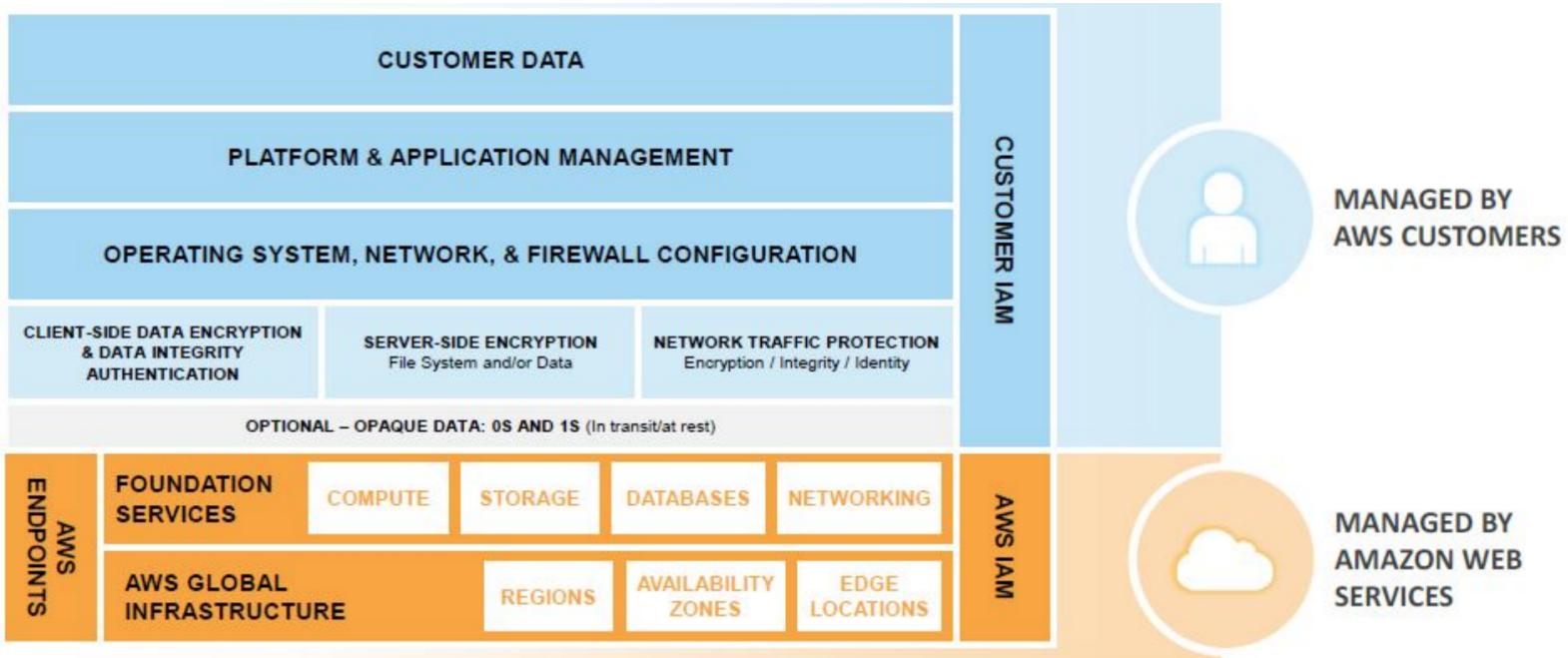
Shared Responsibility Model

<https://aws.amazon.com/compliance/shared-responsibility-model/>

- Nothing new, vendors have used this for years
- Fundamental concept for working with AWS
- Responsibility split between AWS and customer

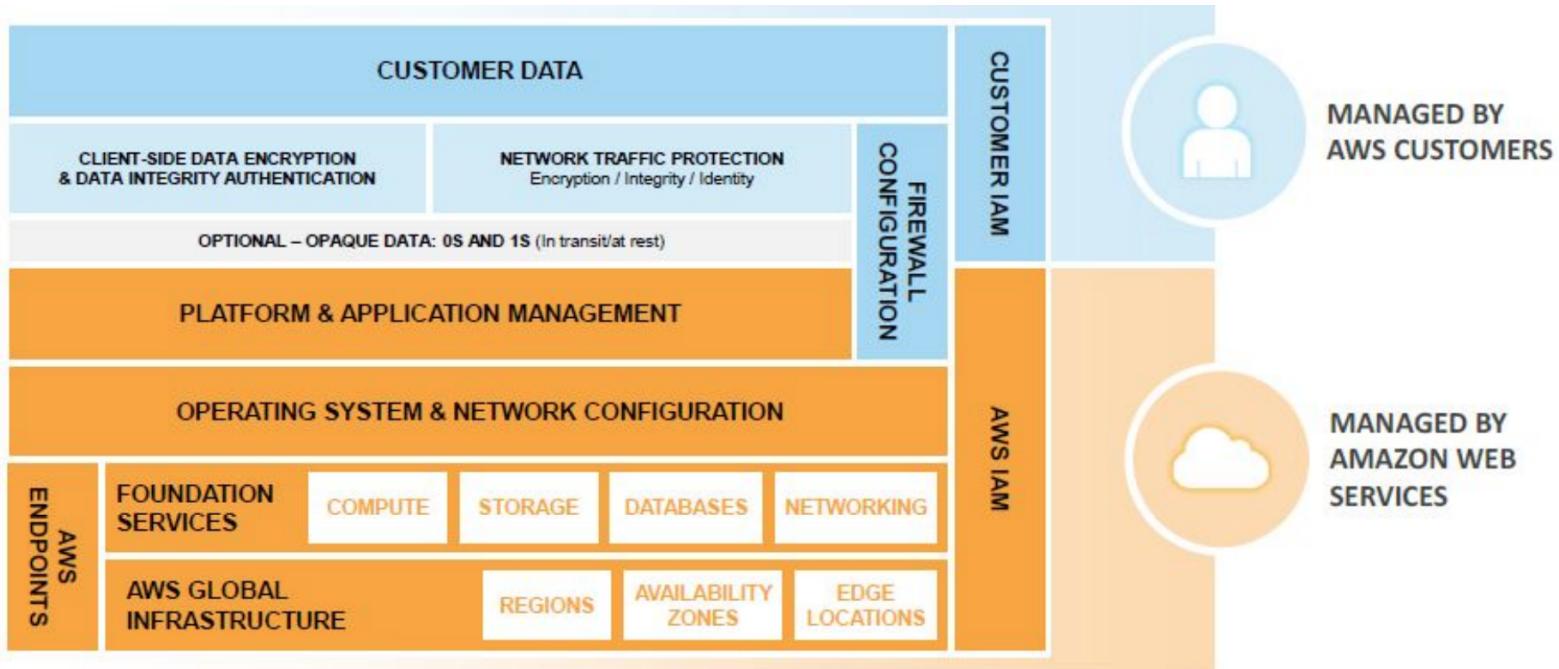
Shared Responsibility Model

Infrastructure services



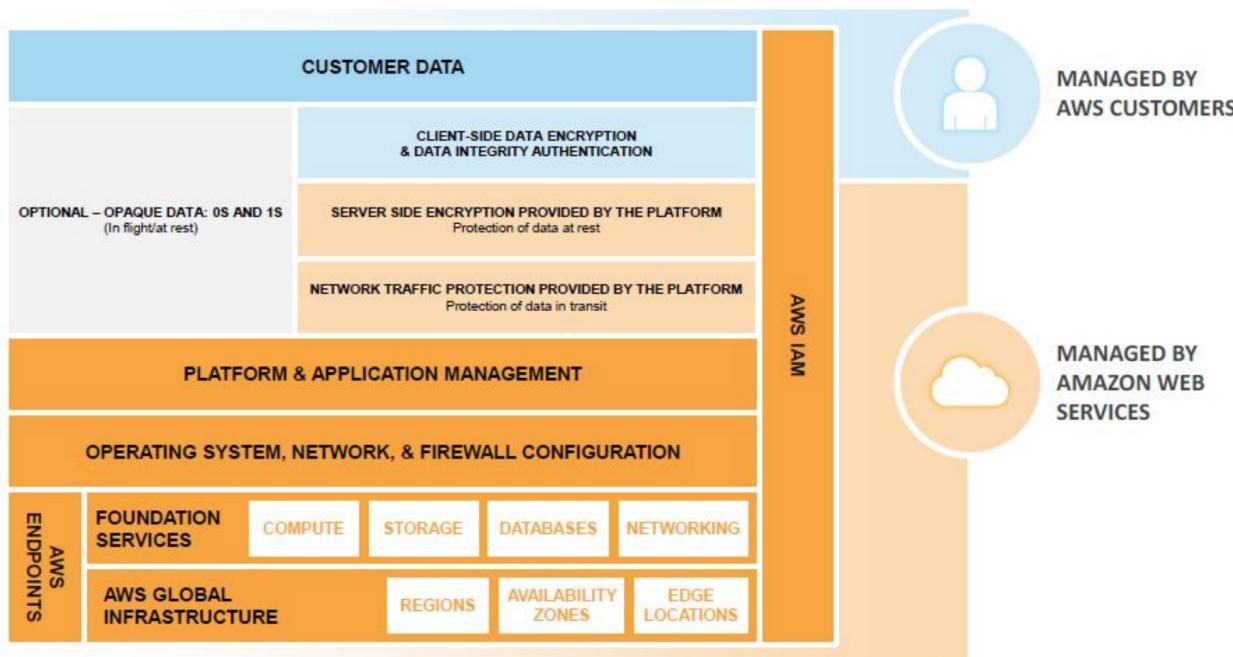
Shared Responsibility Model

Container services



Shared Responsibility Model

Abstract services



Security Assessment

- Inspector – EC2 OS security audit service
- Macie – S3 and CloudTrail
- Guard Duty – CloudTrail, VPC Flow Logs and EC2
- CloudTrail log analysis – very flexible
- Security Hub - NEW!!!

Penetration Testing

<https://aws.amazon.com/security/penetration-testing/>

- Limited scope allowed
- Read the list of prohibited activities
- No permission required

Question Breakdown

AWS CloudTrail logs API requests to resources in your account. Which additional service can you use to track and visualize changes made on those resources?

- A. AWS Config
- B. KMS
- C. Amazon Inspector
- D. AWS CloudFormation

Breakdown – Key Terms

AWS CloudTrail logs API requests to resources in your account. Which **additional service** can you use to **track and visualize changes** made on those **resources**?

- A. AWS Config
- B. KMS
- C. Amazon Inspector
- D. AWS CloudFormation

Breakdown – Answer Selection

AWS CloudFormation
Which of the following services can be used to track changes in AWS resources?

Config allows for resource change tracking and visualization

- A. AWS Config
- B. KMS
- C. Amazon Inspector
- D. AWS CloudFormation

Breakdown – Answer Selection

AWS CloudWatch Metrics can be used to monitor the count of errors in a stream. Which AWS service is responsible for managing the encryption keys used to encrypt data at rest? **KMS manages encryption keys**

- A. AWS Config
- B. **KMS**
- C. Amazon Inspector
- D. AWS CloudFormation

Breakdown – Answer Selection

AWS Ch

Which
change

**Inspector is used for OS
security audit tasks**

count.

lize

- A. AWS Config
- B. KMS
- C. **Amazon Inspector**
- D. AWS CloudFormation

Breakdown – Answer Selection

AWS CloudFormation
Which of the following services is designed for automated deployment of changes to AWS resources?

CloudFormation is designed for automated deployment of resources

- A. AWS Config
- B. KMS
- C. Amazon Inspector
- D. **AWS CloudFormation**

Breakdown – Answer

AWS CloudWatch Metrics can be used to monitor the count of errors in a log stream. Which AWS service can be used to automatically analyze log files for changes in error count?

Answer: A

- A. AWS Config
- B. KMS
- C. Amazon Inspector
- D. AWS CloudFormation

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button on a media player.

AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 6 - Networking

Networking

- 14% of exam content
- Apply AWS networking features
- Implement connectivity features of AWS
- Gather and interpret relevant information for network troubleshooting

TL; DR

- Ability to create VPC from scratch is a requirement
- Many of your resources could be outside VPC
- VPC security groups for whitelisting, NACLs for blacklisting
- VPC route tables are for traffic egress
- ELB/ALB/NLB each have specific use cases
- Know when VPC Flow Logs are required for troubleshooting
- Recognize common causes of connectivity issues

Implement Networking Features

- Understanding service scope
 - Many services don't allow network choices
- VPC networking
- CloudFront
- Elastic Load Balancing
- Route 53

VPC Networking Limits

Learn the default limits and which can be increased when required

- Subnets
- EIPs
- Flow Logs
- Gateways
- NACLs
- ENIs
- Route Tables
- Security Groups
- VPC Peering Connections
- VPC Endpoints
- VPN Connections

VPC External Egress/Ingress

Learn the operations and prerequisites for each



Internet
gateway



VPN
Gateway



Endpoints



Peering

VPC IP Address Space

- Private IP ranges
 - All networking features available
 - RFC1918 compliance
 - 10.0.0.0-10.0.255.255
 - 172.16.0.0-172.31.255.255
 - 192.168.0.0-192.168.255.255

VPC IP Address Space, con'td

- Supported networks from /16 to /28 in size
 - AWS reserves 5 IP addresses from each subnet
- Bring your own IP range
 - Traffic routed to your VPC through AWS

VPC IPv6

- IPv6 supported
 - Even in the same VPC as IPv4!
- IPv6 separates ingress and egress gateways for Internet
- IP range is /56
 - Fixed size
 - Allocated from AWS block, no option to select

VPC Egress/Ingress Key Concepts

- NACLs operate at subnet boundary
- Security groups operate at EC2 host OS boundary
- Host-based firewalls operate at EC2 guest OS boundary
- In-line gateways and proxy servers can provide Layer 7 customization
- NAT Gateways integrate with route tables
- Route tables cannot allow/deny traffic between VPC subnets

VPC Route Table Operations

172.16.0.0

172.16.1.0

172.16.2.0

- Update route tables when external networks change
- Can be automated (think Lambda functions)
- Consider one route table per subnet to minimize impact of improper change

VPC NACL Operations



- Use NACL for blacklisting (deny traffic)
- Can automate blacklist updates by integrating with VPC Flow Logs and Lambda
- Maintain gaps between rule numbers as they are evaluated in order

VPC Security Group Operations

- Delegate ownership to Devops team
- Use for whitelisting (no deny allowed)
- Consider deleting default outbound rule that allows all traffic
- Replace with least privilege outbound rules
- Monitor changes with AWS Config

Security group

VPC Troubleshooting Operations

- Enable VPC Flow Logs on ENI, Subnet or VPC
- Use host-based tools for testing network connectivity
- Check CloudTrail logs
- Enable AWS Config and view resource configuration

CloudFront Operations



- Modify DNS cname list
 - Update SSL certificate
 - Change allowed edge locations
 - Associate a Web ACL
- Tip: Understand how to make assets private

Elastic Load Balancing Operations



- Manage instances (CLB) or target groups (ALB/NLB)
 - Update SSL settings or certificate
 - Update listeners
- Tip: learn differences between the CLB, ALB, NLB

Implement Connectivity Features

Virtual Private Gateway (VGW)

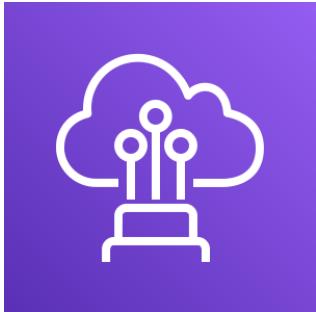


- VPC only
- Supported list of customer gateways
- Encrypts data in transit
- Highly available by default (2 endpoints)

Implement Connectivity Features

Direct Connect

- VPC network connectivity
- **AWS service API endpoint connectivity**
- Cross account features
- Does not encrypt data in transit natively
- Can be integrated with VGW and VPN
- Not highly available by default



Implement Connectivity Features

Resource Access Manager

- Resource sharing between AWS accounts
- Great use case for Organizations

Resources shared

- Route 53 resolver rules
- AWS Transit Gateways
- Subnets
- AWS License Manager Configurations

Question Breakdown

You suspect that one of your EC2 instances is the target of a brute force hacking attempt. Which features could you use to verify this claim? (pick 3)

- A. Check NACL entries
- B. Enable VPC Flow Logs and explore the log output
- C. Check findings in GuardDuty
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Breakdown – Key Terms

You suspect that one of your **EC2** instances is the **target** of a brute force **hacking attempt**. Which features could you use to **verify** this claim? (pick 3)

- A. Check NACL entries
- B. Enable VPC Flow Logs and explore the log output
- C. Check findings in GuardDuty
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Breakdown – Answer Selection

You suspect a
brute force attack
verify traffic of a
NACL entries don't track usage explicitly use to

- A. **Check NACL entries**
- B. Enable VPC Flow Logs and explore the log output
- C. Check findings in GuardDuty
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Breakdown – Answer Selection

You suspect a
brute force attack.
verify that

Flow Log output would indicate traffic from a single source to a specific port

of a
use to

- A. Check NACL entries
- B. **Enable VPC Flow Logs and explore the log output**
- C. Check findings in GuardDuty
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Breakdown – Answer Selection

You suspect a
brute force attack
verify the

**GuardDuty reports on
suspicious EC2 network activity**

of a
use to

- A. Check NACL entries
- B. Enable VPC Flow Logs and explore the log output
- C. **Check findings in GuardDuty**
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Breakdown – Answer Selection

You suspect a
brute force at-
verify t

**Inspector evaluates rules to test OS
for security vulnerabilities, not
hacking attempts**

of a
use to

- A. Check NACL entries
- B. Enable VPC Flow Logs and explore the log output
- C. Check findings in GuardDuty
- D. **Check findings in AWS Inspector**
- E. Explore system logs on the EC2 instance OS

Breakdown – Answer Selection

You suspect a brute force attack. **OS logs could absolutely show proof of a brute force intrusion attempt**

- A. Check NACL entries
- B. Enable VPC Flow Logs and explore the log output
- C. Check findings in GuardDuty
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Breakdown – Answer

You suspect a
brute force attack
verify if

of a
use to

Answers: BCE

- A. Check NACL entries
- B. Enable VPC Flow Logs and explore the log output
- C. Check findings in GuardDuty
- D. Check findings in AWS Inspector
- E. Explore system logs on the EC2 instance OS

Question Breakdown

Your application consists of two EC2 instances that require high node-to-node network throughput and low latency. What configuration choices can meet these requirements?

- A. I3 instance type and same VPC subnet.
- B. R3 instance type and jumbo frames in the VPC.
- C. C5 instance type, same subnet and enhanced networking.
- D. T2 instance type, same subnet, jumbo frames

Breakdown – Key Terms

Your application consists of **two EC2 instances** that require **high node-to-node network throughput** and **low latency**. What configuration choices can meet these requirements?

- A. I3 instance type and same VPC subnet.
- B. R3 instance type and jumbo frames in the VPC.
- C. C5 instance type, same subnet and enhanced networking.
- D. T2 instance type, same subnet, jumbo frames

Breakdown – Answer Selection

Your answer is correct. You require high node-to-node address throughput. This configuration ensures same AZ but doesn't guarantee high address throughput.

- A. I3 instance type and same VPC subnet.
- B. R3 instance type and jumbo frames in the VPC.
- C. C5 instance type, same subnet and enhanced networking.
- D. T2 instance type, same subnet, jumbo frames

Breakdown – Answer Selection

Your answer
node-to-node
configuration

Doesn't address either requirement

- A. I3 instance type and same VPC subnet.
- B. **R3 instance type and jumbo frames in the VPC.**
- C. C5 instance type, same subnet and enhanced networking.
- D. T2 instance type, same subnet, jumbo frames

Breakdown – Answer Selection

Your answer
node-to-node
configuration

C5 addresses throughput, same subnet and enhanced networking addresses latency

- A. I3 instance type and same VPC subnet.
- B. R3 instance type and jumbo frames in the VPC.
- C. **C5 instance type, same subnet and enhanced networking.**
- D. T2 instance type, same subnet, jumbo frames

Breakdown – Answer Selection

Your answer
node-type
configuration

T2 is a bad choice for throughput

- A. I3 instance type and same VPC subnet.
- B. R3 instance type and jumbo frames in the VPC.
- C. C5 instance type, same subnet and enhanced networking.
- D. **T2 instance type, same subnet, jumbo frames**

Breakdown – Answer Selection

Your answer
node-to-node
configuration

Answer: C

- A. I3 instance type and same VPC subnet.
- B. R3 instance type and jumbo frames in the VPC.
- C. C5 instance type, same subnet and enhanced networking.
- D. T2 instance type, same subnet, jumbo frames

A large, light gray circular icon containing a white right-pointing triangle, resembling a play button on a media player.

AWS Certified SysOps Administrator (Associate)
Crash Course

Domain 7 – Automation and Optimization

Automation and Optimization

- 12% of exam content
- Use AWS services and features to manage and assess resource utilization
- Employ cost-optimization strategies for efficient resource utilization
- Automate manual or repeatable process to minimize management overhead

TL; DR

- Monitor utilization to assist with optimization
- Organize resources using tags
- Take advantage of tiered pricing and discounts
- Managed services have lower TCO than unmanaged
- Scale horizontally in small increments for higher efficiency
- Architect infrastructures with automation as a goal

Resource Utilization

CloudWatch

Trusted
Advisor

Detailed
Billing Report

Resource
Tags

Cost Optimization

- Start by understanding your monthly bill
- EC2 cost models
- Temporary resources
- Managed services
- Trusted Advisor dashboard reports

Strategy 1 – when multiple implementation options are present, understand cost differences

Strategy 2 – read the Well-Architected Framework whitepaper on Cost Optimization

Billing Analysis Options

- Detailed Billing Report
- Billing Console
- Budgets
- Billing metrics in Cloudwatch
 - Estimated charges
 - Alarms with actions, not just notifications
- EC2 Marketplace products
- EMR and custom analysis

Consolidated Billing

- NOT HIERARCHICAL
- Multiple linked accounts
- Designated payer account
- Cost Optimization
 - Combined volume discounts
 - Combined EC2 reservations

Free Services

100% Free	Free with asterisk
IAM	VPC
CloudTrail	CloudWatch
Auto Scaling	Other Free Tier services
CloudFormation	AWS Certificate Manager

VPC Cost Asterisk

Free	Charged
Internet Gateway	Virtual Private Gateway
VPC Endpoints for S3 and DDB	All other VPC Endpoints
Same-AZ traffic within VPC	Cross-AZ traffic
	VPC Peering traffic
	Nat Gateway
	Flow Logs

Minimizing Overhead

Managed Services

- RDS

Temporary Resources

- Auto Scaling

Automation Tools

- CloudFormation
- Lambda

Resource Organization

- Tags

Overhead, Tags, and You

Tagging is among the most important concepts when working with AWS resources

- How many tags allowed per resource? 50
- Tags allow 127/255 chars for keys and values
- aws: is reserved
- Great for operations, billing, organization
- Devise a tagging strategy and enforce upon resource provisioning

Features that require tags

Amazon
Inspector



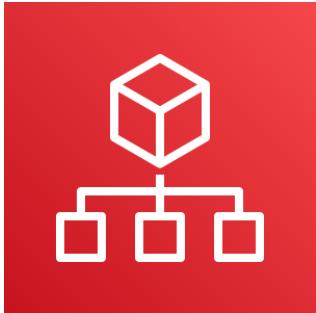
Run
command



AWS Backup



AWS Organizations



Manage multiple AWS accounts

- Hierarchical grouping of accounts
- Treat accounts like OU
- Automatically apply policies to new accounts

Operational ramifications

- Automated cross-account service integration
- Programmatic account creation
- Disables Detailed Billing console for child accounts

Question Breakdown

Your company has a large number of EBS snapshots that have collected over time. You've been asked to remove old snapshots and implement snapshot rotation in the most efficient method. Which of the following accomplishes this? (pick two)

- A. View snapshot creation dates from the console and delete as needed
- B. Write a shell script to delete snapshots older than a given date
- C. Implement Amazon Data Lifecycle Manager
- D. Implement a Lambda function in Python to rotate snapshots

Breakdown – Key Terms

Your company has a large number of **EBS snapshots** that have collected over time. You've been asked to **remove old snapshots** and **implement snapshot rotation** in the **most efficient** method. Which of the following accomplishes this? (pick two)

- A. View snapshot creation dates from the console and delete as needed
- B. Write a shell script to delete snapshots older than a given date
- C. Implement Amazon Data Lifecycle Manager
- D. Implement a Lambda function in Python to rotate snapshots

Breakdown – Answer Selection

Your company has a large collection of snapshots. You want to have efficient snapshot rotation. What is the best way to do this? (pick two)

Inefficient, doesn't address rotation

- A. **View snapshot creation dates from the console and delete as needed**
- B. Write a shell script to delete snapshots older than a given date
- C. Implement Amazon Data Lifecycle Manager
- D. Implement a Lambda function in Python to rotate snapshots

Breakdown – Answer Selection

Your company collects snapshots from multiple databases. You want to have a more efficient way to remove old snapshots. Which two methods could you use to accomplish this? (pick two)

Addresses the removal of old snapshots

- A. View snapshot creation dates from the console and delete as needed
- B. Write a shell script to delete snapshots older than a given date
- C. Implement Amazon Data Lifecycle Manager
- D. Implement a Lambda function in Python to rotate snapshots

Breakdown – Answer Selection

Your company wants to have automated snapshot rotation for their Amazon S3 buckets. You are asked to collect two options that would help them achieve this? (pick two)

Implements rotation in a fully automated fashion

- A. View snapshot creation dates from the console and delete as needed
- B. Write a shell script to delete snapshots older than a given date
- C. **Implement Amazon Data Lifecycle Manager**
- D. Implement a Lambda function in Python to rotate snapshots

Breakdown – Answer Selection

Your collection of snapshots doesn't have
collectors. It's not efficient. What do you do about this?
snapshots. What do you do about this?
efficient. What do you do about this?
(pick two)

Doesn't address initial delete.

Risk of obsolescence if code not updated.

- A. View snapshot creation dates from the console and delete as needed
- B. Write a shell script to delete snapshots older than a given date
- C. Implement Amazon Data Lifecycle Manager
- D. **Implement a Lambda function in Python to rotate snapshots**

Breakdown – Answer Selection

Your company has a large collection of Amazon S3 buckets. You want to have snapshots of all buckets. Which two actions will help you do this most efficiently? (pick two)

Answers: B and C

- A. View snapshot creation dates from the console and delete as needed
- B. Write a shell script to delete snapshots older than a given date
- C. Implement Amazon Data Lifecycle Manager
- D. Implement a Lambda function in Python to rotate snapshots



AWS Certified SysOps Administrator (Associate)
Crash Course

Further Study

AWS Whitepapers

<https://aws.amazon.com/whitepapers/>

- Overview of Security Processes
- Storage Options in the Cloud
- Defining Fault Tolerant Applications in the AWS Cloud
- Overview of Amazon Web Services
- Compliance Whitepaper
- Architecting for the AWS Cloud

Well-Architected Framework

<https://aws.amazon.com/architecture/well-architected/>

- Main whitepaper
- Whitepaper for each of the 5 pillars
 - Focus on Operational Excellence!
- Well-Architected lens whitepapers (2 more!)

Get Out and Do Something!

<https://aws.amazon.com/free/>

Create an account

<https://aws.amazon.com/getting-started/labs/>

Self-paced labs hosted by qwikLABS

<https://aws.amazon.com/getting-started/tutorials/>

10-Minute Tutorials



AWS Certified SysOps Administrator (Associate)
Crash Course

Q&A