35 Concepts You Should Know Before Going AWS Certified SysOps Administrator — Associate Exam (2019)

HK_IT_ER Follow
Dec 29, 2018 · 17 min read

I listed 35concepts you should know before going to the AWS Certified SysOps Administrator — Associate (2019). If you do not familiar any topics listed below, I suggest you to reschedule the exam.

1. ELB Metrics — SurgeQueueLength Vs SpilloverCount

SurgeQueueLength

A count of the total number of requests that are pending submission to a registered instance.

SpilloverCount

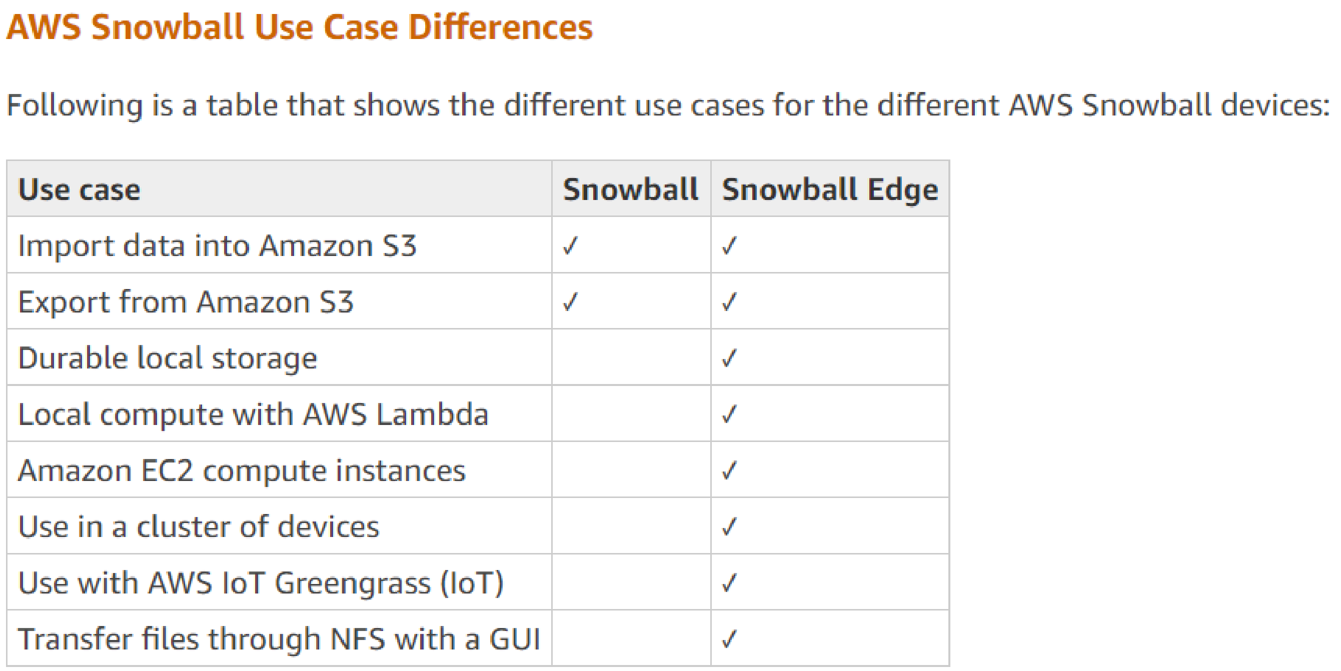
A count of the total number of requests that were rejected due to the queue being full.

2. Burstable Performance Instance

Burstable performance instances, which are **T3** and **T2** instances, are designed to provide a baseline level of CPU performance with the ability to burst to a higher level when required by your workload.

It can be enabled or disabled at any time for a running or stopped instance.

3. Snowball Vs Snowball Edge



AWS Snowball Use Case Differences

Following is a table that shows the different use cases for the different AWS Snowball devices:

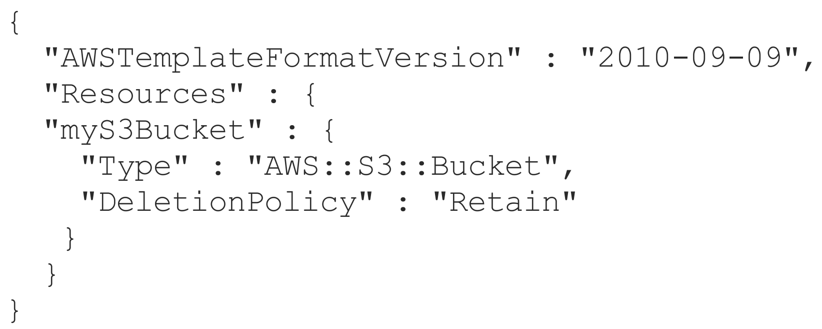
Use case	Snowball	Snowball Edge
Import data into Amazon S3	✓	✓
Export from Amazon S3	✓	✓
Durable local storage		✓
Local compute with AWS Lambda		✓
Amazon EC2 compute instances		✓
Use in a cluster of devices		✓
Use with AWS IoT Greengrass (IoT)		✓
Transfer files through NFS with a GUI		✓

AWS Snowball Use Case Differences

4. CloudFormation — DeletePolicy

1. preserve or (in some cases) backup a resource when its stack is deleted
2. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default.
3. **To keep a resource when its stack is deleted**

4. **specify Retain for that resource, to prevent deletion**
5. **specify Snapshot to create a snapshot before deleting the resource, if the snapshot capability is supported for e.g RDS, EC2 volume etc.**
6. To keep a resource when its stack is deleted, specify Retain for that resource. You can use retain for any resource. For example, you can retain a nested stack, Amazon S3 bucket, or EC2 instance so that you can continue to use or modify those resources after you delete their stacks.
7. For resources that support snapshots, such as AWS::EC2::Volume, specify Snapshot to have AWS CloudFormation create a snapshot before deleting the resource.



```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Resources" : {
  "myS3Bucket" : {
    "Type" : "AWS::S3::Bucket",
    "DeletionPolicy" : "Retain"
   }
  }
}
```

5. S3 — Bucket Policy Vs ACLs Vs IAM Policies

Bucket Policy

You attach S3 bucket policies at the bucket level (i.e. you can't attach a bucket policy to an S3 object), but the permissions specified in **the bucket policy apply to all the objects in the bucket.**

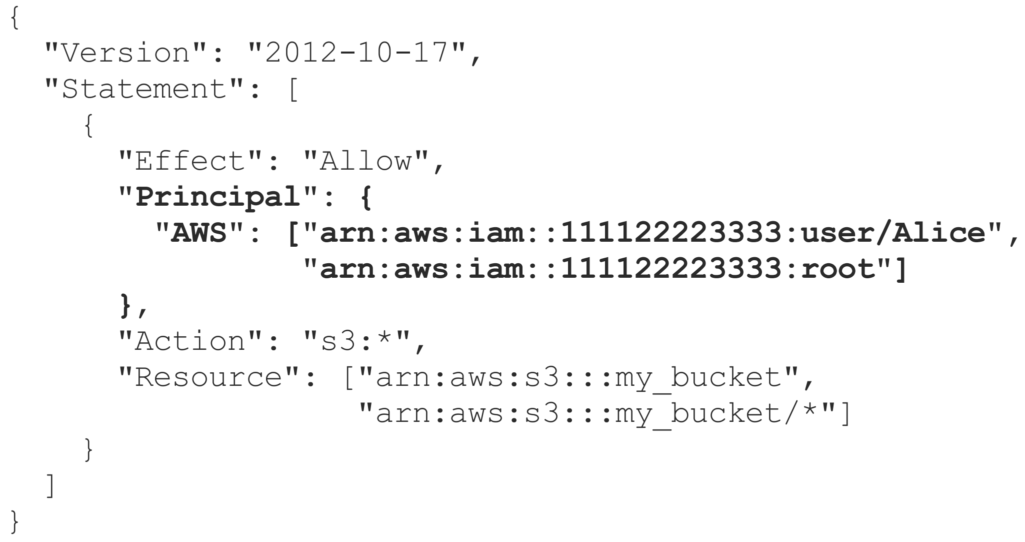
ACLS

As a general rule, AWS recommends using S3 bucket policies or IAM policies for access control. S3 ACLs is a legacy access control mechanism that predates IAM. However, if you already use S3 ACLs and you find them sufficient, there is no need to change.

ACLS Vs Bucket Policy

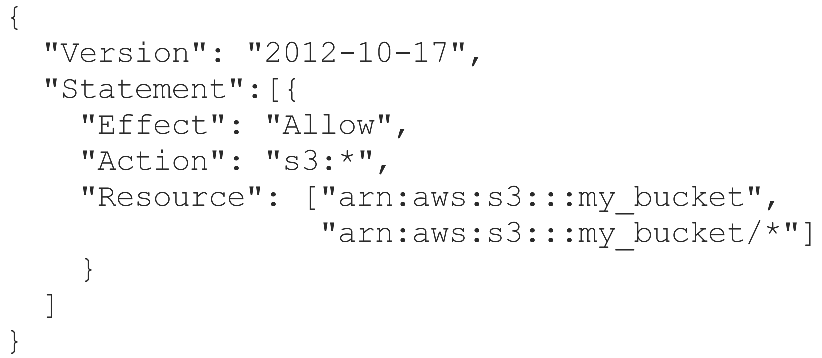
Under certain circumstances, you might find that S3 ACLs meet your needs better than IAM policies or bucket policies. If you want to manage permissions on **individual objects** within a bucket, S3 ACLs enable you to apply policies on the objects themselves, whereas bucket policies can only be applied at the bucket level. In addition, bucket policies are **limited to 20 kb in size, so consider using S3 ACLs** if you find that your bucket policy grows too large.

Sample S3 Bucket Policy



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::111122223333:user/Alice",
                "arn:aws:iam::111122223333:root"]
      },
      "Action": "s3:*",
      "Resource": ["arn:aws:s3:::my_bucket",
                   "arn:aws:s3:::my_bucket/*"]
    }
  ]
}
```

Sample IAM Policy



```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": ["arn:aws:s3:::my_bucket",
                 "arn:aws:s3:::my_bucket/*"]
    }
  ]
}
```

Note that the S3 bucket policy includes a “Principal” element, which lists the principals that bucket policy controls access for. The “Principal” element is unnecessary in an IAM policy, because the principal is by default the entity that the IAM policy is attached to.

When to use IAM policies vs. S3 policies

Use IAM policies if:

1. You need to control access to AWS services other than S3. IAM policies will be easier to manage since you can centrally manage all of your permissions in IAM, instead of spreading them between IAM and S3.
2. You have numerous S3 buckets each with different permissions requirements. IAM policies will be easier to manage since you don't have to define a large number of S3 bucket policies and can instead rely on fewer, more detailed IAM policies.
3. You prefer to keep access control policies in the IAM environment.

Use S3 bucket policies if:

1. You want a simple way to grant cross-account access to your S3 environment, without using IAM roles.
2. Your IAM policies bump up against the size limit (up to 2 kb for users, 5 kb for groups, and 10 kb for roles). S3 supports bucket policies of up 20 kb.

3. You prefer to keep access control policies in the S3 environment.

6. Cross-Account AMI Copy

You can’t copy an AMI with an associated billingProduct code that was shared with you from another account. This includes Windows AMIs and AMIs from the AWS Marketplace. To copy a shared AMI with a billingProduct code, launch an EC2 instance in your account using the shared AMI and then create an AMI from the instance.

You can’t copy an encrypted AMI that was shared with you from another account. Instead, if the underlying snapshot and encryption key were shared with you, you can copy the snapshot while re-encrypting it with a key of your own. You own the copied snapshot, and can register it as a new AMI.

7. Loss Key for Instance Store-Backed

Amazon EC2 doesn’t keep a copy of your private key; therefore, if you lose a private key, there is no way to recover it. If you lose the private key for an instance store-backed instance, you can’t access the instance; you should terminate the instance and launch another instance using a new key pair. If you lose the private key for an EBS-backed Linux instance, you can regain access to your instance.

8. How do I troubleshoot HTTP 5xx errors from Amazon S3?

The error code 500 Internal Error indicates that Amazon S3 is unable to handle the request at that time. The error code 503 Slow Down typically indicates that the requests to the S3 bucket are very high, exceeding the request rates.

9. Getting Credential Reports for Your AWS Account

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the AWS Management Console, the AWS SDKs and Command Line Tools, or the IAM API.

10. AMIs Copying

1. An identical target AMI is created, but with its own unique identifier.
2. For EBS Backed AMI, an identical but distinct root and data snapshots are created.

3. Encryption status of the snapshots are preserved. However, Launch permissions, user-defined tags, or Amazon S3 bucket permissions are not copied from the source AMI to the new AMI. After the copy operation is complete, different launch permissions, user-defined tags, and Amazon S3 bucket permissions to the new AMI.
4. AMI copy image can't be used to create an unencrypted an AMI from an encrypted AMI.
5. AMI copy image can be used to encrypt an AMI from an unencrypted AMI.

11. Glacier Retrieval Options

Expedited

to access data in 1–5 minutes, allow you to quickly access your data when occasional urgent requests for a subset of archives are required.

Standard

archives typically become available within 3–5 hours.

Bulk

access your data in approximately 5–12 hours, Bulk retrievals allow you to cost-effectively access significant portions of your data for things like big data analytics and media transcoding.

12. To create a customer gateway

For IP Address, type the **static, internet-routable IP address for your customer gateway device.** If your customer gateway is **behind a NAT device** that's enabled for NAT-T, use the **public IP address of the NAT device**.

13. Amazon Redshift, High Availability

Q: What happens to my data warehouse cluster availability and data durability if my data warehouse cluster's Availability Zone (AZ) has an outage?

If your Amazon Redshift data warehouse cluster's Availability Zone becomes unavailable, you will not be able to use your cluster until power and network access to the AZ are restored. Your data warehouse cluster's data is preserved so you can start using your Amazon Redshift data warehouse as soon as the AZ becomes available again. In addition, you can also choose to restore any existing snapshots to a new AZ in the same Region. Amazon Redshift will restore your most frequently accessed data first so you can resume queries as quickly as possible.

Q: Does Amazon Redshift support Multi-AZ Deployments?

Currently, Amazon Redshift only supports Single-AZ deployments. You can run data warehouse clusters in multiple AZ's by loading data into two Amazon Redshift data warehouse clusters in separate AZs from the same set of Amazon S3 input files. With Redshift Spectrum, you can spin up multiple clusters across AZs and access data in Amazon S3 without having to load it into your cluster. In addition, you can also restore a data warehouse cluster to a different AZ from your data warehouse cluster snapshots.

14. Identity Federation in the AWS Cloud

Federation enables you to manage access to your AWS Cloud resources centrally. With federation, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML), to exchange identity and security information between an identity provider (IdP) and an application.

Security Assertion Markup Language 2.0 (SAML) is an open standard for exchanging identity and security information with applications and service providers. Applications and service providers that support SAML enable you to sign in using your corporate directory credentials, such as your user name and password from Microsoft Active Directory.

15. Web Identity Federation — Amazon Cognito

Imagine that you are creating a mobile app that accesses AWS resources, such as a game that runs on a mobile device and stores player and score information using Amazon S3 and DynamoDB.

When you write such an app, you'll make requests to AWS services that must be signed with an AWS access key. However, we strongly recommend that you do not embed or distribute long-term AWS credentials with apps that a user downloads to a device, even in an encrypted store. Instead, build your app so that it requests temporary AWS security credentials dynamically when needed using web identity federation. The supplied temporary credentials map to an AWS role that has only the permissions needed to perform the tasks required by the mobile app.

16. EC2 Monitoring

Minimum:

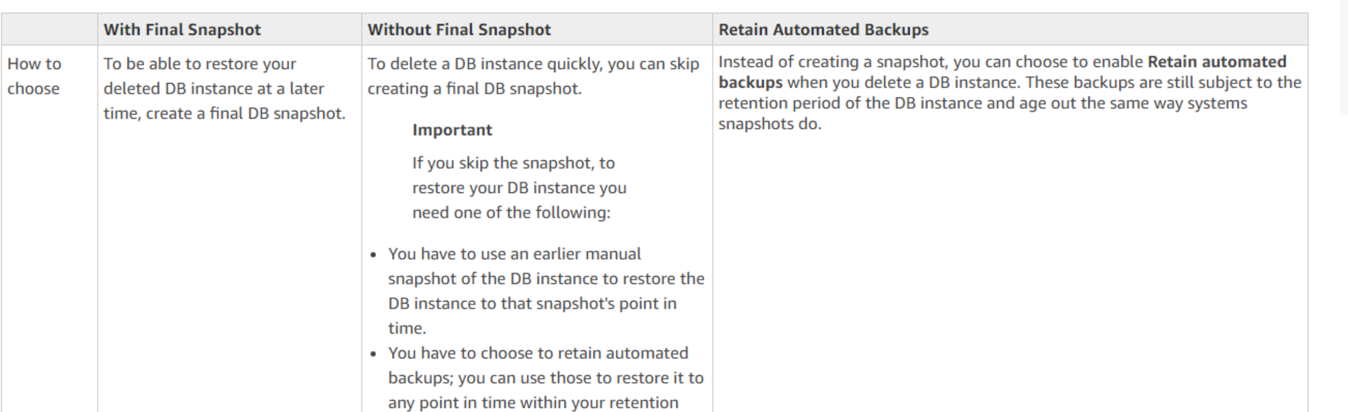
1. CPUUtilization
2. NetworkIn
3. Networkout
4. DiskReadOps

5. DiskWriteOps
6. DiskReadBytes
7. DiskWriteBytes

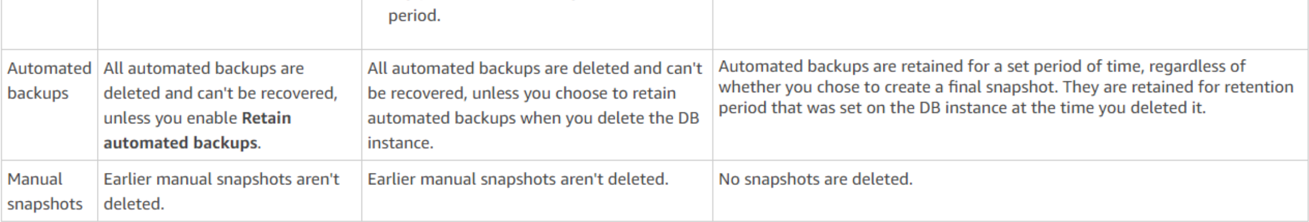
17. What happens to my backups and DB snapshots if I delete my DB instance?

When you delete a DB instance, you can create a final DB snapshot upon deletion; if you do, you can use this DB snapshot to restore the deleted DB instance at a later date. Amazon RDS retains this final user-created DB snapshot along with all other manually created DB snapshots after the DB instance is deleted.

Automated backups are deleted when the DB instance is deleted. Only manually created DB Snapshots are retained after the DB Instance is deleted.



	With Final Snapshot	Without Final Snapshot	Retain Automated Backups
How to choose	To be able to restore your deleted DB instance at a later time, create a final DB snapshot.	To delete a DB instance quickly, you can skip creating a final DB snapshot. **Important** If you skip the snapshot, to restore your DB instance you need one of the following: • You have to use an earlier manual snapshot of the DB instance to restore the DB instance to that snapshot's point in time. • You have to choose to retain automated backups; you can use those to restore it to any point in time within your retention	Instead of creating a snapshot, you can choose to enable **Retain automated backups** when you delete a DB instance. These backups are still subject to the retention period of the DB instance and age out the same way systems snapshots do.



		period.	
Automated backups	All automated backups are deleted and can't be recovered, unless you enable **Retain automated backups**.	All automated backups are deleted and can't be recovered, unless you choose to retain automated backups when you delete the DB instance.	Automated backups are retained for a set period of time, regardless of whether you chose to create a final snapshot. They are retained for retention period that was set on the DB instance at the time you deleted it.
Manual snapshots	Earlier manual snapshots aren't deleted.	Earlier manual snapshots aren't deleted.	No snapshots are deleted.

Summary on AWS RDS Backup

18. MFA Protection for Access to API Operations in the Current Account

1. If user Sofía needs to stop or terminate an Amazon EC2 instance, she calls **GetSessionToken**. This API operation passes the ID of the MFA device and the current TOTP that Sofía gets from her device.
2. User Sofía (or an application that Sofía is using) uses the temporary credentials provided by GetSessionToken to call the Amazon EC2 StopInstances or TerminateInstances action.

19. How do I use an MFA token to authenticate access to my AWS resources through the AWS CLI?

If you plan to interact with your resources using the AWS CLI while using an MFA device, you must create a temporary session token instead. If you are using an MFA hardware device, the ARN value is similar to

GAHT12345678. If you are using a virtual MFA, the value is similar to arn:aws:iam::123456789012:mfa/user.

AWS CLI command

```
aws sts get-session-token --serial-number arn-of-the-mfa-device --
token-code code-from-token
```

Output

```
{
  "Credentials": {
    "SecretAccessKey": "secret-access-key",
    "SessionToken": "temporary-session-token",
    "Expiration": "expiration-date-time",
    "AccessKeyId": "access-key-id"
  ;}
}
```

20. Why can’t I connect to an S3 bucket using a gateway VPC endpoint?

DNS settings in your VPC

DNS resolution must be enabled in your VPC

Route table settings to Amazon S3

Be sure there’s a route to Amazon S3 using the gateway VPC endpoint.

Security group outbound rules

1. The default outbound rule allows all outbound traffic. If the security group doesn’t have the default outbound rule, and instead has more restrictive rules, be sure to add one of the following outbound rules:
2. An outbound rule allowing traffic from the ID of the prefix list associated with the gateway VPC endpoint.
3. Outbound rules with Destination as the public IPs used by Amazon S3.

Network ACL rules

1. In the Inbound Rules view, be sure the rules allow inbound return traffic from Amazon S3 on ephemeral TCP ports 1024–65535.
2. In the Outbound Rules view, be sure the rules allow traffic to Amazon S3.

3. Note: By default, network ACLs allow all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic. If your network ACL rules restrict traffic, you must specify the CIDR block (IP address range) for S3.

Gateway VPC endpoint policy

Review the endpoint policy. Check if the policy blocks access to the S3 bucket or to the IAM user affected by the connectivity issues. Edit the policy to enable access for the S3 bucket or IAM user.

S3 bucket policy

Be sure the bucket policy allows access from the gateway VPC endpoint and the VPC that you want to connect. Edit the policy to enable access from the gateway VPC endpoint and VPC. Your bucket policy can restrict access only from a specific public IP address or an elastic IP address associated with an instance in an Amazon VPC. You can't restrict access based on private IP addresses associated with instances.

IAM policy

21. CloudFormation — Prevent Delete Resource (URL Request Parameter)

1. Set the DisableRollback flag to true, when creating the stack

2. Set the OnFailure to DO_NOTHING, when creating the stack

22. EBS Volume

1. General Purpose SSD (gp2) — General — 16000 (IOPS)
2. Provisioned IOPS SSD (io1) — Large database workloads — 64000 (IOPS)
3. Throughput Optimized HDD (st1) — Big Data
4. Cold HDD (sc1) — lowest storage cost
5. SSD Instance Store — 100000 (IOPS)

23. Vulnerability and Penetration Testing

The form requires you to submit information about the instances you wish to test, identify the expected start and end dates/times of your test, and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 90 days from the start date.

Permission is required for all penetration tests.

What is Amazon EFS Encryption?

24. Amazon EFS offers the ability to encrypt data at rest and in transit.

Data encrypted at rest is transparently encrypted while being written, and transparently decrypted while being read, so you don’t have to modify your applications. **Encryption keys are managed by the AWS Key Management Service (KMS)**, eliminating the need to build and maintain a secure key management infrastructure.

Data encryption in transit uses industry standard Transport Layer Security (TLS) 1.2 to encrypt data sent between your clients and EFS file systems.

When you create a new file system, you can select a key that will be used to encrypt the contents of the files that you store on the file system.

25. Granting Permission to Launch EC2 Instances with IAM Roles (PassRole Permission)

As with other IAM permissions, you can specify a wildcard (*) as the resource for the PassRole permission. For example, the following policy allows a user to associate any role whose name starts with DevTeam with the instance, such as DevTeam1 or DevTeam2.

```
{

  "Version": "2012-10-17",

  "Statement": [{

    "Effect":"Allow",

    "Action":["ec2:*"],

    "Resource":"*"

  },

  {

   "Effect":"Allow",

   "Action":"iam:PassRole",

   "Resource":"arn:aws:iam::123456789012:role/DevTeam*"

  }]

}
```

You can also use a wildcard to indicate that the permission applies to all resources–in this case, that the user is allowed to associate any role with an instance:

```
  "Resource":"arn:aws:iam::123456789012:role/*"
```

26. AWS Config Vs Trust Advisor Notification

Trusted Advisor notification feature

You will be notified by **weekly email** when you opt in for this service, and it is totally **free**.

AWS Config

You can configure AWS Config to stream configuration changes and notifications to an Amazon **SNS** topic. **When a resource is updated, you can get a notification sent to your email, so that you can view the changes.**

27. Network ACL

route.state — The state of a route in the route table (active | **blackhole**). The blackhole state indicates that the route’s target isn’t available (for example, the specified gateway isn’t attached to the VPC, the specified NAT instance has been terminated, and so on).

Route propagation allows a **virtual private gateway** to automatically propagate routes to the route tables so that you **don’t need to manually enter VPN routes** to your route tables. You can enable or disable route propagation.

28. Aurora Reader Endpoint

You use the reader endpoint for read-only connections for your Aurora cluster. This endpoint uses a load-balancing mechanism to help your cluster handle a query-intensive workload. The reader endpoint is the endpoint that you supply to applications that do reporting or other read-only operations on the cluster.

The reader endpoint only load-balances connections to available Aurora Replicas in an Aurora DB cluster. It doesn’t load-balance individual queries. If you want to load-balance each query to distribute the read workload for a DB cluster, open a new connection to the reader endpoint for each query.

Each Aurora cluster has a single built-in reader endpoint, whose name and other attributes are managed by Aurora. You can’t create, delete, or modify this kind of endpoint.

Cost Allocation Tag

29. AWS provides two types of cost allocation tags, an **AWS generated tags and user-defined tags**. You must activate both types of tags separately before they can appear in Cost Explorer or on a **cost allocation report**.

You can't delete or merge tags. Instead, deactivate tags so that they aren't used in your billing reports.

Only master accounts in an organization and single accounts that are not members of an organization have access to the Cost Allocation Tags manager in the Billing console.

30. AWS Organization

master account

A master account is the AWS account you use to create your organization. From the master account, you can create other accounts in your organization, invite and manage invitations for other accounts to join your organization, and remove accounts from your organization. You can also attach policies to entities such as administrative roots, organizational units (OUs), or accounts within your organization. **The master account has the role of a payer account and is responsible for paying all charges**

accrued by the accounts in its organization. You cannot change which account in your organization is the master account.

member account

A member account is an AWS account, other than the master account, that is part of an organization. If you are an administrator of an organization, you can create member accounts in the organization and invite existing accounts to join the organization. You also can apply policies to member accounts. A member account can belong to only one organization at a time.

Control Access

You can create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts. You can specifically Allow or Deny individual AWS Services. For example, you could deny the use of Kinesis or DynamoDB to your HR group within your AWS Organization. Even if **IAM in that account allows it, SCP will override it.**

31. Redshift — The Connection Is Refused or Fails

Example Error:

1. "Failed to establish a connection to <endpoint>."

2. “Could not connect to server: Connection timed out. Is the server running on host ‘<endpoint>’ and accepting TCP/IP connections on port ‘<port>’?”
3. “Connection refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections.”

Generally, when you receive an error message indicating that there is a failure to establish a connection, it is an issue with permission to access the cluster. You must add an **ingress rule** to the cluster security group for the CIDR/IP.

32. Troubleshooting AWS CloudFormation

Delete Stack Fails

1. Some resources must be empty before they can be deleted. For example, you must delete all objects in an Amazon S3 bucket or remove all instances in an Amazon EC2 security group before you can delete the bucket or security group.
2. Ensure that you have the necessary IAM permissions to delete the resources in the stack. In addition to AWS CloudFormation permissions, you must be allowed to use the underlying services, such as Amazon S3 or Amazon EC2.

3. When stacks are in the DELETE_FAILED state because AWS CloudFormation couldn't delete a resource, rerun the deletion with the RetainResources parameter and specify the resource that AWS CloudFormation can't delete. AWS CloudFormation deletes the stack without deleting the retained resource. Retaining resources is useful when you can't delete a resource, such as an S3 bucket that contains objects that you want to keep, but you still want to delete the stack.
4. You cannot delete stacks that have termination protection enabled.

Dependency Error

To resolve a dependency error, add a DependsOn attribute to resources that depend on other resources in your template. In some cases, you must explicitly declare dependencies so that AWS CloudFormation can create or delete resources in the correct order.

For example, if you create an Elastic IP and a VPC with an Internet gateway in the same stack, the Elastic IP must depend on the Internet gateway attachment.

Insufficient IAM Permissions

When you work with an AWS CloudFormation stack, you not only need permissions to use AWS CloudFormation, you must also have permission to use the underlying services that are described in your template. For example, if you're creating an Amazon S3 bucket or starting an Amazon EC2 instance, you need permissions to Amazon S3 or Amazon EC2.

Invalid Value or Unsupported Resource Property

When you create or update an AWS CloudFormation stack, your stack can fail due to invalid input parameters, unsupported resource property names, or unsupported resource property values. For input parameters, verify that the resource exists.

For example, when you specify an Amazon EC2 key pair or VPC ID, the resource must exist in your account and in the region in which you are creating or updating your stack. You can use AWS-specific parameter types to ensure that you use valid values.

For resource property names and values, update your template to use valid names and values. For a list of all the resources and their property names, see AWS Resource and Property Types Reference.

Limit Exceeded

Verify that you didn't reach a resource limit. For example, the default number Amazon EC2 instances that you can launch is 20. If try to create more Amazon EC2 instances than your account limit, the instance creation fails and you receive the error Status=start_failed.

Also, during an update, if a resource is replaced, AWS CloudFormation creates new resource before it deletes the old one. This replacement might put your account over the resource limit, which would cause your update to fail. You can delete excess resources or request a limit increase.

No Updates to Perform

To update an AWS CloudFormation stack, you must submit template or parameter value changes to AWS CloudFormation. However, AWS CloudFormation won't recognize some template changes as an update, such as changes to a deletion policy, update policy, condition declaration, or output declaration. If you need to make such changes without making any other change, you can add or modify a metadata attribute for any of your resources.

Wait Condition Didn't Receive the Required Number of Signals from an Amazon EC2 Instance

Ensure that the AMI you're using has the AWS CloudFormation helper scripts installed. If the AMI doesn't include the helper scripts, you can also download them to your instance.

Verify that the cfn-signal command was successfully run on the instance.

Amazon S3 Inventory

33. You can **use it to audit and report on the replication and encryption status** of your objects for business, compliance, and regulatory needs. You can also simplify and speed up business workflows and big data jobs using Amazon S3 inventory, which provides a scheduled alternative to the Amazon S3 synchronous List API operation.

You can configure multiple inventory lists for a bucket. You can configure what object metadata to include in the inventory, **whether to list all object versions or only current versions**, where to store the inventory list file output, and whether to generate the inventory on a daily or weekly basis. You can also specify that the inventory list file be encrypted.

You can query Amazon S3 inventory using standard SQL by using Amazon Athena, Amazon Redshift Spectrum, and other tools such as Presto, Apache Hive, and Apache Spark. It's easy to use Athena to run queries on your inventory files. You can use Athena for Amazon S3 inventory queries in all Regions where Athena is available.

34. Amazon S3 Analytics

By using Amazon S3 analytics storage class analysis you can analyze storage access patterns to help you decide when to transition the right data to the right storage class. This new Amazon S3 analytics feature observes data access patterns to help you **determine when to transition**

less frequently accessed STANDARD storage to the STANDARD_IA (IA, for infrequent access) storage class.

35. Can I use Amazon ElastiCache for Memcached with an AWS persistent data store such as Amazon RDS or Amazon DynamoDB?

Yes, Amazon ElastiCache is an ideal front-end for data stores like Amazon RDS or Amazon DynamoDB, providing a high-performance middle tier for applications with extremely high request rates and/or low latency requirements.

AWS Aws Certified Aws Sysops Sysops Aws Exam