7-simulacoes profissionais

Notebook:	solutions profissional_ef8e1c0f-5d3c-42ab-ab04-9217e53e12cd		
Created:	19/10/2025 18:37	**Updated:**	21/10/2025 02:39
Author:	erikachen19@gmail.com		
URL:	https://portal.tutorialsdojo.com/courses/aws-certified-solutions-architect-professional...		

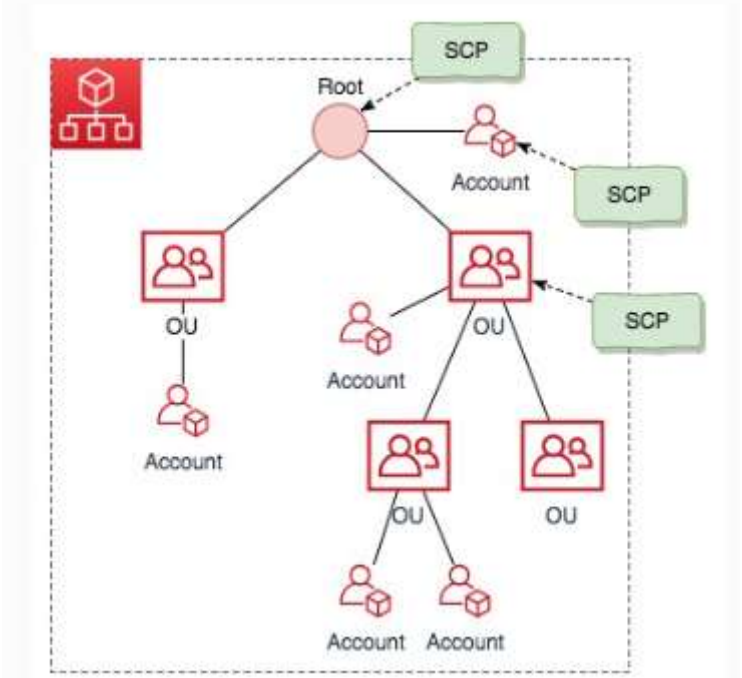
A company is planning to launch a mobile app for the Department of Transportation that allows government staff to upload the latest photos of ongoing construction works such as bridges, roads culverts, and dams all over the country. The mobile app should send the photos to a web server hosted on an EC2 instance which then adds a watermark to each photo that contains the project details and the date it was taken. The solutions architect must design a solution in which the photos generated by the server will be uploaded to an S3 bucket for durable storage.

Which of the following solutions is a secure architecture and allows the EC2 instance to upload photos to S3?

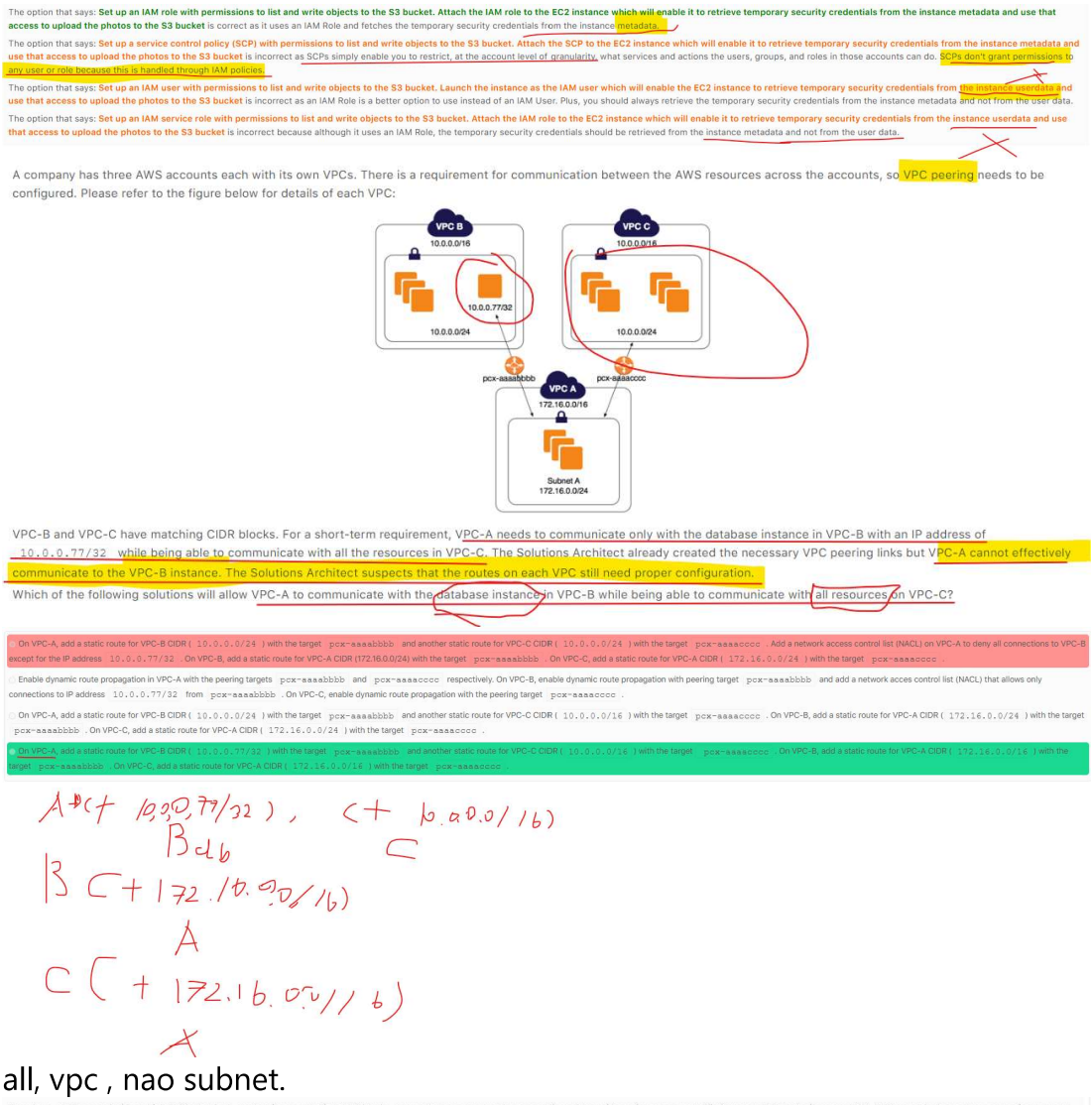
(view) 1 0 1 00:00:00

- Set up a service control policy (SCP) with permissions to list and write objects to the S3 bucket. Attach the SCP to the EC2 instance which will enable it to retrieve temporary security credentials from the instance metadata and use that access to upload the photos to the S3 bucket.
- Set up an IAM user with permissions to list and write objects to the S3 bucket. Launch the instance as the IAM user which will enable the EC2 instance to retrieve temporary security credentials from the instance userdata and use that access to upload the photos to the S3 bucket.
- Set up an IAM role with permissions to list and write objects to the S3 bucket. Attach the IAM role to the EC2 instance which will enable it to retrieve temporary security credentials from the instance metadata and use that access to upload the photos to the S3 bucket.
- Set up an IAM service role with permissions to list and write objects to the S3 bucket. Attach the IAM role to the EC2 instance which will enable it to retrieve temporary security credentials from the instance userdata and use that access to upload the photos to the S3 bucket.

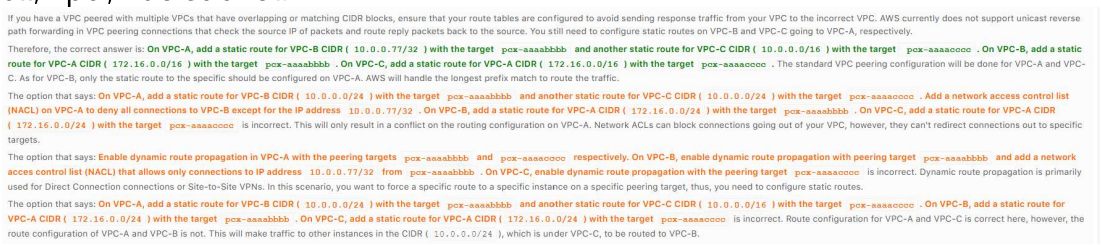
This question tests your understanding of IAM, specifically on when to use an IAM Role over an SCP. Since the server is running on an EC2 instance and the application makes requests to S3 to store the photos, the more suitable option to use here is an IAM Role.

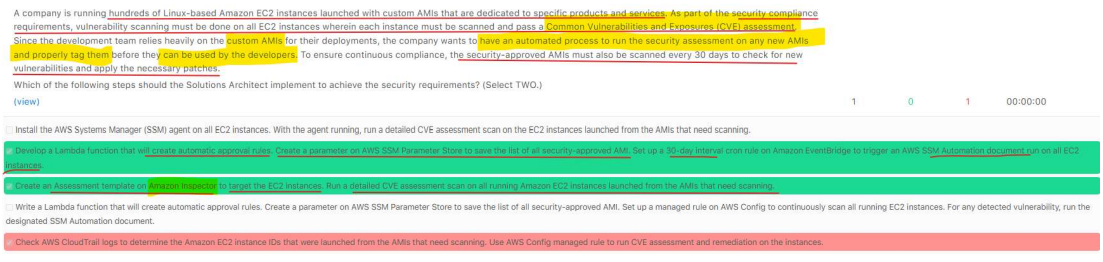


In addition, don't create an IAM user and pass the user's credentials to the application or embed the credentials in the application. That will create a security risk because if an attacker had unauthorized access to that EC2 instance then the user credentials can easily be acquired and exploited. The better way is to create an IAM role that you can attach to the EC2 instance to give applications running on the instance temporary security credentials which can be used to access other AWS resources such as an S3 bucket. The credentials have the permissions specified in the policies attached to the role.



all, vpc , nao subnet.





What is a CVE assessment scan?

A **CVE assessment scan** is the process of scanning systems, applications, containers, or code for known security vulnerabilities that are tracked by **CVE identifiers** (Common Vulnerabilities and Exposures). The aim is to discover

which CVEs affect your assets, assess risk (severity/impact), and prioritize remediation.

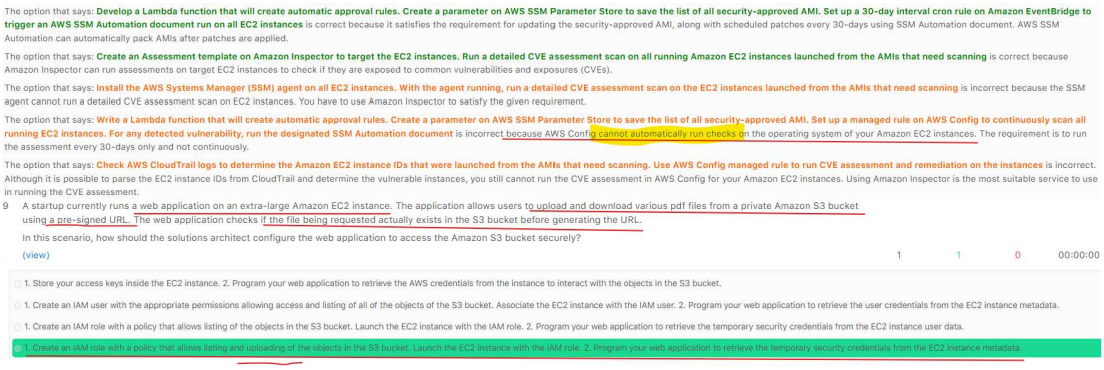
AWS Systems Manager Automation simplifies common maintenance and deployment tasks of **Amazon EC2 instances** and other AWS resources. Automation enables you to do the following:

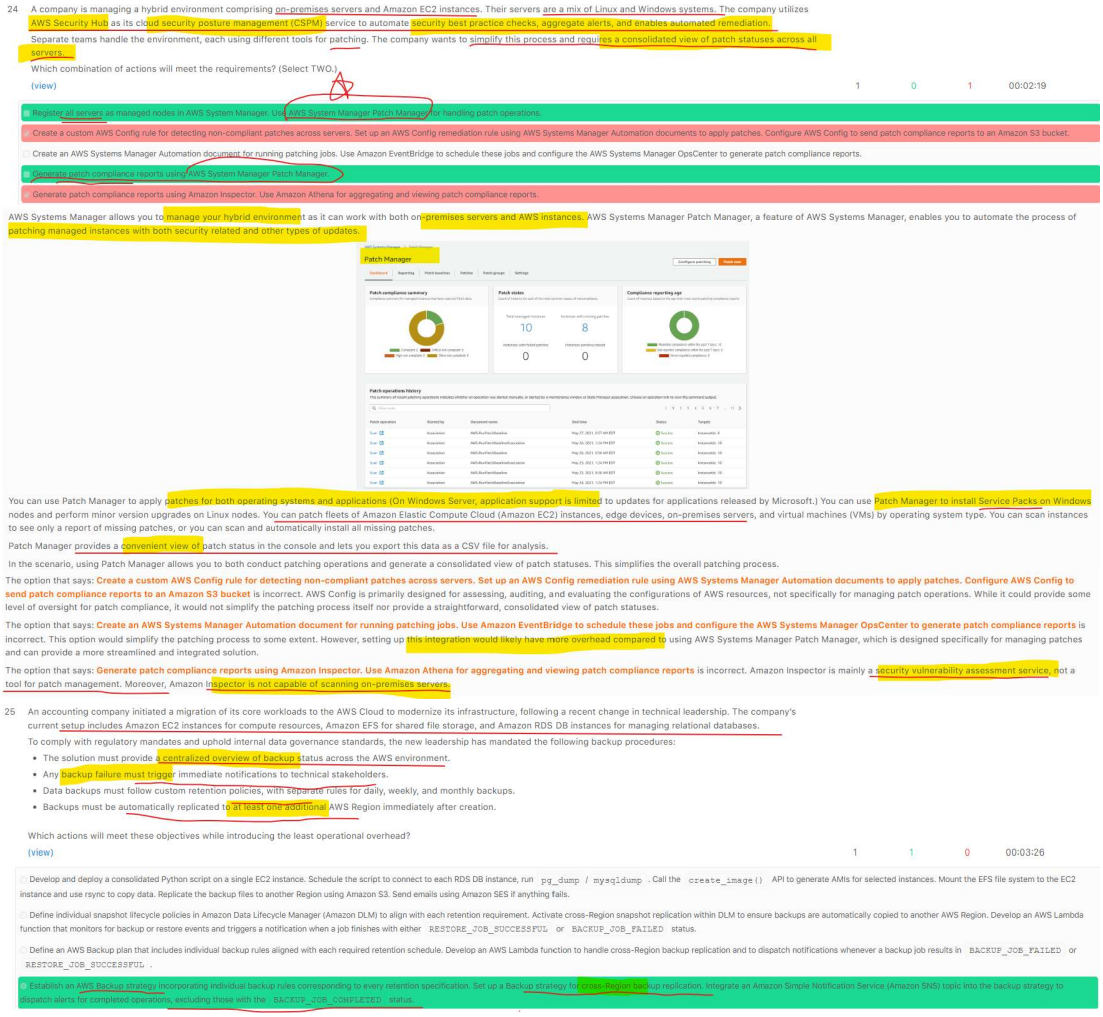
- Build automations to configure and manage instances and AWS resources.
- Create custom runbooks or use pre-defined runbooks maintained by AWS.
- Receive notifications about Automation tasks and runbooks by using Amazon EventBridge.
- Monitor Automation progress and details by using the AWS Systems Manager console.

SSM Automation offers one-click automation for simplifying complex tasks such as creating golden Amazon Machines Images (AMIs) and recovering unreachable EC2 instances. For example, you can use Use the `AWS-UpdateLinuxAmi` and `AWS-UpdateWindowsAmi` runbooks to create golden AMIs from a source AMI. You can run custom scripts before and after updates are applied. You can also include or exclude specific packages from being installed.

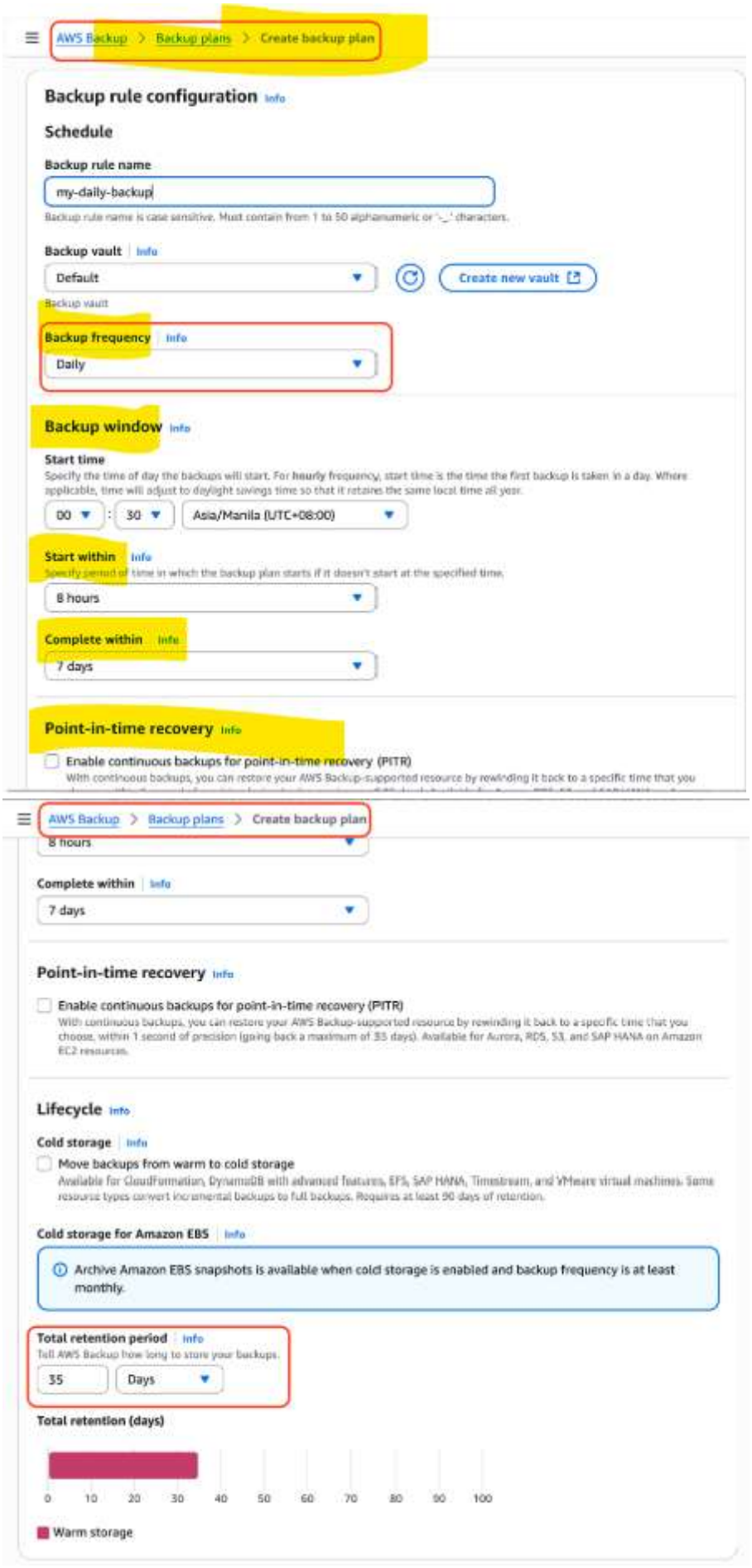
With **AWS EventBridge**, you can create rules that self-trigger on an automated schedule in EventBridge using cron or rate expressions. Rate expressions are simpler to define but don't offer the fine-grained schedule control that cron expressions support. For example, with a cron expression, you can define a rule that triggers at a specified time on a certain day of each week or month. With this, **you can schedule running AWS SSM Automation documents to remediate the vulnerable AMIs.**

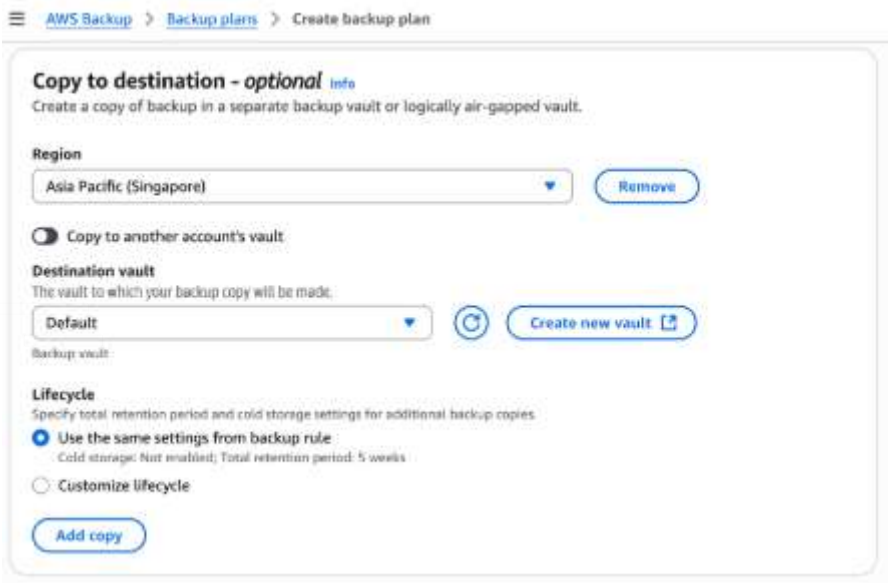
You can use **Amazon Inspector**亚马逊检查员 to conduct a detailed scan for CVE in your fleet of EC2 instances. Amazon Inspector offers **predefined software called an agent that you can optionally install in the operating system of the EC2 instances that you want to assess.** Amazon Inspector also **has rules packages that help verify whether the EC2 instances in your assessment 评估 targets are exposed to common vulnerabilities and exposures (CVEs).** Attacks can exploit unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of your service or data. The CVE system provides a reference method for publicly known information security vulnerabilities and exposures.





AWS Backup is a fully managed service that makes it easy to **centralize and automate data protection across AWS services, in the cloud, and on-premises**. Using this service, you can **configure backup policies and monitor activity for your AWS resource**s in one place. It allows you to automate and consolidate backup tasks previously performed service-by-service, and removes the need to create custom scripts and manual processes. You can automate your data protection policies and schedules with a few clicks in the AWS Backup console.
AWS Backup provides many features and capabilities, including **lifecycle management policies, cross-Region backup, and backup activity monitoring.**

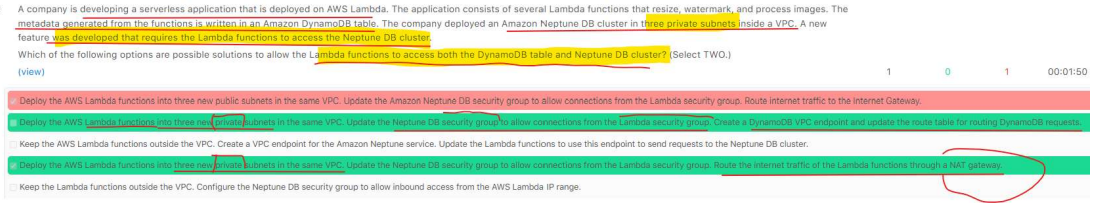

AWS Backup > Backup plans > Create backup plan
Backup rule configuration Info
Schedule
Backup rule name
my-daily-backup
Backup rule name is case sensitive. Must contain from 1 to 50 alphanumeric or '-_' characters.
Backup vault Info
Default
Create new vault
Backup vault
Backup frequency Info
Daily
Backup window Info
Start time
Specify the time of day the backups will start. For hourly frequency, start time is the time the first backup is taken in a day. Where applicable, time will adjust to daylight savings time so that it retains the same local time all year.
00 : 30 Asia/Manila (UTC+08:00)
Start within Info
Specify period of time in which the backup plan starts if it doesn't start at the specified time.
8 hours
Complete within Info
7 days
Point-in-time recovery Info
Enable continuous backups for point-in-time recovery (PITR)
With continuous backups, you can restore your AWS Backup-supported resource by rewinding it back to a specific time that you
AWS Backup > Backup plans > Create backup plan
8 hours
Complete within Info
7 days
Point-in-time recovery Info
Enable continuous backups for point-in-time recovery (PITR)
With continuous backups, you can restore your AWS Backup-supported resource by rewinding it back to a specific time that you choose, within 1 second of precision (going back a maximum of 35 days). Available for Aurora, RDS, S3, and SAP HANA on Amazon EC2 resources.
Lifecycle Info
Cold storage Info
Move backups from warm to cold storage
Available for CloudFormation, DynamoDB with advanced features, EFS, SAP HANA, Timestream, and VMware virtual machines. Some resource types convert incremental backups to full backups. Requires at least 90 days of retention.
Cold storage for Amazon EBS Info
Archive Amazon EBS snapshots is available when cold storage is enabled and backup frequency is at least monthly.
Total retention period Info
Tell AWS Backup how long to store your backups.
35 Days
Total retention (days)
0 10 20 30 40 50 60 70 80 90 100
Warm storage



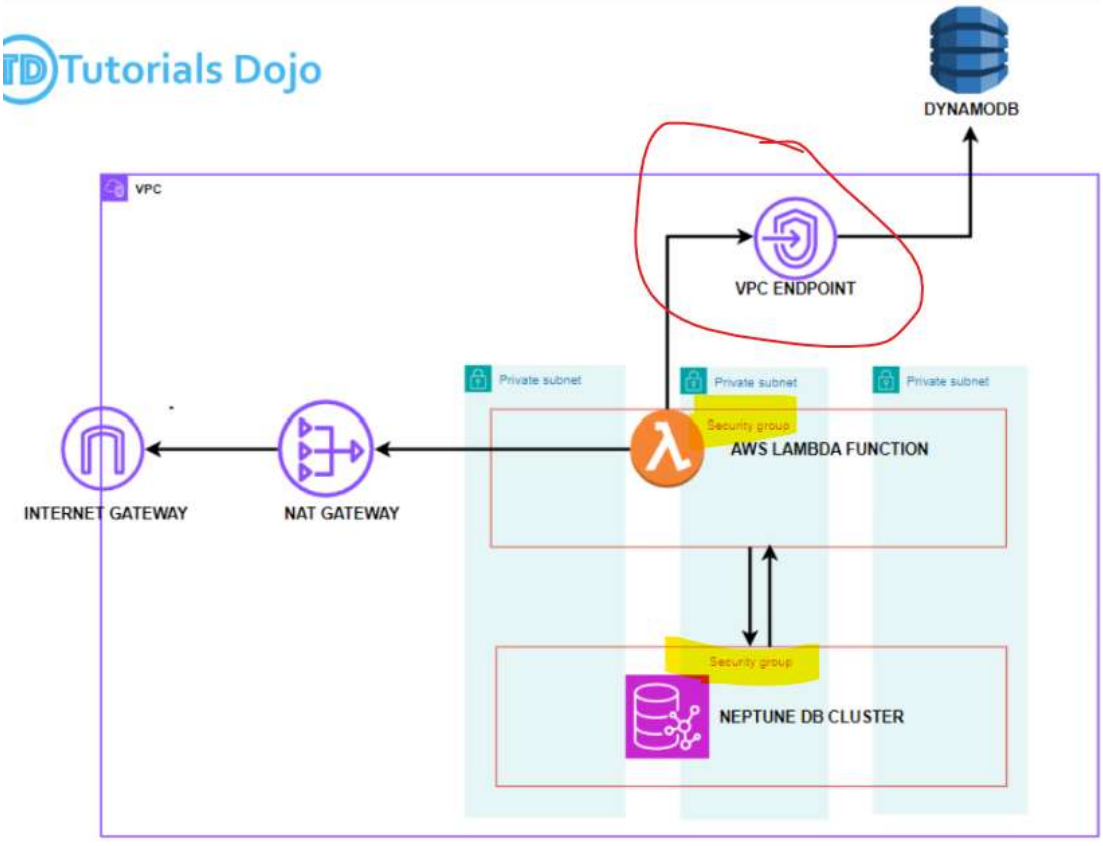
AWS Backup is purpose-built to manage backup operations across EC2, EFS, and RDS with centralized visibility. It allows you to define individual backup rules for each retention period, supports native cross-Region replication, and integrates directly with Amazon SNS to send alerts for specific backup job statuses. The requirement also **states the necessity to trigger immediate notifications on failure.** Since AWS Backup includes multiple possible failure statuses and transitional statuses, the configuration simply sends notifications for all job completions except the successful `BACKUP_JOB_COMPLETED` status, ensuring nothing slips through the cracks. This approach meets all the stated requirements without introducing custom scripting or external monitoring, and it introduces the least operational overhead by using built-in managed features.
Hence, the correct answer is: **Establish an AWS Backup strategy incorporating individual backup rules corresponding to every retention specification. Set up a Backup strategy for cross-Region backup replication. Integrate an Amazon Simple Notification Service (Amazon SNS) topic into the backup strategy to dispatch alerts for completed operations, excluding those with the `BACKUP_JOB_COMPLETED` status.**
The option that says: **Develop and deploy a consolidated Python script on a single EC2 instance. Schedule the script to connect to each RDS DB instance, run `pg_dump`/`mysqldump`. Call the `create_image()` API to generate AMIs for selected instances. Mount the EFS file system to the EC2 instance and use rsync to copy data. Replicate the backup files to another Region using Amazon S3. Send emails using Amazon SES if anything fails** is incorrect. It relies on a custom EC2-based script to manage backups, which requires ongoing maintenance and complex logic to handle failures, retention, and replication. It just does not provide centralized visibility or native integration with AWS services for status tracking and alerting. This method adds operational complexity instead of reducing it and primarily duplicates features that AWS Backup already offers.
The option that says: **Define individual snapshot lifecycle policies in Amazon Data Lifecycle Manager (Amazon DLM) to align with each retention requirement. Activate cross-Region snapshot replication within DLM to ensure backups are automatically copied to another AWS Region. Develop an AWS Lambda function that monitors for backup or restore events and triggers a notification when a job finishes with**

either `RESTORE_JOB_SUCCESSFUL` or `BACKUP_JOB_FAILED` status is incorrect. Amazon DLM is primarily designed for EBS volume snapshots and does not support RDS or EFS. While it can automate retention and replication for EC2 volumes, it simply does not offer centralized backup visibility across all services or native notification mechanisms. Relying on Lambda for alerts adds overhead and does not replace the native features that AWS Backup provides.

The option that says: **Define an AWS Backup plan that includes individual backup rules aligned with each required retention schedule. Develop an AWS Lambda function to handle cross-Region backup replication and to dispatch notifications whenever a backup job results in `BACKUP_JOB_FAILED` or `RESTORE_JOB_SUCCESSFUL`** is incorrect. This solution offloads replication and notifications to custom Lambda functions, even though AWS Backup already supports built-in replication and alert integration through SNS. This approach just adds unnecessary components, making the architecture more complex and challenging to manage. It primarily ignores the full capabilities of AWS Backup and increases operational burden without any real benefit.



dynamodb nao esta na mesma vpc



- Lambdas in **private subnets** (no public IP, no route to Internet Gateway) cannot reach public AWS services like DynamoDB **by default**, because **DynamoDB's public endpoint (https://dynamodb.<region>.amazonaws.com) lives on the internet.**

- Without an internet path (NAT Gateway), your Lambda's requests will fail.

AWS provides a **VPC Endpoint** — a private connection between your VPC and DynamoDB **over the AWS network**, not the internet.
2. Create a **VPC Endpoint for DynamoDB**
In the AWS Console:
Go to VPC → Endpoints → Create endpoint
Service category: AWS services
Service name: com.amazonaws.<region>.**dynamodb**
Type: Gateway
VPC: choose your Lambda's VPC
Route tables: **select the route table used by your private subnets**

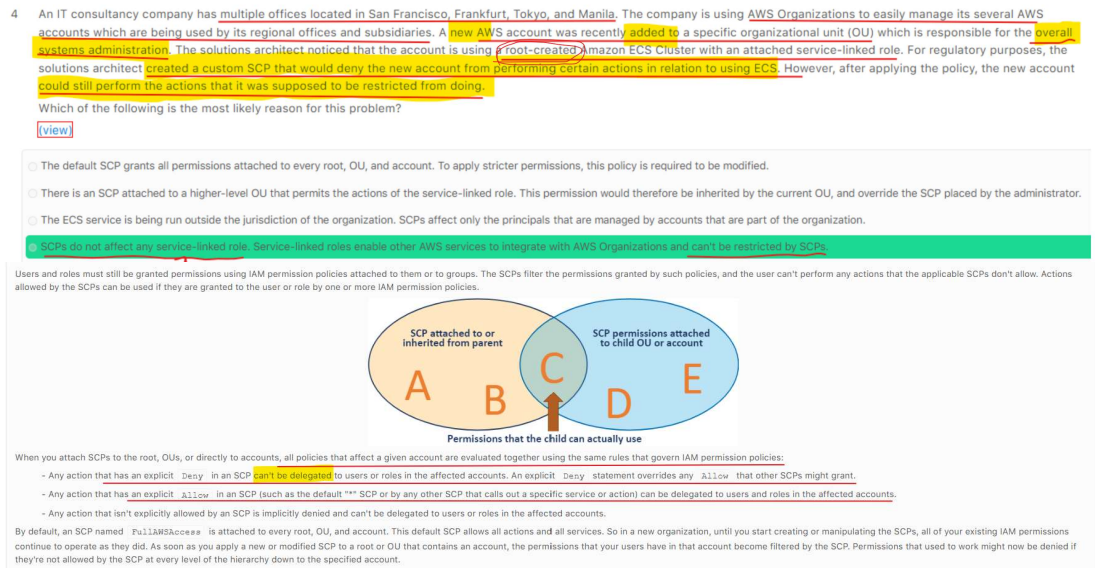
3. Verify route table

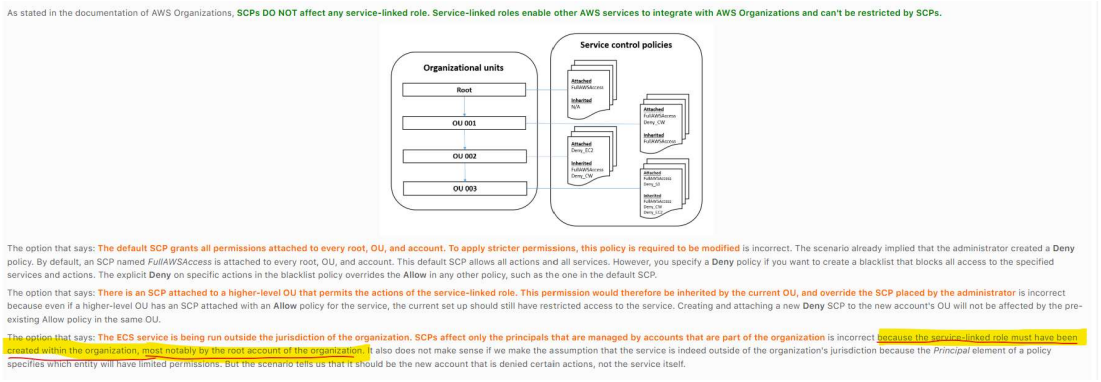
Once created, AWS automatically adds a route:

Destination: com.amazonaws.<region>.dynamodb Target: vpce-xxxxxxxxxxxx
This ensures any traffic to DynamoDB goes through the **VPC Endpoint**, not the internet.

```
import boto3

def lambda_handler(event, context):
    table = boto3.resource('dynamodb').Table('MyTable')
    table.put_item(Item={'id': '123', 'name': 'Erika'})
    return "Success"
```





A **service-linked role** is a **special type of IAM role** that is **directly managed and used by an AWS service —** not by you or your applications.
You generally can't (and shouldn't) edit this directly.
You can't modify the trust or permission policies -> They're AWS-managed
Deleting the role can break the service ->Always check dependencies
Use aws iam list-roles or the console to see which services use them
Some services require a service-linked role before activation (e.g., ECS, Glue, EMR)

Property	Description
Created by AWS	Automatically created when needed
Managed by AWS	Permissions are updated automatically as the service evolves
Scoped to one service	Each service has its own role; not shared
Can be deleted (carefully)	If you delete it, that service might stop working until recreated
Visible in IAM console	Listed under *Roles → AWS Service-linked roles*

5 A media company hosts its entire infrastructure on the AWS cloud. There is a requirement to copy information to or from the shared resources from another AWS account. The solutions architect has to provide the other account access to several AWS resources, such as Amazon S3, AWS KMS, and Amazon OpenSearch Service, in the form of a list of AWS account ID numbers. In addition, the user in the other account should still work in the trusted account, and there is no need to give up the user permissions in place of the role permissions. The solutions architect must also set up a solution that continuously assesses, audits, and monitors the policy configurations.

Which of the following is the MOST suitable type of policy that should be used in this scenario?

(view)

- Set up cross-account access with a user-based policy configuration. Use AWS Config rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration.
- Set up a service-linked role with an identity-based policy. Use AWS Systems Manager rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration.
- Set up cross-account access with a resource-based Policy. Use AWS Config rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration.
- Set up a service-linked role with a service control policy. Use AWS Systems Manager rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration.

For some AWS services, you can grant cross-account access to your resources. To do this, you attach a policy directly to the resource that you want to share, instead of using a role as a proxy. The resource that you want to share must support resource-based policies. Unlike a user-based policy, a resource-based policy specifies who (in the form of a list of AWS account ID numbers) can access that resource.

Cross-account access with a resource-based policy has some advantages over a role. With a resource that is accessed through a resource-based policy, the user still works in the trusted account and does not have to give up his or her user permissions in place of the role permissions. In other words, the user continues to have access to resources in the trusted account at the same time as he or she has access to the resource in the trusting account. This is useful for tasks such as copying information to or from the shared resource in the other account.

The option that says: **Set up cross-account access with a user-based policy configuration. Use AWS Config rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration** is incorrect because a user-based policy only maps the access to a certain IAM user and not to a certain AWS resource.

The option that says: **Set up a service-linked role with an identity-based policy. Use AWS Systems Manager rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration** is incorrect because a service-linked role is just a unique type of IAM role that is linked directly to an AWS service. In addition, it is the AWS Config service, and not the AWS Systems Manager, that enables you to assess, audit, and evaluate the configurations of your AWS resources.

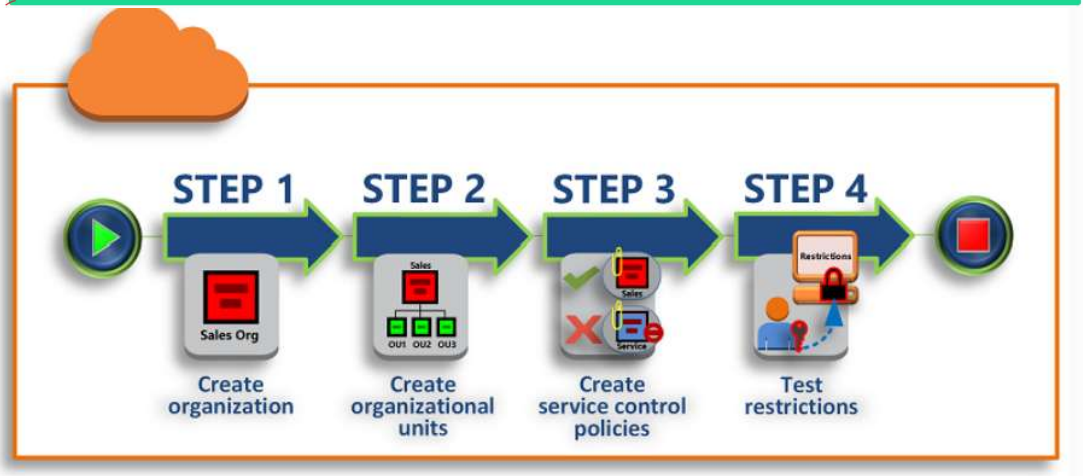
The option that says: **Set up a service-linked role with a service control policy. Use AWS Systems Manager rules to periodically audit changes to the IAM policy and monitor the compliance of the configuration** is incorrect because a service control policy is primarily used in AWS Organizations and not for cross-account access. Service-linked roles are predefined by the service and include all the permissions that the service requires to call other AWS services on your behalf. This is not suitable for providing access to your resources to other AWS accounts, unlike cross-account access. You should also use AWS Config, and not AWS Systems Manager, to periodically audit changes to the IAM policy.

6 A multinational manufacturing company has multiple AWS accounts in multiple AWS regions across North America, Europe, and Asia. The solutions architect has been tasked to set up AWS Organizations to centrally manage policies and have full administrative control across the multiple AWS accounts owned by the company.

Which of the following options is the recommended implementation to achieve this requirement with the LEAST effort?

(view) 1 0 1 00:00:00

- Set up AWS Organizations by establishing cross-account access from the master account to all member AWS accounts of the company. The master account will automatically have full administrative control across all member accounts.
- Set up AWS Organizations by sending an invitation to the master account of your organization from each of the member accounts of the company. Create an `OrganizationAccountAccessRole` IAM role in the member account and grant permission to the master account to assume the role.
- Use AWS Control Tower from the master account and enroll all the member AWS accounts of the company. AWS Control Tower will automatically provision the needed IAM permissions to have full administrative control across all member accounts.
- Set up AWS Organizations by sending an invitation to all member accounts of the company from the master account of your organization. Create an `OrganizationAccountAccessRole` IAM role in the member account and grant permission to the master account to assume the role.



After you create an **Organization** and verify that you own the email address associated with the master account, you can invite existing AWS accounts to join your organization. When you invite an account, AWS Organizations sends an invitation to the account owner, who decides whether to accept or decline the invitation. You can use the AWS Organizations console to initiate and manage invitations that you send to other accounts. You can send an invitation to another account only from the master account of your organization.

If you are the administrator of an AWS account, you also can accept or decline an invitation from an organization. If you accept, your account becomes a member of that organization. Your account can join only one organization, so if you receive multiple invitations to join, you can accept only one.

When an invited account joins your organization, you *do not* automatically have full administrator control over the account, unlike created accounts. If you want the master account to have f**ull administrative control over an invited member account, you must create the `OrganizationAccountAccessRole` IAM role in the member account** and grant permission to the master account to assume the role.