**Configure AWS backup to setup backup and retention policy for following services**

AWS Backup

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud and on premises. Using AWS Backup, you can configure backup policies and monitor backup activity for your AWS resources in one place. AWS Backup automates and consolidates backup tasks that were previously performed service-by-service and removes the need to create custom scripts and manual processes. With just a few clicks on the AWS Backup console, you can create backup policies that automate backup schedules and retention management.

**Supported Resources**

Amazon EFS file systems

DynamoDB tables

Amazon EC2 instances(Does not support Amazon EC2 instance store-backed instances)

Amazon EBS volumes

Amazon RDS databases

AWS Backup provides the following features and capabilities

**Centralized Backup Management**

* The AWS Backup centralized backup console offers a consolidated view of your backups and backup activity logs, making it easier to audit your backups and ensure compliance.

**Cross-Region Backup**

* you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan

**Cross-Account Management**

* you can automatically use backup policies to apply backup plans across the AWS accounts within your organization
* eliminate manually duplicating backup plans across individual accounts

**Limitation:**

* Before you can use the cross-account management feature, you must have an existing organization structure configured in AWS Organizations. An organizational unit (OU) is a group of accounts that can be managed as a single entity. AWS Organizations is a list of accounts that can be grouped into organizational units and managed as a single entity**.**

**Policy-Based Backup Solutions**

* backup policies known as backup plans
* Backup plans make it easy to enforce your backup strategy across your organization and across your applications in a scalable manner

**Tag-Based Backup Policies**

* can use AWS Backup to apply backup plans to your AWS resources by tagging them

Backup Activity Monitoring

* A dashboard that makes it simple to audit backup and restore activity across AWS services.
* Can view the status of recent backup jobs and also restore jobs across AWS services to ensure that your AWS resources are properly protected.
* AWS Backup integrates with AWS CloudTrail and Amazon Simple Notification Service (Amazon SNS)

**Lifecycle Management Policies**

* automatically transition backups from warm storage to cold storage according to a schedule that you define

**Limitation**

* Currently only Amazon EFS file system backups can be transitioned to cold storage

**Backup Access Policies**

* Resource-based access policies for your backup vaults to define who has access to your backups.

**Managing Backups Using Backup Plans**

* A backup plan is a policy expression that defines when and how you want to back up your AWS resources, such as Amazon DynamoDB tables or Amazon Elastic File System (Amazon EFS) file systems.
* You can assign resources to backup plans, and AWS Backup automatically backs up and retains backups for those resources according to the backup plan.
* You can create multiple backup plans if you have workloads with different backup requirements.

Creating Backup Plans

* Backup Plan Name
  + - You must provide a unique backup plan name.
* Backup Rules
* Backup plans are composed of one or more backup rules. Each backup rule consists of the following elements.
* Backup Rule Name
  + Backup rule names are case sensitive. They must contain from 1 to 63 alphanumeric characters or hyphens.

Backup Frequency

The backup frequency determines how often a backup is created

Backup Window

Backup windows consist of the time that the backup window begins and the duration of the window in hours. Backup jobs are started within this window

Lifecycle

The lifecycle defines when a backup is transitioned to cold storage and when it expires

Note:

Backups that are transitioned to cold storage must be stored in cold storage for a minimum of 90 days. Therefore, on the console, the “expire after days” setting must be 90 days longer than the “transition to cold after days” setting.

**Note**

* Currently only Amazon EFS file system backups can be transitioned to cold storage

**Backup Vault**

A backup vault is a container to organize your backups in

You can use backup vaults to set the AWS Key Management Service (AWS KMS) encryption key that is used to encrypt backups in the backup vault and to control access to the backups in the backup vault

**Tags Added to Recovery Points**

The tags that you list here are automatically added to backups when they are created.

**Tags Added to Backup Plans**

These tags are associated with the backup plan itself to help you organize and track your backup plan.

**Assigning Resources to a Backup Plan**

When you assign a resource to a backup plan, that resource is backed up automatically according to the backup plan.

You can assign resources using tags or resource IDs

Using tags to assign resources is a simple and scalable way to back up multiple resources. Any resources with the tags that you specify in the resource assignment are assigned to the backup plan. For example, if you include the tag values "July" and "August," your backup will include all resources tagged with the selected months.

**Note**

When creating a tag-based backup plan, if you choose a role other than **Default role**, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission to access, the backup plan fails.

**Backup Vault Name**

Backup vault names are case sensitive. They must contain from 2 to 50 alphanumeric characters or hyphens.

**KMS Encryption Master Key**

The AWS KMS encryption master key is used to protect your backups in this backup vault. By default, AWS Backup creates a master key with the alias aws/backup for you. You can choose that key or choose any other key in your account

**Backup Vault Tags**

These tags are associated with the backup vault to help you organize and track your backup vaults.

**Inputs**

| **Name** | **Description** | **Type** | **Default** | **Required** |
| --- | --- | --- | --- | --- |
| attributes | Additional attributes (e.g. 1) | list(string) | [] | no |
| backup\_resources | An array of strings that either contain Amazon Resource Names (ARNs) or match patterns of resources to assign to a backup plan | list(string) | n/a | yes |
| cold\_storage\_after | Specifies the number of days after creation that a recovery point is moved to cold storage | number | null | no |
| completion\_window | The amount of time AWS Backup attempts a backup before canceling the job and returning an error. Must be at least 60 minutes greater than start\_window | number | null | no |
| delete\_after | Specifies the number of days after creation that a recovery point is deleted. Must be 90 days greater than cold\_storage\_after | number | null | no |
| delimiter | Delimiter to be used between name, namespace, stage, etc. | string | "-" | no |
| enabled | Set to false to prevent the module from creating any resources | bool | true | no |
| kms\_key\_arn | The server-side encryption key that is used to protect your backups | string | null | no |
| name | Solution name, e.g. 'app' or 'cluster' | string | n/a | yes |
| namespace | Namespace, which could be your organization name, e.g. 'eg' or 'cp' | string | "" | no |
| schedule | A CRON expression specifying when AWS Backup initiates a backup job | string | null | no |
| stage | Stage, e.g. 'prod', 'staging', 'dev', or 'test' | string | "" | no |
| start\_window | The amount of time in minutes before beginning a backup. Minimum value is 60 minutes | number | null | no |
| tags | Additional tags (e.g. map('BusinessUnit,XYZ) | map(string) | {} | no |