

AWS Backup

×

My account

Dashboard

Backup vaults

Backup Vault Lock New

Backup plans

Protected resources

Jobs

Legal holds New

Settings

External resources

Gateways New


Hypervisors

AWS Backup > Dashboard

Dashboard


Info

With the dashboard, create scheduled or on-demand backups of your AWS resources. Manage and monitor AWS Backup activity.

 **Backup plan**


A Backup plan specifies the backup schedule, backup retention rules, and lifecycle rules for your backups.

Create backup plan

 **On-demand backup**

Create a backup of an AWS resource immediately then set lifecycle and retention rules.

Create on-demand backup

 **Frameworks**

Continuously evaluate the compliance of your backup activity with your defined policies.

Get started with frameworks

Job metrics

Copy jobs

Restore jobs

Backup jobs

AWS Backup > Protected resources > Create on-demand backup

Create on-demand backup

Info

Settings

Resource type

Instance ID

EC2

i-08775439128e8565c

↺

Backup window

☒ Create backup now

Starts within 1 hour.

☐ Customize backup window

Retention period

Info

Days

40

Create a new backup vault and select custom IAM role which was created for backup service

Backup vault [Info](#)

Specify the Backup vault this backup is organized in.

Default

Create new Backup vault

IAM role [Info](#)

Specify the IAM role that AWS Backup will assume when creating and managing backups on your behalf.

☐ Default role

If the AWS Backup default role is not present, one will be created for you with the correct permissions.

☒ Choose an IAM role

Role name

Choose an IAM role

Create a new IAM role for aws Backup service:

Identity and Access Management (IAM)

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

IAM > Roles

Roles (40) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Create role

Delete

<input type="checkbox"/>	Role name	Trusted entities
<input type="checkbox"/>	AWSDataLifecycleManagerDefaultRole	AWS Service: dlm
<input type="checkbox"/>	AWSServiceRoleForAmazonGuardDuty	AWS Service: guardduty (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForAmazonGuardDutyMalwareProtection	AWS Service: malware-protection.guardduty (Serv
<input type="checkbox"/>	AWSServiceRoleForAmazonInspector	AWS Service: inspector (Service-Linked Role)

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Select trusted entity [Info](#)

Trusted entity type

☒ **AWS service**

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

☐ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **Lambda**

Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

AWS Backup

☒ **AWS Backup**

Allows AWS Backup to access AWS resources on your behalf based on the permissions you define.

Cancel

Next

AmazonEC2FullAccess
AWSBackupServiceRolePolicyForBackup
AWSBackupServiceRolePolicyForRestores

Permissions policies (3) Info

You can attach up to 10 managed policies.

Refresh

Simulate

Remove

Add permissions ▼

Q

Filter policies by property or policy name and press enter.

< 1 >

⚙

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	<div><div>+</div><div>AmazonEC2FullAccess</div></div>	AWS managed	Provides full access
<input type="checkbox"/>	<div><div>+</div><div>AWSBackupServiceRolePolicyForBackup</div></div>	AWS managed	Provides AWS Backi
<input type="checkbox"/>	<div><div>+</div><div>AWSBackupServiceRolePolicyForRestores</div></div>	AWS managed	Provides AWS Backi

IAM > Roles > Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Seko-Prod-Backup-role

Maximum 64 characters. Use alphanumeric and '+=, @-_' characters.

Description

Add a short explanation for this role.

Allows AWS Backup to access AWS resources on your behalf based on the permissions you define.

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.