

Hands-on tutorials

Amazon RDS Backup & Restore Using AWS Backup



Amazon RDS Backup & Restore Using AWS Backup: Hands-on tutorials

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Amazon RDS Backup & Restore Using AWS Backup	i
Overview	1
What you will accomplish	1
Prerequisites	2
Implementation	2
Additional resources: Working with Amazon RDS and Amazon Aurora	34
Conclusion	34

Amazon RDS Backup & Restore Using AWS Backup

AWS experience	Intermediate
Time to complete	10 minutes
Cost to complete	Free (Amazon RDS Free Tier)
Services used	AWS Backup Amazon Relational Database Service (Amazon RDS)

Overview

[AWS Backup](#) enables you to centralize and automate data protection across AWS services. AWS Backup is a fully managed, policy-based service that simplifies data protection at scale. The service is ideal for use cases such as regulatory compliance obligations, business policies for data protection, and business continuity goals.

In this how-to guide, we will use the AWS Management Console to set up automated backups of select AWS services using Amazon Relational Database Service (Amazon RDS), restore a backup, and clean up our resources to avoid unexpected costs. See [this list](#) for all the AWS and third-party services supported by AWS Backup. When going to production, remember to set up the correct schedules and retention management, and to monitor your costs.

What you will accomplish

- Create an on-demand backup job of an Amazon RDS database
- Use a backup plan to back up Amazon RDS resources - using a backup plan within AWS Backup, you can automate your backups on a schedule
- Add resources to an existing backup plan using tags
- Restore a backup

Prerequisites

You will need the following resources or permissions to proceed with this how-to guide:

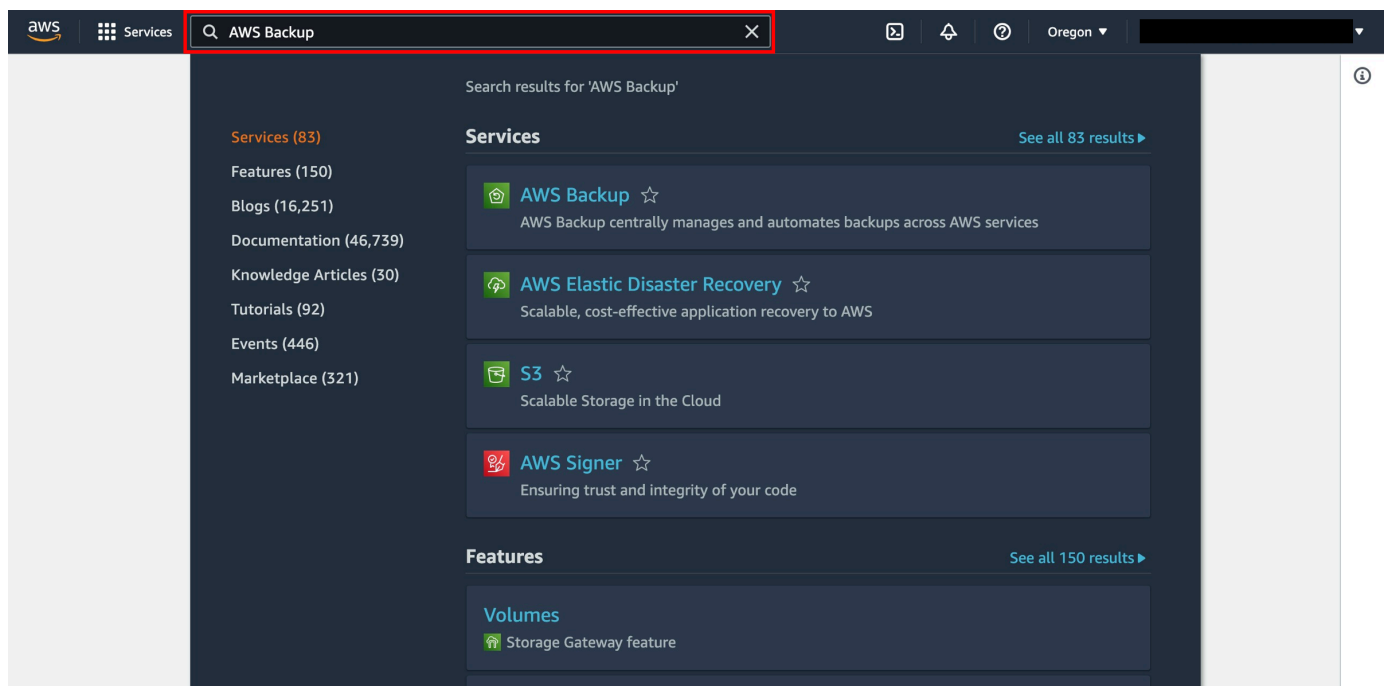
- An [AWS account](#). For more information on using AWS Backup for the first time, view the [AWS Backup Developer Guide](#).
- One or more Amazon RDS databases (including those that are free tier eligible). For the pricing of databases not in the free tier, refer to [Amazon RDS Pricing](#). For AWS Backup pricing, refer to [AWS Backup Pricing](#).
- IAM roles used by AWS Backup to create a backup of the Amazon RDS database.
- If a subsequent role is not created, then the default IAM role can be used - AWSBackupDefaultRole

Implementation

Step 1: Configure an on-demand AWS Backup job of an Amazon RDS database

1. Open the AWS Backup console

Log in to the [AWS Management Console](#), and open the [AWS Backup console](#).



2. Configure the services used with AWS Backup

On the navigation pane on the left side of the [AWS Backup console](#), under **My account**, choose **Settings**.

The screenshot shows the AWS Backup console interface. On the left, the navigation pane is open to 'Settings' under the 'My account' section. The main content area displays the 'AWS Backup' title and a large heading: 'AWS Backup centrally manages and automates backups across AWS services'. Below this heading is a sub-heading: 'Define Backup plans, schedule backups, automate backup retention management, centrally monitor backup activity, and restore backups.' To the right, there is a 'Create a Backup plan' section with a 'Create Backup plan' button. Below that is a 'Pricing' section with a link to the 'AWS Backup pricing guide'.

3. Configure resources

On the **Service opt-in** page, choose **Configure resources**.

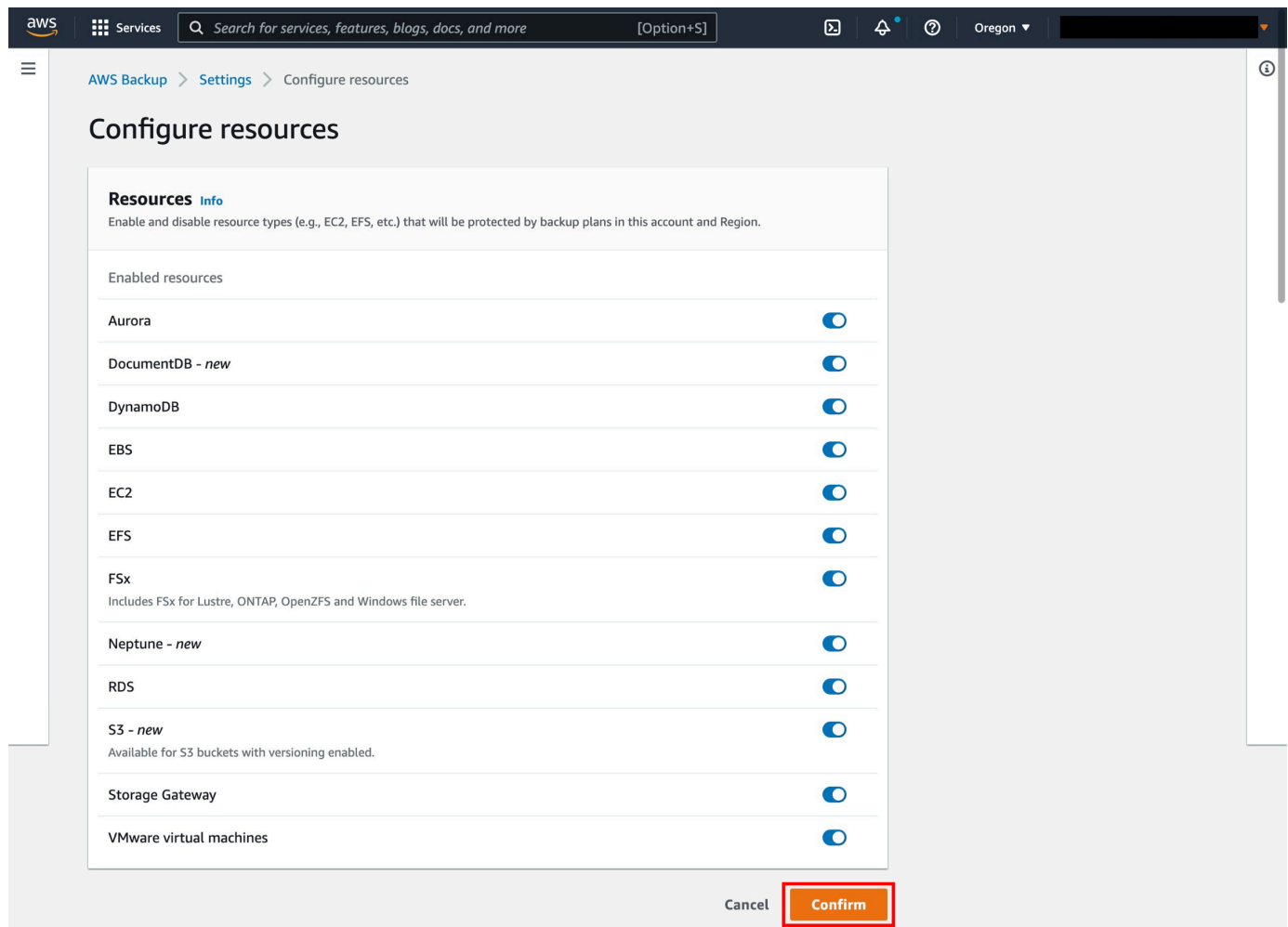
The screenshot shows the 'Service opt-in' page in the AWS Backup console. The left navigation pane is open to 'Settings' under 'My account'. The main content area features a 'Service opt-in' heading with an 'Info' link. Below the heading is a paragraph explaining the purpose of the page. A 'Configure resources' button is highlighted with a red box. Below the button is a table with the following data:

Resource type	Status
Aurora	Enabled
DocumentDB - <i>new</i>	Enabled
DynamoDB	Enabled
EBS	Enabled
EC2	Enabled
EFS	Enabled
FSx Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.	Enabled
Neptune - <i>new</i>	Enabled
RDS	Enabled

4. Select services for backup

On the Configure resources page, use the toggle switches to enable or disable the services used with AWS Backup. Choose Confirm when your services are configured.

- AWS resources that you're backing up should be in the Region you are using for this how-to guide, and resources must all be in the same AWS Region (however, see step 2.11 for information on cross-Region copy). This how-to guide uses the US East (N. Virginia) Region (us-east-1).



5. Create an on-demand backup job of an Amazon RDS database

Back in the [AWS Backup console](#), under **My account** on the left navigation pane, select **Protected resources**.

The resource types that will be protected by backup plans in this account and Region have been updated.

Service opt-in Info
Enable and disable resource types (e.g., EC2, EFS, etc.) that will be protected by backup plans in this account and Region. You will need to enable newly launched resource types before they are protected. Please note that these controls will not apply to backup plans created outside of AWS Backup (i.e., EFS automatic backup).

[Configure resources](#)

Resource type	Status
Aurora	Enabled
DocumentDB - <i>new</i>	Enabled
DynamoDB	Enabled
EBS	Enabled
EC2	Enabled
EFS	Enabled
FSx Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.	Enabled

Feedback Looking for language selection? Find it in the new Unified Settings [↗](#) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

6. Choose Create an on-demand backup

From the dashboard, select the **Create on-demand backup** button.

Protected resources (0) Info
Resources backed up by AWS Backup

[Create on-demand backup](#)

Filter

Resource ID	Resource type	Last backup
Empty resources No resources to display		

Feedback Looking for language selection? Find it in the new Unified Settings [↗](#) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

7. Configure on-demand backup settings

On the **Create on-demand backup** page, choose the following options:

Select the resource type that you want to back up; for example, choose **RDS** for Amazon RDS.


Choose the **database name** or **ID** of the resource that you want to protect; for example, analytics.

Ensure that **Create backup now** is selected. This initiates your backup job immediately and enables you to see your saved resource sooner on the **Protected resources** page.

Select the desired **retention period**. AWS Backup automatically deletes your backups at the end of this period to save storage costs for you.

Choose an existing backup vault. Choosing **Create new Backup vault** opens a new page to create a vault and then returns you to the **Create on-demand backup** page when you are finished.

Under **IAM role**, choose **Default** role.

 **Note**

If the AWS Backup Default role is not present in your account, then an AWS Backup Default role is created with the correct permissions.

Select the **Create on-demand backup** button. This takes you to the **Jobs** page, where you will see a list of jobs.

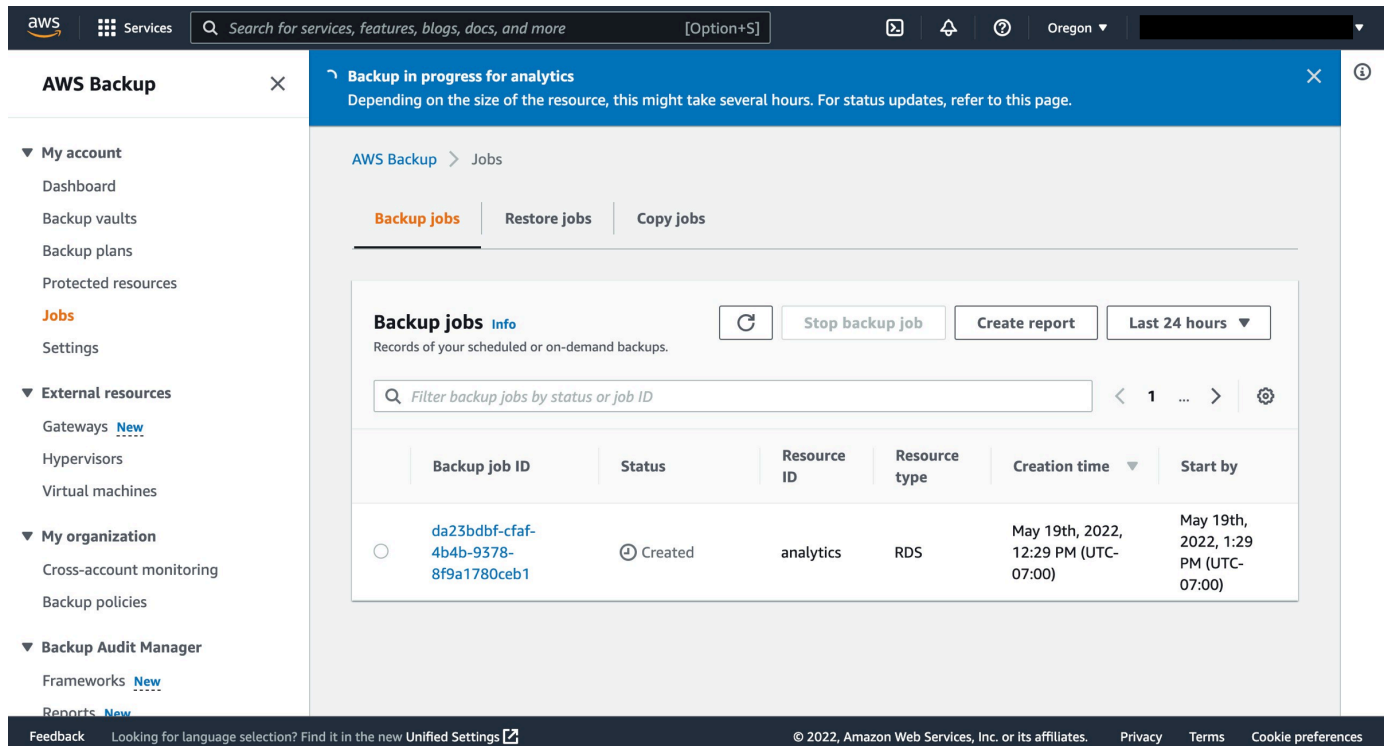
The screenshot shows the AWS Backup console interface for creating an on-demand backup. The breadcrumb navigation is "AWS Backup > Protected resources > Create on-demand backup". The main heading is "Create on-demand backup" with an "Info" link. The settings are organized into sections:

- Settings**
 - Resource type:** RDS (dropdown)
 - Database name:** analytics (dropdown) with a refresh icon.
 - Backup window:** Create backup now (Starts within 1 hour), Customize backup window.
 - Retention period:** Always (dropdown).
 - Backup vault:** Default (dropdown) with a "Create new Backup vault" button.
 - IAM role:** Default role (Specify the IAM role that AWS Backup will assume when creating and managing backups on your behalf. If the AWS Backup default role is not present, one will be created for you with the correct permissions.), Choose an IAM role.
 - Tags added to recovery points:** AWS Backup copies tags from the protected resource to the recovery point upon creation. You can specify additional tags to add to the recovery point.

At the bottom right, there are two buttons: "Cancel" and "Create on-demand backup" (highlighted with a red box).

8. View the backup job details

Choose the **Backup job ID** for the resource that you chose to back up to see the details of that job.



The screenshot shows the AWS Backup console interface. At the top, there's a navigation bar with the AWS logo, 'Services' menu, a search bar, and regional settings for 'Oregon'. A blue banner at the top right indicates 'Backup in progress for analytics' with a note: 'Depending on the size of the resource, this might take several hours. For status updates, refer to this page.'

The left sidebar contains a navigation menu with categories: 'My account' (Dashboard, Backup vaults, Backup plans, Protected resources, **Jobs**, Settings), 'External resources' (Gateways, Hypervisors, Virtual machines), 'My organization' (Cross-account monitoring, Backup policies), and 'Backup Audit Manager' (Frameworks, Reports).

The main content area is titled 'Backup in progress for analytics' and shows 'Jobs' for 'analytics'. It has tabs for 'Backup jobs', 'Restore jobs', and 'Copy jobs'. Below the tabs, there's a 'Backup jobs Info' section with a refresh button, 'Stop backup job', 'Create report', and a filter for 'Last 24 hours'. A search bar allows filtering by status or job ID. A table lists the backup jobs:

Backup job ID	Status	Resource ID	Resource type	Creation time	Start by
da23bdbf-cfaf-4b4b-9378-8f9a1780ceb1	Created	analytics	RDS	May 19th, 2022, 12:29 PM (UTC-07:00)	May 19th, 2022, 1:29 PM (UTC-07:00)

At the bottom, there's a footer with 'Feedback', a link for language selection, and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for Privacy, Terms, and Cookie preferences.

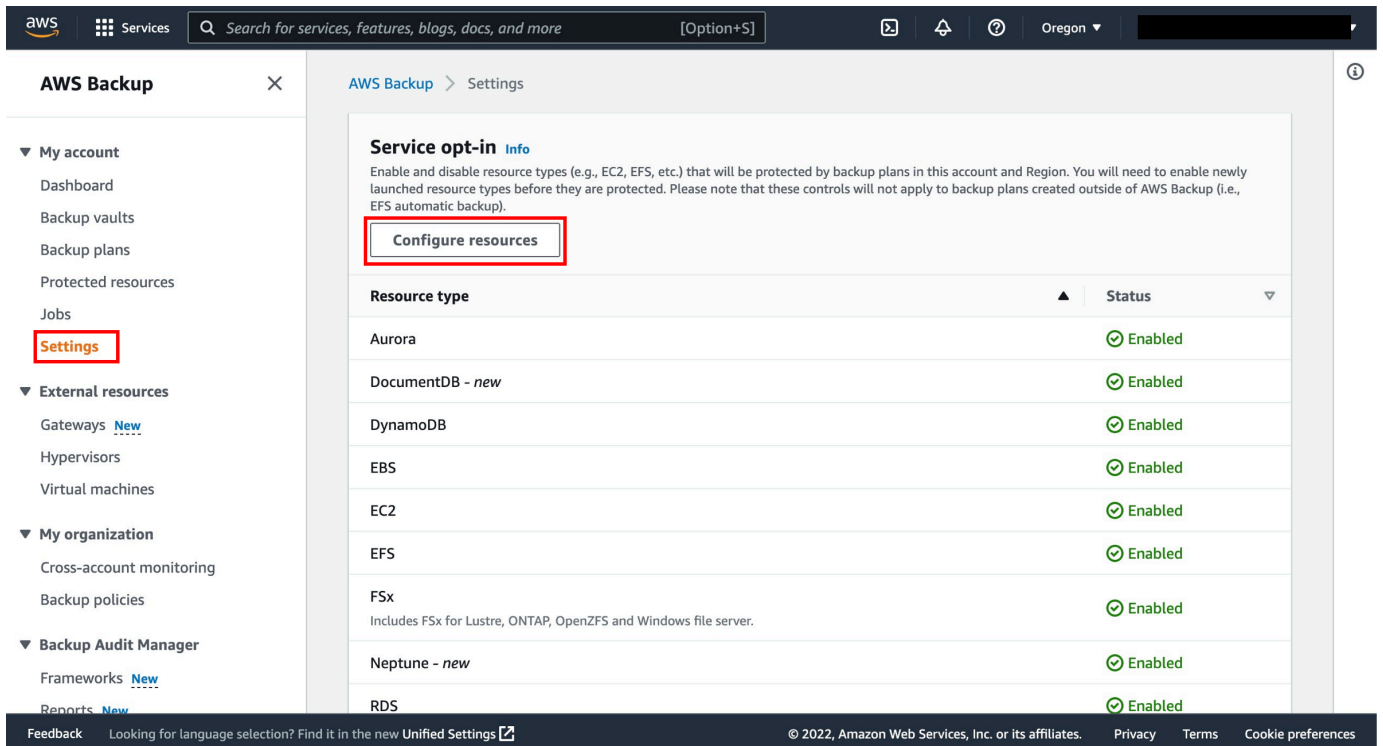
Step 2: Configure automatic AWS Backup jobs of an Amazon RDS database

1. Configure the services used with AWS Backup

Back on the left navigation pane in the AWS Backup console, under **My account**, choose **Settings**.

2. Configure resources

On the **Service opt-in** page, choose **Configure resources**.



Service opt-in [Info](#)

Enable and disable resource types (e.g., EC2, EFS, etc.) that will be protected by backup plans in this account and Region. You will need to enable newly launched resource types before they are protected. Please note that these controls will not apply to backup plans created outside of AWS Backup (i.e., EFS automatic backup).

[Configure resources](#)

Resource type	Status
Aurora	Enabled
DocumentDB - <i>new</i>	Enabled
DynamoDB	Enabled
EBS	Enabled
EC2	Enabled
EFS	Enabled
FSx Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.	Enabled
Neptune - <i>new</i>	Enabled
RDS	Enabled

3. Select services for backup

On the **Configure resources** page, use the toggle switches to enable or disable the services used with AWS Backup. Choose **Confirm** when your services are configured.

AWS resources that you're backing up should be in the Region you are using for this tutorial, and resources must all be in the same AWS Region (however, see step 2.11 for information on cross-Region copy). This tutorial uses the US East (N. Virginia) Region (us-east-1).

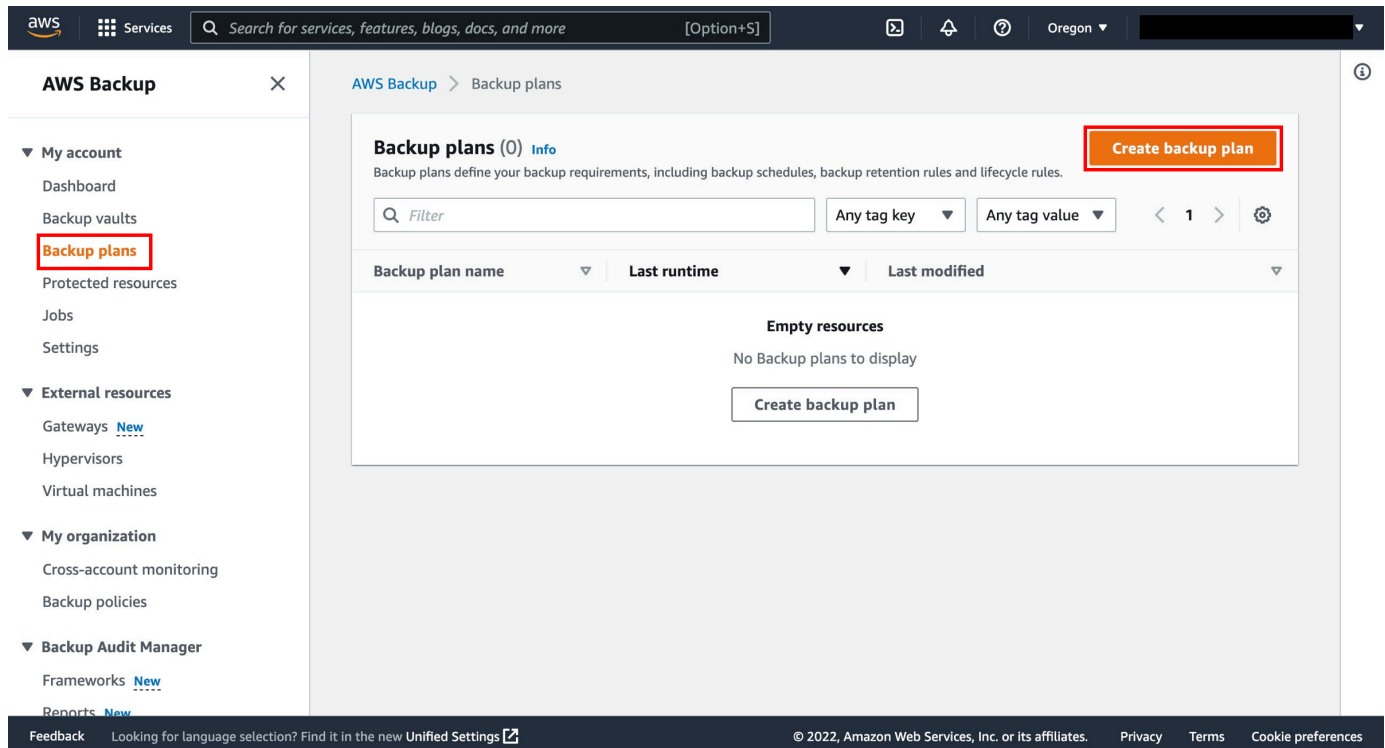
The screenshot shows the AWS Backup console interface. The left navigation pane is open, showing the 'Settings' option under 'My account'. The main content area is titled 'Configure resources' and contains a 'Resources Info' section. Below this, there is a list of resources with toggle switches to enable or disable them. The resources listed are:

Resource	Enabled
Aurora	<input checked="" type="checkbox"/>
DocumentDB - <i>new</i>	<input checked="" type="checkbox"/>
DynamoDB	<input checked="" type="checkbox"/>
EBS	<input checked="" type="checkbox"/>
EC2	<input checked="" type="checkbox"/>
EFS	<input checked="" type="checkbox"/>
FSx <small>Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.</small>	<input checked="" type="checkbox"/>
Neptune - <i>new</i>	<input checked="" type="checkbox"/>
RDS	<input checked="" type="checkbox"/>
S3 - <i>new</i> <small>Available for S3 buckets with versioning enabled.</small>	<input checked="" type="checkbox"/>
Storage Gateway	<input checked="" type="checkbox"/>
VMware virtual machines	<input checked="" type="checkbox"/>

At the bottom right of the page, there are two buttons: 'Cancel' and 'Confirm'. The 'Confirm' button is highlighted with a red border.

4. Configure a backup plan

In the AWS Backup console, select **Backup plans** on the left navigation pane under **My account**, and then **Create backup plan**.



5. Create a new backup plan

AWS Backup provides three ways to get started using the AWS Backup console but for this how-to guide, select **Build a new plan**:

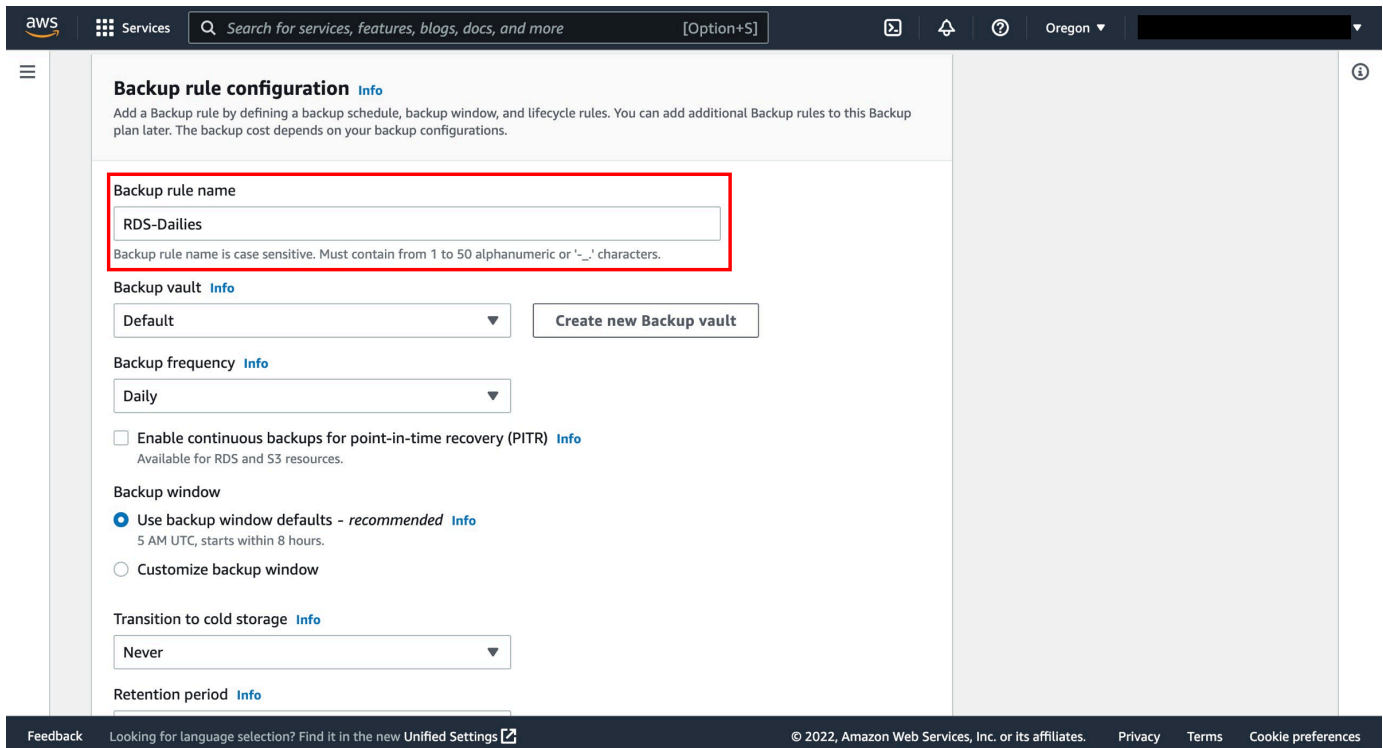
- **Start with a template** — You can create a new backup plan based on a template provided by AWS Backup. Be aware that backup plans created by AWS Backup are based on backup best practices and common backup policy configurations. When you select an existing backup plan to start from, the configurations from that backup plan are automatically populated for your new backup plan. You can then change any of these configurations according to your backup requirements.
- **Build a new plan** — You can create a new backup plan by specifying each of the backup configuration details, as described in the next section. You can choose from the recommended default configurations.
- **Define a plan using JSON** - You can modify the JSON expression of an existing backup plan or create a new expression.

Backup plan name - You must provide a unique backup plan name. If you try to create a backup plan that is identical to an existing plan, you get an *AlreadyExistsException* error. For this how-to guide, enter **RDS-webapp**.

The screenshot shows the AWS Backup console interface for creating a backup plan. The breadcrumb navigation is 'AWS Backup > Backup plans > Create backup plan'. The main heading is 'Create backup plan' with an 'Info' link. Under the 'Start options' section, there are three radio button options: 'Start with a template', 'Build a new plan' (which is selected and highlighted with a red box), and 'Define a plan using JSON'. Below this, the 'Backup plan name' field is labeled 'Name your backup plan' and contains the text 'RDS-webapp', which is also highlighted with a red box. A note below the field states: 'Backup plan name is case sensitive. Must contain from 1 to 50 alphanumeric or '-' characters.' There is also a section for 'Tags added to backup plan' with a right-pointing arrow. At the bottom, the 'Backup rule configuration' section is partially visible, with a note: 'Add a Backup rule by defining a backup schedule, backup window, and lifecycle rules. You can add additional Backup rules to this Backup plan later. The backup cost depends on your backup configurations.'

6. Enter a backup rule name

Backup rule name - Backup plans are composed of one or more backup rules. Backup rule names are case sensitive. They must contain from 1 to 63 alphanumeric characters or hyphens. For this how-to guide, enter **RDS-Dailies**.



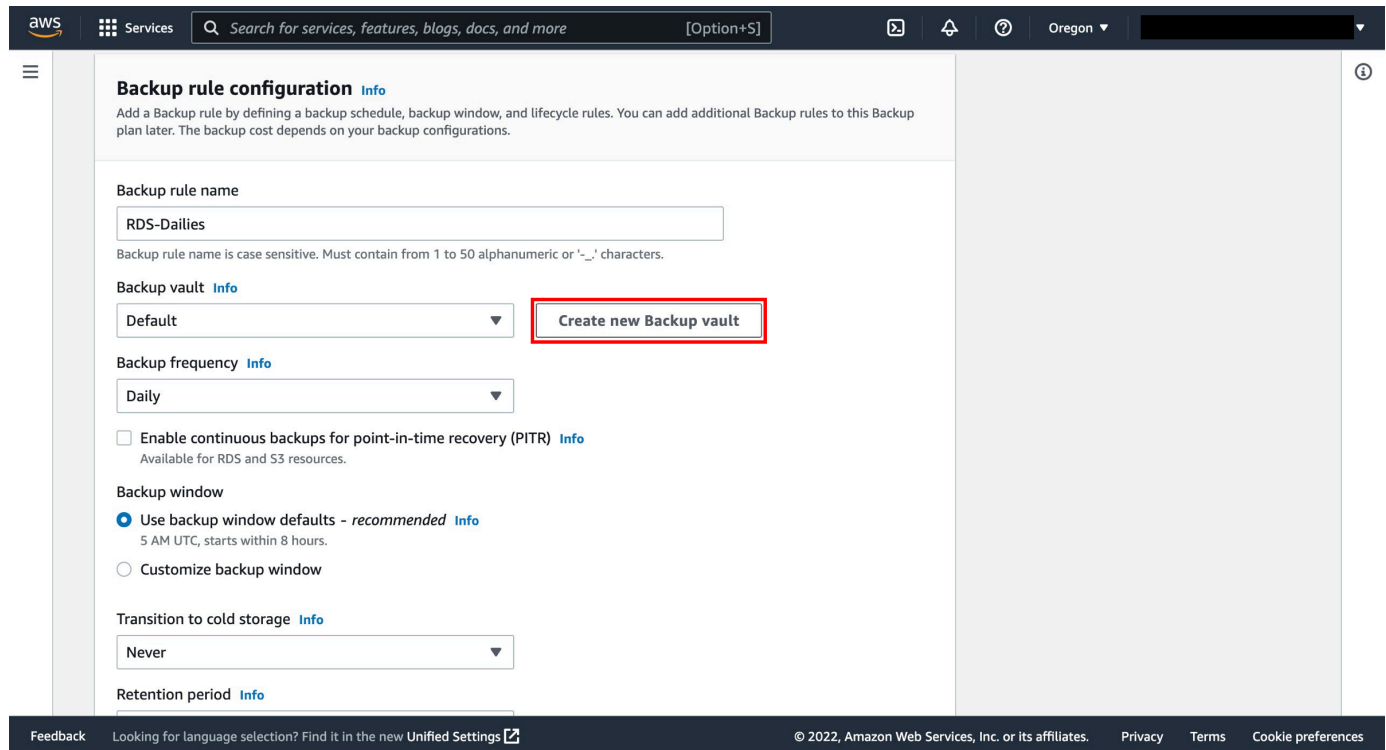
7. Create a backup vault

Backup vault - A backup vault is a container to organize your backups in. Backups created by a backup rule are organized in the backup vault that you specify in the backup rule. 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. You can also add tags to backup vaults to help you organize them. If you don't want to use the default vault, you can create your own.

Create new backup vault - Instead of using the default backup vault that is automatically created for you in the AWS Backup console, you can create specific backup vaults to save and organize groups of backups in the same vault.

- a. To create a backup vault, choose **Create new Backup vault**.
- b. Enter a name for your backup vault. You can name your vault to reflect what you will store in it, or to make it easier to search for the backups you need. For example, you could name it **FinancialBackups**.
- c. Select an AWS KMS key. You can use either a key that you already created or select the default AWS Backup master key.
- d. Optionally, add tags that will help you search for and identify your backup vault.

e. Select **Create Backup vault** button.



8. Configure the backup vault

Create new backup vault - Instead of using the default backup vault that is automatically created for you in the AWS Backup console, you can create specific backup vaults to save and organize groups of backups in the same vault.

- To create a backup vault, choose **Create new Backup vault**.
- Enter a name for your backup vault. You can name your vault to reflect what you will store in it, or to make it easier to search for the backups you need. For example, you could name it **FinancialBackups**.
- Select an AWS KMS key. You can use either a key that you already created or select the default AWS Backup master key.
- Optionally, add tags that will help you search for and identify your backup vault.
- Select **Create Backup vault** button.

Create Backup vault

General

Backup vault name

 Backup vault name is case sensitive. Must contain from 2 to 50 alphanumeric or '-' characters.

Encryption key [Info](#)

Description	Account	Key ID	Status
Default key that protects my Backup data when no other key is defined	This account		Enabled

Backup vault tags - optional
 Tags specified here help organize and track your Backup vault

No tags.

[Add new tag](#)
 You can add up to 50 more tags.

[Cancel](#) [Create Backup vault](#)

9. Configure backup schedule

Backup frequency - The backup frequency determines how often a backup is created. You can choose a frequency of every 12 hours, daily, weekly, or monthly. When selecting weekly, you can specify which days of the week you want backups to be taken. When selecting monthly, you can choose a specific day of the month.

Enable continuous backups for point-in-time recovery - With continuous backups, you can perform point-in-time restores (PITR) by choosing when to restore, down to the second. The most time that can elapse between the current state of your workload and your most recent point-in-time restore is 5 minutes. You can store continuous backups for up to 35 days. If you do not enable continuous backups, AWS Backup takes snapshot backups for you.

Backup window - Backup windows consist of the time that the backup window begins and the duration of the window in hours. The default backup window is set to start at 5 AM UTC (Coordinated Universal Time) and lasts 8 hours.

Backup rule configuration [Info](#)

Add a Backup rule by defining a backup schedule, backup window, and lifecycle rules. You can add additional Backup rules to this Backup plan later. The backup cost depends on your backup configurations.

Backup rule name

RDS-Dailies

Backup rule name is case sensitive. Must contain from 1 to 50 alphanumeric or '-', '_' characters.

Backup vault [Info](#)

Default [Create new Backup vault](#)

Backup frequency [Info](#)

Daily

Enable continuous backups for point-in-time recovery (PITR) [Info](#)

Available for RDS and S3 resources.

Backup window

Use backup window defaults - *recommended* [Info](#)

5 AM UTC, starts within 8 hours.

Customize backup window

Transition to cold storage [Info](#)

Never

Retention period [Info](#)

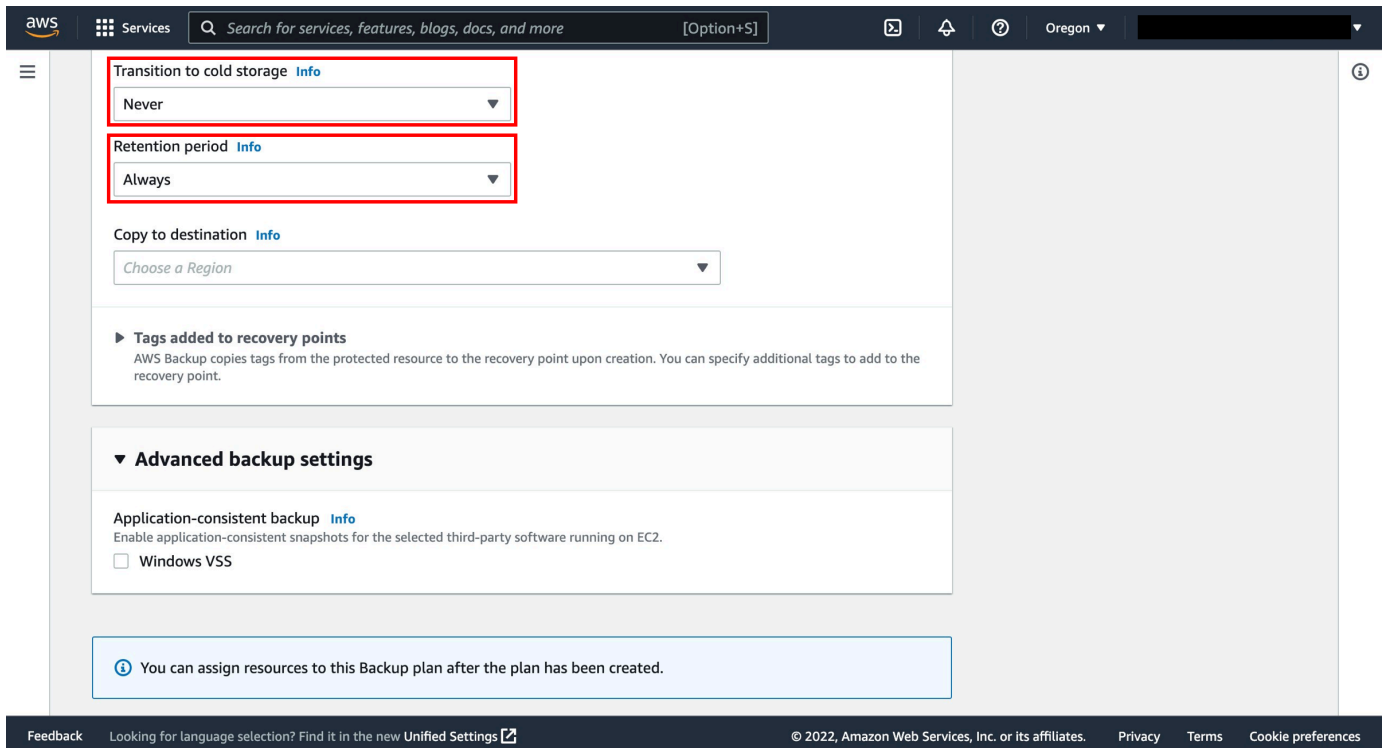
Feedback [Looking for language selection? Find it in the new Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

10. Configure retention settings

Transition to cold storage - Currently only Amazon EFS file system backups can be transitioned to cold storage. The cold storage expression is ignored for the backups of Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Aurora, Amazon DynamoDB, and AWS Storage Gateway.

Retention period - AWS Backup automatically deletes your backups at the end of this period to save storage costs for you. AWS Backup can retain snapshots between 1 day and 100 years (or indefinitely, if you do not enter a retention period), and continuous backups between 1 and 35 days.



The screenshot shows the AWS Backup console configuration page for a backup plan. The top navigation bar includes the AWS logo, a search bar, and the region 'Oregon'. The main content area is divided into several sections:

- Transition to cold storage:** A dropdown menu set to 'Never'.
- Retention period:** A dropdown menu set to 'Always'.
- Copy to destination:** A dropdown menu with the text 'Choose a Region'.
- Tags added to recovery points:** A section explaining that AWS Backup copies tags from the protected resource to the recovery point upon creation.
- Advanced backup settings:** A section with a collapsed arrow and the following options:
 - Application-consistent backup:** A section with the text 'Enable application-consistent snapshots for the selected third-party software running on EC2.' and a checkbox for 'Windows VSS' which is currently unchecked.

At the bottom of the configuration area, there is a blue information box with a question mark icon and the text: 'You can assign resources to this Backup plan after the plan has been created.'

The footer of the console includes a 'Feedback' link, a link to 'Looking for language selection? Find it in the new Unified Settings', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for 'Privacy', 'Terms', and 'Cookie preferences'.

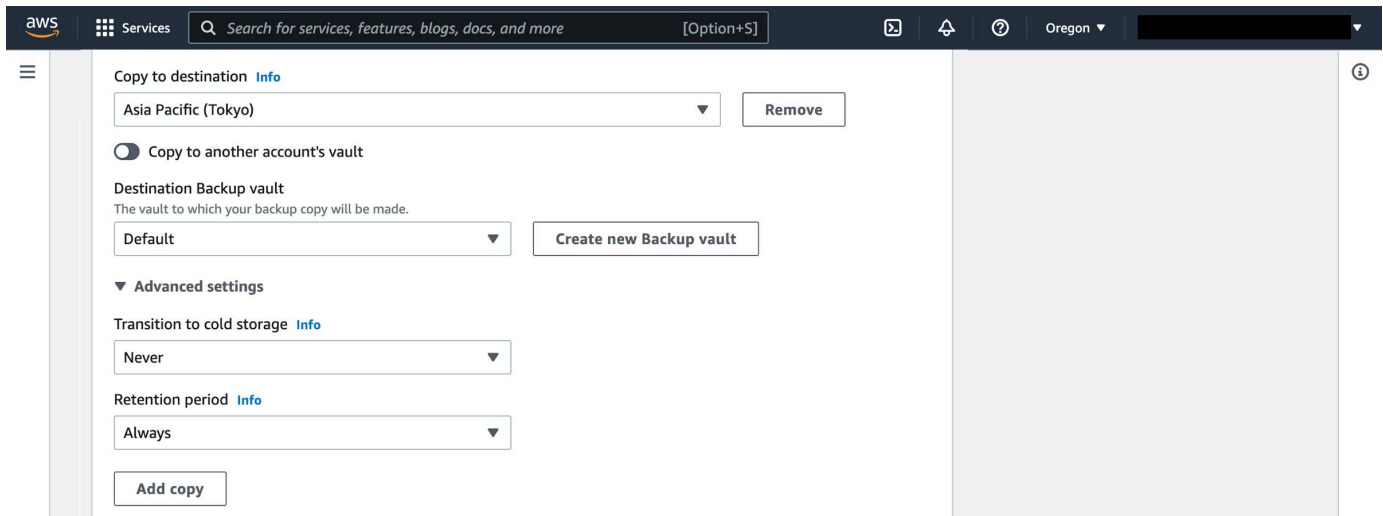
11. (Optional) Copy a backup to multiple regions

Copy to destination - As part of your backup plan, you can optionally create a backup copy in another AWS Region. Using AWS Backup, you can copy backups to multiple AWS Regions on-demand, or automatically as part of a scheduled backup plan. Cross-Region Replication (CRR) is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data. When you define a backup copy, you configure the following options:

- Copy to destination - The destination Region for the backup copy.
- Destination backup vault - The destination backup vault for the copy.
- (Advanced Settings) Transition to cold storage
- (Advanced Settings) Retention period

Note

Cross-Region Copy incurs additional data transfer costs. You can refer to the [AWS Backup pricing page](#) for more information.



12. Create the plan

Tags added to recovery points - The tags that you list here are automatically added to backups when they are created.

Advanced backup settings - Enables application-consistent backups for third-party applications that are running on Amazon EC2 instances. Currently, AWS Backup supports Windows VSS backups. This is only applicable for Windows EC2 Instances running SQL Server or Exchange databases.

Choose **Create plan**.

The screenshot shows the AWS Backup console interface for creating a backup plan. The top navigation bar includes the AWS logo, a search bar, and the region 'Oregon'. The main content area is divided into several sections:

- Tags added to recovery points:** This section explains that AWS Backup copies tags from the protected resource to the recovery point. It states 'No tags.' and provides an 'Add new tag' button. A note below indicates 'You can add up to 50 more tags.'
- Advanced backup settings:** This section includes 'Application-consistent backup' with an 'Info' link and a note: 'Enable application-consistent snapshots for the selected third-party software running on EC2.' Below this is a checkbox for 'Windows VSS'.
- Informational messages:** Two light blue boxes provide additional information: 'You can assign resources to this Backup plan after the plan has been created.' and 'You can add more rules to this Backup plan after the plan has been created.'
- Buttons:** At the bottom right, there are 'Cancel' and 'Create plan' buttons.

The footer of the console includes a 'Feedback' link, a language selection link, and copyright information: '© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

13. Assign resources

When you assign a resource to a backup plan, that resource is backed up automatically according to the backup plan. The backups for that resource are managed 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.

Select the created backup plan, and select the **Assign resources** button.

The screenshot shows the AWS Backup console for a backup plan named 'RDS-webapp'. The left sidebar contains navigation options like 'My account', 'External resources', 'My organization', and 'Backup Audit Manager'. The main content area is divided into three sections:

- Summary:** A table with the following data:

Backup plan name	Version ID	Last modified	Last runtime
RDS-webapp	ZGZmYWI5NjAtODVjMl00ZGYyLWFmODEtMTZjMTBiMTlNTQ0	May 19th, 2022, 8:48 PM (UTC-07:00)	May 19th, 2022, 10:13 PM (UTC-07:00)
Backup plan ID			
59653e78-47d4-41b1-bd0c-5f368f708465			
- Backup rules (1):** A table with one rule named 'RDS-Dailies', using the 'Default' backup vault and 'Default' destination backup vault. Buttons for 'Edit', 'Delete', and 'Add Backup rule' are present.
- Resource assignments (0):** A section with a 'Delete' button and a red-bordered 'Assign resources' button.

14. Enter an assignment name

Resource assignment name - Provide a resource assignment name.

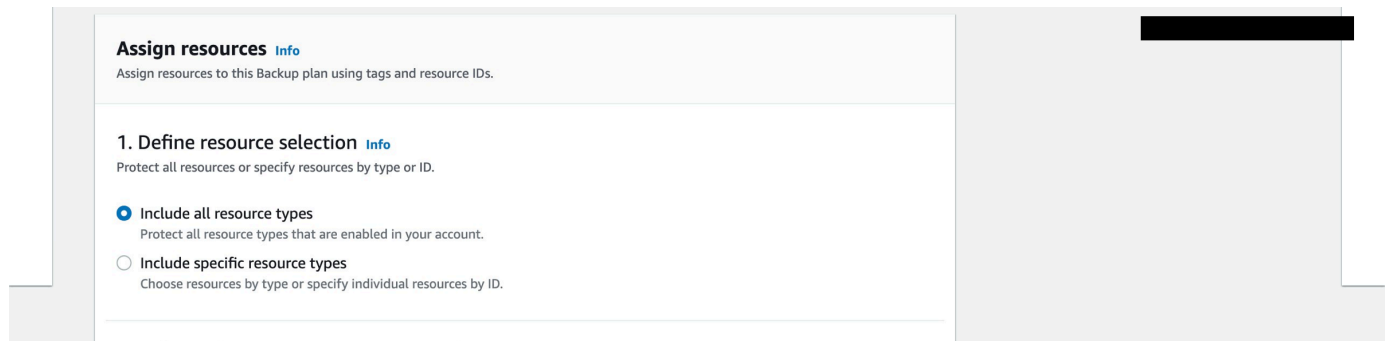
IAM role - When creating a tag-based backup plan, if you choose a role other than **Default role**, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission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

The screenshot shows the 'Assign resources' configuration page in the AWS Backup console. The breadcrumb trail is 'AWS Backup > Backup plans > RDS-webapp > Assign resources'. The page has a 'General' section with the following fields and options:

- Resource assignment name:** A text input field containing 'RDS-DB'. Below it, a note states: 'Resource assignment name is case sensitive. Must contain from 1 to 50 alphanumeric or '-' characters.'
- IAM role:** A radio button selection with two options:
 - Default role** (selected): 'AWS Backup will assume this IAM role when creating and managing recovery points on your behalf. If the AWS Backup default role is not present, one will be created for you with the correct permissions.'
 - Choose an IAM role** (unselected): 'Choose an IAM role'

15. Choose a resource selection type

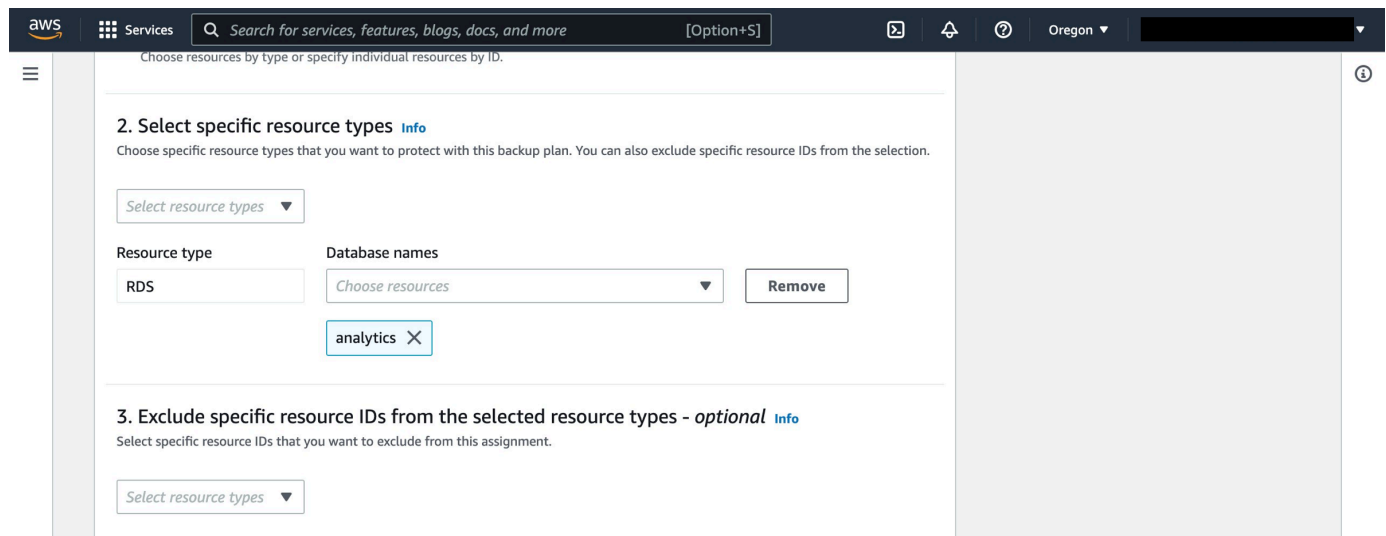
Define resource selection - You can choose to include all resource types or specific resource types.



16. Define resource assignments

For resource ID-based assignment, select **Resource type** and the name of the resource.

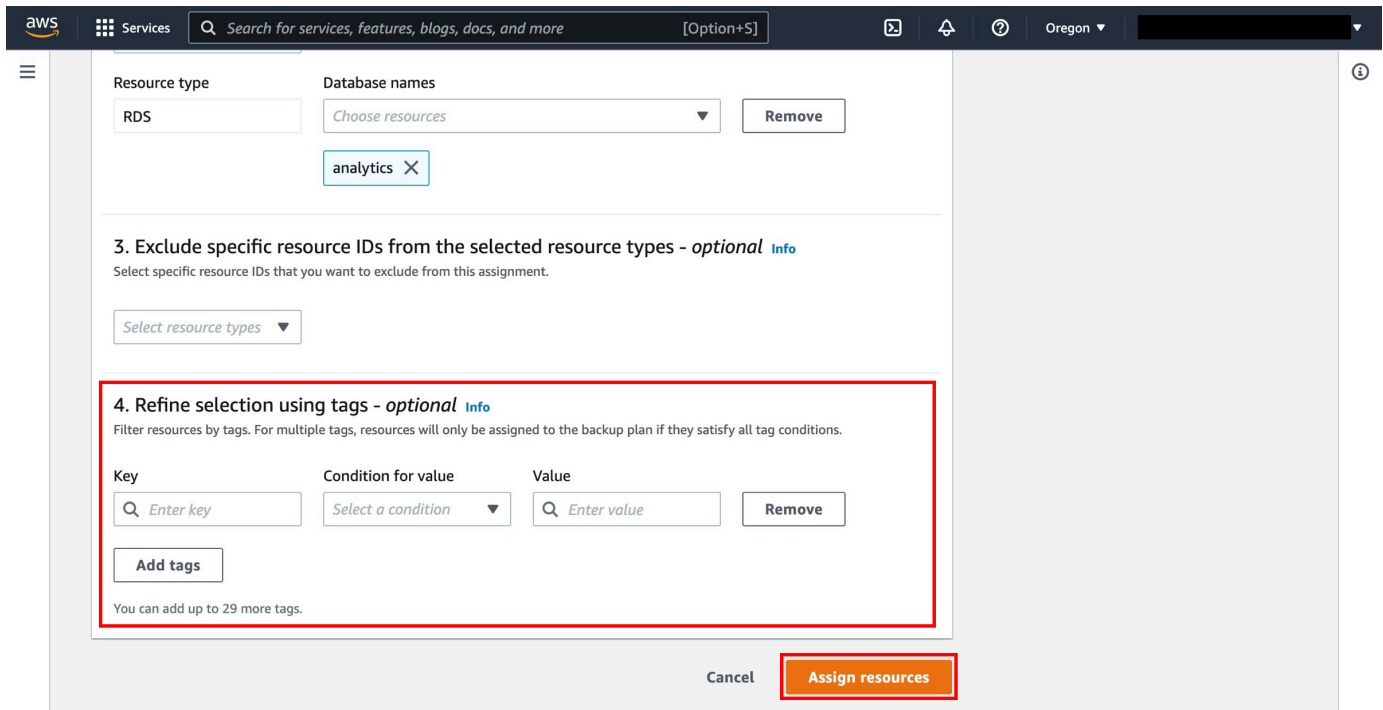
To exclude specific resource IDs, select **Resource type** and the name of the resource.



17. Assign the resources to the backup plan

For tags-based resource assignment, provide the key-value pair of the Amazon RDS database.

Select **Assign resources** and the backup plan has the resources assigned to it.



The screenshot shows the AWS Backup console interface. At the top, there is a search bar with the text "Search for services, features, blogs, docs, and more" and a button labeled "[Option+S]". The region is set to "Oregon".

The main content area is divided into sections:

- Resource type:** A dropdown menu is set to "RDS".
- Database names:** A dropdown menu is set to "Choose resources". A "Remove" button is next to it.
- analytics:** A tag with an "X" icon is shown.
- 3. Exclude specific resource IDs from the selected resource types - optional** [Info](#)
Select specific resource IDs that you want to exclude from this assignment.
A dropdown menu is set to "Select resource types".
- 4. Refine selection using tags - optional** [Info](#)
Filter resources by tags. For multiple tags, resources will only be assigned to the backup plan if they satisfy all tag conditions.

The "4. Refine selection using tags" section is highlighted with a red border. It contains a table with the following structure:

Key	Condition for value	Value	
<input type="text" value="Enter key"/>	<input type="text" value="Select a condition"/>	<input type="text" value="Enter value"/>	<input type="button" value="Remove"/>

Below the table is an "Add tags" button and a note: "You can add up to 29 more tags." At the bottom right, there are "Cancel" and "Assign resources" buttons.

18. View the backup job

Navigate to the [AWS Backup console](#) and the backup jobs will be seen under **Jobs**.

A backup, or recovery point, represents the content of a resource, such as an Amazon Elastic Block Store (Amazon EBS) volume or Amazon RDS database, at a specified time. **Recovery point** is a term that refers generally to the different backups in AWS services, such as Amazon EBS snapshots and Amazon RDS backups. In AWS Backup, recovery points are saved in backup vaults, which you can organize according to your business needs. Each recovery point has a unique ID.

The screenshot shows the AWS Backup console interface. At the top, a green notification bar states: "Resource assignment RDS-DB has been created successfully." The breadcrumb navigation is "AWS Backup > Backup plans > RDS-webapp".

The main content area is titled "RDS-webapp" and includes a "Delete" button and a "View JSON" button. Below this is a "Summary" section with the following details:

Backup plan name	Version ID	Last modified	Last runtime
RDS-webapp	ZGZmYW15NjAtODVjMi00ZGYyLWFmODEtMTZjMTBiMTlNTQ0	May 19th, 2022, 8:48 PM (UTC-07:00)	May 19th, 2022, 10:13 PM (UTC-07:00)
Backup plan ID	59653e78-47d4-41b1-bd0c-5f368f708465		

Below the summary is the "Backup rules (1)" section, which includes an "Add Backup rule" button. The table below shows the existing rule:

Name	Backup vault	Destination Backup vault
<input type="radio"/> RDS-Dailies	Default	Default

The "Resource assignments (1)" section includes an "Assign resources" button. The table below shows the assigned resource:

Name	IAM role ARN	Creation time
<input type="radio"/> RDS-DB	arn:aws:iam::661972857966:role/service-role/AWSBackupDefaultServiceRole	May 19th, 2022, 10:57 PM (UTC-07:00)

Step 3: Restore of an Amazon RDS database using AWS Backup

1. Select the backup

Navigate to the backup vault that was selected in the backup plan and select the latest completed backup.

AWS Backup ×

AWS Backup > Backup vaults > Default

Default

[Manage access](#)

Summary

Backup vault name Default	Creation date April 21st, 2022, 9:28 PM (UTC-07:00)	KMS encryption key ID 80981b2f-a954-48ea-b6ce-c6de46b7f577 ↗
Backup vault ARN arn:aws:backup:us-west-2:661972857966:backup-vault:Default		

Backups (1)

[Refresh](#) [Deselect all](#) [Actions](#)

Filter by resource type, recovery point ID, or source account ID

<input type="checkbox"/>	Recovery point ID	Status	Resource ID	Resource type
<input type="checkbox"/>	awsbackup:job-da23bdbf-cfaf-4b4b-9378-8f9a1780ceb1	Completed	analytics	RDS

Feedback [Looking for language selection? Find it in the new Unified Settings](#) © 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

2. Restore the RDS instance

To restore the database, click on the recovery point ARN and select **Restore**.

AWS Backup > Backup vaults > Default > awsbackup:job-da23bdbf-cfaf-4b4b-9378-8f9a1780ceb1 - RDS

awsbackup:job-da23bdbf-cfaf-4b4b-9378-8f9a1780ceb1 - RDS

[Copy](#) [Delete](#) [Restore](#)

Details

ARN arn:aws:rds:us-west-2:661972857966:snapshot:awsbacku-p:job-da23bdbf-cfaf-4b4b-9378-8f9a1780ceb1	Resource type RDS	Status Completed	Backup type Snapshot
Creation time May 19th, 2022, 12:29 PM (UTC-07:00)	Resource ID analytics	Storage tier Warm	

Backup summary

[Edit](#)

Backup type Manual	Backup vault Default	Backup plan -
-----------------------	-------------------------	------------------

Feedback [Looking for language selection? Find it in the new Unified Settings](#) © 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

3. Review restore configuration

The restore of the ARN will bring you to a **Restore backup** screen that will have Instance specifications and configurations for the Amazon RDS database. Select the **DB engine, License Model, and DB instance class**.

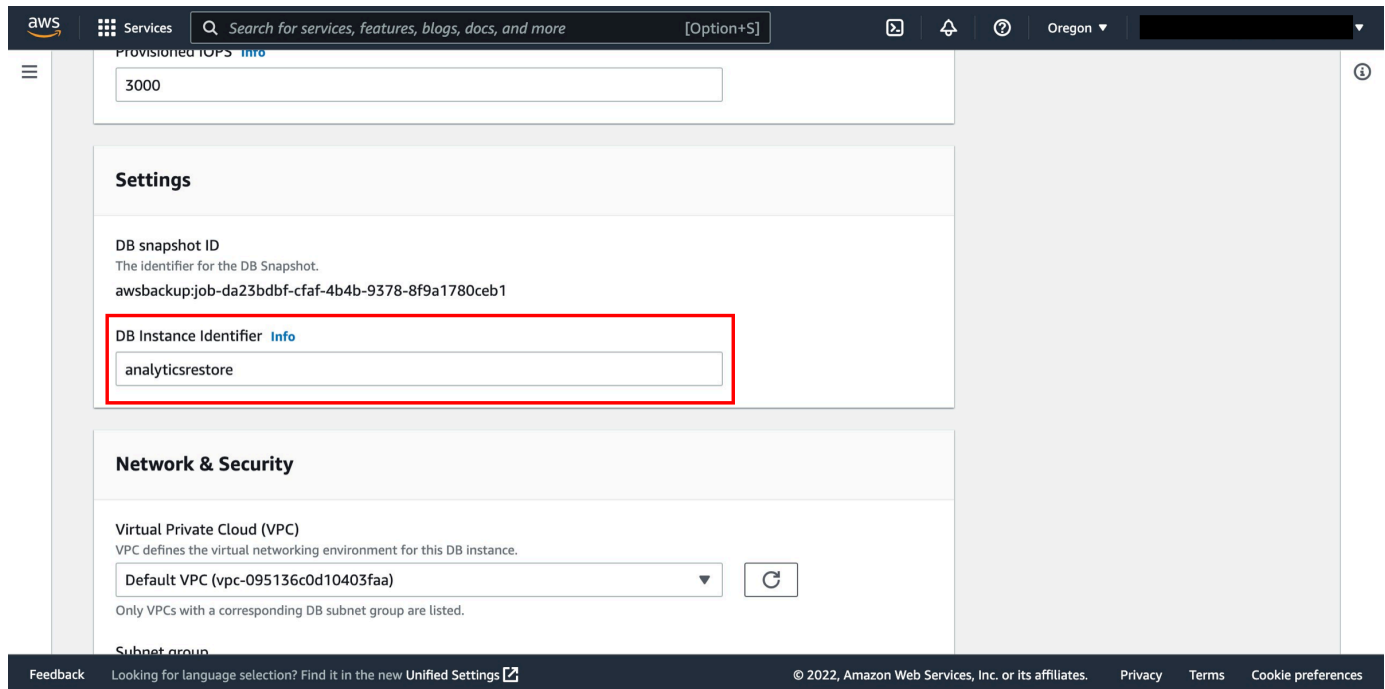
- Multi AZ - Using a Multi-AZ deployment will automatically provision and maintain a synchronous standby replica in a different Availability Zone. Note that you will have to pay for Multi-AZ deployment.
- Storage type - Select **Provisioned IOPS (SSD)**.
- Provisioned IOPS - The requested number of I/O operations per second that the DB instance can support. Enter **3000**.

The screenshot shows the AWS Backup console interface for the 'Restore backup' step. The breadcrumb navigation is 'AWS Backup > Backup vaults > Default > Restore backup'. The main heading is 'Restore backup', followed by a descriptive paragraph: 'You are creating a new DB Instance from a source DB Instance at a specified time. This new DB Instance will have the default DB Security Group and DB Parameter Groups.' Below this is a form titled 'Instance specifications' with the following fields:

- DB engine:** Name of the database engine to be used for this instance. Value: MySQL Community Edition.
- License Model:** License type associated with the database engine. Value: general-public-license.
- DB instance class:** Contains the compute and memory capacity of the DB Instance. Value: db.m4.xlarge — 4 vCPU, 16 GiB RAM.
- Multi AZ:** Specifies if the DB Instance should have a standby deployed in another Availability Zone. Radio buttons for Yes and No. 'No' is selected.
- Storage type:** Info. Value: Provisioned IOPS (SSD).
- Provisioned IOPS:** Info. Value: 3000.

4. Enter a name for the DB instance

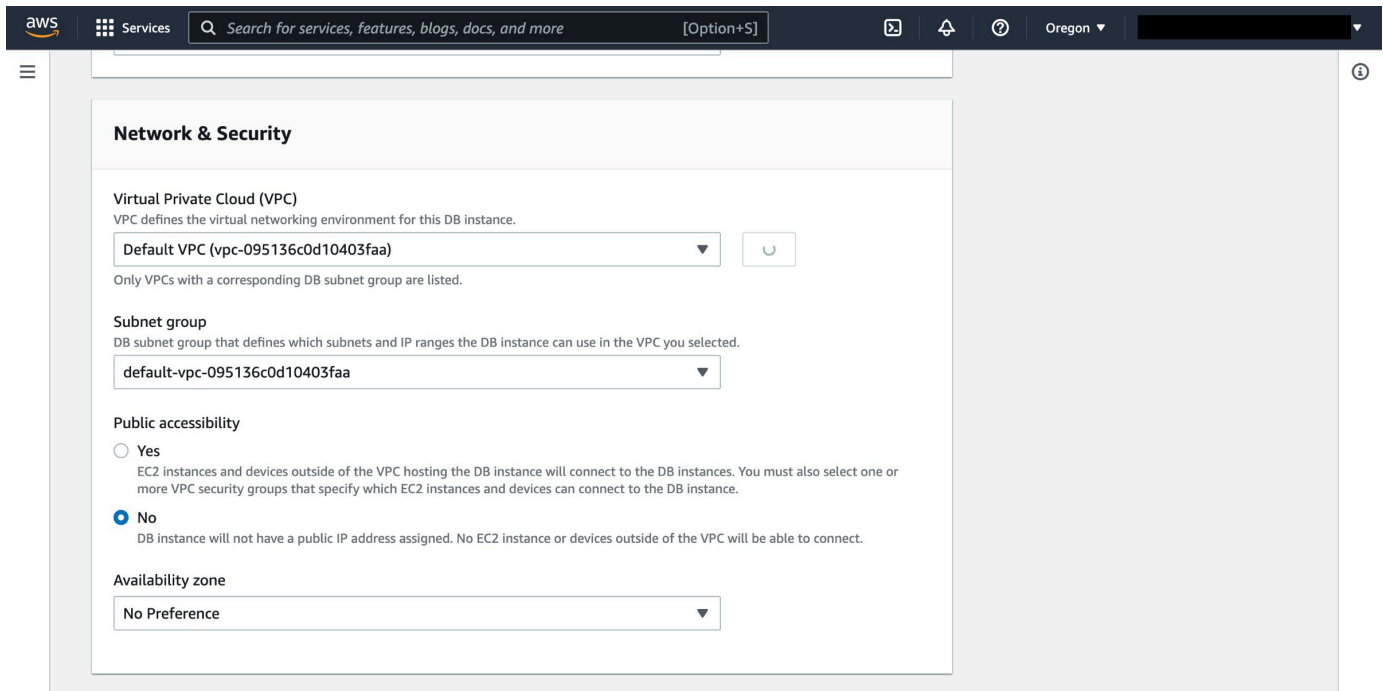
DB Instance Identifier - Type a name for the DB instance that is unique for your account in the Region that you selected. If you're restoring from a DB instance that you deleted after you made the DB snapshot, you can use the name of that DB instance.



5. Configure network and security settings

Select the appropriate network and security settings:

- VPC - Select the VPC where the database needs to be restored to.
- Subnet group - Select the subnet group in the VPC where the database needs to be restored to.
- Public accessibility - You can choose if you need the DB Instances to have a public address or not. If you choose **Yes**, this will allocate an IP address for your database instance so that you can directly connect to the database from your own device.
- **Availability zone** - Choose **No Preference**.



6. Select database options

Select the appropriate database options.

- **Database port** - Leave the default value of **3306**.
- **DB parameter group** - Leave the **default value**.
- **Option Group** - Leave the **default value**. Amazon RDS uses option groups to enable and configure additional features.
- **IAM DB Authentication Enabled** - You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. Select **Enable IAM DB authentication**.

Database options

Database port
Port number on which the database accepts connections.
3306

DB parameter group [Info](#)
default.mysql8.0

Option Group [Info](#)
default:mysql-8-0

IAM DB Authentication Enabled

Enable IAM DB authentication
Manage your database user credentials through AWS IAM users and roles.

Disable

7. Copy tags to snapshots

Copy Tags to Snapshots - Tags can be set on the database instances to be automatically copied to any automated or manual database snapshots that are created from your instances.

Option Group [Info](#)
default:mysql-8-0

IAM DB Authentication Enabled

Enable IAM DB authentication
Manage your database user credentials through AWS IAM users and roles.

Disable

Backup

Copy tags to snapshots

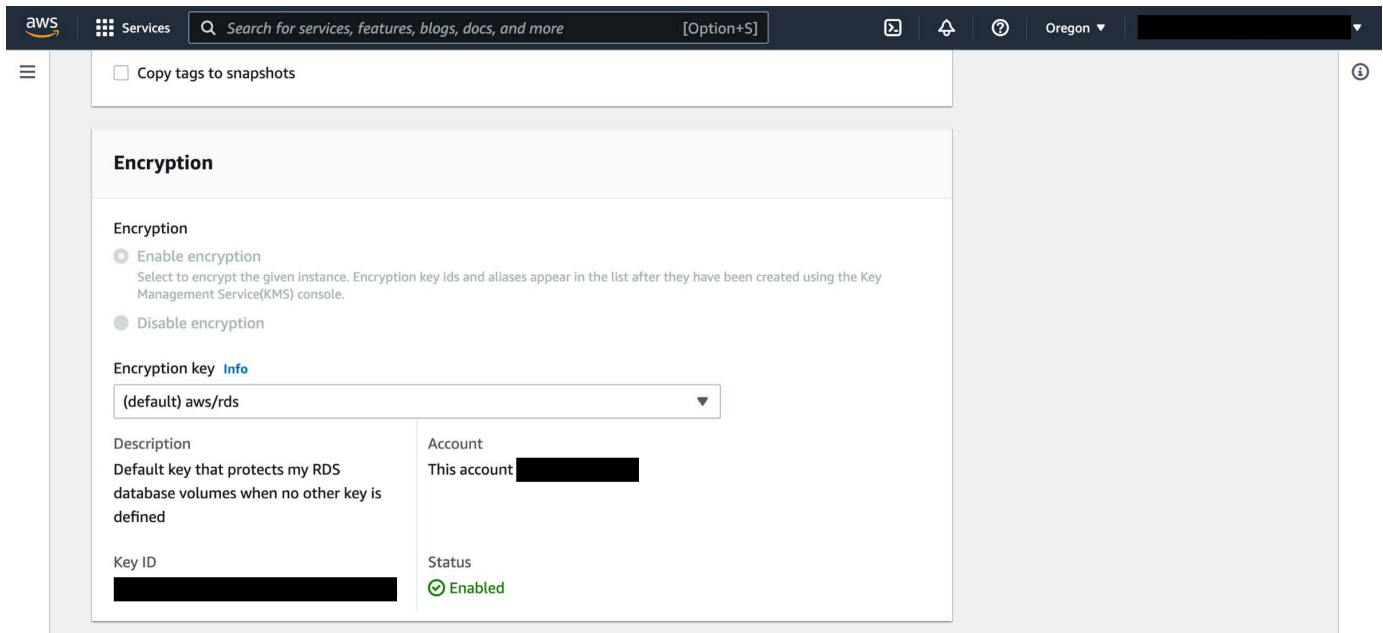
Encryption

Encryption

Enable encryption
Select to encrypt the given instance. Encryption key ids and aliases appear in the list after they have been created using the Key

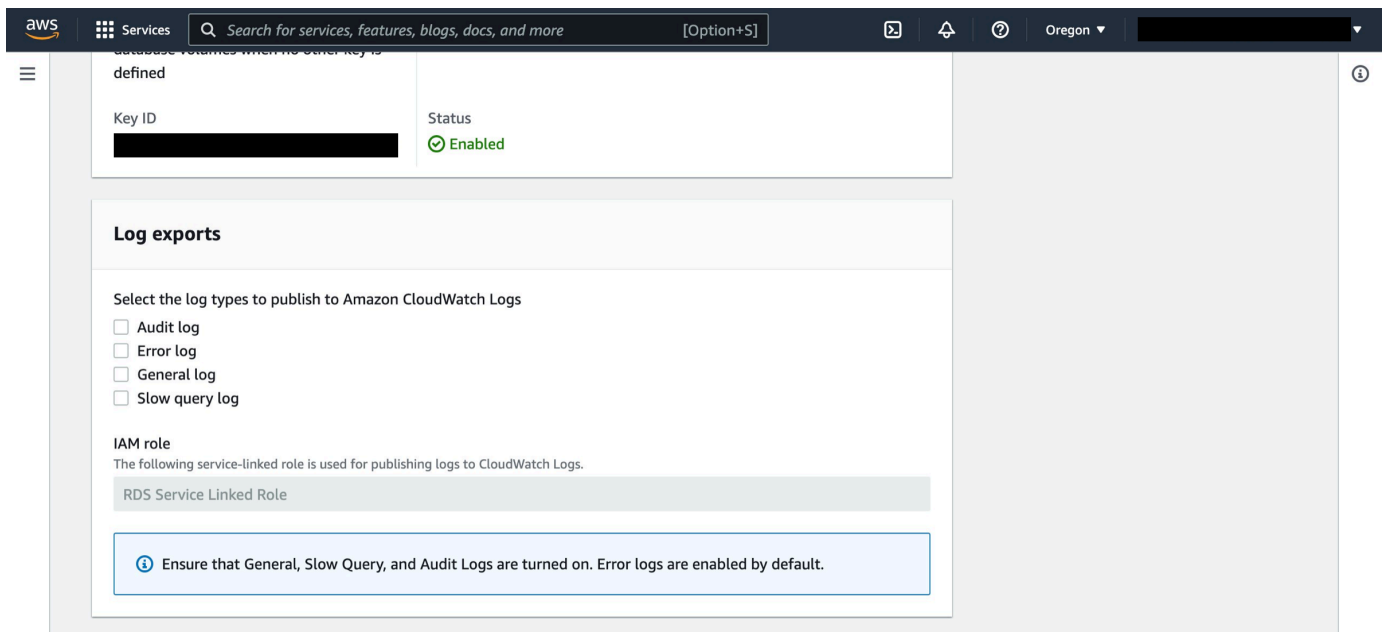
8. Configure encryption

Encryption - This is the master key that will be used to protect the key that is used to encrypt the database volume. You can choose from master keys in your AWS account or enter the Amazon Resource Name (ARN) of a key from a different account.



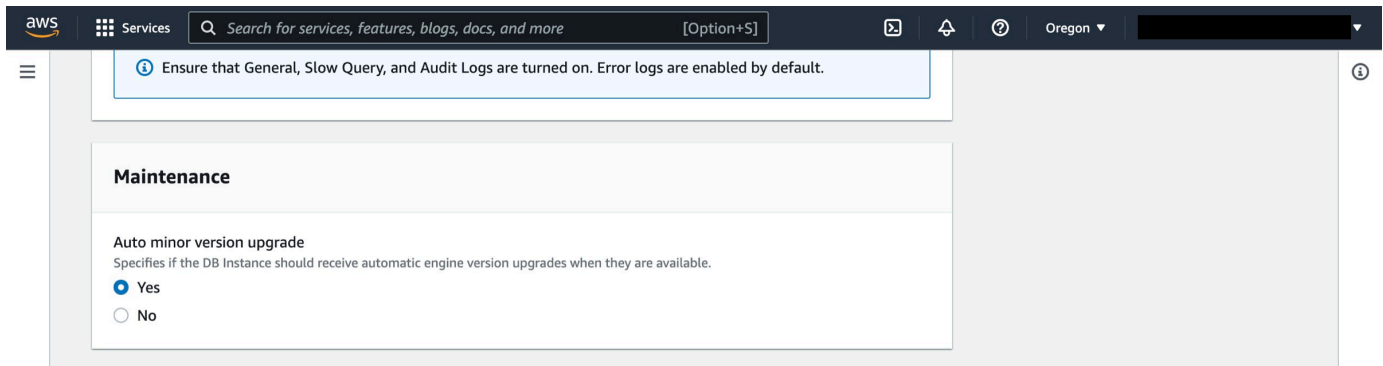
9. Select log types

Log exports - Select the log types to publish to Amazon CloudWatch logs.



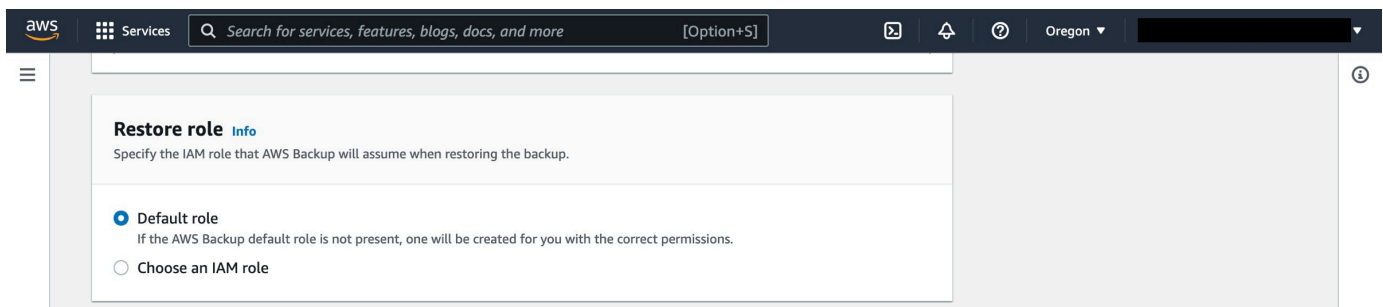
10. Configure automatic maintenance

Maintenance - Select **Yes** if the DB instance should receive automatic engine version upgrades.



11. Choose a restore role

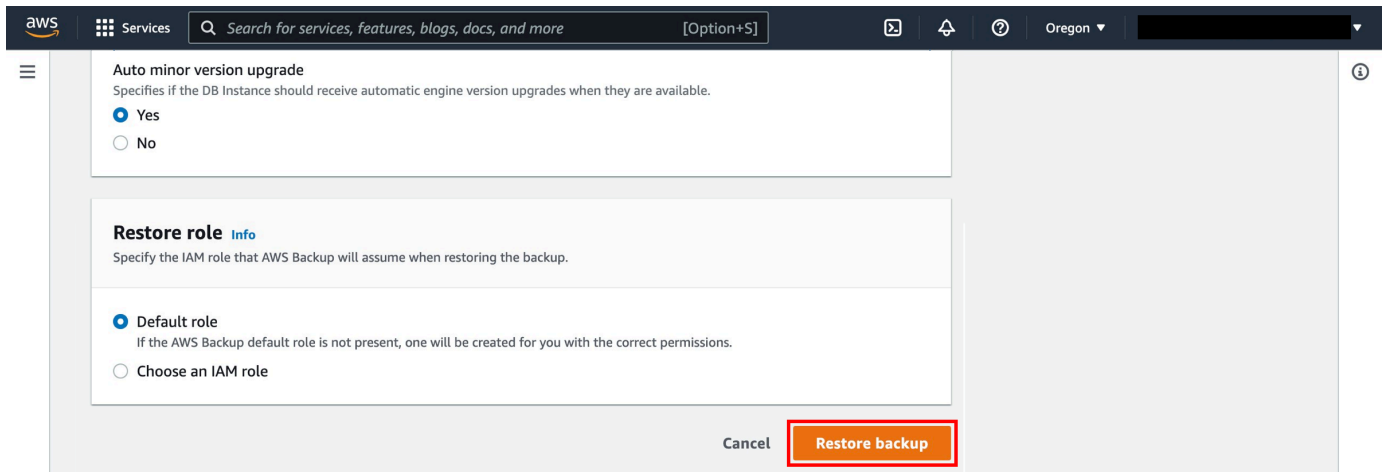
Restore role - Select the **Default role** or **Choose an IAM role**.



12. Restore the backup

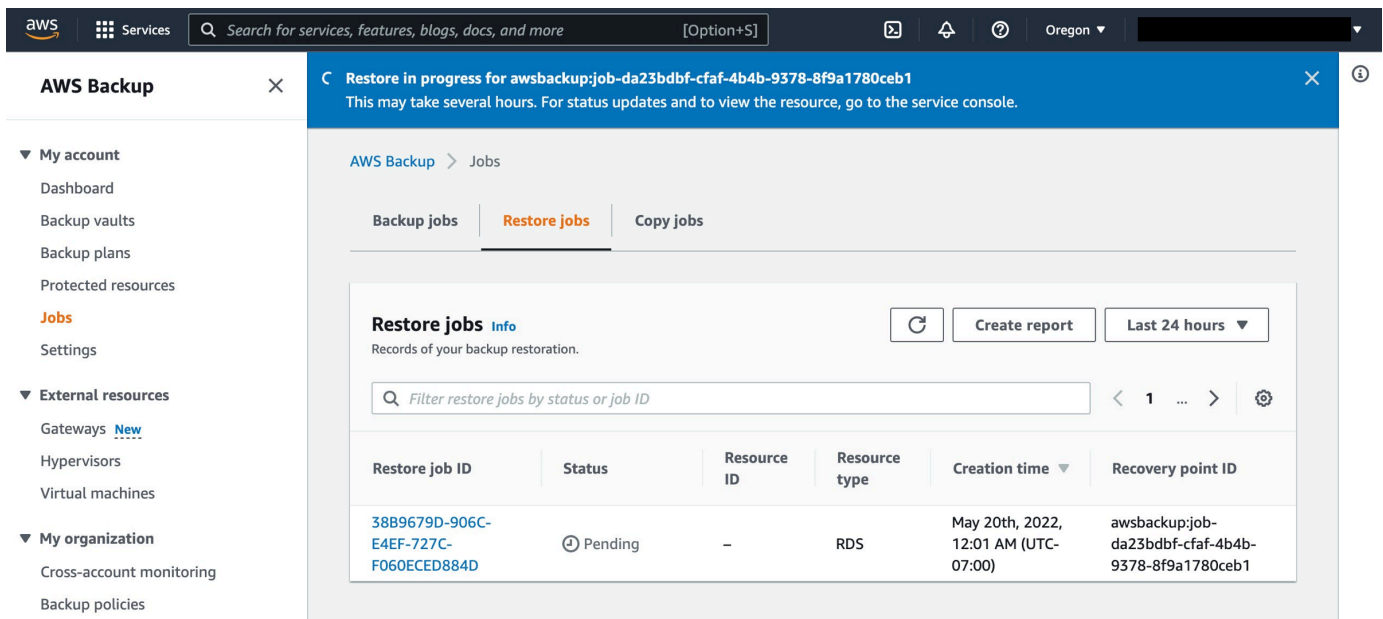
Select **Restore backup**.

- Your job will then appear under the **Jobs** section in the **Restore jobs** tab in the [AWS Backup console](#).
- Once the restore job is completed, you can navigate to the [Amazon RDS console](#) and use the endpoint to connect to the database.



13. Monitor the restore job

Your job will then appear under the **Jobs** section in the **Restore jobs** tab in the [AWS Backup console](#).



14. Find the DB endpoint

Once the restore job is completed, you can navigate to the [Amazon RDS console](#) and use the endpoint to connect to the database.

The screenshot shows the Amazon RDS console interface. On the left is a navigation pane with 'Amazon RDS' selected and a sub-menu for 'Databases'. The main content area shows the details for an instance named 'analyticsrestore'. The 'Summary' section includes:

DB identifier: analyticsrestore	CPU: 6.13%	Status: Modifying	Class: db.m4.xlarge
Role: Instance	Current activity: 0 Connections	Engine: MySQL Community	Region & AZ: us-west-2a

Below the summary are tabs for 'Connectivity & security', 'Monitoring', 'Logs & events', 'Configuration', 'Maintenance & backups', and 'Tags'. The 'Connectivity & security' tab is active, showing:

Endpoint & port Endpoint: analyticsrestore.cbivwjaxqwj5.us-west-2.rds.amazonaws.com	Networking Availability Zone: us-west-2a VPC: vpc-095136c0d10403faa	Security VPC security groups: default (sg-02970cf4e7cc8f909) Active
---	--	--

Clean up resources

In the following steps, you will clean up the resources you created in this how-to guide. It is a best practice to delete instances and resources that you are no longer using so that you are not continually charged for them.

1. Delete the restored database

Open the [Amazon RDS console](#).

In the navigation pane, choose **Databases**.

Select the restored RDS database, and choose **Actions, Delete**.

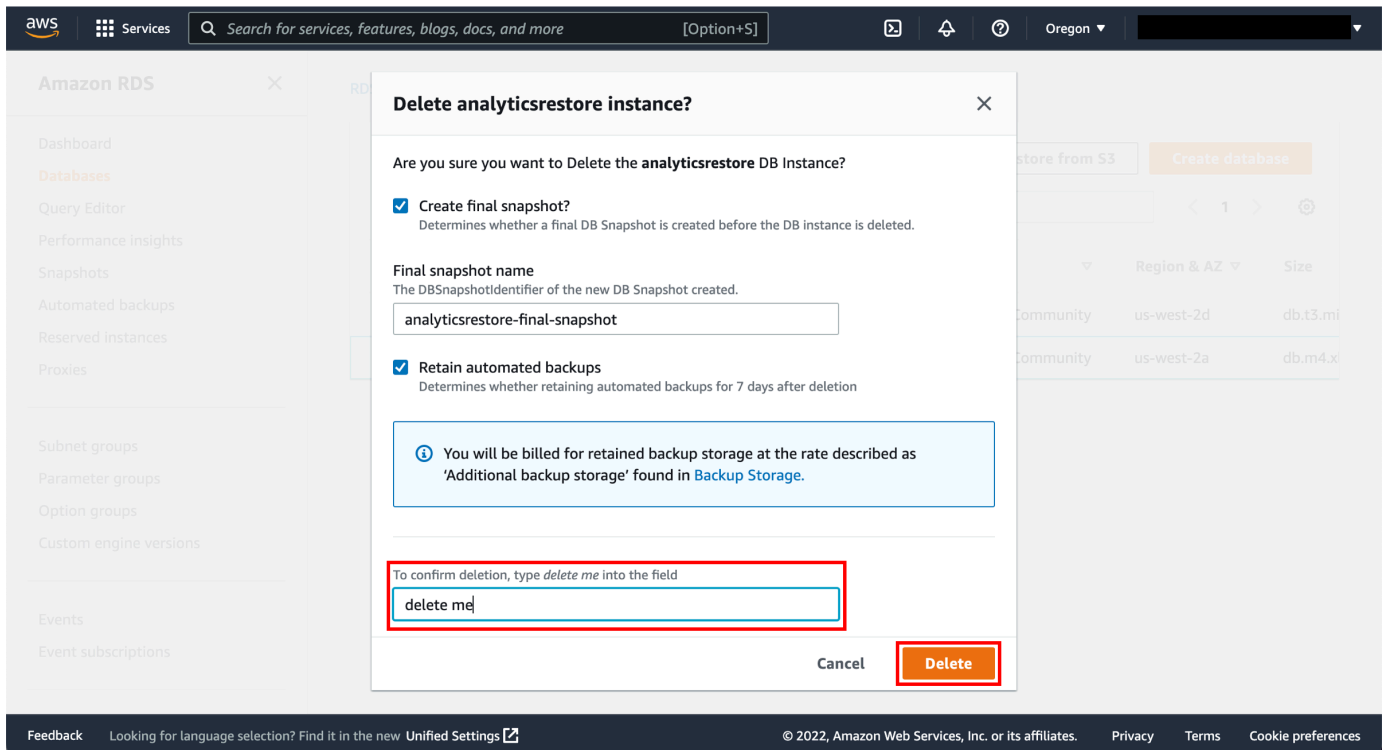
The screenshot shows the Amazon RDS console interface. On the left is a navigation sidebar with options like Dashboard, Databases, Query Editor, Performance insights, Snapshots, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Events, and Event subscriptions. The main content area is titled 'RDS > Databases' and features a 'Databases' header with a 'Group resources' toggle, 'Modify', 'Actions', 'Restore from S3', and 'Create database' buttons. A search bar labeled 'Filter by databases' is present. Below is a table of database instances with columns for 'DB identifier', 'Region & AZ', and 'Size'. Two instances are visible: 'analytics' and 'analyticsrestore'. The 'analyticsrestore' instance is selected, and its 'Delete' action is highlighted in a red box. A dropdown menu is open for the 'Delete' action, listing options: Stop, Reboot, Delete, Create read replica, Create Aurora read replica, Promote, Take snapshot, Restore to point in time, and Migrate snapshot. The footer contains 'Feedback', a language selection link, and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for Privacy, Terms, and Cookie preferences.

2. Confirm deletion

To confirm deletion, type **delete me** into the field.

Note

This process can take several seconds to complete.



Additional resources: Working with Amazon RDS and Amazon Aurora

- [Getting started with AWS Backup](#)
- [How to restore an Amazon RDS database](#)
- [How to restore an Amazon Aurora cluster](#)
- [What is Amazon Relational Database Service \(Amazon RDS\)?](#)
- [What is Amazon Aurora?](#)

Conclusion

You successfully created an on-demand backup job of an Amazon RDS database! You also used a backup plan to back up Amazon RDS resources. As a great next step, check out recently published AWS Backup blogs to further your AWS Cloud knowledge.