



Hands-on tutorials

Amazon EC2 Backup and Restore Using AWS Backup



Amazon EC2 Backup and 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 EC2 Backup and Restore Using AWS Backup i

Overview 1

What you will accomplish 2

Prerequisites 2

Implementation 2

Conclusion 29

Amazon EC2 Backup and Restore Using AWS Backup

AWS experience	Intermediate
Time to complete	10 minutes
Cost to complete	Free Tier eligible (see Amazon EC2 pricing page for more details)
Services used	AWS Backup Amazon EC2
Last updated	January 23, 2023

Overview

[AWS Backup](#) enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed, policy-based service that simplifies data protection at scale. AWS Backup helps you support your regulatory compliance obligations and meet your business continuity goals.

With just a few clicks in the [AWS Backup console](#), you can create backup policies that automate backup schedules and retention management. With AWS Backup, you can create backup policies called backup plans. You can use these plans to define your backup requirements, such as how frequently to back up your data and how long to retain those backups. AWS Backup lets you apply backup plans to your AWS resources by simply tagging them. AWS Backup then automatically backs up your AWS resources according to the backup plan that you defined.

You can use AWS Backup to create on-demand backup jobs, or customize a backup plan to back up the supported resources. When using AWS Backup with [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) instances, you can centralize your compliance and policy control for backups, increase security choices for your organization, and access instant enterprise-level features and functionality. When you back up an [EC2 instance](#), AWS Backup will protect all [Amazon EBS volumes](#) attached to the instance, and will attach them to an AMI that stores all parameters from the original EC2 instance (excluding [Elastic Inference accelerators](#) and [user data scripts](#)).

What you will accomplish

In this tutorial, you will:

- Create an on-demand backup job of an Amazon EC2 instance
- Use a backup plan to back up Amazon EC2 resources—using a backup plan within AWS Backup lets you automate your backups on a schedule
- Add resources to an existing backup plan using tags

Prerequisites

You will need the following resources or permissions to proceed with this tutorial:

- An [AWS account](#). For more information on using AWS Backup for the first time, view the [AWS Backup documentation](#).
- One or more Amazon EC2 instances. You can refer to the [Amazon EC2 pricing page](#) for more details. For AWS Backup pricing, refer to the [AWS Backup pricing page](#).
- IAM roles used by AWS Backup to create a backup of the Amazon EC2 instance.
 - If a subsequent role is not created, then the default IAM role can be used—AWSBackupDefaultRole.

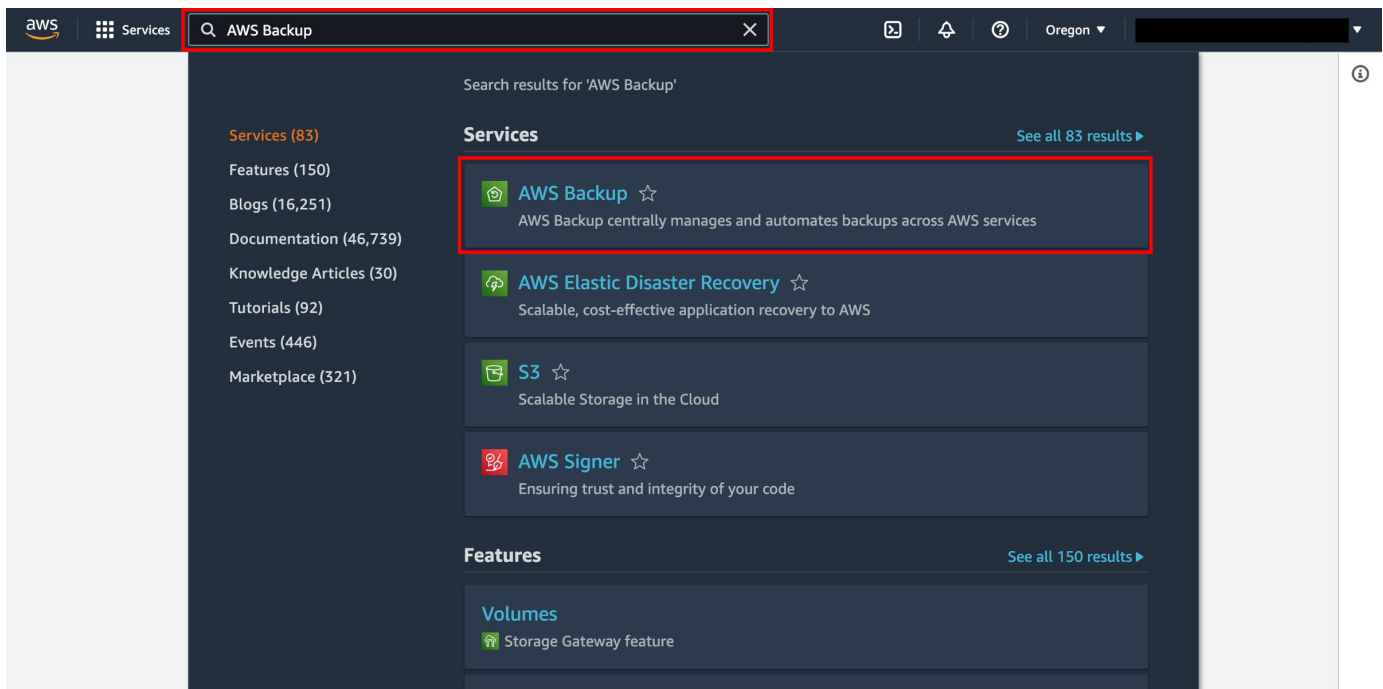
Implementation

In this tutorial, you will learn how to create an on-demand backup job of an Amazon EC2 instance. Then, you will use a backup plan to protect EC2 resources. Using a backup plan within AWS Backup lets you automate backups using tags.

Step 1: Configure an on-demand AWS Backup job of an Amazon EC2 instance

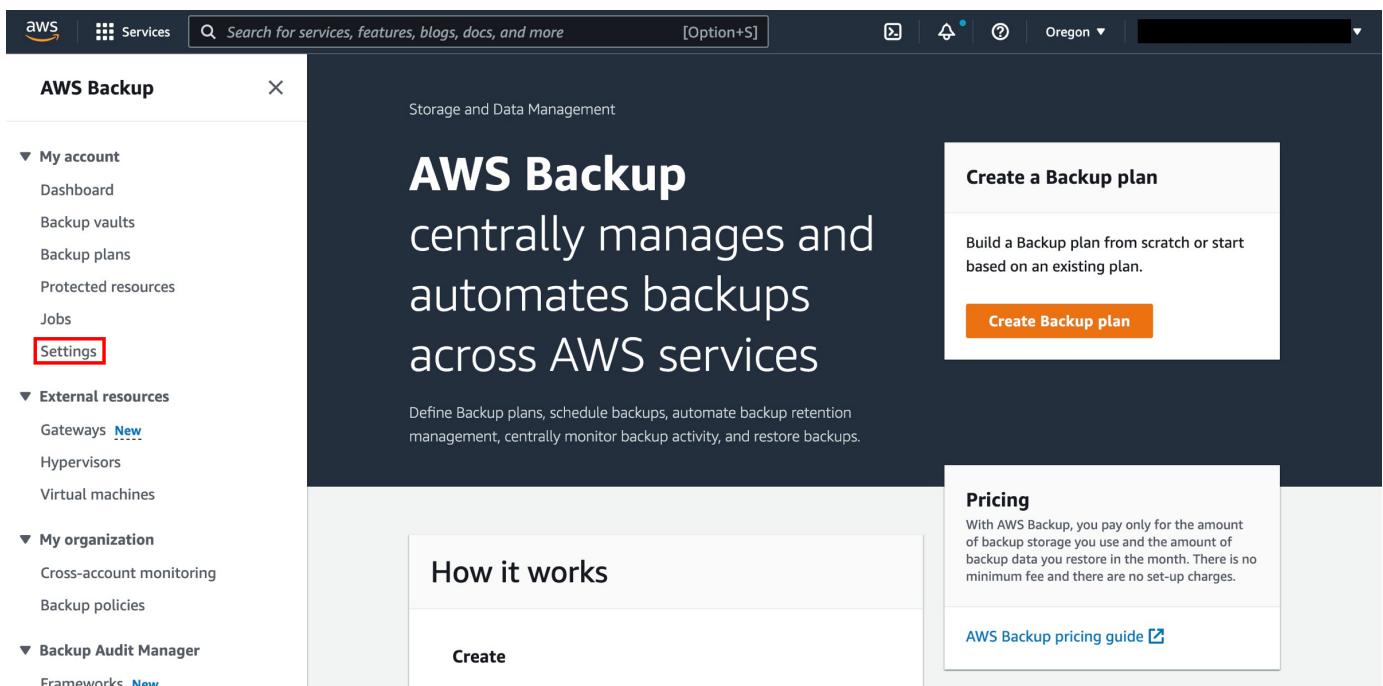
1. Open the AWS Backup console

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



2. Configure the services used with AWS Backup

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



3. Configure resources

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

AWS Backup ×

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	⊖ Disabled
DocumentDB	⊖ Disabled
DynamoDB	⊖ Disabled
EBS	⊖ Disabled
EC2	⊖ Disabled
EFS	⊖ Disabled
FSx Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.	⊖ Disabled
Neptune	⊖ Disabled
RDS	⊖ Disabled

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

4. Select EC2 for backup

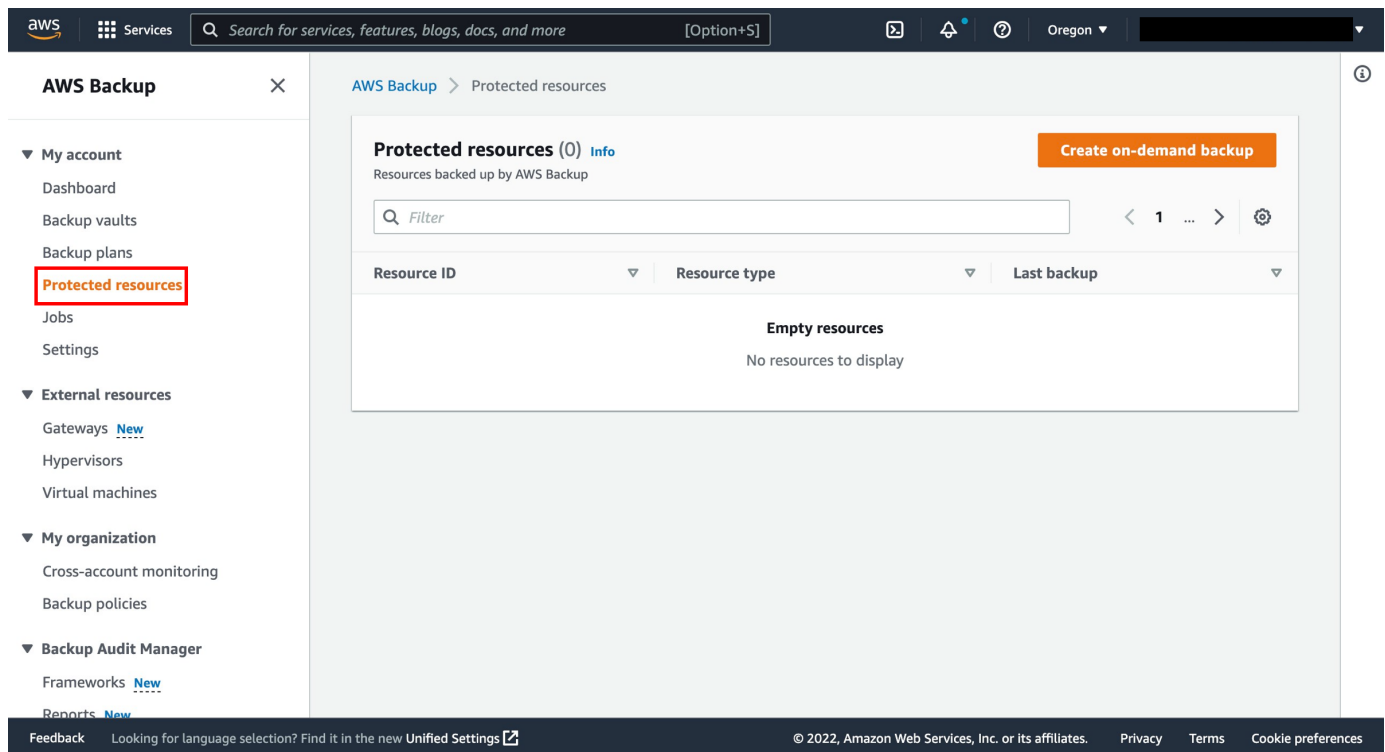
On the **Configure resources** page, use the toggle switches to enable or disable the services used with AWS Backup. In this case, select **EC2**. Choose **Confirm** when your services are configured.

- 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 2.10 for information on Cross-Region Copy). This tutorial uses the US West (Oregon) Region (us-west-1).

The screenshot shows the AWS Backup console's 'Configure resources' page. The breadcrumb navigation is 'AWS Backup > Settings > Configure resources'. The main heading is 'Configure resources'. Below it, there's a section titled 'Resources' with an 'Info' link. The text says: 'Enable and disable resource types (e.g., EC2, EFS, etc.) that will be protected by backup plans in this account and Region.' Below this is a table of 'Enabled resources' with toggle switches. The resources listed are Aurora, DocumentDB, DynamoDB, EBS, EC2, EFS, FSx, Neptune, RDS, S3, Storage Gateway, and VMware virtual machines. The 'EC2' row is highlighted with a red box, and its toggle switch is turned on. At the bottom right of the configuration area, there are 'Cancel' and 'Confirm' buttons. The 'Confirm' button is highlighted with a red box. The footer of the console shows 'Feedback', a link to 'Unified Settings', and copyright information for 2022.

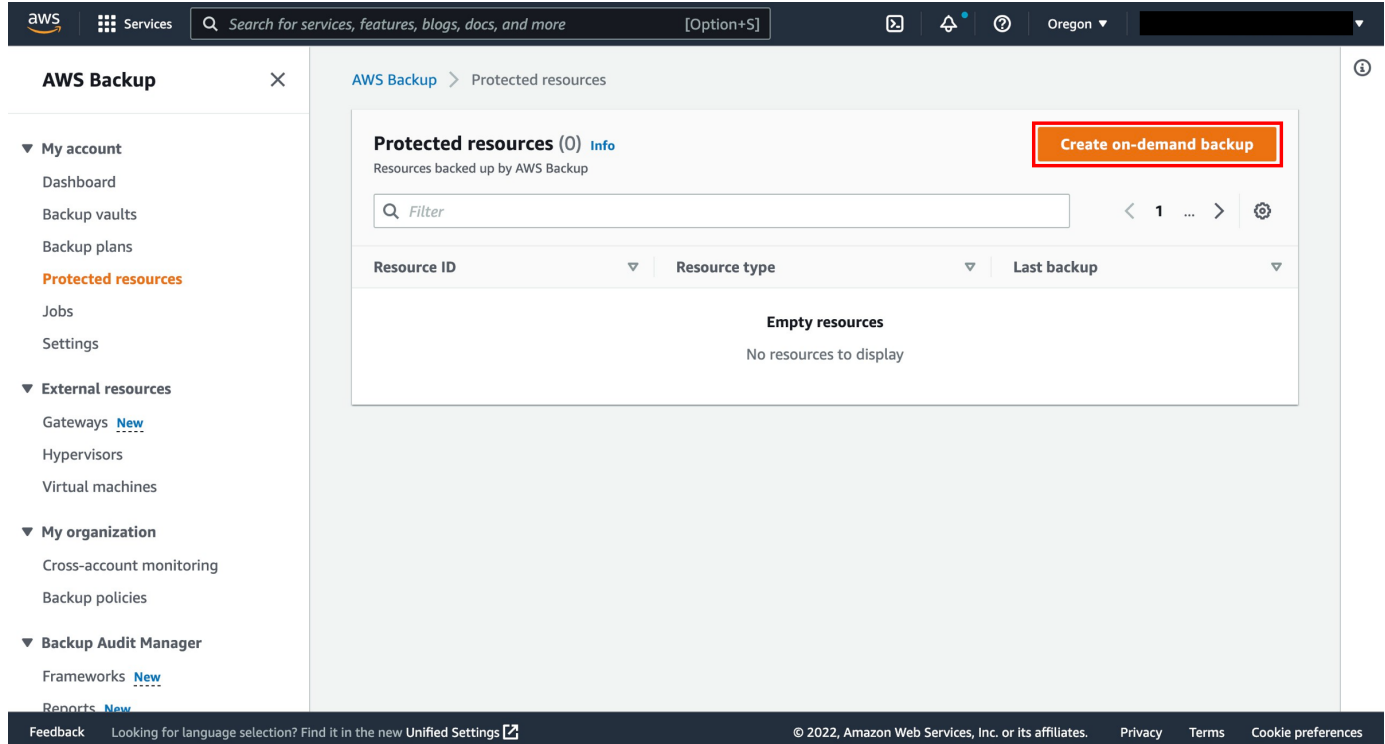
Enabled resources	
Aurora	☐
DocumentDB	☐
DynamoDB	☐
EBS	☐
EC2	☒
EFS	☐
FSx	☐
Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.	
Neptune	☐
RDS	☐
S3	☐
Available for S3 buckets with versioning enabled. Follow instructions for one-time permissions setup	
Storage Gateway	☐
VMware virtual machines	☐

5. Create an on-demand backup job of an Amazon EC2 instance



6. Choose Create an on-demand backup

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



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 **EC2** for Amazon EC2.

Choose the **Instance ID** of the EC2 resource that you want to protect.

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.

Choose 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 trail is: AWS Backup > Protected resources > Create on-demand backup. The main heading is "Create on-demand backup" with an "Info" link. The "Settings" section contains the following fields and options:

- Resource type:** A dropdown menu set to "EC2".
- Instance ID:** A dropdown menu set to "i-0acdf9192e629ffb1" with a refresh icon.
- Backup window:** Two radio buttons. "Create backup now" is selected, with the subtext "Starts within 1 hour." The other option is "Customize backup window".
- Retention period:** A dropdown menu set to "Always" with an "Info" link.
- Backup vault:** A dropdown menu set to "Default" with an "Info" link. Below it is a "Create new Backup vault" button.
- IAM role:** Two radio buttons. "Default role" is selected, with the subtext "If the AWS Backup default role is not present, one will be created for you with the correct permissions." The other option is "Choose an IAM role".
- Tags added to recovery points:** A section with a right-pointing triangle icon and the text: "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". The "Create on-demand backup" button is highlighted with a red rectangular 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.

AWS Backup

Backup in progress for instance/i-0acdf9192e629ffb1
Depending on the size of the resource, this might take several hours. For status updates, refer to this page.

Jobs

In jobs, you can monitor the status and other details of backup, restore, and copy activity.

Backup jobs | Restore jobs | Copy jobs

Backup jobs Info Stop backup job Create report Last 24 hours

Records of your scheduled or on-demand backups.

Filter backup jobs by job ID, status, resource ID or resource type

	Backup job ID	Status	Resource ID	Resource type	Created
☐	0b33a964-f3e2-4ac2-8f1f-97b9afe3962f	Created	instance/i-0acdf9192e629ffb1	EC2	Octo

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 2: Configure an automatic AWS Backup job of an Amazon EC2 instance

1. Configure the services used with AWS Backup

In the left navigation pane in the [AWS Backup console](#), under **My account**, choose **Settings**.

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

AWS Backup ×

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

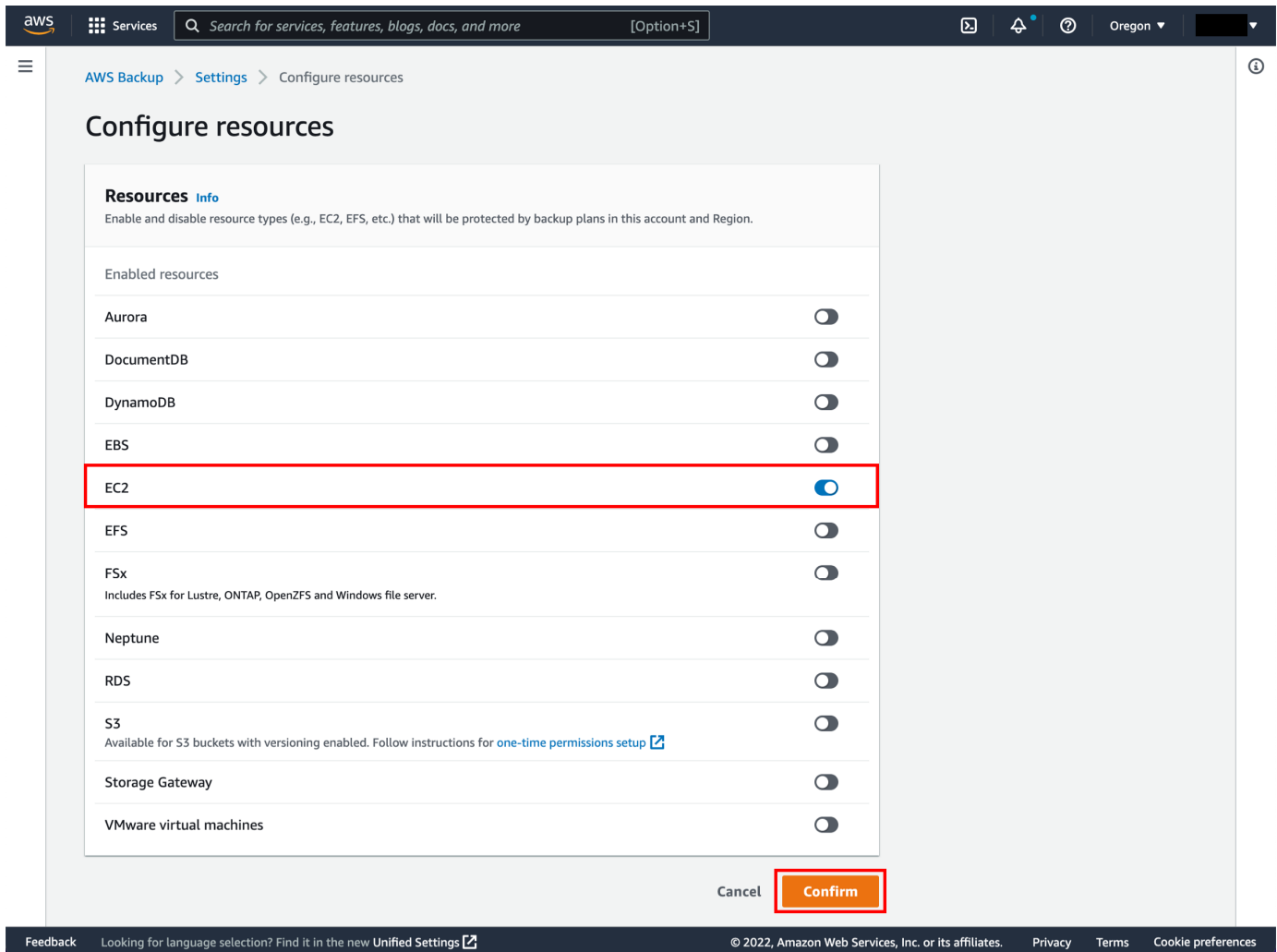
Resource type	Status
Aurora	⊖ Disabled
DocumentDB	⊖ Disabled
DynamoDB	⊖ Disabled
EBS	⊖ Disabled
EC2	⊕ Enabled
EFS	⊖ Disabled
FSx Includes FSx for Lustre, ONTAP, OpenZFS and Windows file server.	⊖ Disabled
Neptune	⊖ Disabled
RDS	⊖ Disabled

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. Select EC2 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 2.10 for information on Cross-Region Copy). This tutorial uses the US West (Oregon) Region (us-west-1).



3. Configure a backup plan for an Amazon EC2 instance

In the [AWS Backup console](#), select **Backup plans** in the left navigation pane under **My account**, and then **Create backup plan**.

4. Create a new backup plan

AWS Backup provides three ways to get started using backup plans, but for this tutorial, 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 tutorial, enter **EC2-webapp**.

The screenshot shows the AWS Backup console interface for creating a new backup plan. The 'Start options' section has three radio buttons: '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 populated with 'EC2-webapp' and 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.' The 'Tags added to backup plan - optional' section is collapsed. The 'Backup rule configuration' section is partially visible at the bottom.

5. 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 tutorial, enter **EC2-Dailies**.

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

EC2-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](#)

6. 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.

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](#)

7. Configure your backup 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 KMS key.
- Optionally, add tags that will help you search for and identify your backup vault.
- Choose the **Create Backup vault** button.

Create Backup vault

General

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

Encryption key [Info](#)
(default) aws/backup

Description Default key that protects my Backup data when no other key is defined	Account This account	Key ID	Status ✓ 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](#)

8. 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 (PITRs) 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](#)

9. Configure retention settings

Transition to cold storage — Currently, only Amazon Elastic File System (Amazon EFS) 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.

10. (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.

aws Services Search for services, features, blogs, docs, and more [Option+S] Oregon

Transition to cold storage [Info](#)
Never

Retention period [Info](#)
Always

Copy to destination [Info](#)
Choose a Region

► **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.

▼ **Advanced backup settings**

Application-consistent backup [Info](#)
Enable application-consistent snapshots for the selected third-party software running on EC2.

☐ Windows VSS

[i](#) You can assign resources to this Backup plan after the plan has been created.

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

11. 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**.

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.

No tags.

[Add new tag](#)

You can add up to 50 more tags.

Advanced backup settings

Application-consistent backup [Info](#)
Enable application-consistent snapshots for the selected third-party software running on EC2.

☐ Windows VSS

[i](#) You can assign resources to this Backup plan after the plan has been created.

[i](#) You can add more rules to this Backup plan after the plan has been created.

[Cancel](#) [Create plan](#)

12. 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 choose the **Assign resources** button.

The screenshot shows the AWS Backup console interface. On the left is a navigation menu with sections: My account, External resources, My organization, and Backup Audit Manager. The main content area is titled 'EC2-webapp' and includes a 'Delete' and 'View JSON' button. Below this is a 'Summary' section with a table of backup plan details. Further down is a 'Backup rules (1)' section with a table showing one rule named 'EC2-Dailies'. At the bottom is a 'Resource assignments (0)' section with a 'Delete' button and an 'Assign resources' button, which is highlighted with a red rectangle.

Backup plan name	Version ID	Last modified	Last runtime
EC2-webapp	M2M4ZGMyYTUtZDZkYi00	October 11th, 2022, 11:22 AM (UTC-07:00)	-

Name	Backup vault	Destination Backup vault
EC2-Dailies	FinancialBackups	-

Name
EC2-Dailies

13. 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.

aws Services Search for services, features, blogs, docs, and more [Option+S] Oregon

AWS Backup > Backup plans > EC2-webapp > Resource selection

Resource selection [Info](#)

General

Resource assignment name

EC2-resources

Resource assignment name is case sensitive. Must contain from 1 to 50 alphanumeric or '-' characters.

IAM role [Info](#)

AWS Backup will assume this IAM role when creating and managing recovery points 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

Resource selection [Info](#)

Assign resources to this Backup plan using tags and resource IDs.

1. Define resource selection [Info](#)

Protect all resources or specify resources by type or ID.

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

14. Choose resource selection type

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

Assign resources [Info](#)

Assign resources to this Backup plan using tags and resource IDs.

1. Define resource selection [Info](#)

Protect all resources or specify resources by type or ID.

☒ **Include all resource types**

Protect all resource types that are enabled in your account.

☐ **Include specific resource types**

Choose resources by type or specify individual resources by ID.

15. 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.

Choose resources by type or specify individual resources by ID.

2. Select specific resource types [Info](#)

Choose specific resource types that you want to protect with this backup plan. You can also exclude specific resource IDs from the selection.

Select resource types

Resource type	Instance IDs	
EC2	Choose resources	Remove
All instances		

3. Exclude specific resource IDs from the selected resource types - optional [Info](#)

Select specific resource IDs that you want to exclude from this assignment.

Select resource types

16. Assign the resources to the backup plan

For tags-based resource assignment, provide the key-value pair of the Amazon EC2 instance.

Choose the **Resource selection** button to assign the resources to the backup plan.

2. Select specific resource types [Info](#)

Choose specific resource types that you want to protect with this backup plan. You can also exclude specific resource IDs from the selection.

Select resource types

3. Exclude specific resource IDs from the selected resource types - optional [Info](#)

Select specific resource IDs that you want to exclude from this assignment.

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.

Key	Condition for value	Value	
			Remove

You can add up to 29 more tags.

17. View the backup job

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

A backup, or recovery point, represents the content of a resource, such as an Amazon EC2 instance 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.

Step 3: Restore an Amazon EC2 instance 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.

The screenshot shows the AWS Backup console interface. On the left is a navigation menu with sections like 'My account', 'External resources', 'My organization', and 'Backup Audit Manager'. The main content area is titled 'Default' and shows a 'Summary' section with details about the backup vault (name, ARN, creation date, vault lock, and KMS encryption key ID). Below this is a table of 'Recovery points (978)'. The table has columns for 'Recovery point ID', 'Status', 'Resource ID', 'Resource type', and 'Backup'. One recovery point is highlighted with a red box: 'image/ami-0ce50ce38075083f7', which has a 'Completed' status and is associated with the resource 'instance/i-0fe4dcceaf4b30ed1' of type 'EC2'.

Recovery point ID	Status	Resource ID	Resource type	Backup
image/ami-0ce50ce38075083f7	Completed	instance/i-0fe4dcceaf4b30ed1	EC2	Image

2. Restore the EC2 instance

To restore the EC2 instance, select the recovery point ARN and choose **Restore**.

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 a region dropdown set to 'Oregon'. Below the navigation bar, the breadcrumb trail reads 'AWS Backup > Backup vaults > Default > ami-0ce50ce38075083f7 - EC2'. The main heading is 'ami-0ce50ce38075083f7 - EC2'. To the right of the heading are three buttons: 'Copy', 'Delete', and 'Restore' (which is highlighted with a red rectangle). Below the heading is a 'Details' section containing a table with the following information:

ARN arn:aws:ec2:us-west-2:image/ami-0ce50ce38075083f7	Resource type EC2	Status Completed	Backup type Image
Creation time October 10th, 2022, 10:00 PM (UTC-07:00)	Resource ID instance/i-0fe4dceaf4b30ed1	Storage tier Warm	Size 30 GB

Below the details is a 'Backup summary' section with an 'Edit' button. It contains a table with the following information:

Backup type Automated	Backup vault Default	Backup plan RDS-webapp
Expiration date -	Move to cold date -	IAM role Default role

At the bottom of the console, there's a footer with 'Feedback', 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'.

3. Review restore configurations

The restore of the ARN will bring you to a **Restore backup** screen that will have the configurations for the EC2 instance using the backed-up AMI and all the attached EBS volumes.

In the **Network settings** pane, accept the defaults or specify the options for the **Instance type**, **Virtual Private Cloud (VPC)**, **Subnet**, **Security groups**, and **Instance IAM role** settings.

This example proceeds with no IAM role. The IAM role can be applied to the EC2 instance after the restore process is completed.

- To successfully do a restore with the original instance profile, you must edit the restore policy. If you apply an instance profile during the restore, you have to update the operator role and add the PassRole permissions of the underlying instance profile role to Amazon EC2. The default service role created by AWS Backup manages creating and restoring backups. It has two managed policies: `AWSBackupServiceRolePolicyForBackup` and `AWSBackupServiceRolePolicyForRestores`. It also allows "Action": `iam:PassRole` to launch EC2 instances as part of a restore.

The screenshot shows the AWS Backup console interface for restoring a backup. The breadcrumb navigation is: AWS Backup > Backup vaults > Default > Restore backup. The main heading is 'Restore backup'. Below it, a description states: 'Restore EC2 instances so they can centrally manage backups with other resources while being able to use the key features like scheduled backups, lifecycle management, and quick restores. To access full instance restore capabilities go to [Instance Launch Wizard](#)'. The 'Network settings' section is expanded, showing the following configuration options:

- Instance type** (Info): Define the compute and memory capacity of the instance. The dropdown shows 't2.micro - 1 vCPU, 1 GiB RAM'.
- Virtual Private Cloud (VPC)**: Select the VPC to define the virtual networking environment. The dropdown shows 'vpc-07b660369d5db35c0' with a refresh button.
- Subnet** (Info): Specify a range of IP addresses in your VPC that can be used to isolate different EC2 resources from each other or from the internet. Each subnet resides in one Availability Zone. The dropdown shows 'subnet-001703c31a7504865' with a refresh button.
- Security groups** (Info): Specify security groups to determine a set of firewall rules that control the traffic for your instance. The dropdown shows 'Add a security group' with a refresh button. Below the dropdown, a tag 'BreakTheMonolith-Demo-EcsSecurityGroup-164FKPR7ZBACU' is visible with a close button.
- Instance IAM role** (Info): Specify the IAM role that will automatically deploy AWS credentials to the EC2 instance. The dropdown shows 'Proceed with no IAM role' and is highlighted with a red box.

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'.

4. Choose a restore role

In the **Restore role** pane, accept the **Default role** or **Choose an IAM role** to specify the IAM role that AWS Backup will assume for this restore.

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The 'Security groups' section has 'BreakTheMonolith-Demo-EcsSecurityGroup-164FKPR7ZBACU' selected. The 'Instance IAM role' section has 'Proceed with no IAM role' selected. The 'Restore role' section is highlighted with a red box and contains two options: 'Default role' (selected) and 'Choose an IAM role'. The 'Advanced settings' section is partially visible at the bottom.

Security groups [Info](#)
Specify security groups to determine a set of firewall rules that control the traffic for your instance.

Instance IAM role [Info](#)
Specify the IAM role that will automatically deploy AWS credentials to the EC2 instance.

Restore role [Info](#)
Specify the IAM role that AWS Backup will assume when restoring the backup.

☒ **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

▼ **Advanced settings**
Customize shutdown and hibernation behavior, termination protection, placement groups, tenancy, and other advanced settings.

Shutdown behavior [Info](#)

5. Restore the backup

In the **Advanced settings** pane, accept the defaults or specify the options for **Shutdown behavior**, **Stop - Hibernate behavior**, **Placement group**, **T2/T3 Unlimited**, **Tenancy**, and **User data** settings. This section is used to customize shutdown and hibernation behavior, termination protection, placement groups, tenancy, and other advanced settings.

AWS Backup will use the SSH key pair used at the time of backup to automatically perform your restore.

After specifying all of your settings, choose **Restore backup**. The **Restore jobs** pane will appear, and a message at the top of the page will provide information about the restore job.

Advanced settings
Customize shutdown and hibernation behavior, termination protection, placement groups, tenancy, and other advanced settings.

Shutdown behavior [Info](#)
Specify the instance behavior when an OS-level shutdown is performed.
Stop

Stop - Hibernate behavior [Info](#)
☐ Enable hibernation as an additional stop behavior

☐ Enable termination protection
Protect instances from being accidentally terminated. Once enabled, you won't be able to terminate this instance via the API or the AWS Management Console until termination protection has been disabled.

Placement group [Info](#)
Provide a name for the logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput.
☐ Add instance to placement group

T2/T3 Unlimited
Enabling T2/T3 Unlimited allows applications to burst beyond the baseline for as long as needed at any time. If the average CPU utilization of the instance is at or below the baseline, the hourly instance price automatically covers all usage. Otherwise, all usage above baseline is billed. [Additional charges may apply](#) [↗](#)
Disabled

Tenancy [Info](#)
Specify whether the use of host tenancy will request to launch instances onto dedicated hosts, or launch instances as dedicated instances.
Shared - Run a shared hardware instance

User data - optional [Info](#)
Specify user data to configure an instance or run a configuration script during launch. If the input is not already encoded, AWS will automatically base64 encode user data for you.

☐ User data is base64 encoded

Cancel **Restore backup**

6. Monitor restore job

Check for your restored backup job under **Restore jobs** in the the [AWS Backup console](#).

Advanced settings
Customize shutdown and hibernation behavior, termination protection, placement groups, tenancy, and other advanced settings.

Shutdown behavior [Info](#)
Specify the instance behavior when an OS-level shutdown is performed.
Stop

Stop - Hibernate behavior [Info](#)
☐ Enable hibernation as an additional stop behavior

☐ Enable termination protection
Protect instances from being accidentally terminated. Once enabled, you won't be able to terminate this instance via the API or the AWS Management Console until termination protection has been disabled.

Placement group [Info](#)
Provide a name for the logical grouping of instances within a single Availability Zone that benefit from low network latency, high network throughput.
☐ Add instance to placement group

T2/T3 Unlimited
Enabling T2/T3 Unlimited allows applications to burst beyond the baseline for as long as needed at any time. If the average CPU utilization of the instance is at or below the baseline, the hourly instance price automatically covers all usage. Otherwise, all usage above baseline is billed. [Additional charges may apply](#) [\[?\]](#)
Disabled

Tenancy [Info](#)
Specify whether the use of host tenancy will request to launch instances onto dedicated hosts, or launch instances as dedicated instances.
Shared - Run a shared hardware instance

User data - optional [Info](#)
Specify user data to configure an instance or run a configuration script during launch. If the input is not already encoded, AWS will automatically base64 encode user data for you.

☐ User data is base64 encoded

Cancel **Restore backup**

7. Confirm restoration

Once the job status appears as completed, navigate to the [Amazon EC2 console](#) and select **Instances** in the left navigation pane to see the restored EC2 instance. The EC2 instance is restored using the backup of the AMI and the attached EBS volume.

You can now connect to the public IP address if you restored your Amazon EC2 instance using SSH.

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availa
☐	-	i-09f4613e5afc69898	Running	t2.micro	Initializing	No alarms	us-we

Clean up resources

In the following steps, you clean up the resources you created in this tutorial. 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 instance

Open the [Amazon EC2 console](#).

In the navigation pane on the left, choose **Instance** under Instances.

Select the restored EC2 instance, and choose **Instance state**, then **Terminate instance**.

Choose **Terminate** when prompted for confirmation.

2. Delete the AWS Backup recovery point

Open the [AWS Backup console](#) and navigate to the vault where the recovery point is stored.

Select the recovery point, then select Delete.

Note

This process can take several seconds to complete.

Conclusion

Congratulations! You have created a backup of an Amazon EC2 instance and performed a restore using AWS Backup.