Hands-on tutorials

Amazon EBS Backup & Restore using AWS Backup

Amazon EBS Backup & Restore using AWS Backup: Hands-on tutorials

Table of Contents

Amazon EBS Backup & Restore using AWS Backup

AWS experience	Beginner
Time to complete	10 minutes
Cost to complete	Free (Amazon EBS free tier)
Services used	Amazon Elastic Block Store (Amazon EBS)

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.

AWS Backup currently supports Amazon Elastic Block Store (Amazon EBS) and Amazon Elastic Compute Cloud (Amazon EC2) instances. When using AWS Backup with Amazon EBS and Amazon EC2, you can centralize your compliance and policy control for backups, increase security choices for your organization, and access instant enterprise level features and functionality. You pay only for the EBS backup capacity you use, and no other added costs. You can use AWS Backup to manage backups of Amazon EBS volumes. Backups managed by AWS Backup are considered manual EBS snapshots, but don't count toward the EBS snapshot quota for Amazon EBS.

What you will accomplish

- Create an on-demand backup job of an Amazon EBS volume

- Use a backup plan to backup Amazon EBS 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

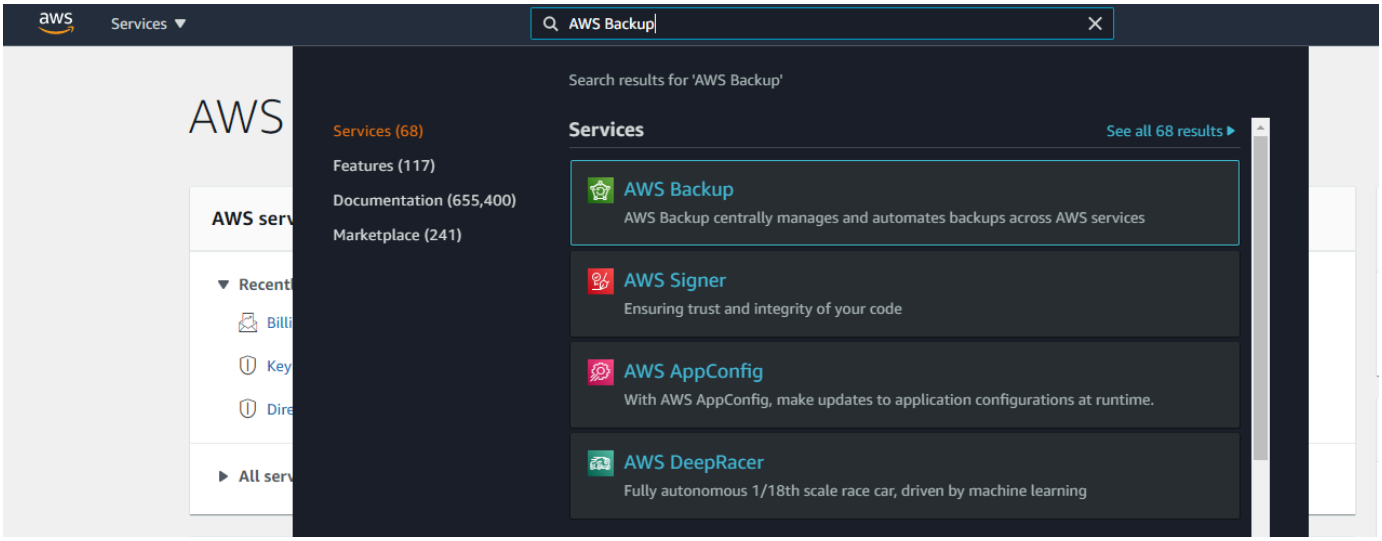
- You will need the following resources or permissions to proceed with this tutorial:
  - An AWS account will be needed for this tutorial. For more information on using AWS Backup for the first time, view the AWS Backup documentation.
  - One or more Amazon EBS volumes (including those that are free tier eligible). For the pricing of volumes not in the free tier, refer to the Amazon EBS pricing page. For AWS Backup pricing, refer to the AWS Backup pricing page.
  - IAM roles used by AWS Backup to create a backup of the Amazon EBS volume.
    - 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 existing EBS volume

1. Open the AWS Backup console

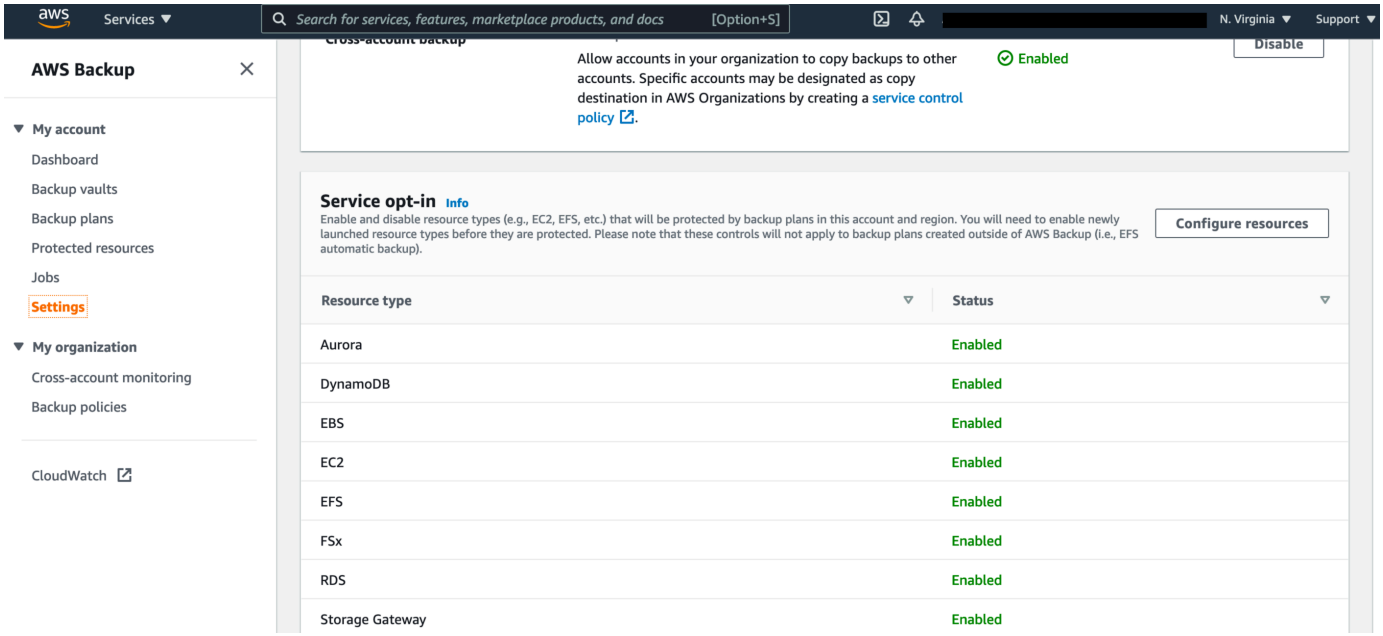
   Log in to the AWS Management Console, and open the AWS Backup console.



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**.

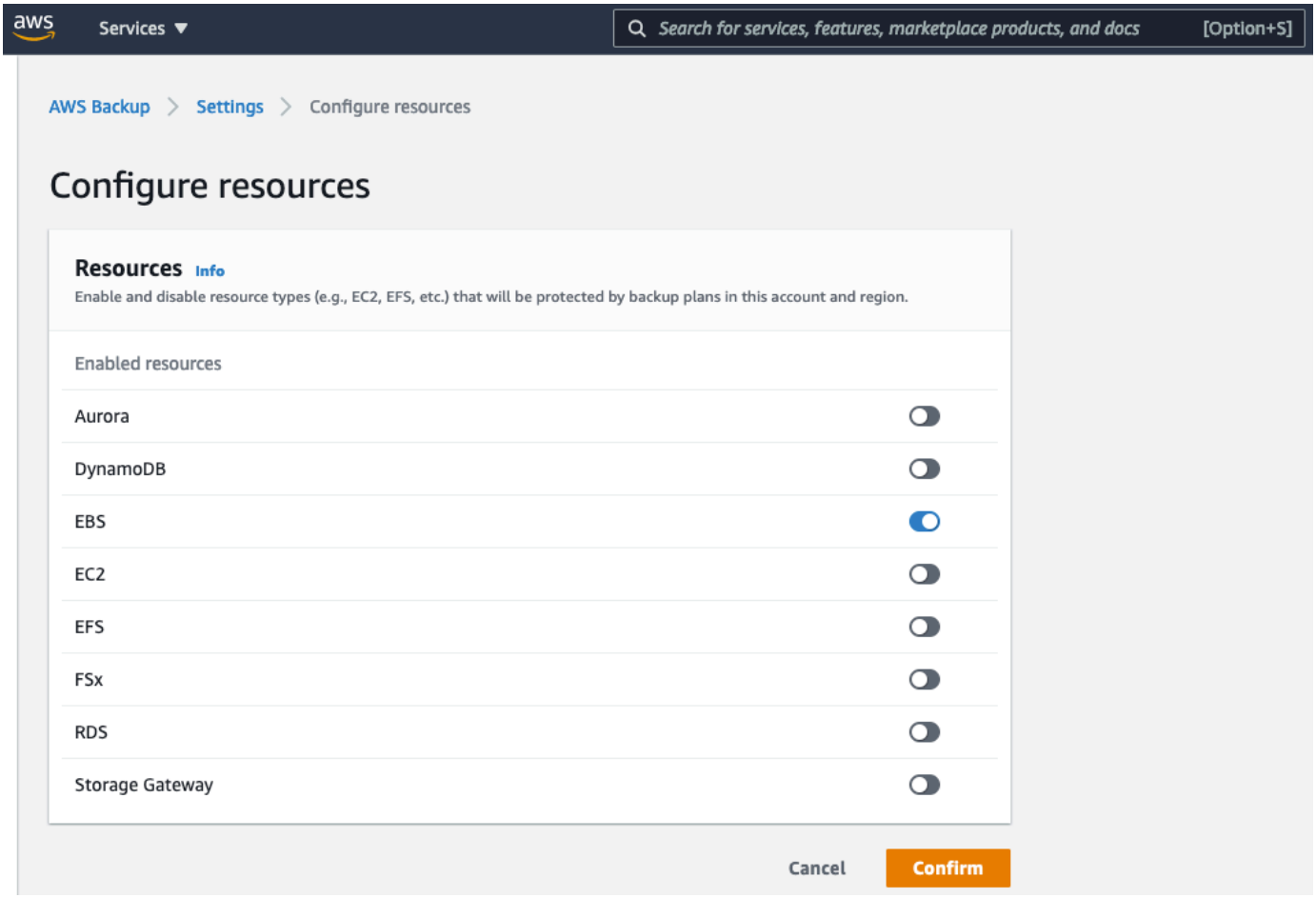
   On the **Service opt-in** page, select the **Configure resources** button.



3. Choose your resources

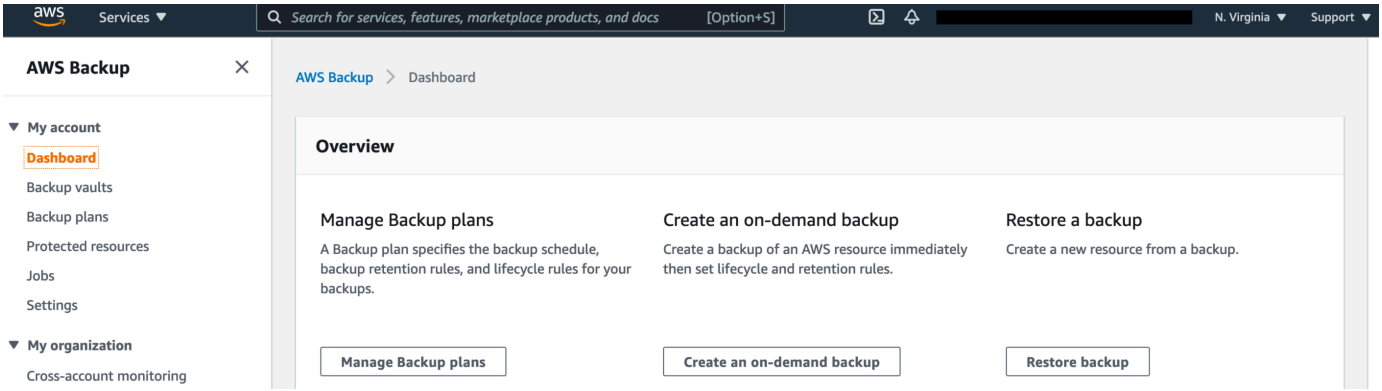
   On the **Configure resources** page, use the toggle switches to enable or disable the services used with AWS Backup. In this case, select **EBS**. Choose **Confirm** when your services are configured.

   - 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 2.6 for information on cross-Region copy). This tutorial uses the US East (N. Virginia) Region (us-east-1).



4. Create an on-demand backup

   Back in the AWS Backup console, under **My account**, select **Dashboard** on the left navigation pane. Then, select the **Create on-demand backup** button.



5. Configure backup settings

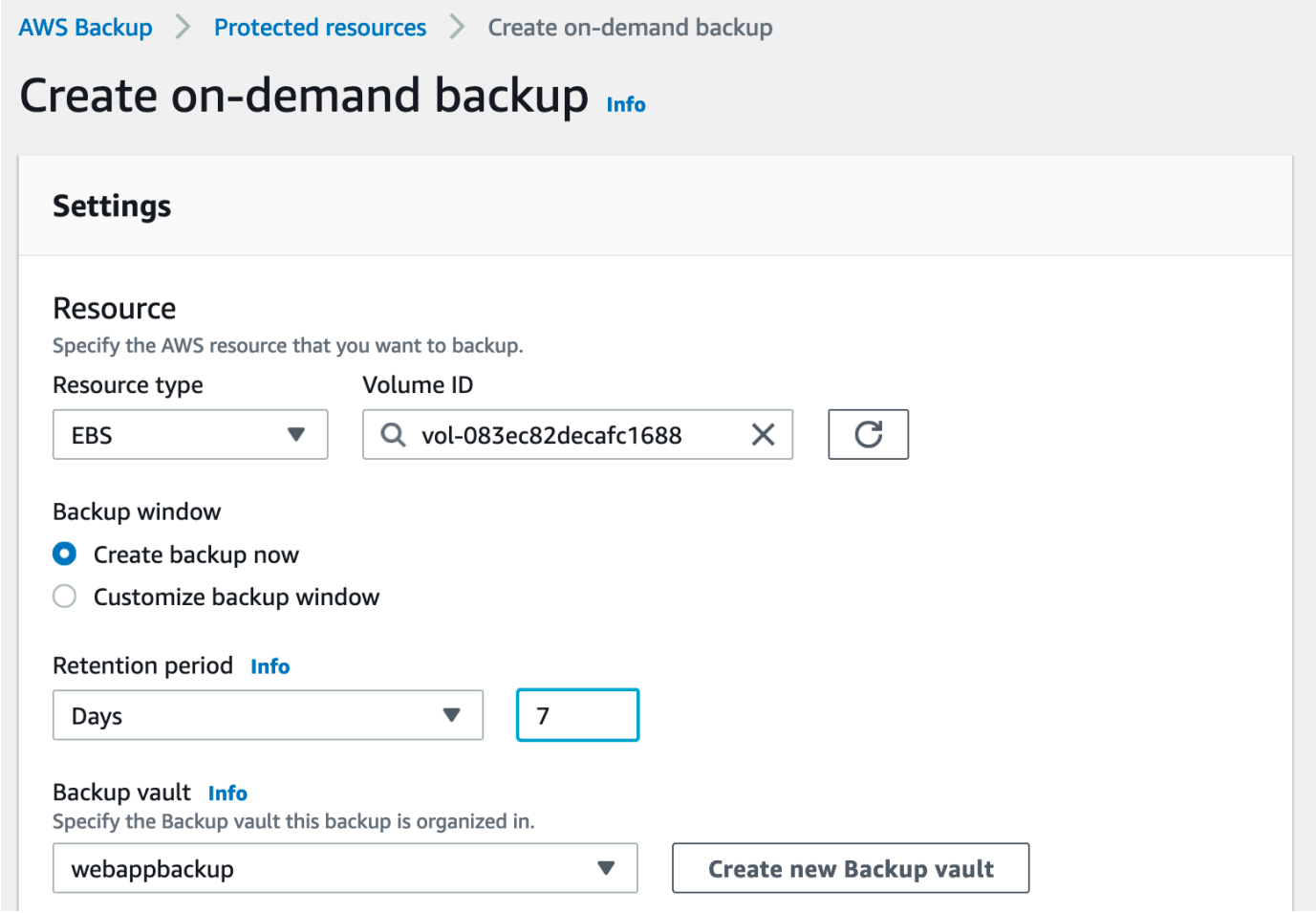
On the **Create on-demand backup** page, choose the **Resource type** that you want to back up; for example, choose **EBS** for Amazon EBS.

Choose the **Volume ID** of the EBS resource that you want to protect.

In the **Backup window** section, select **Create backup now**. This initiates a backup immediately and enables you to see your saved resource sooner on the **Protected resources** page.

In the **Retention period** section, select **Days** and type the number of days you want to retain the backups for. In this example, we entered in "7" days.

In the **Backup vault** section, select one of the pre-existing vaults and continue, or follow the next optional step to create a new backup vault (which begins with selecting **Create new Backup vault**) before continuing.



6. Create a backup vault

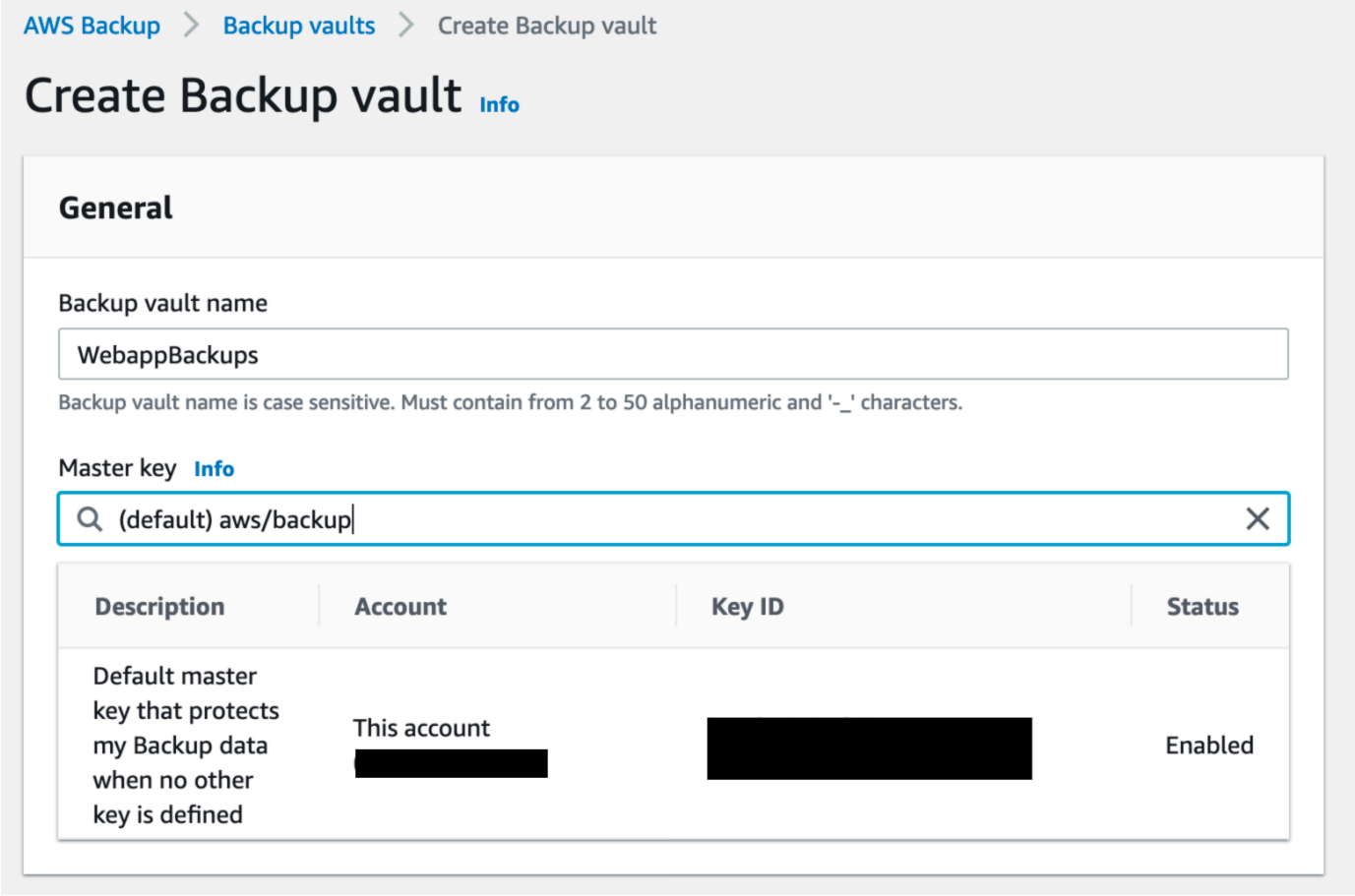
Create a backup vault: Instead of using the default backup vault that is automatically created for you on the AWS Backup console, you can create specific backup vaults to save and organize groups of backups in the same vault.

On the **Create on-demand backup** page, choosing **Create new Backup vault** opens a new page to create a vault, and you are returned to the **Create on-demand backup** page after you are finished.

You can also go to the AWS Backup console in the navigation pane on the left and select **Backup vaults** and then **Create backup vault** to create a backup vault.

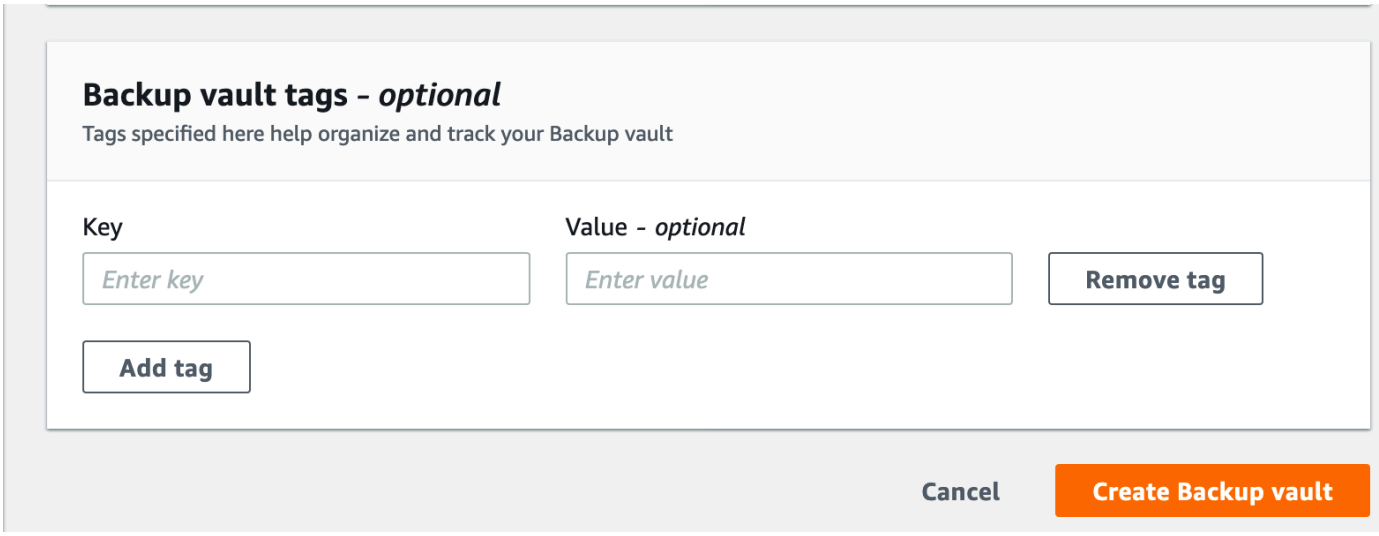
Enter a name for your backup vault. You can name your vault to reflect what you will store in it, or to make it easier to search for the backups you need. For example, you could name it "webappBackups."

Select an AWS Key Management Service (KMS) key. You can use either a key that you already created, or select the default AWS Backup master key.



7. (Optional) Add tags

   Optionally, add tags that will help you search for and identify your backup vault.

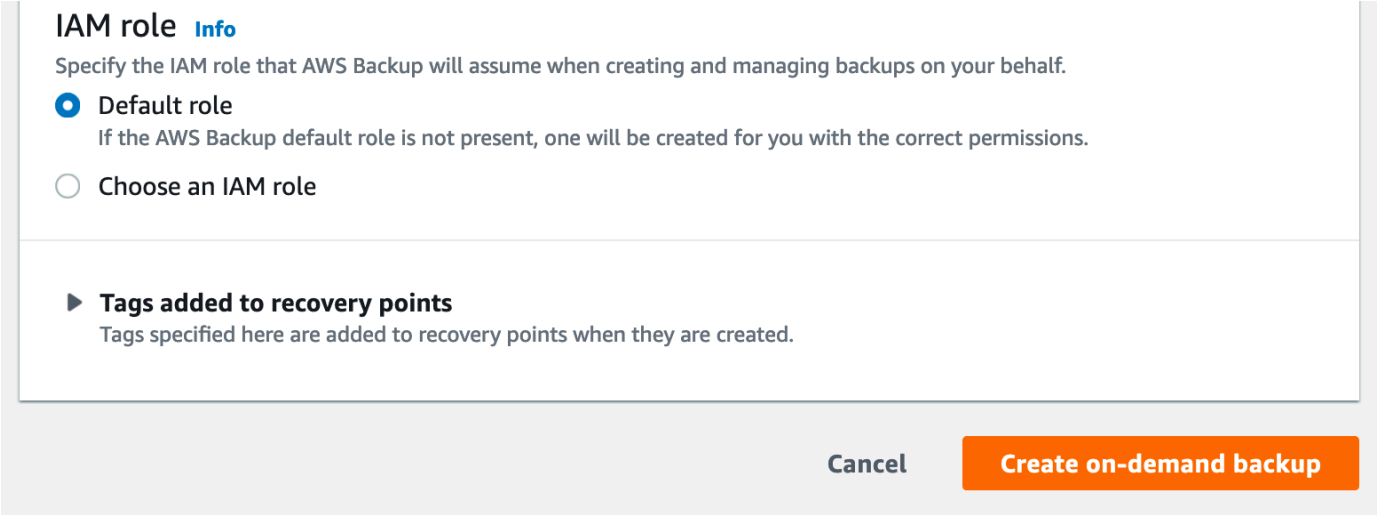


8. Choose a default IAM role

   Back on the **Create on-demand backup** page, after you have selected an existing backup vault or created a new one, choose the **Default role** for the **IAM role**, as shown in the following screenshot, or **Choose an IAM role**.

> **Note**
>
> If the AWS Backup **Default role** is not present in your account, then one 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.

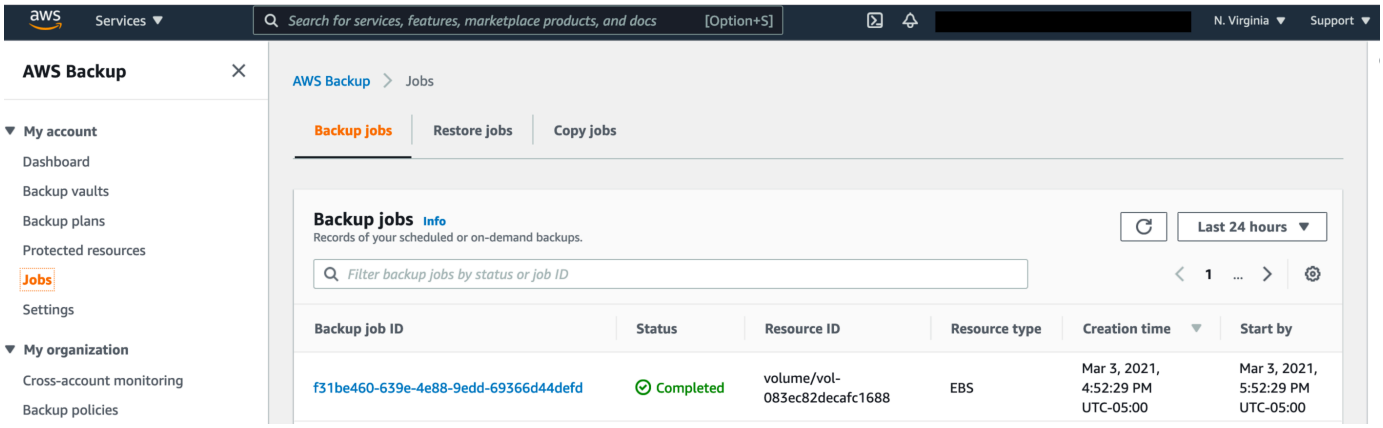


9. Monitor the status of the backup job

   In the **Jobs** panel under **My account**, ensure the **Backup jobs** tab is selected.

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

   After some time, the **Status** of the backup job will go from **Created** to **Completed**.

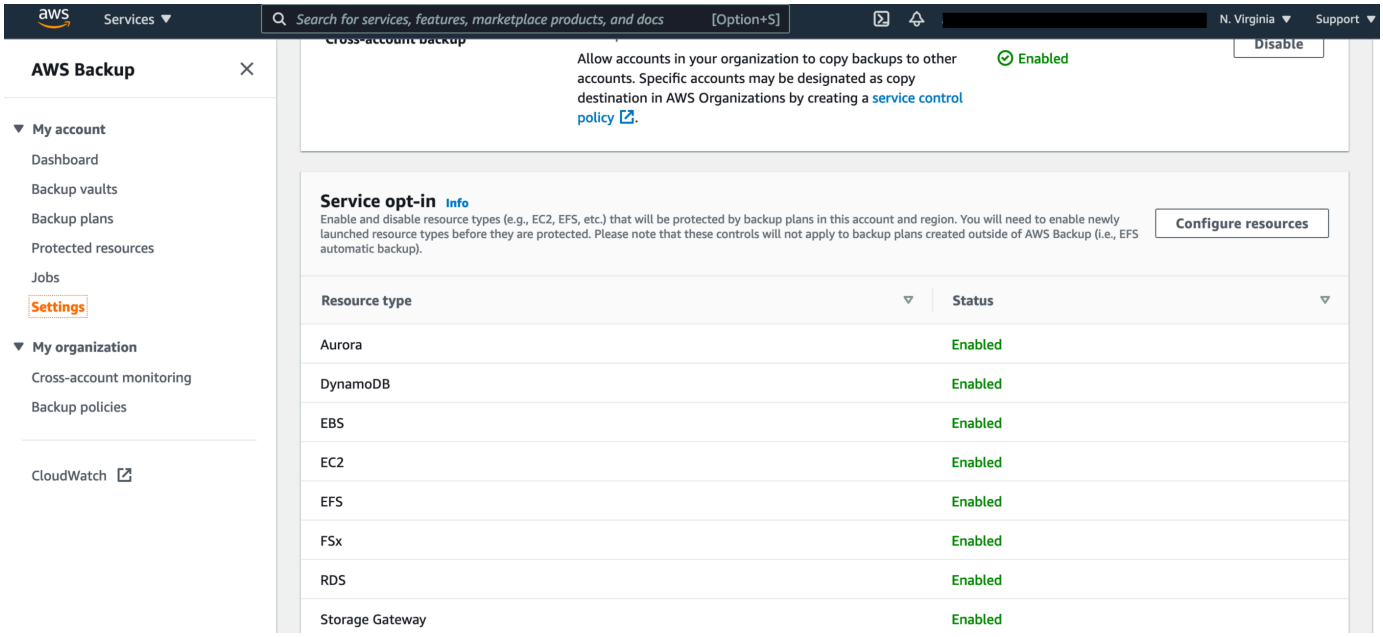


Step 2: Configure an automatic AWS Backup job of an Amazon EBS volume

1. 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**.

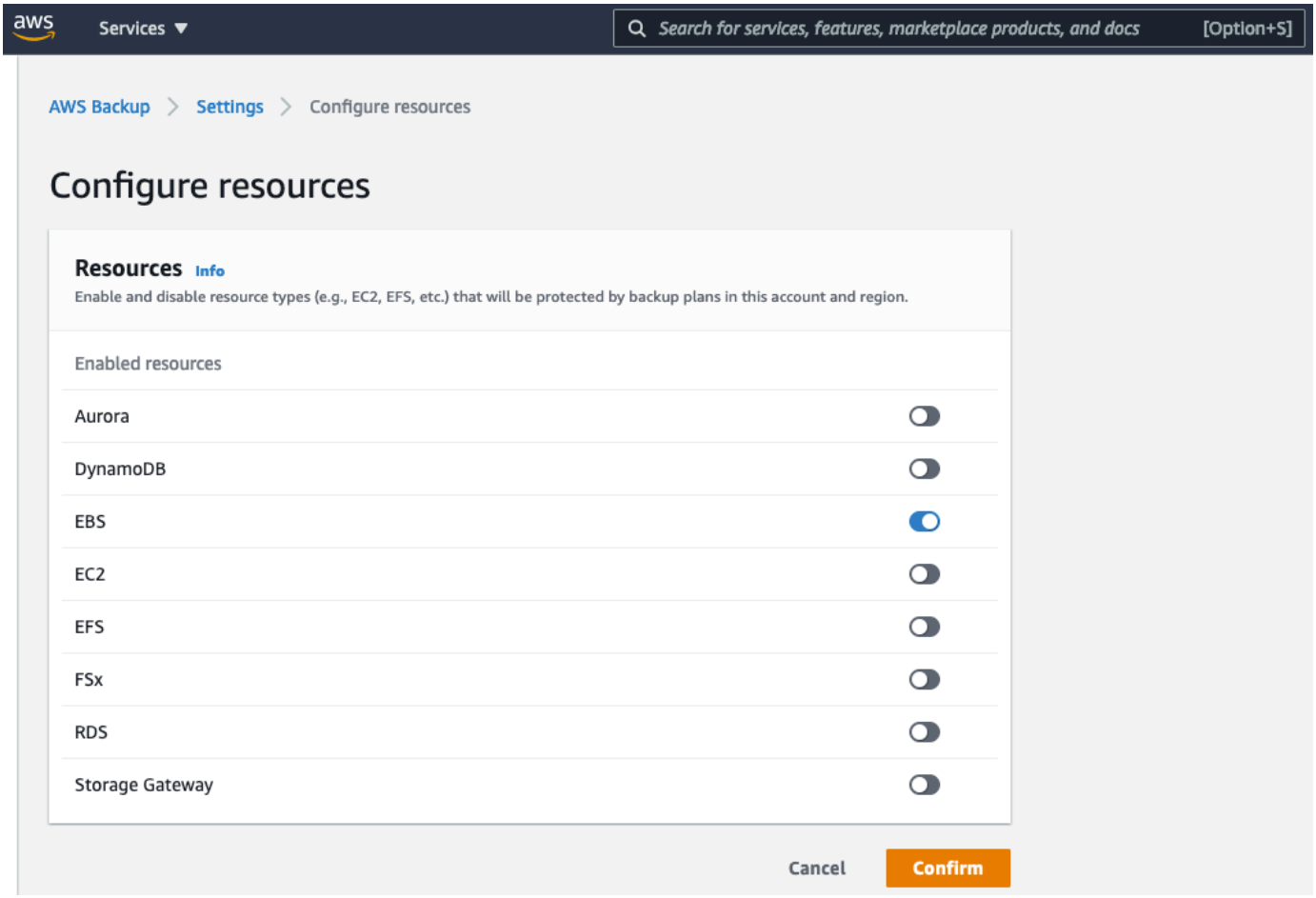
   On the **Service opt-in** page, select the **Configure resources** button.



2. Choose your resources

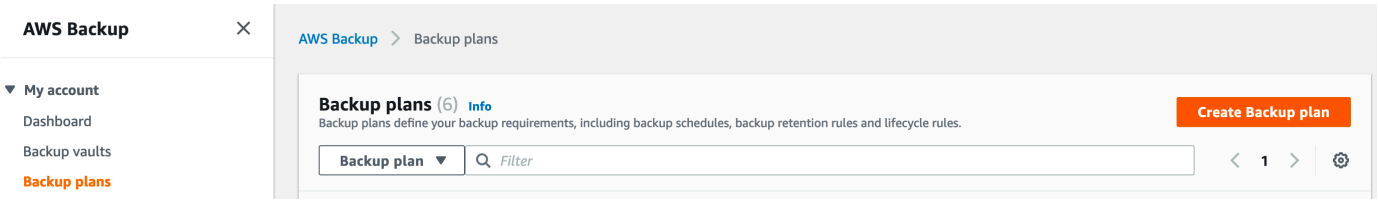
   On the **Configure resources** page, use the toggle switches to enable or disable the services used with AWS Backup. Choose **Confirm** when your services are configured.

   - 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 3.2 for information on cross-Region copy). This tutorial uses the US East (N. Virginia) Region (us-east-1).



3. Configure a backup plan for an Amazon EBS volume

   In the AWS Backup console, select **Backup plans** on the left rail, under **My account**, and then select the **Create Backup plan** button.



4. Choose how to begin

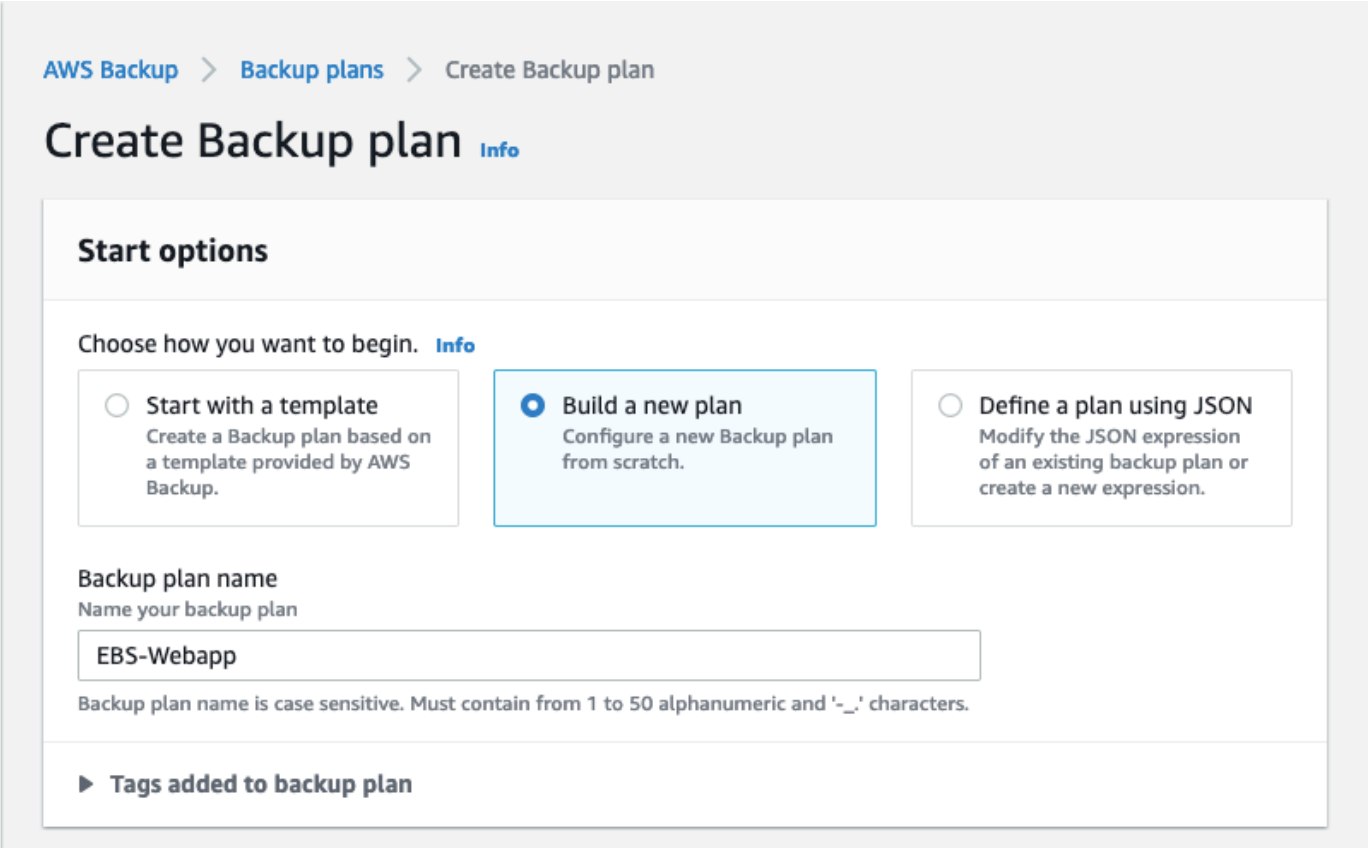
   AWS Backup provides three ways to get started using the AWS Backup console:

   - **Start from an existing plan:** You can create a new backup plan based on the configurations in an existing plan. 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 from scratch:** 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.



5. Configure the backup rule

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.

In the **Backup vault** section, you can select the default vault or one of the pre-existing vaults. 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 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.

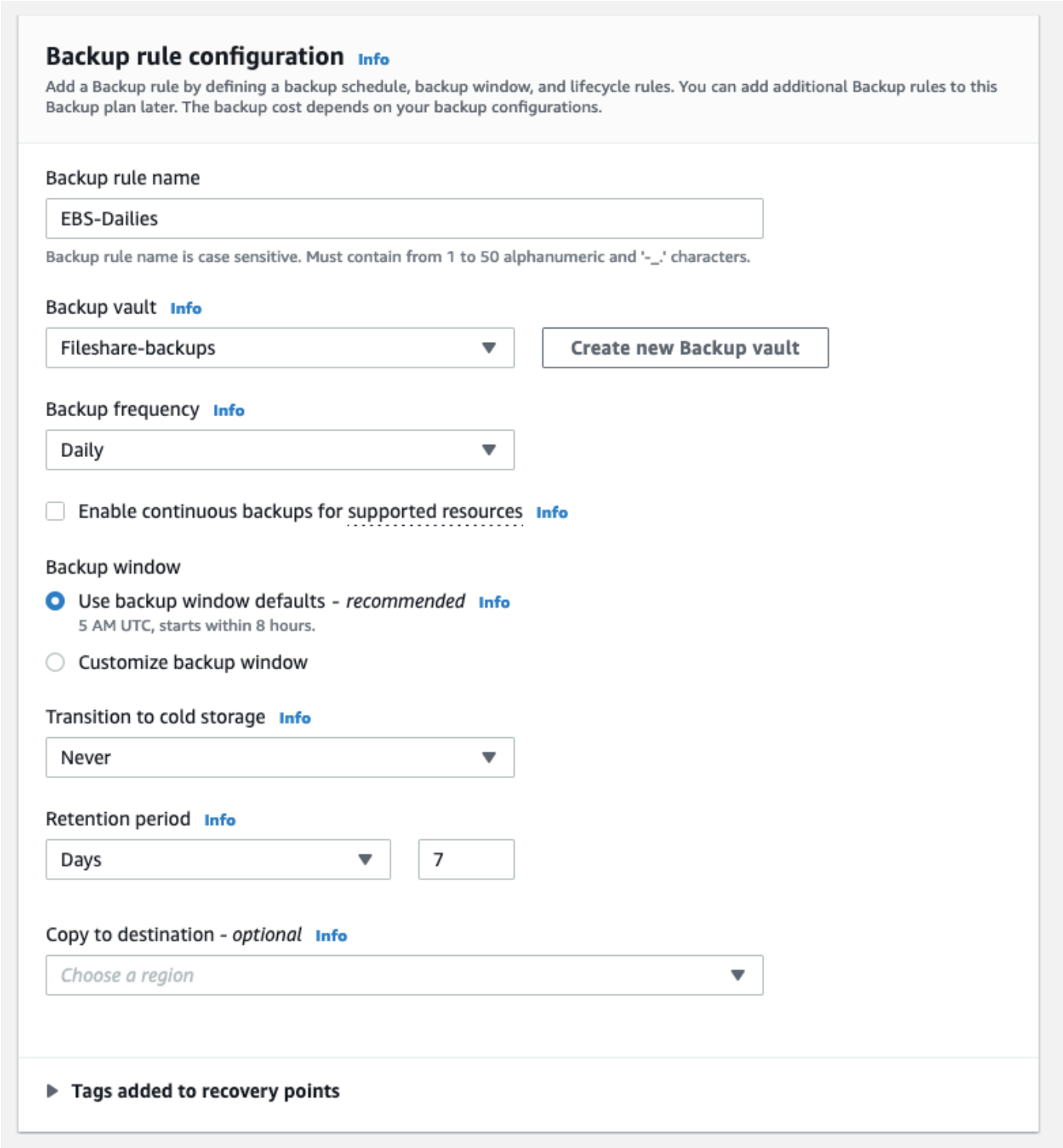
Create new Backup vault - Instead of using the default backup vault that is automatically created for you on the AWS Backup console, you can create specific backup vaults to save and organize groups of backups in the same vault. To create a new backup vault, refer to step 7 below.

In the **Backup Frequency** section, Choose **Daily**. 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.

In the **Backup window** section, select **backup window defaults**, which initiates the backup job at 5 AM UTC (Coordinated Universal Time) and lasts 8 hours. If you would like to customize the backup frequency, refer to the documentation for more information.

In the **Transition to cold storage** section, keep the default - **Never**.

In the **Retention period** section, select **Days** and type "7" (or you can put in any number of days as desired).



6. Continue configuring the backup rule

   In the **Copy to destination** section, leave it as the default, since this tutorial covers backups within the same AWS Region. 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 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:

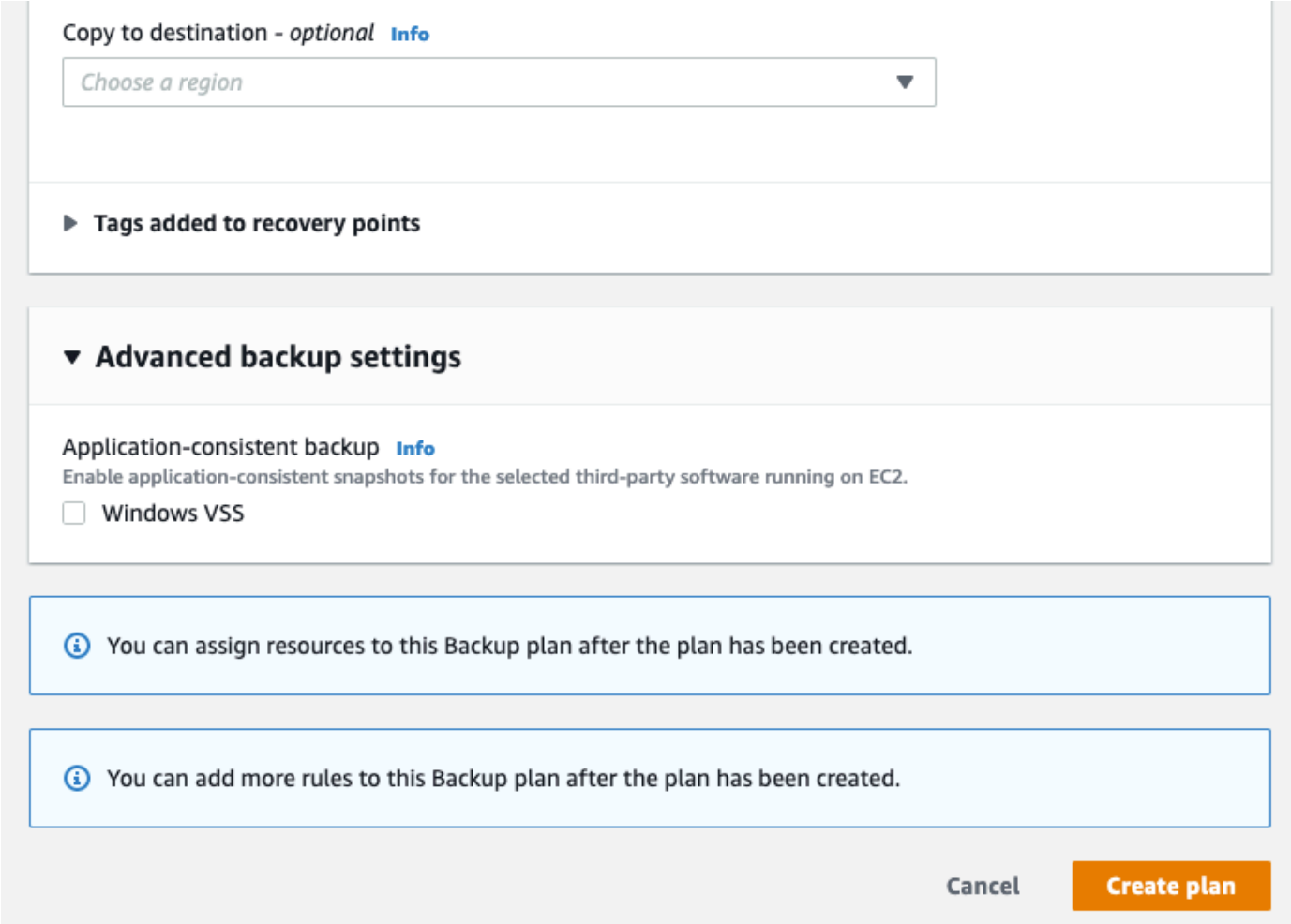
- Destination Region: The destination Region for the backup copy
- (Advanced Settings) Backup Vault: The destination backup vault for the copy.
- (Advanced Settings) IAM Role: The IAM role that AWS Backup uses when creating the copy. The role must also have AWS Backup listed as a trusted entity, which enables AWS Backup to assume the role. If you choose **Default** and the AWS Backup default role is not present in your account, a role is created for you with the correct permissions.
- (Advanced Settings) Lifecycle: Specifies when to expire (delete) the copy.

> **Note**
>
> Cross-region copy incurs additional data transfer costs. You can refer to the AWS Backup pricing page.

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. You can refer to the documentation for more details.

Then, select the **Create Plan** button. Once the plan is created, tags and resources can be added to the backup plan.



7. Create a backup vault

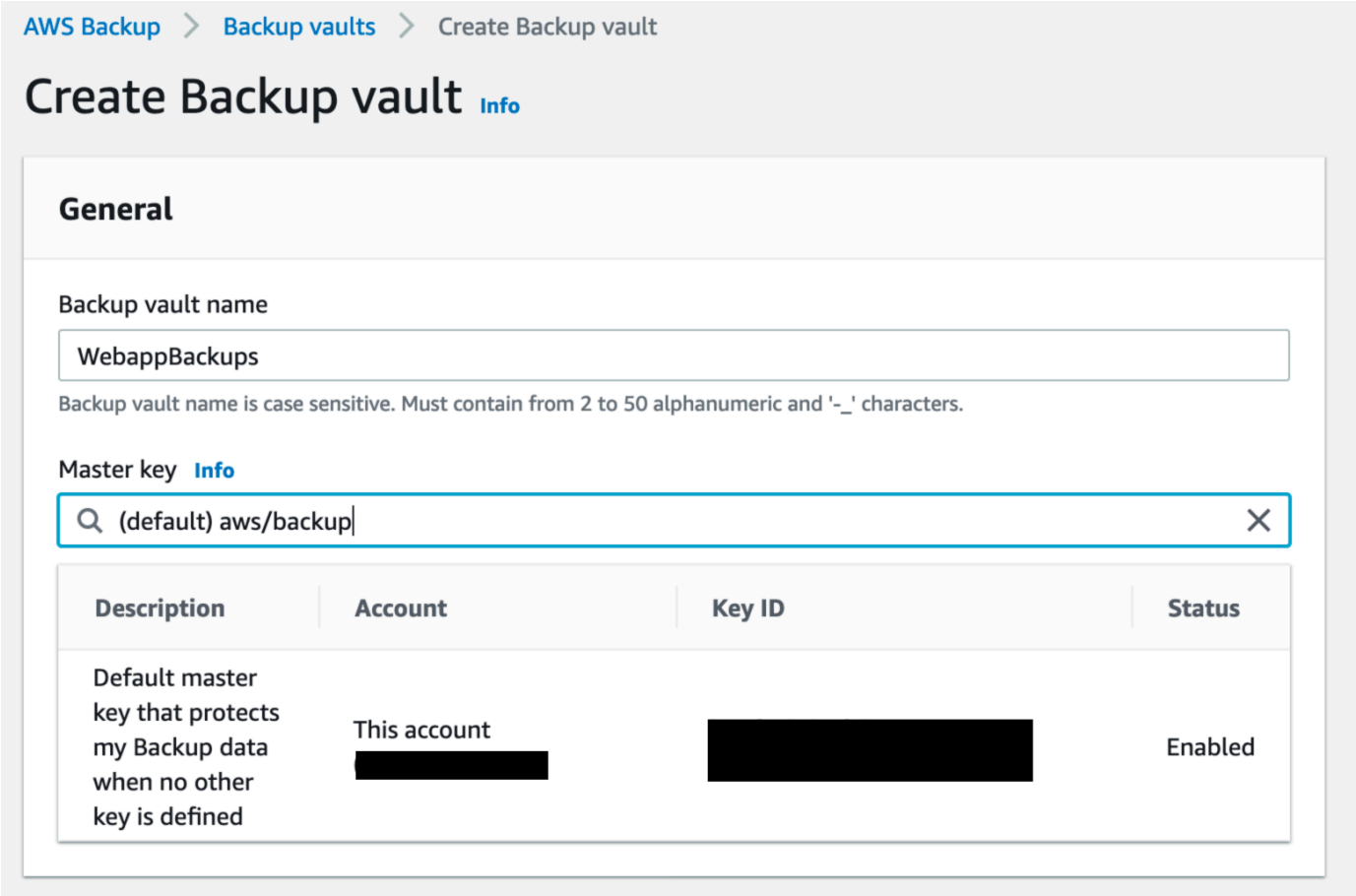
   In the AWS Backup console, in the left navigation pane, select **Backup vaults**.

   Select **Create 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 "WebappBackups."

   Select an AWS KMS key. You can use either a key that you already created, or select the default AWS Backup master key.

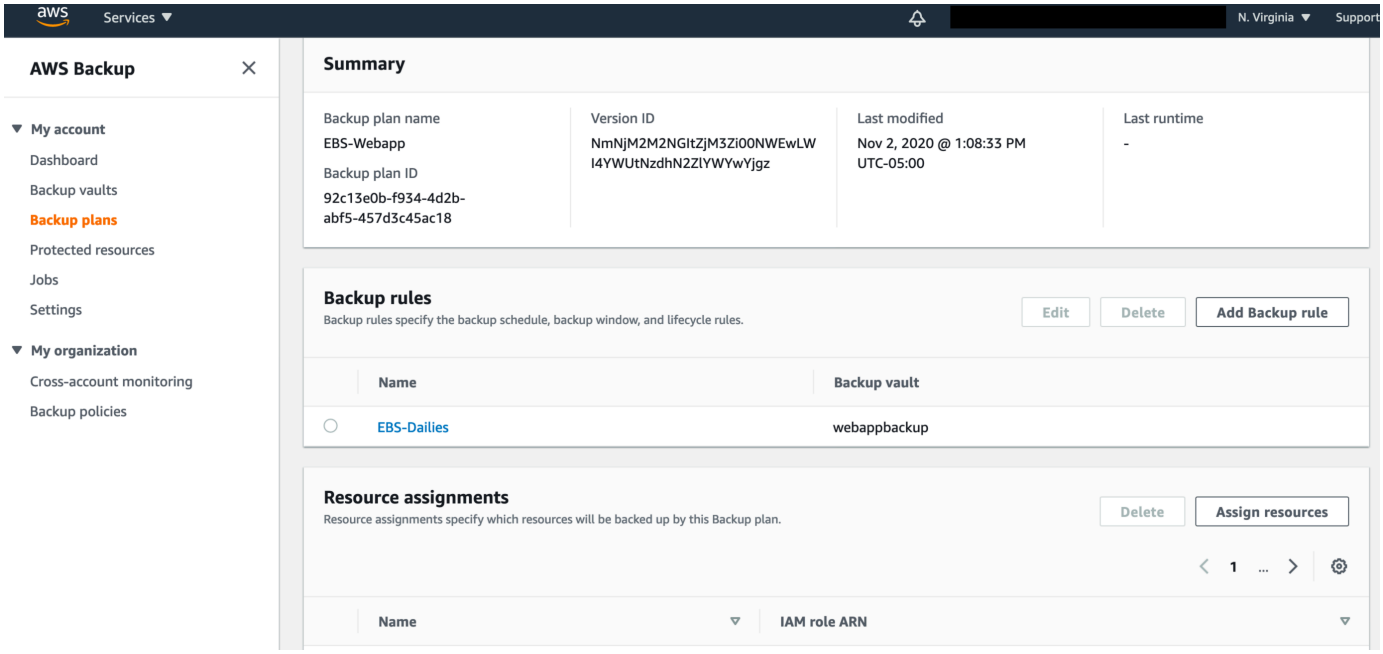
   Optionally, add tags that will help you search for and identify your backup vault.



8. Assign resources to the backup plan

   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.

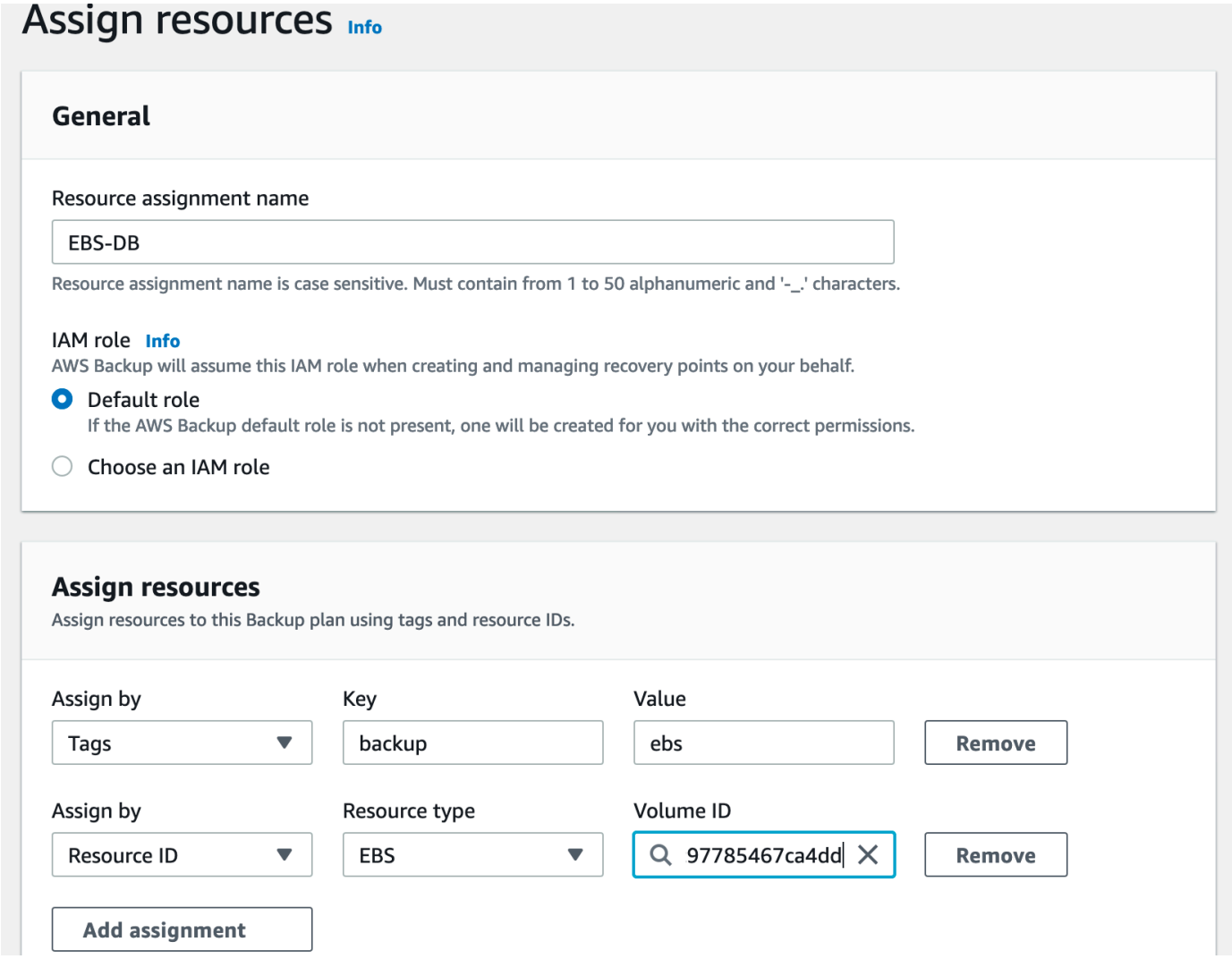
   Select the created backup plan and select the **Assign resources** button.



9. Enter configuration details

   Enter configuration details for your resources.

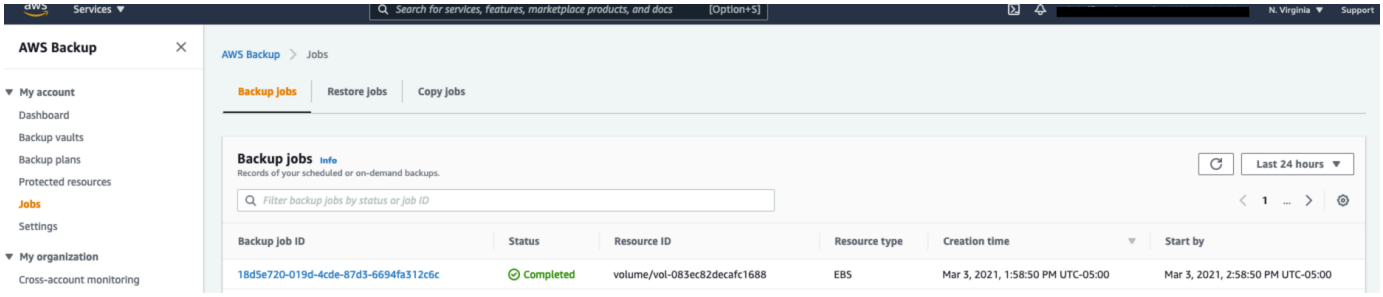
   - **Resource assignment name**:Provide a resource assignment name.
   - **IAM Role**: When creating a tag-based backup plan, if you choose a role other than Default role, make sure that it has the necessary permissions to back up all tagged resources. AWS Backup tries to process all resources with the selected tags. If it encounters a resource that it doesn't have permission to access, the backup plan fails.
   - **Assign by**: You can select **Tags** or **Resource ID**. For a tags-based resource assignment, provide the key-value pair of the EBS Volume.
   - Select **Assign resources.** The backup plan will then have the resources assigned to it.



10. View your backup jobs

    Navigate to the AWS Backup console and select **Jobs** in the left navigation pane. You will then be able to see your **Backup jobs**.

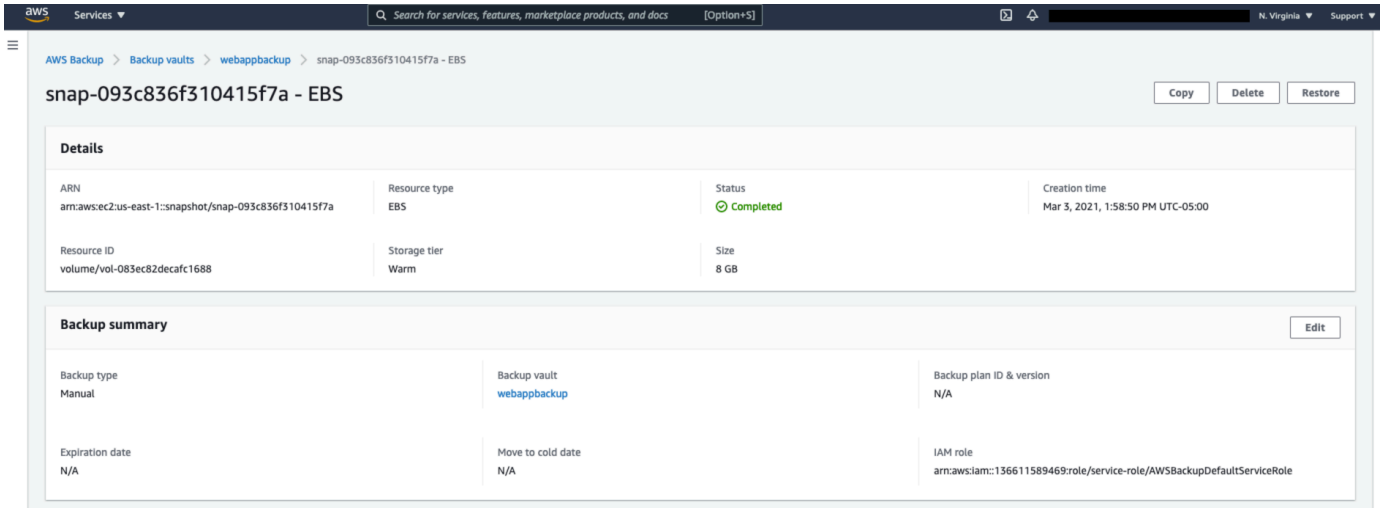
    A backup, or recovery point, represents the content of a resource, such as an Amazon EBS volume or Amazon RDS database, at a specified time. Recovery point is a term that refers generally to the different backups in AWS services, such as Amazon EBS snapshots and Amazon RDS backups. In AWS Backup, recovery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



Step 3: Restore an Amazon EBS volume using AWS Backup

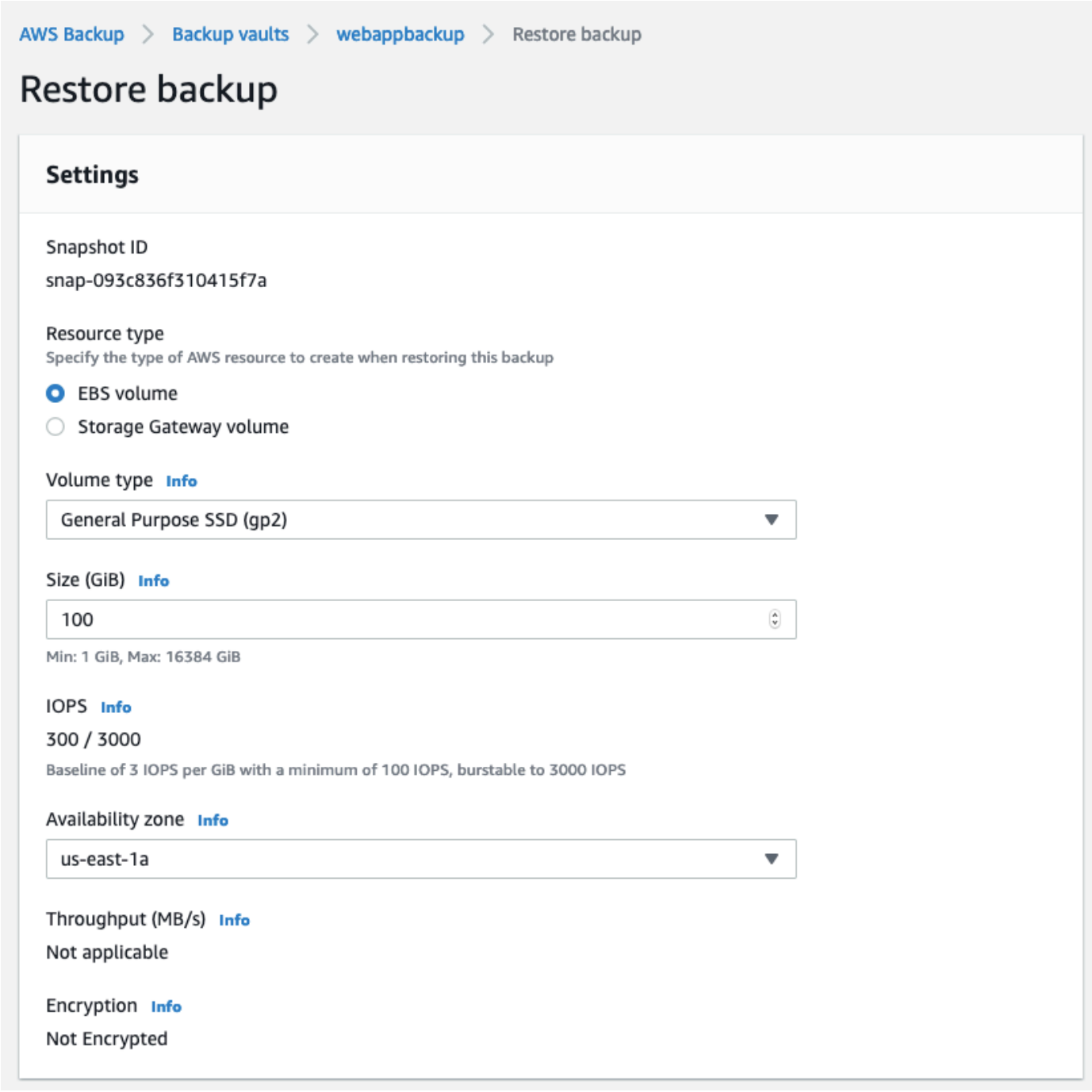
1. Start the restore

   Navigate to the backup vault that was selected in the backup plan and select the latest completed backup. To restore the EBS volume, click on the recovery point ARN and select the **Restore** button.



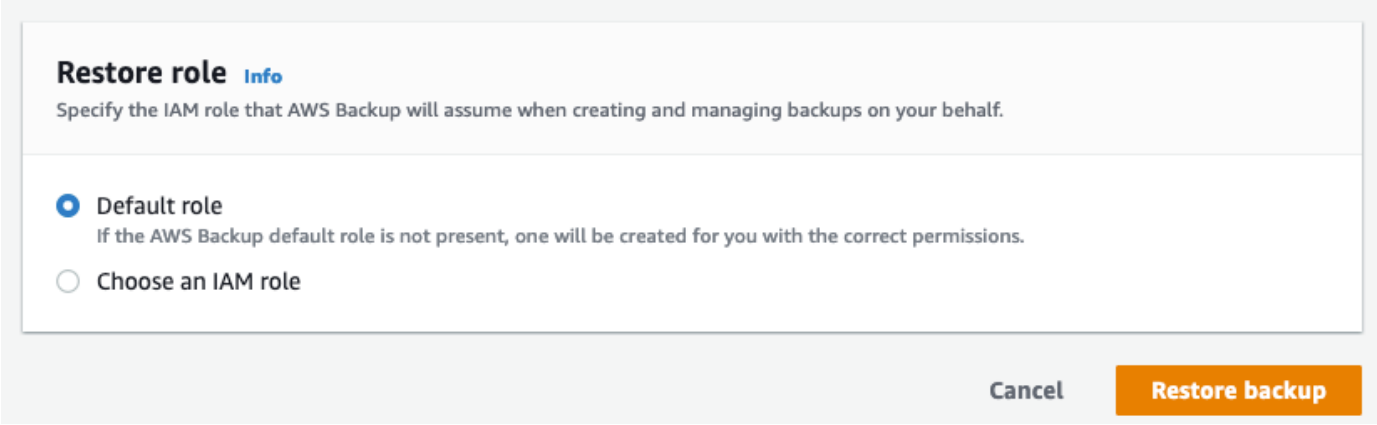
2. Configure restore settings

   - The restore of the ARN will bring you to a **Restore backup** screen that will have the snapshot ID, and other configurations.
   - **Resource Type**: Specify **EBS volume**.
   - **Volume type**: Select **General Purpose SSD (gp2)**.
   - **Size**: Select 100 GB (equivalent size of the backed up EBS volume).
   - **IOPS**: 300/3000 - Baseline of 3 iops per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.
   - **Availability Zone**: Select the Availability Zone, if you have a preference.



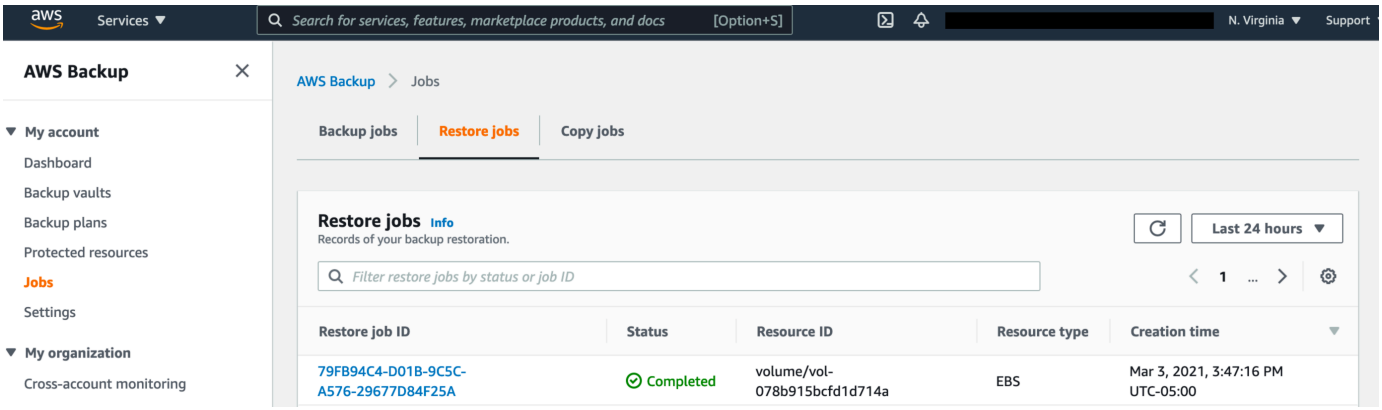
3. Choose a restore role

   Select **Default role** and the select the **Restore backup** button.



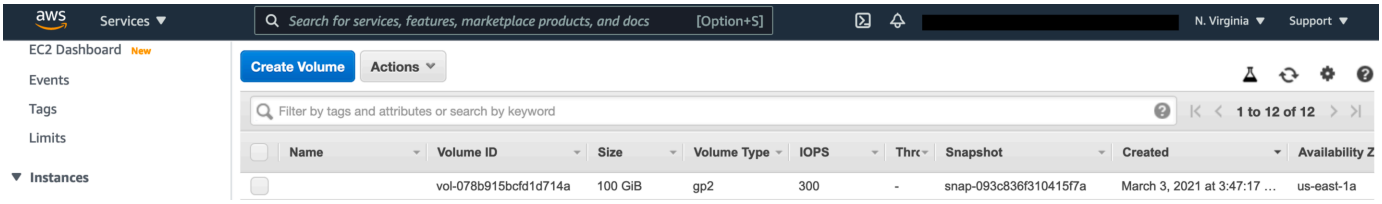
4. View the backup job

   The restored backup job will appear under **Restore jobs** in the the AWS Backup console.



5. View the restored EBS volumes

   Once the job status appears as completed, navigate to the Amazon EC2 console, select V**olumes** under **Elastic Block Store** to see the restored EBS volumes.



Next steps

You can mount the restored Amazon EBS volume on an Amazon EC2 instance to access the files and directories that were restored from a snapshot copy of the EBS volume.

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.

Delete the EBS volume

1. Open the Amazon EC2 console.
2. In the navigation pane on the left, choose **Volumes** under **Elastic Block Store**.
3. Select the restored EBS volume, and choose **Actions**, **Detach Volume**.
4. Once the EBS volume is detached, choose **Actions**, **Delete Volume**. Choose **Yes**, **Terminate** when prompted for confirmation.

Delete the AWS Backup recovery point

1. Open the AWS Backup console and navigate to the vault where the recovery point is stored.
2. Select the recovery point, then select **Delete**.

> **Note**
>
> This process can take several seconds to complete.

Congratulations!

You have created a backup of an Amazon EBS volume and performed a restore of an EBS volume using AWS Backup!