

To configure Veeam Backup for AWS, please follow the outlined process below:

1. ****Create an IAM Role in AWS****

Begin by creating an IAM role in AWS with the necessary permissions to establish an account in Veeam

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "<Role ARN>"
      }
    }
  ]
}
```

Provide the role name and relevant details in the accounts segment of Veeam, then proceed to the next step

← Add IAM Role

Role Name Specify IAM role friendly name and description

Role Settings Friendly name:

Summary Description:

Next, specify the role settings for the account and continue

← Add IAM Role

Role Name

Role Settings

Summary

Specify IAM role type and settings

IAM role from current account

AWS role name: ⓘ

IAM role from another account

Create new IAM role

2. ****Configure the Repository for Veeam****

Specify the repository name and description, then select next.

← Add Repository

Info

Bucket

Summary

Specify repository name and description

Enter a name and description for the repository.

Name:

Description:

Next Cancel

Provide the IAM user and bucket details in this section

The screenshot shows the 'Add Repository' configuration page in the AWS Backup console. The 'Bucket' tab is selected in the left-hand navigation pane. The main content area is titled 'Configure general settings' and includes the following sections:

- Info:** Select an IAM role to be used to access the repository and an Amazon S3 bucket where backup files will be stored.
- IAM role:** A dropdown menu is set to 'Default Backup Restore (Default Backup Restore)'. There are '+ Add' and 'Check Permissions' links.
- Location:** A 'Bucket:' label is followed by a folder icon and a 'Choose bucket...' link.
- Use existing folder:** A radio button is selected, followed by a folder icon and a 'Choose folder...' link.

At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Additionally, define the storage class and immutability settings for the repository

The screenshot shows the 'Add Repository' configuration page in the AWS Backup console, focusing on storage class and immutability settings. The 'Storage class' dropdown is set to 'Select...'. Below it is an information box stating: 'Due to higher retrieval costs and early deletion fees, the S3 Glacier Deep Archive class is best suited for long-term storage. For more information, see the User Guide.' The 'Immutability settings' section includes the text: 'Protect backups from modification or deletion by ransomware, hackers, or malicious insiders using native object storage capabilities.' and a checkbox labeled 'Backups stored in this repository will be immutable', which is currently unchecked. Below this is another information box: 'S3 Object Lock must be enabled at the bucket level to use immutability.' At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.

You can also choose to enable encryption for the repository

Storage class: Select...

i Due to higher retrieval costs and early deletion fees, the S3 Glacier Deep Archive class is best suited for long-term storage. For more information, see the [User Guide](#).

Immutability settings

Protect backups from modification or deletion by ransomware, hackers, or malicious insiders using native object storage capabilities.

Backups stored in this repository will be immutable

i S3 Object Lock must be enabled at the bucket level to use immutability.

Previous Next Cancel

Review the summary and select "Finish" to complete the repository setup.

← Add Repository

Info

Bucket

Encryption

Summary

Review configured settings

Review the repository settings, and click Finish to exit the wizard.

i To verify whether the selected IAM role has all the necessary permissions assigned, run a permission check.

Check Permissions Copy to Clipboard

Info

Name:	NA
Description:	Na

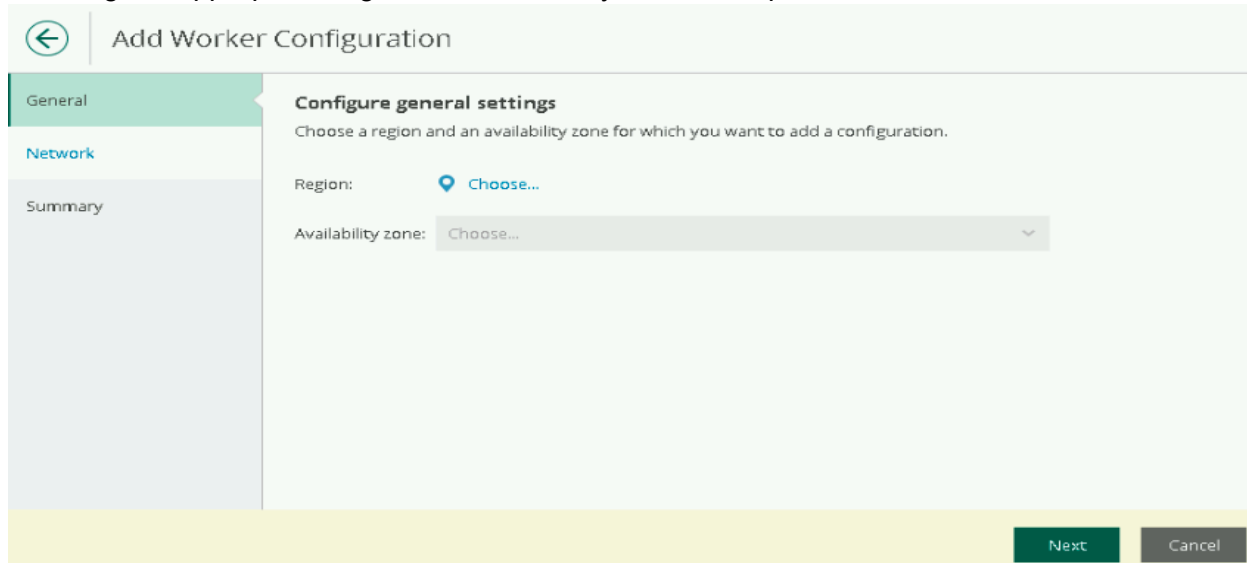
Bucket

IAM role:	veeam-default-user
Storage class:	S3 Standard
Region:	Asia Pacific (Mumbai)

Previous Finish Cancel

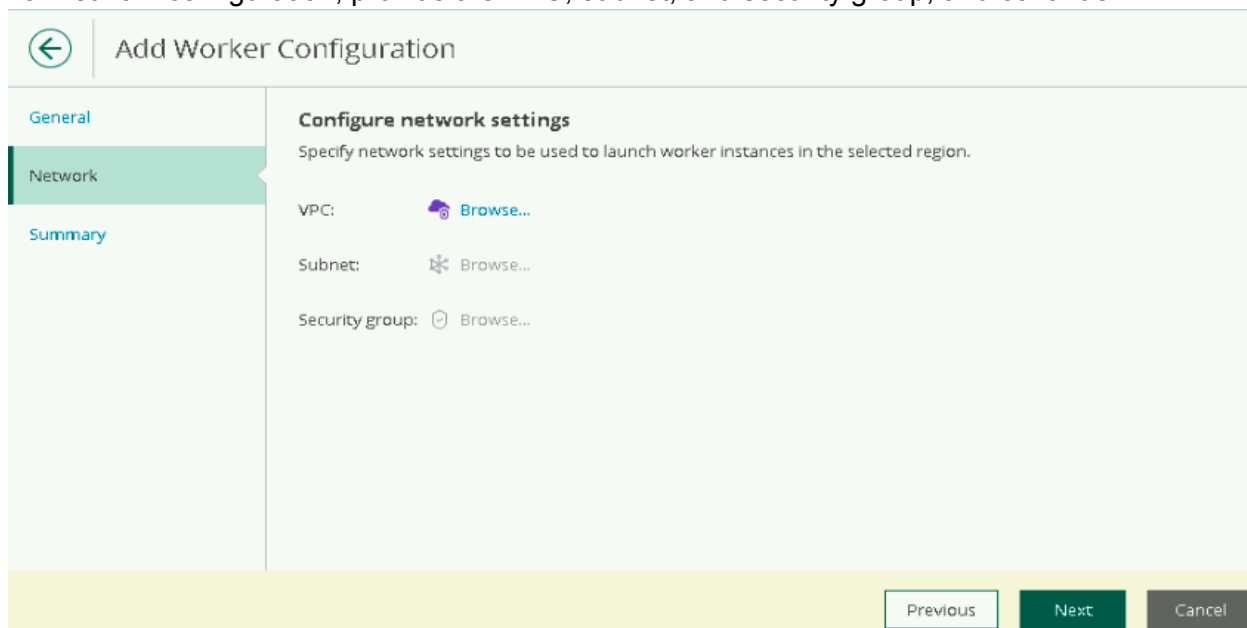
3. ****Create a Worker for Veeam Tasks****

Create a worker for Veeam to execute tasks, Since the worker is region-specific, begin by selecting the appropriate region and availability zone, then proceed



The screenshot shows the 'Add Worker Configuration' wizard in the 'General' step. The left sidebar has 'General' selected, with 'Network' and 'Summary' below it. The main area is titled 'Configure general settings' and contains the instruction: 'Choose a region and an availability zone for which you want to add a configuration.' Below this are two fields: 'Region:' with a location pin icon and a 'Choose...' button, and 'Availability zone:' with a dropdown menu showing 'Choose...'. At the bottom right, there are 'Next' and 'Cancel' buttons.

For network configuration, provide the VPC, subnet, and security group, and continue



The screenshot shows the 'Add Worker Configuration' wizard in the 'Network' step. The left sidebar has 'Network' selected, with 'General' and 'Summary' above it. The main area is titled 'Configure network settings' and contains the instruction: 'Specify network settings to be used to launch worker instances in the selected region.' Below this are three fields: 'VPC:' with a globe icon and a 'Browse...' button, 'Subnet:' with a network icon and a 'Browse...' button, and 'Security group:' with a lock icon and a 'Browse...' button. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons.

After verifying the configuration in the summary, select "Finish" to finalize the update.

The screenshot shows the 'Add Worker Configuration' wizard in the 'Summary' step. The left sidebar has 'Summary' selected. The main content area is titled 'Review configured settings' and contains the following information:

- General**
 - Region: Asia Pacific (Mumbai)
 - Availability zone: ap-south-1a
- Network**
 - VPC: 6eMUM_Prod (10.0.0.0/16)
 - Subnet: 10.0.0.0/24 (ap-south-1a)
 - Security group: 6e-mum-capd-prod
- Verification checks**
 - Auto-assign public IPv4: ⚠ Auto IP-assignment is off. To work in a private network, configure endpoints for Amazon services. For more information, see the [User Guide](#).

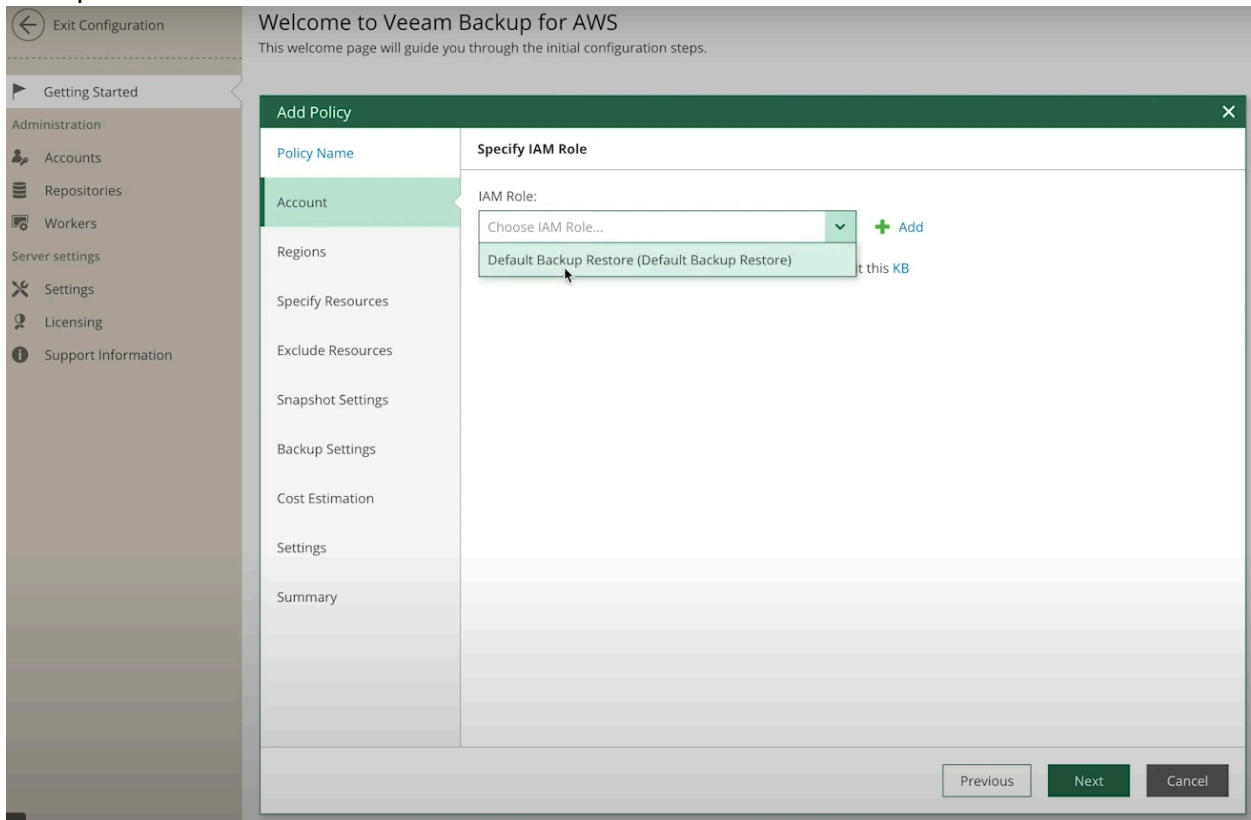
At the bottom right, there are three buttons: 'Previous' (disabled), 'Finish' (active), and 'Cancel' (disabled).

4. ****Configure Backup and Snapshot Policy****

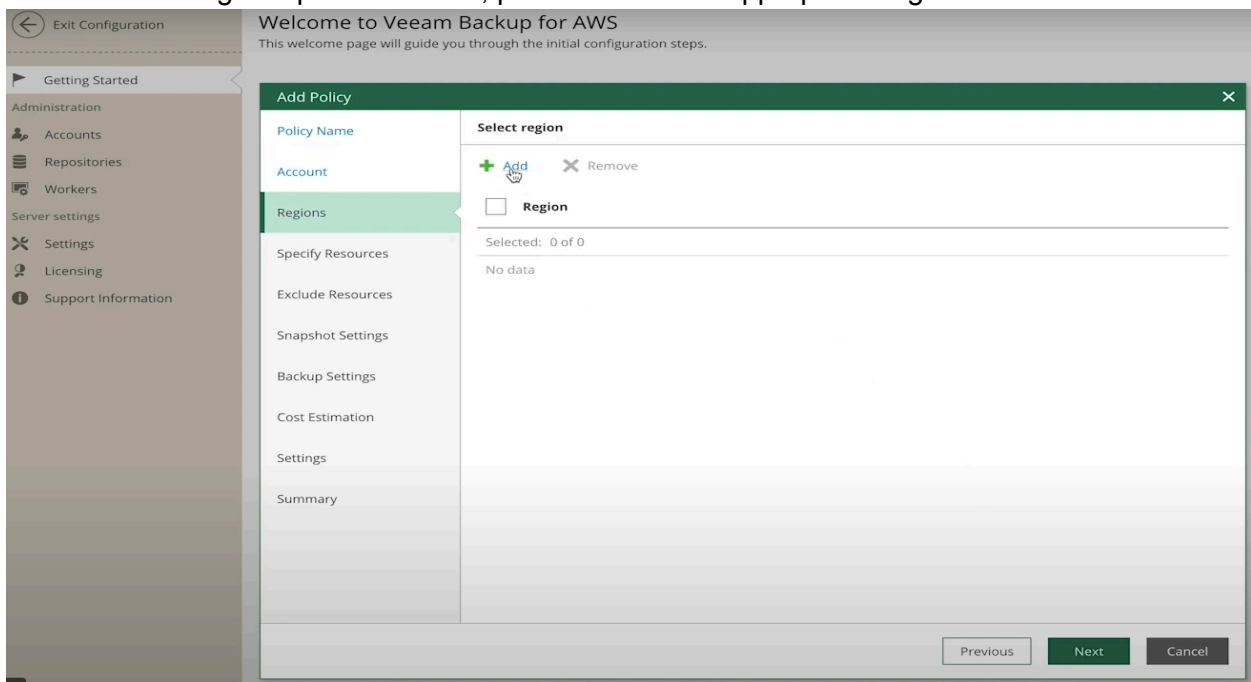
After setting up the Account, Repository, and Agent, configure the policy for taking snapshots and backups. Start by defining the policy name and description.

The screenshot shows the 'Add Policy' dialog box in the Veeam Backup for AWS console. The dialog is titled 'Add Policy' and has a 'Specify policy name and description' section. The 'Policy Name' field contains 'VeeamBackupPolicy' and the 'Description' field is empty. The left sidebar of the console is visible, showing the 'Administration' section with 'Accounts' selected. The 'Add Policy' dialog has a 'Next' button (disabled) and a 'Cancel' button (disabled) at the bottom right.

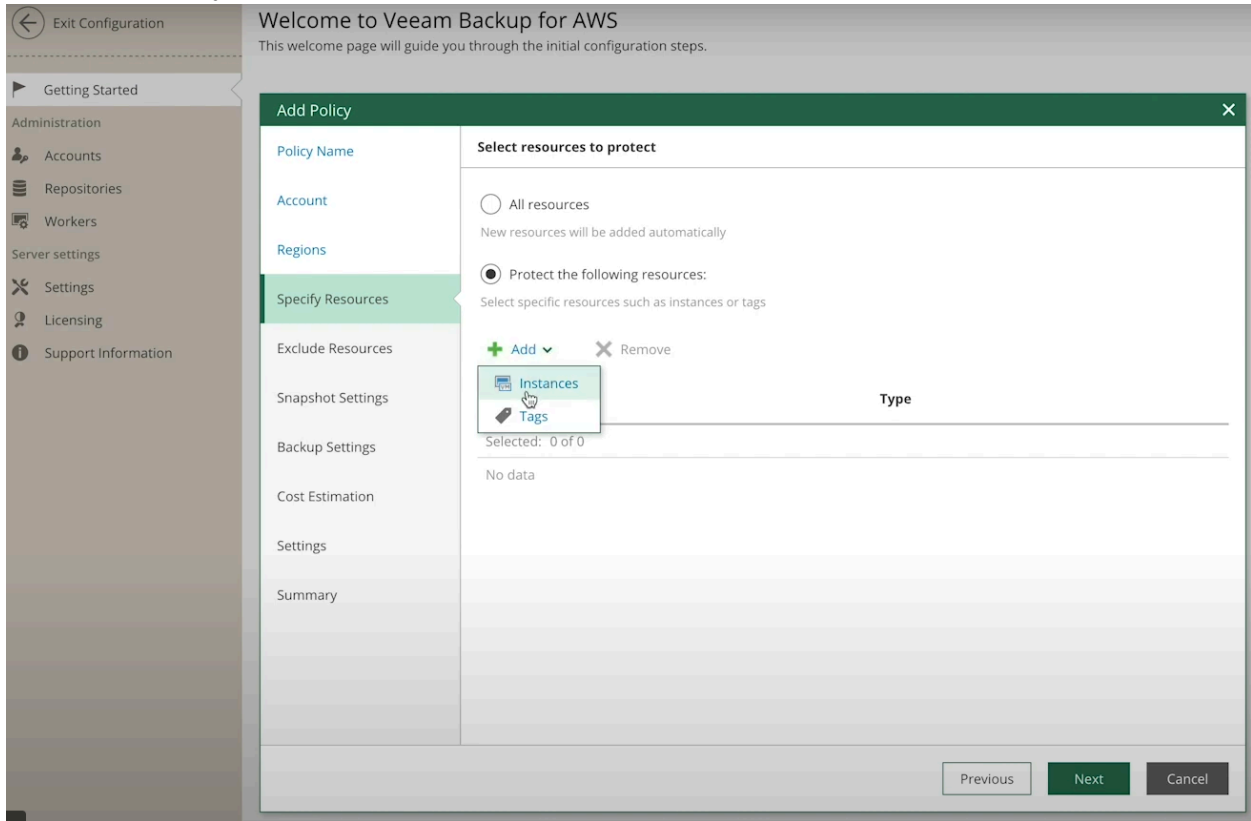
Then provide the IAM account details:



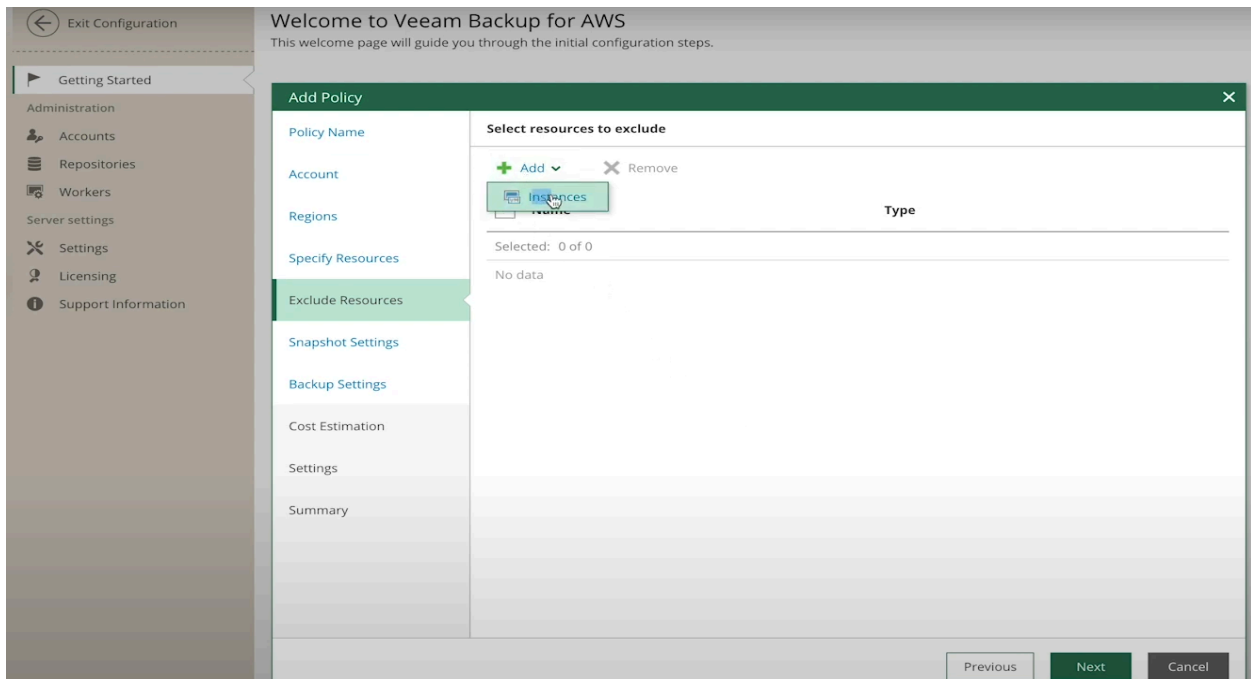
Since this is a region-specific service, please select the appropriate region



Identify the resources within that region for the operation; you may choose to include all resources or only protected ones



We can also exclude certain resources if desired:



Specify the snapshot frequency and retention period:

Exit Configuration

Welcome to Veeam Backup for AWS
This welcome page will guide you through the initial configuration steps.

Getting Started

- Administration
- Accounts
- Repositories
- Workers
- Server settings
- Settings
- Licensing
- Support Information

Add Policy

Policy Name

Account

Regions

Specify Resources

Exclude Resources

Snapshot Settings

Backup Settings

Cost Estimation

Settings

Summary

Specify snapshot settings

Enable snapshots

Snapshot Settings

Number of restore points to keep: 7

Schedule

Create snapshots automatically

Daily at this time: 10:00 PM Everyday 7 Days...

Monthly at this time: 12:00 AM First Monday 30 Months...

Periodically every: 1 Hours Schedule...

Previous Next Cancel

Specify the backup frequency and retention period:

Exit Configuration

Welcome to Veeam Backup for AWS
This welcome page will guide you through the initial configuration steps.

Getting Started

- Administration
- Accounts
- Repositories
- Workers
- Server settings
- Settings
- Licensing
- Support Information

Add Policy

Policy Name

Account

Regions

Specify Resources

Exclude Resources

Snapshot Settings

Backup Settings

Cost Estimation

Settings

Summary

Specify backup settings

Enable backups

Backup Settings

Backup Repository: [Select](#)

Retention duration: 21 Days

Schedule

Create backups automatically

Daily at this time: 10:00 PM Selected Days 7 Days...

Monthly at this time: 12:00 AM First Monday 30 Months...

Periodically every: 1 Hours Schedule...

Previous Next Cancel

This section will present an estimated cost for the resources:

Welcome to Veeam Backup for AWS
This welcome page will guide you through the initial configuration steps.

Add Policy

Policy Name
Account
Regions
Specify Resources
Exclude Resources
Snapshot Settings
Backup Settings
Cost Estimation
Settings
Summary

Cost estimations

General Settings

Estimated daily churn: 3 percent
% of disk usage: 70 percent

Costs

Export...

Instance	Snapshot	Backup	Traffic	Transaction	Total
Total	1.11	2.28	0.64	0.23	4.25
Linux	0.44	0.91	0.26	0.09	1.70
Windows	0.66	1.37	0.39	0.14	2.55

For more information on our cost calculation, please visit this KB

Previous Next Cancel

Additionally, configure the retry policy for failed backups and set up a notification channel for alerts.

Welcome to Veeam Backup for AWS
This welcome page will guide you through the initial configuration steps.

Add Policy

Policy Name
Account
Regions
Specify Resources
Exclude Resources
Snapshot Settings
Backup Settings
Cost Estimation
Settings
Summary

Settings

Schedule

Automatic retry
Retry failed policy: 3 times

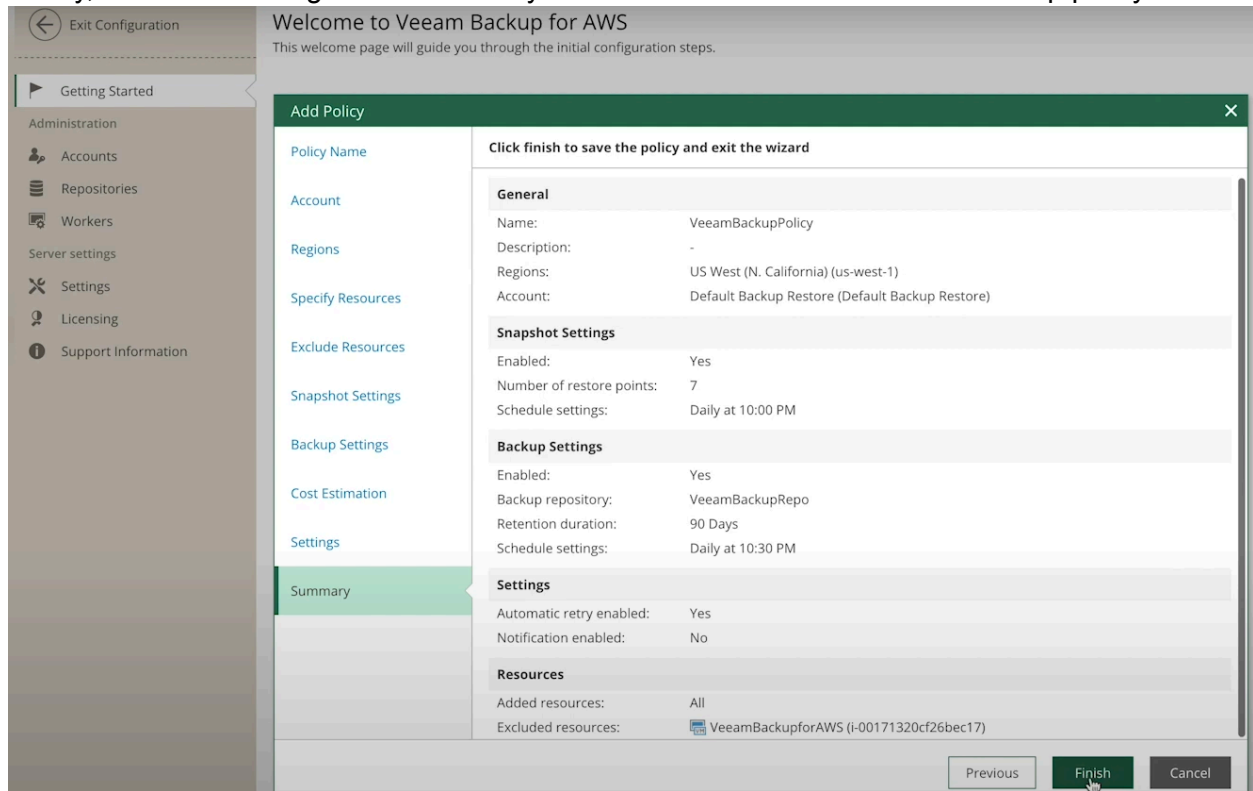
Notifications

Enabled
Email address: [input field]

Notify on success
 Notify on warning
 Notify on failure
 Suppress notifications until the last retry

Previous Next Cancel

Finally, review the configuration summary and select "Finish" to create the backup policy.



Upon successful creation, the policy will be available for review in the overview section.

