



EC2 Backup



TechData-Infinity-Devops with MultiCloud



4. EC2 Backup

let alone protect it from unexpected data loss as a result of hardware failure, software corruption, accidental deletion, malicious attack, or an unpredictable disaster. More issues may arise still when it comes to managing AWS EC2 environments and protecting data stored in the cloud.

In short, AWS EC2 backup instances, you should choose one of the following options:

Take an EBS snapshot;

Create a new AMI;

Design an AWS EC2 Backup plan;

Automate AWS EC2 backup with a third party solution

AWS Backup is a rather new addition to the rich set of AWS services and tools, and is definitely worth your attention. AWS Backup is a valuable tool which can help you automatically back up and protect your data and applications in the AWS cloud as well as on-premises IT environments.

How to Backup AWS EC2 Instances

AWS is a high-performance, constantly evolving cloud computing platform that allows you to store data and applications in the cloud environment. AWS can provide you with the tools you need to create EC2 instances which act as virtual servers with varying CPU, memory, storage, and networking capacity.

Currently, there are three ways to back up AWS EC2 instances: taking EBS snapshots, creating AMIs, or designing an AWS Backup plan. Let's take a closer look at each of these approaches and see how they differ.

Taking EBS Snapshots

If you want to back up an AWS EC2 instance, you should create snapshots of EBS volumes, which are stored with the help of Amazon Simple Storage Service (S3). Snapshots can capture all data within EBS volumes and create their exact copies. Moreover, these EBS snapshots can then be copied and transferred to another AWS region to ensure safe and reliable storage of critical data. Thus, in case of a disaster or accidental data loss, you can be sure that you have a backup copy securely stored in a remote location which you can use for restoring critical data.

Prior to running AWS EC2 backup, it is recommended that you stop the instance or at least detach an EBS volume which is about to be backed up. This way, you can prevent failure or errors from occurring and affecting the newly created snapshots.

Please note that, for security purposes, some sensitive information has been removed.


To back up AWS EC2 instance, you need to take the following steps:

1. Sign in to your AWS account to open the AWS console.
2. Select Services in the top bar and click EC2 to launch the EC2 Management Console

TechData-Infinity-Devops with MultiCloud



aws Services ^ Resource Groups v









History 

Console Home

EC2

AWS Backup

Find a service by name or feature (for example, EC2, S3 or VM, storage).

 Compute	 Robotics	 Analytics
EC2 	AWS RoboMaker	Athena
Lightsail 		EMR
ECR		CloudSearch
ECS	 Blockchain	Elasticsearch Servi
EKS	Amazon Managed Blockchain	Kinesis
Lambda		QuickSight 
Batch	 Satellite	Data Pipeline
Elastic Beanstalk	Ground Station	AWS Glue
Serverless Application Repository		MSK

1. Select Running Instances and choose the instance you would like to back up.

Resources

You are using the following Amazon EC2 resources in the EU West (Ireland) region:

3 Running Instances 	2 Elastic IPs
0 Dedicated Hosts	25 Snapshots
32 Volumes	0 Load Balancers
330 Key Pairs	314 Security Groups
0 Placement Groups	

1. In the bottom pane, you can view the central technical information about the instance. In the Description tab, find the Root device section and select the /dev/sda1 link.

TechData-Infinity-Devops with MultiCloud



Launch Instance ▾ Connect Actions ▾

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name
i-092cacbf2...	i-092cacbf2...	t2.micro	eu-west-1a	stopped	✓	None	-	-	-	rik_ubuntu14...
Amazon EC2...	i-092cacbf2...	t2.medium	eu-west-1b	stopped	✓	None	-	-	-	Amazon EC2...

Instance: **i-092cacbf2...** (Amazon EC2 Transporter PMM) Private IP: -

Description Status Checks Monitoring Tags

Instance ID: i-092cacbf2...

Instance state: stopped

Instance type: t2.medium

Elastic IPs: -

Availability zone: eu-west-1b

Security groups: Amazon EC2 Transporter_a5d78583-6618-4882-921b-446036445e26. view inbound rules, view outbound rules

Scheduled events: -

AMI ID: ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20190204.3 (ami-0bc11fa49cd2ead7)

Platform: -

IAM role: -

Key pair name: Amazon EC2 Transporter_a5d78583-6618-4882-921b-446036445e26

ClassicLink: -

Owner: 9157525117

Launch time: February 13, 2019 at 12:49:34 PM UTC+2 (1463 hours)

Termination protection: False

Lifecycle: normal

Public DNS (IPv4): -

IPv4 Public IP: -

IPv6 IPs: -

Private DNS: ip-10-0-35-147.eu-west-1.compute.internal

Private IPs: -

Secondary private IPs: -

VPC ID: -

Subnet ID: -

Network interfaces: -

Source/dest. check: -

T2/T3 Unlimited: -

EBS-optimized: -

Root device type: -

Root device: /dev/sda1

Block devices: /dev/sda1, /dev/xvda

Block Device /dev/sda1

EBS ID: vol-030712c73aa3194d

Root device type: EBS

Attachment time: 2019-02-13T10:49:35.000Z

Block device status: attached

Delete on termination: True

In the pop-up window, find the volume's EBS ID name and click it.

1. The Volumes section should open. Click Actions and select Create Snapshot.

Create Volume Actions ▴

search : vol-

Modify Volume

Create Snapshot

Delete Volume

Attach Volume

Detach Volume

Force Detach Volume

Change Auto-Enable IO Setting

Add/Edit Tags

Name	Volume Type	IOPS	Snapshot	Created
gp2	gp2	100	snap-031b604...	February 13, 2019 ...

1. The Create Snapshot box should open, where you can add a description for the snapshot to make it distinct from other snapshots, as well as assign tags to easily monitor this snapshot. Click Create Snapshot.

TechData-Infinity-Devops with MultiCloud



Create Snapshot

Volume vol-030782c73aae3194d ⓘ

Description Snapshot 15/04/2019 ⓘ

Encrypted Not Encrypted ⓘ

Key (127 characters maximum) Value (255 characters maximum)

This resource currently has no tags
Choose the Add tag button or click to add a Name tag

Add Tag 50 remaining (Up to 50 tags maximum)

* Required

Cancel Create Snapshot

1. The snapshot creation should start and be completed in a minimal amount of time. The main factor here is the size of data in your Amazon EBS volume.

After the snapshot creation is complete, you can find your new snapshot by selecting the Snapshots section in the left pane. As you can see, we have successfully created a point-in-time copy of the EBS volume, which can later be used to restore your EC2 instance.

	Name	Snapshot ID	Size	Description	Status
<input type="checkbox"/>		snap-0017f4af710d...	8 GiB	Created by CreateImage(i-047f91a2a2fd1fda8) for a...	completed
<input type="checkbox"/>	Recovery poi...	snap-00dea7a5f2d2...	127 GiB	Created by NAKIVO Backup & Replication on Thu, ...	completed
<input type="checkbox"/>	Recovery poi...	snap-016e9d852dd...	10 GiB	Created by NAKIVO Backup & Replication on Wed, ...	completed
<input type="checkbox"/>	Recovery poi...	snap-0197a4b333f3...	10 GiB	Created by NAKIVO Backup & Replication on Wed, ...	completed
<input type="checkbox"/>	Recovery poi...	snap-01cc391ff968...	8 GiB	Created by NAKIVO Backup & Replication on Wed, ...	completed
<input type="checkbox"/>		snap-02563ddd612...	20 GiB	Created by CreateImage(i-01f04e6b4e81213de) for ...	completed
<input type="checkbox"/>	Recovery poi...	snap-026758deefd9...	8 GiB	Created by NAKIVO Backup & Replication on Fri, O...	completed
<input type="checkbox"/>	Recovery poi...	snap-0272b4ccab7...	8 GiB	Created by NAKIVO Backup & Replication on Mon, ...	completed

For this purpose, you need to select the snapshot of the backed up volume, press the Actions button above, and click Create Volume. Following the prompts, configure the volume details (volume type, size, IOPS, availability zone, tags). Then, click Create Volume for the new volume to be created, which can later be added to the AWS EC2 instance of your choice.

Creating a new AMI

The next approach to performing AWS EC2 backups is creating an Amazon Machine Image (AMI) of your AWS EC2 instances. An AMI contains all the information required for creating an EC2 instance in the AWS environment, including configuration settings, the root volume template, launch permissions, and block device mapping. Basically, the AMI can act as a template for launching a new AWS EC2 instance and replacing the

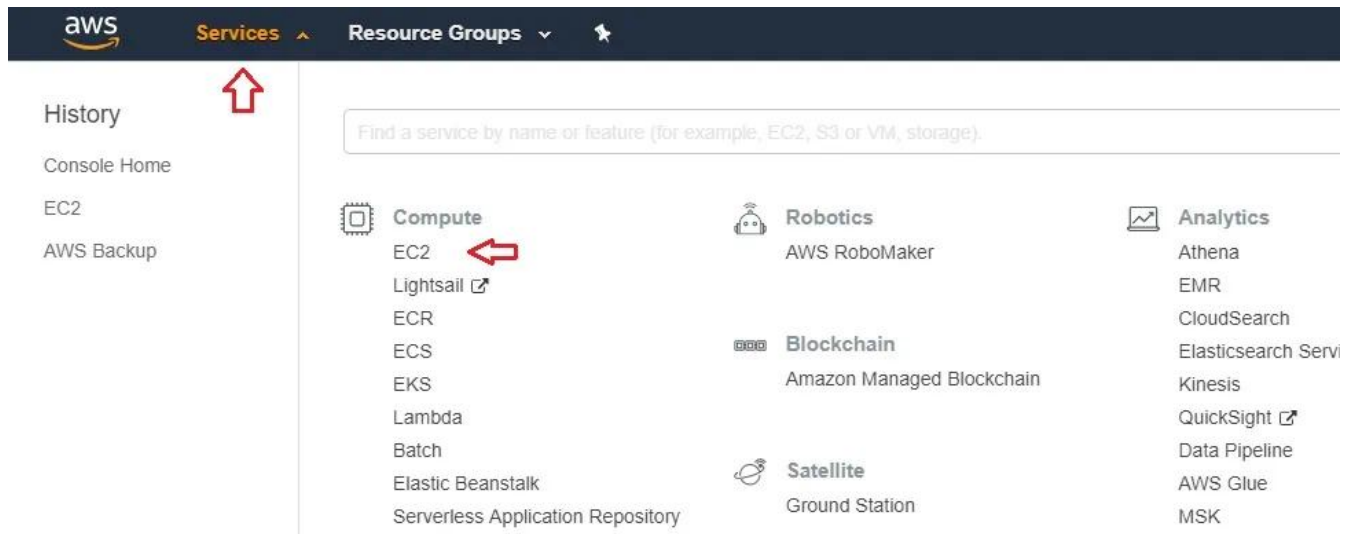
TechData-Infinity-Devops with MultiCloud



corrupted one. Note that, prior to creating the new AMI, it is recommended that you stop the AWS EC2 instance which you want to back up.

To create a new AMI and ensure AWS EC2 backup, you should do the following:

1. Sign in to your AWS account to open the AWS console.
2. Select Services in the top bar and click EC2 to launch the EC2 Management Console.



1. Select Running Instances and choose the instance you want to back up.

Resources

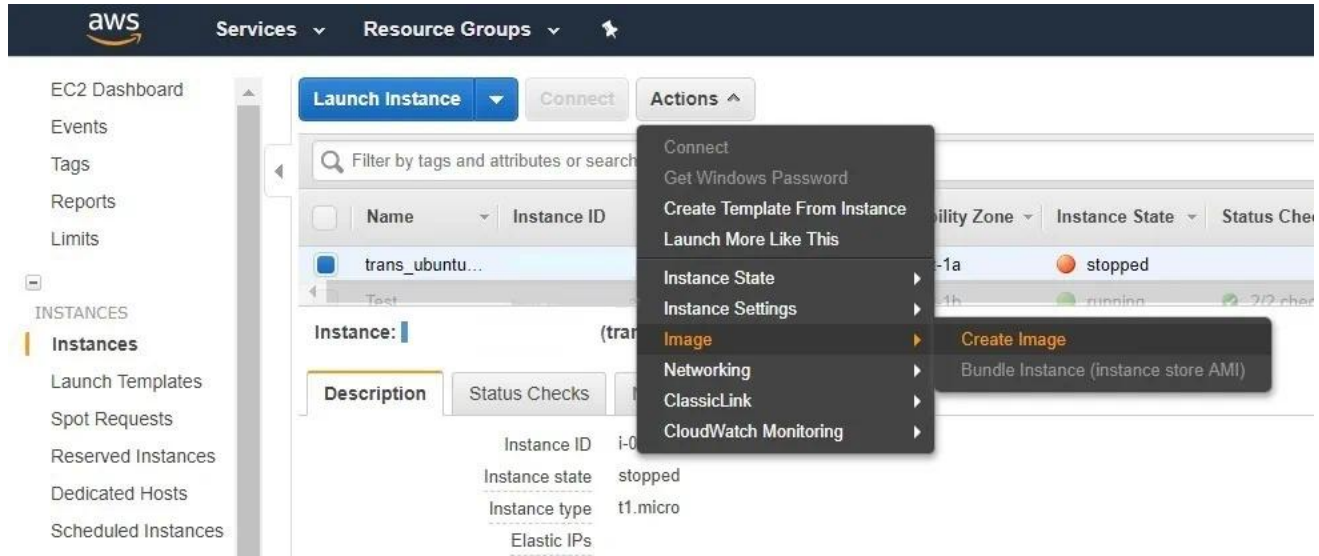
You are using the following Amazon EC2 resources in the EU West (Ireland) region:

3 Running Instances	2 Elastic IPs
0 Dedicated Hosts	25 Snapshots
32 Volumes	0 Load Balancers
330 Key Pairs	314 Security Groups
0 Placement Groups	

TechData-Infinity-Devops with MultiCloud



1. Click Actions > Image > Create Image.



1. The Create Image menu should open. Here, you can specify the image name, add the image description, enable/disable reboot after the AMI creation, and configure instance volumes.

Do note that when you create an EBS image, an EBS snapshot should also be created for each of the above volumes. You can access these snapshots by going to the Snapshots section.

Create Image

Instance ID

Image name

Image description

No reboot

Instance Volumes

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-03dd3803ebdfc92	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Total size of EBS Volumes: 8 GiB

When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Cancel

Create Image

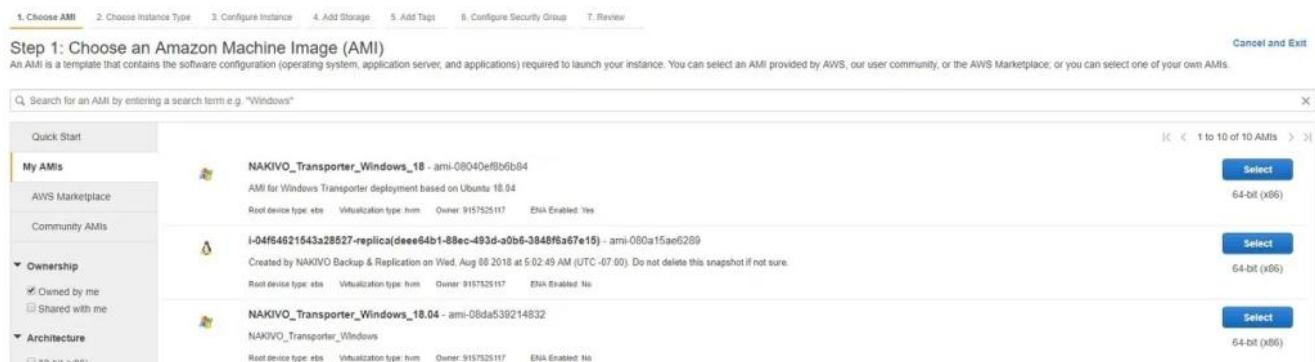
TechData-Infinity-Devops with MultiCloud



1. Click Create Image.
2. The image creation process should now start. Click the link to view the pending AMI.

1. It should take some time for the new AMI to be created. You can start using the AMI when its status switches from pending to available.

After the AMI has been successfully created, it can then be used to create a new AWS EC2 instance, which will be an exact copy of the original instance. For this purpose, simply go to the Instances section, click Launch Instance, select the AMI you have created in the My AMIs section, and follow the prompts to finish the instance creation.



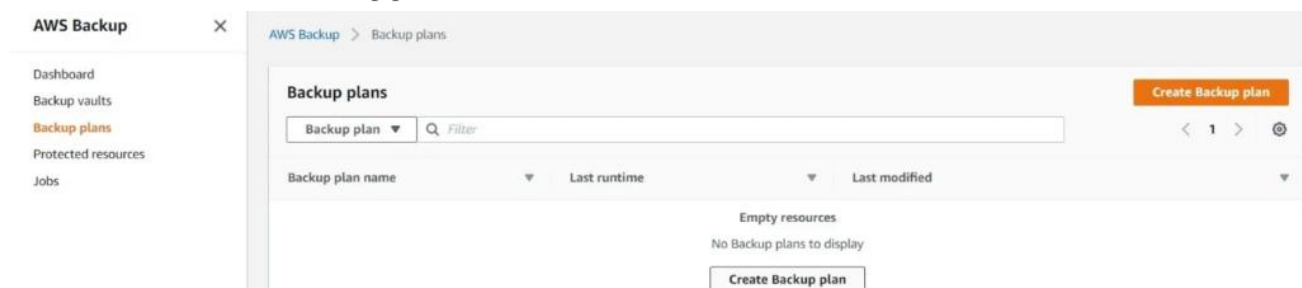
Creating AMIs is arguably a more effective backup strategy than taking EBS snapshots. This is due to the fact that AMIs often contain EBS snapshots as well as a software configuration which allows you to simply and easily launch the new AWS EC2 instance in just a few clicks, created free of charge (you only pay for snapshot storage).

Automating AWS EC2 backup

Previously, the only way to automate AWS EC2 backup was by running scripts or using API calls, which was a very challenging and resource-intensive process. The person responsible for backup automation had to be highly proficient in scripting in order to avoid any issues and inconsistencies. However, there was still a high risk that you would waste your time, effort, and money on a backup job configuration and still be left with failed or corrupted AWS EC2 backups.

To create an AWS backup plan, take the following steps:

1. Sign in to your AWS account to open the AWS Management Console.
2. Select Services in the top bar and then type AWS Backup in the search bar. Click Backup plans in the left pane.
3. Press the Create Backup plan button.



TechData-Infinity-Devops with MultiCloud



1. Here, you have three start options: Start from an existing plan, Build a new plan, and Define a plan using JSON. Click Info if you want to learn more about available options to help you make the right decision.

As we don't have any existing backup plans, let's build a new plan from scratch. Enter the new backup plan name and proceed further.

AWS Backup > Backup plans > Create Backup plan

Create Backup plan

Start options

Choose how you want to begin. [Info](#)

☐ Start from an existing plan
Create a new Backup plan based on an existing Backup plan, including plans created by AWS.

☒ Build a new plan
Enter configuration details to create a new Backup plan.

☐ Define a plan using JSON

Backup plan name

➡ AWSBackup-NAKIVO

Backup plan name is case sensitive. Must contain from 1 to 63 alphanumeric characters or hyphens.

1. The next step is Backup rule configuration. Here, you should specify the backup rule name.
1. After that, you can set up a backup schedule. You should determine the backup frequency (Every 12 hours, Daily, Weekly, Monthly, Custom cron expression); backup window (Use backup window defaults or Customize backup window); backup lifecycle (Transition to cold storage and Expiration of the backup).

TechData-Infinity-Devops with MultiCloud



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.

General

Rule name

NewBackupRule-NAKIVO

Backup rule name is case sensitive. Must contain from 1 to 63 alphanumeric characters or hyphens.

Schedule

Add a Backup rule by defining a backup schedule, backup window, and lifecycle rules.

Frequency

Daily

Backup window

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

☐ Customize backup window

Lifecycle [Info](#)

Schedule transition to cold storage and expiration of the backup.

Transition to cold storage

Never

Expire

Never

1. At this step, you should select the backup vault for storing your recovery points (the ones created by this Backup rule). You can click Create new Backup vault if you want to have a new customizable vault. You can also use the existing Backup vault if you have one. Alternatively, you can choose the default AWS Backup vault.

Backup vault [Info](#)

Specify the Backup vault that recovery points created by this Backup rule are organized in.

Default

Create new Backup vault

TechData-Infinity-Devops with MultiCloud



1. Next, you must add tags to recovery points and your backup plan in order to organize them and easily monitor their current status.

▼ Tags added to recovery points
Tags specified here are added to recovery points when they are created.

Key	Value - optional	
<input type="text" value="RecoveryPoint1"/>	<input type="text" value="PrimaryBackup"/>	<input type="button" value="Remove tag"/>
<input type="button" value="Add tag"/>		

Tags added to Backup plan
Tags specified here help organize and track your Backup plan

Key	Value - optional	
<input type="text" value="BackupPlan1"/>	<input type="text" value="NAKIVO-Backup"/>	<input type="button" value="Remove tag"/>
<input type="button" value="Add tag"/>		

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.

▼ Tags added to recovery points
Tags specified here are added to recovery points when they are created.

Key	Value - optional	
<input type="text" value="RecoveryPoint1"/>	<input type="text" value="PrimaryBackup"/>	<input type="button" value="Remove tag"/>
<input type="button" value="Add tag"/>		

Tags added to Backup plan
Tags specified here help organize and track your Backup plan

Key	Value - optional	
<input type="text" value="BackupPlan1"/>	<input type="text" value="NAKIVO-Backup"/>	<input type="button" value="Remove tag"/>
<input type="button" value="Add tag"/>		

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.

After that, you can click Create plan to proceed to the next stage, the backup rule creation.

1. Your backup plan has been successfully created. However, before you can run this plan and deploy it in your environment, you should also assign resources which need to be backed up. Click the Assign resources button, which can be found in the top bar.

TechData-Infinity-Devops with MultiCloud



Success

Backup plan "AWSBackup-NAKIVO" creation successful. You can now add additional schedule rules and assign resources to the Backup plan by selecting the Backup plan.

Assign resources

AWS Backup > Backup plans > AWSBackup-NAKIVO

Delete

View JSON

AWSBackup-NAKIVO

Summary

Backup plan name	Version ID	Last modified	Last runtime
AWSBackup-NAKIVO	NmJhOTA1MmMTZWRjZC00NDM2LWEONZEtNTFjZW	Apr 15, 2019 @ 11:36:53 AM UTC+03:00	-
Backup plan ID	NINDFmOGNi		
ac9be8cc-d8d6-4a9a-9d66-fd924d17d54f			

Backup rules

Backup rules specify the backup schedule, backup window, and lifecycle rules.

Edit

Delete

Add Backup rule

Name	Backup vault
<input type="radio"/> NewBackupRule-NAKIVO	Default

Resource assignments

Resource assignments specify which resources will be backed up by this Backup plan.

Delete

Assign resources

Name	IAM role ARN
Empty resources	
You don't have any resource assignments.	
<div>Assign resources</div>	

1. In the next menu, you can specify the resource assignment name and define the IAM (Identity and Access Management) role.

By selecting the IAM role, you specify what a user can or cannot do in AWS and determine which users are granted permission to manage selected AWS resources and services.

Additionally, you can assign resources to this Backup plan using tags or resource IDs, meaning that any AWS resources matching these key-pair values should be automatically backed up by this Backup plan.

TechData-Infinity-Devops with MultiCloud



AWS Backup > Backup plans > AWSBackup-NAKIVO > Assign resources

Assign resources

General

Resource assignment name

DailyBackups

Resource assignment name is case sensitive. Must contain from 1 to 63 alphanumeric characters or hyphens.

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

Assign resources

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

Assign by	Key	Value	
Tags	BackupPlan1	NAKIVO-Backup	Remove
Tags	Daily	Backups	Remove
Resource ID	EBS	Q vol-9bc7342b	Remove

Add assignment

Cancel Assign resources

1. Click Assign resources to complete the configuration process. After that, the backup job should run automatically. You can go to the AWS Backup dashboard to see the current status of your backup jobs and verify that they are working as planned.

TechData-Infinity-Devops with MultiCloud



AWS Backup



Dashboard

Backup vaults

Backup plans

Protected resources

Jobs

AWS Backup > Dashboard

Overview

Manage Backup plans

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

Manage Backup plans

Create an on-demand backup

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

Create an on-demand backup

Restore a backup

Create a new resource from a backup.

Restore backup

Backup jobs in the last 24 hours (0)

🕒 1 In progress ➡
✅ 0 Completed
❌ 0 Failed

Backup jobs details

Restore jobs in the last 24 hours (0)

🕒 0 In progress
✅ 0 Completed
❌ 0 Failed

Restore jobs details

As you can see, our backup job is already in progress. In this menu, you can also Manage Backup plans, Create an on-demand backup, or Restore backup. Choose the required option and set up another data protection job in AWS environment following the prompts.