

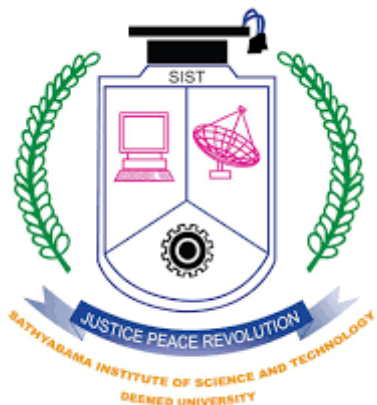
INTER DISCIPLINARY PROJECT REPORT
at
Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for the award
of Bachelor of Technology Degree in Information Technology

By

KOKONDA NIKHIL.

REG. NO. 39120075



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU



SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE
UNIVERSITY)



Accredited with Grade “A” by NAAC

(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI

CHENNAI– 600119

www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of KOKONDA NIKHIL(Reg. No: 39120075) who underwent the training in “Cloud computing” under my supervision from February 2022 to April 2022.

Internal Guide

Dr.P.revathy

Head of the Department

Dr. SUBHASHINI, M.E.,Ph.D,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I, KOKONDA NIKHIL hereby declare that the project report entitled **Instance recovery and backup in AWS** done by me under the guidance of **DR.P.revathy** is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Information Technology.

DATE:

SIGNATURE OF THE CANDIDATE

PLACE:

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. SUBHASHINI, M.E.,Ph.D., Head of the Department of Information Department** providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.P.revathy**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



Abstract:

The paper is intended for enterprise solution architects, backup architects, and IT administrators who are responsible for protecting data in their corporate IT environments. It discusses production workloads and architectures that can be implemented using AWS to augment or replace a backup and recovery solution. These approaches offer lower costs, higher scalability, and more durability to meet Recovery Time Objective (RTO), Recovery Point Objective (RPO), and compliance requirements.

TABLE OF CONTENTS

Chapter No.	Name	Page no.
	Abstract	6
	List of snapshots	8
1	Introduction	
	1.1cloud computing	9
	1.2 Backup and Instance recovery	10
2	Aim and Scope of present Investigation	
	2.1 Aim	14
	2.2 Scope of Present investigation	14
	2.3 Software and Hardware	14
3	Methods and Algorithm	
	3.1 AWS Backup	15
	3.2 Features of backups	17
	3.3 understanding of instance recovery	20
	3.4 Creation of Backup	21
	3.5 Deletion of backup	23
	3.6 Understanding of AWI recovery	24
		21
		24
		25
4	Results and Discussion	
	4.1 Results and discussion	28
5	Summary and Conclusions	
	5.1 Conclusions	29

References	30
Appendixes	31

List of snapshots

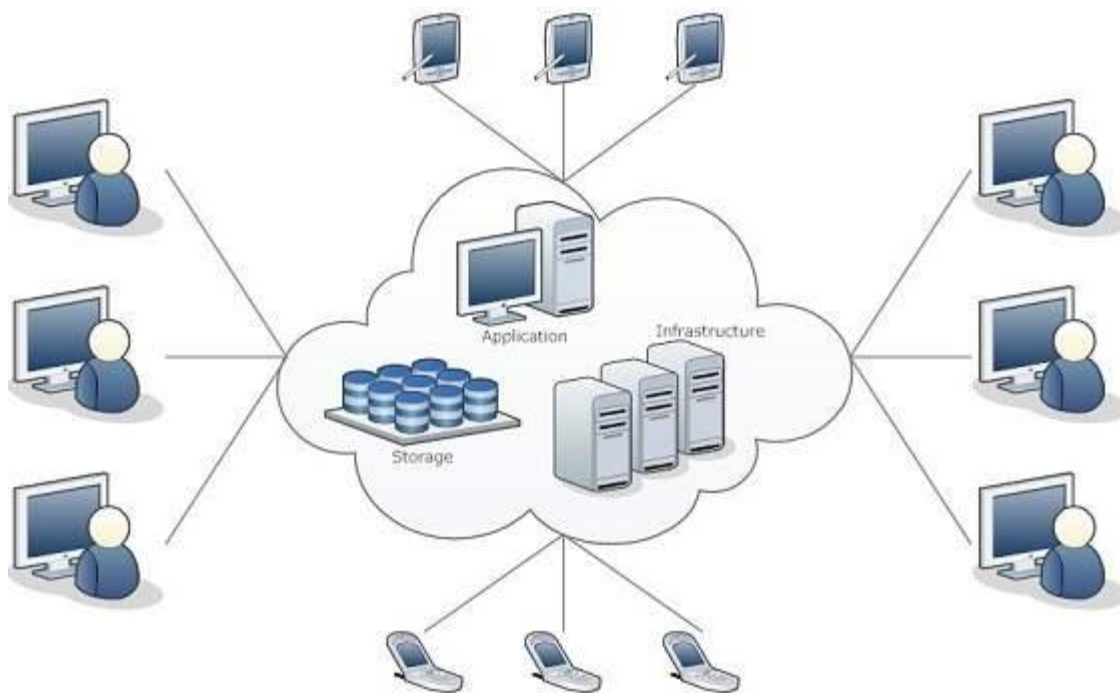
Figure number	Name	Page no
1	Types of clouds	10
2	Instance recovery	22
3	Creation of backup	30
4	AWI Session Connection type – Amazon WorkSpaces	24
5	AWI Session connection type – Auto Detect	25

Chapter No :1

1.Introduction

1.1 Cloud Computing

Cloud Computing refers to **manipulating, configuring, and accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application.



Cloud computing offers **platform independency**, as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative**

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.

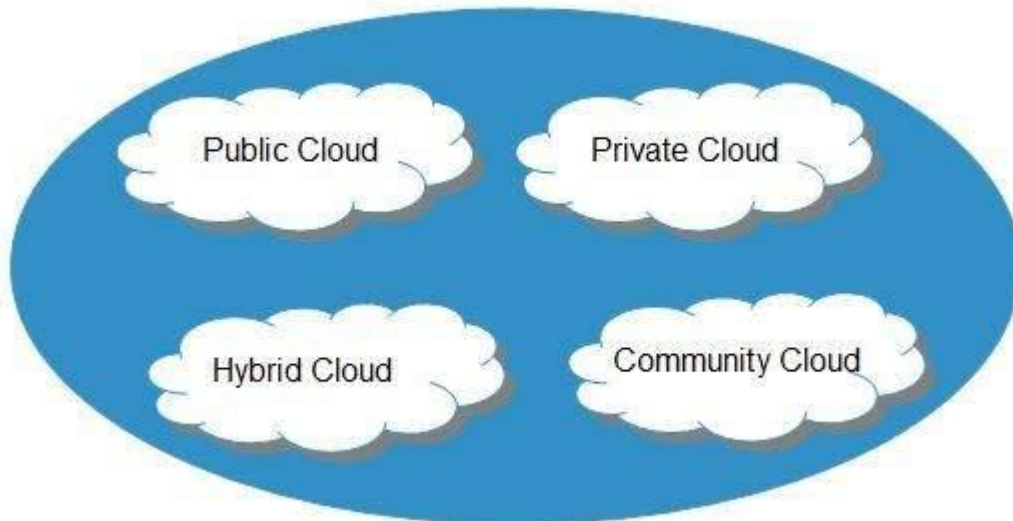


Fig 1 : Types of clouds

Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

1.2 Backup and instance recovery:

When you develop a comprehensive strategy for backing up and restoring data, you must first identify the failure or disaster situations that can occur and their potential business impact. In some industries, you must consider regulatory requirements for data security, privacy, and records retention.

You should implement backup processes that will offer the appropriate level of granularity to meet the RTO and RPO of the business, including:

- ☐ File-level recovery
- ☐ Volume-level recovery

- Application-level recovery (for example, databases)
- Image-level recovery

The following sections describe backup, recovery, and archive approaches based on the organization of your infrastructure. IT infrastructure can broadly be categorized as cloud native, on-premises, and hybrid..

Cloud-Native Infrastructure

This scenario describes a workload environment that exists entirely on AWS. As the following figure shows, it includes web servers, application servers, monitoring servers, databases, and Active Directory.

If you are running all of your services from AWS, you can leverage many built-in features to meet your data protection and recovery needs.

Cloud backup is a service in which the data and applications on a business's servers are backed up and stored on a remote server. Businesses opt to back up to the cloud to keep files and data readily available in the event of a system failure, outage or natural disaster. Cloud backup for business operates by copying and storing your server's files to a server in a different physical location. A business can back up some or all server files, depending on its preference.

Customers typically back up and restore their data and apps using a web browser or a service provider's control panel. Cloud server backup is a necessity for many organizations today because they store most or all of their business-critical data and applications on cloud servers.

File backup and disaster recovery is the second leading use of cloud computing among medium and large enterprises, according to a recent Clutch survey. Sixty-two percent of the enterprise respondents use the cloud for this purpose, with only file storage (70 percent) being more popular.

When developing a comprehensive strategy for backing up and restoring data, you must first identify

possible failure or disaster situations and their potential business impact. In some industries, you must

consider regulatory requirements for data security, privacy, and records retention.

Backup and recovery processes should include the appropriate level of granularity to meet recovery

time objective (RTO) and recovery point objective (RPO) for the workload and its supporting business

processes, including the following:

- File-level recovery (for example, configuration files for an application)
- Application data-level recovery (for example, a specific database within MySQL)
- Application-level recovery (for example, a specific web server application version)
- Amazon EC2 volume-level recovery (for example, an EBS volume)

- EC2 instance-level recovery. (for example, an EC2 instance)
- Managed service recovery (for example, a DynamoDB table)

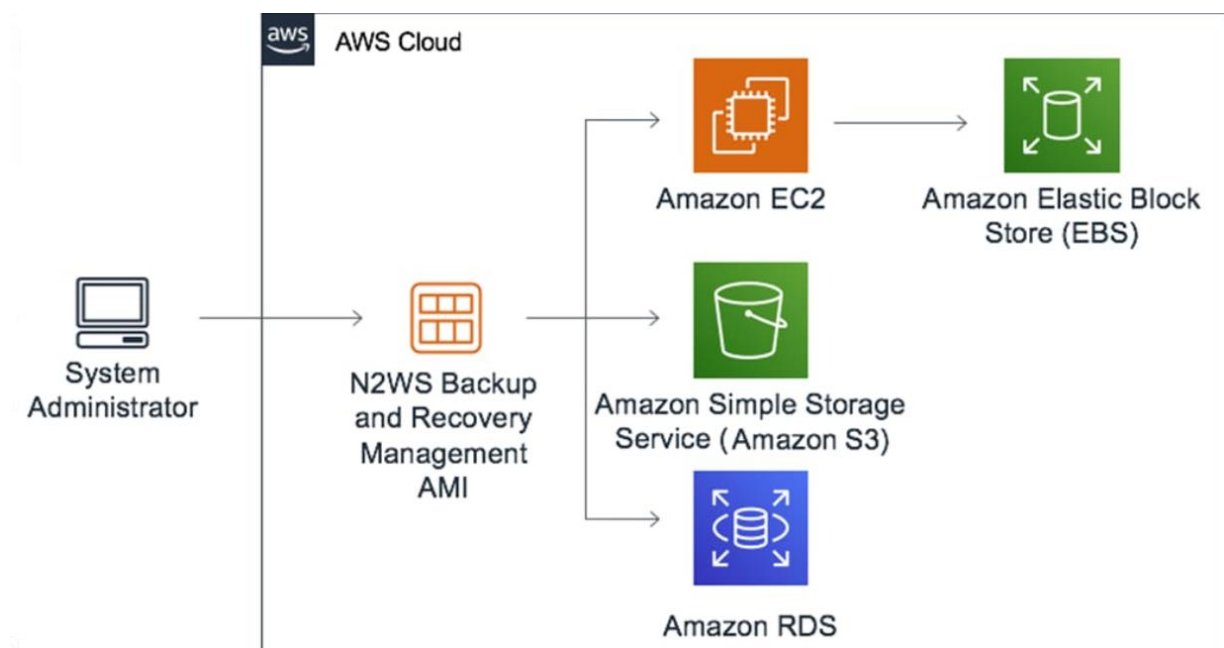
Be sure to consider all the recovery requirements for your solution and the data dependencies between

various components in your architecture. To facilitate a successful restore process, coordinate the backup

and recovery between various components in your architecture.

The following topics describe backup and recovery approaches based on the organization of your

infrastructure. IT infrastructure can broadly be categorized as on-premises, hybrid, or cloud native



Recovery your instance:

You can use the default configuration of the instance or create a

Amazon CloudWatch alarm to automatically recover an instance. If an instance becomes impaired because of an underlying hardware failure or a problem that requires AWS involvement to repair, the instance is automatically recovered. Terminated instances cannot be recovered.

A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance has a public IPv4 address, the instance retains the public IPv4 address after recovery. If the impaired instance is in a placement group, the recovered instance runs in the placement group. During instance recovery, the instance is migrated as part of an instance reboot, and any data that is in-memory is lost.

Examples of problems that require an instance recovery include:

Loss of network connectivity

Loss of system power

Software issues on the physical host

Hardware issues on the physical host that impact network reachability

Chapter No : 2

2.Aim and scope of the present investigation

2.1. Aim:

To create backup, instance recovery and delete backup in AWS

2.2 Scope of present investigation:

AWS Backup enables you to centralize and automate data protection across AWS services and hybrid workloads. AWS Backup offers a cost-effective, fully managed, policy-based service that further simplifies data protection at scale. AWS Backup also helps you support your regulatory compliance or business policies for data protection. Together with AWS Organizations, AWS Backup enables you to centrally deploy data protection policies to configure, manage, and govern your backup activity across your organization's AWS accounts and resources, including Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Block Store (Amazon EBS) volumes, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Relational Database Service (Amazon RDS) databases (including Amazon Aurora clusters), Amazon DynamoDB tables, Amazon Neptune databases, Amazon DocumentDB (with MongoDB compatibility) databases, Amazon Elastic File System (Amazon EFS) file systems, Amazon FSx for Lustre file systems, Amazon FSx for Windows File Server file systems, and AWS Storage Gateway volumes, and VMware workloads on premises and in VMware Cloud on AWS.

2.3 Software and hardware requirements:

****Software Requirements**

- 1.SolarWinds Backup - MSPs
- 2.pCloud – Sharing large files
- 3.ZoolzHome -users, photographers, etc
- 4.IBackup – privacy and security features for small businesses
- 5.Acronis – Advanced Security

****Hardware Requirements**

- 1.GPU
- 2.Any Operating System

Chapter No : 3

3.Instance recovery and backup In AWS

3.1 AWS Backup:

AWS Backup is a fully-managed service that makes it easy to centralize and automate data protection across AWS services, in the cloud, and on premises. Using this service, you can configure backup policies and monitor activity for your AWS resources in one place. It allows you to automate and consolidate backup tasks that were previously performed service-by-service, and removes the need to create custom scripts and manual processes. With a few clicks in the AWS Backup console, you can automate your data protection policies and schedules.

AWS Backup does not govern backups you take in your AWS environment outside of AWS Backup. Therefore, if you want a centralized, end-to-end solution for business and regulatory compliance requirements, start using AWS Backup today.

Feature availability by resource

AWS Backup supports	Cross-Region backup	Cross-account backup	AWS Backup Audit Manager	Incremental backup	Continuous backup and point-in-time restore (PITR)	Full Back man
EC2	✓	✓	✓	✓		
S3			✓†	✓	✓	✓
EBS	✓	✓	✓	✓		
RDS	✓*	✓*	✓	✓	✓	
Aurora	✓*	✓*	✓			
EFS	✓	✓	✓	✓		✓
FSx for Lustre	✓	✓	✓	✓		

AWS Backup support for Amazon FSx is available in all Regions except Asia Pacific (Jakarta) Region and Asia Pacific (Osaka) Region.

AWS Backup support for Storage Gateway is available in all Regions except Asia Pacific (Osaka) Region

AWS Backup support for Amazon S3 is available in all Regions except South America (São Paulo) Region, Asia Pacific (Jakarta) Region, China (Beijing) Region, China (Ningxia) Region, AWS GovCloud (US-West), and AWS GovCloud (US-East) Regions.

AWS Backup support for VMware is not available in China (Beijing) Region or China (Ningxia) Region

AWS Backup provides a dashboard that makes it simple to audit backup and restore activity across AWS services. With just a few clicks on the AWS Backup console, you can view the status of recent backup jobs. You can also restore jobs across AWS services to ensure that your AWS resources are properly protected.

AWS Backup integrates with Amazon CloudWatch and Amazon EventBridge. CloudWatch allows you to track metrics and create alarms. EventBridge allows you to view and monitor AWS Backup events. For more information, see [Monitoring AWS Backup events using EventBridge](#) and [Monitoring AWS Backup metrics with CloudWatch](#).

AWS Backup integrates with AWS CloudTrail. CloudTrail gives you a consolidated view of backup activity logs that make it quick and easy to audit how your resources are backed up. AWS Backup also integrates with Amazon Simple Notification Service (Amazon SNS), providing you with backup activity notifications, such as when a backup succeeds or a restore has been initiated. For more information, see [Logging AWS Backup API calls with CloudTrail](#) and [Using Amazon SNS to track AWS Backup events](#).

Secure your data in backup vaults

The content of each AWS Backup backup is immutable, meaning that no one can alter that content. AWS Backup further secures your backups in backup vaults, which separates them safely from their source instances. For example, your vault will retain your Amazon EC2 and Amazon EBS backups according to the lifecycle policy you choose, even if you delete the source Amazon EC2 instance and Amazon EBS volumes.

Backup vaults offer encryption and resource-based access policies that let you define who has access to your backups. You can define access policies for a backup vault that define who has access to the backups within that vault and what actions they can take. This provides a simple and secure way to control access to your backups across AWS services. To review AWS and customer managed policies for AWS Backup, see [Managed policies for AWS Backup](#).

3.2 Features of backups:

AWS Backup provides many features and capabilities, including:

Centralized backup management

AWS Backup provides a centralized backup console, a set of backup APIs, and the AWS Command Line Interface (AWS CLI) to manage backups across the AWS services that your applications use. With AWS Backup, you can centrally manage backup policies that meet your backup requirements. You can then apply them to your AWS resources across AWS services, enabling you to back up your application data in a consistent and compliant manner. The AWS Backup centralized backup console offers a consolidated view of your backups and backup activity logs, making it easier to audit your backups and ensure compliance.

Policy-based backup

With AWS Backup, you can create backup policies known as *backup plans*. Use these backup plans to define your backup requirements and then apply them to the AWS resources that you want to protect across the AWS services that you use. You can create separate backup plans that each meet specific business and regulatory compliance requirements. This helps ensure that each AWS resource is backed up according to your requirements. Backup plans make it easy to enforce your backup strategy across your organization and across your applications in a scalable manner.

For all the configuration options for backup plans, see [Backup plan options and configuration](#).

Tag-based backup policies

You can use AWS Backup to apply backup plans to your AWS resources in a wide variety of ways, including tagging them. Tagging makes it easier to implement your backup strategy across all your applications and to ensure that all your AWS resources are backed up and protected. AWS tags are a great way to organize and classify your AWS resources. Integration with AWS tags enables you to quickly apply a backup plan to a group of AWS resources, so that they are backed up in a consistent and compliant manner.

For all the ways you can assign your resources to backup plans, see [Assigning resources to a backup plan](#).

Lifecycle management policies

AWS Backup enables you to meet compliance requirements while minimizing backup storage costs by storing backups in a low-cost cold storage tier. You can configure lifecycle policies that automatically transition backups from warm storage to cold storage according to a schedule that you define.

For which resources support teiring to cold storage, see [Feature availability by resource](#). The cold storage expression is ignored for other backups.

Cross-Region backup

Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data. For more information, see [Creating backup copies across AWS Regions](#).

Cross-account management and cross-account backup

You can use AWS Backup to manage your backups across all AWS accounts inside your [AWS Organizations](#) structure. With cross-account management, you can automatically use backup policies to apply backup plans across the AWS accounts within your organization. This makes compliance and data protection efficient at scale and reduces operational overhead. It also helps eliminate manually duplicating backup plans across individual accounts. For more information, see [Managing AWS Backup resources across multiple AWS accounts](#).

You can also copy backups to multiple different AWS accounts inside your AWS Organizations management structure. This way, you can "fan in" backups to a single repository account, then "fan out" backups for greater resilience. [Creating backup copies across AWS accounts](#).

Before you can use the cross-account management and cross-account backup features, you must have an existing organization structure configured in AWS Organizations. An *organizational unit* (OU) is a group of accounts that can be managed as a single entity. AWS Organizations is a list of accounts that can be grouped into organizational units and managed as a single entity.

Auditing and reporting with AWS Backup Audit Manager

AWS Backup Audit Manager helps you simplify data governance and compliance management of your backups across AWS. AWS Backup Audit Manager provides built-in, customizable controls that you can align with your organizational requirements. You can also use these controls to automatically track your backup activities and resources.

AWS Backup Audit Manager can help you locate specific activities and resources that are not yet compliant with the controls that you defined. It also generates daily reports that you can use to demonstrate evidence of compliance with your controls over time.

To include your backup compliance alongside your overall compliance posture, you can automatically import AWS Backup Audit Manager findings into AWS Audit Manager.

Incremental backups

AWS Backup efficiently stores your periodic backups incrementally. The first backup of an AWS resource backs up a full copy of your data. For each successive incremental backup, only the changes to your AWS resources are backed up. Incremental backups enable you to benefit from the data protection of frequent backups while minimizing storage costs.

For a list of which resources support incremental backups, see [Feature availability by resource](#).

Full AWS Backup management

Some resource types support full AWS Backup management. The benefits of full AWS Backup management include:

- **Independent encryption.** AWS Backup automatically encrypts your backups with the KMS key of your AWS Backup vault, instead of using the same encryption key as your source resource. This increases your layers of defense. See [Encryption for backups in AWS Backup](#) for more information.
- **awsbackup Amazon Resource Names (ARNs).** Backup ARNs begin with `arn:aws:backup` instead of `arn:aws:source-resource`. This allows you to create access policies that apply specifically to backups and not the source resources. See [Access control](#) for more information.
- **Centralized backup billing and Cost Explorer cost allocation tags.** Charges for AWS Backup (including storage, data transfers, restores, and early deletion) appear under "Backup" in your Amazon Web Services bill, instead of appearing under each supported resource. You can also use Cost Explorer cost allocation tags to track and optimize your backup costs. See [Metering, costs, and billing](#) for more information.

To see which resource types are eligible for full AWS Backup management, see [Feature availability by resource](#).

Backup activity monitoring

AWS Backup provides a dashboard that makes it simple to audit backup and restore activity across AWS services. With just a few clicks on the AWS Backup console, you can view the status of recent backup jobs. You can also restore jobs across AWS services to ensure that your AWS resources are properly protected.

AWS Backup integrates with Amazon CloudWatch and Amazon EventBridge. CloudWatch allows you to track metrics and create alarms. EventBridge allows you to view and monitor AWS Backup events. For more information, see [Monitoring AWS Backup events using EventBridge](#) and [Monitoring AWS Backup metrics with CloudWatch](#).

AWS Backup integrates with AWS CloudTrail. CloudTrail gives you a consolidated view of backup activity logs that make it quick and easy to audit how your resources are backed up. AWS Backup also integrates

3.3 Instance recovery:

- You can use the default configuration of the instance or create an Amazon CloudWatch alarm to automatically recover an instance. If an instance becomes impaired because of an underlying hardware failure or a problem that requires AWS involvement to repair, the instance is automatically recovered. Terminated instances cannot be recovered.
- A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance has a public IPv4 address, the instance retains the public IPv4 address after recovery. If the impaired instance is in a placement group, the recovered instance runs in the placement group. During instance recovery, the instance is migrated as part of an instance reboot, and any data that is in-memory is lost

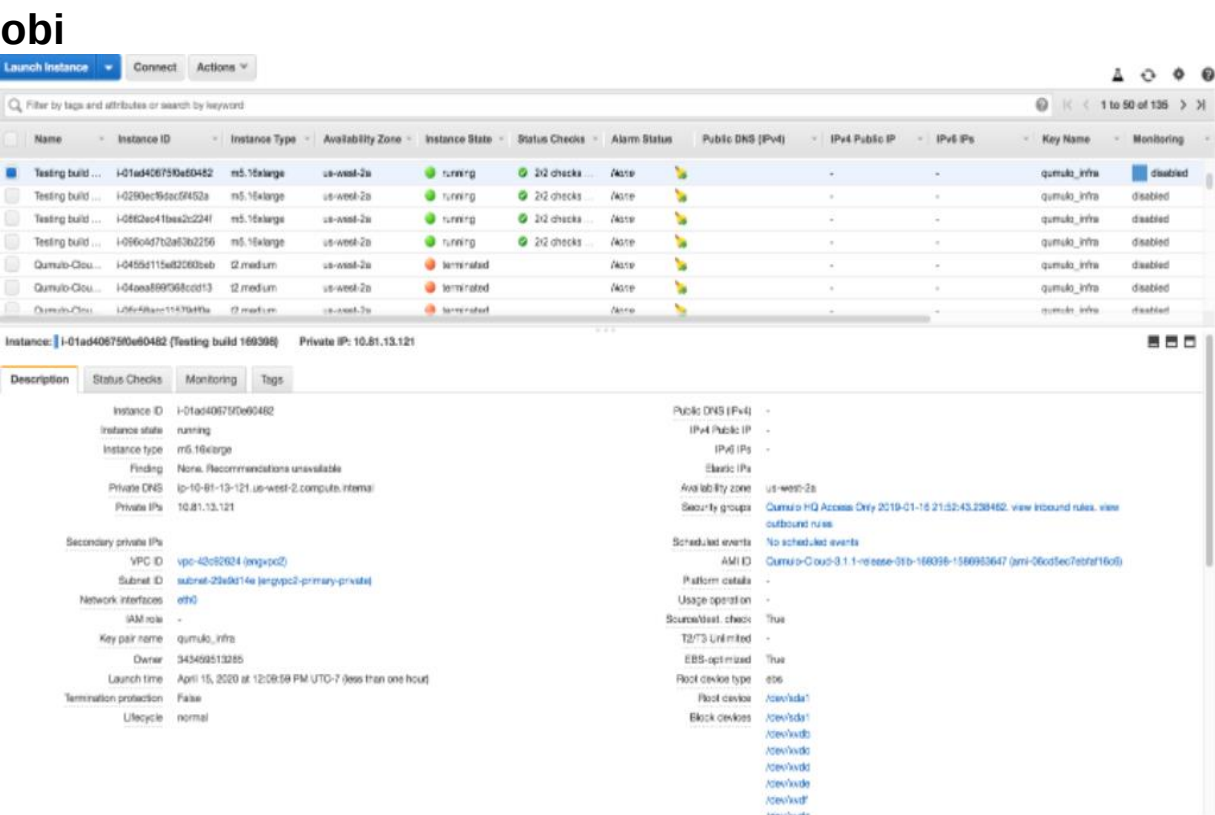


fig 2 instance recovery

3.4 Creation of backup:

An AMI includes the following:

- One or more snapshots. Instance-store-backed AMIs include a template for the root volume of the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it's launched. You can use AMIs to launch new instances with preconfigured software and data. You can create AMIs when you want to establish a baseline, which is a reusable configuration for launching more instances. When you create an AMI of an existing EC2 instance, a snapshot is taken for all the volumes that are attached to the instance. The snapshot includes the device mappings. You can't use snapshots to launch a new instance, but you can use them to replace volumes on an existing instance. If you experience data corruption or a volume failure, you can create a volume from a snapshot that you have taken and replace the old volume. You can also use snapshots to provision new volumes and attach them during a new instance launch

AWS Backup is a fully-managed service that makes it easy to centralize and automate data protection across AWS services, in the cloud, and on premises. Using this service, you can configure backup policies and monitor activity for your AWS resources in one place. It allows you to automate and consolidate backup tasks that were previously performed service-by-service, and removes the need to create custom scripts and manual processes. With a few clicks in the AWS Backup console, you can automate your data protection policies and schedules.

AWS Backup does not govern backups you take in your AWS environment outside of AWS Backup. Therefore, if you want a centralized, end-to-end solution for business and regulatory compliance requirements, start using AWS Backup today.

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

WhizBackup1

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

Fig 3 creation of backup

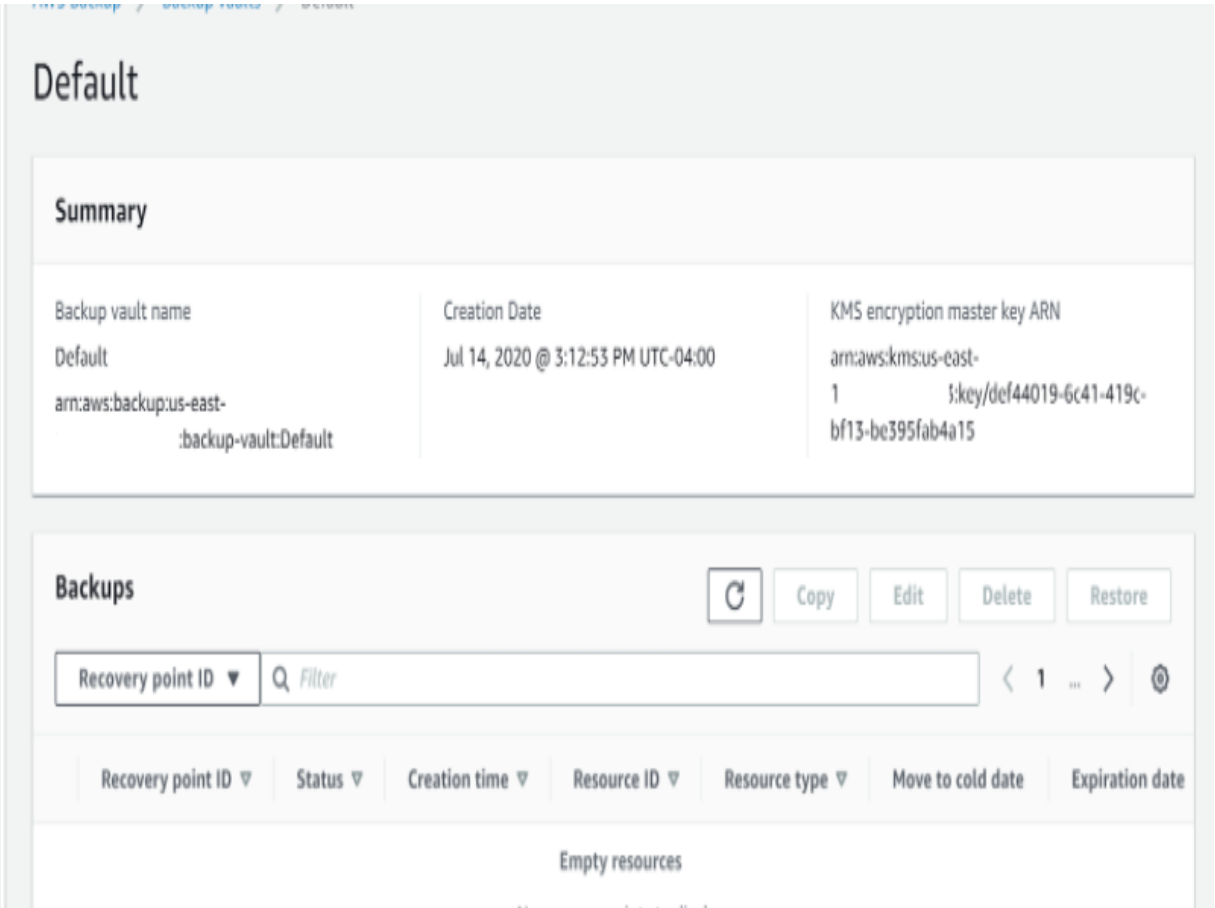
Many resources support incremental backup with AWS Backup. A full list is available in the incremental backup section of the [Feature availability by resource](#) table.

Although each backup after the first one is incremental (meaning it only captures changes from the previous backup), all backups made with AWS Backup retain the necessary reference data to allow a full restore. This is true even if the original (full) backup has reached the end of its lifecycle and been deleted.

For example, if your day 1 (full) backup was deleted due to a 3-day lifecycle policy, you would still be able to perform a full restore with the backups from days 2 and 3. AWS Backup maintains the necessary reference data from day 1 to do so.

3.5. Deletion of backup:

To guard against accidental or malicious mass deletion, you can delete a backup vault in AWS Backup only after you delete (or your backup plan lifecycles) all the recovery points in your backup vault. To delete all your recovery points manually



3.6. AWI RECOVERY

Select the **Amazon WorkSpaces** session connection type from the **Configuration > Session** page to configure the client to connect directly to your Amazon WorkSpaces desktop through multi-factor authentication. This connection type removes the need to deploy and manage the PCoIP Connection Manager for Amazon WorkSpaces in order to connect zero clients to Amazon WorkSpaces.

Security

The connection manager determines the security requirements. Amazon WorkSpaces session type uses an Amazon connection manager which requires multi-factor authentication when connecting to Amazon WorkSpaces.

Session

Configure the connection to a device

Session Connection Type: Amazon WorkSpaces

AWS Registration Code:

AWS Connection Name:

Hide Advanced Options

Desktop Name to Select:

Certificate Check Mode: Warn before connecting to untrusted servers

Certificate Check Mode Lockout: ☐ Prevent users from changing the Certificate Check Mode

Auto Connect: Disabled

Connection Server Cache Mode: Last servers used

Clear cache entries

Auto Launch If Only One Desktop: ☐

Enable Peer Loss Overlay: ☐

Enable Preparing Desktop Overlay: ☐

Enable Session Disconnect Hotkey: ☒ CTRL + ALT + F12

PCoIP Utility Bar Mode: Disabled

TLS Security Mode: Maximum Compatibility: TLS 1.1 or higher with RSA keys

Disconnect Message Filter: Show All

Enable DSCP: ☐

Enable Congestion Notification: ☒

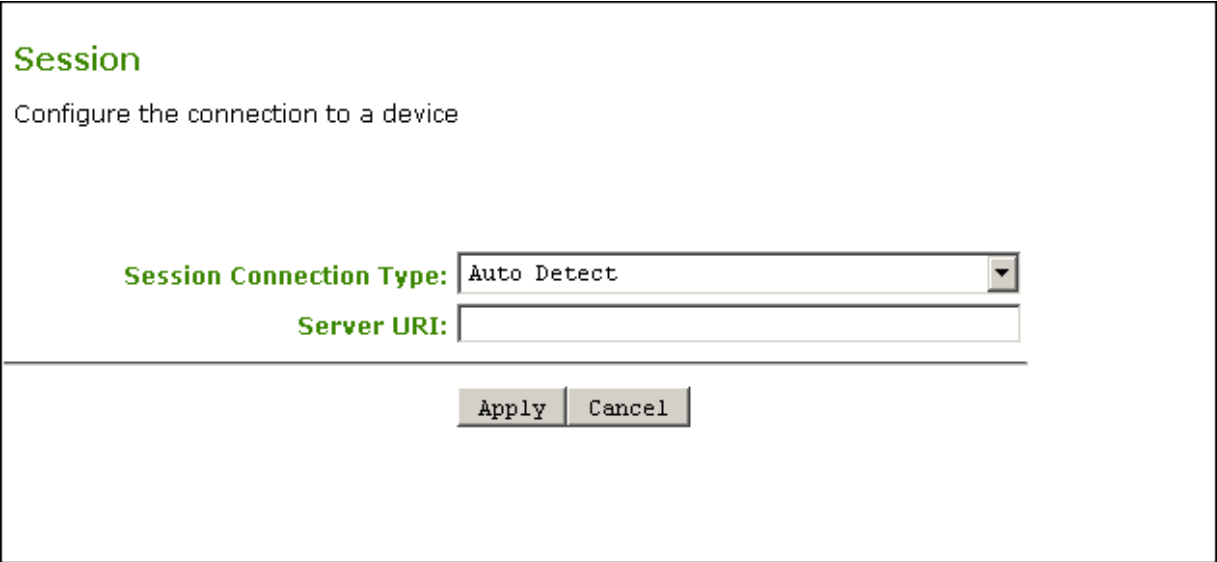
Apply

Cancel

fig 4 AWI Session Connection type – Amazon WorkSpaces

AWI: Auto Detect Session Settings

Select the **Auto Detect** session connection type from the **Configuration > Session** page to let the Tera2 PCoIP Zero Client automatically detect which broker protocol a connection server is using so users in a mixed environment (for example, one that uses View Connection Servers and PCoIP Connection Managers) do not have to manually reconfigure the session type each time they switch brokers. Once a successful connection has been made, the server URI will automatically appear in the **Server** drop-down list on the user's OSD **Connect** screen, along with any other desktops the user has successfully connected to.



The screenshot shows a configuration window titled "Session" with the subtitle "Configure the connection to a device". It contains two fields: "Session Connection Type" with a dropdown menu set to "Auto Detect", and "Server URI" with an empty text box. At the bottom are "Apply" and "Cancel" buttons.

fig 5 AWI Session connection type – Auto Detect

AWI Auto Detect Parameters

Server URI Enter the Uniform Resource Identifier (URI) of the current connection broker. Once a successful connection has been made to this server, it will appear in the Server drop-down list on the OSD Connect page if the Tera2 PCoIP Zero Client is configured to cache servers.

The URL must be in the form **https://<hostname>** or **https://<ip address>**.

AWI: Direct to Host Session Settings

Select the **Direct to Host** session connection type from the **Configuration > Session** page to configure the client to connect directly to a Remote Workstation Card.

Session

Configure the connection to a device

Session Connection Type:

Direct to Host

DNS Name or IP Address:

10.0.34.207

Hide Advanced Options

Wake Host from Low Power State:

Wake-On-LAN Enabled + Peer Address

Host Wake MAC Address:

00-30-04-0E-4F-A2

Enable Auto-Reconnect:

Enable Peer Loss Overlay:

Enable Preparing Desktop Overlay:

Enable Session Disconnect Hotkey:

☒

CTRL + ALT + F12

PCoIP Utility Bar Mode:

Disabled

Session Negotiation Cipher Suites:

Maximum Compatibility: TLS 1.0 or higher with RSA keys

Disconnect Message Filter:

Show All

Enable DSCP:

Enable Congestion Notification:

☒

Apply

Cancel

AWI Session connection type – Direct to Host

PCoIP Utility Bar Mode	When enabled, the PCoIP Utility Bar appears at the top of the primary display when a user is in session and moves the cursor directly under the bar. The utility bar can be used to disconnect a session or to shut down a remote workstation. For Direct to Host session connection types, Local Cursor and Keyboard must be enabled in order for the Tera2 PCoIP Zero Client to process mouse events for the utility bar. For all connection types, the mouse must be locally connected (that is, not bridged). • Disabled: Disables the PCoIP Utility Bar. By default, the utility bar is disabled. • Enabled: Enables and auto-hides the PCoIP Utility Bar. Users can show the utility bar by pointing the mouse at the top of the screen directly under the utility bar. Users can slide the utility bar to the right and left at the top of the screen. • Enabled and Pinned: Enables and pins the PCoIP Utility Bar at the top of the screen. Users cannot hide the utility bar, but they can slide it to the right and left at the top of the screen. This feature is configurable from the PCoIP Management Console and AWI only. It requires firmware version 4.2.0 or higher.
Session Negotiation Cipher Suites	Configure the Transport Layer Security (TLS) cipher to use for negotiating the TLS session between the PCoIP client and the PCoIP host. • Maximum Compatibility: TLS 1.1 or higher with RSA keys: This option provides maximum compatibility. • Suite B: TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption. This option provides a higher level of security.
Disconnect Message Filter	This field lets you control what type of messages appear when a session is disconnected. There are three categories: Information: User- or administrator-initiated actions affecting the session:

- You have been disconnected because you logged in from another location or your host was shut down or restarted.
- You have been disconnected because an administrator disconnected you.
- You have been disconnected because you logged in from another location.
- You have been disconnected because you disconnected from your workstation.

Warning: System-initiated, but expected actions affecting the session:

- You have been disconnected because your session timed out.

Recover AWI account

Go to the Control Panel.

Click on "Recover username" under "Account".

This will take you to the "Recover Username" section.

Enter the email address you used to register the AWI account in the "Email" field, then click on "RECOVER USERNAME".

The system will send an email with the AWI account username to the email address entered.

If the email address entered is incorrect, an error message will appear saying "Check that the email is correct".

Chapter No :4

4.Result and Discussion

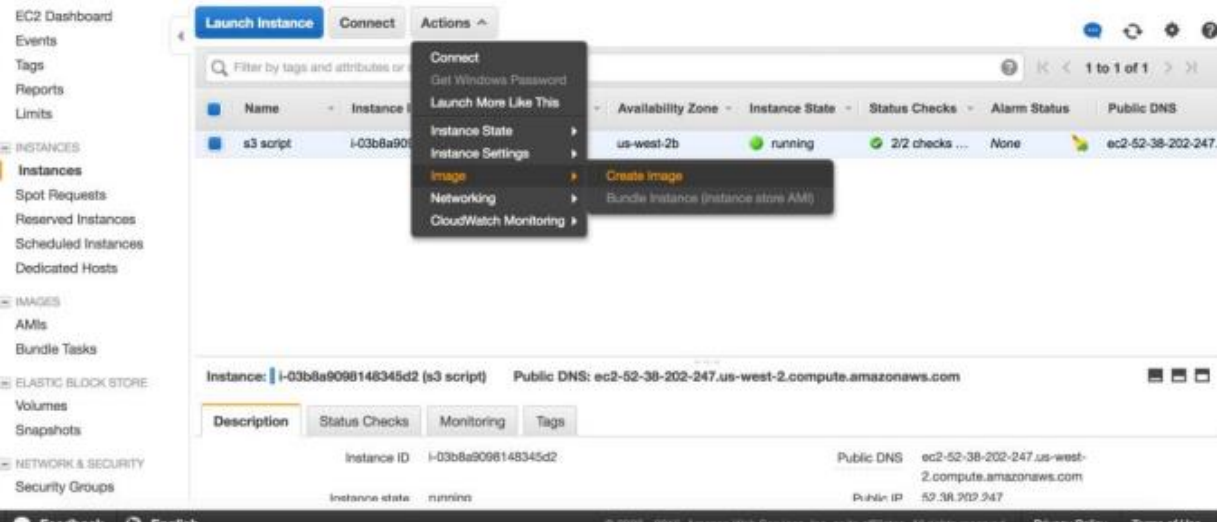
4.1 Result and Discussion:

When you develop a comprehensive strategy for backing up and restoring data, you must first identify the failure or disaster situations that can occur and their potential business impact. In some industries, you must consider regulatory requirements for data security, privacy, and records retention. You should implement backup processes that will offer the appropriate level of granularity to meet the RTO and RPO of the business, including:

- File-level recovery
- Volume-level recovery
- Application-level recovery (for example, databases)
- Image-level recovery

The following sections describe backup, recovery, and archive approaches based on the organization of your infrastructure. IT infrastructure can broadly be categorized as cloud native, on-premises, and hybrid.

Creating EBS Snapshots When you create a snapshot, you protect your data directly to durable disk-based storage. You can use the AWS Management Console, the command line interface (CLI), or the APIs to create the Amazon EBS snapshot. In the Amazon EC2 console, on the Elastic Block Store Volumes page, choose Create Snapshot from the Actions menu. On the Create Snapshot dialog box, choose Create to create a snapshot that will be stored in Amazon S3

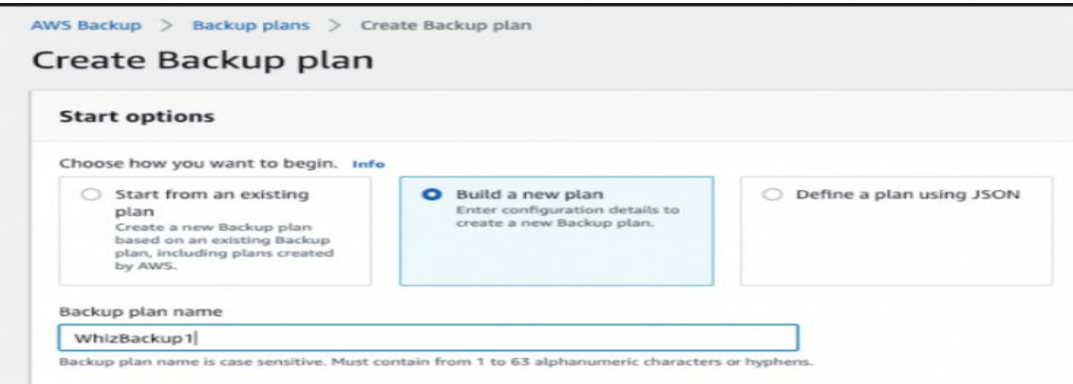
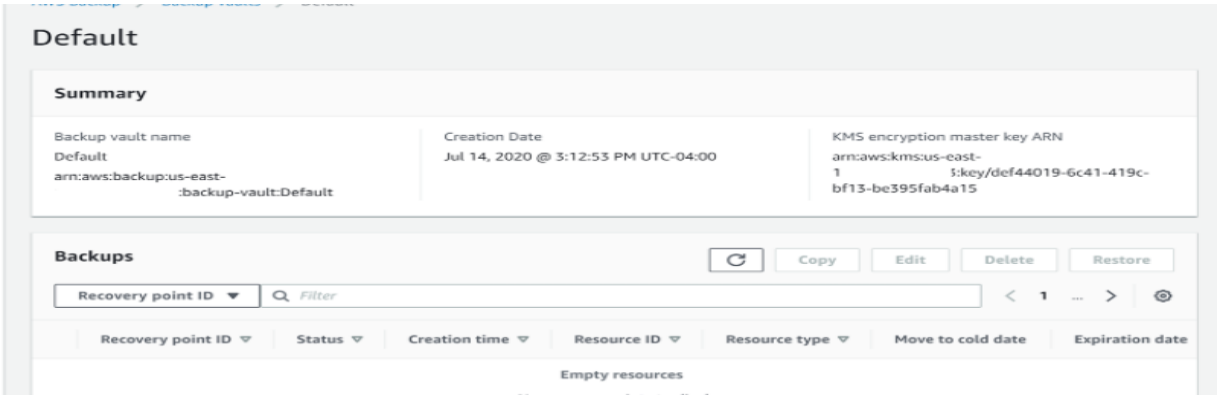


Chapter No : 5

5.Summary and conclusion

5.1 conclusion :

Gartner has recognized AWS as a leader in public cloud storage services¹⁷. AWS is well positioned to help organizations move their workloads to cloud-based platforms, the next generation of backup. AWS provides cost-effective and scalable solutions to help organizations balance their requirements for backup and archiving. These services integrate well with technologies you are using today.

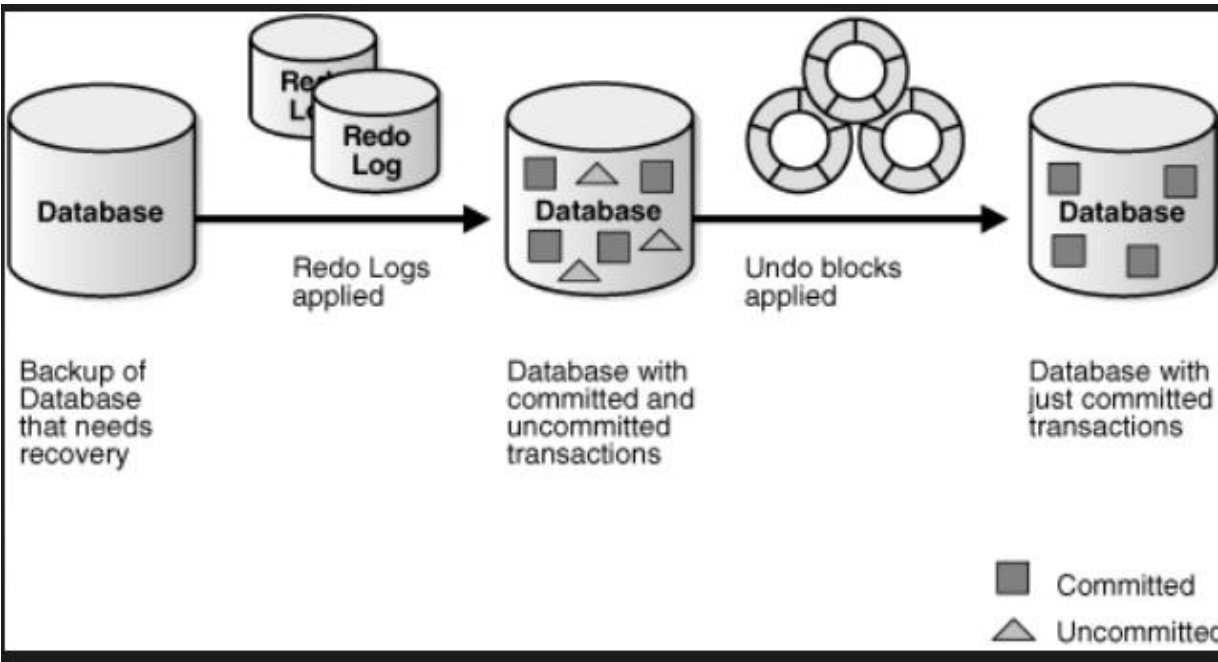


References:

- 17 <http://www.gartner.com/technology/reprints.do?id=1-1WWKTQ3&ct=140709&st=sb>
- Star Cloud Computing (starcertification.org)
- Microsoft Hybrid Cloud Unleashed with Azure Stack and Azure Paperback – Illustrated, 30 July 2018
by Kerrie Meyler (Author), Steve Buchanan (Author), Mark Schulman (Author), Jakob Svendsen (Author), Janaka Rangama (Author)

APPENDIXES:

Instance recovery



Backup in AWS:

