SIDCORP TECH

AWS Backup Using Veeam

A Case Study for Marslab Intelligence

2025

Introduction

Marslab runs a mission-critical FinOps application on Amazon Web Services (AWS). This application processes highly sensitive financial and operational data that directly supports:

- **Business continuity**
- **Reporting and analytics**
- **Compliance requirements**
- **Strategic decision-making**

Ensuring data protection, high availability, and rapid recovery is essential for Marslab to maintain operational resilience and meet internal governance standards. To achieve this, SIDCORPTECH implemented a robust cloud-native backup solution using Veeam Backup integrated with Amazon S3.

Challenges

Ensuring Backup Redundancy & High Availability

- Protect FinOps data continuously.
- Backup strategy lacks zone redundancy
- Need a scalable, durable backup.
- Require cross-region replication.

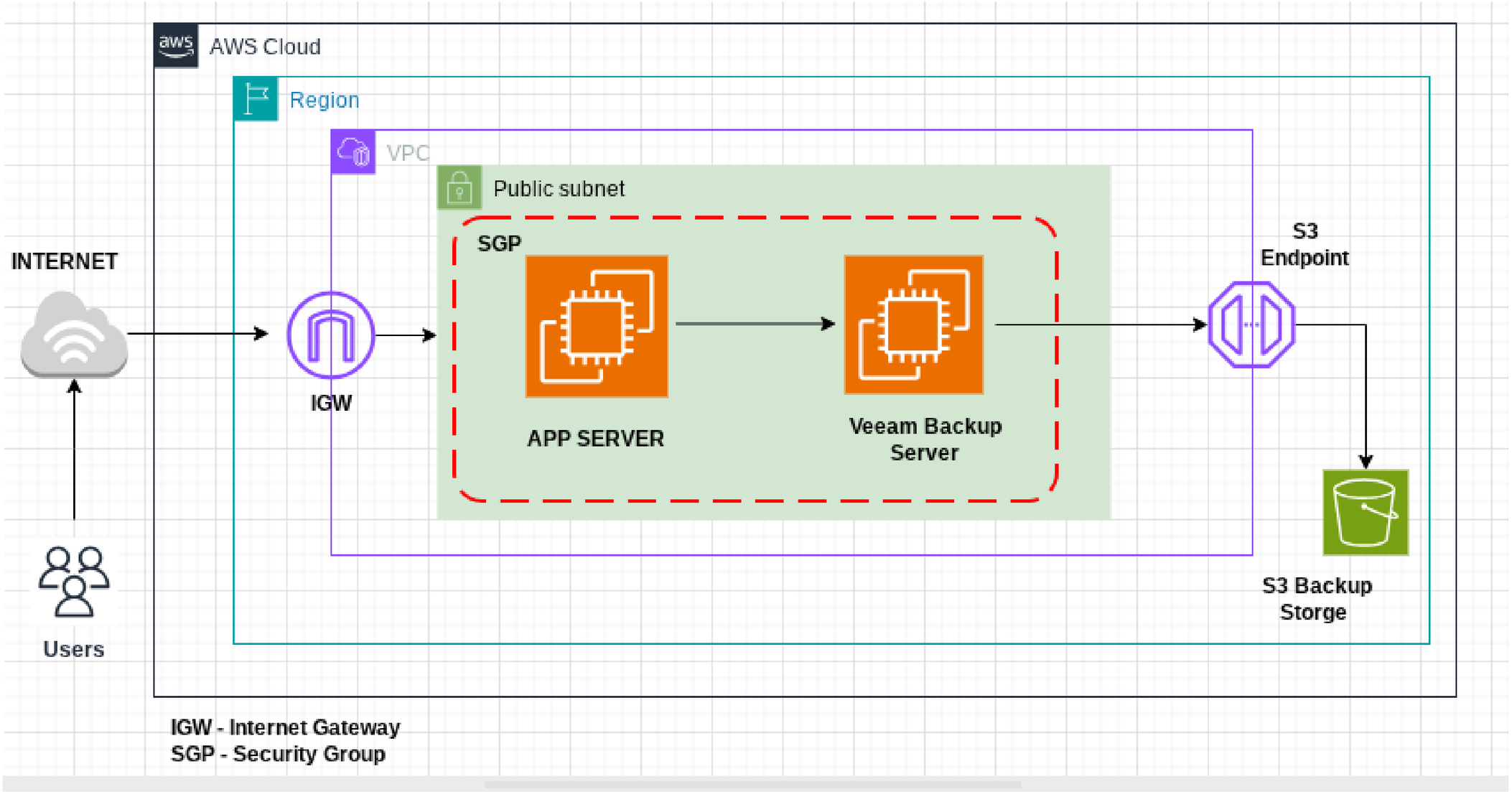
Strict RTO & RPO Requirements

- Marslab required very low RTO and RPO.
- Traditional backups couldn't provide near-real-time results.
- The system needed rapid full and granular file restores.

Compliance & Governance

- Financial data demands enterprise-grade security controls.
- Required IAM-based access control, encrypted backup transfers, and auditable backup pipelines.

Architecture Diagram



Our Solution

Marslab deployed a high-availability cloud backup architecture built on AWS and powered by Veeam Backup & Replication.

Architecture Highlights:

- EC2 App Server and EC2 Veeam Backup Server placed inside a secured VPC public subnet.
- Traffic flows via Internet Gateway (IGW) for Veeam updates and connectivity.
- Backups are directed to Amazon S3 using a secure S3 Endpoint inside the VPC.
- Veeam handles backup scheduling, incremental jobs, encryption, retention, and restore operations.
- Amazon S3 provides multi-AZ durability (11 nines), scalability, and optional Cross-Region Replication (CRR).
- Security Groups (SGP) isolate traffic and enforce least-privilege communication.

Backup Workflow:

- Application data resides on the EC2 App Server.
- Veeam Backup Server pulls data using secure internal traffic.
- Veeam pushes encrypted backup files to Amazon S3 via VPC S3 Endpoint.
- Optional CRR ensures backups exist in a secondary AWS Region for disaster recovery.

Benefits of Our Solution

01.

High Durability & Resilience

- Amazon S3 ensures 99.999999999% durability.
- Backups remain protected even during localized failures or AZ outages.
- CRR provides failover across regions.

02.

Minimal RTO & RPO

- Veeam enables fast incremental backups and near-real-time data capture.
- Supports full, incremental, and application-aware backups.
- Rapid restore options reduce downtime to minutes.

03.

Enhanced Security & Compliance

- Data transfer is encrypted end-to-end.
- IAM-based role access ensures strict governance.
- VPC S3 Endpoint keeps backup traffic private and secure.

04.

Scalability & Cost Optimization

- S3 scales effortlessly with backup growth.
- Lifecycle policies automatically move old backups to S3 Glacier tiers for cost savings.
- Pay-as-you-grow model eliminates hardware investments.

05.

Operational Efficiency

- Automated scheduling reduces manual intervention.
- Simplified backup management through Veeam dashboard.
- Fully auditable logs and reporting.

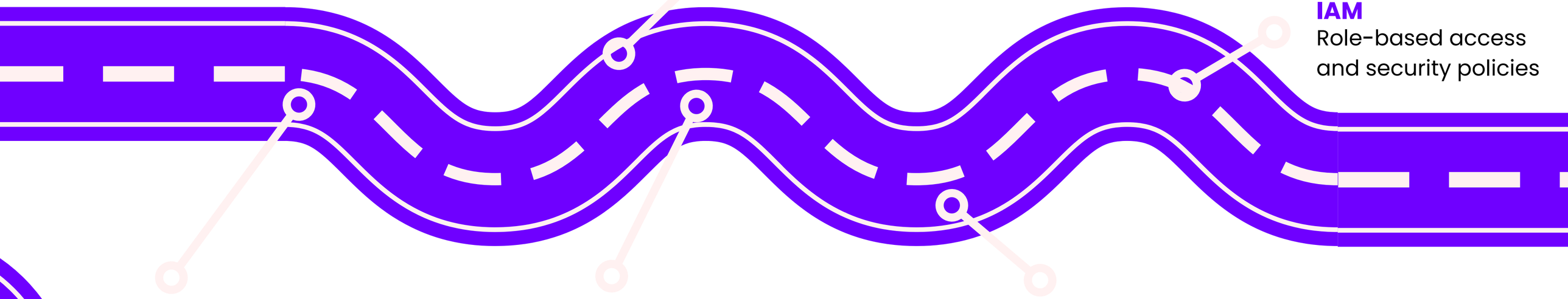
Resources Used

Amazon VPC

Backup storage, versioning, CRR

IAM

Role-based access and security policies



Amazon EC2

Application and Veeam Backup server instances

Amazon VPC

Secure network architecture

Third-Party Tool: Veeam Backup & Replication

Backup engine and restore management

SIDCORP TECH

Thank You