

# Azure Backup and Disaster Recovery Implementation

Portfolio Lab By THATO KGOLE

Date: November 2025

Cloud Platform: Microsoft Azure

## Overview

This project demonstrates how to implement a *complete backup and disaster recovery solution* for Azure Virtual Machines. Using *Azure Backup* and *Azure Site Recovery*, the project ensures that workloads are protected against accidental deletion, corruption, and regional outages. The solution provides business continuity by allowing data recovery and VM failover to a secondary region.

## Problem Statement

Organizations rely on cloud infrastructure for critical workloads. However, VMs can be accidentally deleted, corrupted, or affected by ransomware. Additionally, regional outages can disrupt service. The challenge is to:

- > Protect VM data with automated backups.
- > Ensure workloads can be restored quickly if failure occurs.
- > Maintain business continuity during regional outages through disaster recovery.

### Step 1: Create a Resource Group

To group all related content.

Home > Resource Manager | Resource groups >

## Create a resource group

Basics Tags Review + create

[Automation Link](#)

### Basics

Subscription ZEMBE  
Resource group name ZeroTrustHub  
Region South Africa North

### Tags

None

Previous

Next

Create

## Step 2: Create Recovery Services Vault

A secure container to store backups and replication configurations.

Home > Recovery Services vaults >  
**Create Recovery Services vault** ...

\* Basics   Redundancy   Encryption   Vault properties   Networking   Tags   **Review + create**

**Summary**

**Basics**

Subscription: ZEMBE  
Resource group: ZeroTrustHub  
Vault name: BackupVault1  
Region: South Africa North

**Redundancy**

Backup Storage Redundancy: Geo-redundant  
Cross Region Restore: Disable

**Vault properties**

Immutability: Disabled

**Networking**

Connectivity method: Allow public access from all networks

**Create**

Previous: Tags

Feedback

Download a template for automation

## Step 3: Create a Virtual Machine

A cloud-based server to run workloads.

Home > CreateVm-MicrosoftWindowsServerWindowsServer-202-20251112101907 | Overview >

**WebServerVM** Virtual machine Help me copy this VM in any region Manage this VM with Azure

**Overview** Help me copy this VM in any region

**Essentials**

Resource group <span>(new)</span> : <a href="#">ZeroTrustHub</a>	Status: <span>Running</span>	Stop or suspend
Location: <span>South Africa North (Azure)</span>	Subnet: <span>WebSubnet</span>	Operating system: <span>Windows</span>
Subscription <span>(new)</span> : <a href="#">ZEMBE</a>	Subscription ID: <a href="#">7e04117e-0f6d-4104-aed3-1e0019c111d4</a>	Primary NIC: <span>Standard B1s (1 vCPU, 1GB memory)</span>
Availability zone: <span>1</span>	Tags (edit): <span>2 items</span>	Virtual network/subnet: <a href="#">ZeroTrustHubStandardB1sSubnet</a>
	Properties	DNS name: <span>Not configured</span>
	Monitoring	Health status: <span>OK</span>
	Capabilities (0)	Time created: <span>11/10/2025, 8:04 AM UTC</span>

**Properties** **Monitoring** **Capabilities (0)** **Recommendations** **Tutorials**

**Virtual machine**

Computer name: <a href="#">WebServerVM</a>	Networking
Operating system: <a href="#">Windows</a>	Public IP address: <a href="#">102.37.147.243 (Network interface webservervm#04_21)</a>
	Associated public IPs

Add or remove features by pressing **COMPUTE + F10**

## Step 4: Configure Backup for VM

Protect VM data from accidental deletion or corruption.

The screenshot shows the Azure portal interface for a Backup Vault named "BackupVault1". The top navigation bar includes links for "Increase security level of this vault", "Initiate backup for jobs in this vault", and "Analyze all job failures for this vault". Below the navigation bar, there are tabs for "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", and "Resource visualizer". The "Overview" tab is selected, displaying details such as Resource group (ZeroTrustHub), Location (South Africa North), Subscription (ZMRE), and Subscription ID (4ec5417c-69e8-48d9-bed1-3bd001fa344d). A callout box provides links to "Help me copy this vault settings in any region", "Show me virtual machines that can be protected", and "Analyze all backup job failures for this vault". Below this, the "Backup Items (Azure Virtual Machine)" section lists one item: "WebServerVM" in the ZeroTrustHub resource group, with a status of "Passed" and a warning message about a pending initial backup. Navigation buttons include "Previous", "Page 1 of 1", and "Next >".

## Step 5: Backup Recovery (Documented Step)

Verify that backups are recoverable without affecting the original VM.

### STEPS:

1. Recovery Service Vault – Backup items – Azure Virtual Machine.
2. Select (WebServerVM) – Restore VM
3. Restore Point – Create new VM
4. Configure new VM settings and click Restore.

## Step 6: Configure Azure Site Recovery (Disaster Recovery)

Ensure VM can continue running in case of primary region outage.

The screenshot shows the Azure portal interface for a Site Recovery vault named "site-reco-4sa-asr-automationaccount". The top navigation bar includes links for "List jobs executed by this Automation Account", "How do I troubleshoot issues with this resource?", and "Show me runbook status for this Automation Account". Below the navigation bar, there are tabs for "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Resource visualizer", "Process Automation", "Configuration Management", and "Tags [edit]". The "Overview" tab is selected, displaying details such as Resource group (site-recovery-vault), Location (East US), Subscription (ZMRE), and Status (Active). A callout box provides links to "Control your job execution environment, manage Packages easily and update the Runtime version of your runbooks using Runtime environment. Learn more.", "Azure Automation is revising the service and subscription limits starting 13 January 2023 to ensure fair share of cloud resources for all users. Learn more.", and "JSON View".

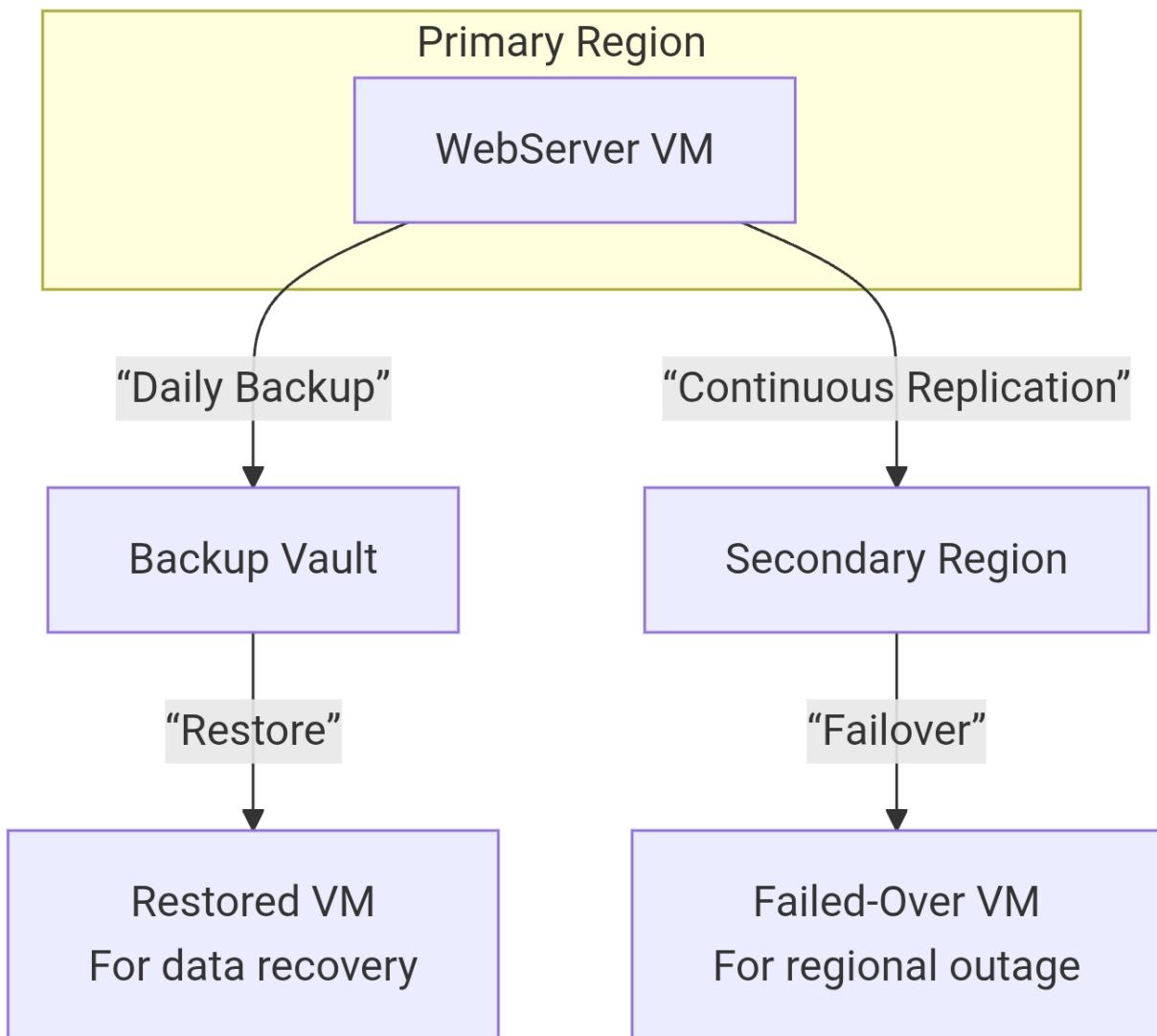
## Step 7: Test Failover (Documented steps)

Ensure disaster recovery works without impacting production VM.

**STEP:**

1. Recovery Service Vault – Site Recovery – Replicated items.
2. Select WebServerVM – Test Failover.
3. Choose the latest recovery point.
4. Select Virtual Network for the test VM.
5. Click OK to start test failover.
6. After verification, Clean up Test Failover

## DIAGRAM



## OUTCOME

- > Automated daily backup for WebServerVM enabled
- > Backup recovery steps documented and can be executed as needed.

- > VM replication to a secondary region established for disaster recovery
- > Test failover steps documented to validate business continuity