Azure Frontrow Insurance – UAT Architecture and Deployment Guide

# 1. Overview

This document describes the UAT environment for Frontrow Insurance portals running on Azure. It covers the infrastructure components, configuration, deployment steps, and failover testing procedure.

Environment consists of two identical application VMs (App1 & App2), one Redis VM, an Azure SMB file share, a managed MySQL PaaS database, and Cloudflare Load Balancer for routing traffic.

# 2. VM Configuration

• App1 VM: Ubuntu, size e.g. Standard B2ms, Availability Zone 1

• App2 VM: Ubuntu, identical configuration to App1, Availability Zone 1

• Redis VM: Ubuntu, separate VM hosting Redis

• Access configured via SSH public key. Evan user account created for deployment.

# 3. Storage – SMB Share

Azure Storage Account File Share created with SMB protocol. Used for shared document storage between App1 and App2.

Mounting Steps on each VM:

1. Go to Azure Portal → Storage Account → File Shares → Your Share → Connect (Linux).

2. Copy the mount command provided.

3. SSH into VM and run:

sudo mkdir -p /mnt/smbshare

sudo mount -t cifs //<storage>.file.core.windows.net/<share> /mnt/smbshare -o vers=3.0,username=<storage>,password=<key>,dir\_mode=0777,file\_mode=0777,serverino

4. Add the same entry to /etc/fstab for persistence.

NSG Rule: Allow outbound port 445 to Destination Service Tag 'Storage'.

# 4. Load Balancing – Cloudflare

Cloudflare Load Balancer configured for round-robin across App1 and App2 VMs.

Setup Steps:

1. Cloudflare Dashboard → Domain frontrowinsurance.com → Traffic → Load Balancing → Create LB.

2. Hostname: backstage.uat.frontrowinsurance.com

3. Pools: Pool1 = App1 VM IP, Pool2 = App2 VM IP.

4. Health Monitor: Protocol HTTP or TCP, Port 80/443, Path '/'.

5. Steering Policy: Round robin (or dynamic for failover).

# 5. DNS Records

CNAME records created to point subdomains to Cloudflare LB hostname:

• Name: backstage.uat

• Content: cflbuat.frontrowinsurance.com (LB hostname)

Remove any old A records pointing directly to VM IPs.

# 6. SSL / Certificates

Cloudflare Edge Certificates provide HTTPS for end users. Currently using Flexible SSL (browser HTTPS, origin HTTP). For Full/Strict SSL, install Cloudflare Origin Certificate on VMs.

# 7. Deployment Steps

• Evan deploys the Laravel applications to App1/App2 using Laravel Forge.

• To add a new portal, update code in Forge and deploy to both VMs; DNS/LB entry may need updating.

# 8. Failover Testing Procedure

1. Log in with test credentials provided by Evan to verify portal functionality.

2. Power off App1 VM and confirm portal remains accessible via App2 VM.

3. Power App1 back on, power off App2, and confirm again.

4. Check headers or test page to verify which VM is serving requests.

# 9. Contacts / Owners

• Code/Deployment: Evan (Developer)

• Infrastructure/DNS: [Your Name] / WebOps Team

• Cloudflare Account: Lead / Security Team