VIDIZMO DISASTER RECOVERY STRATEGY

THIS DOCUMENTATION ENTAILS ALL INFORMATION THAT DESCRIBES VIDIZMO'S ABILITY TO SURVIVE A DISASTER.

TABLE OF CONTENTS

VIDIZMO DISASTER RECOVERY STRATEGY 1

Policy Statement 3

Objective 3

- Introduction 3
- Disaster 3
- Purpose 3

DR Overview 5

- Components 6

Scope 8

Protected Workloads 8

Test Failover 9

Planned Failover 9

Data Backup and Storage Account Redundancy 10

- Storage accounts 10
- Data Backups 10

Emergency Contacts 10

Revision History 11

Policy Statement

- VIDIZMO has developed a comprehensive Disaster Recovery Strategy.
- A formal risk assessment shall be undertaken to determine the requirements.
- The documentation covers all essential and critical technology elements, systems, and networks in accordance with the key business activities.
- The plan must be tested periodically, in a simulated environment to ensure it can be fully and effectively implemented in an emergency.
- All VIDIZMO team members must be made aware of this plan and their own respective roles in carrying it out.
- The DR strategy document must be kept up to date by the DR lead to take changing circumstances into account.

Objective

Introduction

This document is the source of all information that describes VIDIZMO's ability to survive a disaster.

Disaster

A disaster can be caused by many events resulting in VIDIZMO's network infrastructure and services not being able to perform some or all their roles and responsibilities for a period. VIDIZMO defines Disasters as the following:

- One or more vital systems are non-functional
- Azure data center is available, but all systems are non-functional
- Azure data center and all systems are non-functional

The following events can result in a disaster:

- Environmental disaster (flooding, hurricane, fire, etc.)
- Data center hardware failures / server rack failures
- Power outage
- Malware, Ransomware, etc. (data loss)

Purpose

The top priority of VIDIZMO's DR team is to bring all organization groups and departments back to business-as-usual as quickly as possible. This includes:

- Preventing data loss and service outages
- Minimizing downtime related to service availability
- Backup and redundancy plans

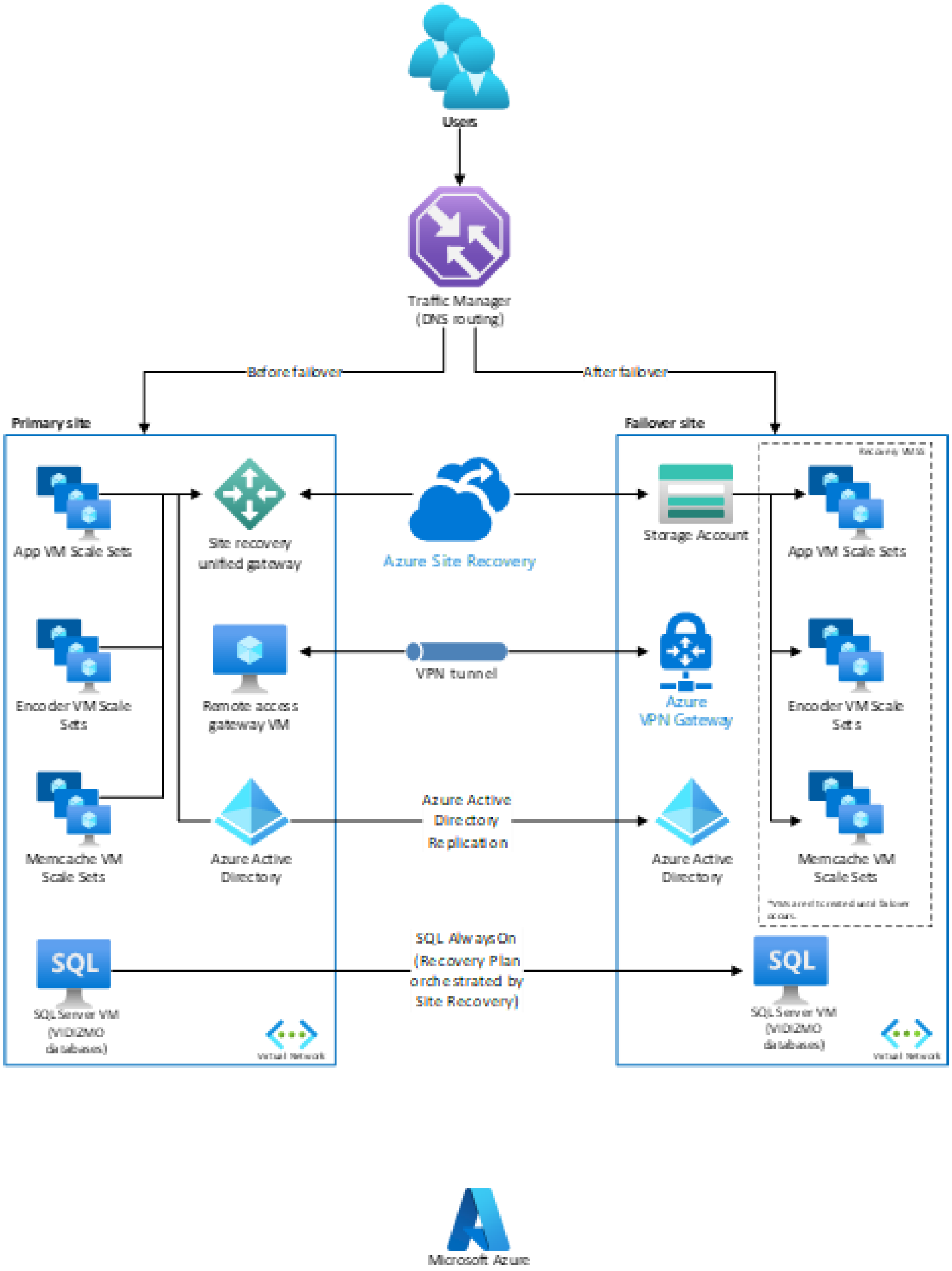
- Failover systems in the event of disaster
- Restore point in time backups in case of data loss

-- Continued on the next page --

DR Overview

Our disaster recovery (DR) solution is powered by MS Azure. We are using Azure Site Recovery (ASR) which is Microsoft's Disaster Recovery-as-a-Service (DRaaS) solution built specifically for Azure workloads. ASR enables quick recovery from catastrophes with minimal downtime.

Here's a diagram that explains how the DR architecture is set up:



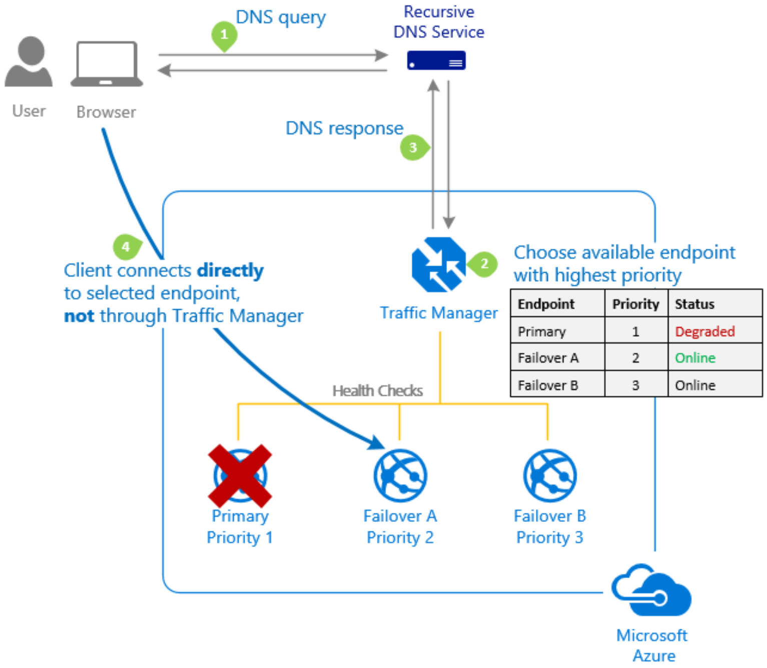
Components

Here is the list of main components to support the disaster recovery solution.

1. **Traffic Manager:** DNS traffic is routed via Traffic Manager, which can easily move traffic from one site to another based on policies defined by the infrastructure team.
2. **Site Recovery:** Azure Site Recovery orchestrates the replication of machines and manages the configuration of the failover procedures.
3. **Blob Storage:** Blob storage stores the replica images of all machines that are protected by Site Recovery.
4. **Azure Active Directory:** Azure Active Directory is a replica of the on-premises Azure Active Directory services allowing cloud applications to be authenticated and authorized.
5. **VPN Gateway:** The VPN gateway supports the communication between the primary network and the cloud network securely and privately.

The VMs deployed under the primary site are intelligently arrayed to be always available, such as by rerouting requests to the available server in case of failover of one of the servers at the primary location.

The architecture has been laid out in such a manner that when in case of a disaster the entire primary site is unavailable, the traffic manager shall move traffic (user requests) from our primary site to the failover site using the priority routing method. Here is how it works:



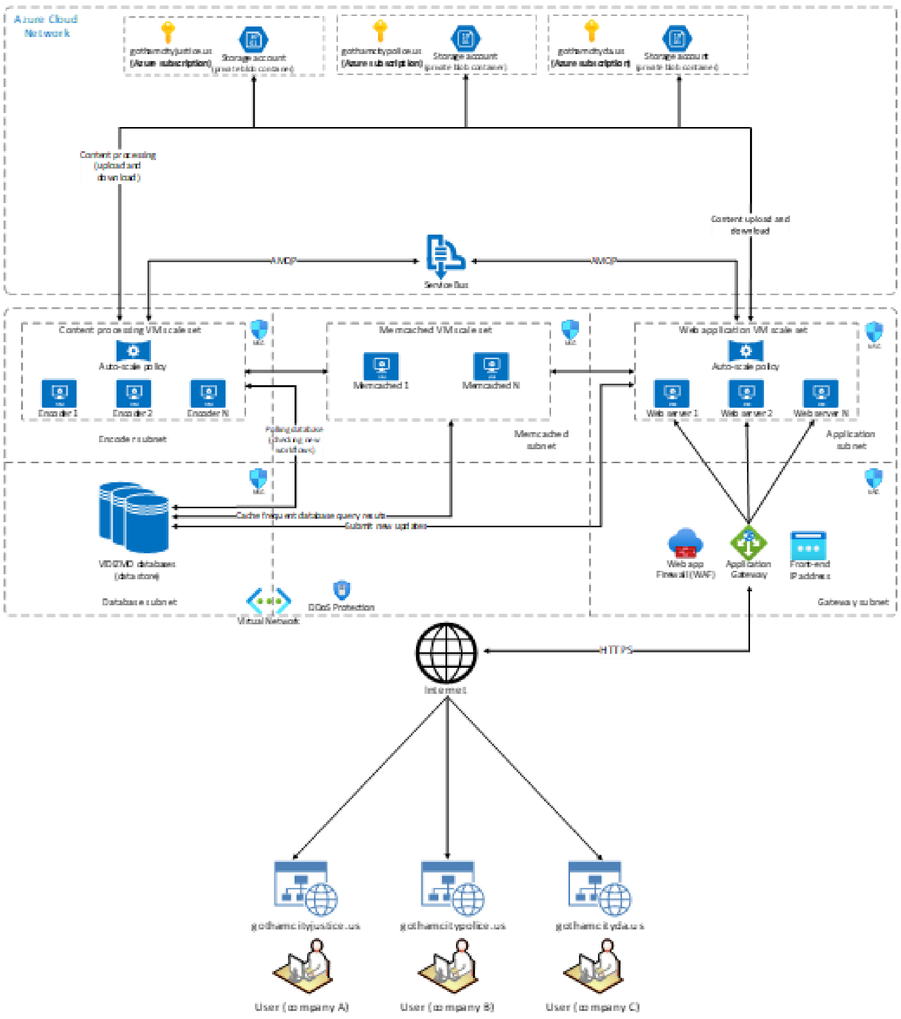
Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

The core application servers are hosted in Azure Virtual machines (VMs), which are physically separated across geo-redundant zones, and a virtual network is created using load balancers at each site. The server configurations at these locations are replicated for high availability, so the applications stay running, despite any issues at the physical locations.

The VM infrastructure is set up and configured in Azure Virtual Machine Scale Sets that group the VMs together to run the app workload and provide sophisticated load-balancing and high availability of application services.

An auto-scale policy is used by Virtual Machine Scale Sets to automate the VM scaling process. It would auto-scale the VMs based on resource consumption, which essentially prevents resource exhaustion, service unavailability, performance issues, etc., and provides continued uninterrupted services. This means that VMs will never have downtime simultaneously when updates are being released on servers.

Below is the system architecture diagram that explains how the infrastructure is currently laid out:



Scope

This DR strategy document takes below technology areas in consideration:

- Network infrastructure
- Storage accounts
- Web application servers
- Content processing servers
- Backend services
- Content delivery (CDN)
- Live streaming services
- Databases

Note: This DR document does not take into consideration any non-technology resources, and related disasters.

Protected Workloads

The following resources are protected with Azure Site Recovery:

S/No.	Resource Name	Resource Type	Service Type	Status
1	Vidappprdusvmss01	VMSS	Web app	Protected
2	Vidappprdusvmss02	VMSS	Web app	Protected
3	Vidoncprdusvmss01	VMSS	Content processing	Protected
4	Vidoncprdusvmss02	VMSS	Content processing	Protected
5	ProdSQL-VM	VM	MS SQL Databases	Protected
6	Vidstrprdus01	VM	Wowza streaming engine	Protected
7	Vidstrprdus02	VM	Wowza streaming engine	Protected
8	Vidstrprdus03	VM	Wowza streaming engine	Protected

9	Vidstrprdus04	VM	Wowza streaming engine	Protected
10	Vidstrprdus05	VM	Wowza streaming engine	Protected

Test Failover

The test failover would validate the replication of VMs and perform a disaster recovery drill without any data loss or downtime. Doing a test failover doesn't have any impact on the ongoing replication and prod environment.

When a test failover is triggered, it involves following steps:

1. **Prerequisites check:** This step ensures that all conditions required for failover are met.
2. **Failover:** This step processes the data and makes it ready so that an Azure virtual machine can be created out of it. If you have chosen the latest recovery point, this step creates a recovery point from the data that has been sent to the service.
3. **Start:** This step creates an Azure virtual machine using the data processed in the previous step.

Reference policy statement: The test shall be conducted every week (outside of normal working hours) to ensure that the VMs are fully backed and in recoverable state.

Planned Failover

When a planned failover is triggered, first the source virtual machines are shut down, the data yet to be synchronized is synchronized and then a failover is triggered.

When a planned failover is triggered, it involves following steps:

1. **Prerequisites check:** This step ensures that all conditions required for failover are met.
2. **Failover:** This step processes the data and makes it ready so that an Azure virtual machine can be created out of it. If you have chosen the latest recovery point, this step creates a recovery point from the data that has been sent to the service.
3. **Start:** This step creates an Azure virtual machine using the data processed in the previous step.

Note: Planned failover shall only be performed after the DR lead has declared a disaster.

Data Backup and Storage Account Redundancy

This section explains replication of storage accounts, data backups, and their RTO and RPO timelines.

Storage accounts

All storage accounts used by VIDIZMO SaaS application are protected with standard GRS (Global Replication Service) provided by Azure. Data recovery is based on following timelines:

- RTO: 48 hours
- RPO: 24 hours

Data Backups

All production databases are backed on scheduled basis, the backups are stored under Azure storage account locations. We are creating full point-in-time backups based on following schedule:

Backup frequency	Lifecycle policy (retention)
Daily	6 backup copies
Weekly	4 backup copies
Monthly	6 backup copies
Bi-annual	2 backup copies

- RTO: 2 hours
- RPO: 24 hours

Emergency Contacts

The below are primary contacts responsible to provide emergency services in the event of a disaster.

Name	Role	Responsibilities	Contact Type	Contact Information
Samreen Farhan	DR Lead	Makes DR decisions, initiates DR procedures	Work email	samreen.farhan@vidizmo.com
James Corden	DR Team	Follow-up recovery procedures,	Work email	james.corden@vidizmo.com

		communications, and Assist DR Lead		

Revision History

Any changes, edits, and updates made to the DR document will be recorded here. It is the responsibility of DR lead that all existing copies of the DR documents be up to date. Whenever there is an update to the DR document, VIDIZMO requires that the version number be updated (below) to indicate this.

Name	**Role**	**Date**	**Version**	**Notes**
James Corden	DR team	4/10/2023	23.2	Revised version
James Corden	DR team	1/1/2023	23.1	Minor updates
Kashif Siddiqui	DR team	10/12/2022	22.4	Minor updates

For questions, please contact support@vidizmo.com and our tech team will be happy to help and provide information.

--End of document--