Milestone Disaster Recovery Testing Results

Table of Contents

Introduction

This Disaster Recovery Testing (DRT) is a multi-step drill of an organization's disaster recovery plan (DRP) designed to assure that information technology (IT) systems will be restored if an actual disaster occurs.

Definition of a Disaster

A disaster can be caused by man or nature and results in Milestone not being able to perform all or some of their regular roles and responsibilities for a period. Milestone defines disasters as the following:

- *One or more vital systems are non-functional*
- *Azure Public Cloud has outage on which Milestone Production Infrastructure hosted.*
- *The building is not available for an extended period, but all systems are functional within it*
- *The building is available, but all systems are non-functional*
- *The building and all systems are nonfunctional*

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- *Fire*
- *Flash flood*
- *Pandemic*
- *Power Outage*
- *War*
- *Theft*
- *Terrorist Attack*

Purpose

Disasters do not occur very often, but when they do, the effects can be devastating. The main objective of DRT is to make sure that, in case a disaster does happen, the DR plan will **work**. A company's DR site will go live, IT systems will go back online with minimal downtime. Perhaps a company uses cloud-based DR, or DRaaS – in either case, DR testing reveals whether the backup is truly as foolproof as it needs to be.

Scope

The Milestone DRP takes all the following areas into consideration:

- *Azure Web server – Hosting Live Production Websites.*
- *Azure Virtual Network Infrastructure*
- *Azure Network Security Group*
- *Geo DNS Service*
- *Azure Site Recovery*
- *Azure Backup Service.*

This DRT does not take into consideration any non-IT, personnel, Human Resources, and real estate related disasters. For any disasters that are not addressed in this document, please refer to the business continuity plan created by Milestone or contact Anil Aggarwal, CEO, Milestone Internet Marketing.

Disaster Recovery vs. Business Continuity Planning

Disaster recovery planning and testing is a term often confused with business continuity planning (BCP). While DRP and BCP are closely related, however, they are not the same.

A DR plan and testing system specifies the steps an IT organization must take to recover systems that will meet the company's technology needs after a disaster.

A BCP, on the other hand, spells out what a business must do to make sure that its products and services remain available to customers. A BCP is made up of a business impact analysis, risk assessment, and an overall business continuity strategy. It is tested through a business continuity test (BCT).

Some organizations treat DRP/DRT and BCP/BCT separately, while others include DR within overall business continuity planning and testing.

DR Testing Techniques

Beyond restoring data and keeping critical applications and services online during the emergency, DR solutions should include ways to alert staff about the disaster and to allow communications during and after the event if regular phone lines and networks go down.

In the planning and testing process, DR teams should also recognize that, despite the disaster, the organization must continue to meet its security and regulatory compliance obligations.

Five types of DRTs are used to test disaster recovery solutions:

Paper test: In a paper test, members of the DR team read and annotate recovery plan documents such as DR policies, procedures, timelines, benchmarks, and checklists. A hard copy of documents should be stored in a secure offline environment, and a digital copy in the cloud.

Walk through test: A walk through test is a group walk through of the DRP to pinpoint any issues that need to be addressed and any modifications that should be made to the disaster recovery environment.

Simulation: In a procedure somewhat along the lines of a fire drill, teams practice the DRP in real life to make sure that it is sufficient for IT disaster recovery.

Parallel test: In a parallel test, failover recovery systems are tested to make sure that, in case of disaster, they can perform real business transactions supporting key processes and applications. Meanwhile, primary systems continue to run the full production workload.

Cutover test: A cutover test goes further to test failover recovery systems built to take over the full production workload in case of disaster. Primary systems are disconnected during the test.

Restoring IT Functionality

Should a disaster actually occur and Milestone need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which Milestone's information system will be recovered for Live Production Infrastructure for CMS Product.

Milestone Facilities:

1. Azure Cloud:
   a) Milestone's website hosting infrastructure and applications reside in Center US Region on Azure Public Cloud Platform.
   b) Primary Site Architecture for CMS Product:

c) CMS DR Architecture:

Live Production DR Architecture – Azure Cloud
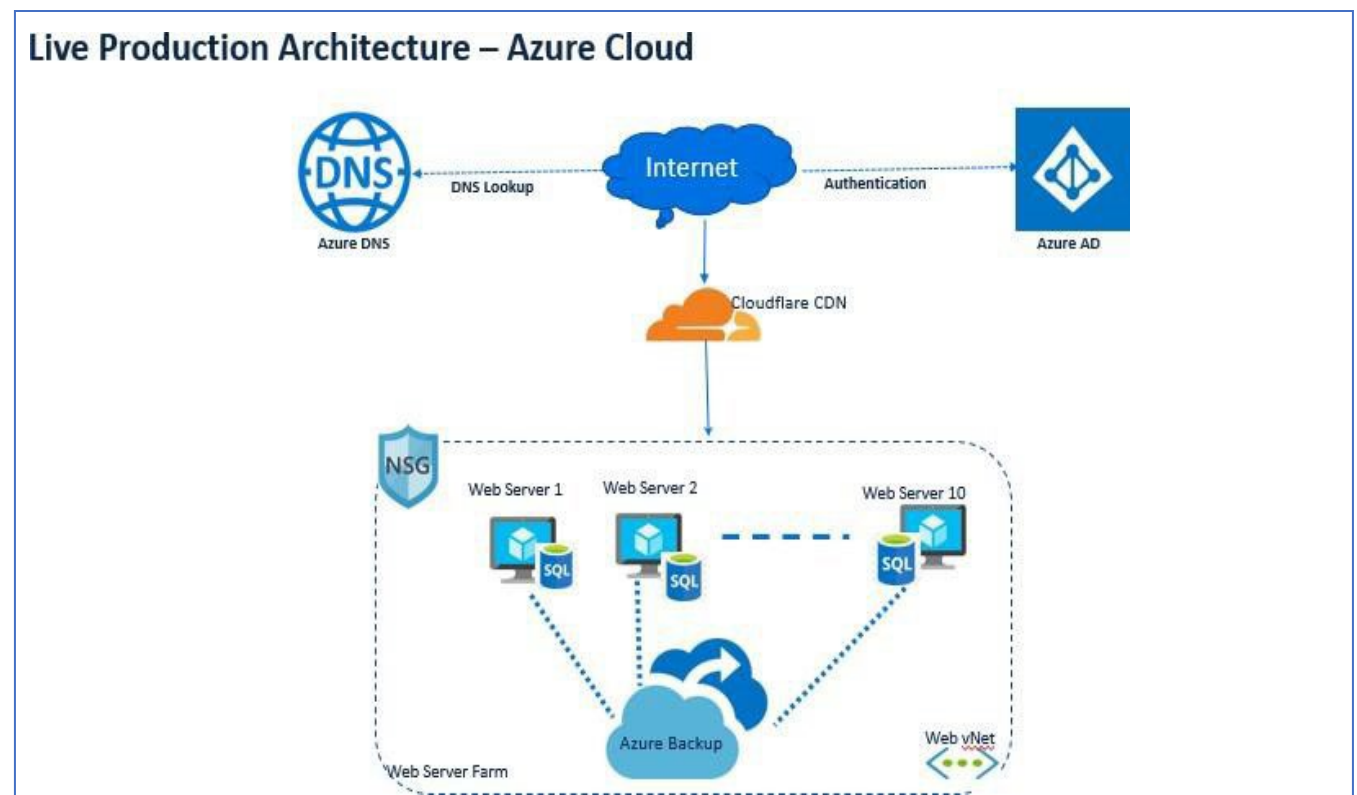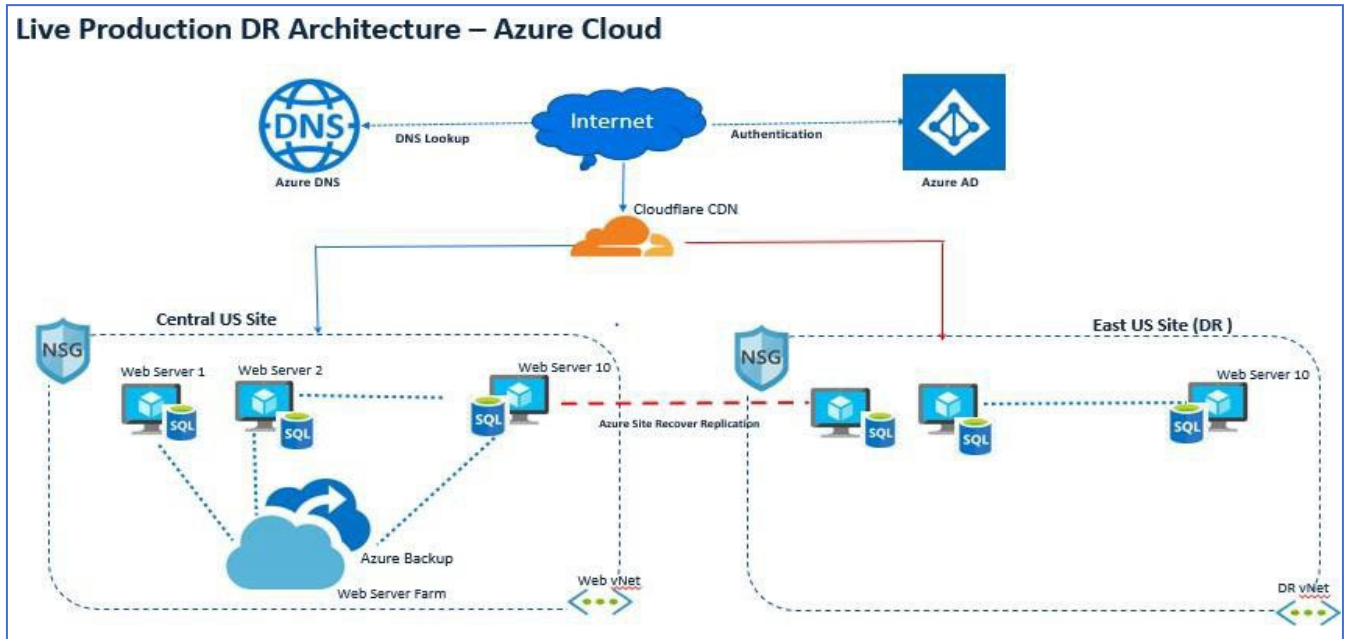
Detailed Report of Disaster Recovery Test

- Milestone has used **Parallel DR Test Technique**. The primary site was up and running and was continuing to be available to serve the service to live production customers. Milestone has performed a DR failover test by manually routing specific user traffic to confirm it should perform real business transaction processes and applications in case of an actual disaster.

- Used Azure Site Recovery to replicate the data from primary Azure region (Central US zone) to secondary Azure region (East US zone).
  - RPO: 10 to 15 Minutes
  - RTO: 30 to 45 Minutes
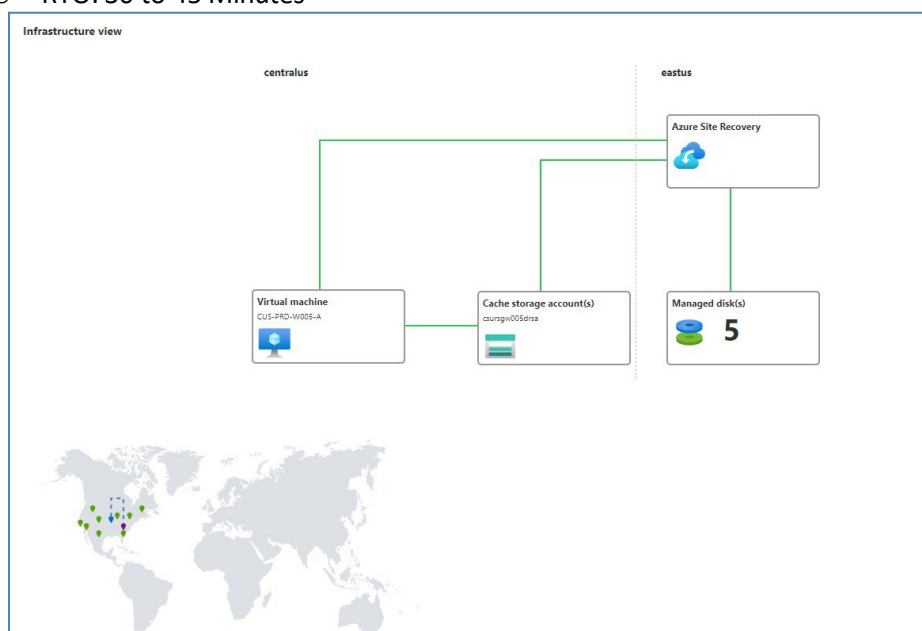
- Run Azure Site Recovery test failover (disaster recovery drill)

- Results from Run Azure Site Recovery test failover

- Verify Customer Website from DR Site.