# Domain Controller Replication and DNS Failover Implementation

## 1. Objective

To extend the on-premises Active Directory (AD) environment to the cloud by deploying a replica (child) Domain Controller (DC) in Microsoft Azure. Additionally, to configure DNS replication between both DCs and automate DNS failover using a PowerShell-based failover script for disaster recovery (DR) purposes.

## 2. Architecture Overview

This setup includes an on-premises primary Domain Controller and a replica in Azure. The DNS failover script monitors the availability of the on-prem DC and performs automatic DNS redirection during failures.

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Location | Role | Description |
| DC1 | On-premises | Primary Domain Controller | Hosts the root domain and DNS zones |
| DC2 | Azure Cloud | Replica Domain Controller | Joined to the same forest and replicates AD/DNS data |
| Failover Script | Azure Cloud DC | DR Automation | Monitors reachability of DC1 and performs DNS failover actions |

## 3. Prerequisites

- Functional on-prem Domain Controller (corp.local)  
- Site-to-Site VPN or ExpressRoute for secure AD replication  
- Azure subscription with VM and networking permissions  
- Administrative credentials for on-prem DC

## 4. Cloud Domain Controller (Replica) Setup Steps

### Step 1: Create Azure Virtual Machine

1. Create a Windows Server 2022 VM in Azure.  
2. Assign a static private IP address.  
3. Set the DNS server to the on-prem DC’s IP address.

### Step 2: Initial Configuration on Cloud VM

1. Log in to the VM.  
2. Disable Windows Firewall temporarily.  
3. Set timezone same as on-prem.  
4. Verify DNS points to on-prem DC IP.  
5. Join domain using on-prem DC credentials.  
6. Reboot VM after successful domain join.

### Step 3: Promote to Domain Controller

1. Open Server Manager → Add Roles and Features.  
2. Install AD DS and DNS roles.  
3. Promote the server to a domain controller in existing forest.  
4. Enter domain name and credentials, select replication source, and set DSRM password.  
5. Proceed with installation and reboot.

## 5. DNS Replication Validation

Create A records on both DCs and verify replication. Ensure records like host1, na2 replicate across both controllers.

## 6. DNS Failover Automation (Disaster Recovery Script)

A PowerShell script monitors the reachability of the on-prem DC. If unreachable, it backs up all A records, deletes them, and creates CNAMEs pointing to DR records. When the DC is back online, the script restores the original records.

Sample Backup File Format:  
ZoneName,RecordName,RecordType,IPAddress  
yash.local,host1,A,10.10.1.10  
hamed.local,na2,A,10.10.1.20

## 7. Validation Steps

1. Simulate DC1 failure.  
2. Run failover script from DC2.  
3. Verify CNAME creation and redirection.  
4. Restore DC1 and validate record restoration.

## 8. Post-Setup Checks

- Run repadmin /syncall /AeD to confirm replication.  
- Validate DNS zone replication with dnscmd /enumzones.  
- Verify both DCs under Active Directory Sites and Services.

## 9. Security & Maintenance Notes

- Re-enable firewall after replication.  
- Schedule health checks and DNS backups.  
- Automate failover monitoring.  
- Monitor AD and DNS logs regularly.

## 10. Outcome

✔ On-prem and Azure-based Domain Controllers are synchronized.  
✔ DNS zones replicate bidirectionally.  
✔ Automated failover ensures name resolution continuity.  
✔ Environment is DR-ready with minimal manual intervention.