Active Directory Infrastructure Design Document

Written By
Sainath KEV
Microsoft MVP – Directory Services
Microsoft Author – TechNet Magazine, Microsoft Operations Framework
Microsoft Speaker - Singapore

![Document Information Table](image)

<table>
<thead>
<tr>
<th>Document Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document Version</strong></td>
</tr>
<tr>
<td>Active Directory Design Change For Flexi Corp</td>
</tr>
<tr>
<td><strong>Created by</strong></td>
</tr>
<tr>
<td>Wednesday, 11 May, 2011</td>
</tr>
<tr>
<td><strong>Creation Date</strong></td>
</tr>
<tr>
<td>Sainath Kev</td>
</tr>
<tr>
<td><strong>Reviewed by</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
</tr>
</tbody>
</table>

![Management Review Table](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Approved Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1 Introduction

SS Technologies identifies the required information to perform the Active Directory Infrastructure change for Flexi Corp.

SS Technologies provides Enterprise Consulting Services to Mid-size – Enterprise level customers with diverse infrastructures including Health, Pharmaceuticals, Shipping, Mining and Software Industries. SS Technologies also provides Outsourced and Managed Services which assists customers in managing Data-Centers, Cloud based infrastructure along with different Application Tiers. SS Technologies provides world class solutions for proactive monitoring of the Servers, Applications, Databases and Security Appliances.

This infrastructure design change offering helps Flexi Corp to restructure the Read Only Domain Controller server and lock down the server as per the request. This offering also provides the methods to monitor the RODC server.
SS Technologies has successfully implemented the similar projects in the past, we are confident to deliver Flexi Corp objective of restructuring the Active Directory. SS Technologies looks forward to work closely with Flexi Corp for designing a cost effective solution for this infrastructure change.

For further communication please do call at the below number or email us at the below mentioned address.

< Director’s Name>
<Title>
<Hand Phone number>
<Email address>
1.0 Understanding Flexi Corp Requirements

SS Technologies understands that Flexi Corp currently has 2 sites configured with single Active Directory forest with Root Domain in Primary Site and Additional Domain in Disaster Recovery Site.

As part of the requirement, Flexi Corp has the requirement to setup a Domain Controller at their Disaster Recovery site and test the failover process.

SS Technologies would be providing the following services:

1. Planning and Design of Disaster Recovery site
2. Install and configure Active Directory Additional Domain Controller
3. Configure the users to authenticate against Additional Domain Controller
4. Rolling back the users to authenticate against Primary Domain Controller.

All servers, network devices and circuits will be owned by Flexi Corp and managed by Flexi Corp. We will provide Consulting service to design and setup the infrastructure based on Flexi Corp production environment in Malaysia. The design includes healthy Active Directory replication between Primary and Disaster Recovery sites.

2.0 Solutions Overview

SS Technologies provides Active Directory design solution for configuring Additional Domain Controller at the Disaster Recovery site. The solution implements, configures and test the availability of the services during the shutdown of the primary site. SS Technologies involves best pool of talent to implement the changes.

3.0 Solutions Diagram

The solution diagram below defines the proposed disaster recovery site which will be used to implement Additional Domain Controller.
4.0 Scope Of Work

SS Technologies provides the following services to Flexi Corp IT Infrastructure.

4.1.1 Server Management

a) Operating System Installation:
SS Technologies will install and configure Operating System on Flexi Corp server hardware and perform the OS Patch installation on the server.

b) Network Configuration:
SS Technologies will configure the IP-Address and relevant subnet on the Windows Server 2008 based on the information provided by Flexi Corp and set the NIC speed accordingly.

c) Active Directory Installation:
SS Technologies will install and configure the Active Directory service on the Windows Server 2008 R2 server and configure the DNS server according to the domain name space. Also configure the replication across the Primary Domain Controller and Additional Domain Controller.

d) AntiVirus Installation:
SS Technologies will install and configure Antivirus on the windows server 2008 R2 Additional domain controller and configure the definition files accordingly.

e) Firewall configuration:
SS Technologies will configure the relevant firewall ports on the Additional domain controller and ensure all the relevant ports are opened for the communication.

4.1.2 Testing
After configuration of the Additional Domain Controller on Data Center 2, SS Technologies will monitor the server for a week as per the SLA and will fix all the problems related to the server and Active Directory.

4.1.3 Assumptions
- Flexi Corp to provide the Network infrastructure including the Routers, Switches and Gateways.
- Flexi Corp to configure the Routers, Switches and Gateways
- Flexi Corp to provide the Hardware to configure Windows Server 2008 R2 server
- Flexi Corp to provide the license for the server
- Any issues pertaining to Network / Infrastructure will be resolved by Flexi Corp.
- Third party products are managed and supported by Flexi Corp.

5.0 Design Phase

5.0.1 Server Installation and Configuration
Following are the checklist for installation of the Operating System at Flexi Corp Data Center 2 site location:

- Make sure the DVD / CD Rom is working
- Make sure Vendor provide the license key of the Windows Server 2008 R2 OS
- Make sure Internet Access is available
- Verify that server can be reachable to Data Center 1 / Primary Domain Controller
- Make sure to configure Static IP address on the domain controller.
Once the Operating System is installed following are the below steps needs to be performed.

- Make sure to activate the Windows Server 2008 R2 license
- Install and upgrade server with all the latest patches.
- Configure the server with Primary DNS server pointing at Primary DC and Secondary to itself
- Make sure the IPconfig / all is appropriate as per the data provided by Flexi Corp
- Make sure the server is able to ping to Primary domain controller

### 5.0.2 Active Directory Installation and Configuration

Following are the procedure for installing and configuring Active Directory on Flexi Corp Data Center 2 location

1. Open Server Manager. Click Start, point to Administrative Tools, and then click Server Manager.

2. In Roles Summary, click Add Roles.

3. If necessary, review the information on the Before You Begin page, and then click Next.

4. On the Select Server Roles page, click the Active Directory Domain Services check box, and then click Next.

5. If necessary, review the information on the Active Directory Domain Services page, and then click Next.

6. On the Confirm Installation Selections page, click Install.

7. On the Installation Results page, click Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

8. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.

   If you want to install from media, identify the source domain controller for AD DS replication, or specify the Password Replication Policy (PRP) for an RODC as part of the installation of the additional domain controller, select Use advanced mode installation.

9. On the Operating System Compatibility page, review the warning about the default security settings for Windows Server 2008 and Windows Server 2008 R2 domain controllers, and then click Next.
10. On the Choose a Deployment Configuration page, click Existing forest, click Add a domain controller to an existing domain, and then click Next.

11. On the Network Credentials page, type the name of any existing domain in the forest where you plan to install the additional domain controller. Under Specify the account credentials to use to perform the installation, click My current logged on credentials or click Alternate credentials, and then click Set. In the Windows Security dialog box, provide the user name and password for an account that can install the additional domain controller. To install an additional domain controller, you must be a member of the Enterprise Admins group or the Domain Admins group. When you are finished providing credentials, click Next.

12. On the Select a Domain page, select the domain of the new domain controller, and then click Next.

13. On the Select a Site page, select a site from the list or select the option to install the domain controller in the site that corresponds to its IP address, and then click Next.

14. On the Additional Domain Controller Options page, make the following selections, and then click Next:

- **DNS server**: This option is selected by default so that your domain controller can function as a Domain Name System (DNS) server. If you do not want the domain controller to be a DNS server, clear this option.

  If the DNS server role is not installed on the Primary Domain Controller (PDC) emulator in the forest root domain, then the option to install DNS server on an additional domain controller is not available. As a workaround in this situation, you can install the DNS server role before or after the AD DS installation.

- **Global Catalog**: This option is selected by default. It adds the global catalog, read-only directory partitions to the domain controller, and it enables global catalog search functionality.

- **Read-only domain controller**: This option is not selected by default. It makes the additional domain controller read only; that is, it makes the domain controller an RODC.

If you do not have static IPv4 and IPv6 addresses assigned to your network adapters, a warning message might appear advising you to set static addresses for both of
these protocols before you can continue. If you have assigned a static IPv4 address to your network adapter and your organization does not use IPv6, you can ignore this message and click, Yes, the computer will use a dynamically assigned IP address (not recommended).

15. On the Location for Database, Log Files, and SYSVOL page, type or browse to the volume and folder locations for the database file, the directory service log files, and the system volume (SYSVOL) files, and then click Next.

Windows Server Backup backs up the directory service by volume. For backup and recovery efficiency, store these files on separate volumes that do not contain applications or other nondirectory files.

16. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password, and then click Next. This password must be used to start AD DS in Directory Service Restore Mode (DSRM) for tasks that must be performed offline.

17. On the Summary page, review your selections. Click Back to change any selections, if necessary.

To save the settings that you have selected to an answer file that you can use to automate subsequent AD DS operations, click Export settings. Type the name for your answer file, and then click Save.

When you are sure that your selections are accurate, click Next to install AD DS.


19. You can either select the Reboot on completion check box to have the server restart automatically or you can restart the server to complete the AD DS installation when you are prompted to do so.

5.0.3 Client Side Configuration And Settings:
For the Disaster Recovery to work, following are the mandatory settings we need to perform on the Client operating systems as well on Server operating systems.

- On every client operating system (both Windows XP and Windows 7), configure the Primary DNS server as Primary Domain Controller IP address and configure the
Secondary DNS server IP address pointing to Disaster Recovery Additional Domain Controller.

- Perform the same on all the servers which are requiring Active Directory authentication.
- Test the connectivity by pinging both the primary domain controller and secondary domain controller (If ping is disabled, you can try access the servers default shares (sysvol))

5.0.4 Server Side Check List
Following are the check list need to perform on the Windows Server 2008 R2 servers.

- Make sure both the servers are replicating, run the require utilities like replmon, repadmin, dcdiag to troubleshoot and debug the problems
- Make sure you use PortQry utility to check the relevant ports to be opened on both the servers for replication to work

The above document combines the Solution Architecting and Design document which will help Customers / Engineers / Architects to use this proposal and Design document for similar requirement. In my next posts I will add more details related to service management and bring different architecture flavor.