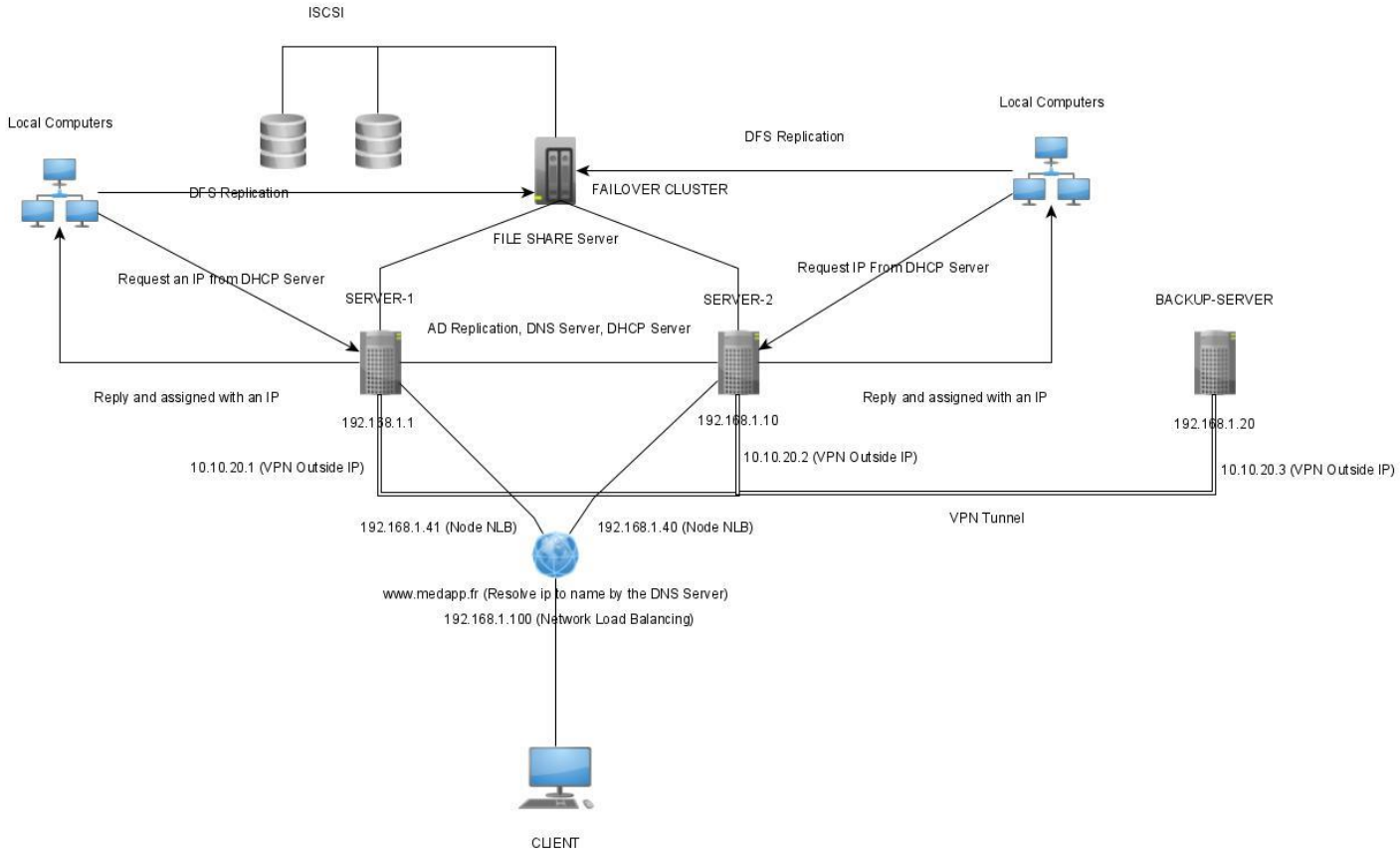
2PROJ NETWORK ADMINISTRATION AND ARCHITECTURE



I. Diagram Overview

According to the diagram we will have 4 main machines to do the demonstration. 3 Windows Server and 1 Window 10. SERVER-1 and SERVER-2 will be the main server that will located in France and BACKUP-SERVER will be the backup server that will be located outside France. CLIENT on the other hand will be used to access the website by acting as a normal user or a doctor. Local Computers are computers for employees who works at the company, but we will not need to create another machine to test that because our main focus will be the server and the client. Even though, we won't have a machine for the local computers but in terms of architecture, services, securities and how a real company function will be implemented and presented. SERVER-1 and SERVER-2 will be a replication of each other meaning every configuration on one server will be replicated on the other one. Both servers will also act as a DNS Server and DHCP Server providing the services to both the clients and local computers. Information being shared or sent between the server or in the company will go through a secure tunnel called VPN. 2 nodes were created on one for each of the 2 servers in order to configure the Network Load Balancing so Client will benefit the services from the servers even one of the servers is down or crash. Backup server will only use to backup and recover the server configuration if somehow both server in France is destroyed for example. File Server are for file sharing and storage for the 2 servers, and we will also implement a failover cluster just in case there's a disk failure. File sharing will be configured for a real live network and company works.

II. DNS Server

DNS also known as (DOMAIN NAME SYSTEM) is hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. Its main purpose here is to assign domain names and mapping those names to the respective domain, in order words it resolve the domain names from the IP address so user can access the website with a user-friendly URL. For example, here the DNS Server translate the 192.168.1.100 which is the website IP address to www.medapp.fr a readable user-friendly URL. More advanced purpose we used it for machines to communications in a local environment.

III. DHCP Server

In order to make a real live company network local computers will be assigned IP addresses by the DHCP Server in order to identify each device and access the internet in the network. How it works? Local computers will request an IP address from the DHCP Server and DHCP Server will reply with and IP address (which is in a range that was configured) with a duration of lease before it will be renewed.

IV. Active Directory Domain Services

According to Wikipedia, A server running the Active Directory Domain Service (AD DS) role is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network. Assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. In our case SERVER-1 and SERVER-2 is a replication of each other meaning everything we do on server 1 will be replicate to server 2 or the other way around. It will use to manage users, computers, groups and generate trust with company partners if needed. We will also configure site links and set bandwidth limitation.

V. IIS (Internet Information Server)

IIS is used as a web server for our website which the client will access through the internet. This is how the client will see the web interface of our website.

VI. Network Load Balancing

NLB aka Network Load Balancing is the ability to balance traffic across two or more servers. 2 nodes were set up. One on each server, 2 dedicated network adapters were configured. 192.168.1.100 is the IP address of the Network Load Balancer. If one server is down, client will still be able to benefits the services on the server because it will redirect to the other server. Network Load Balancing is an important part for high availability so we can ensure that the client will always benefit services from the server. For example, if server one is down, users will always be able to access the website because of the other server is still up so, user will automatically redirect to the other server.

VII. PHP and MySQL

Since our website will code in PHP and the database will be use as MySQL, IIS must support PHP and have MySQL Server on the servers, so PHP and MySQL were also configured on the servers.

VIII. HTTP To HTTPS

In order to secure our website, we converted HTTP URL to HTTPS by using a self-signed certificate since we're only doing it locally. HTTPS doesn't mean it completely secure the whole website it's more like

adding a protection layer to the website, in simple words its like locking your door with a lock instead of having nothing.

IX. VPN

Transmitting information, sending files, or communicating through a network in a company are important when it comes to security. VPN aka Virtual Private Network is a secure connection which all companies need in their security plans. VPN allows employees in the company to send data or communicate with each other in a secure way by creating a tunnel which is encrypted so no man in the middle can access or see the activities. IKEV2 is our choice of VPN since it's the most recent technologies and have minutes failover connections, it's one of the most secure types of VPN since it has shared keys that needs to match for the VPN to be able to connect. We configured VPN between the 3 sites also known as Site-To-Site VPN. Each servers have an inside IP and outside IP, so people won't be able to trace the real inside IP.

X. DFS Replication

Imagine there's a fire in one of the sites, employee's data on that site will be lost. So, a good backup plan is to create DFS Replication which replicated employee's data to the domain and can be access even though one of the sites is destroyed. DFS aka Distributed File System allow an organization using Microsoft Windows servers to organize many distributed SMB file shares into a distributed file system. Local

computers files and folders will be replicated to the domain so users can access the files and folders on network instead of local. DFS has two components to its service: Location transparency (via the namespace component) and Redundancy (via the file replication component). Together, these components improve data availability in the case of failure or heavy load by allowing shares in multiple different locations to be logically grouped under one folder, the "DFS root", according to Wikipedia.

XI. ISCSI

Conforming to Wikipedia, ISCSI is an acronym for Internet Small Computer Systems Interface, an Internet Protocol (IP)-based storage networking standard for linking data storage facilities. It provides block-level access to storage devices by carrying SCSI commands over a TCP/IP network. Easier words would be it's a shared storage used in local environment for local computers to access data on the shared storage we will also use it for failover cluster which is very important for high availability. ISCSI was created by using 2 disks.

XII. Failover Cluster

To ensure the high availability, we configured the servers to be able to withstand a failure in storage. Failover cluster is crucial when it comes to high availability and redundancy. Without clustering, if a server running a particular application crashes, the application will be

unavailable until the crashed server is fixed. Failover Cluster remedies this situation by detecting hardware/software faults, and immediately restarting the application on another system without requiring administrative intervention. In order to set this up we created ISCSI Target with 2 more nodes. If one server is down everything to the other server so, all services, data and important features will still be accessible.

XIII. GPO

Group Policy Management centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. We use GPO in order to manage users and computers in the company. It’s important for company security and ensure everyone has the right rules and restrictions.

XIV. Backup Server

In case the 2 servers in France are destroyed, a third dedicated server outside France will do a daily backup of everything including databases, configurations, and data which we can use to recover once the 2 servers are back online. It backs up everything everyday at 2AM.

XV. Database Roles

For the management for security, we've created different roles for each different user. Those roles include:

- - accessadmin : this user grant access to the database but doesn't allow management of any database level security
- - datareader : this user is only allow to read data that are stored in a database
- - datawriter : this user can only create new records and edit existing record
- - securityadmin : allow to manage roles and permissions of other database users

  These are the 4 roles that we've gone for but on top of that there'll be a backup operator whose job is to perform backup daily but doesn't allow to restore the database and also each user will have their own account and password must be change daily just in case someone has other user password.