Data Sharing between Clients and a Server using a Secure Connection

Padma Raju G M
MSc in Information Systems with Computing
Dublin Business School

CONTENTS

LIST OF FIGURES

Data Sharing between Clients and a Server using a Secure Connection

I. Introduction

Data, A group or collection of information that can be stored and manipulated in order to be utilized for further processing, gaining insights into trends developing over time, etc. Data these days are massive in volume and most of the time useful and garbage data are all mixed up and sent from one client to another through vulnerable/exposed channels. The first step in order to tackle these issues is to divide the problem into parts and solve them. The first part, in this case, would be data acquisition, the Second part would be data storage, and the Third part would be data sharing. The standard procedure would be to implement all three of these together on a single server application. But, when dealing with vast amounts of data we need to see to it that none of these three parts ever fail and even if they do so, we should be able to troubleshoot them easily.

So to tackle this issue we need to implement a few technologies to make the data stored in the server to make the transmission and receiving of the data from the server is more secure and there is a connection between the Client machines connected to the domain server. Data sharing is more secure and it is been handled by a few technologies such as Light Directory Access Protocol, Server Message Block, Domain Name System; etc.

A. THE AIM OF THE PRODUCT

The AIM of this project is to the versatility of the Active Directories and its connection with other file securing protocols and the restrictions for the user and letting the user access the amount of data the user is allowed to.

B. THE SCOPE OF THE PRODUCT

The SCOPE in this system, I would be implementing a few of these secure technologies to emit a secure connection between the host server and the machines connected to the host machine under the domain controller and the elasticity of multiple users able to access their files shared to them via secure connections and able to share among the client machines easily and securely.

C. THE APPROACH USED

Using Microsoft Azure, I created one Virtual Server and two Client machines and connected the Client Machines to the Virtual Server.

The server is implemented with LDAP Host so that only the authentic computers and users of that domain can access the files from the server, SMB is implemented for file sharing between the server and the users who are connected to the domain via certificates through DNS System. Active Directory is also implemented on the server to keep the track of all the user certificates and computers and also Active Directory is used to add new users and computers to the domain with certificates securely.SFTP technology is used to connect the client machines to each other so that they can share files between them securely.The users can only log in to only those machines which are connected to the domain and while they try to connect the certificate is authorized with the server for authentication to create a secure connection between the client computer and the server.

DIAGRAM.jpg

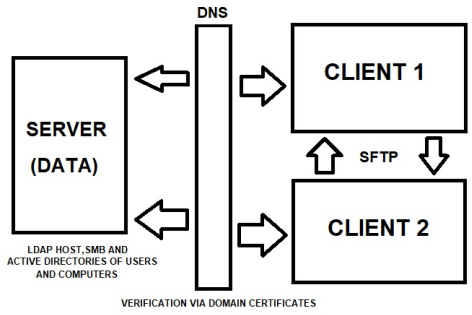


Fig. 1. Block Diagram

II. BACKGROUND

The main focus of this paper is to model a prototype of client server based file sharing system. The earliest design uses a central server to coordinate participating nodes and to maintain an index of all available files being shared. When a peer node joins the system, it contacts the central server and sends a list of the local files that are available for other peers to download (shared files). To locate a file, a peer sends a query to the central server, which performs a database lookup and responds with a list of peers that have the desired file. Broadly the paper can be divided into 3 major modules. Mainly, User authentication, file organization, and sharing and Multi-user request handling. Let us look at each of these modules in discrete and the technical background associated with it.

A. THE SOFTWARE USED AND THE TECHNOLOGIES IMPLEMENTED

- MICROSOFT AZURE: Microsoft Azure is a cloud-based technology provides a variety of cloud services

including analytics, storage , and networking. Microsoft Azure helps the business requirements by providing a low cost and less time to meet the demands.

- LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP): A directory is similar to a database, but tends to contain more descriptive, attribute-based information. The information in a directory is generally read much more often than it is written. Directories are tuned to give quick-response to high-volume lookup or search operations. They may have the ability to replicate information widely in order to increase availability and reliability, while reducing response time. When directory information is replicated, temporary inconsistencies between the replicas may be OK, as long as they get in sync eventually. LDAP runs over TCP/IP or other connection oriented transfer services.

- SIMPLE MESSAGE BLOCK (SMB): It's a file-sharing protocol that was invented by IBM and has been around since the mid-eighties. Since it's a protocol (an agreed-upon way of communicating between systems) and not a particular software application, if you're troubleshooting, you're looking for the application that is said to implement the SMB protocol. The SMB protocol was designed to allow computers to read and write files to a remote host over a local area network (LAN). The directories on the remote hosts made available via SMB are called "shares."

- ACTIVE DIRECTORY DOMAIN SERVICES (ADDS):A server running Active Directory Domain Service (AD DS) 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.[4] Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services

- DOMAIN NAME SYSTEM (DNS) : It is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

B. THE BENEFITS OF THE PRODUCT

The main intention behind this project is to create a conceptual working prototype of a server to which the client machines can communicate using a secure connection and share files from the server and also restricting the file permission if the files are shared between the clients themselves.

C. TYPICAL USERS OF THE PRODUCT

The typical users for this product scenario would be an advertising agency or any agencies working in the creative scenario as there would be a lot of files that need to be shared between the artists' and also files that need to be taken from the server for the other departments. Also, the artists' can share their idea of artwork and then share it with each other via a secure connection and work on the project together and once it is completed they can store it on the server so that the other departments can process the project accordingly.

III. TECHNICAL DESCRIPTION OF THE PROOF OF CONCEPT

During my initial days of the research about the product implementation I always wanted to implement LDAP in a way in which it works smoothly between the client machines and also it helps in the connection of binding all the machines associated to the domain and keep them connected to the domain and the server,but LDAP also sometimes takes in extreme measures where even the smallest changes in the Domain or the Server can make the connection to be terminated between the machines and the Server. So I have tried to connect LDAP with Active Directory as Active Directory is also a secure connection but there are instances where there are numerous loopholes that could be found. So I've tried to implement the LDAP Connection between the computers and the server using LDAP certificates associated with the users and computers. To check the certificates are associated with the Server or not I've used a DNS SYSTEM to check the connection and get the connection to be authenticated with the domain server.Also we can use Active Directory to grant new user and computer access and also we can create the certificates from the server to get the new computer or user to be connected to the server or domain.Ive tried establish a SFTP connection between the client machines so that they can also exchange data or files among them without the data moving from Client1-Server-Client2 but rather the data would move from Client1-Client2 using the help of the certificates which are allocated to the machines while creation of the OU for the computer. Using this we have tried to establish a peer-to-peer connection between the clients so that the data transferred is only happening between them and it is happening securely at the same time.

At first, I created a virtual network group under which the computer an the servers can be accessed. After the network group was created, I created a virtual server and installed Active Directory Domain Services along with Web Services (IIS) and DNS Server using the "Add roles and Features" option, and once these were installed restarted the server so that the configuration can take place. Once restarted, promoted the Active Directory Domain Services as a domain controller by creating a new forest.once the forest was created with a DRSM (Directory Restore System Password)Password we added the clients created to the domain using subnets. and

once the computers are connected we restart the server once as the changes can take place. Once restarted we add the Active Directory Certificate Services and LDAP protocol onto the server.We add the certificate option using the ADSI Edit. Once they are installed, we configure them by adding the IP of the server as the main Server IP so it can be accessed by the clients connected to it. Once the clients are connected under the domain group, We have a connection with LDAP certificates within the computers and they are all connected to the server. We create a couple of users and also add them to the Users group and also to the Remote Desktop Users and Remote Login Users, so that the users can log in to any machine connected to the domain and still have access to all their data and their profile. After this, we Install FTP server under Web Services and configured the FTP site user the Firewall Support user the IPV4 user Advanced Settings under Adapter settings and access is given to the admin users or to the users and we would establish a secure connection between the users so that they have a particular home drive where they can share data securely and also edit the edit the data if needed. Here the data connection is secure between the clients and also among the clients and the Server.

A. PROJECT TESTING AND EVALUATION

I have implemented a Windows Server 2019 Data Center so that it can handle the load of all the data set implemented on the server. I have a created two Virtual machines of Win 10 Pro of so it can handle the basic load of a computer the transfer initiated. While testing the concept proposed i found the there are sometimes connection behavioural issues between the clients and sometimes when the load is too much the server tends to crash at a stretch and we have to re-configure the server with the machines.To terminate the Server crash I have tried to implement a temporary Backup server and added it under the Server Group through the server Manager so it can help in balancing the load thrown at the server while many users are connected at the same time and the traffic rate is High.

IV. REFERENCES AND BIBLOGRAPHY

A. VIDEO REFERENCES

https://www.youtube.com/user/MSFTWebCast
https://www.youtube.com/watch?v=J6IJ7JPAuN8&t=600s
https://www.youtube.com/watch?v=JFPa_uY8NhY

APPENDIX A
CODES, SNIPPETS AND SCREENSHOTS

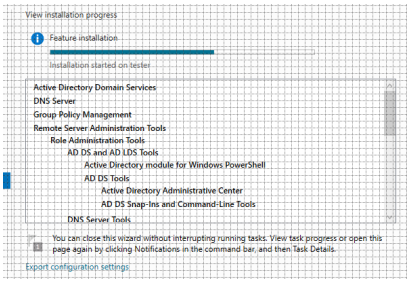


Fig. 2. ADDS INSTALL

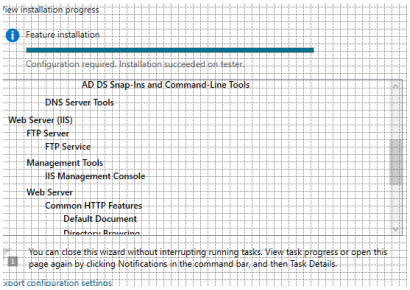


Fig. 3. IIS

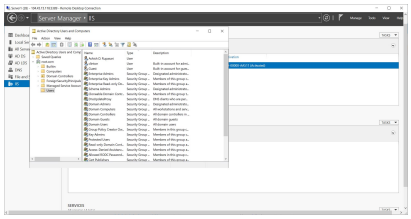
Config.JPG 

Fig. 4. AD-DS Config

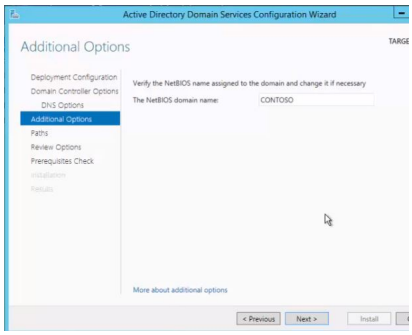
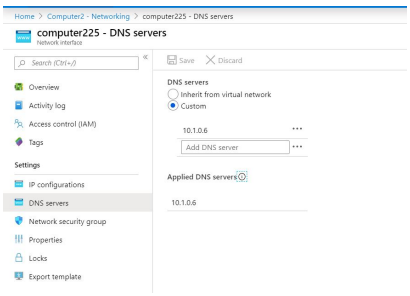
server.JPG 

Fig. 5. DNS



Client config.JPG

Fig. 6. DNS client configuration

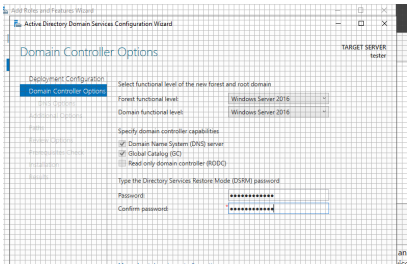
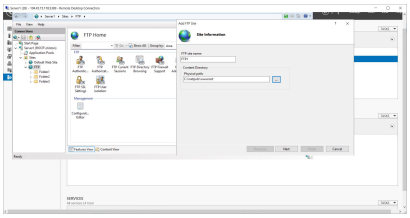
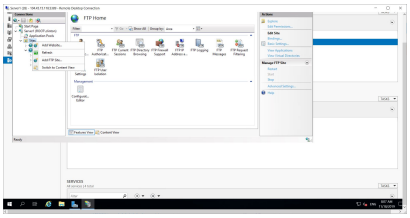


Fig. 7. DRSM



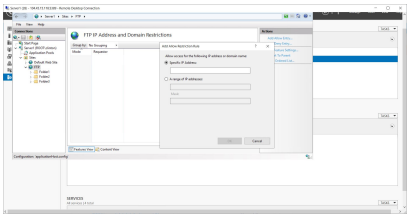
directory.JPG

Fig. 8. FTP Directory



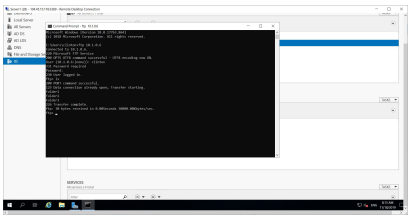
add.JPG

Fig. 9. FTP ADD



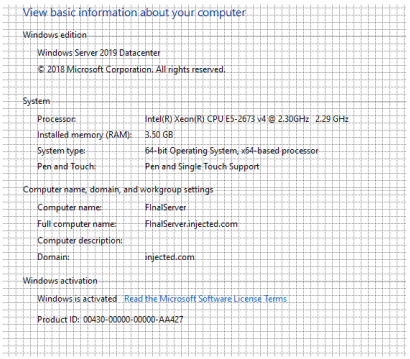
restrict.JPG

Fig. 10. FTP RESTRICT



console.JPG

Fig. 11. FTP CONSOLE



Server.PNG

Fig. 12. Domain Server

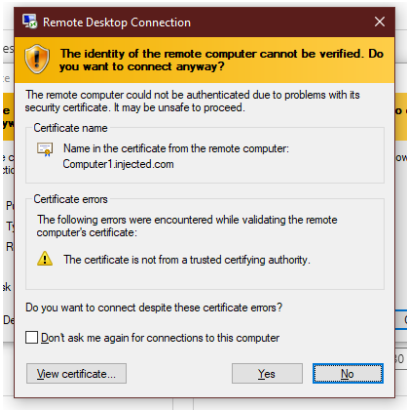
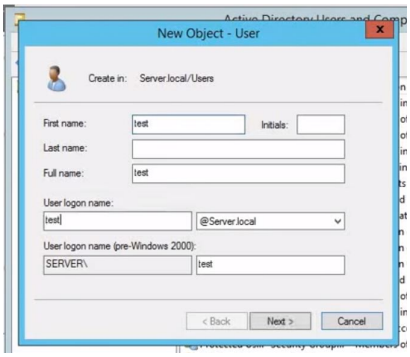
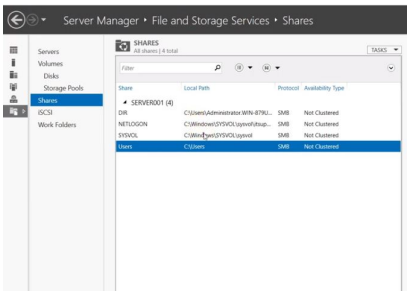


Fig. 13. ComputerCertificate



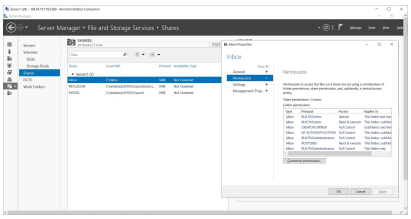
user in AD-DS.JPG

Fig. 14. Creating user in AD-DS



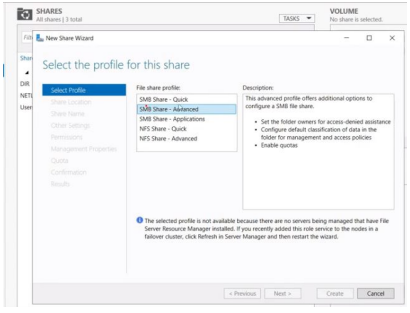
.JPG

Fig. 15. Creating user in AD-DS



with permission.JPG

Fig. 16. Creating user in AD-DS



SMB.JPG

Fig. 17. Creating user in AD-DS