Logo

Description automatically generated

**IT221 T PROJECT 2022 – first semester**

**Group Members**

| Name | ID |
| --- | --- |
| الاء خالد الشعيبي | 442005420 |
| منيرة ابراهيم المبارك | 442002988 |
| ساره مجدي الجهني | 442005104 |
| ساره عبدالعزيز الطويل | 442000786 |
| ندى حمد العتيبي | 442003374 |

PNU

The project is about NFS Application protocol

Section 51S

1. *Introduction*:

The NFS protocol, which stands for Network File System, is a network protocol that allows files stored on a file server the ability to be accessed by any computer on the network.

NFS is a file access protocol, and that means it is expected to function without transferring the file. Hence, it is possible to edit and manipulate the files that are stored on the server as if they were stored locally.

Therefore, it is easier to update a large file following the NFS protocol because it allows multiple clients to use the same files and share applications, which reduces storage costs and reduces security concerns. **[1]**

1. *Protocol operation*:

A Network File System (NFS) enables remote computers to mount file systems across a network

and interact with them as if they were mounted locally. 1-A simple system is used in the

Network File System (NFS), where a "mount command" instructs the server to connect to

multiple clients. 2- The clients will then have access to all files on the server via the appropriate

platform. 3-This design allows many security protocols to function in one location, dictating

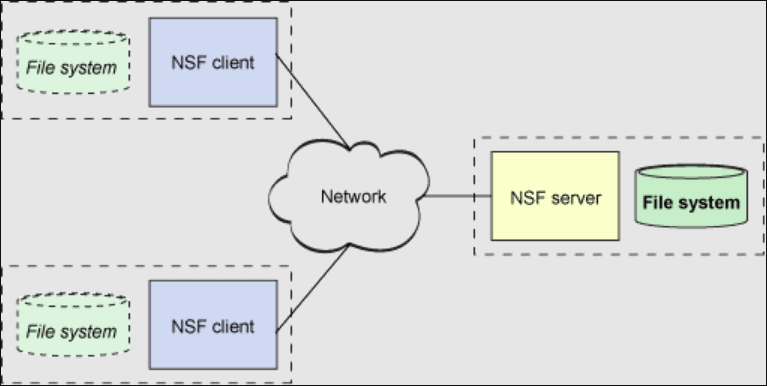
who has access to which files, making it safer to work. 4-A Network File Scheme (NFS) can also

employ a file locking system, allowing several clients to access the same files. 5- The Network

File System (NFS) has the ability to manage many applications. 6-The Network File System

(NFS) uses several hosts that will access the same files. It does not require one application for

its operation, providing a simple design that can be easily handled.



**HOW WORKS THE NFS? AN EXAMINATION OF THE THREE VERSIONS**

Today, three NFS versions are in use. The Network File

System (NFS) operates differently depending on the version you choose. with each having its

own set of rules for how it will run.

**NFSv2 Network File System (NFSv2):**

NFS Version 2, the first version of the NFS protocol, is the most extensively used and supported version. It communicates over an IP network using the User Datagram Protocol (UDP). The IP network enables a reliable network connection. On this configuration, UDP does not technically

establish a connection before it can begin transferring data. The feature is useful since it

allows connections to be established in less time. However, User Datagram Protocol (UDP)

clients can continue to submit requests to a server even if the server is not operational. The

**Network File System, Version 3 (NFSv3):**

The NFS Version 3 protocol, in contrast to the NFS Version 2 protocol, supports asynchronous writes and can handle files larger than 2 Gbytes. When compared to version 2, the architecture produces improved buffering. NFSv3 can also handle faults and manage larger files more efficiently. NFSv3 has a number of enhancements: support for 64-bit file sizes and offsets, allowing files greater than 2 gigabytes to be handled (GB).To increase writing efficiency, the server now supports asynchronous writes.extra file characteristics in several answers to avoid having to re-fetch them When scanning a directory, use a READDIRPLUS operation to acquire file handles and characteristics in addition to file names.

Version 4 of the Network File System (NFS) (NFSv4) :

NFSv4 is the most recent version of the Network File System protocol you can use. It can work on the internet. it is easier to run it in more places. In this NFS format, the Transmission Control Protocol (TCP) is used. TCP connections exist between an application and an IP address. It keeps track of data segments and only needs to receive missing frames in the TCP set when something needs to be sent a second time. This update introduced the following new and improved features: 1-strong authentication, integrity, and privacy support. 2-Advanced file caching support. 3-Better internationalization capability. 4-improved interaction with Microsoft Windows file sharing 5- improved support for integrated locking.**[2]**

**Negotiation between Versions 2 and 3**

The protocol level is negotiated as part of the commencement process since NFS servers may be serving clients who are not running NFS version 3 software. Version 3 is utilized when it can be supported by both the client and the server. Version 2 is chosen if neither the client nor the server can support any other version.

**Negotiation between UDP and TCP**

The transport protocol is also negotiated during initiation. The first connection-oriented transport that is accepted by the client and server is chosen by default. The first connectionless transport protocol that becomes available is utilized if this choice fails.

**Negotiations over file transfer size**

The size of the buffers utilized for sending data between the client and the server is determined by the file transfer size. Larger transfer sizes are preferable in general. Although the NFS version 3 protocol allows for unlimited transfer sizes, as of the Solaris 2.6 release, the software bids a 32 Kbyte default buffer size. If necessary, the customer can provide a reduced transfer size at mount time, however in most cases this bid is not necessary.

With systems that make use of the NFS version 2 protocol, the transfer size is not negotiable. The maximum transfer size is set to 8 Kbytes in this case.**[3]**

1. *Vulnerabilities*:

Like any other unprotected network protocol, NFS is vulnerable to many different types of attacks.

One of them is eavesdropping and imposter attacks: An eavesdropping attack happens when a hacker intercepts, alters or deletes data being transmitted between two devices. Data in transit between machines can be accessed through eavesdropping, also known as sniffing or snooping, which relies on insecure network interactions.

Falsified file handles cannot be distinguished from those created by the mounted daemon by an NFS server. Any file on the server that is not owned by the root can be read and modified by a client who is able to monitor the network and steal a file handle. **[4]**

1. *Alternatives*:

The following alternatives are used to overcome vulnerabilities:

1- The Secure Shell (SSH) protocol is a method for safe remote login from one computer to another. Strong encryption is used to safeguard the security and integrity of communications, and it offers a number of additional alternatives for strong authentication.

It offers a safe substitute for unsafe file transfer protocols, and unprotected login protocols like Telnet and rlogin (such as FTP). **[5]**

2- Accessing remote files and directories is made simple by the Secure Shell Filesystem (SSHFS). Using an SSHFS connection, you may view, access, and edit files and folders on your A2 Hosting account.

SSHFS utilizes SSH (Secure Shell), which encrypts and secures all connections, to connect with the server. **[6]**

3- AFS is a distributed file system that enables client and server hosts to cooperatively share file system resources in an effective manner.

NFS cannot scale as well as the AFS. With great performance on wide-area configuration and security based on Kerberos mutual authentication, it works effectively in small and very large deployments. **[7]**

1. *References*: Use IEEE reference style. (Minimum three references)

**[1]B. Callaghan, *NFS illustrated*. Reading, Mass.: Addison-Wesley,.**

**[2]“What is NFS - Network File System (How it Works),” *Cloud Infrastructure Services*, Mar.12,2022.**[**https://cloudinfrastructureservices.co.uk/what-is-nfs-network-file-system-how-it-works/**](https://cloudinfrastructureservices.co.uk/what-is-nfs-network-file-system-how-it-works/)

**[3]“How the NFS Service Works (System Administration Guide: Resource Management and Network Services),” *docs.oracle.com*. https://docs.oracle.com/cd/E19683-01/806-4076/6jd6amr0j/index.html (accessed Sep. 21, 2022).**

**[4]S. Sheinin, “NFS Security” Global Information Assurance Certification Paper, 2000.**

**[5]Usenix Association, Uniforum (Organization, and Computer Emergency Response Team, *Proceedings of the sixth annual USENIX Security Symposium : focusing on applications of cryptography : July 22-25, 1996, San Jose, California*. Berkeley, Ca: The Association, 1996.**

**[6]“How to use SSHFS (Secure Shell Filesystem),” *www.a2hosting.com*. https://www.a2hosting.com/kb/getting-started-guide/accessing-your-account/using-sshfs-secure-shell-filesystem (accessed Sep. 21, 2022).**

**[7]“Alternate File Sharing Systems,” *ibgwww.colorado.edu*. http://ibgwww.colorado.edu/~lessem/psyc5112/usail/network/nfs/afss.html#:~:text=Alternatives%20to%20NFS%20include%20AFS%2C%20DFS%20and%20RFS (accessed Sep. 21, 2022).**

**‌**

**‌**

**‌**

**‌**

**‌**

**‌**

**‌**