IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Authenticate the Centralized Network Using NIS(Network Information System) in Linux Environment

Upasna Chaudhary[*1], Poonam Kshtriya[2]

[*1,2] Department of Computer Science, Banasthali Vidyapith University, Rajasthan, India.

truptiverlekar@yahoo.com

Abstract

Security is the degree of resistance to, or protection from, harm and illegal accessing the services from networks. NIS server used for high security in LINUX or another environment. NIS, or Network Information Systems, is a network service that allows authentication and login information to be stored on a centrally located server. This includes the username and password database for login authentication, database of user groups, and the locations of home directories [1]. We use NIS services in centralized Network between client and server. For accessing the NIS server services in centralized Network we have to configure the client and server configuration files at the client end and server end. We will use the LINUX operating system.

Keywords: Centralized Network, NIS server, Linux operating system.

Introduction

The Network Information System (NIS) is a safe environment for sharing data among large number of network (Internet or intranet) users. Also, this environment provides a secure and controlled access to the shared data[2]. The Network information Service (NIS) provides a robust and reliable naming service that holds information on network users, groups, host machines, servers, and generally all information necessary to operate a network. We use these services in Centralized network.

Limitations

The original NIS design was seen to have inherent limitations, especially in the areas of scalability and security, so other technologies have come to replace it.NIS used to have a major security flaw:

It left your password file readable by virtually anyone in the entire Internet, which made for quite a number of possible intruders. As long as an intruder knew your NIS domain name and the address of your server, he could simply send it a request for the password . Byname map and instantly receive all your system's encrypted passwords. With a fast password-cracking program like crack and a good dictionary, guessing at least a few of your users' passwords is rarely a problem. This is what the secure nets option is all about. It simply restricts access to your NIS server to certain hosts, based on their IP addresses or network numbers. The latest version of ypserv implements this feature in two ways. The first relies on a special configuration file called /etc/ypserv. Securenets and the second conveniently uses the /etc/hosts.allowand /etc/hosts.deny files. Thus, to restrict access to hosts from within the Brewery, their network manager would add the following line to hosts.allow:So other technologies have come to replace it.

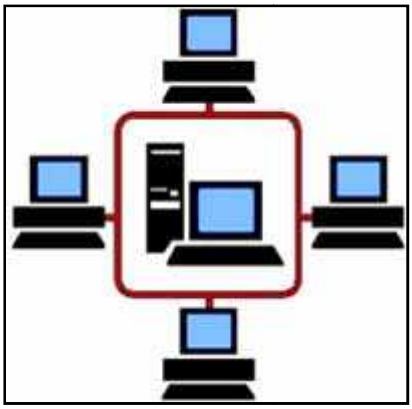


Fig. Centralized Network

Uses of the NIS Server

1. NIS allows a central server to manage password authentication, host, services, etc which would normally be provided by the local files.
2. A NIS/YP system maintains and distributes a central directory of user and group information, hostnames, e-mail aliases and other text-based tables of information in a computer network.

3. NIS adds another "global" user list which is used for identifying users on any client of the NIS domain.
4. NIS server is set up in a single system and configured to hold user accounts and their passwords and access information. Then any user on that network can login to his/her account that is set up in the NIS server from any system (with nis client running) on that configured network. This gives a look and feel that the user is logged into his/her own system. But actually its the account on the NIS server that is mounted on the local sytem on user login .

Installation

At the LINUX environment, we have to install the client and server packages. For installing the client and server package we have to used some commands which are given below:

- **Client Installation**

ypbind:-

ypbind finds the server for NIS domains and maintains the NIS binding information. The client (normaly the NIS routines in the standard C library) could get the information over RPC from ypbind or read the binding files. The binding files resides in the directory **/var/yp/binding** and are conventionally named **[domainname]. [version]**. The supported versions are 1 and 2. There could be several such files since it is possible for an NIS client to be bound to more then one domain.

- **Server Installation**

1)ypserv:-

The ypserv daemon is typically activated at system startup. ypserv runs only on NIS server machines with a complete NIS database.

2)rpcbind:-

The rpcbind utility is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine. When an RPC service is started, it tells rpcbind the address at which it is listening, and the RPC program numbers it is prepared to serve. When a client wishes to make an RPC call to a given program number, it first contacts rpcbind on the server machine to determine the address where RPC requests should be sent. The rpcbind utility should be started before any other RPC service. Normally, standard RPC servers are started by port monitors, so rpcbind must be started before port monitors are invoked. When rpcbind is started, it checks that certain name-to-address translation-calls function correctly. If they fail, the network configuration databases may be corrupt. Since RPC services cannot function correctly in this situation, rpcbind reports the condition and terminates.

Configuration

In centralized network, we configure the client and server by using several files in LINUX which are given below:

Client Configuration

After installation we have to configure many files which are given below:

a)/etc/sys.config/network:-

The **/etc/sysconfig/network** file is used to specify information about the desired network configuration. The following values may be used:
NETWORKING=<*value*>, where **<*value*>** is one of the following boolean values:
yes — Networking should be configured.
no — Networking should not be configured.
HOSTNAME=<*value*>, where **<*value*>** should be the *Fully Qualified Domain Name* (*FQDN*), such as**hostname.expample.com**, but can be whatever hostname is necessary.
GATEWAY=<*value*>, where **<*value*>** is the IP address of the network's gateway.
GATEWAYDEV=<*value*>, where **<*value*>** is the gateway device, such as **eth0**. Configure this option if you have multiple interfaces on the same subnet, and require one of those interfaces to be the preferred route to the default gateway.
NISDOMAIN=*sits*,where **<*value*>** is the NIS domain name.
NOZEROCONF=<*value*>, where setting **<*value*>** to **true** disables the zeroconf route.

b)/etc/sysconfig/authconfig:

-The **/etc/sysconfig/authconfig** file sets the authorization to be used on the host. It contains one or more of the following lines:
USEMD5=<*value*>, where **<*value*>** is one of the following:
yes —MD5 is used for authentication.
no —MD5 is not used for authentication.
USEKERBEROS=<*value*>, where **<*value*>** is one of the following:
yes —Kerberos is used for authentication.
no —Kerberos is not used for authentication.
USELDAPAUTH=<*value*>, where **<*value*>** is one of the following:
yes—LDAP is used for authentication.
no—LDAP is not used for authentication.

c)/etc/yp.conf:-

ypbind finds the server for NIS domains and maintains the NIS binding information. The client (normaly the NIS routines in the standard C

library) could get the information over RPC from ypbind or read the binding files. The binding files resides in the directory /var/yp/bind-ing and are conventionally named [domainname].[version]. The supported versions are 1 and 2. There could be several such files since it is possible for an NIS client to be bound to more then one domain. After a binding has been established, ypbind will send YPPROC_DOMAIN requests to the current NIS server at 20 seconds intervals. If it doesn't get an response or the NIS server reports that he doesn't have this domain any longer, ypbind will search for a new NIS server. All 15 minutes ypbind will check to see if the current NIS server is the fastest. If it find a server which answers faster, it will switch to this server. You could tell ypbind to use network broadcasts to find a new server, what is insecure, or you could give it a list of known secure servers. In this case ypbind will send a ping to all servers and binds to first one which answers. Unless the option -debug is used, ypbind detaches itself from the controlling terminal and puts itself into background. ypbind uses syslog(3) for logging errors and warnings. At startup or when receiving signal SIGHUP, ypbind parses the file /etc/yp.conf and tries to use the entries for its initial binding. Valid entries are domain nisdomain server hostname. Use server hostname for the domain nisdomain. You could have more than one entry of this type for a single domain. domain nisdomain broadcast Use broadcast on the local net for domain nisdomain. ypserver hostname Use server server for the local domain. A broadcast entry in the configuration file will overwrite a ypserver/server entry and a ypserver/server entry broadcast. If all given server are down, ypbind will not switch to use broadcast. Ypbind will try at first /etc/hosts and then DNS for resolving the hosts names from /etc/yp.conf. If ypbind couldn't reconfigure the search order, it will use only DNS. If DNS isn't available, you could only use IP-addresses in /etc/hosts. ypbind could only reconfigure the search order with glibc 2.x. If the -broadcast option is specified, ypbind will ignore the configuration file. If the file does not exist or if there are no valid entries, ypbind exit. This ypbind is a special version which uses pthreads. It will start 2 more threads. The master process services RPC requests asking for binding info. The first thread initializes the binding and checks it periodically. Upon failure, the binding is invalidated and the process tries again to find a valid server. The second thread will handle all the signals.

d)/etc/nsswith.conf:-

The operating system uses a number of "databases" of information about hosts, users (passwd/shadow), groups and so forth. Data for these can come from a variety of sources: host-names and -addresses, for example, may be found in /etc/hosts, NIS, NIS+ or DNS. One or more sources may be used for each database; the sources and their lookup order are specified in the /etc/nsswitch.conf file.

e)/etc/pam.d/system-auth:-

The purpose of these configuration files are to provide a common interface for all applications and service daemons calling into the PAM library. The system-auth configuration file is included from nearly all individual service configuration files with the help of the include directive.The password-auth fingerprint-auth smartcard-auth configuration files are for applications which handle authentication from different types of devices via simultaneously running individual conversations instead of one aggregate conversation.

Server Configuration

a)/var/yp/Makefile:-

Makefile is used for change the MERGE GROUP=false in line no. 42 and in line no. 117 we replace group by shadow and remove the mail option.

b)/var/yp/securenets:-

NIS listens to all networks, if the **/var/yp/securenets** file is blank or does not exist (as is the case after a default installation). One of the first things to do is to put netmask/network pairs in the file so that ypserv only responds to requests from the proper network. Below is a sample entry from a **/var/yp/securenets** file:

255.255.255.0:192.168.0.0

c)/etc/hosts:-

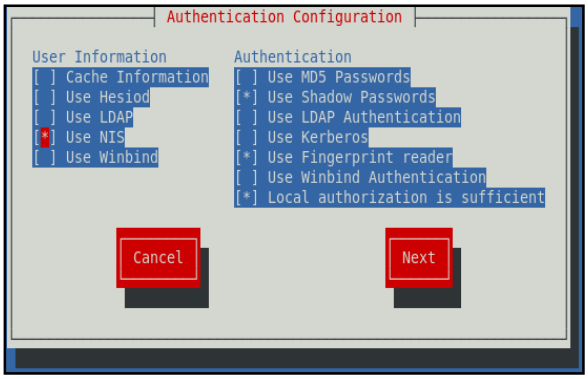
The hosts file is one of several system facilities that assists in addressing network nodes in a computer network. It is a common part of an operating system's Internet Protocol (IP) implementation, and serves the function of translating human-friendly hostnames into numeric protocol addresses, called IP addresses, that identify and locate a host in an IP network. In some operating systems, the hosts file's content is used preferentially to other methods, such as the Domain Name System (DNS), but many systems implement name service switches e.*g.*, nsswitch.conf for Linux and Unix) to provide customization. Unlike the DNS, the hosts file is under the direct control of the local computer's administrator.

Steps Are Followed For Making Connection between Client and Server

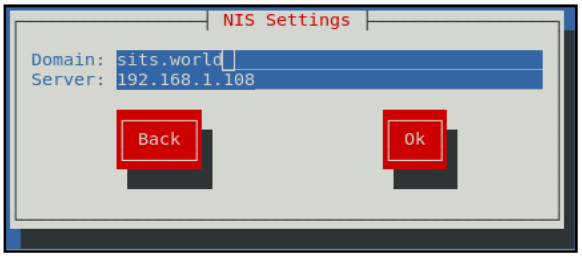
a)Steps are followed for client

Client connect to the server's user account which are given below:-

1) authconfig-tui command run on the client side:



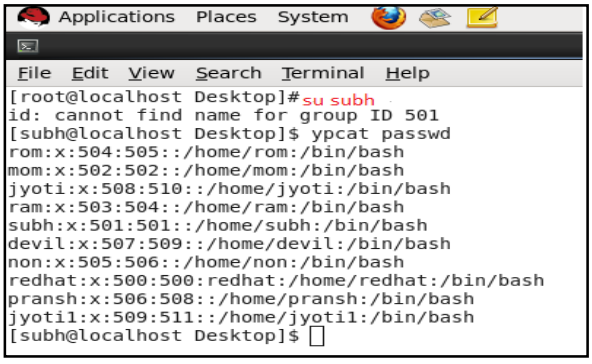
Here we are selecting the NIS server option.



Here we have to give the domain name of the server side and server IP address and click on OK button. After completing this process NIS server binding completed.

After that we switch the user using su command.

su subh



After that we can accesss the any account and permissions like reading, writing and executing. By using the ypcat command we can check all users of the server side. In the above figure we can see many user account like **rom, mom, jyoti, ram, subh, devil, non, redhat, pransh and jyoti**.

b)Steps are followed for server:-

Above server configuration steps are followed for making the server.

Conclusion

Security is the major problem in the centralized network. Authentication gives the best security in the network. In LINUX, NIS server is used for authentication services. NIS server hold the all client information and client can access the all account information and use it without any workload. Without having information of the server client can not aacess the information or user account of the server.But NIS does not send the information in encrypted form, so this is the main flaw of the NIS server.This can be solved by LDAP server(Light Directory Access Protocol). LDAP server, we will implement in future.

Future Work

Some drawbacks we are facing in the implementation like NIS server is not secure. Transfered information is not in encrypted. LDAP (light directory access protocol) removes the limitations. We will authenticate the centralized network by using LDAP.

References

[1] http://computernetworkingnotes.com/network-administrations/nis-server.html.

[2] http://www.diwan.com/nis/NIS_Tutorial/tutorial.htm.

[3] http://www.learnerstv.com.

[4] NIS-04, authentication - parallel session 10, "Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on."