Centralized Authentication Using Network Information System (NIS)

S Taruna, Jyoti Chauhan
Computer Science Department
Banasthali Vidypith

ABSTRACT

This paper describes a clustering solution that a large number of users can use Linux at the same time with authentication. This scheme uses NIS(Network Information Service). Users can login the system at the unified entrance and have centralized authentication. This gives specific configuration，also analyzes the performance of the scheme

Keywords—Yellow Pages (YP), Network Time Protocol (NTP), Network Information Service (NIS), Redhat Package Management (rpm), NIS Domain.

1. INTRODUCTION

The Network Information Service, or NIS (originally called Yellow Pages or YP) is a client–server directory service protocol for distributing system configuration data such as user and host names between computers on a computer network. Sun Microsystems developed the NIS.

Network Information Service(NIS)/YP provides centralized control over a more than just machine names and addresses. NIS stores information about machine names and addresses, users, the network itself, and network services. This is known as the 'NIS namespace'. The namespace information is stored in NIS maps. NIS maps were designed to replace UNIX /etc files, as well as other configuration files, so they store much more than names and addresses. A network using a NIS relies on it completely for normal operation so maintaining its integrity is vital

1.1.Why We Need NIS

When a user wants to login to a computer system he has to go through the process of authentication. If the same user wants to authenticate against two computer systems he needs to authenticate twice. This becomes unpractical very fast as the number of systems grow, especially if the user has to remember separate usernames and passwords for each system.

Another problem with this is that the management of the user accounts becomes complicated as we need several user accounts for each user. So, if we for example want to remove one user completely, we need to update all our systems. The solution to this problem is to use a centralized authentication server. This means that every time a user wants to authenticate, he always does it against the same server. This also means that all the accounts are stored in the same place, so there is no redundancy. In order to use centralized authentication, the systems have to include support for it. There are different protocols and applications that can be used for central authentication.NIS is a distributed naming service. It is a mechanism for identifying and locating network objects and resources. It provides a uniform storage and retrieval method for network-wide information in a transport-protocol and media-independent fashion.

2. NIS STRUCTURE

NIS is based upon the Remote Procedure Call (RPC) protocol which uses the External Data Representation(XDR) standard. Below this level are the raw communications services of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) provided by the Internet Protocol (IP). The relationships between these protocols are shown below

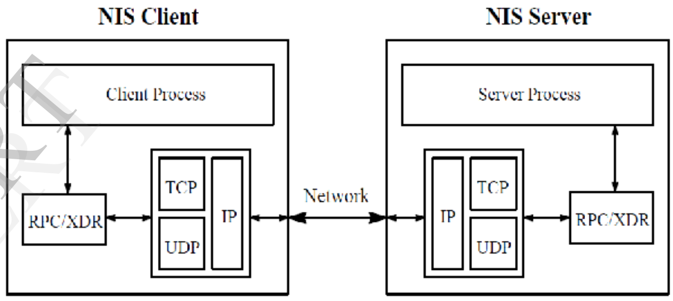


Fig1: NIS protocol structure

RPC implements a method by which a *client* process on one machine can perform a virtual procedure call to a *server* process on a remote machine. The client is considered to be accessing a feature of a service provided by the server. The client calls an RPC procedure with the arguments for the remote procedure and does not return from the call until the request has been sent to the server, processed, and a reply received. The message is encoded using XDR so that RPC can be used between heterogeneous machines using different internal data representations. The actual transmission of data is performed using either TCP or UDP depending on the desires of the client and the design of the server

NIS Maps: NIS stores information in a set of files called *maps*. NIS maps were designed to replace traditional UNIX **/etc** files, as well as other configuration files, so they store much more than names and addresses. As a result, the NIS namespace has a large set of maps[5].

3. NIS MACHINE TYPE

In a network when we configure NIS we need to configure the NIS server and client. Three types of NIS machines are made which is given below

- Master server
- Slave server
- Clients of NIS server

3.1. NIS SERVERS

NIS servers come in two varieties, master and slave.

3.1.1. Master Server*:* The machine describes as master server contains the set of maps that the system administrator creates and updates as necessary. Each NIS domain must have one, and only one, master server, which can propagate NIS updates with the least performance degradation.

3.1.2. Slave Server*:* Other can describes in the domain as slave servers. A slave server has a complete copy of the master set of NIS maps. Whenever the master server maps are updated, the updates are propagated among the slave servers. Slave servers can handle any overflow of requests from the master server, minimizing "server unavailable" errors. Normally, the system administrator designates one master server for all NIS maps. However, because each individual NIS map has the machine name of the master server encoded within it, you could designate different servers to act as master and slave servers for different maps. To minimize confusion, designate a single server as the master for all the maps you create within a single domain.

4. TIME SYNCHRONIZATION FOR NIS

An NIS domain must have their time synchronization, both client and server time should be synchronized with each other and this can be done with the help of NTP (Network Time Protocol).

Network Time protocol is installed by the rpm (red hat package management) and daemon for ntp is ntpd .We have to configure NTP server first and then at client side by the following commands we can synchronize the client time with the server

- yum install ntp - this command is used to install the NTP at client side.
- vim /etc/ntp.conf – in this configuration file we have to insert either the IP address or the name server of NTP server. so that client can understand that by which sever it is to be synchronized.
- Service ntpd restart-After changes of the NTP configuration, the NTP service needs to be restarted. This needs to be done for NTP server or client. Depending on operating system, the easiest way to do this is to reboot the system.
- chkconfig ntpd on – this command is used to make the ntp service permanent in the system.
- ntpdate –b (IP of the server)- command is used to synchronize the time of client with the NTP server

5. NIS CONFIGURATION

Before configuring NIS in the network there are some issues that must be completed, first one is the planning of NIS domain. Set of NIS clients and NIS server is known as NIS domain.

- We have to decide which machines will be in our NIS domain. A network can have more than one NIS domain, and there can be machines on our network that are outside of our NIS domain. Choose an NIS domain name, which can be 256 characters long. A good practice is to limit domain names to no more than 32 characters. Domain names are case-sensitive. For convenience, we can use our Internet domain name as the basis for our NIS domain name. For example, if our Internet domain name is *`sits.world`*, we can name our NIS domain *`sits.world`*. If we wanted to divide `sits.world` into two NIS domains, one for the sales department and the other for the manufacturing department, we could name one *`sales.sits.world`* and the other *`manf.sits.world`*`(7).`
- Identifying NIS server and clients, select one machine to be the master server and if we want to create any slave server then decide that which one would be slave server and then select client machine. Typically all machines in the domain are set to be NIS clients, although this is not necessary.

5.1. Configuring an NIS server

Following are the packages that should be installed in the system before configuring the NIS server within the network.

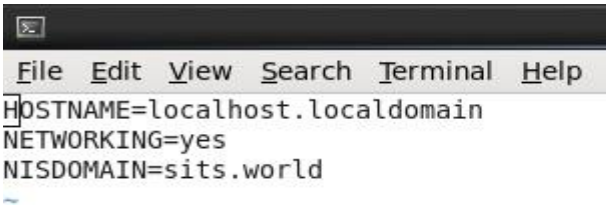
Installation of packages

- *yum install ypserv -* ypserv is the daemon for NIS Services. NIS clients' requests for information from an NIS map. ypserv is a daemon that runs on NIS servers with a complete set of maps. At least one ypserv daemon must be present on the network for NIS service to function.
- *yum install rpcbind –* rpcbind is the replacement of portmap it is required to import or export the network file system shared directories

Configuration files:

After the installation of above packages some of the configuration files need to be configure which are given below

- vim /etc/sysconfig/network – Insert the following line in this file

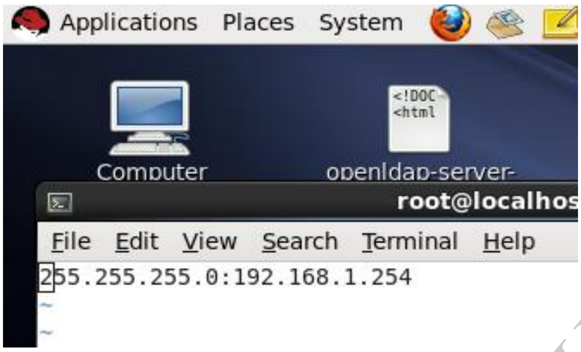


```
HOSTNAME=localhost.localdomain
NETWORKING=yes
NISDOMAIN=sits.world
~
```

- vim /var/yp/Makefile –It contains all the instructions necessary to create all the default map this is used to bind the database

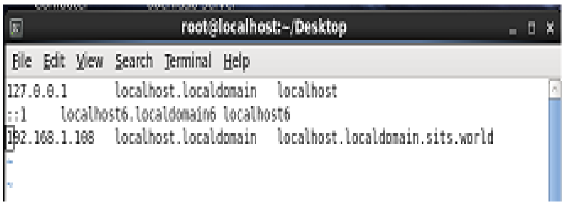
- vim /var/yp/securenets – in this config file we have to insert the value of netmask and subnet. This authorizes only a single subnet to authenticate with the NIS server

Config file: vim /var/yp/securenets


Applications Places System
Computer
<!DOC
<html
openldap-server-
root@localhos
File Edit View Search Terminal Help

```
255.255.255.0:192.168.1.254
~
~
```

- vim /etc/hosts –It is used to create a map that uses each host name as a key , and IP addresses as a value.In this configuration file we enter the value of server IP, hostname and hostname.NIS domain name
  Configuration file: vim /etc/hosts



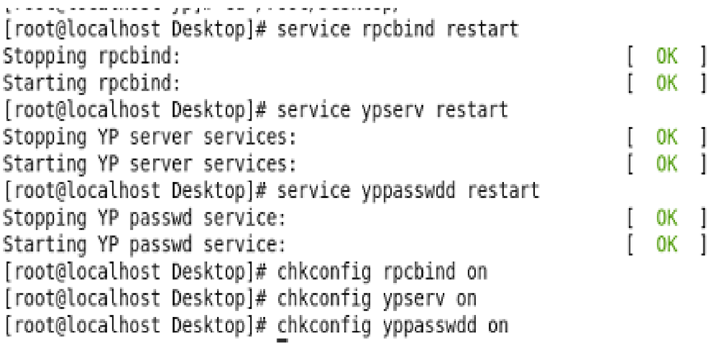
```
127.0.0.1       localhost.localdomain   localhost
::1     localhost6.localdomain6 localhost6
192.168.1.108   localhost.localdomain   localhost.localdomain.sits.world
~
~
```

Services Restart

- service rpcbind restart
- service ypserv restart
- service yppasswdd restart

after restarting the services we have to make them permanent by applying the chkconfig command with the following daemons.

- chkconfig rpcbind on
- chkconfig ypserv on
- chkconfig yppasswdd on



```
[root@localhost Desktop]# service rpcbind restart
Stopping rpcbind:                                          [  OK  ]
Starting rpcbind:                                          [  OK  ]
[root@localhost Desktop]# service ypserv restart
Stopping YP server services:                               [  OK  ]
Starting YP server services:                               [  OK  ]
[root@localhost Desktop]# service yppasswdd restart
Stopping YP passwd service:                                [  OK  ]
Starting YP passwd service:                                [  OK  ]
[root@localhost Desktop]# chkconfig rpcbind on
[root@localhost Desktop]# chkconfig ypserv on
[root@localhost Desktop]# chkconfig yppasswdd on
```

5.2. Configuring an NIS client :

Following packages should be installed in machine to make it NIS server in NIS domain enviornment: **ypbind** - NIS client daemon **authconfig** - used for automatic configuration of NIS client.

yp-tools: Contains utilities like ypcat, yppasswd, ypwhich and so on used for viewing and modifying the user account details within the NIS server.

portmap (mandatory)

➢ There are two methods to configure an NIS client.

Method 1: Manual method

Enter the following line in the **/etc/sysconfig/network** file:

NISDOMAIN=domain-name-of server

Append the following line in **/etc/yp.conf** :

domain sits.world server 172.24.254.254 # replace this with our NIS server address.

Make sure the following lines contain '**nis**' as an

option in the file **/etc/nsswitch.conf** file:

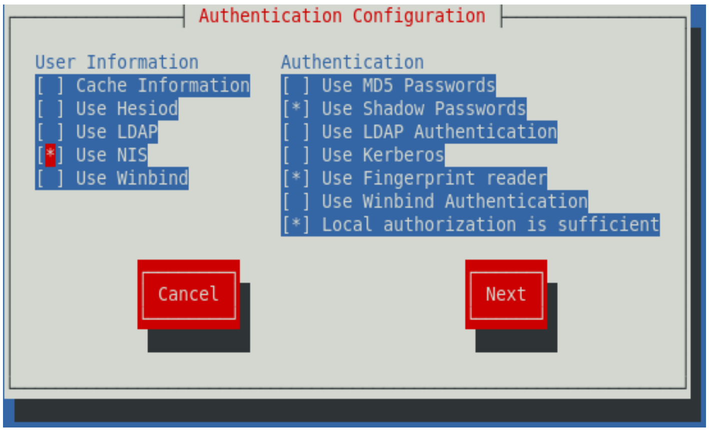
passwd: files **nis**
shadow: files **nis**
group: files **nis**
hosts: files **nis** dns
networks: files **nis**
protocols: files **nis**
publickey: nisplus
automount: files **nis**

netgroup: files **nis**
aliases: files **nisplus**

Finally restart ypbind and portmap.

Method 2: Run *authconfig-tui* and follow directions.

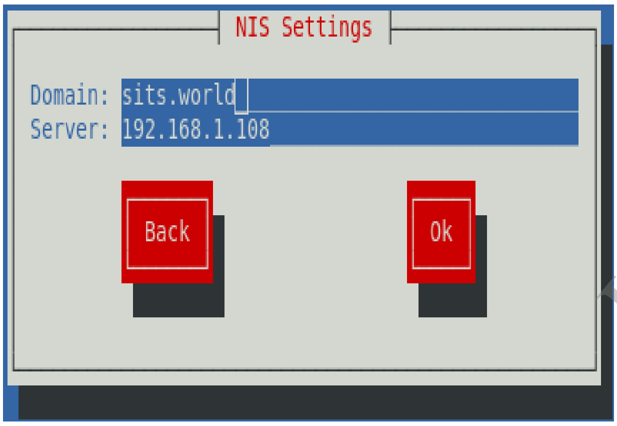
Command used is *authconfig-tui*



```
Authentication Configuration

User Information            Authentication
[ ] Cache Information       [ ] Use MD5 Passwords
[ ] Use Hesiod              [*] Use Shadow Passwords
[ ] Use LDAP                [ ] Use LDAP Authentication
[*] Use NIS                 [ ] Use Kerberos
[ ] Use Winbind             [*] Use Fingerprint reader
                            [ ] Use Winbind Authentication
                            [*] Local authorization is sufficient
```

Press next button

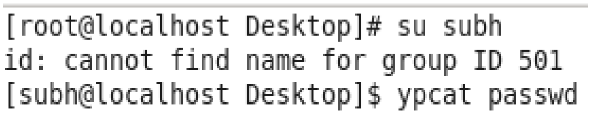


```
NIS Settings

Domain: sits.world
Server: 192.168.1.108
```

In this dialogue box enter the NIS domain name and IP of the server then enter OK

Afetr this action if we run the command su username of the server then it will provide the shell of the user of NIS server that is shown below:

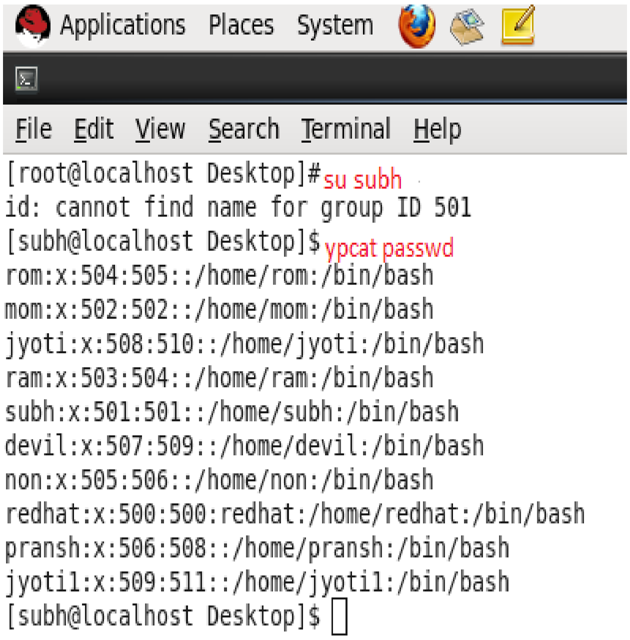


```
[root@localhost Desktop]# su subh
id: cannot find name for group ID 501
[subh@localhost Desktop]$ ypcat passwd
```

In above dialogue box we can se that we can access the shell of NIS server as user subh is at the NIS server machine.

To check if we have succesfully configured NIS client, We need to execute the following command:

# ypcat passwd



Applications Places System
File Edit View Search Terminal Help

```
[root@localhost Desktop]#su subh
id: cannot find name for group ID 501
[subh@localhost Desktop]$ ypcat passwd
rom:x:504:505::/home/rom:/bin/bash
mom:x:502:502::/home/mom:/bin/bash
jyoti:x:508:510::/home/jyoti:/bin/bash
ram:x:503:504::/home/ram:/bin/bash
subh:x:501:501::/home/subh:/bin/bash
devil:x:507:509::/home/devil:/bin/bash
non:x:505:506::/home/non:/bin/bash
redhat:x:500:500:redhat:/home/redhat:/bin/bash
pransh:x:506:508::/home/pransh:/bin/bash
jyoti1:x:509:511::/home/jyoti1:/bin/bash
[subh@localhost Desktop]$
```

The output will be the contents of the /etc/passwd file residing on the NIS server having user IDs greater than or equal to 500.

6. LIMITATIONS OF NIS

Although NIS can be very efficient in responding to queries for network information, it is not a secure mechanism for providing strong authentication and authorization services. For example:

If NIS clients use the broadcast service to locate NIS servers on the network, intruders can easily introduce their own NIS server with their own privileged accounts. Once a client binds to the rogue NIS server, the intruder can gain access to that client and perform unauthorized operations.

The NIS server's only security policy is the securenets setting. The securenets setting identifies which NIS clients to accept queries from. If an intruder impersonates a client that the securenets setting allows the NIS server to accept, he can download all of the NIS data. Even if an intruder fails the securenets test, he could potentially inspect all of the NIS requests and decode the data to gain access.

If NIS is used for authentication, password hashes are sent around the network in clear text and can be easily captured and cracked, making client systems vulnerable.

NIS performs no authentication at the RPC level; any machine on any network could easily create a fake RPC reply simply by pretending to be the NIS server

7. CONCLUSION

NIS is not a secure facility. Yet many of the authentication procedures used on Unix machines implicitly use NIS when it is enabled. The problem comes about from the assumption that a NIS access across the network is as secure as a disk access to the local file. It is safe to assume that a read from a local file cannot be interfered with short of actually changing the file.

However with NIS and more generally RPC with no authentication, a corresponding read can be made to return whatever data or lack of data is desired. This is not an acceptable situation. Security is not an issue that should be slighted in the desire for ease in maintenance. In this case compromising NIS gives an intruder complete access to a NIS client rendering useless many security features of the system.

8. FUTURE WORK

As we have seen that there are many shortcomings of NIS therefore we need to move some other protocol for the secure networking authentication process within the organizations.LDAP is the server which is used over the NIS.This will be our next focus.As LDAP provide secure centralized authentication over NIS .

REFERENCES

1. http://www.yolinux.com/TUTORIALS/NIS.html.

2.A Unix Network Protocol Security Study: Network Information Service
David K. Hess, David R. Safford and Udo W. Pooch
Texas A&M University

dhess@cs.tamu.edu

3.Sun Microsystems, Inc., *Network Programming Guide*, March 1990

4.http://bradthemad.org/tech/notes/redhat_nis_setup.php

©1998-2013 by Brad The Mad

5. Network Information Serviec(NIS and NIS+ guide)

6.http://beginlinux.com/blog/2010/02/nis-server-config/

Mike may 4,2010 at 3:15 pm

7.http://docs.oracle.com/cd/E18752_01/html/816-4556/cnis1-32365.html

8.http://www.linux-nis.org/nis-howto/HOWTO/settingup_client.html

9.http://www.freebsd.org/doc/en/books/handbook/network-nis.html