SECURITE DES SYSTEMES D'INFORMATION

FREEIPA

Projet de semestre ITI 3eme année

Etudiant RAZAFIMAHATRATRA LAURE

Professeur : Gérald LITZISTORF

h e p i a
Haute école du paysage, d'ingénierie
et d'architecture de Genève

Année académique 2013-2014
Projet de semestre

SECURITE DES SYSTEMES D'INFORMATION
FREEIPA

Descriptif :

Cette étude concerne la solution Open Source FreeIPA (Identity Policy Audit) que l'on peut comparer à Active Directory de Windows.
Elle doit permettre de comprendre ses principales fonctionnalités dans une perspective d'utilisation dans le monde de la virtualisation (OpenStack, …).

L'étudiant doit proposer puis mettre en œuvre divers scénarios utilisant FreeIPA

Cadre du projet :

- Directory Server (LDAP, …)
- Authentification basée sur Kerberos
- Contexte applicatif (client, serveur de fichiers, …)

Travail demandé :

Cette étude comprend les étapes suivantes :

1) Recherche des documents utiles (manuel d'installation, best practices, …) sur www.freeipa.org, …

2) Spécification du scénario 1
Tenir compte des dépendances
Validation par le prof.

3) Configuration et tests sur PCs du labo

4) Répéter 2) et 3) pour d'autres scénarios si le temps le permet

5) Recommandations pour étapes futures (virtualisation, …)

Sous réserve de modification en cours du projet de semestre

Candidat :
M. RAZAFIMAHATRATRA LAURE
Filière d'études : ITI
Département : ITI

Professeur(s) responsable(s) :
Litzistorf Gérald

En collaboration avec :
Projet de semestre soumis à une convention de stage en entreprise : non
Projet de semestre soumis à un contrat de confidentialité : non

Timbre de la direction

Le but de ce projet est la mise en place d'une architecture client-serveur avec une authentification de type Kerberos. Dans notre cas, un PC client fait un accès fichier sur un serveur nfs.

Dans ce projet, on utilisera
- 2 PCs (1 servant de serveur freeipa en meme temps serveur nfs, 1 servant de client freeipa et client nfs).

qu'on réalisera par les etapes suivantes:
- configuration d'un serveur freeipa
- configuration d'un client freeipa
- configurer le serveur freeipa comme serveur nfs et configuration l'accès nfs à partir des clients freeipa.

I- INTRODUCTION

Cette étude permet de mettre une infrastructure securisée par un controlleur de domaine avec l'utilisation de la solution Open Source FreeIPA (Identity Policy Audit).

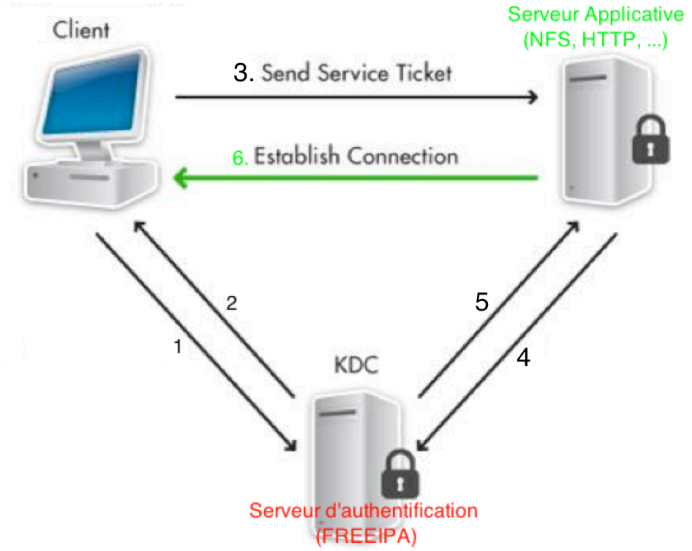
Selon http://www.freeipa.org/page/About :
« FreeIPA est une solution pour les environnements réseau Linux / UNIX pour une meilleur gestion centralisée des identités et d'authentification. Un serveur. FreeIPA fournit une authentification centralisée, l'autorisation et les informations de compte en stockant les données sur l'utilisateur, les groupes, les hôtes et autres objets nécessaires à la gestion des aspects de sécurité d'un réseau d'ordinateurs.

FreeIPA est construit sur des composants Open Source bien connus et des protocoles standard avec la facilité de gestion et d'automatisation des tâches d'installation et de configuration.

FreeIPA :
• Permet à tous les utilisateurs d'accéder à toutes les machines avec les mêmes informations d'identification et les paramètres de sécurité.
• Accède aux fichiers personnels de manière transparente depuis n'importe quelle machine de manière authentifiée et sécurisée.
• Utiliser le mécanisme de regroupement avancé pour restreindre l'accès réseau aux services et fichiers uniquement à des utilisateurs spécifiques.
• Gère de manière centralisée mécanisme de sécurité comme les mots de passe, clés, les règles de contrôle d'accès.
• Délègue, sélectionne tâches administratives à d'autres utilisateurs. »

II- ANALYSE

Pour ce projet, l'objectif finale est de réaliser une communication avec un serveur applicative et un client via une authentification kerberos[1] qui sera gérer par un serveur freeipa.



1.demande de ticket de service au serveur d'authentification freeipa
2.obtention du ticket
3.requête de service (accès fichier)
4.verification du ticket
6.validation du ticket

figure1. Flexible Authentication Support Diagram

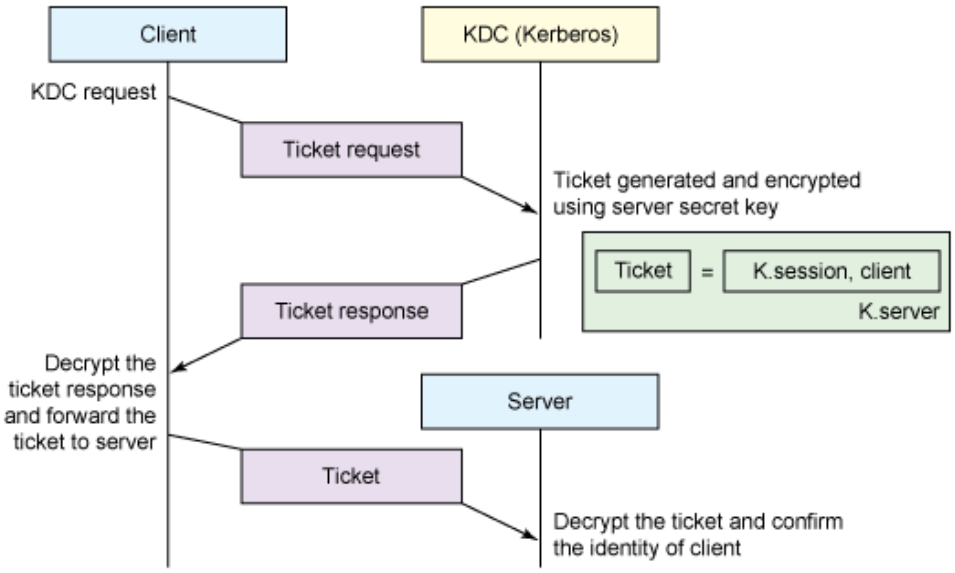


figure2. Kerberos authentication protocol (KAP)[2]

[1] http://fr.wikipedia.org/wiki/Kerberos_(protocole)
[2] http://www.ibm.com/developerworks/aix/library/au-aixsecuritydce/

III- REALISATION

Pour ce projet j'utilise 3PCs (A3, A4, A45) sous Fedora 18 GLI du laboratoire qui sert de clients et serveurs[3], ces postes sont dans un réseau isolé (intranet) et sont configurés avec des IP statiques et se trouvant dans un même domaine.

Les postes sont configurés de manière suivante:

PC(nom)	Adresse IP	Domaine	DNS	Masque	Port ethernet
ipaserver	192.168.1.10	demo	192.168.1.10	255.255.255.0	Carte-mère
Ipaclient1	192.168.1.15				

Avec les comptes:
Login: labotd mot de passé: labolabo
Login: root mot depasse: rootroot

Pourqoi Fedora 18 GUI ?
« Fedora est une distribution Linux basée sur le système d'exploitation GNU/Linux servant de vitrine aux logiciels libres les plus récents ».[4]

Etape 1 : Téléchargement des paquets nécessaires.

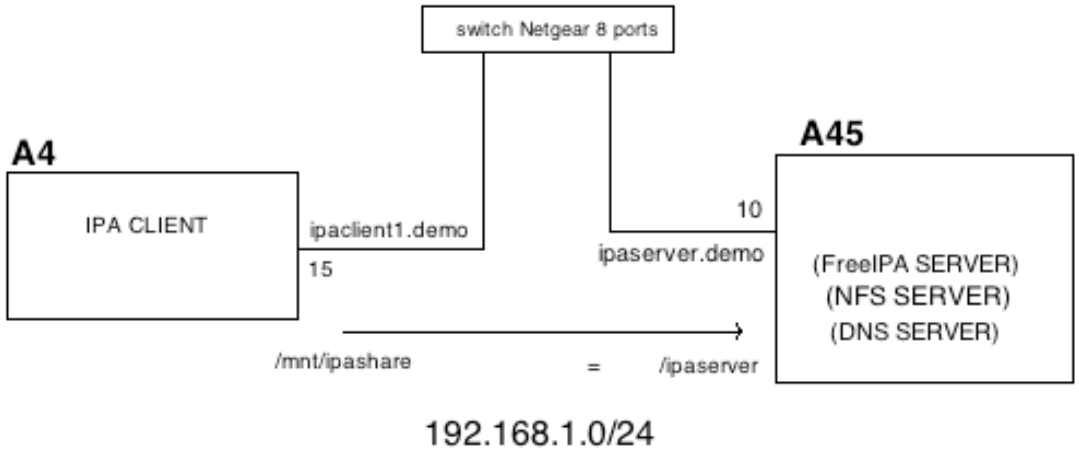
L'installation du serveur freeipa nécéssite le paquet freeipa-server qu'on obtient avec la commande "*yum install freeipa-server bind bind-dyndb-ldap*", bind permettant une gestion de DNS comme indiqué dans la documentation[5].
En suite pour on va aussi télécharger le paquet nfs avec la commande "*yum install –y nfs-utils*" pour lui ajouter la fonction de serveur nfs.

Et sur le PC servant de client freeipa " *yum install freeipa-client freeipa-admintools*" avec l'option freeipa-admintools permettant de l'utiliser les commades d'administration[6].

Etape 2 : Configuration réseau en IP statique de tous les PCs avec les valeurs du tableau ci-dessus (annexe 2).

[2] http://www.ibm.com/developerworks/aix/library/au-aixsecuritydce/
[3] serveur DNS et serveur Freeipa
[4] http://www.fedora-fr.org/
[5] http://docs.fedoraproject.org/en-US/Fedora/18/html/FreeIPA_Guide/Installing_the_IPA_Server_Packages.html
[6] http://docs.fedoraproject.org/en-US/Fedora/18/html/FreeIPA_Guide/Installing_the_IPA_Client_on_Linux.html

Etape 3: Réalisation d'un partage nfs entre le serveur freeipa et le client freeipa selon http://wiki.linux-nfs.org/wiki/index.php/NFS_and_FreeIPA



- ouverture des ports (en premier temps, on arrête le firewall pour faciliter la communication entre le client et le serveur)

[ipaserver]# systemctl stop firewalld.service
[ipacclient]# systemctl disable firewalld.service
//**disable** pour désactiver au démarrage

- création des fichier de configuration du serveur freeipa sur le PC serveur

[ipaserver]# ipa-server-install --setup-dns

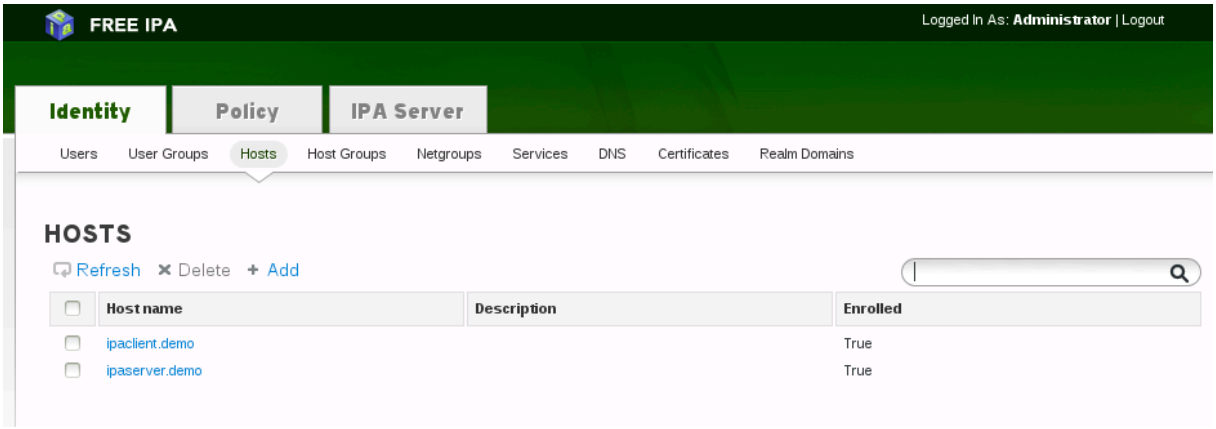
```
[root@ipaserver labotd]# ipa-server-install --setup-dns

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will set up the FreeIPA Server.

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the Network Time Daemon (ntpd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure DNS (bind)

To accept the default shown in brackets, press the Enter key.
```

Pour verifier que le serveur est configuré on peut aller sur l'interface de gestion graphique du serveur freeipa en mettant comme FQDN le nom du serveur freeipa pui est ici ipaserver.

- création des fichier de configuration du client freeipa sur le PC client

[ipacclient]# ipa-client-install

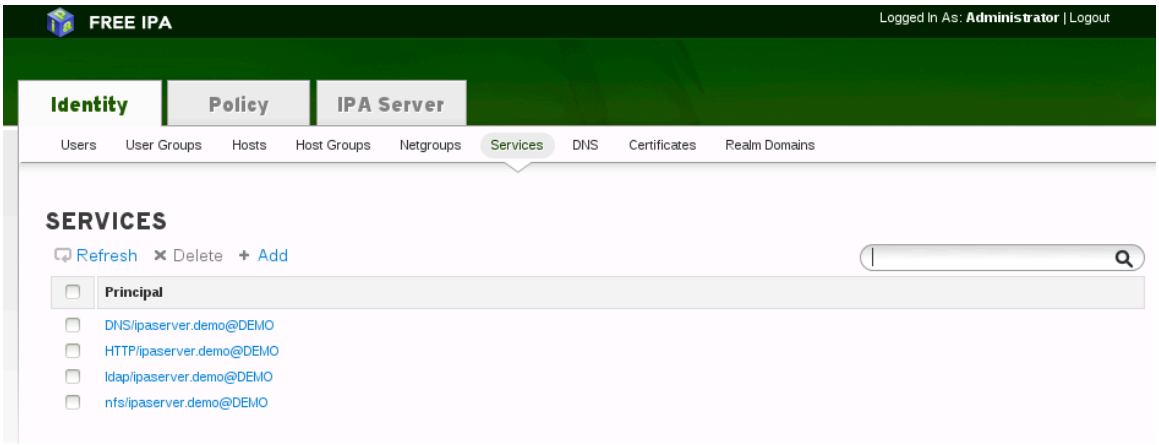
cette commande ajoute aussi le PC dans le domaine kerberos, c'est l'équivalent de la commande « *ipa host-add ipaclient.demo* » qu'on peut lancer depuis le serveur.



On peut aussi vérifier par un ping du client pour vérifier qu'il est bien dans le domaine et qu'il a été pris en compte par le serveur DNS du domaine

- Ajout du service nfs sur le serveur freeipa

[ipaserver]# ipa service-add nfs/ipaserver.demo



- Acquisition de la clé de service nfs pour le serveur nfs

[ipaserver]# ipa-getkeytab -s ipaserver.domaine -p nfs/ipaserver.domaine -k /etc/krb5.keytab

- vérification des clés dans la table de clé (commande kerberos)

[ipaserver]# klist -ke /etc/krb5.keytab
[ipaserver]# klist -c

```
[root@ipaserver labotd]# klist -c
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@DEMO

Valid starting     Expires            Service principal
04/10/14 14:32:31  04/11/14 14:32:28  krbtgt/DEMO@DEMO
04/10/14 14:34:00  04/11/14 14:32:28  HTTP/ipaserver.demo@DEMO
[root@ipaserver labotd]# klist -ke /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 host/ipaserver.demo@DEMO (aes256-cts-hmac-sha1-96)
   2 host/ipaserver.demo@DEMO (aes128-cts-hmac-sha1-96)
   2 host/ipaserver.demo@DEMO (des3-cbc-sha1)
   2 host/ipaserver.demo@DEMO (arcfour-hmac)
[root@ipaserver labotd]# ipa-getkeytab -s ipaserver.demo -p nfs/ipaserver.demo -k /etc/krb5
.keytab
Keytab successfully retrieved and stored in: /etc/krb5.keytab
[root@ipaserver labotd]# klist -ke /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 host/ipaserver.demo@DEMO (aes256-cts-hmac-sha1-96)
   2 host/ipaserver.demo@DEMO (aes128-cts-hmac-sha1-96)
   2 host/ipaserver.demo@DEMO (des3-cbc-sha1)
   2 host/ipaserver.demo@DEMO (arcfour-hmac)
   1 nfs/ipaserver.demo@DEMO (aes256-cts-hmac-sha1-96)
   1 nfs/ipaserver.demo@DEMO (aes128-cts-hmac-sha1-96)
   1 nfs/ipaserver.demo@DEMO (des3-cbc-sha1)
   1 nfs/ipaserver.demo@DEMO (arcfour-hmac)
```

- Configuration du serveur nfs

  . Edition du fichier "/etc/sysconfig/nfs" pour le debugging

  [ipaserver]# vi /etc/sysconfig/nfs

  RPCGSSDARGS="-vvv"
  RPCSVCGSSDARGS="-vvv"

  [ipaserver]# vi /etc/sysconfig/nfs
  [ipaclient]# vi / etc/sysconfig/nfs

  en ajoutant la ligne SECURE_NFS="yes"

  . Création des dossier de partages

  [ipaclient]# mkdir /mnt/ipashare/
  [ipaserver]# mkdir /ipashare/

  . Edition de droit du fichier de partage

  [ipaserver]# chmod 777 -Rf /ipashare/

  . Modification du fichier export sur le serveur

  [ipaserver]# vi /etc/exports en ajoutant
  /ipashare gss/krb5p(rw,subtree_check,no_root_squash,fsid=0)

  . Demarrage et activation du service nfs securisé

  [ipaserver]# service nfs enable
  [ipaserver]# service nfs start
  [ipaserver]# service nfs-secure-server enable
  [ipaserver]# service nfs-secure-server start
  [ipaclient]# service nfs enable
  [ipaclient]# service nfs start
  [ipaclient]# service nfs-secure enable
  [ipaclient]# service nfs-secure start

- Montage avec la commande

[ipaclient]# mount -v -t nfs4 -o sec=krb5p ipaserver.demo:/ /mnt/ipashare/

- **Test** avec la création d'un fichier dans /mnt/ipashare du client freeipa et observer sa presence dans /ipashare du serveur freeipa

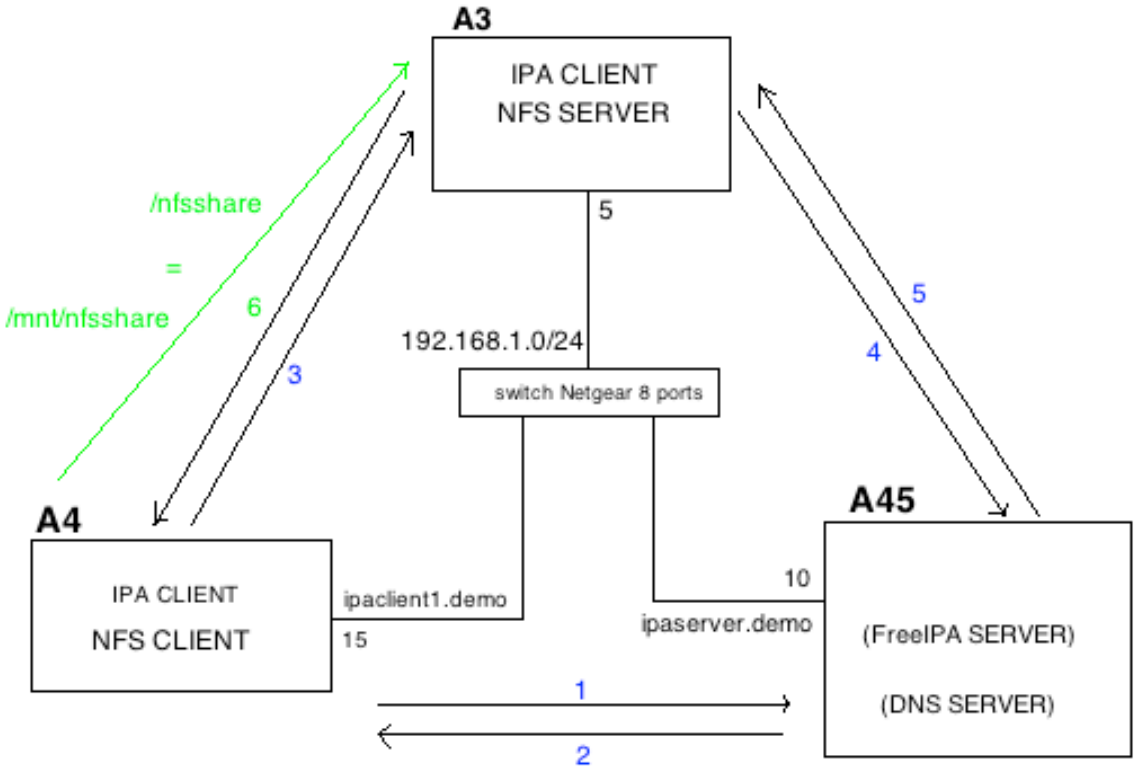
[ipaclient]# touch /mnt/ipashare/test.txt
[ipaserver]# ls /ipashare/

IV- PROBLEMES RENCONTRES

- Compréhension du tutorial, dont ambiguité dans les commandes sur le client ou le serveur.
- Dans le **Partage nfs avec le serveur freeipa**, j'vais un "accès refuse à cause de permission du serveur freeipa" lors du montage de dossier de partage, un message d'erreur indiquant un réfus de permission apparait, problème résolu grâce a l'aide de l'assistant Mr Khaled B. en proposant un autre tutorial: http://wiki.linux-nfs.org/wiki/index.php/NFS_and_FreeIPA paragraphe 5.2 Setup Kerberos principals, éstimation de temps passé sur le tutoriel 30 heures.
  Et en vérifiant le fichier de log /var/log/messages avec la commande *"tail -n=100 -f /var/log/messages"*.
- Connexion avec le serveur d'application qui est un serveur nfs, problèmes non encore résolu, depuis 20 heures. Problème similaire à celui abordé ci-dessus.
- Redemarrage du service network, redemarrage de l'ordinateur pour la prise en compte.

IV- AMELIORATION

Réalisation d'un partage nfs entre le serveur nfs et le client nfs via une authentification kerberos



V- CONCLUSION

Les objectifs de ce travail ont été partiellement atteints. Ce travail m'a permis de découvrir les fonctionnements d'un serveur d'authentification et configurer des serveurs d'applications comme le serveur dns, serveurs nfs et une connaissance de plus dans le monde linux.

Ce projet a amélioré ma méthodologie de travail ainsi que mes motivations à surmonter les difficultés.

LIENS

http://docs.fedoraproject.org/en-US/Fedora/18/html/FreeIPA_Guide/Installing_the_IPA_Client_on_Linux.html

http://docs.fedoraproject.org/en-US/Fedora/17/html/FreeIPA_Guide/kerb-nfs.html

http://wiki.linux-nfs.org/wiki/index.php/NFS_and_FreeIPA

http://www.freeipa.org/docs/1.2/Client_Setup_Guide/en-US/html/chap-Client_Configuration_Guide-Configuring_Fedora_as_an_IPA_Client.html

http://www.freeipa.org/page/About

http://docs.fedoraproject.org/en-US/Fedora/18/html/FreeIPA_Guide/index.html

http://www.datadirect.com/products/datadirect-connect/jdbc-drivers/features/data-connectivity-features/anatomy-of-a-driver/security/flexible-authentication-support

http://www.bga.org/~lessem/psyc5112/usail/network/nfs/tips.html

ANNEXES

1. Configuration réseau en IP Statique

Selon http://www.tutonline.fr/tutoriels/linux/linuxhostname

#service NetworkManager stop

#chkconfig NetworkManager off

#chkconfig network on

#vi /etc/hostname remplacer le contenu par "ipaserver.demo"

#vi /etc/sysconfig/network, y ajouter les lignes suivantes:

HOSTNAME=dnsserver.demo par exemple

#ifconfig pour connaitre l adresse ip actuelle afin de le comparer après changement

#vi /etc/sysconfig/network-scripts/ifcfg-p255p1 ,y jouter les configurations suivantes:

```
BOOTPROTO=STATIC          //mis en ip static c-a-d remplacer la
BROADCAST=192.168.1.255
IPADDR=192.168.1.5        //l adresse ip static qu on attribue a l interface
NETMASK=255.255.255.0
NETWORK=192.168.1.0       //aderesse reseau
DNS1=192.168.1.5          //serveur dns utilisé
```

#vi /etc/resolv.conf, editer le fichier de resolution en ajoutant le nom de domaine demo et le serveur dns

#service network restart

#systemctl restart network.service

Afin de voir le changement de l adresse ip, utiliser la commande "ifconfig" et constater le changement par rapport a celui d avant et aussi par rapport a la valeur introduite qui est 192.168.1.5

Pour tester que la nouvelle configuration a ete pris en compte, un redemarrage de l ordinateur est necessaire, ensuite lancer la commande ifconfig et comparer les valeurs obtenues par a port a celles de la config.

Ensuite redemarrer l'ordinateur et verifier a nouveau la configuration IP avec la commande "ifconfig".

```
[root@localhost labotd]# service NetworkManager stop
Redirecting to /bin/systemctl stop  NetworkManager.service
[root@localhost labotd]# chkconfig NetworkManager off
Note: Forwarding request to 'systemctl disable NetworkManager.service'.
rm '/etc/systemd/system/network.target.wants/NetworkManager-wait-online.service'
rm '/etc/systemd/system/multi-user.target.wants/NetworkManager.service'
rm '/etc/systemd/system/dbus-org.freedesktop.NetworkManager.service'
[root@localhost labotd]# chkconfig network on
[root@localhost labotd]# vi /etc/hostname
[root@localhost labotd]# vi /etc/sysconfig/network
[root@localhost labotd]# cat /etc/hostname
ipaserver.demo
[root@localhost labotd]# cat /etc/sysconfig/network
# Generated by anaconda
NETWORKING=yes
HOSTNAME=ipaserver.demo
[root@localhost labotd]# cat /etc/sysconfig/network-scripts/ifcfg-
ifcfg-em1     ifcfg-lo      ifcfg-p255p1
[root@localhost labotd]# cat /etc/sysconfig/network-scripts/ifcfg-p255p1
# Generated by parse-kickstart
IPV6INIT=no
HWADDR=90:e2:ba:28:9b:2a
BOOTPROTO=dhcp
DEVICE=p255p1
ONBOOT=yes
UUID=cc854b6a-6c0f-4f19-b3c9-58971f21f0e1
[root@localhost labotd]# vi /etc/sysconfig/network-scripts/ifcfg-p255p1
[root@localhost labotd]# cat /etc/sysconfig/network-scripts/ifcfg-p255p1
# Generated by parse-kickstart
IPV6INIT=no
HWADDR=90:e2:ba:28:9b:2a
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
DNS=162.168.1.10
DEVICE=p255p1
ONBOOT=yes
UUID=cc854b6a-6c0f-4f19-b3c9-58971f21f0e1
[root@localhost labotd]# vi /etc/resolv.conf
[root@localhost labotd]# cat /etc/resolv.conf
# Generated by NetworkManager
domain localdomain
search localdomain
nameserver 192.168.1.10
[root@localhost labotd]#
```

2. Configuration DNS et du serveur freeipa

```
Server host name [ipaserver.demo]:

Warning: skipping DNS resolution of host ipaserver.demo
The domain name has been determined based on the host name.

Please confirm the domain name [demo]:

Unable to resolve IP address for host name
Please provide the IP address to be used for this host name: 192.168.1.10
Adding [192.168.1.10 ipaserver.demo] to your /etc/hosts file
The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

Please provide a realm name [DEMO]:
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password:
Password (confirm):

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

IPA admin password:
Password (confirm):

Do you want to configure DNS forwarders? [yes]: no
No DNS forwarders configured
Do you want to configure the reverse zone? [yes]:
Please specify the reverse zone name [1.168.192.in-addr.arpa.]:
Using reverse zone 1.168.192.in-addr.arpa.

The IPA Master Server will be configured with:
Hostname:      ipaserver.demo
IP address:    192.168.1.10
Domain name:   demo
Realm name:    DEMO

BIND DNS server will be configured to serve IPA domain with:
Forwarders:    No forwarders
Reverse zone:  1.168.192.in-addr.arpa.

Continue to configure the system with these values? [no]: yes

The following operations may take some minutes to complete.
Please wait until the prompt is returned.
```

REMERCIEMENT

Je tiens à remercier Mr. LITZISDORF de m’avoir accorder ce projet et de m’avoir guider dans les methodologies de travail, et Mr.Basbous pour son aide apropos de la réalisation de ce projet.

TABLE DES MATIERES