

05.616 – TFG PLATAFORMA GNU/LINUX

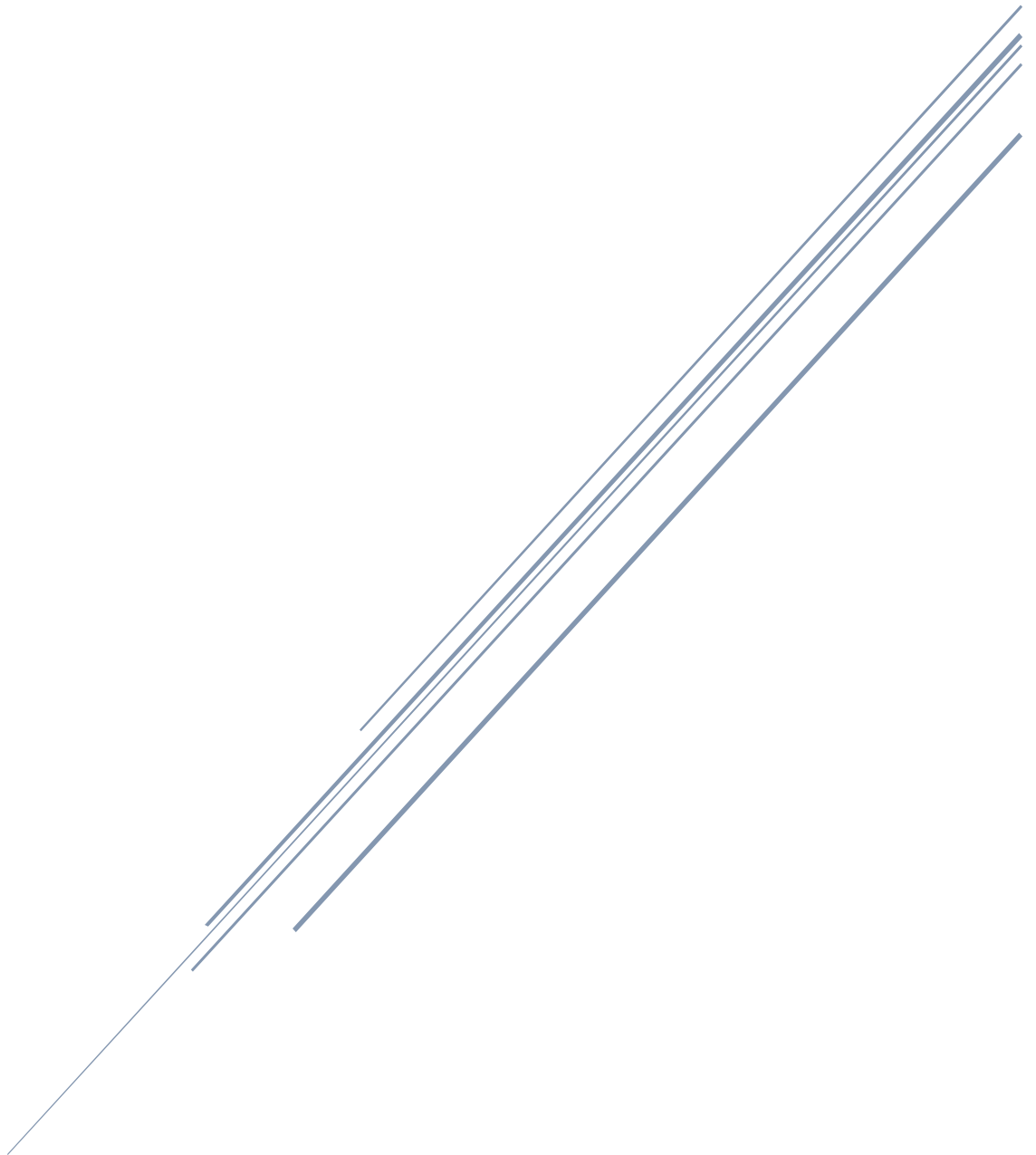
MEMORIA DEL PROYECTO

Alumne

Jordi Guillem Ferrer Bozzano

Tutor

Joaquin López Sánchez-Montañez



Resum del projecte

Davant el creixement de les infraestructures informàtiques i de la integració entre sistemes de la informació, es necessita un sistema integrat i centralitzat per gestionar les identitats d'usuari i administrar els serveis de directori amb l'objectiu de controlar, des d'un sol punt, les polítiques de seguretat, el control d'accessos i la identificació única dels usuaris.

Per la implementació d'aquest sistema és necessari incorporar recursos hardware, software i elements de configuració integrats per disposar d'un servei fiable, eficient i amb alta disponibilitat. La implementació d'aquest sistema es realitza en una organització fictícia amb una duració de 3 mesos amb data de finalització en l'estiu del any 2019.

El servei de directori centralitzat ha de permetre als usuaris una identificació única en els diferents recursos de xarxa utilitzant les seves diferents eines TIC i donar agilitat i seguretat en l'accés als recursos de xarxa de l'organització.

Per altra banda, el departament de TI ha de poder minimitzar el seu esforç en la gestió i administració de recursos de directori amb l'objectiu de millorar la qualitat de servei, minimitzar el temps de resposta i reduir les tasques monòtones i operatives.

Project summary

Given the growth of computer infrastructures and the integration of information systems, an integrated and centralized system is needed to manage user identities and manage directory services with the aim of controlling, from a single point, security policies, access control and the unique identification of users.

For the implementation of this system, it is necessary to incorporate hardware, software and integrated configuration elements to have a reliable, efficient and high availability service. The implementation of this system is carried out in a fictitious organization with a duration of 3 months ending in the summer of 2019.

The centralized directory service must allow users a unique identification in the different network resources using their different ICT tools and give agility and security in accessing the network resources of the organization.

On the other hand, the IT department must be able to minimize its efforts in the management and management of directory resources with the aim of improving service quality, minimizing response time and reducing monotonous and operational tasks.

Índex

Resum del projecte	1
<i>Project summary</i>	1
Pròleg	5
1. Que és un servei de directori	7
2. Que és FreeIPA	8
3. Treballar amb FreeIPA	11
3.1. Accés per Web UI	11
3.2. Accés per CLI	11
3.3. Funcionalitats FreeIPA	12
4. Preparació de l' entorn de laboratori	14
4.1. Infraestructura de servidors	14
4.1.1. Instal·lació del sistema operatiu CENTOS	14
4.1.2. Actualització del sistema	16
4.1.3. Instal·lació de Guest tools	16
4.1.4. Clonació de màquines	17
4.2. Infraestructura de xarxa	18
4.3. Diagrama de infraestructura	19
5. Servidors IPA	21
5.1. Requeriments dels servidors IPA	22
5.2. Preparació de servidors apolo.lab i zeus.lab	22
5.3. Administració de les rèpliques	27
5.4. Creació de usuaris i grups de domini	29
5.5. Administració sudo	30
6. Servidors DHCP	32
6.1. Preparació de servidors hercules.lab i poseidon.lab	32
6.2. Instal·lació servei DHCP	34
6.2.1. Compilació, instal·lació de codi font	34
6.2.2. Configuració servei DHCP	35
6.2.3. Arranc automàtic servei DHCP	36
6.3. Actualització DDNS	38
7. Servidors Samba i NFS	40
7.1. Preparació servidor atenea.lab	41
7.2. Instal·lació i configuració dels serveis	43

7.2.1. Procés d'instal·lació	43
7.2.2. Configuració de serveis Kerberitzats	43
7.2.3. Configuració de servei Samba	44
7.2.4. Configuració de servei NFS	45
7.3. Configuració SELinux.....	46
7.4. Configuració Automount FreeIPA	47
8. Preparació de clients IPA	50
9. Conclusions.....	51
10. Bibliografia	52

Pròleg

És un plaer per Jordi Ferrer Bozzano estudiant de la UOC del grau d'enginyeria informàtica presentar aquest treball de fi de carrera sobre el servei de directori FreeIPA.

Les raons per presentar aquest treball han sigut la d'obtenir coneixement per administrar entitats i polítiques centralitzadament i la de millorar el coneixement sobre aquest producte de codi lliure.

El treball queda estructurat en la explicació de que es FreeIPA i els seus components, la preparació del laboratori per realitzar les proves i la configuració de les peces que solen formar un servei de directori.

Jordi Ferrer Bozzano

Estudiant de la UOC per el projecte final de carrera GNU/Linux

1. Que és un servei de directori

Un servei de directori és un conjunt de infraestructura, aplicacions i processos que permeten emmagatzemar organitzada i centralitzadament les dades dels usuaris i dels recursos de xarxa. El servei de directori actua com a intermediari entre els usuaris i el repositori de directori.



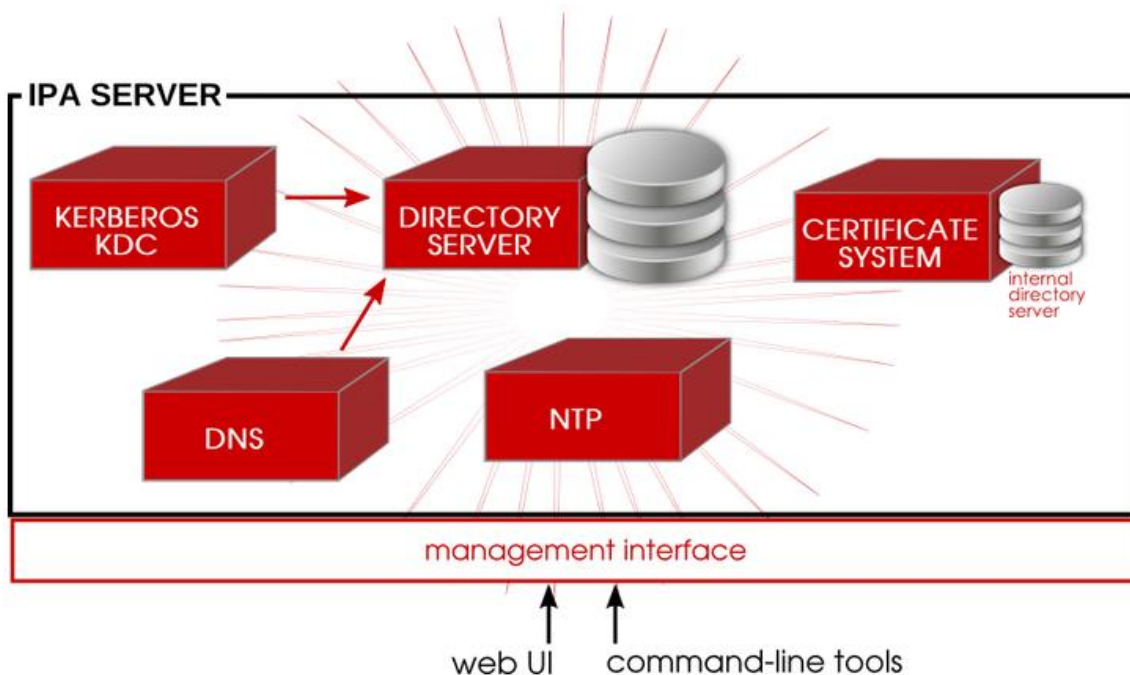
No s'ha de confondre el servei de directori amb el repositori del directori, mentre que el repositori de directori pot ser utilitzat per diferents serveis per emmagatzemar informació d'una manera jeràrquica per una funcionalitat genèrica, el servei de directori és un servei per un propòsit específic que té com objectiu gestionar els recursos que s'utilitzen en una xarxa de computadors.

Exemples de repositoris de directori pot ser LDAP o 389 Directory Server, mentre que serveis de directori pot ser FreeIPA o Active Directory. Un servei de directori s'encarrega de relacionar els recursos de xarxa com a objectes i cada un d'aquests amb els seus corresponents atributs. Cada un d'aquests objectes s'emmagatzemen d'una manera inequívoca per poder aconseguir que siguin únics.

Els principals beneficis que dona un servei de directori és administrar, organitzar i localitzar els recursos de xarxa per donar més eficiència als administradors de xarxa com la centralització i assegurar l'autenticació dels usuaris. Altres beneficis que aporten valor al negoci és la possibilitat d'utilitzar polítiques de seguretat i gestió d'identitats.

2. Que és FreeIPA

FreeIPA és un projecte de software lliure mantingut per el projecte Fedora i patrocinat per Redhat que dona serveis de directori, solucions d'autenticació i gestió d' identitats. El seu nom indica **I**dentitat, **P**olítiques, **A**utenticació **F**ree (Lliure). FreeIPA combina sistemes com el 389 Directory Server com a servidor de LDAP, Kerberos com a protocol d' autenticació entre dos computadors, NTP com a protocol de sincronització de temps, DNS com a sistema de resolució de noms i CA com a entitat certificadora. La administració dels serveis que dona FreeIPA es pot realitzar a través de línia de comandes com també mitjançant una interfície web.



Els elements que poden formar un IPA Server són el 389 Directory server, Autenticació Kerberos KDC, NTP, resolució de noms DNS i entitat certificadora CA.

389 Directory server. És el repositori de directori i és on s' emmagatzema tota la informació de FreeIPA com usuaris, grups, computadors, polítiques de seguretat, zones DNS, etc. Aquest servei escolta per el port TCP 389 i permet la possibilitat de replicar amb altres servidors per donar serveis d' alta disponibilitat.

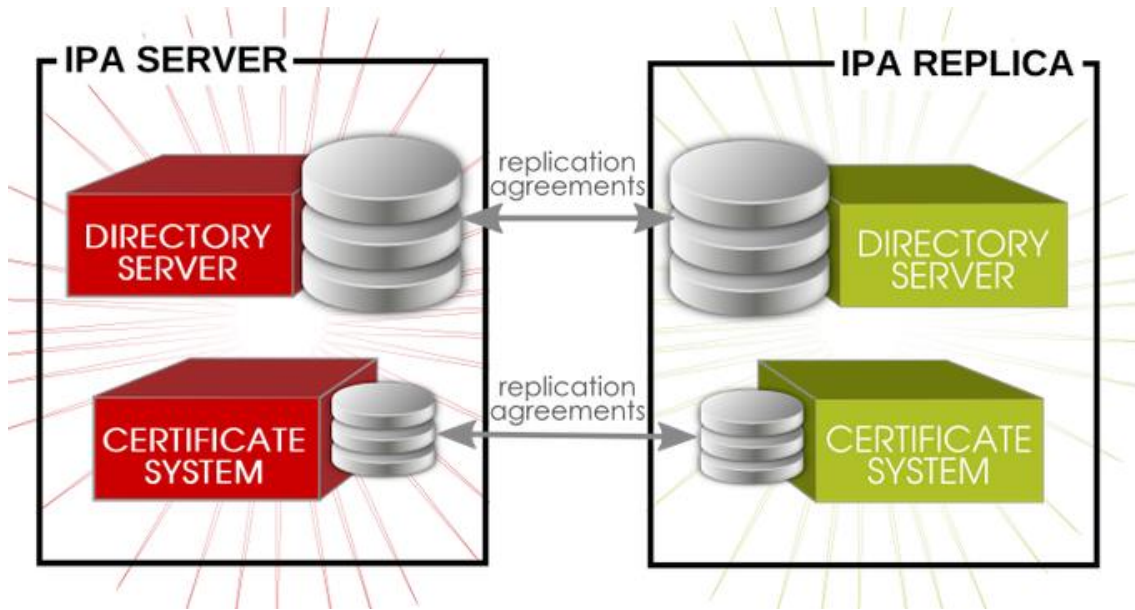
Kerberos KDC. FreeIPA utilitza aquest protocol d' autenticació simètric que es basa en el funcionament de generació de tickets o tokens als usuaris. L'autenticació inicial es basa en contrasenya però les posteriors autenticacions es realitza mitjançant aquests tokens. Amb aquest tipus d' autenticació no és necessari enviar la contrasenya per la xarxa.

NTP. FreeIPA utilitza el protocol de sincronització de temps per la xarxa NTP per poder sincronitzar el rellotge dels sistemes. Aquesta sincronització es essencial per alguns components i serveis com pot ser el d' autenticació i certificació. FreeIPA té la possibilitat de ser el servidor NTP i que faci de servidor NTP a altres computadors de la xarxa.

DNS. El sistema de resolució de noms a IP o DNS és essencial per el correcte funcionament del servei de directori perquè permet associar noms als diferents recursos de xarxa. FreeIPA permet la gestió de zones DNS com també permet la utilització d' altres servidors DNS externs.

Entitat Certificadora CA. El servei de directori necessita certificats per poder comunicar-se amb seguretat i poder-se autenticar, alguns dels serveis que necessita de la CA pot ser Kerberos. FreeIPA dona servei de CA a través del projecte **Dogtag Certificate Services**. Dogtag integra una infraestructura de clau pública PKI la qual permet signar, publicar o revocar certificats.

La disponibilitat del servei de directori és un factor molt important per el funcionament dels recursos, FreeIPA permet la possibilitat de disposar de servidors de rèplica amb l' objectiu de donar alta disponibilitat en el cas que el servidor principal faci fallida. La replicació es realitza a través d' unes polítiques establertes per poder propagar les dades entre els masters i esclaus.



La integració d' un client amb el servidor de FreeIPA es realitza amb la configuració dels components que forment FreeIPA, com són NTP, Kerberos, DNS, NTP i la entitat certificadora. A l' hora d' integrar un client a un domini amb FreeIPA es prepara en el propi client una base de dades anomenada LDB que conté informació dels usuaris, computadors i recursos en format LDAP com també les polítiques en fitxers XML. La base de dades LDB és utilitzada per diferents objectius com el de disposar de la informació en *offline* com també la de donar més eficiència a les consultes de directori.

System Security Services Daemon o SSSD, els clients IPA utilitzen el dimoni sssd el qual dona accés a proveïdors d' autenticació i d' identitat com IdM o FreeIPA. Aquest servei emmagatzema les credencials en la seva caché i permet l'autenticació si el servidor està *offline* i redueix les crides a l'autenticació.

Gestió de renovació de certificats amb Certmonger, el domini IPA gestiona els certificats dels dispositius clients amb un dimoni anomenat certmonger, el qual està executant-se en tots els clients. Aquest dimoni treballa conjuntament amb la entitat certificadora CA de IPA. El seu objectiu es analitzar els certificats per renovar-los en cas de expiració.

3. Treballar amb FreeIPA

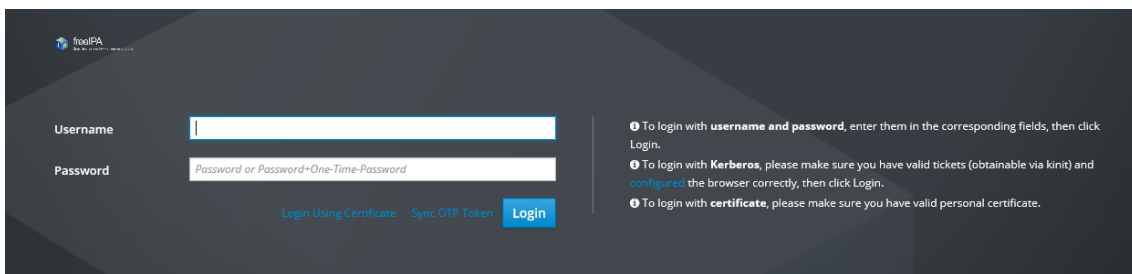
FreeIPA permet la seva administració per una interfície gràfica via web anomenada Web UI o mitjançant línia de comandes CLI. Web UI pot utilitzar-se per administradors de sistemes per la corresponent administració del domini FreeIPA o també per els usuaris amb uns limitats privilegis per poder inicialitzar la seva contrasenya o personalitzar les seves dades.

3.1. Accés per Web UI

L' accés es realitza mitjançant qualsevol navegador certificat amb protocol SSL especificant la URL de qualsevol servidor FreeIPA.

<https://apolo.lab/ipa/ui/>

L' inici de sessió s' efectua inicialment mitjançant Kerberos, si no és possible, l'usuari pot especificar usuari i contrasenya per iniciar sessió.



3.2. Accés per CLI

FreeIPA dona un conjunt de comandes per poder administrar el directori sense tenir que fer us del Web UI. La opció del CLI és molt potent per poder automatitzar tasques i dona molta eficiència a administradors del directori. Qualsevol tasca que es pugui fer en el Web UI es pot efectuar amb el CLI mitjançant la comanda ipa i les comandes ipa-*

Abans d'executar qualsevol d'aquestes comandes és necessari obtenir un tiquet Kerberos mitjançant la comanda `kinit`. En el següent exemple es mostra els usuaris creats en el directori

```
[root@apolo ~]# kinit admin
Password for admin@LAB:

[root@apolo ~]# ipa user-find | grep login
User login: admin
User login: bartuser
User login: lisouser
```

Es possible llistar el conjunt de comandes disponibles per interactuar amb FreeIPA amb la comanda:

```
[root@apolo ~]# ipa help commands
```

I les opcions per cada command amb la següent comanda:

```
[root@apolo ~]# ipa help <command>
```

3.3. Funcionalitats FreeIPA

Les funcionalitats FreeIPA es mostren en la Web UI per la millor claredat dels conceptes. Dins del marc general de configuració es disposa de les característiques d'identitat, política, autenticació, serveis de xarxa i configuració IPA.

Identitat, en el menú d'identitat es poden operar amb els usuaris i grup de domini, addicionalment es poden gestionar els serveis HBAC Host Based Access Control definits en el domini per donar un accés restringit a certes màquines i usuaris.

Política, en aquest menú es poden gestionar les regles dels serveis HBAC, gestionar les regles i comandes SUDO, afegir o modificar la política de contrasenyes de domini i configurar la política de tiquet de Kerberos.

Autenticació, en aquest menú es poden llistar els certificats registrats en IPA, configurar el tipus d' autenticació de doble factor o contrasenyes d' un sol us i configurar servidor d' autenticació RADIUS per la utilització de xarxes wifi

Serveis de xarxa, en aquest menú es permet la configuració de l' automount en IPA i la configuració del servei DNS en el domini.

Configuració IPA, en aquest menú es permet la configuració pròpia del domini IPA com és el cas del nom del domini, les relacions de confiança amb altres dominis, la topologia del domini amb els corresponents rols per a cada servidor IPA i les configuracions globals per el comportament del domini entre altres opcions.

4. Preparació de l' entorn de laboratori

Per veure el funcionament del servei de directori FreeIPA es prepara un entorn de laboratori amb servidors virtuals, l' eina utilitzada de virtualització és Oracle VirtualBox amb la versió 5.2.26.

4.1. Infraestructura de servidors

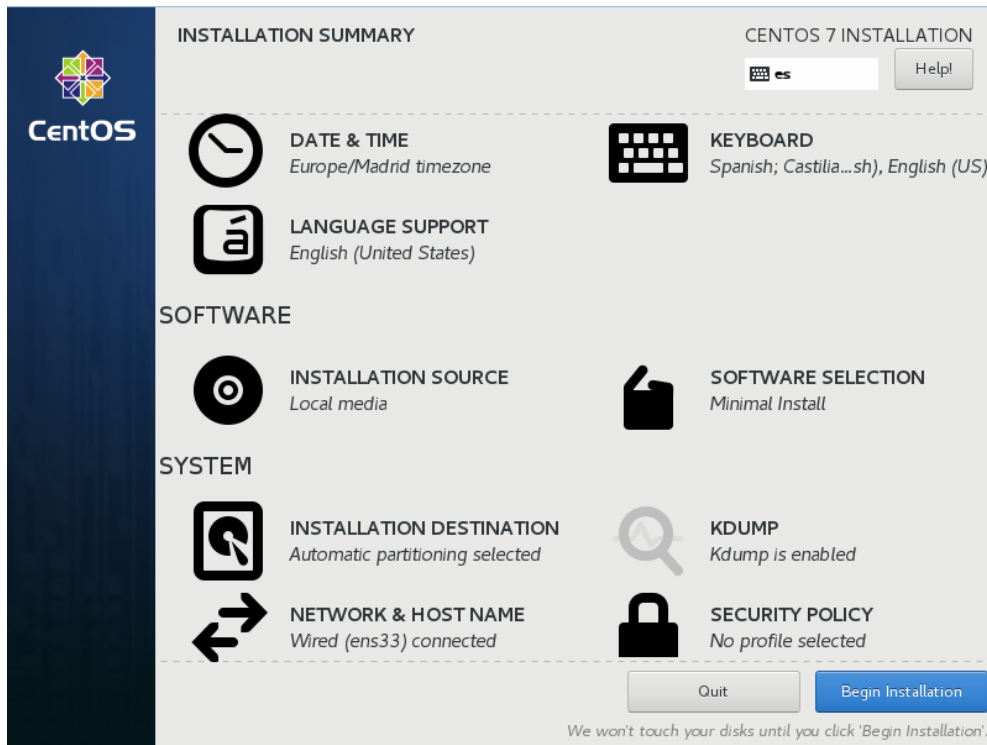
Les màquines virtuals s'han desplegat a partir d'una plantilla amb les distribucions Centos i Fedora amb les corresponents Guest Tools i amb el sistema operatiu instal·lat.

4.1.1. Instal·lació del sistema operatiu CENTOS

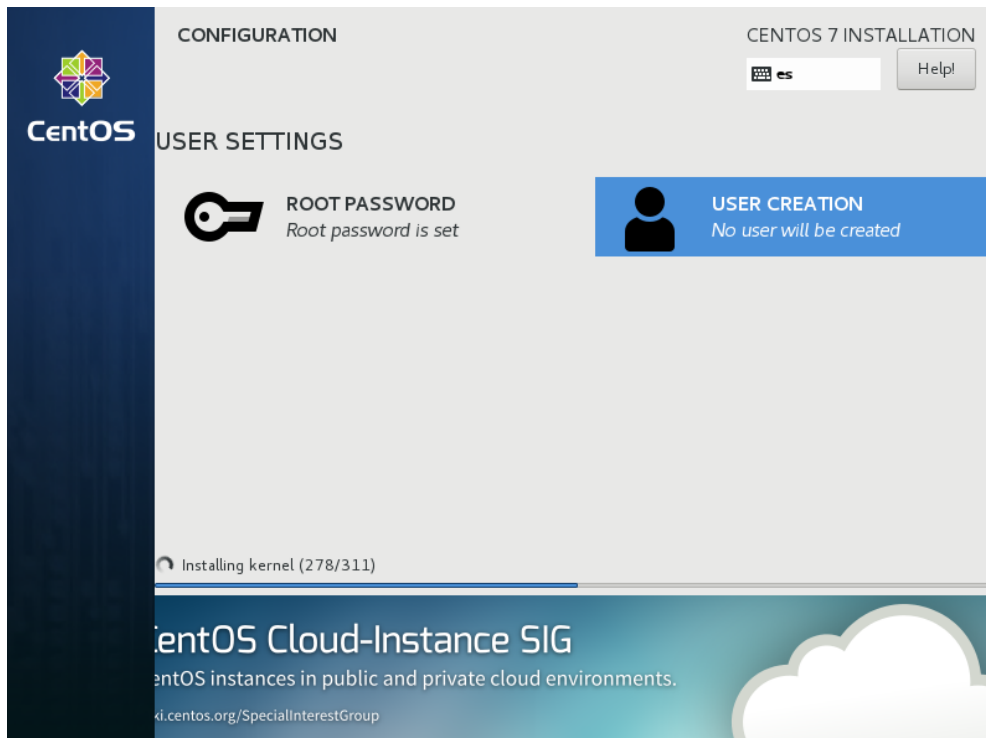
El procés d' instal·lació de la distribució Centos es realitza a partir d' una ISO descarregada des de <https://www.centos.org/download/>. El procés d' instal·lació comença amb la selecció del idioma.



Seguidament, es configura la zona horària, la distribució del teclat i la configuració de xarxa. Entre altres opcions està la de configuració de particions del sistema, en aquest cas es selecciona particionat amb LVM automàtic per el sistema.



Mentre finalitza el procés d'instal·lació hi ha la possibilitat de establir una contrasenya per l'usuari root i poder crear un usuari addicional.



Una vegada finalitza el procés de verificació i instal·lació es reinicia el sistema.

4.1.2. Actualització del sistema

L'actualització del sistema es realitza com usuari root amb la comanda.

```
[root@template ~]# yum update -y
```

Una vegada finalitza el procés de verificació i actualització es reinicia el sistema.

4.1.3. Instal·lació de Guest tools

Les guest tools possibiliten una millor integració del sistema virtual amb la màquina host i afegeix divers millorats per la configuració de xarxa i altres perifèrics. Inicialment, s'instal·la el repositori de paquets *epel* per poder disposar de paquets addicionals RPM que no faciliten els repositoris oficials de Centos:

```
[root@template ~]# rpm -Uvh  
https://dl.fedoraproject.org/pub/epel/epel-release-latest-  
7.noarch.rpm
```

Els paquets necessaris per instal·lar les guest tools son variis.

```
[root@template ~]# yum install perl gcc dkms kernel-devel  
kernel-headers make bzip2
```

Es crea el directori per muntar la imatge de les guest additions:

```
[root@template ~]# mkdir /mnt/cdrom  
[root@template ~]# mount /dev/cdrom /mnt/cdrom
```

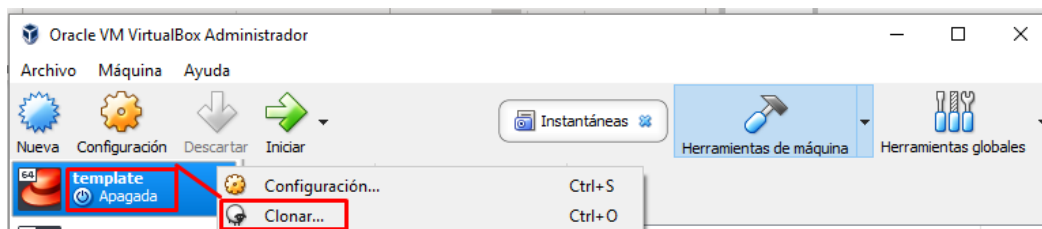
Amb la imatge muntada s'executa el instal·lador:

```
[root@template ~]# ./VBoxLinuxAdditions.run
```

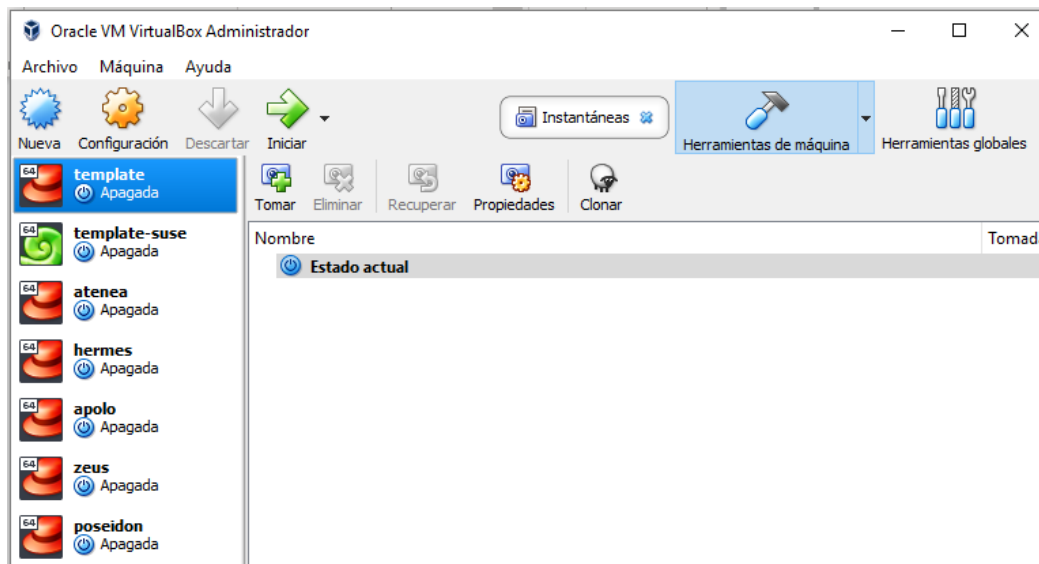
Una vegada finalitza el procés d'instal·lació es recomanable reiniciar el sistema.

4.1.4. Clonació de màquines

Una vegada preparada la plantilla es desplega les màquines virtuals amb el seu corresponent nom en Oracle VirtualBox mitjançant la opció **clone**.



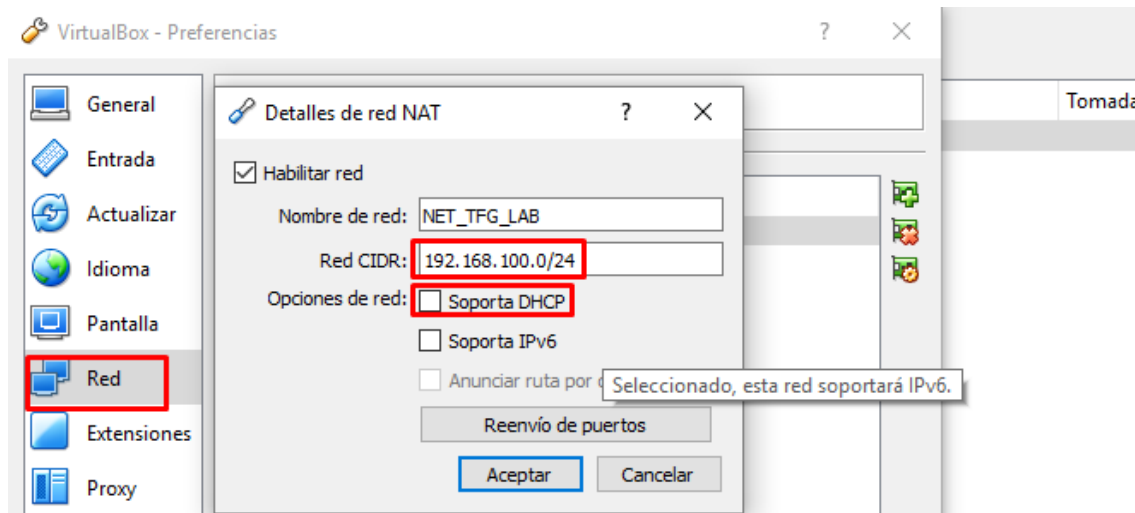
La clonació es necessària per crear totes les màquines virtuals.



4.2. Infraestructura de xarxa

Per minimitzar l'impacte d'interferència entre la xarxa de la màquina host i les màquines virtuals, com és el cas de la col·lisió del servei DHCP i la mobilitat de la màquina host en altres xarxes, es crea una xarxa del tipus Red NAT en Oracle VirtualBox. Amb aquesta xarxa NAT les màquines que la integren tindran visibilitat entre elles però no tindran accés a la xarxa host excepte per la sortida a Internet. Cal dir que amb l'eina de Red NAT d'Oracle VirtualBox es possible realitzar NAT estàtic de la màquina host a les màquines virtuals.

En l'aplicació Oracle VirtualBox es selecciona *Archivo > Preferencias > Red* i es configura una xarxa NAT amb nom *NET_TFG_LAB* sense DHCP ja que el servei DHCP el donaran els servidors corresponents i l'identificador de xarxa *192.168.100.0/24*.



Per el reenviament de ports de la màquina host a les màquines virtuals s'utilitza el *Reenvío de puertos*.

Reglas de reenvío de puertos

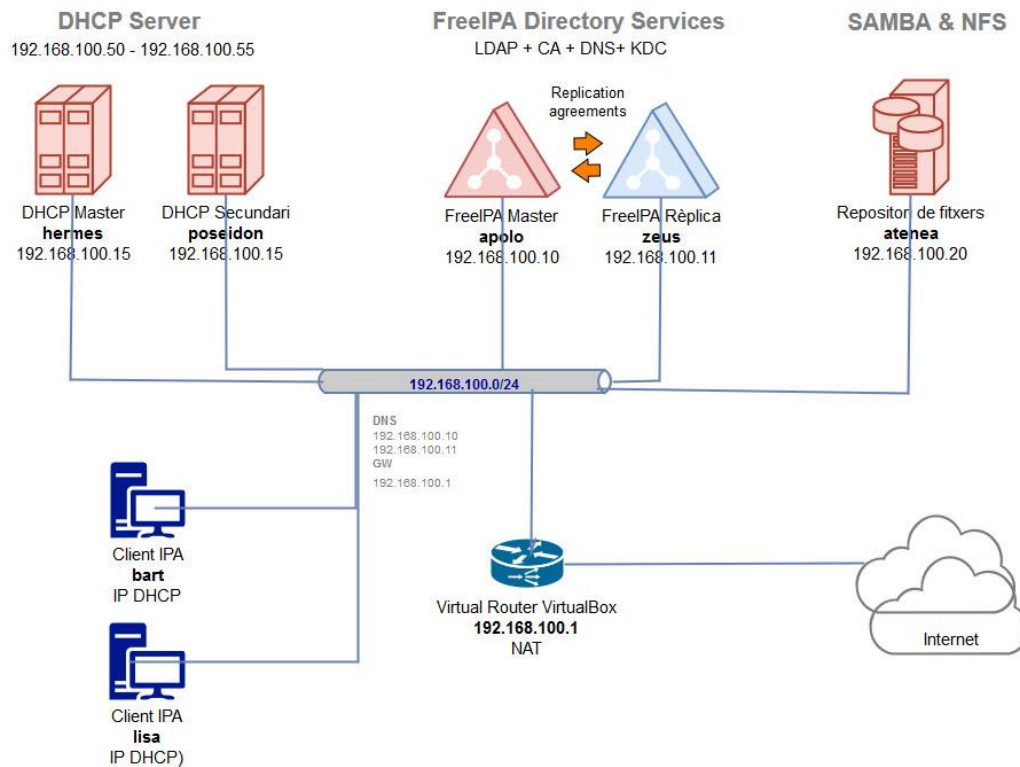
IPv4 IPv6

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
Rule 1	TCP		2210	192.168.100.10	22
Rule 2	TCP		443	192.168.100.10	443
Rule 3	TCP		2215	192.168.100.15	22

4.3. Diagrama de infraestructura

El diagrama d'infraestructura corresponent al domini LAB està format per els servidors corresponents als rols de servidors FreeIPA, DHCP, Repositori de fitxers i clients.

Diagram .LAB domain



Es presenta les característiques dels servidors i la corresponent IP de xarxa.

Nom	Funció	IP	Memòria	vCPU	S.O
Apol·lo	IPA Master	192.168.100.10	2GB	2	Centos 7.6
Zeus	IPA Rèplica	192.168.100.11	2GB	2	Centos 7.6
Hermes	DHCP	192.168.100.15	1GB	2	Centos 7.6
Poseidon	DHCP	192.168.100.16	1GB	2	Centos 7.6
Atenea	Repositori	192.168.100.20	1GB	2	Centos 7.6
Bart	Client	Dinàmica	1GB	2	Fedora
Maggie	Client	Dinàmica	1GB	2	Fedora

5. Servidors IPA

Múltiples servidors FreeIPA poden ser configurats en un domini per poder aportar alta disponibilitat i redundància del servei de directori gràcies a la replicació de la informació i a l'automàtic balanceig en cas de que algun servidor IPA entri en fallada. Aquest balanceig es dona gràcies als registres SRV del DNS del domini els quals donen l'ordre de prioritat dels servidors IPA a consultar. En el cas que el servidor master entri en fallada, el registre SRV adreçarà del següent servidor IPA de la llista.

En la topologia de directori existeix un servidor IPA master que correspon al primer en la topologia i els servidors IPA addicionals anomenats rèpliques del master. Tant el servidor master com les rèpliques comparteixen les mateixes dades d'usuaris, certificats i recursos de xarxa mitjançant acords de replicació. Encara que els servidors IPA poden donar els serveis de DNS, NTP i CA conjuntament es possible que puguin obviar aquests serveis delegant-los a un altre controlador de domini. És important conèixer que en els dominis de FreeIPA existeixen nivells funcionals que indiquen si un domini té disponible certes operacions.

Automàticament, en les versions que s'utilitzen en aquest laboratori, el nivell funcional del primer servidor que s'instal·la és el nivell 1. Una vegada elevat el nivell funcional no es pot revertir aquest canvi.



La versió de FreeIPA utilitzat en les proves de l'entorn de laboratori és la **4.6.4**.

5.1. Requeriments dels servidors IPA

Es presenta una llista amb els requeriments necessaris per preparar el servidor de FreeIPA.

- Mínim de 2GB de RAM (1GB Swap).
- Llista de serveis oberts al Firewall
 - HTTP, HTTPS (TCP 80,443)
 - LDAP, LDAPS (TCP 389,636)
 - Kerberos (TCP i UDP 88, 864)
 - DNS (TCP i UDP 53)
 - NTP (UDP 123)
 - Dogtag CA (TCP 7389)

- Les versions IPA del master i rèplica han de ser les mateixes.
- El servidor IPA rèplica no pot utilitzar el port 7389 perquè és el port utilitzat per comunicar els acords de replicació.
- Els ports 9443, 9444 i 9445 són necessaris per la configuració entre el master i la rèplica.

5.2. Preparació de servidors apolo.lab i zeus.lab

La preparació dels servidor FreeIPA del laboratori corresponents a apolo.lab com servidor master i zeus.lab com rèplica es compon per la configuració de xarxa, el nom de servidor, la configuració DNS, configuració arxiu hosts local, configuració del firewall i la instal·lació de FreeIPA.

Configuració de xarxa, és obligatori establir una IP privada i estàtica als servidors FreeIPA i desactivar el servei DHCP. Per fer aquest canvi i que sigui permanent es necessari modificar el fitxer `/etc/sysconfig/network-scripts/ifcfg-enp0s3` i establir les directives `BOOTPROTO`, `IPADDR`, `GATEWAY`, `NETMASK` i `ONBOOT` de la següent manera.

apolo.lab	zeus.lab
TYPE="Ethernet" BOOTPROTO="static" IPADDR=192.168.100.10 GATEWAY=192.168.100.1 NETMASK=255.255.255.0 NAME="enp0s3" DEVICE="enp0s3" ONBOOT="yes"	TYPE="Ethernet" BOOTPROTO="static" IPADDR=192.168.100.11 GATEWAY=192.168.100.1 NETMASK=255.255.255.0 NAME="enp0s3" DEVICE="enp0s3" ONBOOT="yes"

Desactivació de Network Manager, per recomanacions de les pàgines oficials de Fedora i Redhat es desactiva el servei Network Manager perquè s'informa que pot causar problemes en el funcionament entre FreeIPA i Kerberos, s'utilitza la comanda `systemctl` per aquest propòsit.

```
systemctl stop NetworkManager
systemctl disable NetworkManager
```

Especificar nom de servidor, per poder distingir el servidor es necessari establir un nom el qual serà el que s'utilitzi en la resolució DNS per el funcionament del directori, s'utilitza la comanda `hostnamectl` per aquest propòsit.

```
hostnamectl set-hostname apolo.lab
hostnamectl set-hostname zeus.lab
```

Configurar client DNS, per poder realitzar les resolucions de noms de domini es necessari configurar els clients DNS correctament, temporalment es configuren amb uns servidors externs per poder descarregar els binaris de FreeIPA. Es veurà en passos posteriors com aquests servidors s'establiran com reenviadors i els servidors FreeIPA seran els servidors DNS del directori. Es modificar el fitxer de sistema `/etc/resolv.conf` per aconseguir aquest propòsit.

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```


Configurar el fitxer hosts, per la resolució interna de noms i no tenir que dependre d'un servidor DNS extern es configura el fitxer `/etc/hosts` solament en els servidors FreeIPA. S'edita el fitxer `/etc/hosts` amb el següent contingut en els corresponents servidors `apolo.lab` i `zeus.lab`.

En `apolo.lab`,

```
127.0.0.1          localhost          localhost.localdomain
::1               localhost
192.168.100.10    apolo.lab
```

En `zeus.lab`,

```
127.0.0.1          localhost          localhost.localdomain
::1               localhost
192.168.100.11    zeus.lab
```

Configurar Firewall de sistema operatiu, es necessari donar accés als ports necessaris a cada un dels servidors `apolo.lab` i `zeus.lab` des de les xarxes necessàries per disposar d'un correcte funcionament del servei FreeIPA. S'utilitza la comanda `firewall-cmd` del servei `firewalld` per aconseguir aquest objectiu.

```
firewall-cmd --zone=public --permanent --add-service=https
firewall-cmd --zone=public --permanent --add-service=http
firewall-cmd --zone=public --permanent --add-service=ldaps
firewall-cmd --zone=públic --permanent --add-service=ldap
firewall-cmd --zone=public --permanent --add-service=kerberos
firewall-cmd --zone=public --permanent --add-port=53/tcp
firewall-cmd --zone=public --permanent --add-port=53/udp
firewall-cmd --zone=public --permanent --add-service=ntp
firewall-cmd --zone=public --permanent --add-port=464/tcp
firewall-cmd --zone=public --permanent --add-port=464/udp
firewall-cmd --zone=public --permanent --add-port=9443/tcp
firewall-cmd --zone=public --permanent --add-port=9444/tcp
firewall-cmd --zone=public --permanent --add-port=9445/tcp
firewall-cmd --zone=public --permanent --add-port=7389/tcp
```

El port TVP 7389 és utilitzat per la comunicació entre el servidor IPA master i els de IPA rèplica per replicar els acords de replicació.

Instal·lació de IPA master, el procés d'instal·lació es realitza amb la comanda `yum` la qual gestiona els repositoris oficials de Centos per realitzar instal·lacions de paquets en el sistema. El paquet per instal·lar IPA és `ipa-server` i `bind-dyndb-ldap`. En el servidor `apolo.lab` s'utilitza la següent comanda.

```
[root@apolo ~]# yum install ipa-server ipa-server-dns bind-dyndb-ldap -y
```

Una vegada la instal·lació dels paquets finalitza, s'executa la comanda de instal·lació de IPA.

```
[root@apolo ~]# ipa-server-install
```

El procés d'instal·lació pot ser interactiu o desatès. En el servidor `apolo.lab` es realitza el procés interactiu el qual realitza les preguntes bàsiques de configuració.

- Integració del directori amb DNS. El qual es respon a **YES**.
- `hostname` del master. El qual es respon a **apolo.lab**.
- Nom de domini. Es respon **lab**.
- Nom del reinat de Kerberos realm. Es respon **LAB**.
- Credencials administració IPA i del administració del directori.
- Configuració del DNS forwarders. Es respon a **YES** amb els DNS de Google **8.8.8.8** i **8.8.4.4**. Aquests servidors seran utilitzats per el directori per realitzar la resolució de noms de les zones en les que no es tingui autoritat.
- Configuració de la zona reversa. Es respon a **YES**.

Les operacions de la instal·lació es registren en `/var/log/ipaserver-install.log`. És important tenir en compte que el certificat de CA utilitzat per crear les rèpliques és el `/root/cacert.p12` el qual s'ha de tenir resguardat.

Instal·lació de FreeIPA rèplica, el procés d' instal·lació de IPA rèplica en zeus.lab, igual que en el servidor IPA master apolo.lab, és la instal·lació dels paquets ipa-server i bind-dyndb-ldap. Una vegada finalitzada la instal·lació es promociona a zeus.lab en un client IPA.

```
[root@zeus ~]# ipa-client-install
```

El propi programa realitza un descobriment del servidor IPA master existent i demana les credencials de l' usuari administrador de directori admin per unir el nou servidor en el domini. Aquest procés incorpora la configuració implícita del serveis sssd, nsswitch i Kerberos corresponents als fitxers de configuració /etc/sssds/sssds.conf, /etc/nsswitch.conf i /etc/krb5.conf respectivament. El següent pas és afegir a zeus.lab al grup de servidors IPA amb la següent comanda des de apolo.lab.

```
[root@apolo ~]# kinit admin
[root@apolo ~]# ipa hostgroup-add-member ipaservers --hosts
zeus.lab
```

S'afegeix el registre PTR de 192.168.100.11 corresponent a zeus.lab des del GUI i s'executa la comanda de instal·lació de rèplica en zeus.lab.

```
[root@zeus ~]# ipa-replica-install --setup-dns --setup-ca
```

És possible la instal·lació de la rèplica sense els rols de DNS i CA i instal·lar-los posteriorment amb les següent comandes.

```
[root@zeus ~]# ipa-dns-install
[root@zeus ~]# ipa-ca-install
```

En el cas de voler desinstal·lar un servei de IPA server en qualsevol dels servidors es pot utilitzar la següent comanda.

```
[root@zeus ~]# ipa-server-install --uninstall
```

5.3. Administració de les rèpliques

La informació del directori LDAP, claus, configuració de polítiques i certificats es propaguen amb coherència entre els servidors IPA mitjançant la replicació. A l'hora de crear una rèplica es generen acords de replicació bidireccional entre el servidor IPA master amb els servidors IPA rèplica. La topologia de replicació crea un conjunt de servidors IPA el qual aporta funcions d'alta disponibilitat i tolerància a errors. Cal tenir present que la replicació bidireccional es genera per defecte entre el servidor master i els de rèplica i no entre rèpliques. En cas de necessitat de replica entre rèpliques seria necessari crear acords de replicació.

Entre les tasques més importants d'administració de rèpliques en un domini amb IPA es la de llistar i consultar l'estat de les rèpliques, crear i eliminar acords de replicació, forçar la replicació o reinicialitzar dades de replicació d'un servidor.

La comanda de sistema operatiu utilitzada per aconseguir aquestes funcions és `ipa-replica-manage`. Cal tenir present que es necessari obtenir un ticket kerberos amb la comanda `kinit` per utilitzar aquestes comandes.

Llistar i consultar l'estat de les rèpliques, la consulta de la topologia de replicació entre servidors es pot recuperar amb la comanda següent:

```
[root@apolo ~]# ipa-replica-manage list
zeus.lab: master
apolo.lab: master
```

Es possible llistar la llista d'acords de replicació d'un servidor concret amb la comanda següent:

```
[root@apolo ~]# ipa-replica-manage list apolo.lab
zeus.lab: replica
```

En el cas de necessitar més informació, és possible amb ajuda del flag `-v`

```
[root@apolo ~]# ipa-replica-manage list apolo.lab
last init status: None
last init ended: 1970-01-01 00:00:00+00:00
last update status: Error (0) Replica acquired successfully:
Incremental update succeeded
last update ended: 2019-05-03 07:22:35+00:00
```

Crear acords de replicació entre rèpliques, és possible crear acords de replicació entre rèpliques. Aquesta connexió entre rèpliques es pot realitzar mitjançant LDAP xifrat o no xifrat. En el cas hi hagués una tercera rèplica anomenada hercules.lab, la creació de l' acord de replicació entre zeus.lab i hercules.lab seria la següent:

```
[root@apolo ~]# ipa-replica-manage connect zeus.lab hercules.lab
```

Eliminar acords de replicació entre rèpliques, per poder eliminar l' acord entre el servidor IPA rèplica zeus.lab i hercules.lab creada en l' exemple anterior s'utilitza la comanda següent:

```
[root@apolo ~]# ipa-replica-manage disconnect zeus.lab
hercules.lab
```

En els anteriors casos s' elimina i es creen acords de replicació entre servidors IPA però aquests servidors continuen existint en la topologia de replicació. Si es necessita eliminar les dades d' un servidor es pot realitzar amb la comanda següent:

```
[root@apolo ~]# ipa-replica-manage del hercules.lab
```

Forçar replicació manualment, existeix la possibilitat de poder forçar la replicació en el cas que s' hagi d' aturar algun servidor IPA degut a un manteniment amb la que seria convenient forçar la replicació manualment. En el cas necessari d' aturar el servidor zeus.lab es podria forçar de la següent manera:

```
[root@apolo ~]# ipa-replica-manage force-sync --from zeus.lab
```

Reinicialitzar la informació de rèplica, en cas que la base de dades interna d'una rèplica estigui en estat corrupte o si ha estat en *offline* durant molt de temps es possible reinicialitzar la informació amb la còpia actual i en bon estat d'una altra rèplica. En cas necessari de reinicialitzar la informació de zeus.lab des de apolo.lab es pot realitzar la comanda següent:

```
[root@zeus ~]# ipa-replica-manage re-initialize --from apolo.lab
```

5.4. Creació de usuaris i grups de domini

La principal funcionalitat de IPA és la gestió dels usuaris en una ubicació centralitzada la qual permet el login centralitzat dels usuaris de domini. A més del inici de sessió amb usuari i contrasenya, IPA permet autenticar-se mitjançant certificats SSH, servidors RADIUS, contrasenyes d'un sol us OTP i tickets Kerberos. La creació d'usuari i grups es pot realitzar a través de WebUI o a través de CLI a través d'aquestes comandes:

Creació del grup gs_finances:

```
[root@apolo ~]# ipa group-add --desc='Finances' gs_finances
```

Creació del usuari maggiuser:

```
[root@apolo ~]# ipa user-add maggiuser --homedir=/home/maggie  
--first=Maggie --last=Simpson -password
```

Afegir usuari maggie dins de gs_finances:

```
[root@apolo ~]# ipa group-add-member gs_finances --  
users=maggiuser
```

Amb les anteriors comandes, el identificador únic d'usuari i grup UID i GID respectivament són creats automàticament seguint un autonumèric definit en el rang de UID. Aquest rang es pot consultar des de WebUI o CLI a través de la comanda `ipa range-find`.

El tipus d'autenticació es com `password`, `otp` o `RADIUS` es pot especificar amb la opció `--user-auth-type` i es pot pujar una clau pública SSH amb la opció `-shpubkey`.

5.5. Administració sudo

La delegació de funcions a usuaris o grups és una necessitat per millorar la administració i gestió del domini. En certes ocasions és necessari permetre la execució de certes comandes a certs usuaris no administradors per poder delegar tasques.

`sudo` treballa amb un fitxer de configuració local `/etc/sudoers` el qual es pot indicar comandes i grup de comandes per realitzar la delegació de tasques però no hi ha una manera eficient per poder compartir aquests fitxers en un domini IPA, d'aquesta manera la informació de regles, grup de comandes i comandes `sudo` s'emmagatzemen en el directori LDAP per centralitzar aquesta informació.

Una regla `sudo` especifica qui pot fer què, on ho podrà fer i com ho farà i és necessari especificar comandes o grup de comandes creades anteriorment. La configuració `sudo` en un domini IPA es pot realitzar a través de WebUI o a través de CLI. El següent exemple mostra com l'usuari `bartuser` pot utilitzar el grup de comandes per llegir fitxers de totes les màquines del domini, en primer lloc s'especifiquen les comandes:

```
[root@apolo ~]# ipa sudocmd-add --desc=tail /usr/bin/tail
[root@apolo ~]# ipa sudocmd-add --desc=less /usr/bin/less
[root@apolo ~]# ipa sudocmd-add --desc=cat /usr/bin/cat
```

Es crea el grup de comandes readfiles per llegir fitxers:

```
[root@apolo ~]# ipa sudocmdgroup-add readfiles --desc='Read Files'
```

S'afegeix les comandes cat, tail i less dins del grup readfiles:

```
[root@apolo ~] ipa sudocmdgroup-add-member readfiles --
sudocmds=/usr/bin/cat
[root@apolo ~] ipa sudocmdgroup-add-member readfiles --
sudocmds=/usr/bin/less
[root@apolo ~] ipa sudocmdgroup-add-member readfiles --
sudocmds=/usr/bin/tail
```

Finalment es crea la regla sudo:

```
[root@apolo ~] ipa sudorule-add read-files
```

S'assigna en la regla el grup de comandes necessàries:

```
[root@apolo ~] ipa sudorule-add-allow-command read-files --
sudocmdgroups=readfiles
```

S'assigna el grup gs_it per poder gaudir d'aquestes comandes en el domini com usuari root.

```
[root@apolo ~] ipa sudorule-add-user read-files --groups=gs_it
```


6. Servidors DHCP

El servei DHCP *Dynamic Host Configuration Protocol* és un protocol que té com objectiu donar automàticament adreces IP i altres paràmetres de xarxa a clients. Un servidor DHCP facilita la configuració automàtica de xarxa als dispositius clients d'una xarxa, això implica que no és necessari configurar la xarxa



manualment als diferents dispositius. El software utilitzat per realitzar la instal·lació i configuració del servei de DHCP és **kea 1.5.0**, desenvolupat per el Internet System Consortium ISC. La

implementació del servei DHCP és important per completar el funcionament del directori amb FreeIPA ja que per completar la identitat del host amb DHCP cal integrar el servei DHCP amb l' arbre de LDAP.

6.1. Preparació de servidors hercules.lab i poseidon.lab

La preparació del servidor DHCP corresponent a hermes.lab com servidor es compon per la configuració de xarxa, el nom de servidor, la configuració DNS, configuració del firewall i la instal·lació del servei DHCP kea.

Configuració de xarxa, és obligatori establir una IP privada i estàtica al servidor DHCP i desactivar el servei DHCP al propi servidor. Per fer aquest canvi i que sigui permanent es necessari modificar el fitxer `/etc/sysconfig/network-scripts/ifcfg-enp0s3` i establir les directives `BOOTPROTO`, `IPADDR`, `GATEWAY`, `NETMASK` i `ONBOOT` de la següent manera.

```
TYPE="Ethernet"
BOOTPROTO="static"
IPADDR=192.168.100.15
GATEWAY=192.168.100.1
NETMASK=255.255.255.0
NAME="enp0s3"
DEVICE="enp0s3"
ONBOOT="yes"
```

Especificar nom de servidor, per poder distingir el servidor es necessari establir un nom el qual serà el que s' utilitzi en la resolució DNS per el funcionament del directori, s' utilitza la comanda `hostnamectl` per aquest propòsit.

```
hostnamectl set-hostname hermes.lab
```

Configurar client DNS, per poder realitzar les resolucions de noms de domini es necessari configurar els clients DNS correctament. Els corresponents DNS seran els servidors IPA que formen el directori . Es modifica el fitxer de sistema `/etc/resolv.conf` per aconseguir aquest propòsit.

```
nameserver 192.168.100.10  
nameserver 192.168.100.11
```

Configurar Firewall de sistema operatiu, es necessari donar accés als ports necessaris des de les xarxes necessàries per disposar d'un correcte funcionament del servei DHCP. S'utilitza la comanda `firewall-cmd` del servei `firewalld` per aconseguir aquest objectiu.

```
firewall-cmd --zone=public --permanent --add-service=dhcp
```

La instal·lació del servei DHCP s' explica en el següent secció.

6.2. Instal·lació servei DHCP

La instal·lació es realitza amb la descarrega del codi font amb la corresponent compilació i instal·lació del software. Cal tenir present que la instal·lació per paquets RPM des de Centos no està disponible i com s'ha comentat la instal·lació es realitza amb la compilació del software kea.

“This page documents Kea 1.5 installation on CentOS and RedHat version 7. Unfortunately, rpm install is not available for any current version of Kea.” (Internet Systems Consortium)

6.2.1. Compilació, instal·lació de codi font

La instal·lació es realitza seguint el manual oficial (Internet Systems Consortium) Per poder disposar de les eines necessàries per la compilació del codi font del servei DHCP kea és imprescindible instal·lar les dependències necessàries amb la comanda yum.

```
[root@hermes ~]# yum install wget gcc gcc-c++ openssl openssl-  
devel log4cplus-devel -y
```

Es descarrega el codi font, es descomprimeix i s'accedeix en la carpeta descomprimida:

```
[root@hermes ~]# wget https://www.isc.org/downloads/file/kea-1-  
5-0/?version=tar-gz  
[root@hermes ~]# tar -zxvf /root/kea-1.5.0.tar.gz  
[root@hermes ~]# cd /root/kea-1.5.0
```

Es validen dels requeriments del programa per compilar i instal·lar:

```
[root@hermes ~]# ./configure --with-openssl
```

Una vegada la comanda anterior ens doni una correcta validació es procedeix a la compilació del codi amb la utilitat make:

```
[root@hermes ~]# make
```

Posteriorment, s'instal·la i es col·loca els binaris en les corresponents carpetes del PREFIX:

```
[root@hermes ~]# make install
```

6.2.2. Configuració servei DHCP

La configuració del servei DHCP kea es realitza mitjançant els propis fitxers de configuració ubicats en `/usr/local/etc/`. Inicialment, es modifica el fitxer corresponent al servei DHCP IPv4 `/usr/local/etc/kea-dhcp4.conf`. Cal posar èmfasi en les següents clàusules:

La clàusula `interfaces-config` es fixa a la interfície de xarxa que dona el servei de DHCP en la xarxa del domini LAB:

```
"interfaces-config": {  
    "interfaces": [ "enp0s3" ]  
},
```

La clàusula `lease-database` defineix quina base de dades s'utilitzarà per emmagatzemar la informació d'adreces IP cedides per el servei DHCP, en el nostre cas s'utilitza un fitxer local.

```
"lease-database": {  
    "type": "memfile",  
}
```

La clàusula `option-data` especifica al servei DHCP quins són els servidors DNS que haurà de proporcionar als clients DNS, en el nostre cas son `192.168.100.10` i `192.168.100.11`. Addicionalment, s'especifica la informació del TLD de domini del directori, en el nostre cas és `lab`.

```
"option-data": [  
  {  
    "name": "domain-name-servers",  
    "data": "192.168.100.10,192.168.100.11"  
  }  
  {  
    "name": "domain-search",  
    "data": "lab"  
  }  
]
```

La clàusula `subnet` especifica la xarxa on es facilitaran les adreces IP com el rang vàlid acceptat, en el nostre cas el servei DHCP facilita 6 adreces corresponents al rang 192.168.100.50 al 192.168.100.55.

```
"subnet4": [  
  {  
    "subnet": "192.168.100.0/24",  
    "pools": [{ "pool": "192.168.100.50 - 192.168.100.55" } ],  
  }  
]
```

Finalment, el servei DHCP dona la informació del routers per configurar als clients DHCP el seu gateway, 192.168.100.1.

```
"option-data": [  
  {  
    "name": "routers",  
    "data": "192.168.100.1"  
  }  
]
```

6.2.3. Arranc automàtic servei DHCP

L'arranc automàtic del servei per el DHCP per IPv4 i el servei de actualització dinàmica de DNS és necessari per el funcionament correcte del servei de DHCP de la xarxa del domini LAB. Per afegir l'arranc automàtic s'utilitza el conjunt de

dimonis systemd. Es crea el fitxer de servei en `/etc/systemd/system/kea-dhcp4.service` per iniciar automàticament el servei DHCP per adreces IPv4 amb els següent contingut:

```
[Unit]
Description=Kea DHCPv4 Server
Documentation=man:kea-dhcp4(8)
Wants=network-online.target
After=network-online.target
After=time-sync.target

[Service]
ExecStart=/usr/local/sbin/kea-dhcp4 -c /usr/local/etc/kea/kea-dhcp4.conf

[Install]
WantedBy=multi-user.target
```

Es crea el fitxer de servei en `/etc/systemd/system/kea-dhcp-ddns.service` per iniciar automàticament el servei DHCP d'actualització dinàmica amb els següent contingut:

```
[Unit]
Description=Kea DHCP-DDNS Server
Documentation=man:kea-dhcp-ddns(8)
Wants=network-online.target
After=network-online.target
After=time-sync.target

[Service]
ExecStart=/usr/local/sbin/kea-dhcp-ddns -c /usr/local/etc/kea/kea-dhcp-ddns.conf

[Install]
WantedBy=multi-user.target
```

Seguidament, s'activen els serveis amb la comanda `systemctl` i s'inicia el servei:

```
[root@hermes ~]# systemctl enable kea-dhcp4.service
```

```
[root@hermes ~]# systemctl start kea-dhcp4.service
```

Per comprovar l'estat de funcionament del servei es poden utilitzar les següents comandes:

```
[root@hermes ~]# keactrl status  
[root@hermes ~]# systemctl status kea-dhcp4.service
```

6.3. Actualització DDNS

L'actualització dinàmica de DNS DDNS té l'objectiu de refrescar la informació dels noms del domini amb la IP que correspon a cada client, d'aquesta manera si hi ha clients que obtenen l'adreça IP de un DHCP amb la característica de DDNS la resolució del nom dels clients sempre estarà actualitzada amb la IP correcta.

Els clients IPA envien actualitzacions DNS quan es compleixen les següents :

- Clients integrats amb el domini IPA corresponent.
- Zona DNS configurada amb actualització dinàmica.
- Clients integrats amb IPA amb el flag `--enable-dns-updates`.

Zona DNS configurada amb DDNS, per habilitar la actualització dinàmica de DNS en la zona es pot realitzar per WebUI o per línia de comandes, per defecte està habilitada en la zona principal però no s'activa en les zones noves.

Mitjançant WebUI cal dirigir-se a la opció :

Network Services > Zona DNS > Seleccionar domini > Configuració > Seleccionar habilitar DDNS.

Actualización dinámica	<input checked="" type="radio"/> Verdad <input type="radio"/> Falso
Política de actualización de BIND	<pre>grant LAB krb5-self * A; grant LAB krb5-self * AAAA; grant LAB krb5-self * SSHFP;</pre>

Mitjançant línia de comandes s'aconsegueix amb la comanda:

```
[root@apolo ~]$ ipa dnszone-mod lab. --dynamic-update=TRUE
```

Clients integrats al domini amb DDNS, la integració dels clients al domini IPA realitzat amb la comanda `ipa-client-install` realitza automàticament la DDNS, es pot marcar explícitament amb la següent comanda:

```
[root@bart ~]$ ipa-client-install --enable-dns-updates
```


7. Servidors Samba i NFS

El servei de repositori de fitxers de xarxa és un servei imprescindible en una xarxa d'ordinadors on usuaris de diferents departaments intercanvien documents i treballen en equip. Els serveis més utilitzats en GNU/Linux són Samba i NFS.

Samba, Samba és un conjunt de serveis i protocols que dona servei de fitxers, servei d'impressores, autenticació, autorització, descobriment de recursos i resolució de noms NetBios. Samba implementa els SMB Server Message Block i CIFS Common Internet File System els quals tenen l'objectiu de poder intercanviar fitxers entre ordinadors en una xarxa LAN.

El servei Samba està gestionat per dos dimonis, el dimoni `smbd` el qual gestiona el servei de fitxers, servei d'impressores i autenticació i el dimoni `nmbd` el qual gestiona el de descobriment de recursos i NetBIOS.

La implementació del protocol SMB permet a clients de Windows poder accedir a directoris compartits per un servidor GNU/Linux d'una manera transparent.

Amb relació a la seguretat, Samba utilitza autenticació per contrasenya i pot emmagatzemar la seva base de dades per LDAP o en un fitxer local, addicionalment Samba es pot integrar en entorn Kerberos per millorar la seguretat de la xarxa.

NFS Network File System, NFS és un protocol que va ser creat per SUN Microsystems i té el mateix objectiu que SMB que és la d'intercanvi de fitxers entre ordinadors en una xarxa LAN. El protocol d'intercanvi de fitxers NFS és utilitzat en sistemes que són puraments Unix ja que és incompatible amb el protocol SMB.

El servidor NFS s'implementa amb dos serveis de xarxa anomenats `mountd` i `nfsd`. El servei `mountd` té l'objectiu de comprovar que el muntatge de fitxers realitzat per un client és vàlid. El servei `nfsd` es dedica a atendre les peticions d'accés a fitxers i directoris del muntatge.

En una xarxa on convisin sistema Microsoft Windows i sistemes Unix pot ser necessari disposar d'un sistema d'intercanvi de fitxers de SMB per poder

compartir documents d' una manera transparent, cal tenir en compte, per això, que en entorns purament Unix el sistema de compartició més eficient és NFS.

Amb relació a la seguretat, el protocol NFS es protegeix per permissions d' adreces IP i per els permisos dels fitxers i directoris. Per protegir d' una manera més segura un entorn amb NFS és possible integrar-lo amb Kerberos.

En el entorn de laboratori es prepara i es configura el servei Samba i NFS en el servidor atenea.lab.

7.1. Preparació servidor atenea.lab

La preparació del servidor Samba i NFS corresponent a atenea.lab com servidor es compon per la configuració de xarxa, el nom de servidor, la configuració DNS, configuració del firewall i la instal·lació de Samba i NFS.

Configuració de xarxa, és obligatori establir una IP privada i estàtica al servidor Samba i NFS i desactivar el servei DHCP al propi servidor. Per fer aquest canvi i que sigui permanent es necessari modificar el fitxer `/etc/sysconfig/network-scripts/ifcfg-enp0s3` i establir les directives BOOTPROTO, IPADDR, GATEWAY, NETMASK i ONBOOT de la següent manera.

```
TYPE="Ethernet"  
BOOTPROTO="static"  
IPADDR=192.168.100.20  
GATEWAY=192.168.100.1  
NETMASK=255.255.255.0  
NAME="enp0s3"  
DEVICE="enp0s3"  
ONBOOT="yes"
```

Especificar nom de servidor, per poder distingir el servidor es necessari establir un nom el qual serà el que s' utilitzi en la resolució DNS per el funcionament del directori, s' utilitza la comanda `hostnamctl` per aquest propòsit.

```
hostnamectl set-hostname atenea.lab
```

Configurar client DNS, per poder realitzar les resolucions de noms de domini es necessari configurar els clients DNS correctament. Els corresponents DNS seran els servidors IPA que formen el directori. Es modifica el fitxer de sistema `/etc/resolv.conf` per aconseguir aquest propòsit.

```
nameserver 192.168.100.10
nameserver 192.168.100.11
```

Configurar Firewall de sistema operatiu, es necessari donar accés als ports necessaris des de les xarxes necessàries per disposar d'un correcte funcionament del servei DHCP. S'utilitza la comanda `firewall-cmd` del servei `firewalld` per aconseguir aquest objectiu.

```
firewall-cmd --zone=public --permanent --add-service=samba
firewall-cmd --zone=public --permanent --add-service=nfs
firewall-cmd --zone=public --permanent --add-service=rpc-bind
```

Integració de servidor atenea.lab al domini, per disposar de les avantatges d'autorització i autenticació amb Kerberos en el servei de directori. Per poder realitzar aquesta operació s'instal·la i s'executa el client IPA:

```
[root@atenea ~]# yum -y install ipa-client
```

Seguidament s'executa el binari de IPA client i s'integra en domini amb la característica de creació de home de usuaris activada:

```
[root@atenea ~]# ipa-client-install --mkhomedir
Discovery was successful!
...
Enrolled in IPA realm LAB
...
The ipa-client-install command was successful
```

La instal·lació i configuració dels serveis Samba i NFS s'expliquen en la següent secció.

7.2. Instal·lació i configuració dels serveis

El servei de Samba i NFS poden venir integrats en GNU/Linux, en el cas que no es disposin dels paquets instal·lats es poden instal·lar amb el gestor de paquets yum.

7.2.1. Procés d'instal·lació

Per la instal·lació de Samba és necessari instal·lar les llibreries necessàries, s'utilitza el gestor de paquets yum amb les següents comandes:

```
[root@atenea ~]# yum -y install samba samba-client sssd-libwbclient
```

Per altra banda, per la instal·lació del servei NFS s'executa:

```
[root@atenea ~]# yum -y install nfs-utils
```

7.2.2. Configuració de serveis Kerberitzats

Des d'un servidor IPA es realitza una petició Kerberos a l'administrador del directori i s'activa el servei Samba i NFS especificant el servidor atenea.lab:

```
[root@apolo ~]# kinit admin
[root@apolo ~]# ipa service-add cifs/atenea.lab
[root@apolo ~]# ipa service-add nfs/atenea.lab
```

Es crea una key Kerberos associada als serveis anteriorment creats de Samba i NFS amb la comanda ipa-getkeytab. Aquesta comanda s'executa des del servidor atenea.lab especificant un servidor IPA i la ubicació on s'emmagatzemarà el keytab de Samba i NFS.

```
[root@atenea ~]# ipa-getkeytab -s apolo.lab -p cifs/atenea.lab -k /etc/samba/samba.keytab
[root@atenea ~]# ipa-getkeytab -s apolo.lab -p nfs/atenea.lab -k /etc/krb5.keytab
```

7.2.3. Configuració de servei Samba

El fitxer de configuració de Samba s'ubica per defecte en `/etc/samba/smb.conf`. En aquest fitxer de configuració és on es configura el comportament general del servei.

En la secció `global` s'indica la configuració general del servei, en el nostre cas s'indica el fitxer de keytab generat anteriorment amb el mètode d'autenticació Kerberos, addicionalment s'especifica el nom del domini `lab` i el tipus de seguretat a `user`.

```
[global]
    client signing = auto
    server signing = auto
    dedicated keytab file = FILE:/etc/samba/samba.keytab
    kerberos method = dedicated keytab
    realm = lab
    security = user
    log file = /var/log/samba/log
```

En la secció `homes` s'indica el comportament de les carpetes `home` dels usuaris en el nostre cas desactivarem l'accés.

```
[homes]
    browseable = No
    writable = No
```

En les següents seccions es poden indicar els recursos compartits definits per l'administrador com també el servei d'impressió. En el nostre cas es crearà un recurs compartit amb el nom de `Finances` el qual estarà ubicat en el directori `/home/finances` del servidor `atenea.lab` i que serà accedit per els usuaris que integrin el grup de domini `gs_it`:

```
[Finances]
    path = /home/finances
    writable = yes
    browsable=yes
    valid users = @gs_it
```

Es important tenir en compte que per qualsevol canvi que es realitzi en el fitxer de configuració es necessari reiniciar el servei samba amb la comanda `systemctl`. Per altra banda, s'utilitza també la comanda `systemctl` per activar el servei a l'arranc del sistema:

```
[root@atenea ~]# systemctl enable smb  
[root@atenea ~]# systemctl start smb
```

7.2.4. Configuració de servei NFS

En NFS els directoris que es publiquen per l'intercanvi de fitxers s'anomenen punt de muntatges, aquests punts de muntatges han d'estar definits per el servidor NFS juntament amb les corresponents opcions d'accés. La darrera versió de NFS és la versió 4 que millora la seguretat de les versions anteriors, unes de les característiques són la eliminació de la interacció del amb `rpc` i l'altre que permet utilitzar l'autenticació Kerberos.

La configuració de muntatge de directoris de NFS es realitza per el fitxer de configuració `/etc/exports`. En aquest fitxer s'especifica altres opcions com són la d'especificar si el punt de muntatge ha de ser solament lectura, si ha de funcionar amb autenticació, integritat i privacitat Kerberos, etc. El contingut del fitxer `/etc/exports` en `atenea.lab` és el següent:

```
/home/nfshomes 192.168.100.0/24(rw,sec=krb5:krb5i:krb5p)
```

En la primera columna s'especifica el directori publicat, en la segona columna les adreces IP que han de tenir accés i entre parèntesis les opcions requerides. En el nostre cas s'utilitza el directori `/home/nfshomes` amb escriptura/lectura amb autenticació, integritat i privacitat Kerberos.

Per millorar la seguretat de la xarxa és possible desactivar versions anteriors a la versió 4 de NFS. Cal tenir en compte que clients que no suportin la versió 4 no funcionaran. Per desactivar versions anteriors es modifica el fitxer `/etc/nfs.conf` del servidor com en el client NFS i s'activen les següents clàusules.

```
[nfsd]
vers2=n
vers3=n
```

Amb relació als serveis requerits per la versió 4 de NFS es desactiva rpcbind:

```
[root@atenea ~]# systemctl disable rpcbind
```

i s'activa el nfs:

```
[root@atenea ~]# systemctl start nfs
[root@atenea ~]# systemctl enable nfs
```

El port de comunicacions per defecte de NFS és el port TCP/2049.

7.3. Configuració SELinux

SELinux necessita etiquetar els fitxers amb atributs estesos per fer funcionar les seves polítiques de seguretat, si es necessita publicar recursos amb Samba i NFS cal informar a SELinux del context com també informar del tipus accés al recurs. En el cas de Samba serà necessari especificar el context `samba_share_t` amb els permisos `samba_export_all_rw` i `samba_export_all_ro` a `true`.

Les comandes necessàries per permetre el recurs Samba `/home/finances` a són les següents:

```
[root@atenea ~]# semanage fcontext -at samba_share_t
"/home/finances(/.*)?"
[root@atenea ~]# setsebool -P samba_export_all_ro=1
[root@atenea ~]# setsebool -P samba_export_all_rw=1
[root@atenea ~]# setsebool -P samba_enable_home_dirs on
```

Es restaura el context SELinux:

```
[root@atenea ~]# restorecon /home/finances
```

En el cas de NFS s'activen els valors booleans següents:

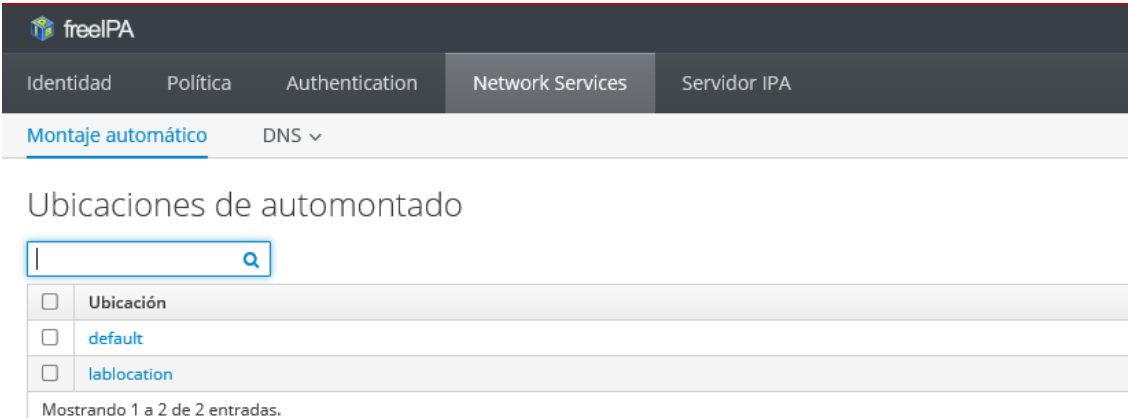
```
[root@atenea ~]# setsebool -P use_nfs_home_dirs 1
[root@atenea ~]# setsebool -P nfs_export_all_ro 1
[root@atenea ~]# setsebool -P nfs_export_all_rw 1
```

7.4. Configuració Automount FreeIPA

Automount és una funcionalitat que permet el muntatge automàtic d'un directori remot publicat per un protocol d'intercanvi de fitxers, en el nostre cas NFS i SMB. El muntatge automàtic es realitza quan l'usuari demanda la necessitat d'accedir al seu punt de muntatge.

Automount anomena *keys* als punt de muntatge, moltes *keys* poden estar agrupades en un *map* i els *maps* estan associats a una ubicació. El fitxer de configuració principal de automount s'ubica en `/etc/auto.master`, cal dir per això que la informació de la configuració d'automount en IPA s'emmagatzema en el directori LDAP per no tenir que emmagatzemar la informació en fitxers. La configuració d'automount es pot realitzar mitjançant WebUI o mitjançant CLI i una vegada configurat cal configurar al client.

Creació d'ubicació automount, per crear una ubicació d'automount cal dirigir-se a la secció de **Network services**, seleccionar **Automount** i **Afegir** una entrada. En el nostre cas crearem la ubicació **lablocation**:



The screenshot shows the FreeIPA web interface. At the top, there is a navigation bar with tabs for 'Identidad', 'Política', 'Authentication', 'Network Services', and 'Servidor IPA'. The 'Network Services' tab is selected. Below the navigation bar, there is a sub-menu with 'Montaje automático' and 'DNS'. The main content area is titled 'Ubicaciones de automontado' and contains a search box. Below the search box, there is a table with two entries: 'default' and 'lablocation'. The 'lablocation' entry is highlighted. At the bottom of the table, it says 'Mostrando 1 a 2 de 2 entradas.'

<input type="checkbox"/>	Ubicación
<input type="checkbox"/>	default
<input checked="" type="checkbox"/>	lablocation

La comanda específica en CLI seria la següent:

```
[root@apolo ~]# ipa automountlocation-add lablocation
```

Creació del map, per la creació d'un map cal seleccionar la ubicació desitjada, el tipus de mapeig ja sigui directe o indirecte i el nom de mapeig, en el nostre cas es crea el map dins de la ubicació **lablocation** i es creen el **auto.cifsshared** i el **auto.nfs**. Dins d'aquests maps s'indica la informació del directori remot i protocol utilitzat per el muntatge:

Llaves de montaje automático: auto.nfs

Llaves de montaje automático		Configuración
<input type="text" value=""/>		
<input type="checkbox"/>	Llave	Información de montaje
<input type="checkbox"/>	*	-fstype=nfs4,rw,sec=krb5 atenea.lab:/home/nfshomes/&
Mostrando 1 a 1 de 1 entradas.		

Llaves de montaje automático: auto.cifsshared

Llaves de montaje automático		Configuración
<input type="text" value=""/>		
<input type="checkbox"/>	Llave	Información de montaje
<input type="checkbox"/>	Finances	-fstype=cifs,sec=krb5,multiuser ://atenea.lab/Finances
Mostrando 1 a 1 de 1 entradas.		

En el cas del map **auto.nfs** s'observa que s'utilitza la key * i el caràcter & per especificar que la carpeta correspon amb el nom de l'usuari que inicia sessió. Les comandes utilitzades per CLI són les següents (exemple cas de **auto.cifsshared**):

```
[root@apolo ~]# ipa automountmap-add lablocation auto.cifsshared
[root@apolo ~]# ipa automountkey-add lablocation --key
"Finances" --info "-fstype=cifs,sec=krb5,multiuser
: //atenea.lab/Finances" auto.cifsshared
```

Creació del automount, el procés final de creació del automount consisteix en indicar la *key* o directori local de muntatge i el fitxer de *map* creat anteriorment. Com es pot observar en la imatge es crea el automount amb les keys `/mnt/Finances` i `/mnt/nfs` per muntar els maps **auto.cifs** i **auto.nfs** respectivament:

Llaves de montaje automático: auto.master

Llaves de montaje automático		Configuración
<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	Llave	Información de montaje
<input type="checkbox"/>	<code>/mnt/cifs</code>	auto.cifsshared
<input type="checkbox"/>	<code>/mnt/nfs</code>	auto.nfs
Mostrando 1 a 2 de 2 entradas.		

8. Preparació de clients IPA

La inscripció d'un client al domini IPA consisteix en la configuració del dimonis SSSD i certmonger per connectar al domini IPA. Aquesta inscripció es pot realitzar amb la utilització de la comanda `ipa-client-install` del paquet `freeipa-client` o es pot realitzar manualment editant fitxers de configuració. Existeixen certes distribucions Linux que no disposen d'aquest paquet i és necessari configurar els fitxers de configuració necessaris.

A l'hora d'afegir un client al domini IPA és necessari proporcionar les credencials d'un administrador de domini, una vegada afegit es crea automàticament en el directori IPA els certificats de host corresponents. Les comandes necessàries per inscriure un client al domini mitjançant la comanda `ipa-client-install` són les següents:

```
[root@bart ~]# yum install freeipa-client -y
[root@bart ~]# ipa-client-install --mkhomedir
```

S'especifica la opció `--mkhomedir` per tal de que es pugui crear la carpeta de perfil de l'usuari. Aquesta comanda crea fitxers de configuració de IPA `/etc/ipa/default` i configura els fitxers de configuració relacionats amb els dimonis Kerberos, SSSD i LDAP que corresponen a `/etc/krb5.conf`, `/etc/sss/sss.conf` i `/etc/openldap/ldap.conf` respectivament.

Per poder utilitzar les funcionalitats d'automount en el client és necessari utilitzar la comanda `ipa-client-automount` especificant la ubicació corresponent amb la següent comanda:

```
[root@bart ~]# ipa-client-automount --location=lalocation
```

Aquesta comanda edita els fitxers `/etc/sysconfig/nfs` i `/etc/idmapd.conf`.

9. Conclusions

Amb la informació recopilada i les proves realitzades en l'entorn de laboratori s'arriba a la conclusió que el programari FreeIPA és molt adequat en entorns on es necessita una gestió centralitzada d'identitats, d'autenticació i de polítiques de seguretat.

Amb relació a la disponibilitat del servei, la possibilitat de poder disposar d'una topologia de replicació entre servidors IPA aporta a les organitzacions un servei de directori d'alta disponibilitat i contingència en cas de fallida.

La seva facilitat d'us a nivell gràfic i a nivell d'execució de comandos fan que FreeIPA sigui una solució potent i eficient per a administradors avançats i administradors novells.

Com a punts negatius cal mencionar la falta d'eines automàtiques per la configuració d'un client FreeIPA en certes distribucions Unix i la dificultat de la integració del servei DHCP en el servei de directori.

10. Bibliografia

Curry Nathan www.nathancurry.com [En línia] = NFS Kerberitzat amb FreeIPA en Centos 7. - <https://www.nathancurry.com/blog/07-kerberized-nfs-with-freeipa-on-centos-7/>.

Fedora docs.fedoraproject.org [En línia] = Introducció FreeIPA. - https://docs.fedoraproject.org/en-US/Fedora/15/html/FreeIPA_Guide/introduction.html.

FreeIPA www.freeipa.org [En línia] = Integrar Samba amb FreeIPA. - https://www.freeipa.org/page/Howto/Integrating_a_Samba_File_Server_With_IPA.

FreeIPA www.freeipa.org [En línia] = Integració DHCP amb FreeIPA. - https://www.freeipa.org/page/DHCP_Integration_Design.

Fundación Wikimedia Inc. es.wikipedia.org [En línia] // es.wikipedia.org. - https://es.wikipedia.org/wiki/Network_File_System.

Fundación Wikimedia Inc. es.wikipedia.org [En línia] = Explicació de Samba. - [https://es.wikipedia.org/wiki/Samba_\(software\)](https://es.wikipedia.org/wiki/Samba_(software)).

Internet Systems Consortium Inc. ftp.isc.org [En línia] = Instal·lació del programari DHCP kea. - [ftp://ftp.isc.org/isc/kea/1.5.0/doc/kea-guide.html#install](http://ftp.isc.org/isc/kea/1.5.0/doc/kea-guide.html#install).

Internet Systems Consortium Inc. kb.isc.org [En línia] = Notes per la instal·lació de codi kea en Centos & RH. - <https://kb.isc.org/docs/kea-build-on-centos>.

Ltd JGraph Draw.io = Utilitat per la creació de diagrames.

Oracle Oracle Virtualbox = <https://www.virtualbox.org> - Programari per virtualització.

RedHat access.redhat.com [En línia] = Introducció al servei d'identitat, autenticació i polítiques IPA. - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/introduction.

RedHat access.redhat.com [En línia] = Configuració d'un servei NFS amb Kerberos. - [https://access.redhat.com/docuhttps://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/kerb-nfs](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/kerb-nfs).

RedHat access.redhat.com [En línia] = Gestió i administració de rèpliques IPA. - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/ipa-replica-manage.

Technology Massachusetts Institute of web.mit.edu [En línia] = Sistema de fitxers NFS. - <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-nfs.html>.

Varonis www.varonis.com [En línia] = Diferències entres Samba, CIFS i SMB. - <https://www.varonis.com/blog/cifs-vs-smb/>.