
freeIPA
identity | policy | audit

Índice

FreeIPA

INTRODUCCIÓN

Esta herramienta se utiliza para crear un controlador de dominio entre máquinas Linux y Unix. En FreeIPA se define el dominio y las máquinas del dominio, por lo que se proporciona una estructura centralizada, la cual no era posible en entornos Unix.

FreeIPA trabaja con información de seguridad sobre usuarios, máquinas y servicios por identidades. Una vez que la identidad se verifica, entonces el acceso a los servicios y recursos pasa a ser controlada.

Por temas de eficiencia, prevención de fallos, y la facilidad que presta a la administración, los administradores de sistemas tratan de gestionar esos servicios de forma centralizada. Esto hace de FreeIPA una herramienta ideal para administradores, ya que históricamente, los entornos de Linux no habían tenido este tipo de gestión.

En FreeIPA se utilizan muchos tipos de protocolos, como pueden ser *NIS* y *Kerberos*, que se encargan de definir los dominios, mientras que los datos de otras aplicaciones pueden utilizar *LDAP.*

Estas herramientas no se comunicaban entre si normalmente, o simplemente se utilizaban con herramientas de gestión, por lo que cada aplicación tenía que ser administrada por separado y a nivel local. La única manera de conseguir una política de identidad consistente era copiar los archivos de configuración manualmente.

El objetivo de FreeIPA es simplificar que la sobrecarga administrativa. Los usuarios, máquinas, servicios y políticas están configuradas en un solo lugar, con las mismas herramientas. Debido a que FreeIPA crea un dominio, múltiples máquinas pueden utilizar la misma configuración y los mismos recursos solo con unirse al dominio.
Los usuarios sólo tienen que inscribirse en los servicios del dominio y los administradores pueden gestionar una única cuenta de usuario.

FreeIPA es un servidor de dominio basado en Linux y controlado mediante Linux o Unix, lo que hace que no sea una herramienta administrativa para máquinas Windows, por lo que no admite clientes Windows, pero si puede sincronizar con un dominio de Active Directory para permitir la integración con servidores de Windows.

Realmente, FreeIPA no hace ninguna tarea que un administrador no pudiese realizar antes de su existencia, ya que lo único que hace es unir todas las herramientas y hacerlo mas fácil y cómodo.

FreeIPA se divide en los siguientes apartados:

- **Directorio Activo**

El directorio activo está constituido sobre un servidor LDAP, el cual se encarga de la gestión de identidades, autenticación (Kerberos), servicios de autorización y otras políticas.

La configuración o los certificados se almacenan en el servidor de directorios, almacenándose en un sufijo calculado a partir del nombre del árbol.

El acceso a diferentes partes del árbol del directorio activo está protegidos por la configuración del DS ACI. Algunas partes del árbol pueden estar abiertos a todo el mundo de forma anónima, otros pueden estar abiertos sólo a los usuarios autentificados y por otra parte, los usuarios con privilegios.

Igual que el directorio activo de Windows, se comunica con el protocolo LDAPv3 estándar. Los clientes LDAP se pueden utilizar para leer todos los objetos de identidad y política. Sin embargo, la adicción o modificación de entradas de LDAP personalizadas no se recomiendan, ya que podría dar lugar a entradas incompletas o inconsistentes en el árbol.

Para hacer que la manipulación de las entradas sea más fácil, FreeIPA proporciona una interface CLI y Web para el usuario de forma que resulte mas sencillo el manejo de las herramientas y la modificación de los datos.

- **Kerberos**

Kerberos proporciona servicios de autenticación para todo el bosque de FreeIPA, para los usuarios, servicios y componentes.

Su función es permitir que en una red insegura poder demostrar las identidades de los clientes de forma segura. Para ello utiliza un sistema mediante tickets, los cuales se utilizan para demostrar la autenticidad de los usuarios.

- **PKI**

Es un servicio integrado en FreeIPA que ofrece servicios de CRL y OCSP para todo el software, y su función es como gestión de certificados.

- **DNS**

FreeIPA permite gestionar y servir registros DNS en el dominio utilizado la interfaz web o CLI como en la gestión de identidades y políticas.

La integración de DNS se basa en el proyecto bind-dyndb-ldap, que mejora el servidor de nombres BIND, para poder utilizar instancias LDAP.

- **Certmonger**

Es un demonio que supervisa los certificados y alerta de una inminente expiración. También puede actualizar opcionalmente los certificados antes de que estén vencidos con la ayuda de una CA. Como era de esperar, su funcionamiento es a través de OpenSSL.

- **Web UI**

Sirve para administrar FreeIPA por una aplicación Web. Tiene las mismas capacidades que la utilidad IPA (CLI), por tanto, los administradores pueden elegir libremente con cual de ellos quieren realizar las tareas libremente.

Está construida con JavaScript y para el desempeño de su tarea utiliza JSON-RPC.

- **Trusts**

Es el que se encarga del servicio de directorio activo, para ello utiliza componentes de Samba.

- **Client**

FreeIPA utiliza componentes y protocolos estándar, por lo que cualquier LDAP/Kerberos (incluso NIS) pueden operar con un directorio FreeIPA Server para la autenticación básica y la enumeración de usuarios y grupos.

RECOPILACIÓN DE DATOS

Para empezar a montar FreeIPA hay reunir una serie de datos y elegir entre varias opciones, como puede ser la elección del sistema operativo, si hay replica o no, la forma de gestionar, etc.

En este caso se a optado por los siguientes datos:

```
Dominio:  acid-sfw.es
Reino:          ACID-SFW.NET
Servidor1:      server1.acid-sfw.net
Servidor2:      server2.acid-sfw.net
Cliente:  cliente1.acid-sfw.net
```

Los sistemas elegidos son Cent0S 6.5 64 bits para los servidores, y teniendo en cuenta que los clientes tienen que ser Linux, se ha elegido un Debian Wheezy 7.4 64 bits.

VIRTUALIZACIÓN DEL ESCENARIO

Para montar el escenario se va a usar el sistema de virtualización KVM sobre un Debian Wheezy 64 bits de anfitrión.

Las máquinas van a tener las siguientes características:

- Anfitrión

  ```
  Sistema: Debian Wheezy 7.4 64 bits
  Memoria RAM: 4 GB
  HDD: 160 Gbex
  Tarjetas de red: 1 (con bridge)
  Función: Virtualización en KVM
  ```

- Servidor1:

  ```
  Sistema: CentOS 6.5 64 bits
  Memoria RAM: 700 MB
  HDD: 30 GB
  Tarjetas de red: 1
  Dirección IP: 192.168.1.152/24
  Función: Servidor FreeIPA principal
  ```

- Servidor2:

```
Sistema: CentOS 6.5 64 bits
Memoria RAM: 700 MB
HDD: 30 GB
Tarjetas de red: 1
Dirección IP: 192.168.1.152/24
Función Servidor FreeIPA replica
```

- Cliente1:

```
Sistema: CentOS 6.5 64 bits
Memoria RAM: 600 MB
HDD: 15 GB
Tarjetas de red: 1
Dirección IP: DHCP
Función: Cliente para el directorio activo
```

CONFIGURACIÓN DE RED

Para los dos servidores se van a establecer una IP estática por cada servidor, ya que no es recomendable que se obtenga de forma dinámica, ya que en la mayoría de los casos, el servidor DHCP está en los propios servidores.

En primer lugar tenemos que desactivar la aplicación Network-Manager en caso de que esté instalada. Para ello se ejecuta la siguiente orden:

```
[root@centos1 ~]# chkconfig NetworkManager off

[root@centos2 ~]# chkconfig NetworkManager off
```

Activamos el network, por si no estuviese activado al inicio.

```
[root@centos1 ~]# chkconfig network on

[root@centos12~]# chkconfig network on
```

Ahora editamos el fichero de configuración para introducir los datos estáticos de la red:

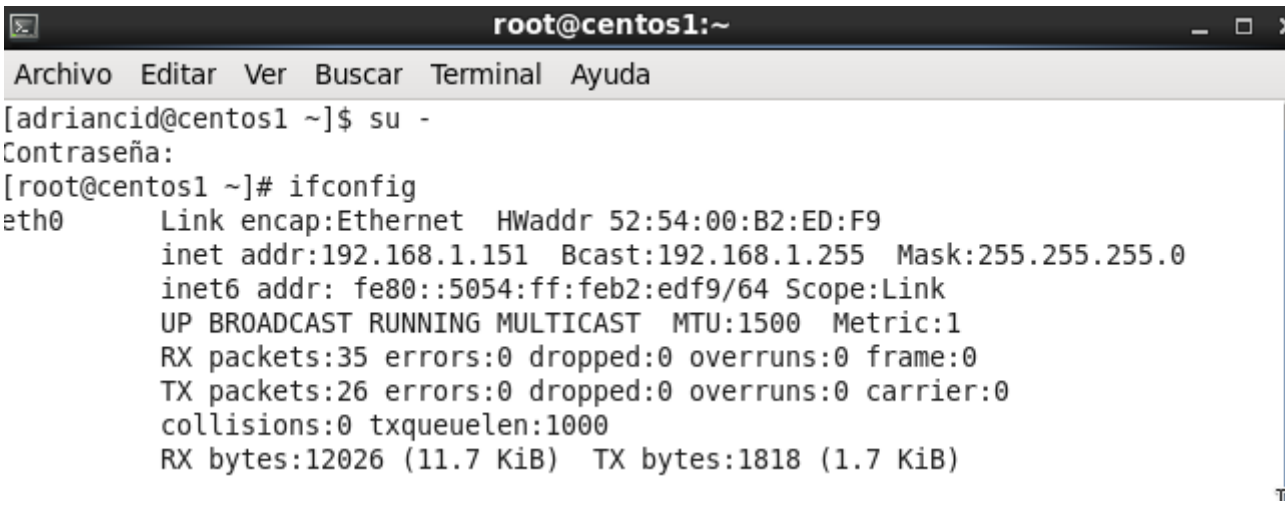
```
[root@centos1 ~]# nano /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0
HWADDR=52:54:00:B2:ED:F9
TYPE=Ethernet
UUID=13cabc95-737b-40f0-a301-0d0a0e813447
ONBOOT=yes
```

```
NM_CONTROLLED=no
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=192.168.1.151
GATEWAY=192.168.1.1
USERCTL=no
DNS1=8.8.8.8
DNS2=8.8.4.4
```

[root@centos2 ~]# nano /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=52:54:00:B2:ED:F7
TYPE=Ethernet
UUID=13cabc95-737b-40f0-a301-0d0e3e813447
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=192.168.1.152
GATEWAY=192.168.1.1
USERCTL=no
DNS1=8.8.8.8
DNS2=8.8.4.4
```

Aquí vemos como se han aplicado el fichero:



Ahora cambiamos el nombre de las maquinas y añadimos el FQDN. Para ello editamos el fichero 'hosts' para que quede de la siguiente manera en el servidor1:

```
# nano /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost6 localhost6.localdomain6
::1       localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.151  server1.acid-sfw.net server1 localhost
```

Una vez realizado este paso también el server2 cambiando el nombre, cambiamos los nombres de las máquinas. Para ello hacemos lo siguiente:

```
# nano /etc/sysconfig/network
```

```
NETWORKING=yes
HOSTNAME=server1
```

Para aplicar todos los cambios es conveniente reiniciar las máquinas, aunque también pueden aplicarse de la siguiente forma:

```
# /etc/init.d/network restart
```

INSTALACIÓN DE FREEIPA EN EL SERVIDOR PRINCIPAL

Antes de instalar el paquete de FreeIPA hay que tener los sistemas actualizados, por lo que ejecutamos la siguiente orden en los dos servidores:

```
# yum update
```

Una vez actualizados los sistemas, ya podemos instalar FreeIPA, la cual es una instalación sencilla, sin apenas interacción del usuario.

```
# yum -y install ipa-server
```

Ahora, especificamos el dominio y el reino LDAP con el siguiente comando:

```
# ipa-server-install --domain=acid-sfw.net –realm=ACID-SFW.NET
```

Nos preguntará el nombre del host, el cual simplemente lo escribimos o le damos a Enter, ya que es el que tiene que salir por defecto.

Después nos pedirá la contraseña del directorio activo, la cual introducimos las dos veces que nos pide.
Aparte nos pedirá la contraseña del usuario 'admin', el cual también introducimos.

Una vez hechos los pasos, confirmamos los datos y el directorio activo empezará a montarse.

Cuando termine el proceso tenemos que pedir un ticket a kerberos, por lo que ejecutamos lo siguiente:

```
# kinit admin
```

Introducimos la contraseña de admin y comprobamos con klist:

```
[root@servidor1 ~]# kinit admin
Password for admin@EXAMPLE.COM:
[root@servidor1 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@EXAMPLE.COM

Valid starting     Expires            Service principal
05/27/14 09:55:39  05/28/14 09:55:33  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Habilitamos el servicio al inicio del servidor de la siguiente forma:

```
# chkconfig ipa on
```

INSTALACIÓN Y CONFIGURACIÓN DE REPLICA

En primer lugar hay que preparar el servidor principal para la replica que se va a alojar en el servidor dos. Para ello se ejecuta el siguiente comando en 'server1':

```
# ipa-replica-prepare server2.acid-sfw.net
```

Pasamos la clave gpg al server2 con scp

```
# scp /var/lib/ipa/replica-info-server2.acid-sfw.net.gpg
root@server2.acid-sfw.net:/var/lib/ipa/
```

Una vez terminado hay que instalar y configurar la replica en 'server2', para ello hay que ejecutar lo siguiente en 'server2':

```
# yum -y install ipa-server
```

Configuramos el servidor como replica.

```
# ipa-replica-install /var/lib/ipa/replica-info-
ipareplica.server2.acid-sfw.net.gpg
```

Nos pedirá la contraseña del directorio activo y del admin de LDAP, por lo que la introducimos y esperamos a que se configure totalmente. Por último lo habilitamos en el inicio.

```
# chkconfig ipa on
```

HABILITAR ACCESO A WEBUI

Por defecto el acceso sólo esta permitido a clientes IPA, para que los clientes no-IPA puedan acceder hay que habilitar la autenticación por Kerberos, lo cual hay que realizar en todos los servidores IPA.

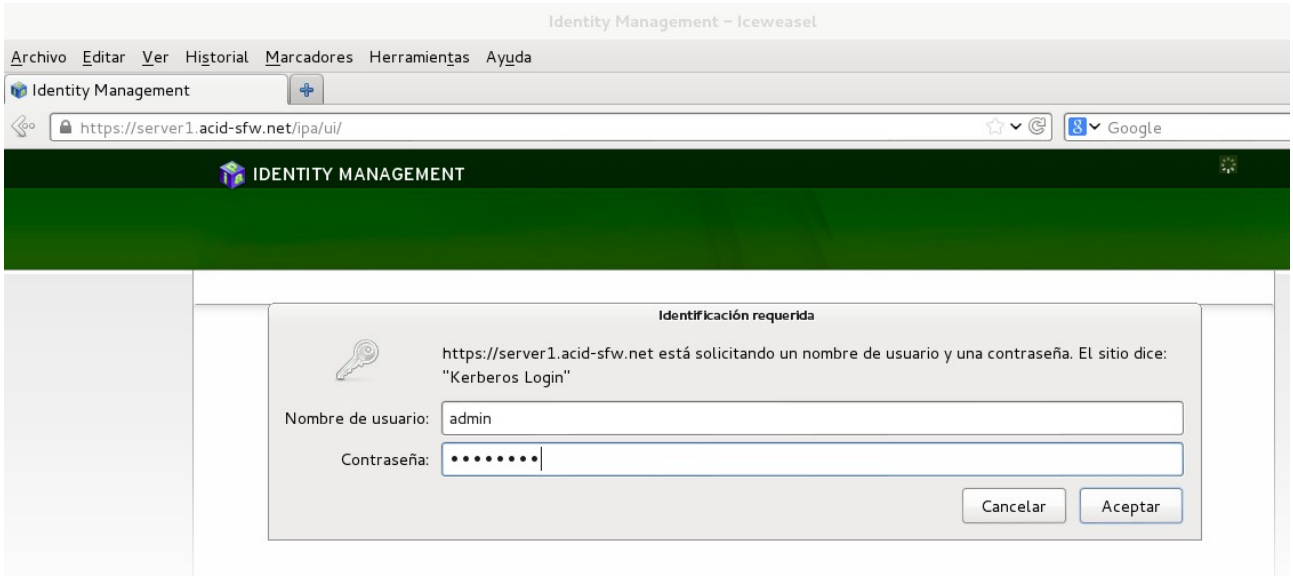
```
# nano /etc/httpd/conf.d/ipa.conf
```

```
.
<Location “/ipa”>
- KrbMethodK5Passwd off
+ KrbMethodK5Passwd on
```

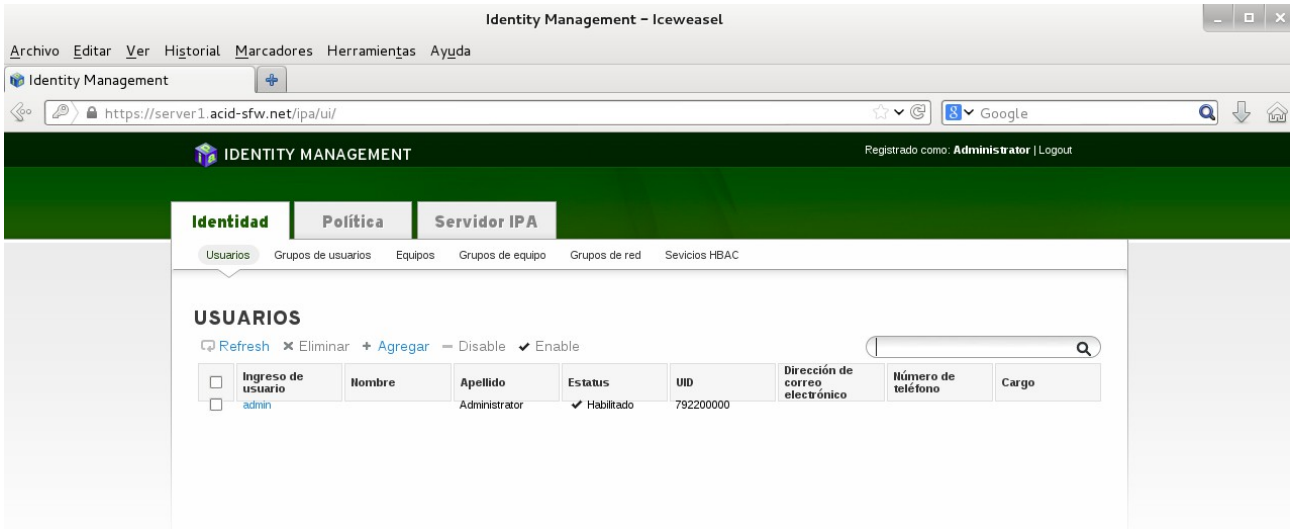
Reiniciamos el httpd para aplicar los cambios.

```
# service httpd restart
```

Una vez hecho esto, ya nos podemos autenticar por la aplicación Web de FreeIPA accediendo desde un navegador a https://server1.acid-sfw.net/ o https://server2.acid-sfw.net/ y introduciendo el usuario admin y la contraseña que especificamos en la instalación.



Como vemos, entramos en la página principal de la administración de FreeIPA.



CONFIGURACIÓN DE BIND9 CON LDAP

Para empezar, vamos a instalar el paquete bind9 preparado para ldap desde los repositorios en server1 y server2.

```
# yum install bind-dyndb-ldap
```

Una vez instalado, configuramos el dns de IPA.

```
# ipa-dns-install
```

Cuando nos pregunte por el reenviador, ponemos un o unos servidores de nombre externo, como pueden ser los de Google.

Esto añade la zona inversa y directa de acid-sfw.net.

AÑADIR CLIENTE CENTOS 6.5

En Freeipa se pueden añadir todo tipo de clientes Linux, como pueden ser Ubuntu, Fedora, Debian, etc. Como primer cliente se va a utilizar un CentOS 6.5 con entorno gráfico básico.

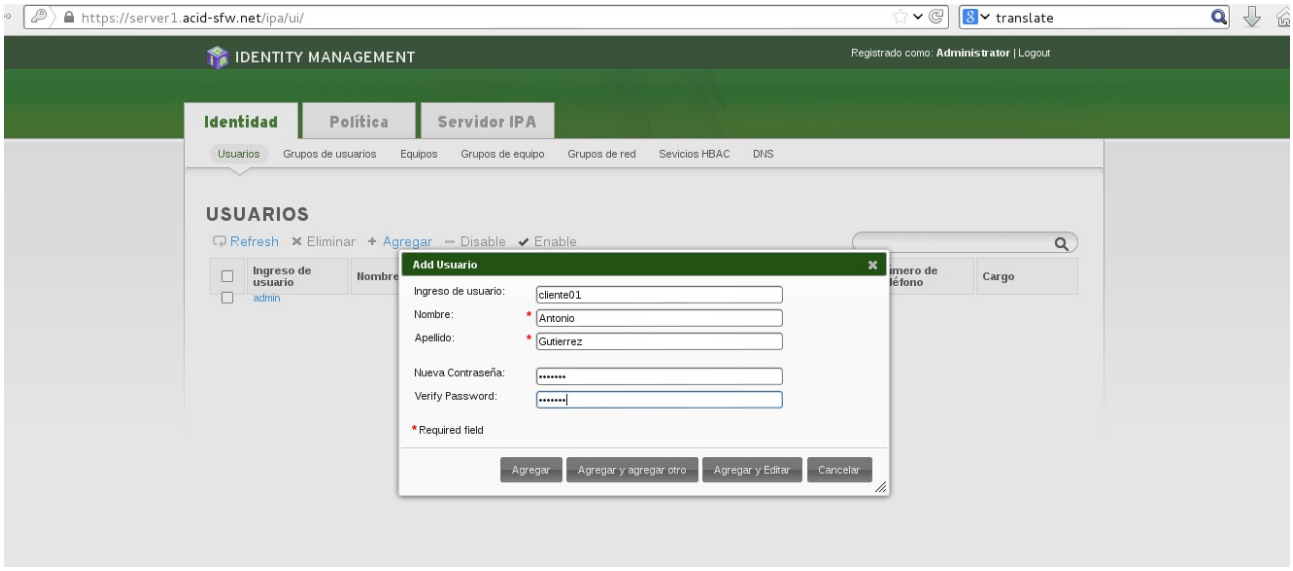
ESPECIFICACIONES

Las especificaciones son las siguientes:

```
Sistema: CentOS 6.5 64 bits
Memoria RAM: 700 MB
HDD: 10 GB
Tarjetas de red: 1
Dirección IP: 192.168.1.160
Función: Cliente para el directorio activo
```

AÑADIR USUARIO EN EL SERVIDOR FREEIPA

Antes de añadir un cliente hay que añadirlo al directorio activo mediante el panel web. Para hacerlo solo hay que entrar en https://server1.acid-sfw.net/ y dentro de 'Identidad' encontramos la pestaña usuarios. Hay que agregar un usuario de la siguiente manera:



Aceptamos y comprobamos que se haya añadido correctamente al panel.

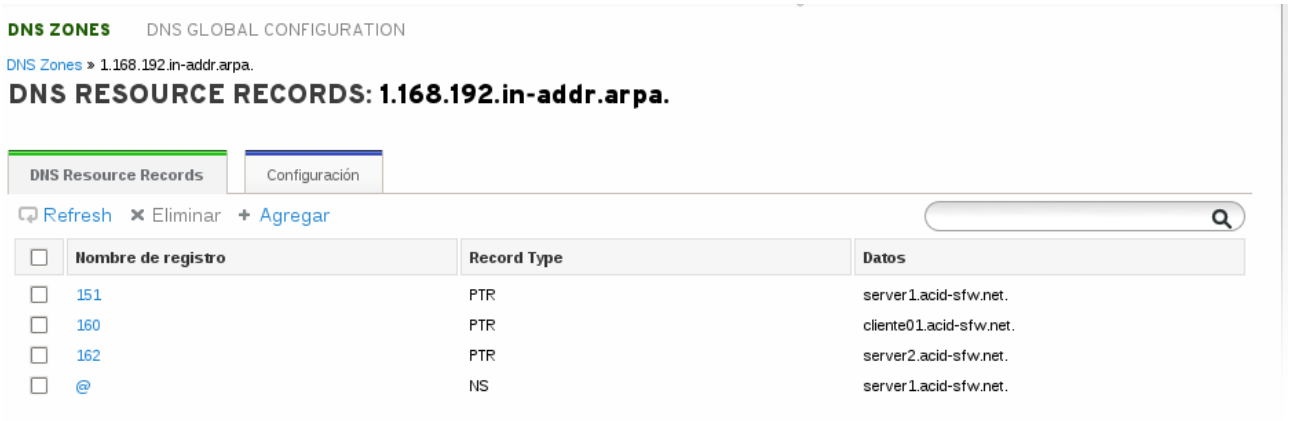
Si entramos en los grupos de usuario guarda el usuario cliente01 directamente en ipausers, que sería el grupo de los usuario básicos. Esto se puede cambiar al crear usuario o una vez hecho desde el mismo menú.

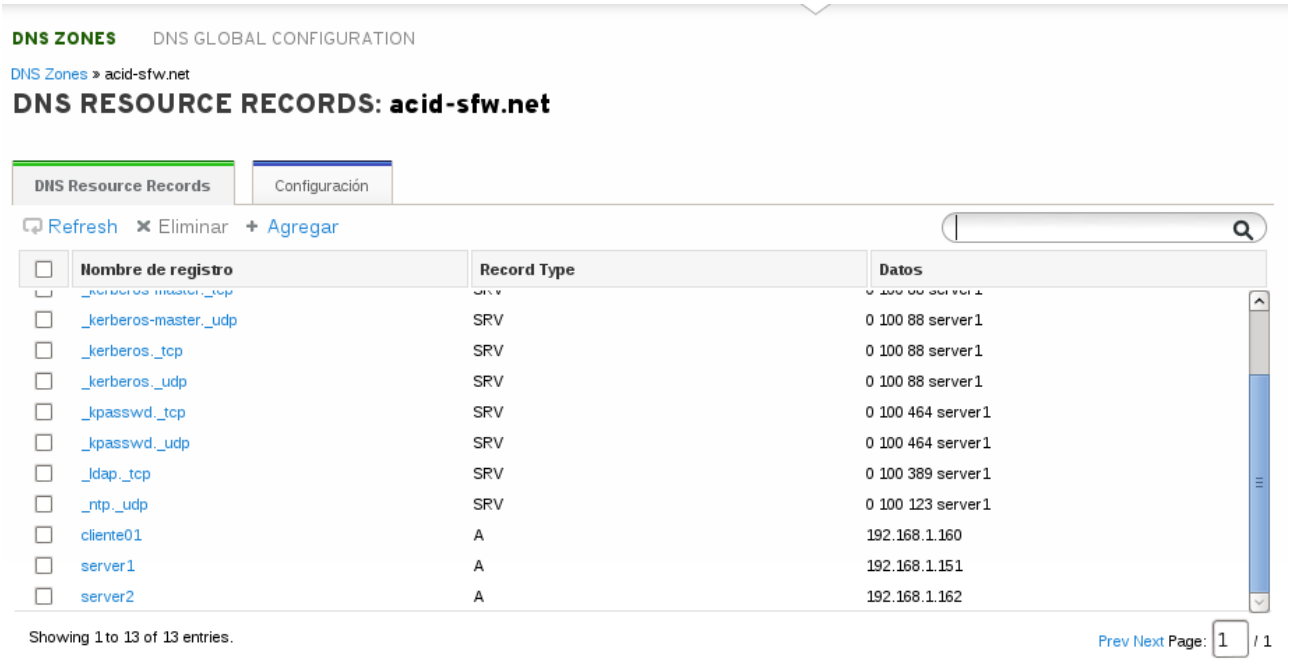
Ahora nos vamos a la pestaña 'Equipos' y le damos a agregar. En el cuadro rellenamos los datos de del equipo del cliente.

Comprobamos que el equipo se a agregado correctamente:

En la pestaña DNS vamos a agregar la dirección dns de cliente01 dándole a agregar, agregando la información y creando la zona inversa.

Si nos fijamos en las dos zonas, el cliente fue agregado correctamente.





Para asegurarnos podemos buscar y pedir información del usuario agregado de la siguiente forma:

```
# ipa user-find cliente01
--------------------
1 usuario coincidente
--------------------
  Ingreso de usuario: cliente01
  Nombre: antonio
  Apellido: gutierrez
  Directorio principal: /home/cliente01
  Shell de ingreso: /bin/sh
  Dirección de correo electrónico: cliente01@acid-sfw.net
  UID: 792200003
```

GID: 792200003
Cuenta inhabilitada : False
Contraseña: True
Kerberos keys available: True

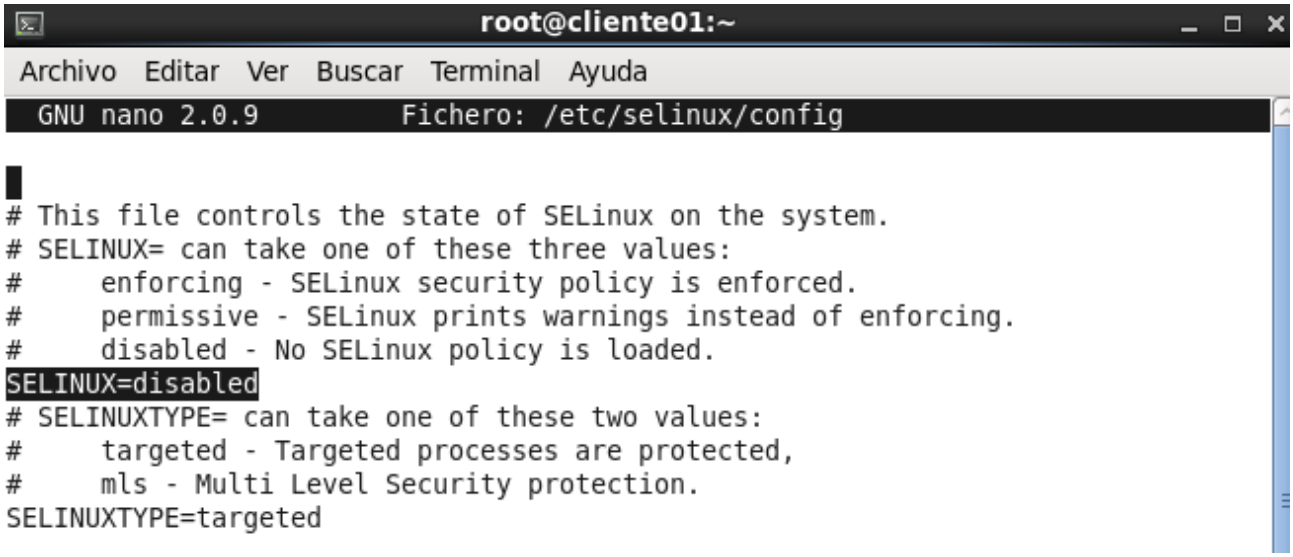
Number of entries returned 1

PRECONFIGURACION DEL CLIENTE

Al tratarse de un CentOS hay que tener varias cosas en cuenta.

1º- Deshabilitar selinux

Para realizar esta acción hay que editar el archivo config, sitado en /etc/selinux/ y poner selinux en disabled de la siguiente forma:



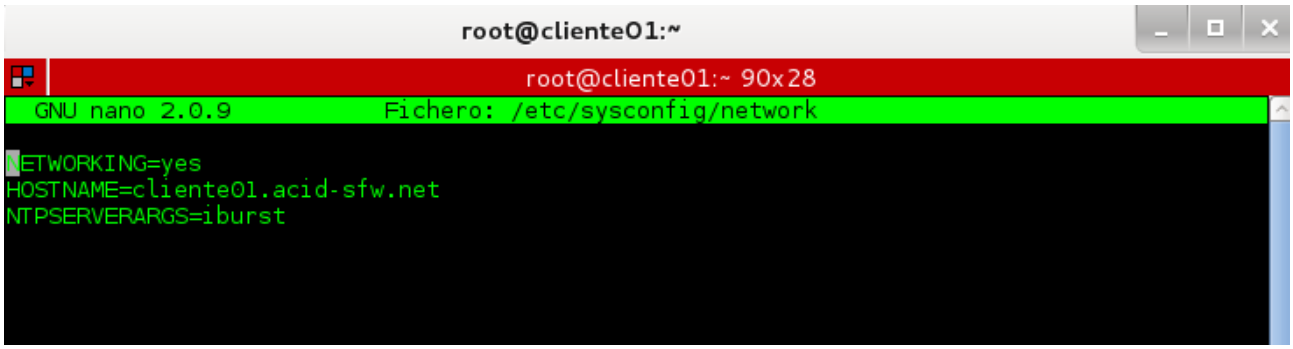
2º- Deshabilitar iptables

Para deshabilitar iptables únicamente hay que ejecutar el siguiente comando:

```
# chkconfig iptables off
```

3º- Configurar el nombre del cliente

Para ello hay que editar el fichero network, en /etc/sysconfig/



4º- Configurar la red

En este apartado se a decidido que todos los clientes tengan una ip superior a la 192.168.1.160, por lo que la red se a configurado de forma estática editando el fichero ifcfg-eth0 que se situa en /etc/sysconfig/network-scripts/

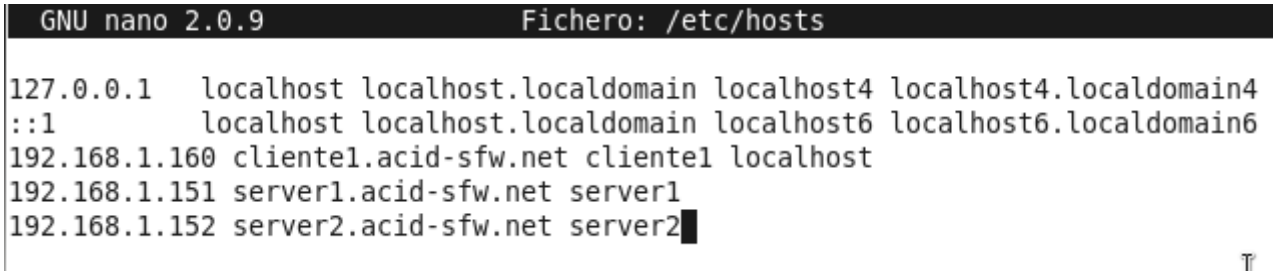
```
  GNU nano 2.0.9      Fichero: /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0
HWADDR=52:54:00:F6:05:15
TYPE=Ethernet
UUID=b8503231-6fc6-47d7-baae-fbb3260e18c0
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
NETMASK=255.255.255.0
IPADDR=192.168.1.160
GATEWAY=192.168.1.1
USERCTL=no
```

También configuramos el DNS de la siguiente manera.

```
nano /etc/resolv.conf

search acid-sfw.net
domain acid-sfw.net
nameserver 192.168.1.151
nameserver 192.168.1.152
nameserver 8.8.8.8
nameserver 8.8.4.4
```

5º- Configuración del archivo hosts

Ya que aún no está metido en el dominio, hay que especificar la dirección de los servidores. Para ello, editamos el fichero hosts de la siguiente forma:

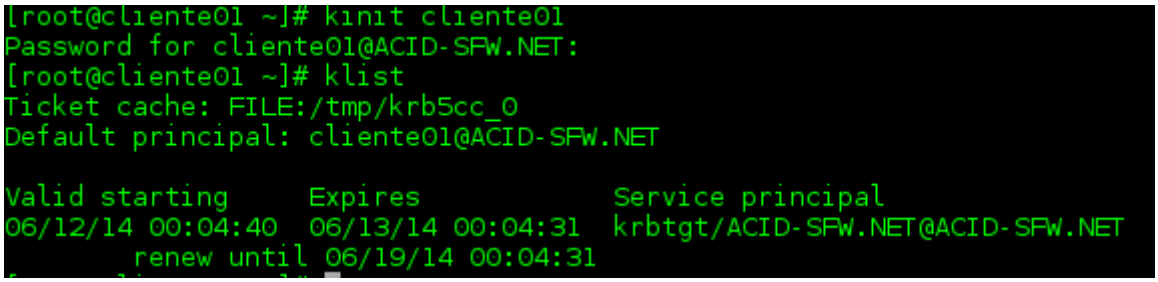


8º- Adaptar Kerberos.

Ahora vamos a editar la configuración de Kerberos para que coja la configuración en el script de instalación automáticamente. Para ello editamos el siguiente archivo de esta manera:

```
nano /etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = ACID-SFW.NET
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 ACID-SFW.NET = {
  kdc = server1.acid-sfw.net
  admin_server = server1.acid-sfw.net
 }

[domain_realm]
 .acid-sfw.net = ACID-SFW.NET
 acid-sfw.net = ACID-SFW.NET
```

Si intentamos realizar la petición de un ticket ahora desde el cliente, este sería el resultado:



7º- Actualizar y reiniciar.

Para instalar el cliente y aplicar los cambios es necesario actualizar los repositorios y los paquetes que lo necesiten y reiniciar el sistema. Para realizar esta tarea se introduce el siguiente comando:

```
# yum update && reboot
```

INSTALACIÓN DE PAQUETES IPA Y INTEGRACIÓN

En primer lugar hay que instalar la aplicación de ipa-client.

```
# yum install ipa-client
```

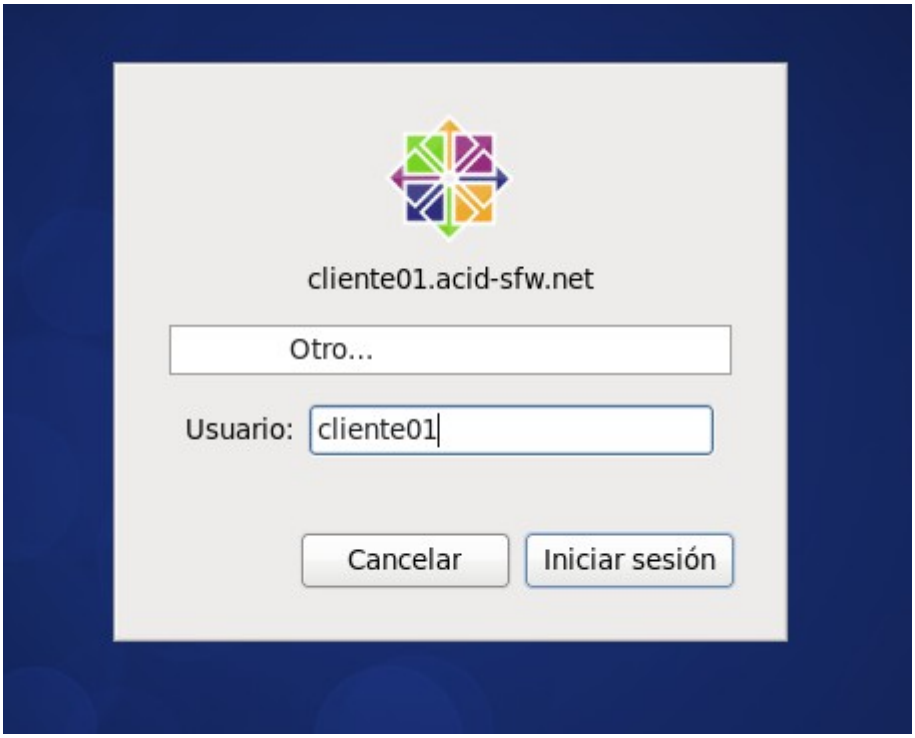
Ahora ejecutamos el script para configurar el cliente.

```
# ipa-client-install --mkhomedir
```

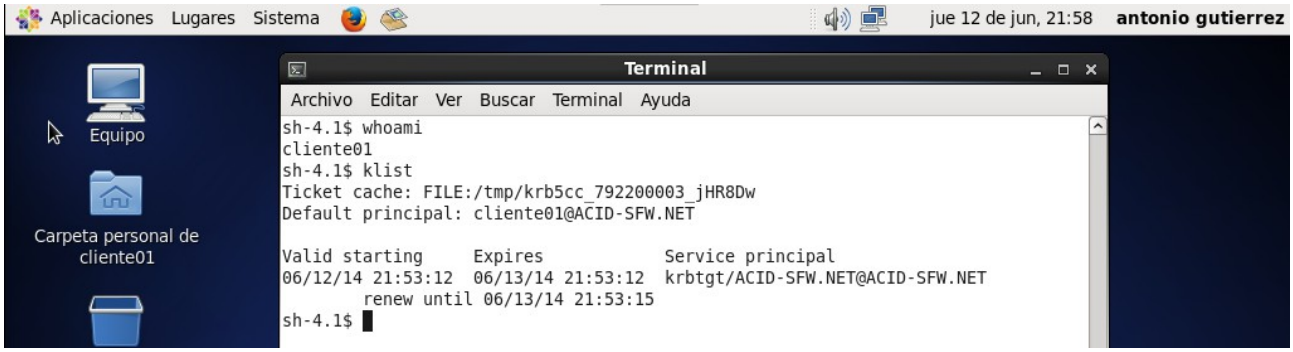
```
[root@cliente01 ~]# ipa-client-install --mkhomedir
Discovery was successful!
Hostname: cliente01.acid-sfw.net
Realm: ACID-SFW.NET
DNS Domain: acid-sfw.net
IPA Server: server1.acid-sfw.net
BaseDN: dc=acid-sfw,dc=net

Continue to configure the system with these values? [no]: yes
User authorized to enroll computers: admin
Synchronizing time with KDC...
Unable to sync time with IPA NTP server, assuming the time is in
sync. Please check that 123 UDP port is opened.
Password for admin@ACID-SFW.NET: contraseñaadmin
```

```
Enrolled in IPA realm ACID-SFW.NET
Created /etc/ipa/default.conf
New SSSD config will be created
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm ACID-SFW.NET
trying https://server1.acid-sfw.net/ipa/xml
Forwarding 'env' to server u'https://server1.acid-sfw.net/ipa/xml'
Hostname (cliente01.acid-sfw.net) not found in DNS
DNS server record set to: cliente01.acid-sfw.net -> 192.168.1.160
Adding SSH public key from /etc/ssh/ssh_host_dsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Forwarding 'host_mod' to server u'https://server1.acid-
sfw.net/ipa/xml'
SSSD enabled
Configured /etc/openldap/ldap.conf
NTP enabled
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Client configuration complete.
```

Una vez terminado reiniciamos la máquina y cuando termine entramos con el usuario cliente01.

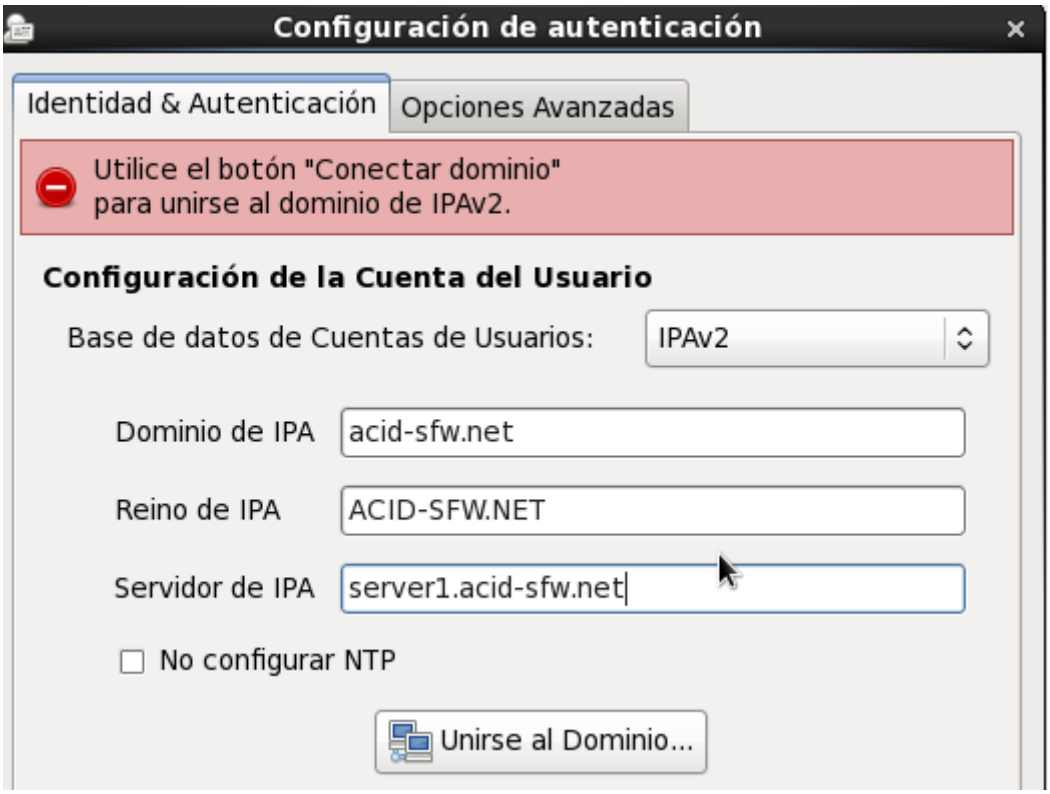


Como vemos, el nombre del usuario es el que pusimos al darlo de alta en FreeIPA server y como el cliente01 a recibido el Ticket de Kerberos automáticamente.



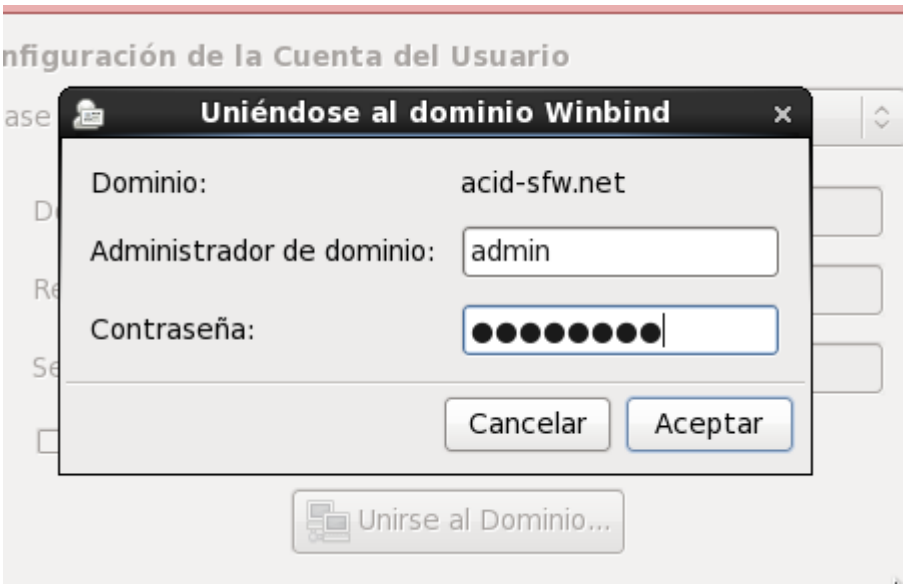
O podemos entrar directamente desde la instalación del cliente en la sección de creación de usuarios.

Entramos en la opción de ingreso por Red y seleccionamos como base de datos de cuentas de usuarios la opción IPAv2



Le damos a unirse al dominio una vez rellenados los campos y guardamos.

Nos pedirá el usuario y contraseña del administrador del dominio.

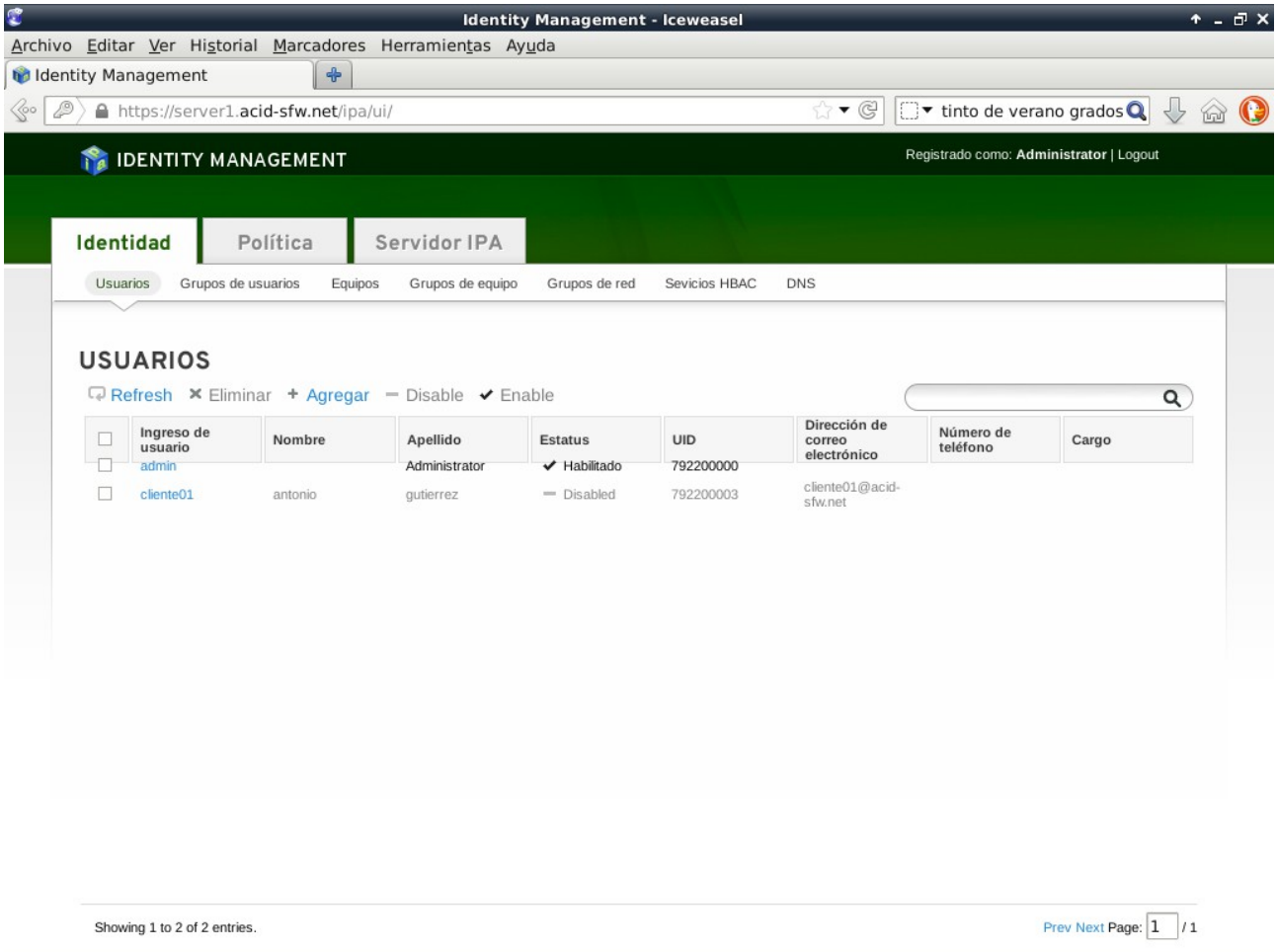


ADMINISTRACIÓN DE FREEIPA

En este punto se va a explicar todo lo relacionado con la configuración de los servicios a los que da posibilidad FreeIPA, como puede ser el DNS, el agregado de grupos, etc.

USUARIOS

En este apartado veremos como controlar los diferentes usuarios que podemos identificar con el servidor FreeIPA. Para ello hay que acceder al panel web introduciendo la dirección server1.acid-sfw.net o server2.acid-sfw.net. Una vez dentro del la página de administración tenemos que irnos a la pestaña de Usuarios, en la que encontraremos la siguiente pantalla:



Como se aprecia, podemos refrescar, eliminar, agregar, habilitar y deshabilitar usuarios.

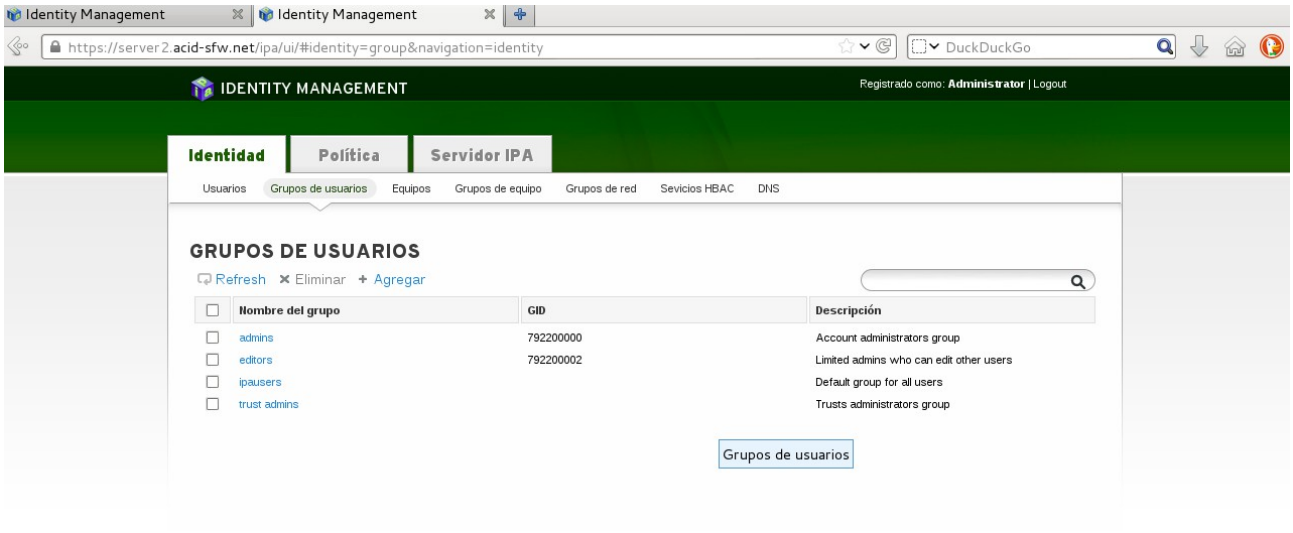
Para personalizar y editar un usuario agregado hay que presionar sobre el usuario y se seplegará las siguientes opciones:

La mayoría de las pestañas vienen con configuración predeterminadas, como los grupos, los grupos de red, los roles, los HBAC Rules y los Sudo Rules. Más adelante veremos como se agregan y personalizan cada uno

En la pestaña configuración podemos personalizar diferentes datos del usuario, restaurar la contraseña del mismo, agregar claves publicas, cambiar el uid y gid, editar la shell, cambiar el directorio principal, agregar datos personales, como el número de teléfono, su página, etc.

GRUPOS DE USUARIOS

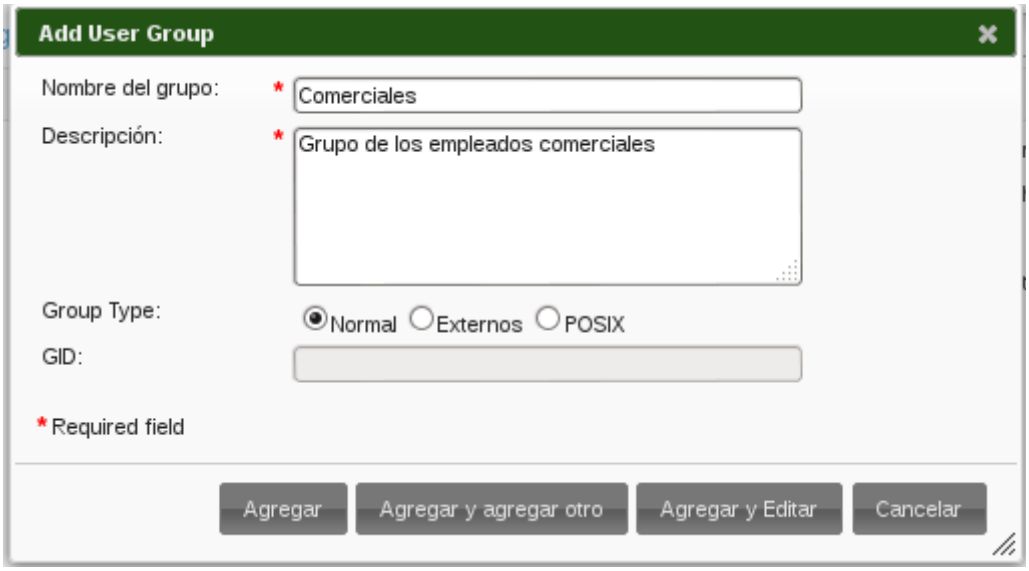
Dentro de la pestaña 'Identidad' podemos gestionar los grupos de usuario.



Como se muestra en la imagen, FreeIPA ya trae cuatro grupos de forma predeterminada, en los que que vemos el grupo admins (Adminitradores), editros (Administradores limitados), ipausers (usuarios normales) y trust admins.

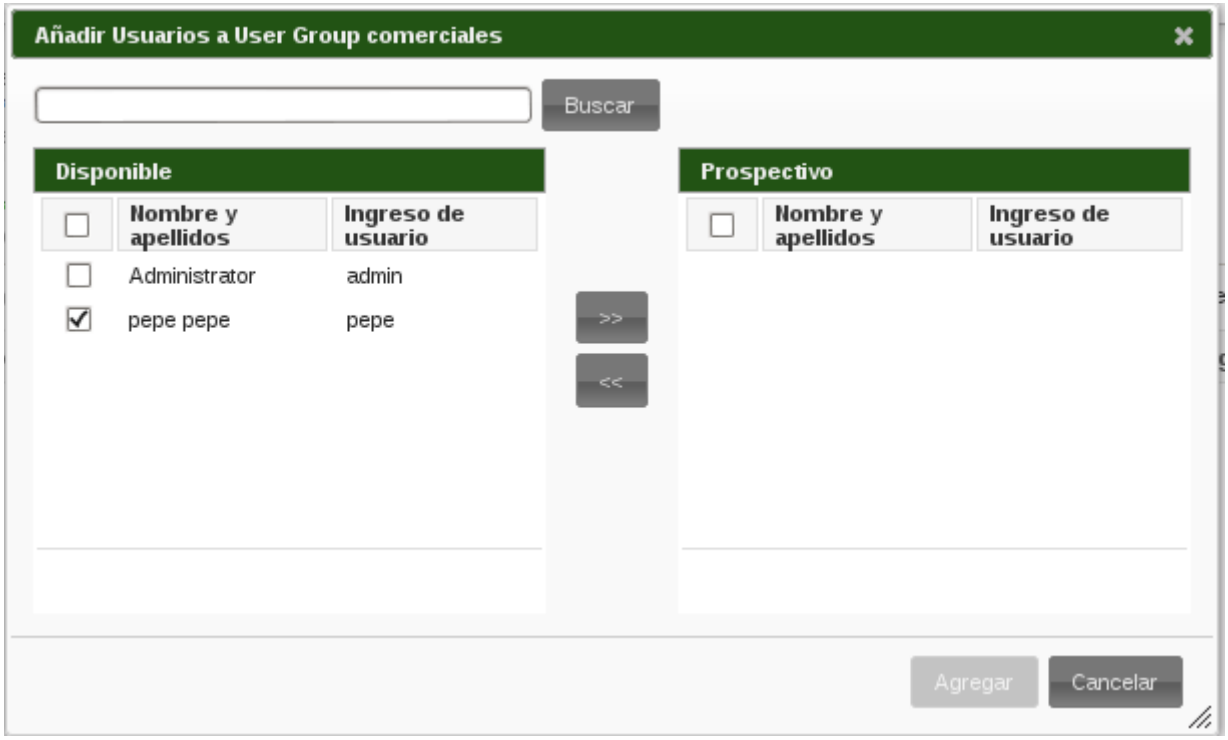
Ahora vamos a agregar un grupo personalizado para un departamento de ejemplo de una empresa, como puede ser “comerciales”.

Para hacerlo hay que presionar sobre 'Agregar'. Ponemos el nombre del grupo, una descripción y lo marcamos como “Normal”



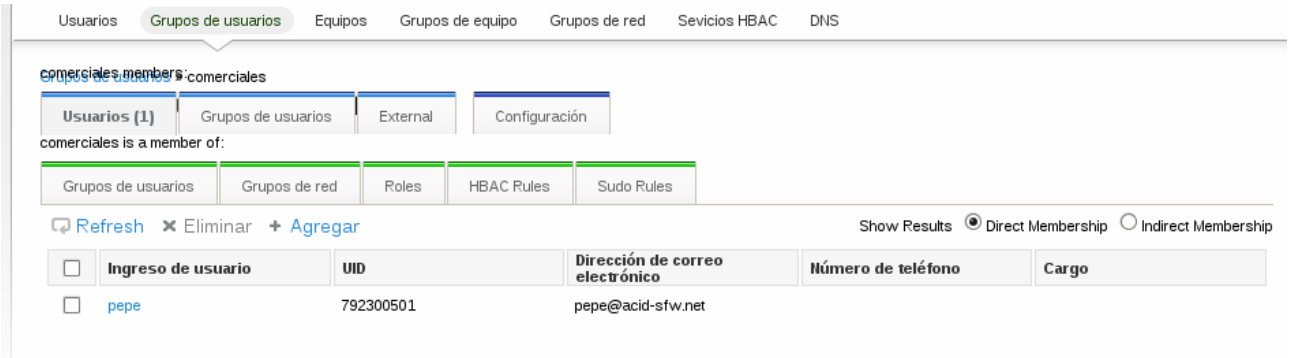
Ahora agregamos y editamos para ver todas las opciones, en las que podemos agregar usuarios, etc.

Para agregar un usuario tenemos que entrar en la pestaña “Usuarios” y presionar sobre “Agregar”



Marcamos el usuario y lo mandamos a la derecha.

Aceptamos y vemos como el usuario fue agregado con éxito.



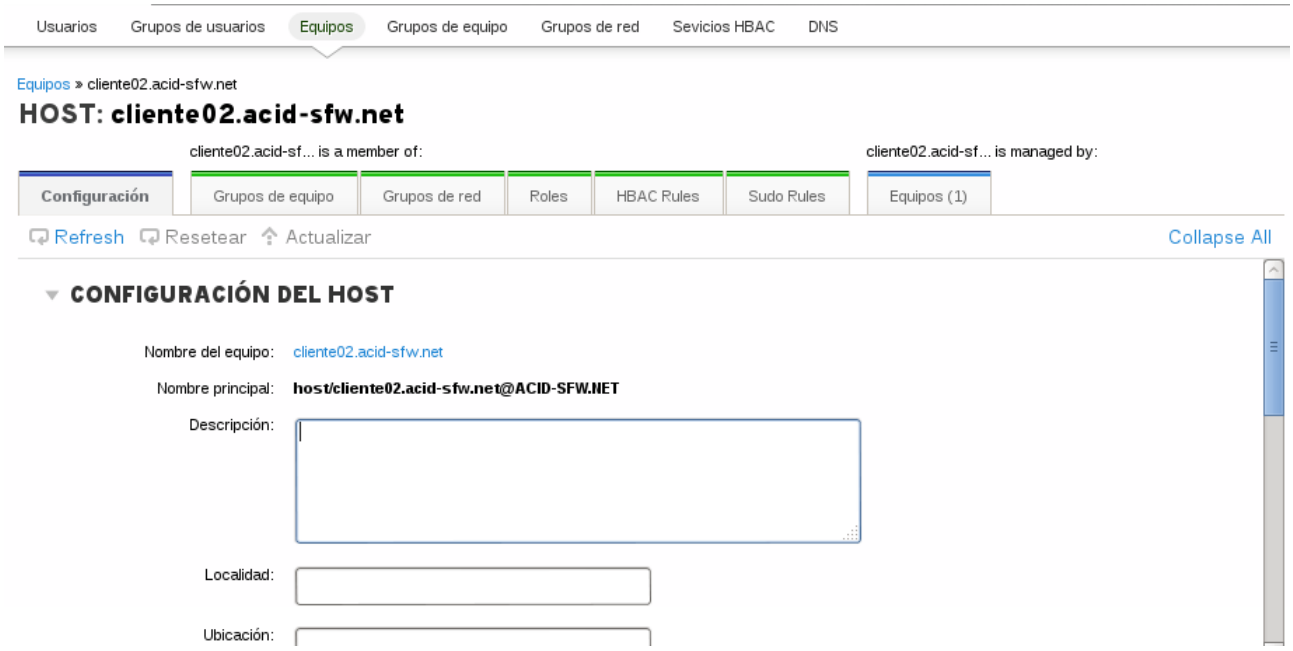
También podemos agregar otros grupos de usuarios y incluso meter usuarios externos, aparte de configurar roles y grupos de red específicos para los usuarios de ese grupo.

EQUIPOS

En este apartado gestionaremos los equipos de los servidores y clientes que tendrán acceso a FreeIPA. Lo podemos encontrar dentro de la pestaña “Identidad”

Para agregar un equipo simplemente hay que seleccionar “Agregar” y rellenar los campos.

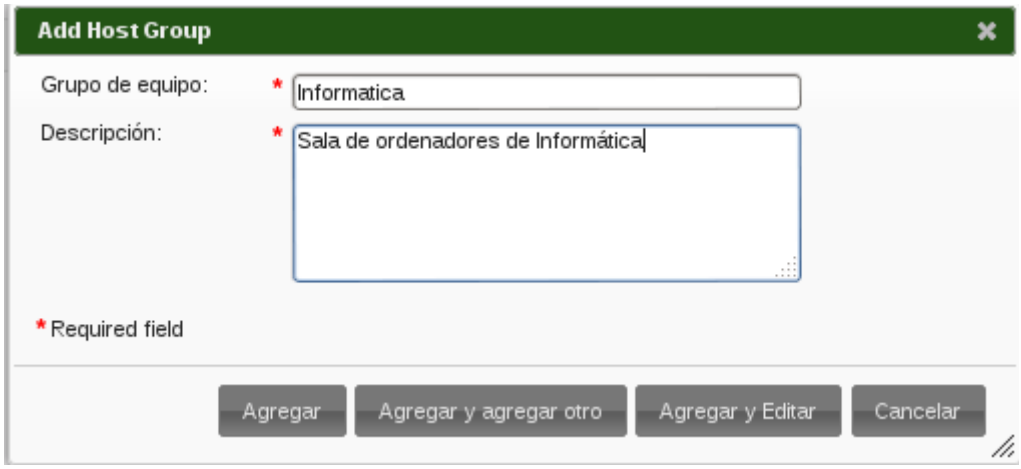
Si le damos a editar tenemos mas opciones que se pueden configurar, como un grupo de equipo, roles, información, etc.



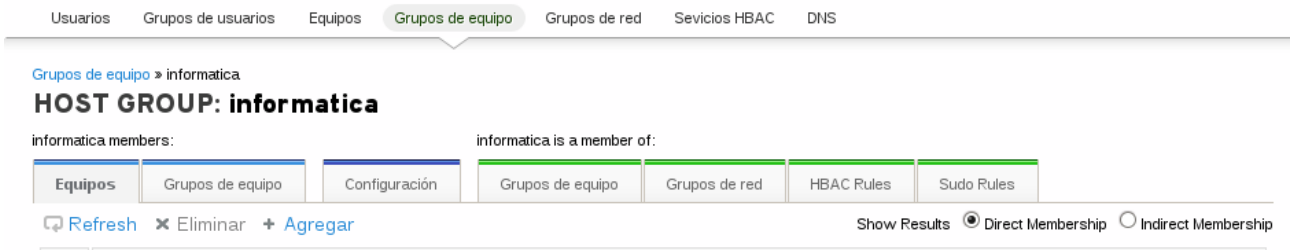
GRUPOS DE EQUIPOS

Los grupos de equipos es algo similar a los grupos de usuario, sólo que es para organizar los equipos.

Con el botón “Agregar” se pueden agregar nuevos grupos, como puede ser un despacho de “Informática” para el siguiente ejemplo.



Dentro de los grupos podemos editar como siempre las diferentes opciones, como agregar otros grupos dentro del grupo, soles, etc.

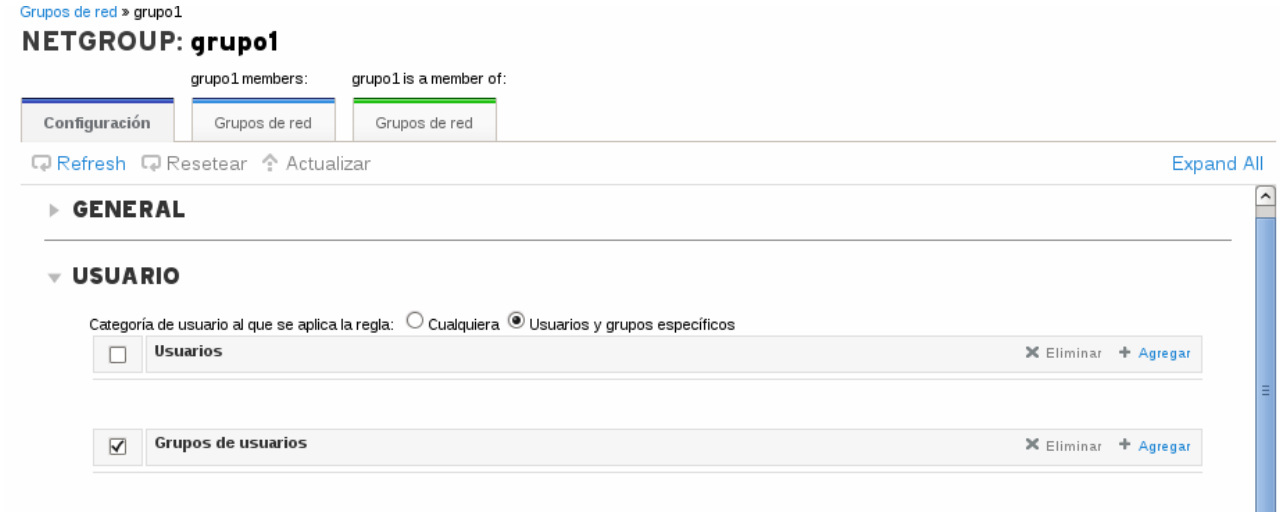


GRUPOS DE RED

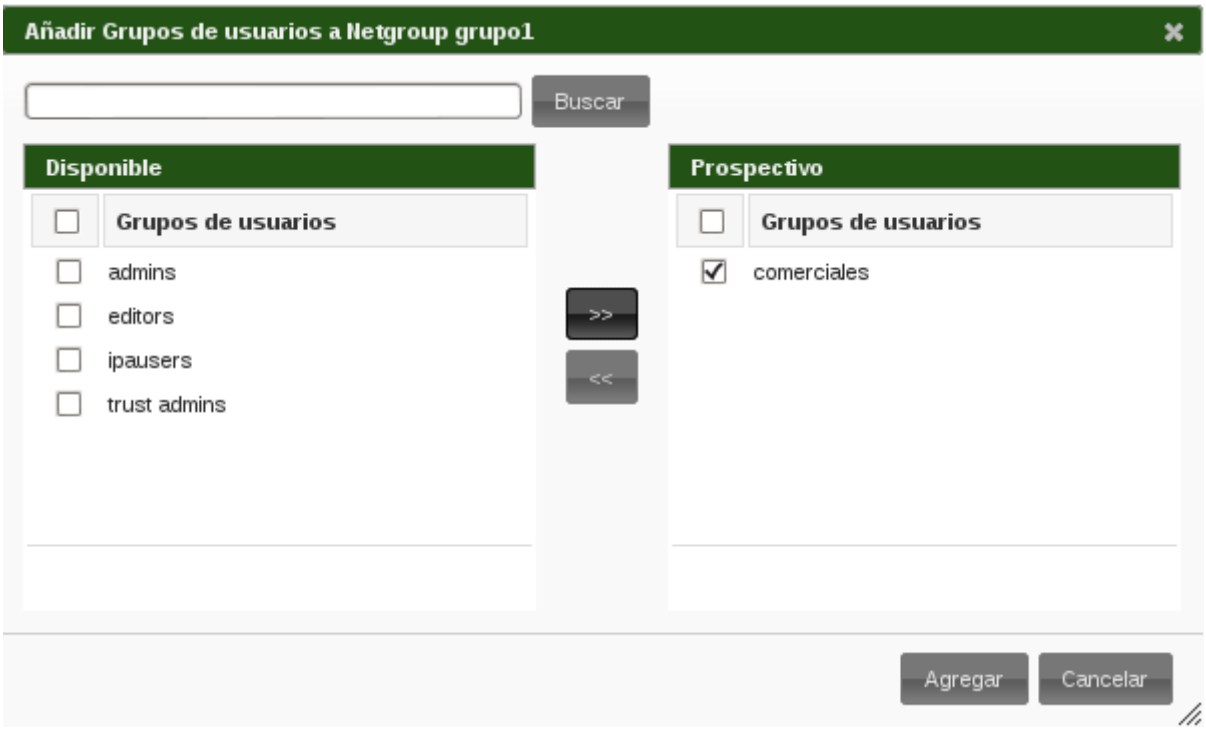
Esta opción nos permite dividir los usuario, grupos, equipos o grupo de equipos en grupos de red, lo cual permite tener mejor organizado el directorio activo.

Para agregar un nuevo grupo de red hay que darle al botón “Agregar” y rellenar los campos tal cual queramos realizar el planteamiento de la red.

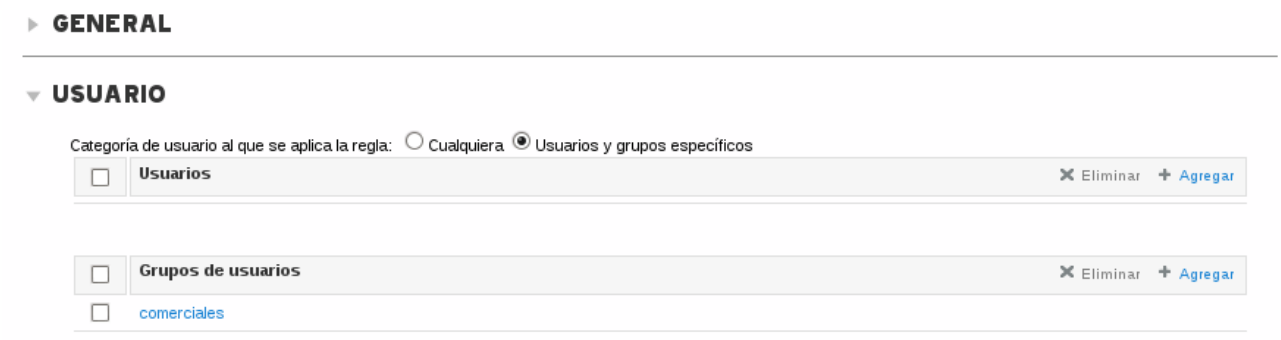
Presionamos sobre “Agregar y editar” y agregamos los componentes que queremos meter en el grupo.
Como ejemplo se va agregar un grupo de usuarios, por lo que desplegamos el menú usuario y seleccionamos “Grupos de usuarios”.



Le damos a agregar y movemos de derecha a izquierda el grupo deseado.



Ahora el grupo comerciales se encuentra dentro del grupo de trabajo “grupo1”

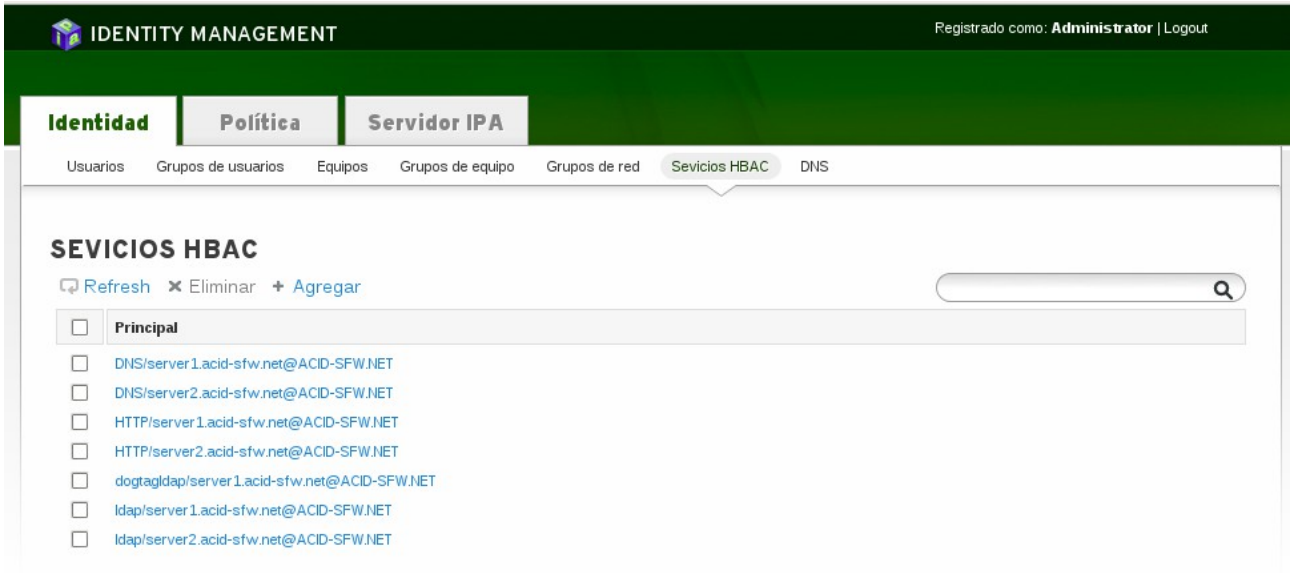


SERVICIOS HBAC

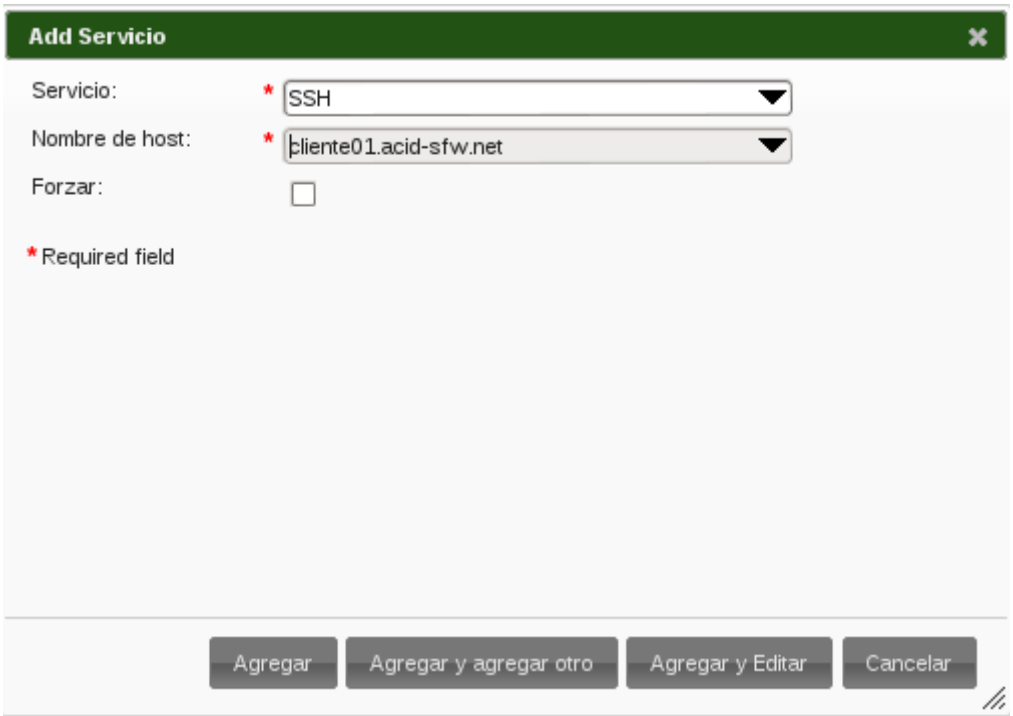
HBAC (Configuring Host-Based Access Control) es el servicio que se encarga del control de acceso en el domino FreeIPA. Las reglas definen quién puede acceder dentro del dominio. Estas reglas de control de acceso permiten el acceso con el resto de usuarios y hosts, que de forma predeterminada está negado.

Se puede configurar dentro de la pestaña “Identidad”, en la opción Servicios HBAC, y ya por defecto trae una serie de servicios habilitados.

Entre ellos las reglas DNS, HTTP, LDAP...



Un ejemplo sería agregar permiso SSH a cliente01@acid-sfw.net. Lo cual sería de la siguiente forma:



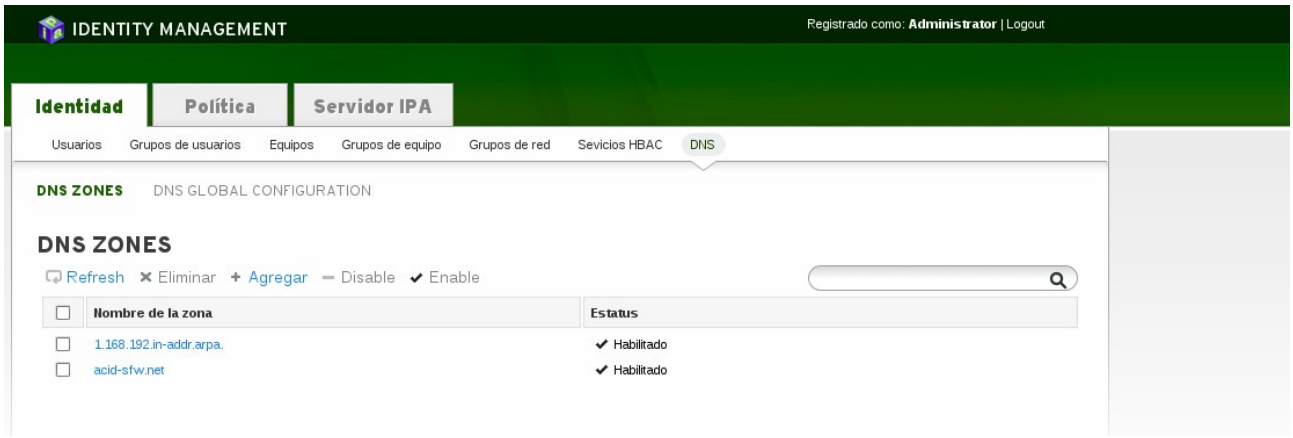
Aquí se ve como el servicio fue agregado una vez aceptado:

DNS

En este apartado es donde se configura todo lo referente a DNS, siempre y cuando se hubiese incluido en la instalación, ya que es un servicio adicional.

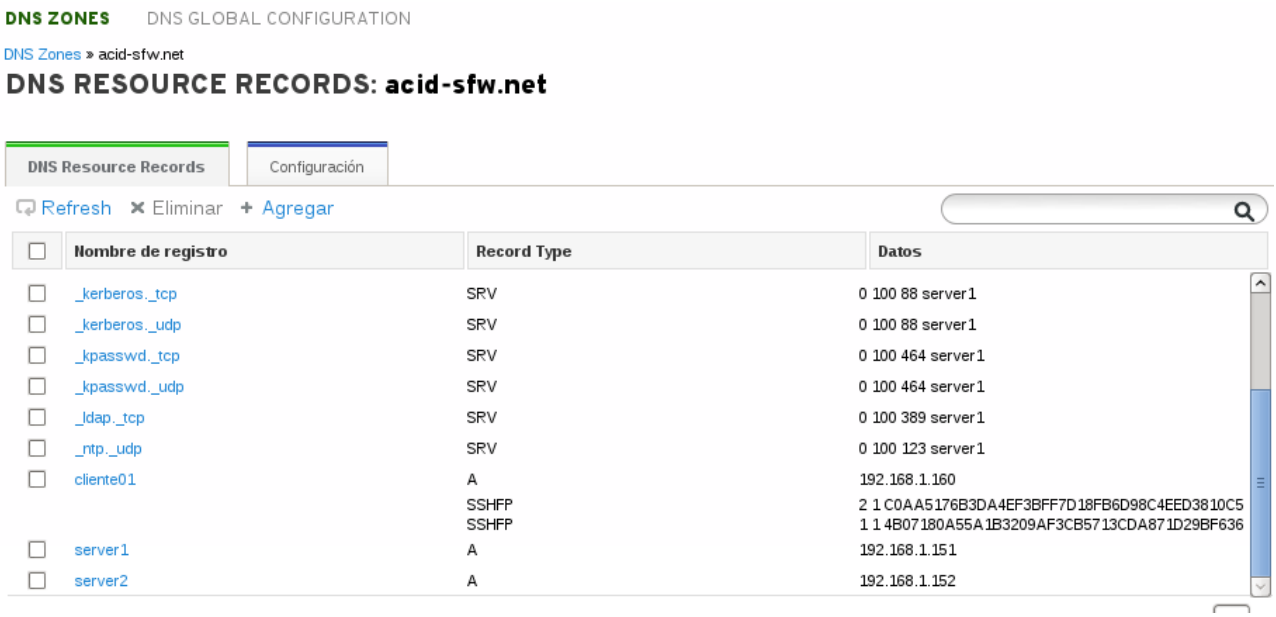
Su configuración es sencilla si se domina y controla el funcionamiento de DNS, ya que lo que utiliza la aplicación es un Bind9 con Kerberos.

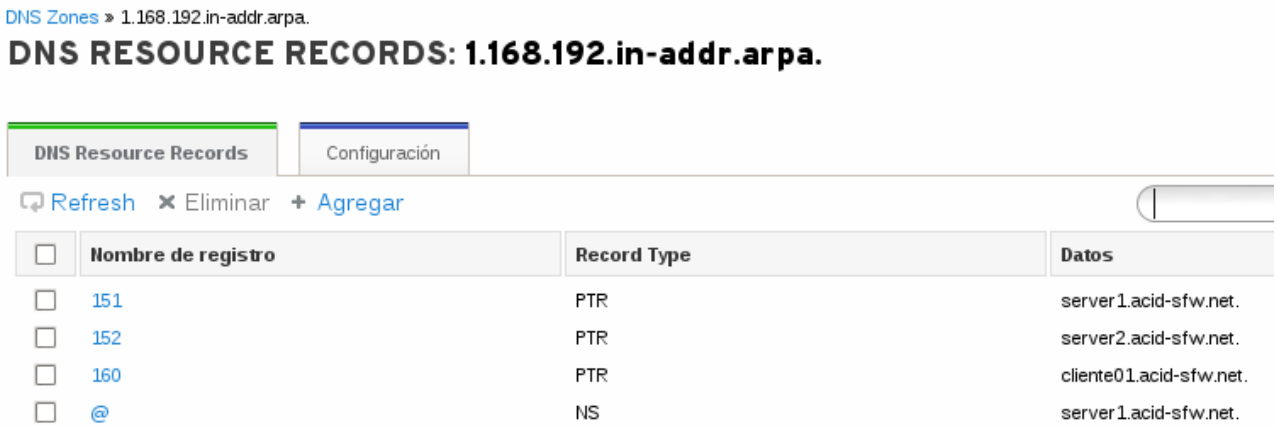
En la primera pantalla podemos observar la zona directa y la zona inversa del dominio.



Si queremos agregar la dirección de un cliente, como puede ser la del cliente01@acid-sfw.net hay que entrar en la zona directa y presionar sobre “Agregar”. Introducimos los datos del cliente01, marcamos para que se cree la zona inversa y le damos a agregar.

Ahora aparecerá tanto en la zona inversa como en la zona directa.



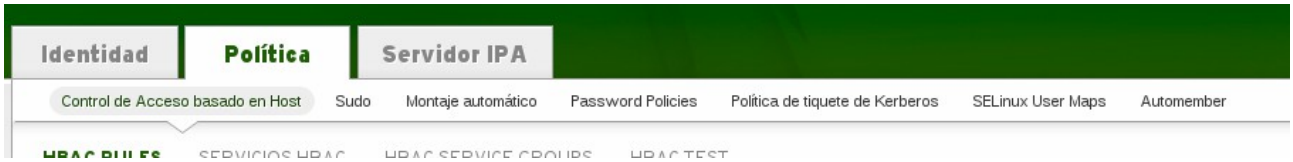


Dentro de las zonas, podemos configurar opciones sobre el DNS que ya pusimos en la instalación, como cambiar el correo del administrador, el tiempo de validez del DNS servido, etc.

POLÍTICA

En este apartado nos encontramos todo lo referente a los controles de acceso y políticas de seguridad de FreeIPA.

Estas opciones se pueden encontrar en la pestaña “Política” de la página principal del servidor Freeipa.



CONTROL DE ACCESO BASADO EN HOST

En este menú encontramos las formas de controlar el acceso y realizar test para comprobar su funcionamiento.

HBAC RULES

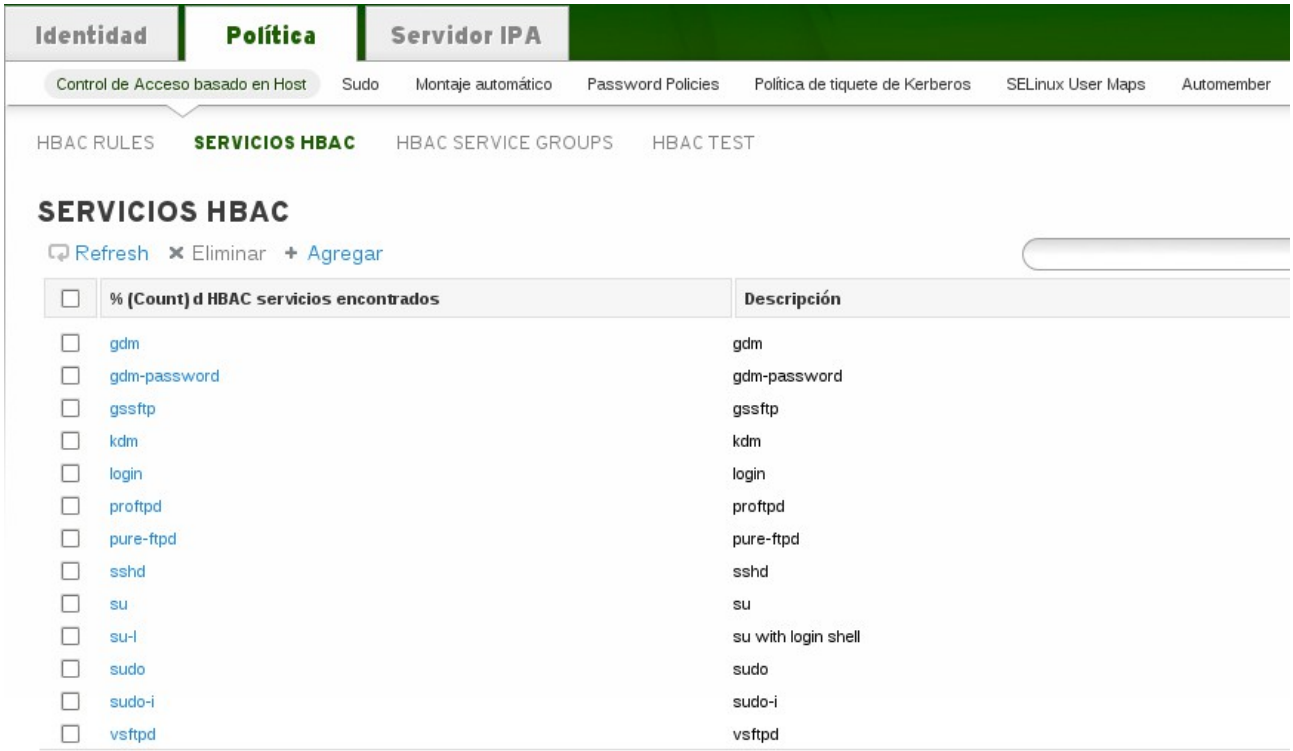
En HBAC RULES por defecto tiene una política de acceso abierta para todos los usuarios.

Esto podemos editarlo o crear una regla nueva desactivando la anterior.

En las opciones se encuentra la posibilidad de añadir usuarios y grupos, aparte de poder elegir en que tipos de servicios se pueden hacer los accesos por regla general.

SERVICIOS HBAC

Por defecto hay una lista de servicios predefinidos bastante completa para poder añadir, como puede ser ssh, su, login, etc.

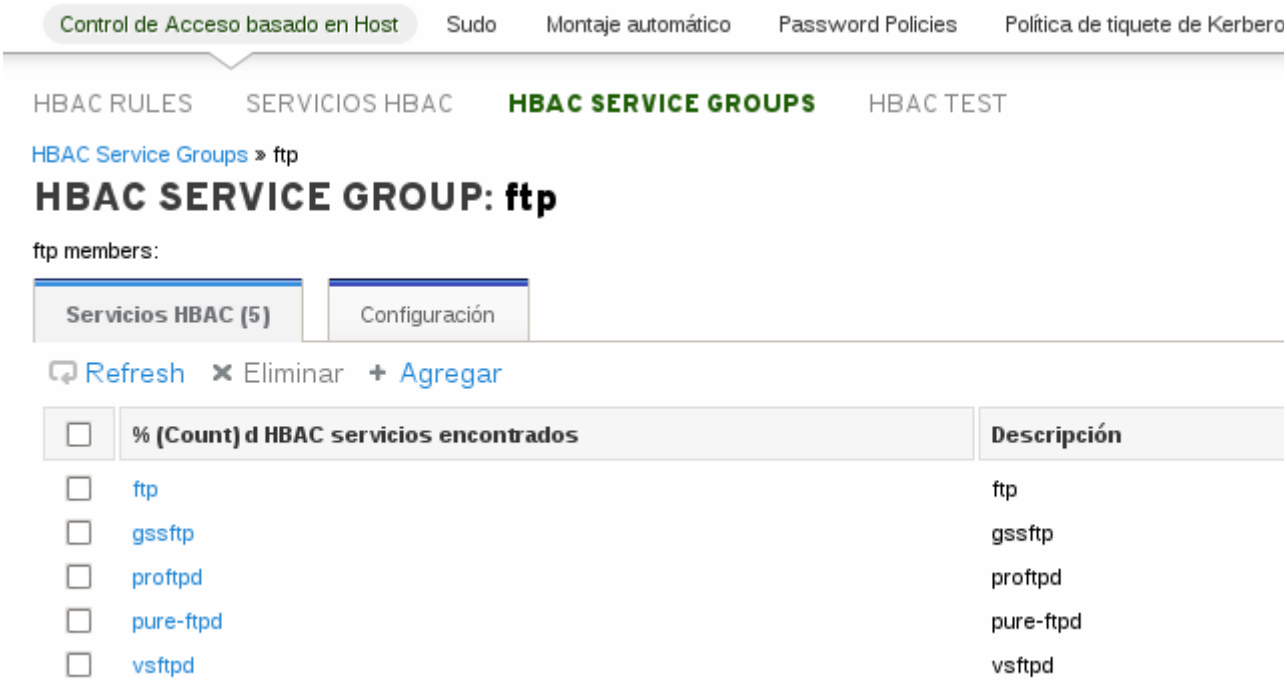


También es posible agregar nuevos servicios de forma manual con la opción “Agregar”.

HBAC SERVICE GROUPS

Con este apartado se puede organizar los servicios HBAC por grupos, ya que hay muchos que pueden ir juntos y así ahorrar trabajo a la hora de asignarlos.

Un ejemplo es ftp, el cual reúne algunos servicios ftp que pueden darse en el dominio.



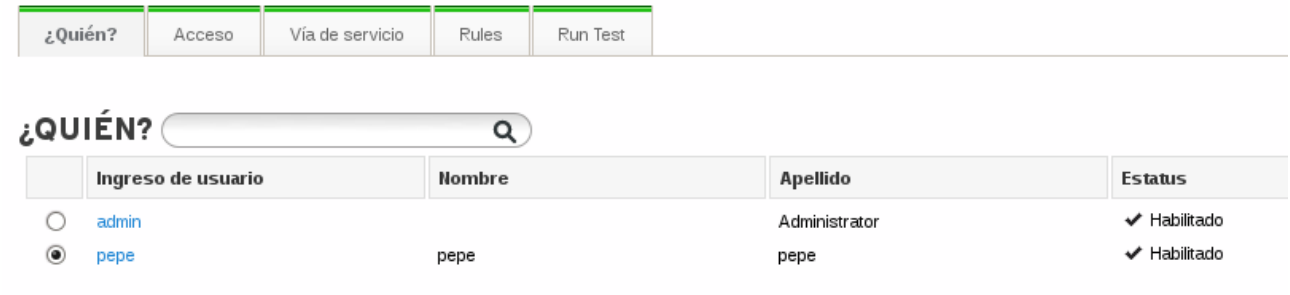
Aunque si realmente sólo queremos utilizar uno o mas de uno o queremos más control no se debería utilizar el grupo.

Como en los casos anteriores, podemos agregar y borrar grupos con el botón “Agregar”

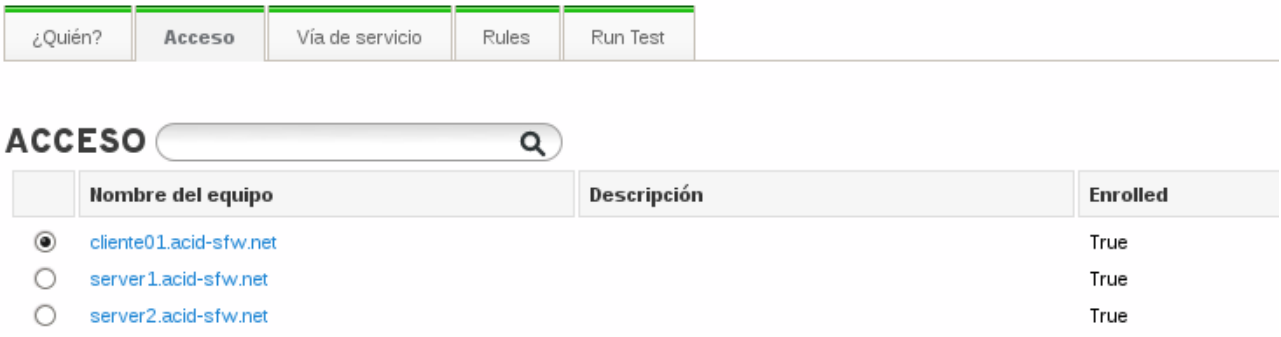
HBAC TEST

Esto es una herramienta para probar que los HBAC funcionan correctamente. En ella podemos especificar todo lo referente a usuarios, grupos y hosts que queremos probar con las reglas que hemos creado, modificado o eliminado con anterioridad.

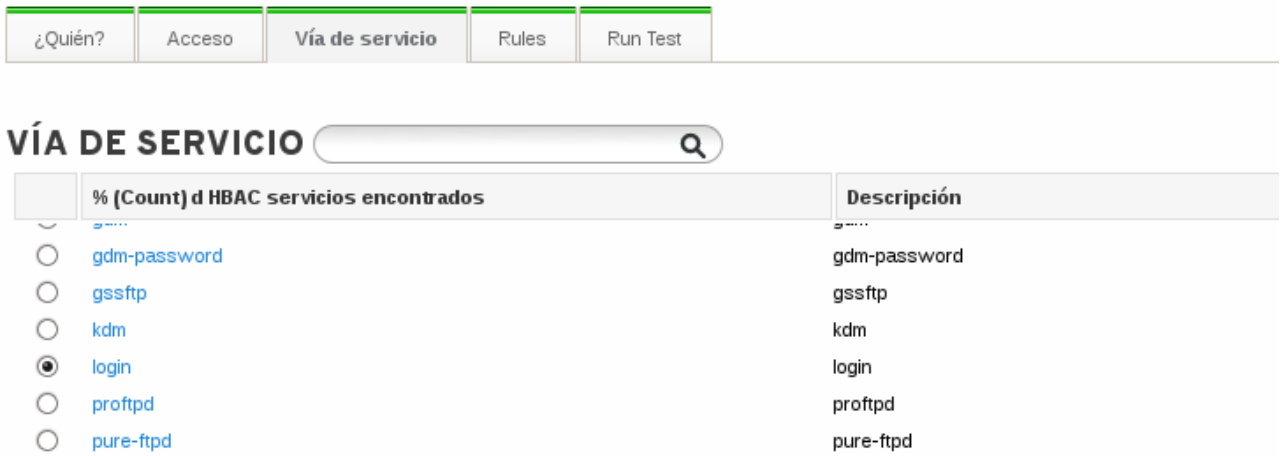
Para probarlo se va a realizar una prueba de login con el usuario “pepe”. Para hacerlo hay que seleccionar el usuario pepe en la primera pregunta.



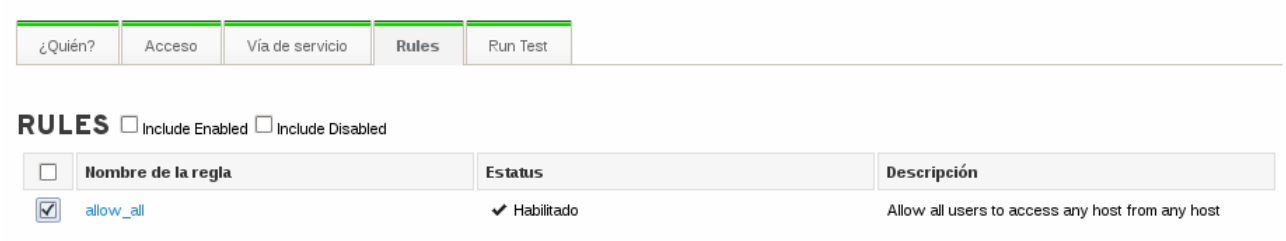
Después de darle a “Next” seleccionamos el nombre del equipo del cual queremos comprobar el acceso.



Le damos a “Next” y seleccionamos el servicio que hay que comprobar.



Seleccionamos el rol

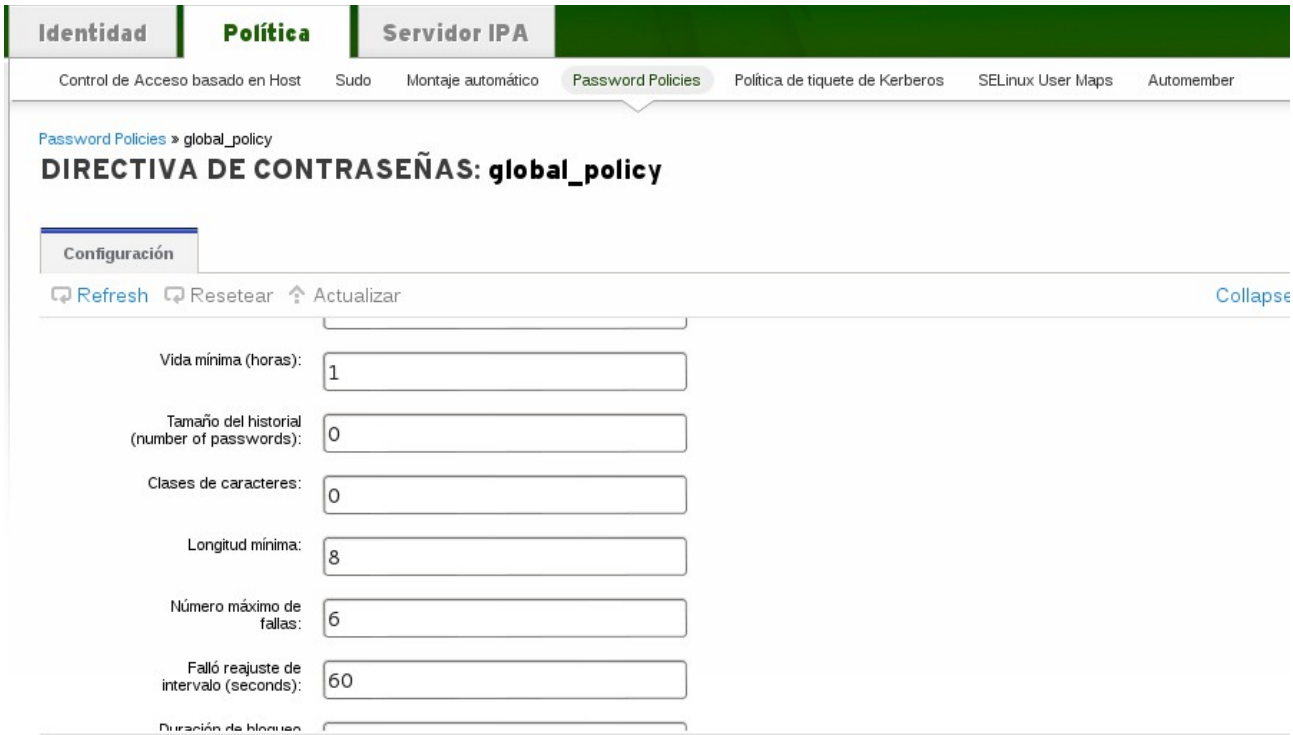


Y cuando ya estemos en la última pestaña le damos a “Run Test”

Como vemos, el acceso está permitido, por lo que la configuración funciona correctamente.

PASSWORD POLICIES

Aquí podemos editar todo lo referente a la creación de claves, el tiempo de validez, el tipo de caracteres, longitud, el tiempo de reintento, las veces que se puede reintentar y la duración del bloqueo.



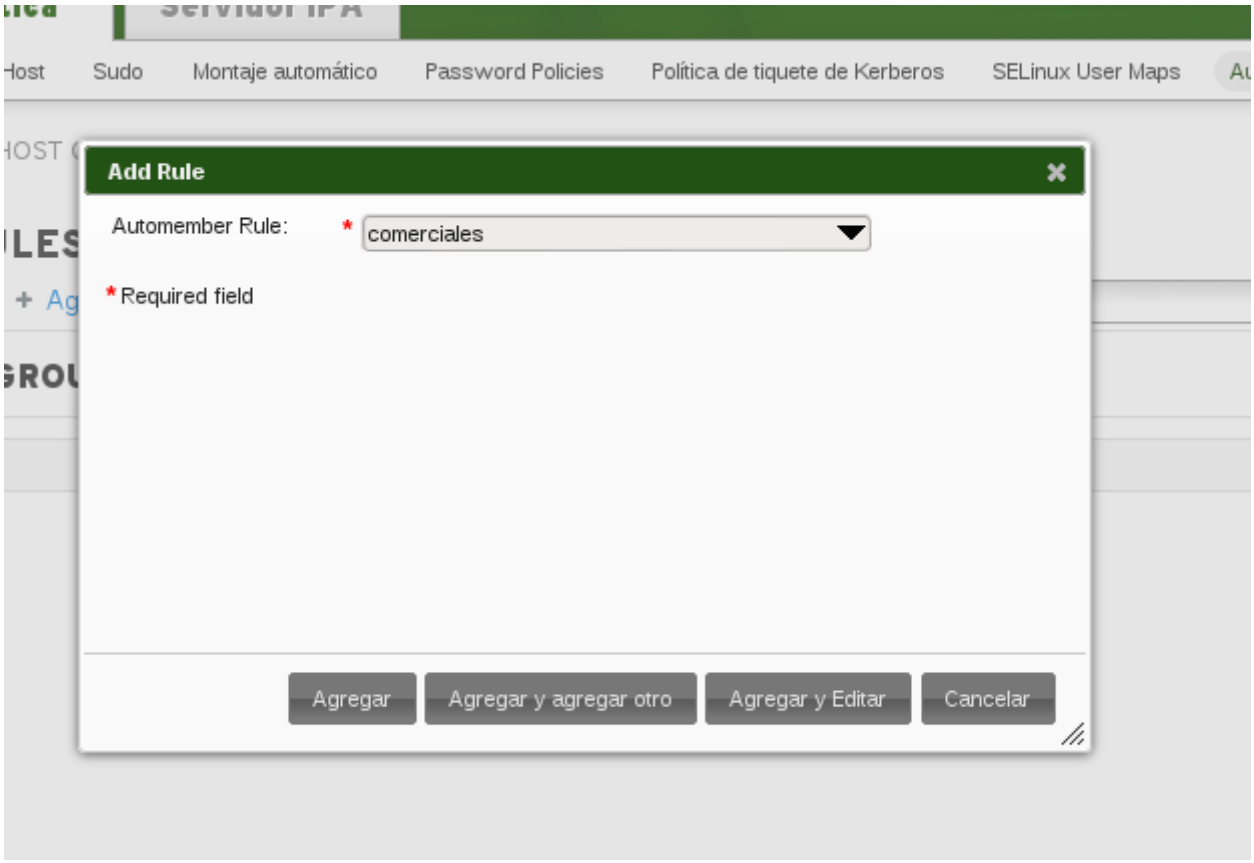
POLÍTICA DE TICKETS DE KERBEROS

En este punto podemos configurar el tiempo de renovación máximo y la vida de cada ticket en segundos.

AUTOMEMBER

Con automember existe la posibilidad de que entren miembros de forma automática, especificando el tipo de usuario y en que grupo se encontrará.

Para agregar miembros automáticos hay que presionar sobre “Agregar” y seleccionar el grupo a los que se asignarán de forma predeterminada.



Al igual que se puede hacer con los grupos de usuario, también es posible hacerlo con los hosts.

CONFIGURACIÓN DE SERVIDOR IPA

Estas configuraciones se encuentran en la pestaña “Servidor IPA” del panel web de administración. En este apartado se administra la configuración del servidor, ya sean los roles, los permisos de autoservicio, las delegaciones, los rangos de identidades, las zonas de confianza o la configuración por defecto.

CONTROL DE ACCESO BASADO EN ROLES

ROLES

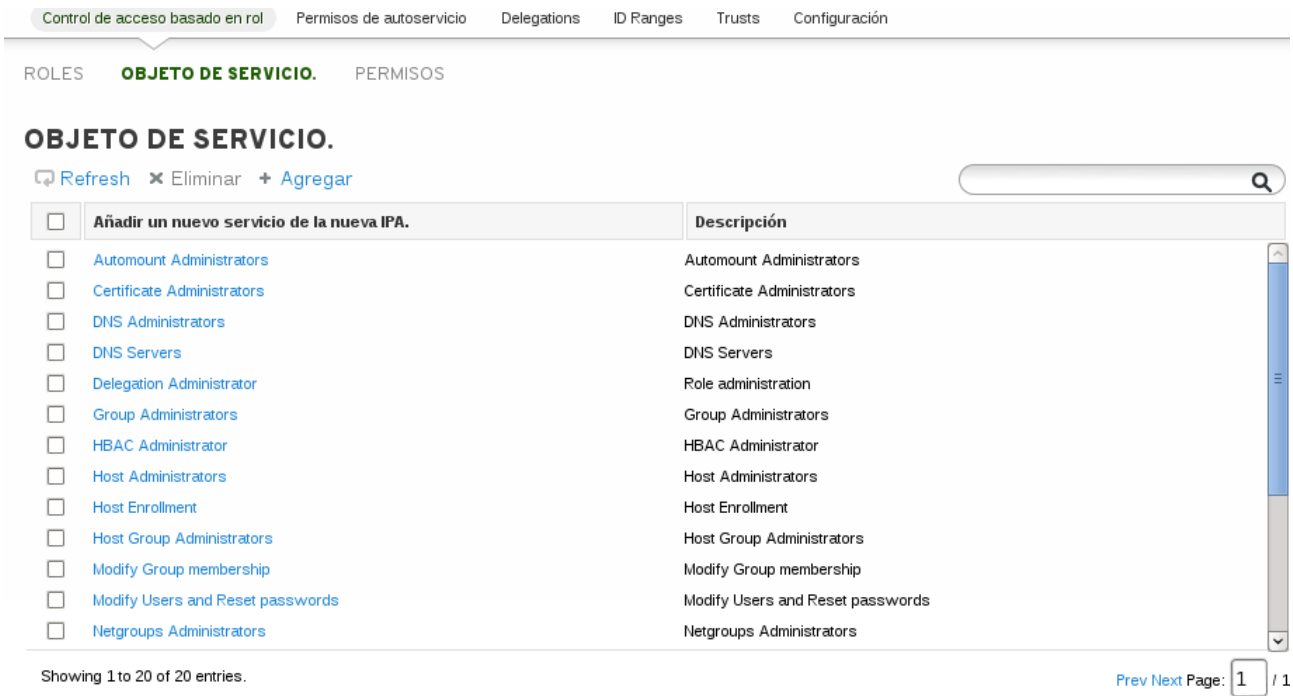
Es el control de acceso que define los derechos a los usuarios o otros objetos con el fin de realizar operaciones con otros usuario o objetos. Esto incluye la política de tickets de Kerberos.

Aquí se muestra los roles predeterminados en FreeIPA, los cuales se pueden editar o eliminar. Aparte también es posible agregar nuevos no predefinidos.

OBJETOS DE SERVICIO

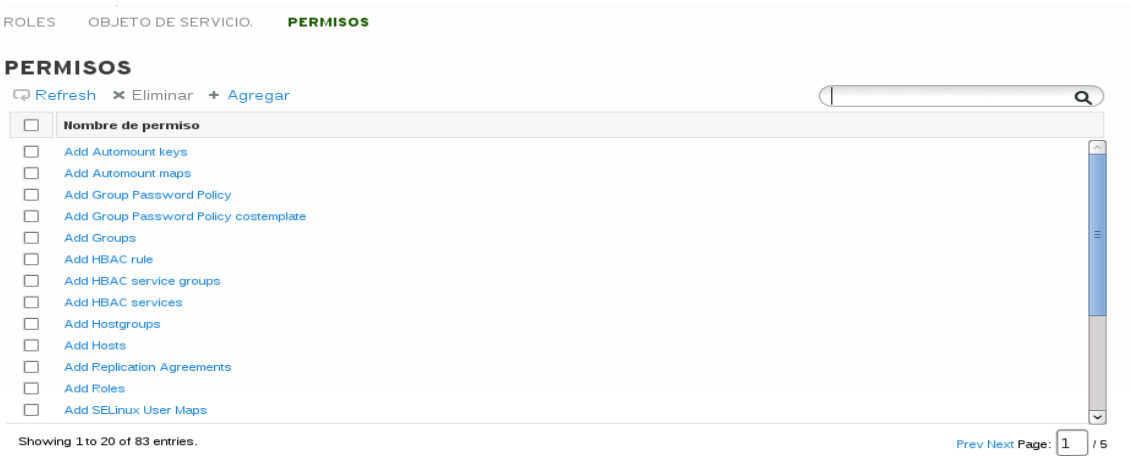
Estos son los objetos a los que se les puede aplicar los roles, que en su mayoría son grupos de tipos de usuarios o host.

Como se puede apreciar, también se pueden borrar, editar y agregar nuevos objetos donde aplicar roles.



PERMISOS

En permisos se puede definir que tipo de servicios podemos aplicar a los diferentes usuarios y grupos.

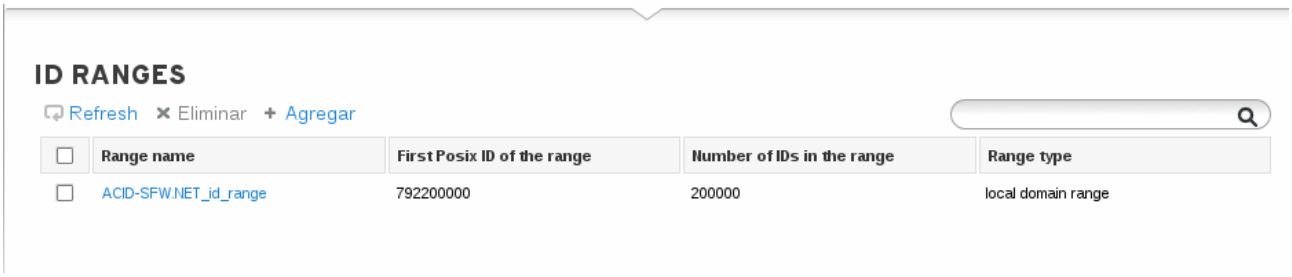


PERMISOS DE AUTOSERVICIO

ID RANGES

Son identificadores únicos de 32 bits de los objetos de usuario/grupo en el ámbito de un dominio del directorio activo.

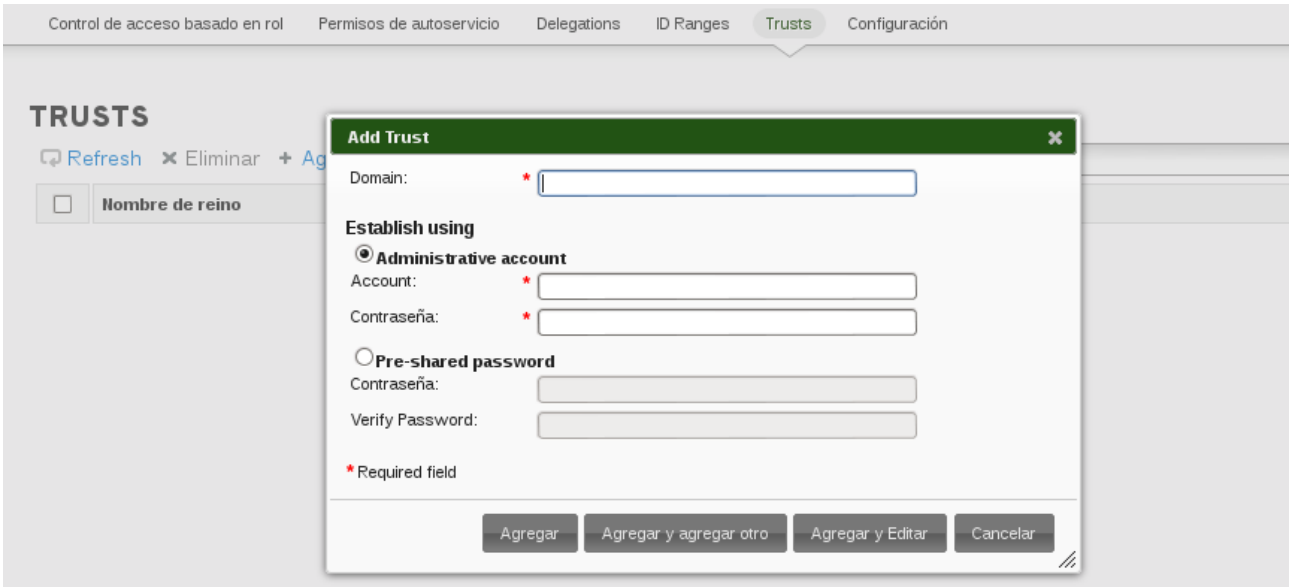
En caso de querer exportar objetos de usuario/grupo necesitamos generar un SID. Todo SID es una cadena única para el dominio para así poder mantener cada objeto con una clave diferente.



TRUSTS

Los trusts utilizan componentes de Samba que se incluyen en el directorio activo. Para agregar este tipo de servicio hay que presionar sobre “Agregar” y introducir los datos y así poder configurarlo.

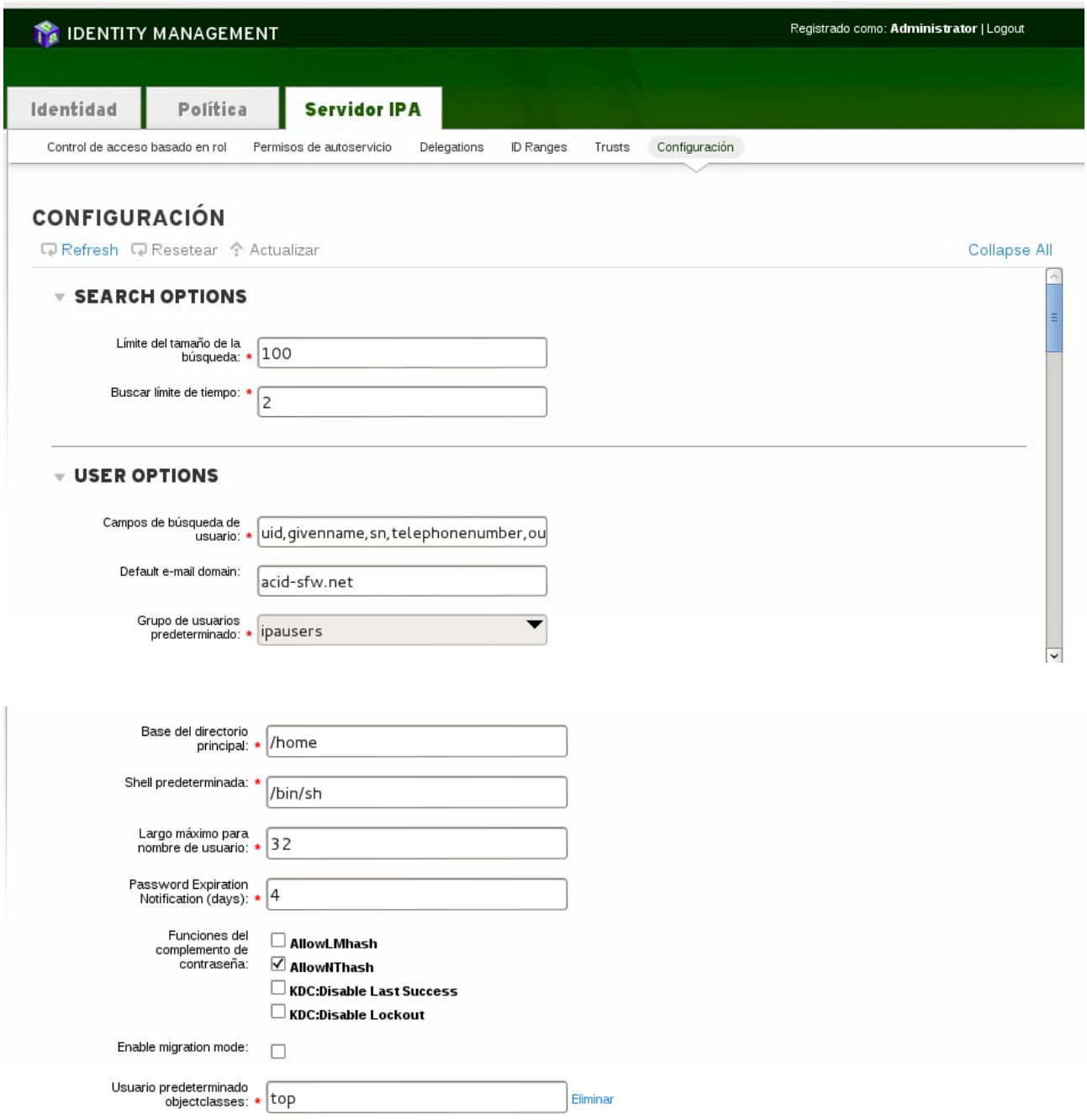
Para poder utilizar este componente hay que instalar el paquete server-trust-ad.

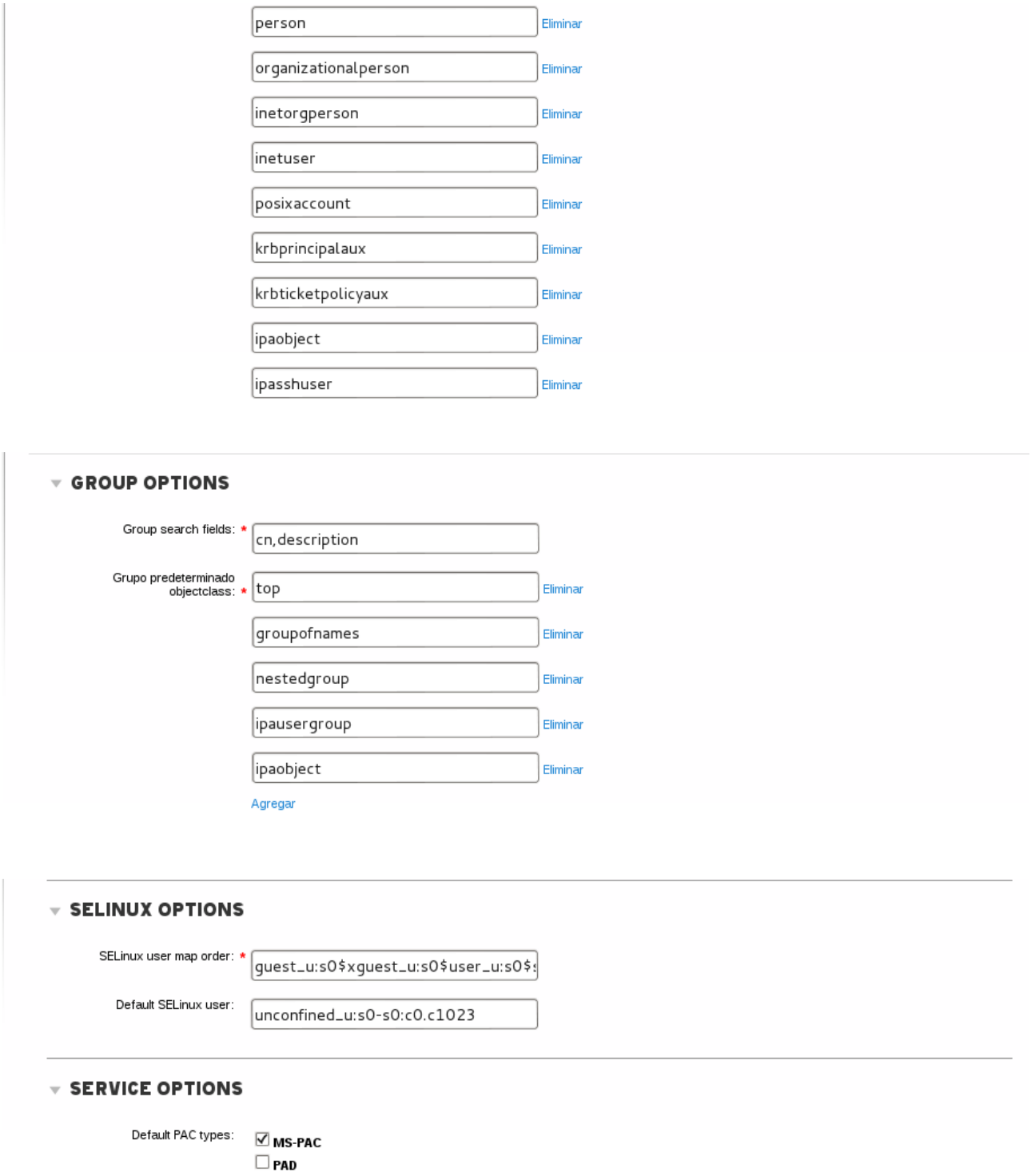


CONFIGURACIÓN

Este es el panel de configuración general de FreeIPA, en el cual podemos adecuar las opciones por defecto del directorio activo.

Las opciones de configuración son las siguientes:





Como podemos ver, es posible modificar directorios por defecto, las opciones de SELINUX, etc.

KERBERIZAR NFS SERVER

SERVIDOR

Para poder montar el servicio NFS en clientes hay que realizar la siguiente tarea en el servidor:

```
# yum install nfs-utils
```

Editamos la configuracion de NFS.

```
# nano /etc/sysconfig/nfs
```

```
SECURE_NFS=”yes”
```

Especificamos el dominio

```
# nano /etc/idmapd.conf
```

```
Domain = acid-sfw.net
```

configurarmos el fichero exports donde añadimos la información de kerberos.

```
# /export  *(rw,sec=sys:krb5:krb5i:krb5p)
```

Reiniciamos el servicio

```
# service nfs restart
```

CLIENTE

En el lado del cliente también modificamos los mismos archivos

Editamos la configuracion de NFS.

```
# nano /etc/sysconfig/nfs
```

```
SECURE_NFS=”yes”
```

Especificamos el dominio

```
# nano /etc/idmapd.conf
```

```
Domain = acid-sfw.net
```

Iniciamos el demonio GSS.

```
# service rpc.gssd start
```

Por último montamos el directorio añadiéndolo al fstab

```
# echo "$NFSSERVER:/this /mnt/this nfs4
sec=krb5i,rw,proto=tcp,port=2049" >>/etc/fstab
```

```
# mount -av
```

CONCLUSIÓN

FreeIPA es una gran apuesta en software libre frente al directorio activo de Windows, ya que consigue reunir la mayoría de servicios necesarios para que esta función sea muy completa. También hay que tener en cuenta que tiene mucha posibilidad de expansión, como la posibilidad de añadir servicios de DNS, samba 4, NFS, etc.

Una gran limitación es que como servidor sólo es posible su instalación en RedHat y CentOS por el momento, y que como clientes sólo podemos agregar otros sistemas RedHat, CentOS, HP-UX y AIX System.

Otro problema es que sólo el administrador puede restablecer las contraseñas y no tenga un servicio de restablecimiento de la misma de parte del cliente.

Un resumen sería que FreeIPA puede llegar a ser un gran competidor de Windows Server, pero aún le queda mucho camino y más teniendo en cuenta otras alternativas como Samba 4 con una compatibilidad más amplia.

REFERENCIAS

http://docs.fedoraproject.org/en-US/Fedora/15/html-single/FreeIPA_Guide/

http://sgros.blogspot.com.es/2012/06/installing-freeipa-on-minimal-centos.html

http://inbaudwetrust.com/2014/02/12/freeipa-serverclient-setup-on-centos-6-5/

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

http://www.howtoforge.com/installing-freeipa-with-replication

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

http://serverfault.com/questions/560772/using-freeipa-for-centralized-sudo-using-sssd-for-sudoers