DISICO

Instalación Free BSD 7.0 Servidor DNSI-DNSE

Manual

Instalación FreeBSD 7.0 Servidor DNSI – DNSE DISICO

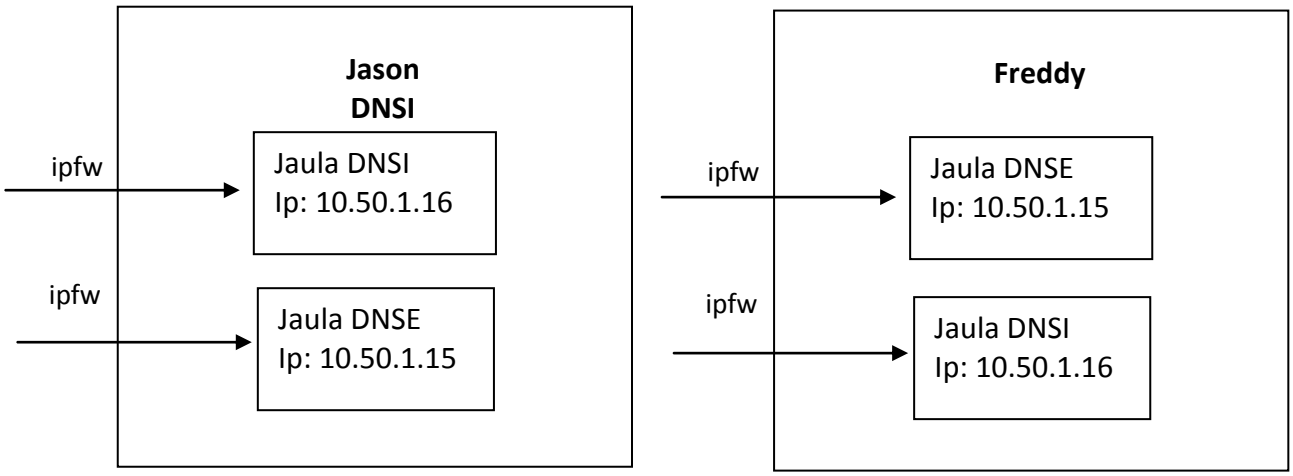
Introducción

Se remplazarán 2 servidores de DNS, uno será el DNS interno y el otro DNS externo, ambos servidores se encontrarán con jails (jaulas).

Ambas máquinas contarán con 2 jaulas, ambas contarán con DNS interno (DNSI) y DNS externo (DNSE), para tener redundancia en los servidores.

El ingreso a las jaulas será restringido con ipfw, además de contar con ssh con encriptación asimétrica.

La máquina donde se instalarán los servidores se encuentran con nivel RAID 1, lo cual permitirá respaldo de discos, y redundancia en caso de daños de alguno de ellos. El esquema que se realizará será el siguiente:



Configuración de discos RAID

Para la instalación del OS FreeBSD se necesita que estos discos estén funcionando con el nivel de seguridad RAID 1. Para chequear que esto funcione correctamente se realiza el siguiente tipo de pruebas.

En las BIOS de la máquina se deben realizar los siguientes cambios:

1º En Main/SATA Controller Mode Option se pone la opción Enhanced (mejorado).

2º Luego se desplegaran 2 opciones más SATA RAID Enable y ICH Raid CodeBase, la primera opción se marca como Enabled (habilitado) y la segunda se deja como Intel

3º Una vez terminada esta configuración en la BIOS se procede a entrar a la configuración de RAID, con Ctrl. + i, nos mostrará un menú en el cual pide crear un volumen de disco, luego la opción siguiente, señala el nivel RAID que se desea, en este caso particular se pone el nivel RAID 1. luego se guardan los cambios.

4º En este paso comienza la instalación de OS FreeBSD 7.0, este se instala en la partición de RAID, es decir, en arxx.

Obs: FREEBSD NUNCA PUEDE PARTIR CON LA CONTROLADORA, SIEMPRE SE DEBE DESACTIVAR

Para desactivar la controladora SATA Controller Mode Option se pone Compatible

5º Una vez instalado el OS, se realiza una prueba, se crea un directorio o archivo en el OS, luego se apaga y se saca uno de los discos para luego partir con uno de ellos y ver si el respaldo se produjo.

Set de pruebas 02 para verificación de RAID 1

Se debe instalar FreeBSD 7.0 en la máquina, luego se procederá a realizar la configuración del servidor, es decir, nombre, ip, entre otros, de tal forma que tenga navegabilidad.

Con este set de pruebas se busca darle una mayor carga al servidor para poder comprobar que se puede realizar RAID 1 en la máquina con mayor información cargada en el servidor.

Una vez instalado este servidor se procederá a crear la jaula base y 2 jaulas normales, una vez realizada esta carga se procederá a ver el resultado del respaldo con el nivel RAID 1, sacando los discos.

#Ifconfig em1 10.50.1.177 netmask 255.255.255.0
#route add default 10.50.1.254

Para las pruebas de Raid 1

1.- Se crean 3 jaulas
Dnsi: 10.50.1.178
Dnse: 10.50.1.179
Home: 10.50.1.180
2.- En la jaula DNSI, se instala Bind 9
3.- En la máquina (10.50.1.177) se instala Apache y SSH
4.- Se compila el kernel agregando las siguientes líneas

 # cd /usr/src/sys/i386/conf/
 # cp GENERIC FREDDY

#options BRIDGE # linea alternative //No lo reconoce FreeBSD 7.0
options IPFIREWALL # Activa firewall ipfw
options IPFIREWALL_VERBOSE
options IPFIREWALL_VERBOSE_LIMIT
options IPFIREWALL_DEFAULT_TO_ACCEPT
options DUMMYNET #permite realizar adminstracion de ancho de banda

vi **etc/rc.conf**

firewall_enable="YES"
firewall_type="OPTIMUS"
firewall_quiet="YES"

Al cargar el servidor con toda la información señalada, los respaldos se hacen sin problemas, tal como lo señala la tabla SET de pruebas 01. Luego de realizar estas pruebas se considera poner un nuevo HD modificando la controladora para así poder ver la situación en que un HD bueno pueda copiar la información por RAID 1 a un HD nuevo.

Las pruebas que se consideraron no cumplieron con las expectativas, es decir, en el caso que uno de los HD falle, no es posible poner un HD Nuevo y respaldar de forma de RAID 1, ya que se producen los problemas ya conocidos en la controladora realizados en la segunda iteración de la prueba de discos RAID 1, por lo que una alternativa (aun no comprobada) sería el respaldo bit a bit del HD bueno a un HD nuevo.

Esta prueba se realizó cambiando la controladora de Intel a Apaptec copiando de un HD con OS e información instalada (mostradas en SET de pruebas 02) a un HD nuevo, esto falló.

2.3.- Distribución de particiones

HD: 150 GB con RAID 1

Var: 55GB 36%
Usr: 50GB 33%
Swap: 4 GB3%
Tmp: 15 GB 10%
Home: 20 GB 13%
/: Lo restante

Checklist de configuraciones y aplicaciones		
Acciones	**Aplicaciones**	**Versiones**
Máquina Jason		
1	Conf TCP / IP Ip D-G DNS	
	Configuracion de Maquina rc.conf, hosts, host.conf, resolv.conf, bash, mc.	
2	Creacion de jaulas dnsi, dnse, dnsi.resp, dnse.resp	
3	Agregar configuración de jaulas en rc.conf	
4	Adm. de usuarios	
5	SSH con certificado	
6	Ipfw	
DNSI - DNSE		
5	Configuracion de Maquina rc.conf, hosts, host.conf, resolv.conf, bash, mc.	
6	Bind 9	
7	Adm de usuarios	
8	SSh con certificado	
9	Compilar Kernel para Adm BW	
10	Zonas uv (exportar desde antiguo DNS)	

Instalación de Ports en la máquina

Los Ports se descargan desde internet, ya que al instalar el FreeBSD en el server no se instalan los ports.

Primero se dejan los últimos ports en el directorio /root luego posicionándome dentro del directorio usr de la jaula descomprimo los ports,.

jason# cd /usr/
jason# gzip -dc /root/ports.tar.gz | tar -xvf –

III JAULAS
Construcción de una jaula base

Ejecutando el comando sysinstall en la máquina en la ruta configure/disttribution/src es posible obtener las fuentes que quedarán almacenadas en /usr/src.

Esto generalmente tarda varios minutos (100 min app)

Se presentan a continuación todos los requerimientos para crear e instalar una jaula base que puede ser clonada posteriormente para obtener jaulas según se necesite.

Antes utilizar el shell cts..

jason#tcsh
jason#setenv D /usr/jails/baseJail
jason#cd /usr/src
jason#mkdir –p $D
jason#make world DESTDIR=$D
jason#cd etc
jason#make distribution DESTDIR=$D

Con lo anterior se consigue poblar el directorio /usr/jails/baseJail con una estructura de archivo similar al sistema base, es decir, dentro de este directorio existen los directorios /bin, /etc y /var, entre otros.

Para creado de jaula DNSI

jason# mkdir /usr/jails/dnsi (nombre jaula)
jason # tcsh
You have mail.
jason # cd /usr/jails/baseJail
jason # tar -cpf - . | tar -C /usr/jails/dnsi -xpf -

De forma análoga se crean las otras jaulas DNSE, DNSI2 y DNSE2

Asignación de ip a la jaula y "link"con kernel a la máquina

jason# ifconfig em1 inet alias 10.100.6.178
jason# mount -t devfs devfs /usr/jails/dnsi/dev
jason# cd /usr/jails/dnsi
jason# ln -sf dev/null kernel

Comando para iniciar jaula

jason# jail /usr/jails/dnsi dnsi 10.50.1.178 /bin/sh etc/rc
Loading configuration files.
dnsi
Setting hostname: dnsi.
Generating nsswitch.conf.
Generating host.conf.
Creating and/or trimming log files:.
ln: /dev/log: Operation not permitted
Starting syslogd.

Activando ping a las jaulas

jason# echo security.jail.allow_raw_sockets=1 >> /etc/sysctl.conf

Archivos a configurar

Los archivos a configurar son hosts y resolv.conf ubicado en el directorio etc

Archivo hosts – Jaula DNSI

```
dnsi# cat /etc/hosts
::1             localhost localhost.my.domain
127.0.0.1       localhost localhost.my.domain
10.50.1.178     dnsi.uv.cl      dnsi
10.50.1.178     dnsi.uv.cl.
#
```

Archivo resolv.conf – Jaula DNSI

```
dnsi# cat /etc/resolv.conf
nameserver 10.50.1.16
dnsi#
```

Comandos básicos de jaulas

jls: Lista las jaulas creadas y activas en el servidor

```
jason# jls
  JID  IP Address      Hostname                Path
    4  10.50.1.181     dnsi2                   /usr/jails/dnsi2
    3  10.50.1.180     dnse2                   /usr/jails/dnse2
    2  10.50.1.179     dnse                    /usr/jails/dnse
    1  10.50.1.178     dnsi                    /usr/jails/dnsi
jason#
```

exec 1 /bin/sh: entra a la jaula con JID 1, en este caso a la jaula dnsi

```
jason# jexec 1 /bin/sh
# tcsh
dnsi#
```

rc.conf de máquina con información de jaulas

```
################## Declaracion de Jaulas ###################################

jail_enable="YES"
jail_list="dnsi dnse"

#################### Jaula DNSI ####################################

ifconfig_em1_alias0="inet 10.50.1.178 netmask 255.255.255.0"
jail_dnsi_rootdir="/usr/jails/dnsi"
jail_dnsi_hostname="dnsi"
jail_dnsi_ip="10.50.1.178"
jail_dnsi_exec_start="/bin/sh /etc/rc"
jail_dnsi_devfs_enable="YES"
jail_dnsi_fdescfs_enable="YES"
jail_dnsi_procfs_enable="YES"

#################### Jaula DNSE ####################################

ifconfig_em1_alias1="inet 10.50.1.179 netmask 255.255.255.0"
jail_dnse_rootdir="/usr/jails/dnse"
jail_dnse_hostname="dnse"
jail_dnse_ip="10.50.1.179"
jail_dnse_exec_start="/bin/sh /etc/rc"
jail_dnse_devfs_enable="YES"
```

Compilación de Kernel

Se compila el kernel para agregar herramientas de administración de ancho de banda, el nuevo kernel se llamara JASON.

 # cd /usr/src/sys/i386/conf/
 # cp GENERIC JASON

Editamos con:
 # vi JASON

Y se agrega lo siguiente

```
options     BRIDGE                      # linea alternativa #Para  FBSD 70 no se coloca esta opción
options     IPFIREWALL                  # Activa firewall ipfw
options     IPFIREWALL_VERBOSE
options     IPFIREWALL_VERBOSE_LIMIT
options     IPFIREWALL_DEFAULT_TO_ACCEPT
options     DUMMYNET                    #permite realizar adminstracion de ancho de banda
```

Esc :wq!

Compilación del Kernel

Ahora se debe compilar el Kernel, para esto se realizan los siguientes pasos:

 # /usr/sbin/config JASON
 # cd ../compile/JASON
 # make depend
 # make
 # make install

Con esto ya se encuentra instalado el Nuevo Kernel (**JASON**) del sistema operativo solo basta con reiniciar el servidor.

Instalación de ports en la jaula

Para la instalación de ports en las jaulas:

Primero se dejan los últimos ports en el directorio **/root** luego posicionándome dentro del directorio **usr** de la jaula descomprimo los ports, esto se realiza para cada una de las jaulas.

jason# cd /usr/jails/dnsi/usr/

jason# gzip -dc /root/ports.tar.gz | tar -xvf –

5 DNSI + Samba + Wins + Active Directory

Funcionamiento de DNSI con Samba y servidor de Dominio (Wins)

DNSI (Bind 9+ Samba3)

Instalación de Bind 9

Para trabajar con DNSI es necesario instalar bind 9 en ambas jaulas

dnsi# cd /usr/ports/dns/bind9
dnsi#make
dnsi#make install

>> Agregar linear rc.conf

agregar en el **/etc/rc.conf** de la jaula

named_enable="YES"

>> Agregando ip donde va a escuchar el DNS (En este caso es la de la jaula)

En el archivo **/etc/namedb/named.conf** debo agregar la ip donde va a escuchar el **DNS**, en el caso de la jaula que se está configurando será la 10.50.1.116 Esto sería en:

dnsi# vi /etc/namedb/named.conf

```
//
// Refer to the named.conf(5) and named(8) man pages, and the documentation
// in /usr/share/doc/bind9 for more details.
//
// If you are going to set up an authoritative server, make sure you
// understand the hairy details of how DNS works.  Even with
// simple mistakes, you can break connectivity for affected parties,
// or cause huge amounts of useless Internet traffic.

options {
        directory       "/etc/namedb/master";
        pid-file        "/var/run/named/pid";
        dump-file       "/var/dump/named_dump.db";
        statistics-file "/var/stats/named.stats";

        allow-transfer { 200.6.103.241; 200.54.144.227; localhost; };
        allow-recursion { 10.100.0.0/16; 10.50.0.0/16; localhost; };
```

>> Agregando zonas

```
 type master;
 file "/master/127.0.0.in-addr.arpa";
};


zone "rapanui.uv.cl"{
        type master;
        allow-query { any; };
        file "rapanui.uv.cl.zone";
};


zone "rectoria.uv.cl"{
        type master;
        allow-query { any; };
        file "rectoria.uv.cl.zone";
};


zone "sanfelipe.uv.cl"{
        type master;
        allow-query { any; };
        file "sanfelipe.uv.cl.zone";
```

>> Chequeando named.conf

dnsi# named-checkzone uvalpo.cl /var/named/etc/namedb/master/uvalpo.cl.zone

```
[root@dnsi /var/named/etc/namedb]#
[root@dnsi /var/named/etc/namedb]# named-checkconf -z /var/named/etc/namedb/named.conf
zone 0.0.127.in-addr.arpa/IN: loading from master file /master/127.0.0.in-addr.arpa failed: file not found
_default/0.0.127.in-addr.arpa/IN: file not found
zone rapanui.uv.cl/IN: loaded serial 2009073101
zone rectoria.uv.cl/IN: loaded serial 2009073101
zone sanfelipe.uv.cl/IN: loaded serial 2009072901
zone procesos.uv.cl/IN: loaded serial 2009102001
zone alm.uv.cl/IN: loaded serial 2009072901
zone divisionacademica.uv.cl/IN: loaded serial 2009073101
zone melipilla.uv.cl/IN: loaded serial 2009073101
zone auditoria.uv.cl/IN: loaded serial 2009310701
zone cienciasuv.cl/IN: loaded serial 2004090603
zone ici.uv.cl/IN: loaded serial 2009072901
zone mbauv.cl/IN: loaded serial 2009082001
zone cliinffo.uv.cl/IN: loaded serial 2009073101
zone cseconomicas.uv.cl/IN: loaded serial 2009073101
zone decom.uv.cl/IN: loading from master file decom.uv.cl.zone failed: file not found
```

>>Cargando las zonas

dnsI# named-checkzone uvalpo.cl /var/named/etc/namedb/master/uvalpo.cl.zone

```
[root@dnsi /var/named/etc/namedb]# named-checkzone uvalpo.cl /var/named/etc/namedb/master/uvalpo.cl.zone
zone uvalpo.cl/IN: loaded serial 2009070901
OK
[root@dnsi /var/named/etc/namedb]#
```

>>Arrancando named (DNS)

dnsi# /etc/rc.d/named start

Samba

dnsi# cd /usr/ports/net/samba3
dnsi# make
dnsi# make config

Agregar lassiguientes opciones

WINBIND, ACL_SUPPORT, SYSLOG, UTMP, PAM_SMBPASS, EXP_MODULES, POPT

dnsi# make install clean

>> Agregar linear rc.conf

agregar en el **/etc/rc.conf** de la jaula dnsi

nmbd_enable="YES"

smbd_enable="YES"

winbindd_enable="YES"

>>Partiendo Samba

dnsi# /usr/local/etc/rc.d/samba start

Funcionamiento Samba + WINS

Actualmente el servidor Samba se encuentra trabajando como servidorWins El orden en que Samba usa las diferentes técnicas para resolución de nombres es definido por la opción de configuración name resolve order, comomuestra la configuración de DNSI de la UV.

name resolve order = wins lmhosts hosts bcast

Puedes configurar Samba como sever WINS configurando dos opciones globales del fichero de configuración:
En FreeBSd este archive se encuentra en **/usr/local/etc/smb.conf**

[global]
wins support = yes
name resolve order = wins lmhosts hosts bcast

La opción **wins support** convierte a Samba en un servidor **WINS**.

Las opciones **wins support=yes** y **wins server** son **mutuamente excluyentes** (esta modalidad se muestra posteriormente en este documento en la sección "introducción de un caso habitual Samba + Wins"); no puedes al mismo tiempo ofrecer a Samba a como **server WINS** y además apuntar a otro sistema para que actúe como servidor.
Si Samba está actuando como server WINS, deberías familiarizarte con la opción name resolve order mencionada anteriormente. Esta opción le dice a Samba el orden a seguir en cuanto a la utilización de métodos para la resolución de un nombre NetBIOS. Puede tomar hasta cuatro valores:

1.- lmhosts Usa el fichero de control de red LMHOSTS.
2.- hosts Usa los métodos de resolución de nombres standard de un sistema Unix system, /etc/hosts, DNS, NIS, o una combinación (según esté configurado en dicho sistema).
3.- wins Usa el servidor WINS.
4.- bcast Usa un método de multidifusión o broadcast.

El orden en que los especificas es el orden en que Samba intentará la resolución de nombres cuando actúe como servidor WINS

name resolve order = wins lmhosts hosts bcast

Esto significa que Samba intentará usar primero sus entradas WINS par la resolución de nombres, y a continuación el fichero **LMHOSTS** de su sistema. Después, el valor hosts provoca que use los métodos Unix para la resolución de nombres. La palabra hosts puede llegar a engaño; no sólo cubre el fichero /etc/hosts, sino también el uso de DNS o NIS (según esté configurado en el sistema Unix). Finalmente, si ninguno de los tres funcionó, usará broadcast para intentar localizar la máquina correcta.

Por último, puedes instruir al server Samba para que actúe como WINS que chequee co el servidor DNS del sistema si una petición no pudo ser encontrada en su base de datos WINS. Con un típico sistema Linux, por ejemplo, puedes encontrar la dirección IP del servidor DNS buscando el fichero /etc/resolv.conf. En su interior, deberías ver una entrada parecida a esta:

nameserver 127.0.0.1
nameserver 10.50.1.16

Esto nos indica que un servidor DNS se encuentra en 10.50.1.16 (La IP 127.0.0.1 es la dirección de la máquina local, y nunca es una dirección DNS válida).

Usa la opción global dns proxy para indicar a Samba que use el servidor DNS:

[global]

wins support = yes

name resolve order = wins lmhosts hosts bcast dns

dns proxy = yes

Otros archivos a configurar

1.- smbuser

dnsi# vi /usr/local/etc/samba/smbusers

#Unix_name = SMB_name1 SMB_name2 ...

root = administrator admin administrador

nobody = guest pcguest smbguest

2.-resolv.conf

dnsi# vi /etc/resolv.conf

nameserver 127.0.0.1

nameserver 10.50.1.16

3.- make.conf

dnsi# vi /etc/make.conf

added by use.perl 2009-03-19 14:00:30

PERL_VERSION=5.8.9

WITHOUT_CUPS=yes

WITHOUT_ADS=yes

WITH_SYSLOG=yes

WITH_WINBIND=yes

WITH_EXP_MODULES=yes

WITH_PAM_SMBPASS=yes

WITH_ACL_SUPPORT=yes

Información relacionada con el archive smb.conf (información general no de configuración DNSII)

wins support

Samba proporcionará servicio de nombres WINS a todas las máquinas de la red si estableces lo siguiente en la sección [global] del fichero smb.conf:

[global] wins support = yes

El valor por defecto es no, lo cual es usado normalmente para permitir a un servidor Windows NT convertirse en server WINS. Si activas esta opción, recuerda que un servidor WINS Samba actualmente no puede intercambiar datos con ningún servidor de seguridad (o respaldo) WINS NT. Si lo activas, esta opción es mutuamente excluyente con el parámetro wins server; no puedes activar ambas opciones a yes al mismo tiempo, o Samba dará error.

wins server

Samba usará un server WINS existente en la red si especificas esta opción en tu fihero de configuración. El valor para esta opción es la dirección IP o el nombre DNS (no el nombre NetBIOS) del servidor WINS. Por ejemplo:

[global] wins server = 192.168.220.110

[global] wins server = wins.example.com

Para que esto funcione, la opción wins support debe estar a no (por defecto). De lo contrario, Samba reportará un error. Puedes especificar sólo un servidor WINS usando esta opción.

wins proxy

Esta opción permite que Samba actúe como proxy para otro servidor WINS, y que además haga 'relay' o reenvío de las peticiones de registro y resolución de nombres que le lleguen a él hacia el verdadero servidor WINS, normalmente fuera de la actual subred. El server WINS puede ser indicado a través de la opción wins server. El proxy retornará la respuesta WINS al cliente. Puedes activar esta opción especificando lo siguiente en la sección [global]:

[global] wins proxy = yes

dns proxy

Si queires que el Servidor de Nombres de Dominio (DNS) sea usado si un nombre no es encontrado en WINS, puedes establecer la siguiente opción:

[global] dns proxy = yes

Esto provocará que nmbd haga peticiones para nombres de máquinas usando el servicio de nombres de dominio estándar. Puede que desees desactivar esta opción si no tienes una conexión permanente con tu servidor DNS. Recomendamos usar un servidor WINS. Si no tienes ningún server WINS en tu red, convierte a la máquina Samba en server WINS. No conviertas, sin embargo, a dos máquinas Samba en servidores WINS (uno primario y el otro de respaldo) ya que actualmente no pueden intercambiar sus bases de datos WINS.

name resolve order

La opción global name resolve order especifica el orden de los servicios que Samba usará cuando intente resolución de nombres. El orden por defecto es usar el fichero LMHOSTS, seguido de los métodos de resolución Unix estándares (una combinación de /etc/hosts, DNS, y NIS), después interroga a una server WINS, y finalmente usa broadcasting para determinar la dirección de un nombre NetBIOS. Puedes modificar esto especificando el cambio como sigue:

[global] name resolve order = lmhosts wins hosts bcast

Esto causa que la resolución use primero el fichero LMHOSTS, luego interroge a un server WINS, el fichero de máquinas del sistema, y finalmente haga broadcasting. No necesitas usar las cuatro opciones si no quieres. Esta opción se cubre con más detalle en la sección 7.3.3, Configurando Samba como Servidor WINS.

max ttl

Esta opción le da el tiempo máximo de vida (TTL) durante el cual un nombre NetBIOS registrado en el servidor Samba permanecerá activo. No deberías alterar nunca este valor.

max wins ttl

Esta opción da el máximo tiempo de vida (TTL) durante el cual un nombre NetBIOS resuelto por un server WINS permanecerá activo. No deberías alterar nunca este valor.

min wins ttl

Esta opción da el tiempo mínimo de vida (TTL) durante el cual un nombre NetBIOS resuelto por un server WINS permanecerá activo. No deberías alterar nunca este valor.

Introducción de un caso habitual Samba + Wins

Escenario Server Wins en otra red (Noeselcaso UV)

Puedes configurar Samba para usar otro server WINS que se encuentre en la red, simplemente apuntando a la dirección IP de dicho servidor WINS. Esto se hace con la opción de configuración global wins server, como se muestra aquí:

[global] wins server = 10.50.1.5

Con esta opción activada, Samba redirigirá todas las peticiones WINS al servidor que se encuentra en 192.168.200.122. Advierte que debido a que la petición es redirigida a una única máquina

Cabe señalar que este caso **NO** se da con el servidor de DNS interno de laUV deberá encontrar en un archivo habitualmente **lmhosts**, la asociación de maquinas e ip se encuentra en el archivo **lmhosts** u otro que se pueda especificar.

########################## Explicación Coloquial DNSI + SAMBA + WINS DISICO ############

Al tener configurado Samba como servidor Wins, el servidor deberá encontrar en un archivo como lmhosts, la asociación de maquinas e ip en este caso si dicha asociacion no es encontrada en el archivo lmhosts u otro que se pueda especficar entonces el servidor wins chequeara al DNS especificamente en el archivo /etc/resolv.conf en el cual se contrará algo así

nameserver 127.0.0.1

nameserver 10.50.1.16

Esto nos indicaría que el servidor DNS es 10.50.1.16 y no entregará mas información que esta pero como existe en smb.conf, la opción dns proxy = yes, le dira a Samba que use el servidor DNS para encontrar dicha asociacion máquina e ip, y esta asociación se encontrará en las zonas de DNS interno, es decir, en uv.cl

En resumen lo que existe actualmente en DISICO es Samba configurado como servidor WINS

Donde la asociacion de ip y máquinas (esto ocurre para utilizar dominios windows) es respondida por el servidor DNS con sus respectivas zonas.

##

Instalación de Aplicaciones

Para instalar aplicaciones, es necesario tener DNS en la jaula para que se puedan realizar las descargas de las distintas aplicaciones.

Recordar, que cuando se va al directorio **Ports**, este se dirige al directorio **distfile**, si la aplicación no se encuentra ahí, la descargará de Internet.

Instalación de Bash

dnsi#cd /usr/ports/shell/bash
dnsi#make
dnsi#make install

Instalación de UPS

Primero se instala la aplicación para eso hay que ir a la siguiente ruta

cd /usr/ports/sysutils/apcupsd
make

Aquí se marcan

cgi
usb
snmp

Luego:
make install

Configuración de archivo agregando el tipo de cable

En el archivo apcupsd.conf se agregan l,os parámetros para que reconozca el tipo de cable que se va a utilizar en la instalación de la UPS.
Para eso hay que realizar lo siguiente:

cd /usr/local/etc/apcupsd

vi apcupsd.conf

>>Con cable USB

Dentro de este archivo (apcupsd.conf) se agregan las siguientes lineas.

En la línea 19 aparecerá UPSCABLE se deja de la siguiente forma

UPSCABLE usb

En la líea 65 aparecerá UPSTYPE se deja de la siguiente forma

UPSTYPE usb

>>Con cable serial

Dentro de este archivo (apcupsd.conf) se agregan las siguientes lineas.

En la línea 19 aparecerá UPSCABLE se deja de la siguiente forma

UPSCABLE 940-0024C

En la líea 65 aparecerá UPSTYPE se deja de la siguiente forma

UPSTYPE apcsmart

DEVICE /dev/ttyd0

Ejecutando el demonio

Una vez realizado los pasos anteriores solo queda ejecutar el script, este es.

IMPORTANTE: Antes de ejecutar el demonio se debe encontrar agregada la opción

apcupsd_enable="YES" en **/etc/rc.conf**

/usr/local/etc/rc.d/apcupsd start

Importante

Si al instalar la UPS (make) y aparecen las opciones y no es marcada usb y luego se instala la UPS, es recomendable una vez que se quiera instalar la UPS a través de cable usb que se desinstale la UPS, esto se hace de la siguiente forma

cd /usr/ ports/sysinstall/apcupsd

make deinstall

Una vez desinstalada la UPS se realizan nuevamente los pasos, para agregar las opciones de los cables, en este caso el cable usb se encontrara agregado, pero deberá hacerse

cd /usr/local/ports/sysinstall/apcups

make clean

Luego:

make install clean

Una vez instalada la UPS se ejecuta el siguiente comando

apcaccess

Uso de SSH con Certificados / Encriptación asimétrica

Creación del grupo

Para crear un certificado lo primero que se debe tener es un grupo creado y obviamente una cuenta que pertenezca a este grupo

jason# pw groupadd topicos

En este caso el grupo se llamará tópicos

Creación del usuario

jason# adduser –v
username: mferrand

Generación de claves

Para generar la clave (llave) se debe ingresar con el usuario al cual se quiere crear dicha clave, en este caso se quiere crear la clave para el usuario mferrand, se debe ingresar por ssh con el usuario mferrand, una vez que genere todas las claves puedo modificar el sshd_config que aparece señalado en el punto “configuración ssh”

jason# ssh-keygen –t rsa
Generará las llaves públicas y privadas, pedirá contraseña y la confirmación de esta.

Luego se entra al directorio para ver que estén generadas las llaves públicas y privadas
En este caso el usuario es **mferrand**.
Estando dentro de la jaula se accede al directorio del usuario

jason# cd /home/mferrand/.ssh
Desde este directorio se podrán listar las claves publicas y privadas, estas son:

jason# id_rsa

jason# id_rsa.pub

Luego se debe crear el archivo **authorized_keys** con el mismo contenido que id_**rsa.pub**, eso se realiza de la siguiente forma

jason# cat id_rsa.pub >> authorized_keys

Luego se comprueba que ambos archivos tengan el mismo peso.
Una vez verificado lo anterior, y chequear que se tiene los tres archivos en la cuenta **id_rsa, id_rsa.pub, authorized_keys,** para este ejemplo los archivos deberán encontrarse en **/home/mferrand/.ssh** se copian los archivos al equipo desde donde se conectará por ssh, una vez copiado estos archivos solo faltaría un archivo con la extensión **.ppk**.

Software puttygen-x86

Para generar este archivo se utiliza un software llamado puttygen-x86.

Este software en su parte superior tiene un menú con 4 pestañas, File, Key, Conversions y Help, se debe dirigir a Conversions, se escoge la opción Import Key, y se carga el archivo ids_rsa, luego se presiona el botón Save Private Key, ya realizado esto, se revisa en el mismo directorio (PC que se conectara por ssh al servidor) y se encontrará el archivo .ppk que en este ejemplo fue denominada como mferrand.ppk

Configuración SSH

Para este caso en particular donde se realiza el ssh con certificado, fue realizado en una jaula, por lo que se modifica el ssh de la jaula, el archivo a modificar es **/etc/ssh/sshd_config.**
Las líneas que se deben descomentar son las siguientes:

RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_key

La siguiente línea se debe modificar, esta línea aparece como

#UsePAM yes

Se debe descomentar y dejar de la siguiente forma:

UsePAM no

Luego se reinicia el **ssh, /etc/rc.d/sshd restart**, y se entra con el usuario que se creo el certificado, cabe señalar que para cada usuario se deben realizar todos estos pasos señalados

Ingreso de usuarios por ssh y uso de comando "su"

Una vez que ingresen los usuarios por ssh, no podrán pasar a modo root a menos que estos pertenezcan también al grupo Wheel.

Por defecto, FreeBSD sólo permite acceso root a usuarios incluidos en el grupo *wheel*, un grupo reservado para tareas de administración al que inicialmente sólo pertenece el propio root. Por tanto, si queremos que nuestro usuario "mferrand" pueda tener permisos de superusuario, una buena manera es "loguearnos" como root y agregar "mferrand" al grupo *wheel*.

En primer lugar comprobamos si ya está incluido:

jason# pw showgroup wheel
wheel:*:root

No, no está. Para añadirlo:

jason# pw user mod mferrand -G wheel

Comprobamos de nuevo si "mferrand" está en el grupo wheel:

jason# pw showgroup wheel
wheel:*:root,mferrand

Ahora sí; ya podemos usar nuestra cuenta "mferrand" y con un simple *su* (+ contraseña) obtener privilegios de root cuando los necesitemos. Al finalizar las operaciones debemos abandonar la cuenta root tecleando exit (o Ctrl-D).

Respaldo de Servidores

Respaldo de información antiguo DNS interno FOBOS a nuevo DNS interno JASON

Maquina: FOBOS	
DNS Interno	
ip: 10.50.1.16	
Directorio: var/name	
#	**Nombre de archivo a respaldar**
1	10.100.10.in-addr.arpa.zone
2	1.100.10.in-addr.arpa.zone
3	11.100.10.in-addr.arpa.zone
4	12.100.10.in-addr.arpa.zone
5	127.0.0.in-addr.arpa.zone
6	13.100.10.in-addr.arpa.zone
7	14.100.10.in-addr.arpa.zone
8	1.50.10.in-addr.arpa.zone
9	15.100.10.in-addr.arpa.zone
10	1.60.10.in-addr.arpa.zone
11	16.100.10.in-addr.arpa.zone
12	17.100.10.in-addr.arpa.zone
13	18.100.10.in-addr.arpa.zone
14	19.100.10.in-addr.arpa.zone
15	200.100.10.in-addr.arpa.zone
16	20.100.10.in-addr.arpa.zone
17	2.100.10.in-addr.arpa.zone
18	26.100.10.in-addr.arpa.zone
19	27.100.10.in-addr.arpa.zone
20	28.100.10.in-addr.arpa.zone
21	3.100.10.in-addr.arpa.zone
22	32.100.10.in-addr.arpa.zone

23	4.100.10.in-addr.arpa.zone
24	41.100.10.in-addr.arpa.zone
25	42.100.10.in-addr.arpa.zone
26	43.100.10.in-addr.arpa.zone
27	44.100.10.in-addr.arpa.zone
28	45.100.10.in-addr.arpa.zone
29	46.100.10.in-addr.arpa.zone
30	50.100.10.in-addr.arpa.zone
31	5.100.10.in-addr.arpa.zone
32	6.100.10.in-addr.arpa.zone
33	70.100.10.in-addr.arpa.zone
34	7.100.10.in-addr.arpa.zone
35	72.100.10.in-addr.arpa.zone
36	8.100.10.in-addr.arpa.zone
37	90.100.10.in-addr.arpa.zone
38	9.100.10.in-addr.arpa.zone
39	arquitecturauv.cl.zone
40	artenlau.cl.zone
41	bibliotecasuv.cl.zone
42	biolmar.cl.zone
43	cienciasdelmar.cl.zone
44	cienciasuv.cl.zone
45	cimfav.cl.zone
46	cnv.cl.zone
47	congresodeodontologia.cl.zone
48	decom.cl.zone
49	disico.uv.cl.zone
50	eltrauco.cl.zone
51	enefa2003.cl.zone
52	escuelaodontologiauv.cl.zone
53	facultadodontologiauv.cl.zone
54	ingenieriaoceanica.cl.zone
55	localhost.zone
56	named.ca
57	named.local
58	named.root
59	neurocirugia.cl.zone
60	portalpsicologia.cl.zone
61	portalpsicologia.com.zone
62	portalpsicologia.org.zone

63	slave
64	uvalparaiso.cl.zone
65	uvalpo.cl.zone
66	uv.cl.zone

Respaldo de información
antiguo DNS externo XEON a nuevo DNS externo JASON

Maquina: XEON	
DNS Externo	
ip: 10.50.1.15	
Directorio: /var/named/chroot/var/named	
#	**Nombre de archivo a respaldar**
1	103.27.200.in-addr.arpa.zone
2	127.0.0.in-addr.arpa.zone
3	184.54.200.in-addr.arpa.zone
4	2.27.200.in-addr.arpa.zone
5	68.14.200.in-addr.arpa.zone
6	69.14.200.in-addr.arpa.zone
7	70.14.200.in-addr.arpa.zone
8	71.14.200.in-addr.arpa.zone
9	arquitecturauv.cl.zone
10	artenlau.cl.zone
11	atenlau.cl.zone
12	bibliotecasuv.cl.zone
13	biolmar.cl
14	cienciasdelmar.cl.zone
15	cienciasuv.cl.zone
16	cimfav.cl.zone
17	cnv.cl.zone
18	congresodeodontologia.cl.zone
19	data
20	decom.cl.zone
21	disico.uv.cl.zone
22	eea.cl.zone
23	emprendimientouv.cl.zone
24	escuelaodontologiauv.cl.zone
25	facultadodontologiauv.cl.zone
26	ingenieriaoceanica.cl.zone

27	ingenieriaoceanica.cl.zone.ant
28	localdomain.zone
29	localhost.zone
30	named.broadcast
31	named.ca
32	named.ip6.local
33	named.local
34	named.root
35	named.zero
36	oceanica.cl.zone
37	portalpsicologia.cl.zone
38	portalpsicologia.com.zone
39	portalpsicologia.org.zone
40	**slaves (dir)**
41	**tablas (dir)**
42	**tablas.tar.gz**
43	uvalparaiso.cl.zone
44	uvalpo.cl.zone
45	uvalpovirtual.cl.zone.back
46	uv.cl.zone
Directorio: /var/named/chroot/var/named/tablas	
#	**Nombre de archivo a respaldar**
1	103.27.200.in-addr.arpa.zone
2	127.0.0.in-addr.arpa.zone
3	184.54.200.in-addr.arpa.zone
4	2.27.200.in-addr.arpa.zone
5	68.14.200.in-addr.arpa.zone
6	69.14.200.in-addr.arpa.zone
7	70.14.200.in-addr.arpa.zone
8	71.14.200.in-addr.arpa.zone
9	artenlau.cl.zone
10	atenlau.cl.zone
11	bibliotecasuv.cl.zone
12	cienciasuv.cl.zone
13	cimfav.cl.zone
14	cnv.cl.zone
15	congresodeodontologia.cl.zone
16	decom.cl.zone
17	eea.cl.zone
18	emprendimientouv.cl.zone

19	localdomain.zone
20	localhost.zone
21	named.broadcast
22	named.ca
23	named.ip6.local
24	named.local
25	named.root
26	named.zero
27	portalpsicologia.cl.zone
28	portalpsicologia.com.zone
29	portalpsicologia.org.zone
30	uvalparaiso.cl.zone
31	uvalpo.cl.zone
32	uvalpovirtual.cl.zone.back
33	uv.cl.zone