Administración de Infraestructuras

Tecnólogo en Informática

LINUX – CENTOS 6 DNS Software bind



Año 2012

DNS

- Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usado por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.
- Esta organizado en un órden jerarquico.



DNS

- En una organización que tenga uno o mas servidores web, o servidor de correo, debe tener funcionando un servidor DNS.
- Con un servidor DNS correctamente funcionando el resto del mundo podrá acceder a los servicios ofrecidos por la organización.

INSTALACIÓN

SERVIDOR DNS EN CENTOS 6 BIND9

Paquetes de bind

[root@www ~]# yum -y install bind-chroot bind-libs bind bind-utils_

[root@web ~]# <u>rpm -qa |grep ^bind-</u> bind-chroot-9.7.3-2.el6.i686 bind-libs-9.7.3-2.el6.i686 bind-9.7.3-2.el6.i686 [root@web ~]# _

Archivos

[root@web_sample]#_pwd /usr/share/doc/bind-9.7.3/sample root@web sample]# ll total 8 lrwxr-xr-x. 2 root root 4096 abr 21 08:19 <mark>etc</mark> lrwxr-xr-x. 3 root root 4096 abr 21 08:19 <mark>var</mark> [root@web_sample]#

Copiar los archivos

```
[root@web sample]# ls etc/
named.conf named.rfc1912.zones
[root@web sample]# cp etc/* /var/named/chroot/etc/
[root@web_sample]#_ls_var/named/
                   my.internal.zone.db named.empty named.loopback
my.external.zone.db named.ca named.localhost slaves
[root@web sample]# cp -r var/named/* /var/named/chroot/var/named/
[root@web_sample]#
```

Directorio de configuración



Directorio de configuración /var/named/chroot/etc

[root@web sample]# cd /var/named/chroot/etc/ [root@web_etc]#]] total 24 -rw-r--r--. 1 root root 3519 abr 21 08:22 localtime drwxr-x---. 2 root named 4096 jul 19 2011 named -rw-r--r--. 1 root root 7687 abr 21 08:46 named.conf -rw-r--r--. 1 root root 931 abr 21 08:46 named.rfc1912.zones drwxr-xr-x. 3 root root 4096 abr 21 08:22 pki [rootQweb_etc]#

Creación de las zonas

- En el archivo named.conf se configuran el comportamiento general del DNS. Este incluye el archivo named.rfc1912.zones, en el cual se definen las zonas de autoridad.
- Se define la zona de autoridad con el nombre, el tipo y el pais: solange.edu.uy
- Luego la zona inversa, donde se define la dirección IP.

- **zone** "solange.edu.uy" nombre de la zona.
- type "master" tipo, puede ser master o slave.
- file "named.solange" archivo donde estarán los datos de los hosts.
- **allow-update** si se actualiza o no, en el caso de un master nunca se actualiza.

- zone "2.0.10.in-addr.arpa"
- Esta configuración se realiza descartando el último valor de la dirección IP, y dando vuelta el valor.
- Dirección IP: 10.0.2.15



zone "solange.edu.uy" IN {
 type master;
 file "named.solange";
 allow-update { none; };
...

zone "2.0.10.in-addr.arp<u>a</u>" IN { type master; file "named.solange.rev"; allow-update { none; };

Archivo named.conf

Modificaciones a realizar:

- En la configuración predeterminada solo está habilitada la consulta local.
- Incluir en las consultas externas la configuración de la zona.
- Generar e incluir la clave.
- Comentar las zonas no utilizadas.

named.conf Habilitar las consultas

//listen-on port 53 _listen-on port 53

53 { any; }; { 127.0.0.1; };



named.conf Habilitar las consultas

//allow-query <u>a</u>llow-query

{ localhost; }; { localhost; any; }; allow-query-cache { localhost; any; };

named.conf Incluir zona externa



Generar la clave

[root@web_etc]#_dnssec-keygen -a hmac-md5 -b 128 -n HOST host1

[root@web_etc]#_ls Khost1.+157+63863.key localtime_named.conf <mark>pki</mark> Khost1.+157+63863.private_named named.rfc1912.zones

```
[root@web_etc]#_cat_Khost1.+157+63863.private
Private-key-format: v1.3
Algorithm: 157 (HMAC_MD5)
Key: l6mQeY9EDkWkk00akx4JZA==
Bits: AAA=
Created: 20120421123252
Publish: 20120421123252
Activate: 20120421123252
[root@web_etc]#
```



key ddns_key { algorithm hmac-md5; secret "16mQeY9EDkWkk00akx4JZA=="; };

named.conf Comentar las zonas

//	zone "my.internal.zone" {
11	type master:
11	file "my.internal.zone.db";
11	<pre>};</pre>
11	zone "my.slave.internal.zone" {
11	type slave;
11	file "slaves/my.slave.internal.zone.db";
11	masters { /* put master nameserver IPs here */ 127.0.0.1; } ;
11	// put slave zones in the slaves/ directory so named can update
them	
11	};
11	zone "my.ddns.internal.zone" {
11	type master;
11	allow-update { key ddns_key; };
11	file "dynamic/my.ddns.internal.zone.db";
	// put dynamically updateable zones in the slaves/ directory so
named	can update them
11	<pre>};</pre>
_	

11	zone "my.external.zone" {	
11	type master;	
11	file "my.external.zone.db";	
11	<pre>};</pre>	

Archivos de zona

- Se deben crear los dos archivos de zona definidos en el archivo named.rfc1912.zones
- Directorio: /var/named/chroot/var/named

Archivo de zona

/var/named/chroot/etc/named.rfc1912.zones



.rootWweb named]# pwd						
/var/named/chroot/var/named						
[root@web named]# ls						
lata	named.ca	named.loopback				
ny.external.zone.db	named.empty	named.solange				
my.internal.zone.db	named.localhost	named.solange.rev				
[rootQweb named]# _						

Tipos de registros

	Тіро	Nombre	Función
Zona	SOA	Start Of Authority	Define una zona representativa del DNS
	NS	Name Server	Identifica los servidores de zona.
Básicos	А	Dirección IPv4	Traducción de nombre a dirección
	PTR	Puntero	Traducción de dirección a nombre
	MX	Mail eXchanger	Controla el enrutado del correo
Opcional	LOC	Localización	Localización geográfica y extensión
	RP	Persona responsable	Especifica la persona de contacto de cada host
	SRV	Servicios	Proporciona la localización de servicios conocidos
	ТХТ	Texto	Comentarios o información sin cifrar

named.solange archivo de zona

STTL 1D						
0	IN SOA	solange	.edu.uy. root.l	local (
				0	1	serial
				1D	;	refresh
				1H	3	retry
				1₩	1	expire
				3H)	1	minimum
	NS	ns1.sol	ange.edu.uy.			
web		A	10.0.2.15			
ns1		A	10.0.2.15			

named.solange.rev archivo de zona

and the second second				
) 117 Th	IN SOA	2.0.10.in-addr.arpa. root.loca	1 (
		0	;	serial
		1D	1	refresh
		1H	- ;	retry
		1₩	- ;	expire
		3H)	1	minimum
		NS ns1.solange.edu.uy.		
<u>1</u> 5	PTR	ns1.solange.edu.uy.		

Propietario

- El servicio named se ejecuta con el usuario del sistema named.
- Se debe modificar los archivos para que le pertenezcan a este usuario y su grupo.

/var/named/chroot

```
[root@web chroot]# pwd
/var/named/chroot
[root@web_chroot]# ]]
total 16
drwxr-x---. 2 root named 4096 abr 21 08:22 <mark>de</mark>v
drwxr-x---. 4 root named 4096 abr 21 09:06 <mark>etc</mark>
drwxr-xr-x. 3 root root  4096 abr 21 08:22 <mark>usr</mark>
drwxr-x---. 6 root named 4096 abr 21 08:22 <mark>var</mark>
[root@web_chroot]#_chown -R_named.named_etc/__var/
[root@web_chroot]#
```

Pasos finales

- Crear el archivo /var/named/chroot/etc/rndc.key con la misma clave de named.conf. Este archivo habilita la utilización del front-end **rndc**.
- Crear los enlaces simbólicos.
- Chequear la configuración.
- Iniciar el servicio.
- Configurar los clientes.

Crear el archivo rndc.key

```
[root@web etc]# pwd
/var/named/chroot/etc
[root@web etc]# cat rndc.key
key "dnsadmin" {
        algorithm hmac-md5;
        secret "l6mQeY9EDkWkk00akx4JZA==";
};
[root@web etc]# _
```

Enlaces simbólicos

ln -s /var/named/chroot/etc/named.conf
ln -s /var/named/chroot/etc/named.rfc1912.zones
ln -s /var/named/chroot/etc/rndc.key

/etc/named.conf /etc/named.rfc1912.zones /etc/<mark>rndc</mark>.key

Chequear la configuración

```
[root@web named]# cd /var/named/chroot/var/named/
[root@web named]# pwd
/var/named/chroot/var/named
[root@web named]# ls
                  named.ca named.loopback slaves
my.external.zone.db named.empty named.solange
[root@web named]# named-checkzone solange.edu.uy named.solange
zone solange.edu.uy∕IN: loaded serial U
OK
[root@web named]# named-checkzone 2.0.10.in-addr.arpa named.solange.rev
zone 2.0.10.in-addr.arpa/IN: loaded serial 0
OK
[root@web named]# named-checkconf
[root@web_named]# __
```

Levantar el servicio

[root@web named]# service named start Iniciando named: [root@web named]# rndc status version: 9.7.3-RedHat-9.7.3-2.elb CPUs found: 1 worker threads: 1 number of zones: 50 debug level: Ø xfers running: 0 xfers deferred: 0 soa queries in progress: 0 query logging is OFF recursive clients: 0/0/1000 tcp clients: 0/100 server is up and running [root@web named]# chkconfig named on [root@web named]#

NK

Configurar los clientes

[root@web etc]# cat /etc/resolv.conf nameserver 10.0.2.15 [root@web etc]# _

Consultas al DNS

[root@web etc]# host -a solange.edu.uy Trying "solange.edu.uy" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56075 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1 ;; QUESTION SECTION: ANY :solange.edu.uy. TN :: ANSWER SECTION: solange.edu.uy. 86400 TN SOA solange.edu.uy. root.local.solan ge.edu.uy. 0 86400 3600 604800 10800 solange.edu.uy. 86400 ΤN NS ns1.solange.edu.uy. :: ADDITIONAL SECTION: IN A 10.0.2.15 ns1.solange.edu.uy. 86400 Received 113 bytes from 10.0.2.15#53 in 8 ms [root@web_etc]#_host_ns1.solange.edu.uy ns1.solange.edu.uy has address 10.0.2.15 [root@web etc]# host 10.0.2.15 15.2.0.10.in-addr.arpa domain name pointer ns1.solange.edu.uy. [root@web_etc]# _

Agregar el servidor de correo

- El servidor de correo se especifica con el registro MX.
- Una vez funcionando el DNS, se pueden agregar nuevos hosts modificando los archivos de zona.
- Luego con el comando **rndc reload** se actualiza el servidor sin tener que reiniciarlo.

Archivos de zona

STTL 1D						
2	IN SOA	solang	e.edu.u	y. root.	local (
					0	; serial
					1D	: refresh
					1H	; retry
					1W	; expire
					3H)	; minimum
	NS	ms1.so	lange.ed	du . uy . 👘		
лер		A	10.0.3	2.15		
ns1		A	10.0.3	2.15		
มเมเม		A	10.0.3	2.16		
2			MX	10	correo	
correo		A 10.0	.2.17			

\$TTL	1 D			
		IN SOA	2.0.10.in-addr.arpa. root.local (
			🛛 🕺 🕴 🕄 serial	
			1D ; refresh	
			1H ; retry	
			1W ; expire	
			3H) ; minimum	
			NS ns1.solange.edu.uy.	
15		PTR	ns1.solange.edu.uy.	
<u>1</u> 6		PTR	www.solange.edu.uy.	
17		PTR	correo.solange.edu.uy. 🚽 🚽	

rndc reload

[root@web named]# rndc reload server reload successful [root@web named]# host -a solange.edu.uy Trying "solange.edu.uy ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58880 ;; flags: gr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2 ;; QUESTION SECTION: ;solange.edu.uy. IN ANY :: ANSWER SECTION: solange.edu.uy. 86400 MX 10 correo.solange.edu.uy. ΙN solange.edu.uy. root.local.solan solange.edu.uy. 86400 IN SOA ge.edu.uy. 0 86400 3600 604800 10800 solange.edu.uy. 86400 IN NS ns1.solange.edu.uy. :: ADDITIONAL SECTION: IN correo.solange.edu.uy. 86400 Ĥ 10.0.2.17 ns1.solange.edu.uy. 86400 IN Ĥ 10.0.2.15 Received 152 bytes from 10.0.2.15#53 in 11 ms [root@web_named]#_host -t_MX_solange.edu.uu solange.edu.uy mail is handled by 10 correo.solange.edu.uy. [root@web named]#

DNS SECUNDARIO

DNS SECUNDARIO (SLAVE)

- Un servidor DNS puede tener muchas consultas o fallar.
- Por este motivo es conveniente tener un servidor secundario con la misma información del master.
- De esta forma se reparte la carga de las consultas, cuando el master no responde los clientes consultan al slave.

Configuración

- El Slave obtendrá los registros de zona del Master. Si luego modifica el Master solo debe actualizar el Slave para que esten sincronizados.
- Se debe modificar el Master para que envie los datos al Slave.
- Al Slave se debe configurar para que pida los registros del Master.

Configuración

- El Slave tendrá los mismos archivos del directorio: /var/named/chroot/etc
- Se pueden copiar los archivos de forma segura utilizando: **scp origen destino**
- Solo se modificará el archivo: named.rfc1912.zones una vez copiado.

Copiar los archivos

- Para copiar los archivos necesitamos el servicio sshd levantado en los dos hosts.
- service sshd start

[root@web_etc]#_scp_named.*_rndc.key_10.0.2.27:/var/named/chroot/etc/

zone	"solange.edu.uy" IN {
	type slave;
	file "named.solange";
	<u>m</u> asters {10.0.2.15; };
};	
zone	"2.0.10.in-addr.arpa" IN {
	type slave;
	file "named.solange.rev";
	<pre>masters { 10.0.2.15; };</pre>
};	

Configuración Slave

- Hay que recordar los pasos realizados en la configuración del master.
- Links simbólicos
- Propietario.

Master named.rfc1912.zones

• Habilitar la transferencia al Slave



Paso final

- Reinciar el Master
- Iniciar el Slave
- Si todo funciono bien en el directorio /var/named/chroot/var/named deben aparecer los archivos de zona.
- Comprobar la configuración con un cliente incluyendo en el archivo /etc/resolv.conf la dirección del Slave.

