

UNIVERSIDAD CENTRAL DEL ECUADOR
FACULTAD DE INGENIERIA CIENCIAS FISICAS Y MATEMATICA
PROTOCOLOS DE COMUNICACIÓN

2DO HEMISEMESTRE

NOMBRE: Sánchez Rosero Mónica

Domain Name System DNS

«Sistema de Nombres de Dominio» es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. Durante la resolución DNS, los mensajes DNS se envían desde clientes DNS a los servidores DNS o entre servidores DNS. Los mensajes se envían a través de UDP y servidores DNS bind al puerto UDP 53. Cuando la longitud del mensaje supera el tamaño de mensaje predeterminado para un datagrama de protocolo de datagramas de usuario (UDP) (512 octetos)

Instalacion y configuración el protocolo

#yum instal bind bind-utils

Renombrar el hostname de nuestra maquina

#hostnamectl set-hostname dns1.gaar.net

#hostnamectl set-hostname dns2.zmani.net

Habilitamos el Puerto 53 en tcp y udp

#Firewall -cmd - --permanent - --add-port=53/tcp

#Firewall -cmd - --permanent - --add-port=53/udp luego

#fierawall -cmd --reload

Luego nos vamos a /etc/sysconfig/networkscript/ifcfg-enp0s3 y configuramos los siguiente agregando nuestras direcciones IP en los respectivos servidores.

```
root@dns1:/etc/sysconfig/network-scripts
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=914bd49e-8b4b-4f25-b328-3aeced57cf36
ONBOOT=no
HWADDR=08:00:27:AC:5F:19
PEERDNS=yes
PEERROUTES=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPADDR=10.3.0.50
PREFIX=16
GATEWAY=10.3.0.1
DNS=10.3.0.50
-
-
"ifcfg-enp0s3" 20L, 348C 20,1 Todo
```

Configurar el archivo /etc/named.conf agragar los subrayado en cada uno delos servidores como se indica

SERVIDOR dns2

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { 127.0.0.1; 10.3.0.30 };
    // listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { localhost; 10.3.0.0/16 };

    /*
     * If you are building an AUTHORITY DNS server, do NOT enable recurs
ion.
     * If you are building a RECURSIVE (caching) DNS server, you need to ena
ble
-- INSERTAR --
12,3 Comienzo
```

SERVIDOR dns1

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { 127.0.0.1; 10.3.0.50; };
    // listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { localhost; 10.3.0.0/16; };

    /*
     * If you are building an AUTHORITY DNS server, do NOT enable recurs
ion.
     * If you are building a RECURSIVE (caching) DNS server, you need to ena
ble
1,1 Comienzo
```

```
root@localhost:/etc

Archivo  Editar  Ver  Buscar  Terminal  Ayuda

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "zmon1.net" IN {
type master;
file "zona.di";
};

zone "0.3.10.in-addr.arpa" IN {
type master;
file "zona.in";
allow-update {none};
};
-- INSERTAR --
```

```
root@dns1:/etc/sysconfig/network-scripts

Archivo  Editor  Ver  Buscar  Terminal  Ayuda

    file "data/named.run";
    severity dynamic;
};

zone "." IN {
    type hint;
    file "named.ca";
};
zone "gaar.net" IN {
    type master;
    file "zona.di";
    allow-update {none;};
};
zone "0.3.10.in-addr.arpa" IN {
    type master;
    file "zona.in";
    allow-update {none;};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Crear los archivos nombrados zona.in y zona.di en el directorio /var/named/
#vim zona.id y agragamos las siguientes líneas

```
Archivo Editar Ver Buscar Terminal Ayuda
```

SERVIDOR dns2

```
$TTL 86400
$ORIGIN gaar.net.
@           IN SOA      dns1.gaar.net. root.gaar.net. (
                                2015010900          ; serial
                                1D                   ; refresh
                                1H                   ; retry
                                1W                   ; expire
                                3H                   ; minimum
)
;servidor 1 principal
@           IN NS       dns1.gaar.net.
;servidor 2
@           IN NS       dns2.zmani.net.
;servidor de correo
@           IN MX       10    mail.gaar.net.
;servidor www
www.gaar.net. IN A       10.3.0.50
;direcciones ip
dns1.gaar.net. IN A       10.3.0.50
dns2.zmani.net. IN A       10.3.0.30
mail.gaar.net.  IN A       10.3.0.50
cliente.gaar.net. IN A     10.3.0.55
cliente2.zmani.net. IN A   10.3.0.35
;
; A 127.0.0.1
; AAAA ::1
```

```

Archivo Editor Ver Búscar
SERVIDOR dns1

$TTL 86400
@ IN SOA dns2.zmon1.net. root.zmon1.net. (
                                2015010900 ; serial
                                1D          ; refresh
                                1H          ; retry
                                1W          ; expire
                                3H )        ; minimum

@ IN NS dns2.zmon1.net.
@ IN MX 10 mail.zmon1.net.
www IN A 10.3.0.30
dns2 IN A 10.3.0.30
mail IN A 10.3.0.30
cliente IN A 10.3.0.35
; A 127.0.0.1
; AAAA ::1

~
~
~
~
~
~
-- INSERTAR --

```

#vim zona.in y agragamos las siguientes líneas

SERVIDOR dns2SFRVIDOR dns1

```

root@localhost:/var/named
Archivo Editar Ver Buscar Terminal Ayuda
$TTL 86400
@ IN SOA dns2.zmoni.net. root.zmoni.net. (
    2015011000 ; serial
    10 ; refresh
    1H ; retry
    1W ; expire
    3H ) ; minimum

@ IN NS dns2.zmoni.net.
@ IN PTR zmoni.net.
@ IN MX 10 mail.zmoni.net.
dns2 IN A 10.3.0.30
cliente IN A 10.3.0.35
30 IN PTR dns2.zmoni.net.
30 IN PTR www.zmoni.net.
35 IN PTR cliente.zmoni.net.

; A 127.0.0.1
; AAAA ::1

"zona.in" 18L, 374C
18,1 Todo

```

```

root@dns1:/etc/sysconfig/network-scripts
Archivo Editar Ver Buscar Terminal Ayuda
$TTL 86400
$ORIGIN 3.10.IN-ADDR.ARPA.
@ IN SOA dns1.gaar.net. root.gaar.net. (
    2015011001 ; serial
    10 ; refresh
    1H ; retry
    1W ; expire
    3H ; minimum

;servidor dns principal
@ IN NS dns1.gaar.net.
@ IN NS dns2.zmani.net.
@ IN PTR gaar.net.
@ IN PTR zmani.net.

;servidor de correo
@ IN MX 10 mail.gaar.net.
dns1.gaar.net IN A 10.3.0.50
dns2.zmani.net IN A 10.3.0.30
cliente.gaar.net IN A 10.3.0.55
50 IN PTR dns1.gaar.net.
50 IN PTR www.gaar.net.
55 IN PTR cliente.gaar.net.
30 IN PTR dns2.zmani.net.
35 IN PTR cliente2.zmani.net.
; A 127.0.0.1
; AAAA ::1

"/var/named/zona.in" 26L, 584C
9,1 Todo

```

Luego configuramos los archivos resolv.conf en el directorio /etc de los servidores

```

SRVIDOR dns1
Archivo Editar Ver Buscar Terminal Ayuda
Generated by NetworkManager
search gaar.net
nameserver 10.3.0.50
nameserver 10.3.0.30

```

Luego actualizar los archivos

#Restorecon -rv /etc/named.conf

#Restorecon -rv /var/named/zona.di

#Restorecon -rv /var/named/zona.in

Reiniciar el servicio named

#Systemctl restart named

#Systemctl status named

#Systemctl restart network

Realizamos las pruebas de funcionamiento

```

[root@dns2 ~]# lookup dns2.zmani.net
bash: lookup: comando no encontrado...
[root@dns2 ~]# nslookup dns2.zmani.net
Server:      10.3.0.30
Address:     10.3.0.30#53

```

```

Name:  dns2.zmani.net
Address: 10.3.0.30

```

```

[root@dns2 ~]# nslookup dns1.gaar.net
Server:      10.3.0.50
Address:     10.3.0.50#53

```

```

Name:  dns1.gaar.net
Address: 10.3.0.50

```

```

[root@dns2 ~]# █

```

```

root@dns2:/var/named
Archivo Editar Ver Buscar Terminal Ayuda
[root@dns2 named]# ping 10.3.0.50
PING 10.3.0.50 (10.3.0.50) 56(84) bytes of data.
^C
--- 10.3.0.50 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3002ms

[root@dns2 named]# nslookup
bash: nslookup: comando no encontrado...
[root@dns2 named]# nslookup
> 10.3.0.30
Server:      10.3.0.30
Address:     10.3.0.30#53

30.0.3.10.in-addr.arpa name = dns2.zmani.net.
30.0.3.10.in-addr.arpa name = www.zmani.net.
> 10.3.0.50
Server:      10.3.0.30
Address:     10.3.0.30#53

50.0.3.10.in-addr.arpa name = www.gaar.net.
50.0.3.10.in-addr.arpa name = dns1.gaar.net.
> exit

```

Hypertext Transfer Protocol o HTTP

Protocolo de transferencia de hipertexto es el protocolousado en cada transacción de la World Wide Web. Usa puerto 80 en TCP.

Instalación y configuración del protocolo

Primero instalamos los paquetes de http con el comando

yum -y install httpd

Eliminamos el siguiente archivo

#rm -f /etc/httpd/conf/welcome.conf

configuramos el archivo httpd.conf:

#vi /etc/httpd/conf/httpd.conf

```
# line 86: change to admin's email address
ServerAdmin
root@server.world
# line 95: change to your server's name
ServerName
www.server.world:80
# line 151: change
AllowOverride
All
# line 164: add file name that it can access only with directory's
name
DirectoryIndex index.html
index.cgi index.php
# add follows to the end
# server's response header
ServerTokens Prod
# keepalive is ON
KeepAlive On
```

Luego reiniciamos los servicios

#systemctl start httpd

#systemctl enable httpd

luego creamos una pagina html para realizar las pruebas en /var/www/html/

#vim index.html y ponemos:

```
<html>
<body>
<div style="width: 100%; font-size: 40px; font-weight:
bold; text-align: center;">
Test Page
</div>
</body>
</html>
```

Luego vamos al navegador y digitamos
www.zmani.net/index.html



SEGURIDAD CON .htaccess y .htpasswd

En el directorio /var/www/html

Creamos un nuevo directorio

#Mkdir protección

Dentro de este creamos los archivos

.htaccess y .htpasswd

#touch .htaccess

#touch .htpasswd

Luego editamos el primero .htaccess con lo siguiente

```
root@dns2:/var/www/html/proteccion

Archivo  Editar  Ver  Buscar  Terminal  Ayuda

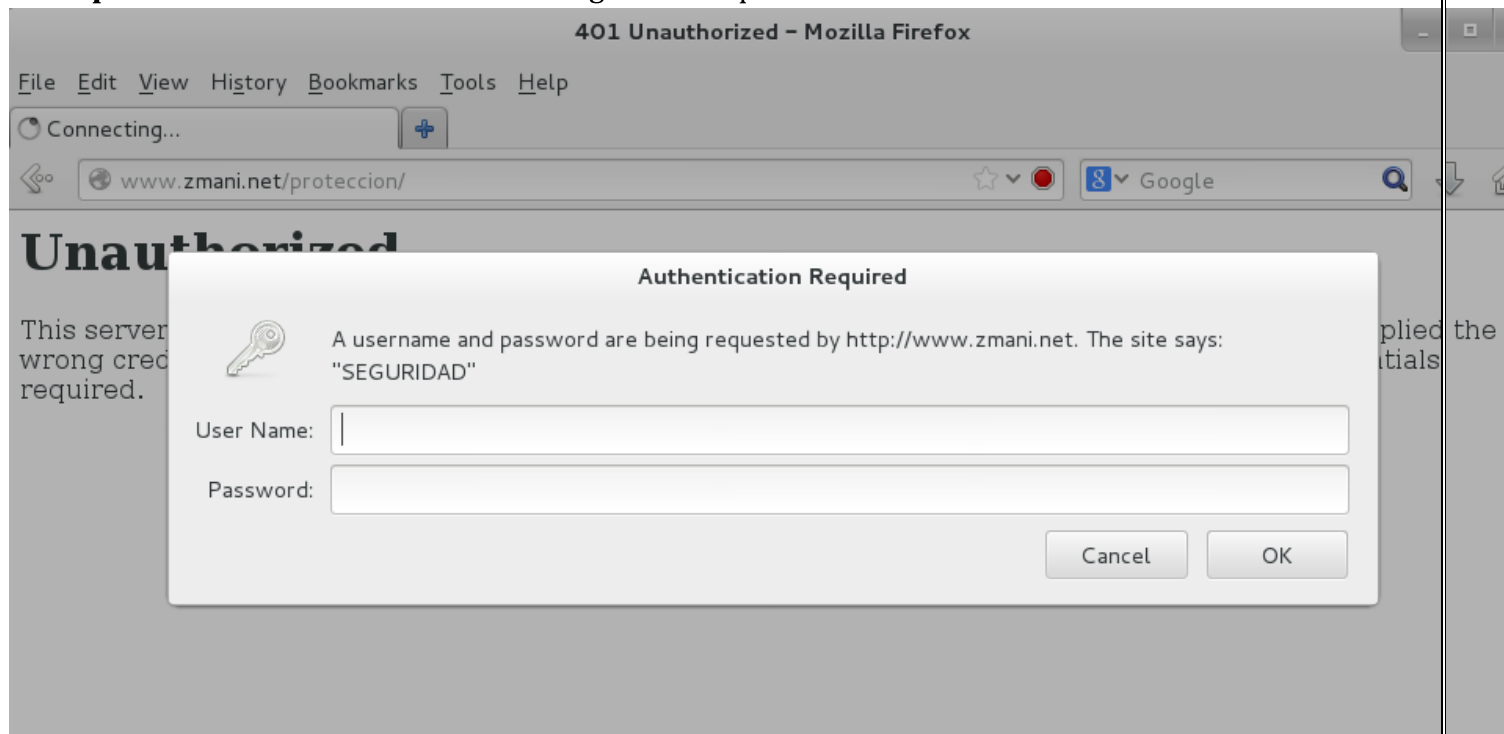
AuthName "SEGURIDAD"
AuthType Basic
AuthUserFile /var/www/html/proteccion/.htpasswd
require valid-user
~
~
```

Y para el archivo .htpasswd ingresamos los usuarios y contraseña de la siguiente manera
#htpasswd -c .htpasswd cliente y nos pide contraseña.

```
[root@dns2 proteccion]# htpasswd -c .htpasswd cliente
New password:
Re-type new password:
Adding password for user cliente
[root@dns2 proteccion]# cat .htpasswd
cliente:$apr1$ov406pzQ$YeytsLVaF0l2v5JMY4LEM0
[root@dns2 proteccion]#
```

Creamos un archivo .html

#vim protección.html escribimos en código html la prueba



HTTPS Hypertext Transfer Protocol Secure

Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas **HTTPS**, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP. Usa el puerto 443 /TCP

Instalación y configuración del protocolo

Instalamos los paquetes necesarios

#yum install mod_ssl openssl

Generar un certificado autofirmado

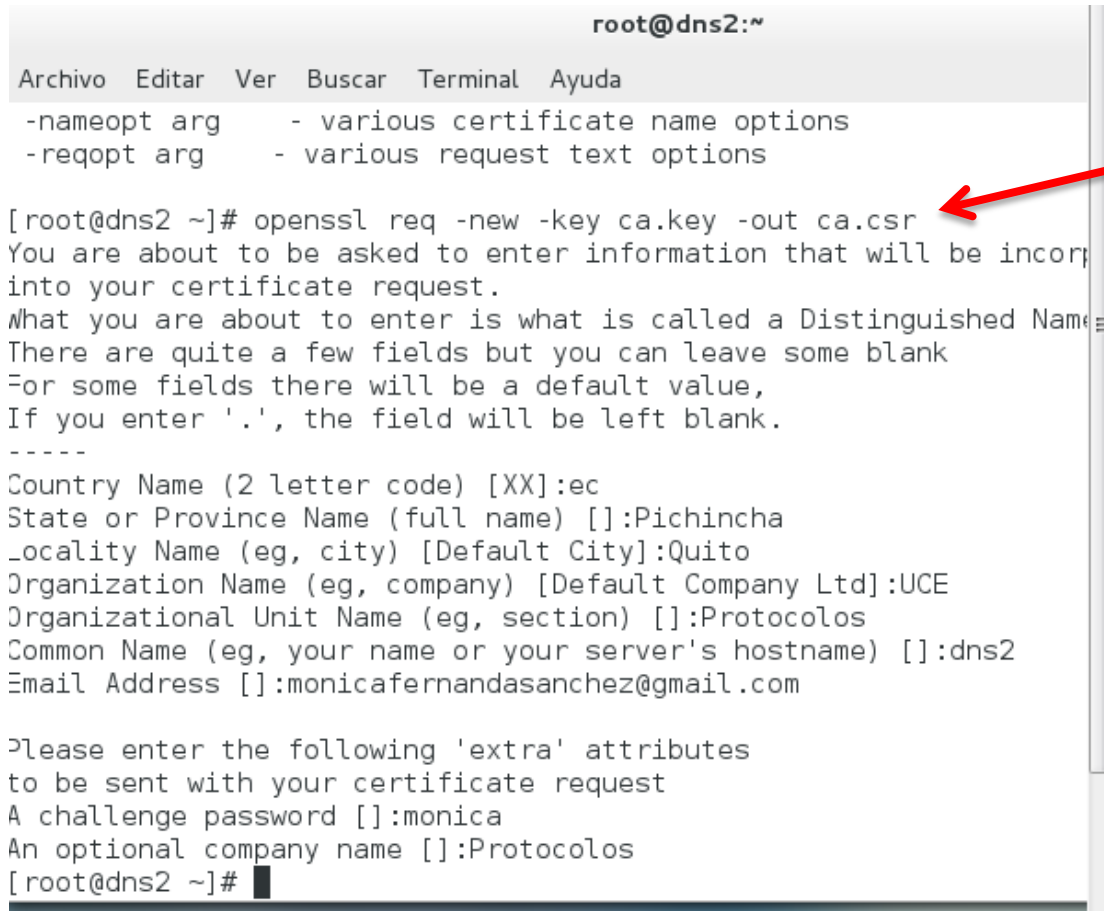
En primer lugar, generar una clave privada con cifrado de 2048 bits.

Si no ponemos 2048 se genera uno con 1024bits

openssl genrsa -out ca.key 2048

Luego genere solicitud de firma de certificado (CSR).

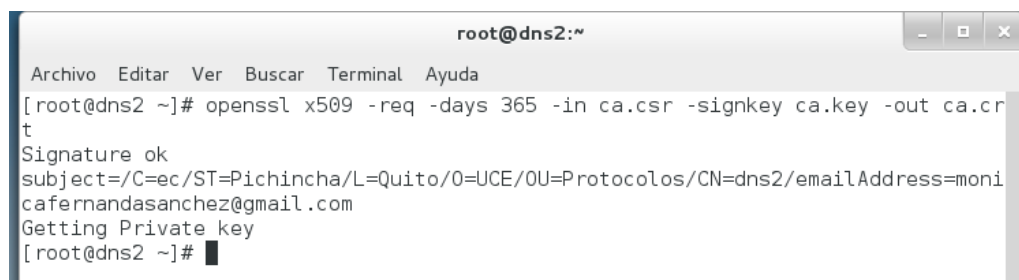
openssl req -new -key ca.key -out ca.csr luego llenamos los datos que nos va pidiendo



```
root@dns2:~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
-nameopt arg      - various certificate name options  
-reqopt arg       - various request text options  
  
[root@dns2 ~]# openssl req -new -key ca.key -out ca.csr  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [XX]:ec  
State or Province Name (full name) []:Pichincha  
Locality Name (eg, city) [Default City]:Quito  
Organization Name (eg, company) [Default Company Ltd]:UCE  
Organizational Unit Name (eg, section) []:Protocolos  
Common Name (eg, your name or your server's hostname) []:dns2  
Email Address []:monicafernandasanchez@gmail.com  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:monica  
An optional company name []:Protocolos  
[root@dns2 ~]#
```

Por último, generar un certificado auto-firmado de tipo X 509, que tiene una validez de 365 días.

openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt



```
root@dns2:~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
[root@dns2 ~]# openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt  
t  
Signature ok  
subject=C=ec/ST=Pichincha/L=Quito/O=UCE/OU=Protocolos/CN=dns2/emailAddress=monicafernandasanchez@gmail.com  
Getting Private key  
[root@dns2 ~]#
```

Luego se nos han generado 3 archivos ca.crt ca.csr y ca.key


```
[root@dns2 ~]# ls
anaconda-ks.cfg  Escritorio      prueba2
asegurado        Imágenes       prueba3.txt
ca.crt           initial-setup-ks.cfg  pruebatftp.txt
ca.csr          Maildir        Público
ca.key          Música         samba
Descargas       Plantillas     squirrelmail-webmail-1.4.22.zip
Desktop         pruebal5.txt   Vídeos
Documentos      pruebal6.txt
[root@dns2 ~]#
```

estos los copiados a los siguientes directorios

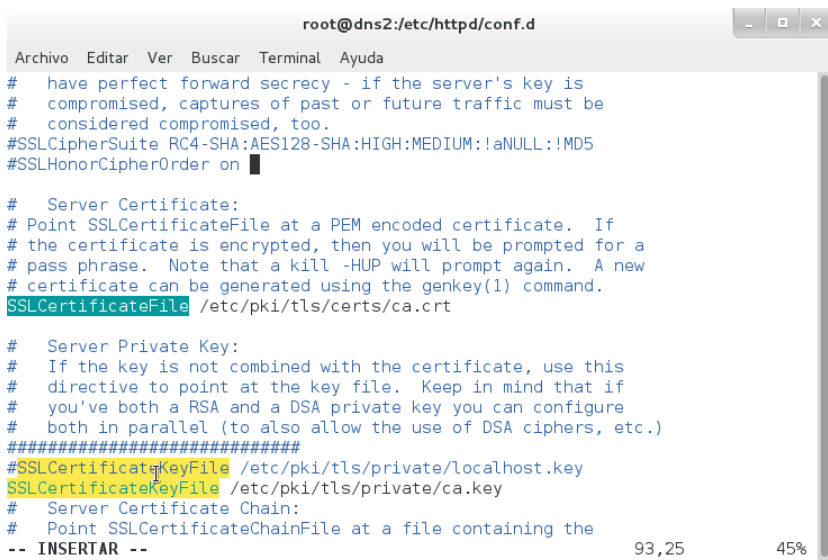
```
[root@dns2 ~]# ls
anaconda-ks.cfg  Escritorio      prueba2
asegurado        Imágenes       prueba3.txt
ca.crt           initial-setup-ks.cfg  pruebatftp.txt
ca.csr          Maildir        Público
ca.key          Música         samba
Descargas       Plantillas     squirrelmail-webmail-1.4.22.zip
Desktop         pruebal5.txt   Vídeos
Documentos      pruebal6.txt
[root@dns2 ~]# cp ca.crt /etc/pki/tls/certs/
[root@dns2 ~]# cp ca.key /etc/pki/tls/private/
[root@dns2 ~]# cp ca.csr /etc/pki/tls/private/
[root@dns2 ~]#
```

Luego editamos el archive /etc/httpd/conf.d/ssl.conf las líneas siguientes

vim /etc/httpd/conf.d/ssl.conf

SSLCertificateFile /etc/pki/tls/certs/ca.crt

SSLCertificateKeyFile /etc/pki/tls/private/ca.key



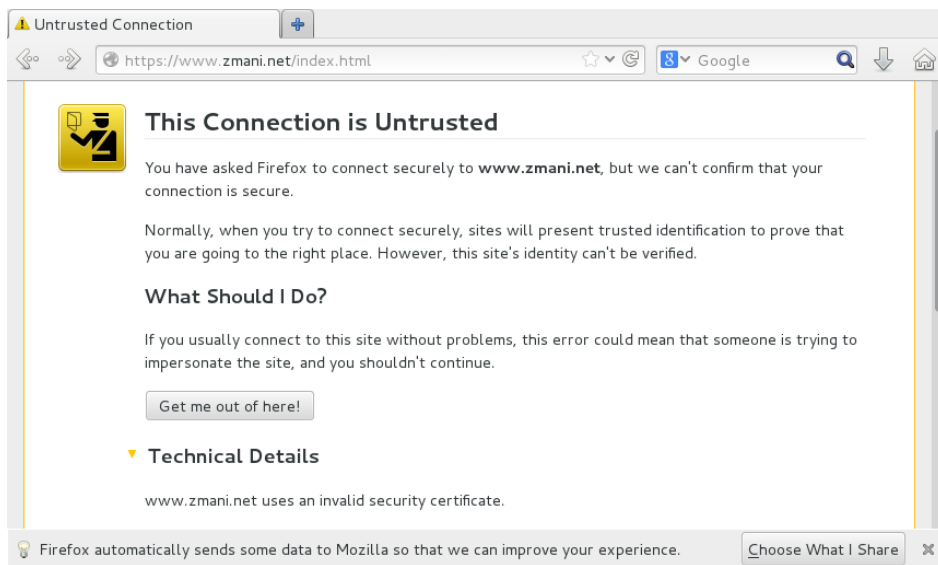
```
root@dns2:/etc/httpd/conf.d
Archivo  Editar  Ver     Buscar  Terminal  Ayuda
# have perfect forward secrecy - if the server's key is
# compromised, captures of past or future traffic must be
# considered compromised, too.
#SSLCipherSuite RC4:SHA:AES128:SHA:HIGH:MEDIUM:!aNULL:!MD5
#SSLHonorCipherOrder on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/ca.crt

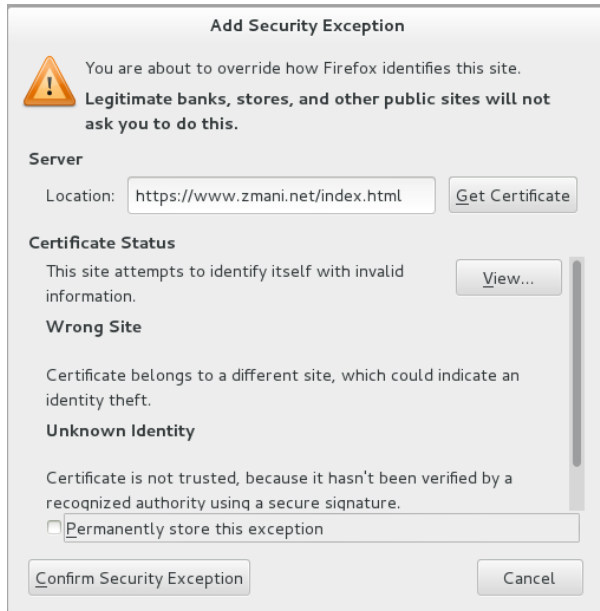
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
#####
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
-- INSERTAR --
```

Ahora ingresamos al navegador a la pagina de nuestro servidor web

Al ingresar a nuestro sitio sale la siguiente advertencia



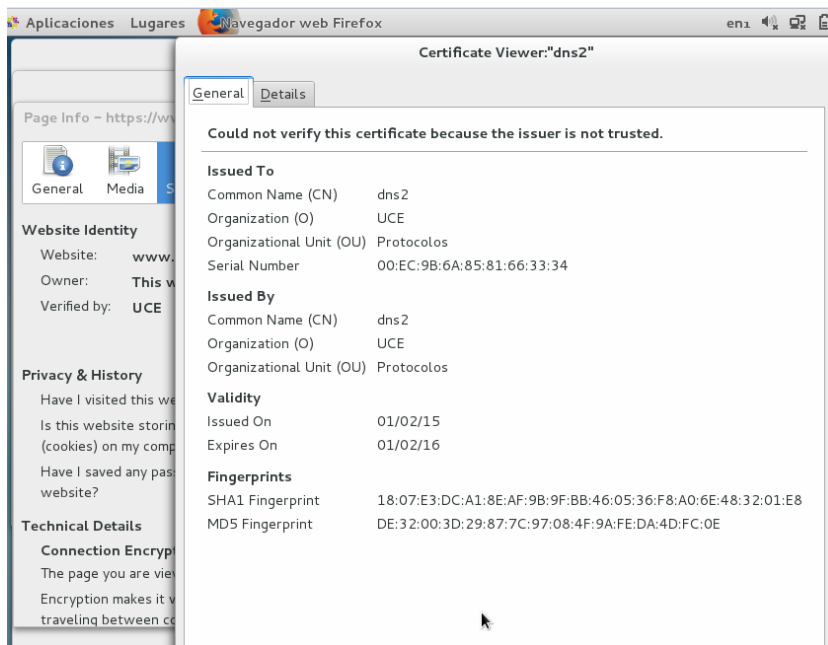
Al final de esta damos **click en add exception**



Click en confirm security



Nos dirigimos a los detalles de la conexión podemos ver los detalles del certificado



SMTP -Simple Mail Transfer Protocol

Protocolo para la transferencia simple de correo electrónico), es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, etc.

Los administradores de servidor pueden elegir si los clientes utilizan TCP puerto 25 (SMTP) o el puerto 587 (Presentación) para retransmitir el correo saliente a una inicial del servidor de correo.³ Las especificaciones y muchos servidores soportan ambos. Aunque algunos servidores soportan el puerto 465 para el legado SMTP seguro en violación de las especificaciones

Instalacion y configuración del protocolo

Primero instalamos y configuramos postfix

#yum -y install postfix

luego configuramos el archivo main.cf

#vim /etc/postfix/main.cf

Archivo principal de configuración de postfix, comentar línea 116 y 164.

#inet_interfaces = localhost

#mydestination = \$myhostname, localhost.\$mydomain, localhost

Lineas que se añaden en el mismo archivo que editamos.

myhostname = mail.zmani.net

mydomain = mail.zmani.net

myorigin = \$mydomain

home_mailbox = mail/

#permitir que todos los clientes del servidor le envíen mail

mynetworks = 10.3.0.0/16,127.0.0.1/8(linea265)

echo "prueba desde Centos hacia Hotmail" | mail -s "primer asunto" monica@zmani.net

Instalamos dovecot para poder recibir los mensajes del usuario

#yum -y install dovecot

#gedit /etc/dovecot/dovecot.conf

Configuramos el archivo /etc/dovecot/conf.d/10-auth.conf

```
10-auth.conf X
##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.

disable_plaintext_auth = no
```

Configuramos el archivo dovecot mail para los correos /etc/dovecot/conf.d/10-mail.conf

```
10-mail.conf X
#
# There are a few special variables you can use, eg.:
#
# %u - username
# %n - user part in user@domain, same as %u if there's no domain
# %d - domain part in user@domain, empty if there's no domain
# %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%n/%n:INDEX=/var/indexes/%d/%n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location =
```

#Systemctl restart dovecot

Para probar que todo esta bien configurado hacemos:

#telnet localhost 110

```
[root@dns2 Escritorio]# telnet localhost 110
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
```

#telnet localhost 143

```
[root@dns2 Escritorio]# telnet localhost 143
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

Enviando un mensaje de prueba hacia el usuario de nuestro servidor , llamado “servidor”

```
root@dns2:/home/servidor/Maildir/new
Archivo Editar Ver Buscar Terminal Ayuda
[root@dns2 new]# echo "hola esta es una prueba prueba" | mail -s "prueba de centos" servidor
```

Revisamos el mensaje en la carpeta del usuario servidor en `cd /home/servidor/Maildir/new` Ls y están todos los mensajes enviados

```
[root@dns2 new]# ls
1421792644.Vfd01I236f4d0M116281.dns2.zmani.net
1422827507.Vfd01I23708d7M930589.dns2.zmani.net
1422827638.Vfd01I23708d8M420641.dns2.zmani.net
...
[root@dns2 new]# cat 1422827638.Vfd01I23708d8M420641.dns2.zmani.net
Return-Path: <root@zmani.net>
X-Original-To: servidor
Delivered-To: servidor@zmani.net
Received: by mail.zmani.net (Postfix, from userid 0)
        id 3ED2841DB1C6; Sun,  1 Feb 2015 16:53:58 -0500 (ECT)
Date: Sun, 01 Feb 2015 16:53:58 -0500
To: servidor@zmani.net
Subject: prueba de centos
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20150201215358.3ED2841DB1C6@mail.zmani.net>
From: root@zmani.net (root)

hola esta es una prueba prueba
[root@dns2 new]#
```

Ahora creamos los usuarios MONICA Y GUSTAVO en cada uno de los servidores entonces nos vamos a enviar correos con Thunderbird

CONFIGURACIÓN DEL CLIENTE

Permitir al Firewall los puertos TCP 993 (IMAP4S) y 995(POP3S).

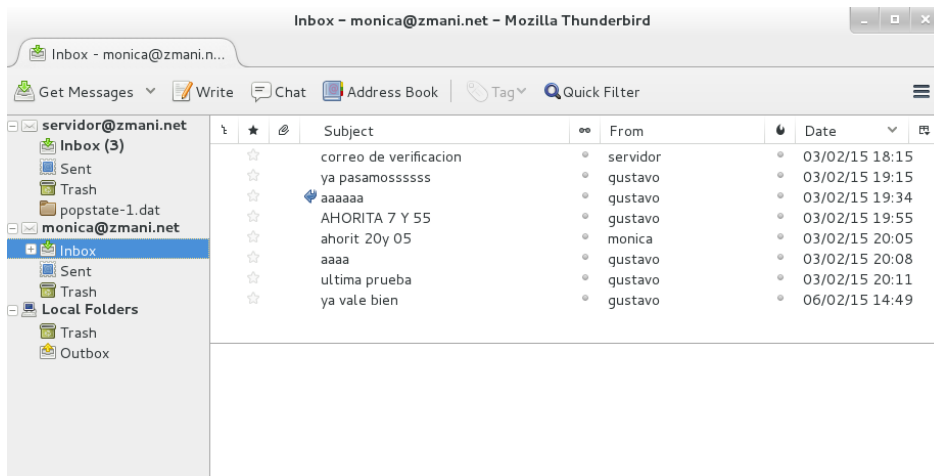
Instalamos thunderbird con el commando si no funciona, primero instalamos yum install epel-release y luego el comando siguiente:

yum install thunderbird

Enviar y recibir correo de un servidor

Se ejecuta thunderbird. En la primera pantalla se ingresa un nombre, una cuenta real con su respectivo password del usuario del servidor .

Luego se elige IMAP (en este caso elegimos IMAP) y clic en “Create Account”:



Simple Network Management Protocol o SNMP

Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento. El agente SNMP recibe solicitudes en el puerto UDP 161. El administrador puede enviar solicitudes de cualquier puerto de origen disponible para el puerto 161 en el agente

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. E

Instalacion y configuración del protocolo

Instalamos las dependencias necesarias:

#yum install gd gd-devel gcc glibc glibc-common

Activamos los repositorios de epel para poder instalar nagios

#yum install epel-release

Instalamos nagios

#yum install nagios*

Habilitamos el puerto 80 en tcp del firewall

En el archivo /etc/nagios/objects/contacts.cfg colocamos en correo del administrador en la línea email

```
root@snmp:/etc/nagios/objects
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
#####
# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-con
:act'
# template which is defined elsewhere.

define contact{
    contact_name      nagiosadmin      ; Short name of
user
    use                generic-contact  ; Inherit default
: values from generic-contact template (defined above)
    alias             Nagios Admin     ; Full name of u
ser
    email              administrador@gaar.net ; <<***** CHANGE
THIS TO YOUR EMAIL ADDRESS *****
}

#####
41,1 62%
```

Abrimos la configuración de nagios /etc/httpd/conf.d/nagios.conf

Comentamos las líneas:

#Order allow,deny

#Allow from all

Descomentamos las líneas y agregamos la ip de nuestra red:

Order deny,allow

Deny from all

Allow from 127.0.0.1 10.3.0.0/16

```
root@snmp:/etc/httpd/conf.d
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
AllowOverride None

AuthName "Nagios Access"
AuthType Basic
AuthUserFile /etc/nagios/passwd

<IfModule mod_authz_core.c>
    # Apache 2.4
    <RequireAll>
        Require all granted
        # Require local
        Require valid-user
    </RequireAll>
</IfModule>
<IfModule !mod_authz_core.c>
    # Apache 2.2
    Order allow,deny
    Deny from all
    Order deny,allow
    Allow from 127.0.0.1 10.3.0.0/16
    Require valid-user
</IfModule>

29,6 28%
```

Le asignamos una contraseña al usuario de nagios

```
#htpasswd /etc/nagios/passwd nagiosadmin
```

Activamos e iniciamos los servicios de necesarios:

```
# systemctl start nagios
```

```
# systemctl start httpd
```

```
# chkconfig nagios on
```

```
# chkconfig httpd on
```

Para acceder a la página de administración, en un navegador abrimos localhost/nagios

Configuración del archivo **/etc/nagios/nagios.cfg**

Aquí debemos des comentar la línea: `cfg_dir=/etc/nagios/servers`



```
root@snmp:/etc/nagios
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

# Definitions for monitoring a network printer
#cfg_file=/etc/nagios/objects/printer.cfg

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

cfg_dir=/etc/nagios/servers
#cfg_dir=/etc/nagios/printers
#cfg_dir=/etc/nagios/switches
#cfg_dir=/etc/nagios/routers

cfg_dir=/etc/nagios/conf.d

# OBJECT CACHE FILE
# This option determines where object definitions are cached when
# Nagios starts/restarts. The CGIs read object definitions from
# this cache file (rather than looking at the object config files
56,1 3%
```

Registrar un nuevo host (por ejemplo el servidor de nombres dns1.gaar.net):

Creamos un nuevo archivo en `/etc/nagios/objects` con nombre `dns1.gaar.net.cfg`

Este archivo debe quedar así:


```
root@snmp:/etc/nagios/objec

Archivo  Editar  Ver  Buscar  Terminal  Ayuda

define host{
use                linux-server
host_name          dns1.gaar.net
alias              dns1
address            10.3.0.50
max_check_attempts 5
check_period        24x7
notification_interval 30
notification_period 24x7
}
~
~
~
```

En el archivo /etc/nagios/nagios.cfg, en la sección de `cfg_file`, agregamos una nueva línea: `cfg_file=/etc/nagios/objects/dns1.gaar.net.cfg` (Nota: es el archivo que acabamos de crear)

```
root@snmp:/etc/nagios

Archivo  Editar  Ver  Buscar  Terminal  Ayuda

# host groups, contacts, contact groups, services, etc
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/etc/nagios/objects/commands.cfg
cfg_file=/etc/nagios/objects/contacts.cfg
cfg_file=/etc/nagios/objects/timeperiods.cfg
cfg_file=/etc/nagios/objects/templates.cfg
cfg_file=/etc/nagios/objects/cliente.gaar.net.cfg
cfg_file=/etc/nagios/objects/dns1.gaar.net.cfg
cfg_file=/etc/nagios/objects/dns2.zmani.net.cfg
cfg_file=/etc/nagios/objects/cliente.zmani.net.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/etc/nagios/objects/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/etc/nagios/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/etc/nagios/objects/switch.cfg

35,1 1%
```

Debemos crear un archivo de configuración para cada host que queremos gestionar, y agregar la línea correspondiente en el archivo anterior.

#systemctl restart nagios

EN EL HOST QUE QUEREMOS GESTIONAR

Instalamos net-snmp

#yum install net-snmp

Editamos el archivo: `cd /etc/snmp/snmpd.conf`

Al final agregamos la línea `rocommunity public 10.3.0.99` (Ip del servidor nagios)

```
root@dns1:/etc/snmp

Archivo  Editor  Ver  Buscar  Terminal  Ayuda

# enterprises.ucdavis.255.1 = "life the universe and everything"
# enterprises.ucdavis.255.2.1 = 42
# enterprises.ucdavis.255.2.2 = OID: 42.42.42
# enterprises.ucdavis.255.3 = Timeticks: (363136200) 42 days, 0:42:42
# enterprises.ucdavis.255.4 = IPAddress: 127.0.0.1
# enterprises.ucdavis.255.5 = 42
# enterprises.ucdavis.255.6 = Gauge: 42
#
# % snmpget -v 1 localhost public .1.3.6.1.4.1.2021.255.5
# enterprises.ucdavis.255.5 = 42
#
# % snmpset -v 1 localhost public .1.3.6.1.4.1.2021.255.1 s "New string"
# enterprises.ucdavis.255.1 = "New string"
#

# For specific usage information, see the man/snmpd.conf.5 manual page
# as well as the local/passtest script used in the above example.

#####
# Further Information
#
# See the snmpd.conf manual page, and the output of "snmpd -H".
community public 10.3.0.99
"snmpd.conf" 463L, 18890C                                     463,1      Final
```

#systemctl restart snmpd
#chkconfig snmpd on

EN EL SERVIDOR NAGIOS

Ya podemos acceder a la consola web de Nagios

Nagios Core - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Nagios Core

localhost/nagios/

Nagios®

General
Home
Documentation

Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
(Unhandled)
Hosts (Unhandled)
Network Outages

Quick Search:

Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log

Current Network Status
Last Updated: Sun Feb 8 14:53:33 PET 2015
Updated every 30 seconds
Logged in as nagiosadmin

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals
Up Down Unreachable Pending
5 0 0 0
All Problems All Types
0 5

Service Status Totals
Ok Warning Unknown Critical Pending
6 2 0 0 0
All Problems All Types
2 0 0

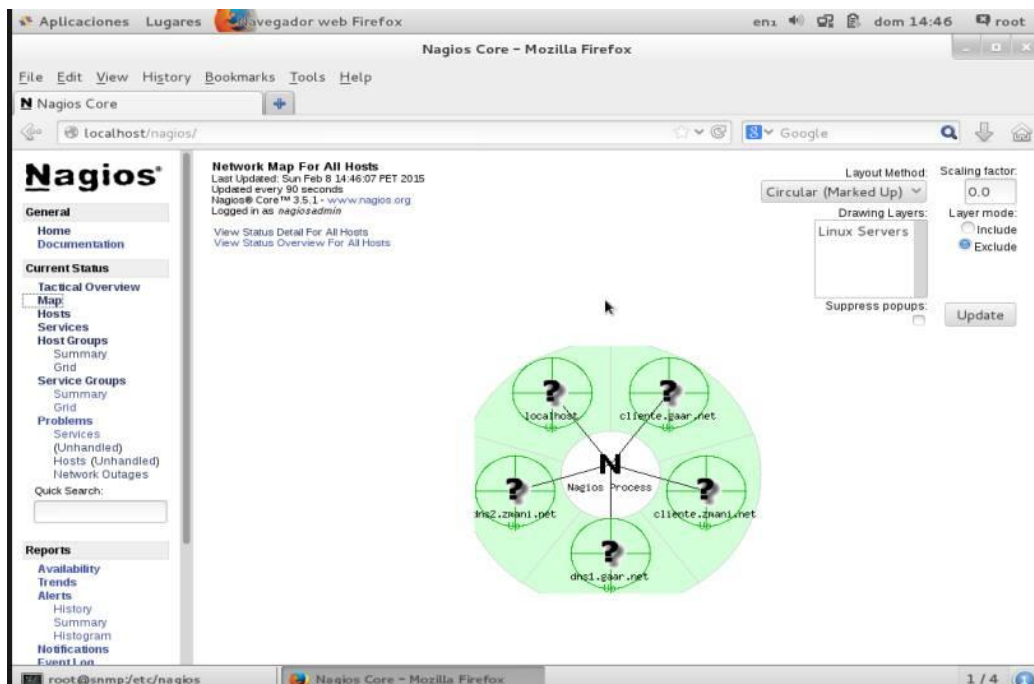
Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	02-08-2015 14:52:33	0d 17h 8m 40s	1/4	OK - load average: 0.53, 0.33, 0.26
	Current Users	OK	02-08-2015 14:50:03	0d 17h 8m 2s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	02-08-2015 14:53:11	0d 17h 7m 25s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5162 bytes in 0,004 second response time
	PING	OK	02-08-2015 14:50:54	0d 17h 6m 47s	1/4	PING OK - Packet loss = 0%, RTA = 0.24 ms
	Root Partition	OK	02-08-2015 14:48:48	0d 17h 6m 10s	1/4	DISK OK - free space: / 12617 MB (70% inode=99%):
	SSH	OK	02-08-2015 14:51:18	0d 17h 5m 32s	1/4	SSH OK - OpenSSH_6.4 (protocol 2.0)
	Swap Usage	OK	02-08-2015 14:49:25	0d 17h 4m 55s	1/4	SWAP OK - 72% free (1464 MB out of 2047 MB)
	Total Processes	WARNING	02-08-2015 14:49:55	0d 4h 46m 38s	4/4	PROCS WARNING: 253 processes with STATE = RSZDT

Results 1 - 8 of 8 Matching Services

root@snmp/etc/nagios Nagios Core - Mozilla Firefox 1 / 4



LDAP *Lightweight Directory Access Protocol*

Protocolo Ligero/Simplificado de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Instalación y configuración del protocolo

#yum -y install openldap-servers openldap-clients

[root@ldap ~]# vi /etc/openldap/slapd.conf

```
# create new
pidfile
/run/openldap/slapd.pid
argsfile
```

[root@ldap ~]# rm -rf /etc/openldap/slapd.d/*

[root@ldap ~]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d

config file testing succeeded

[root@ldap ~]# vi /etc/openldap/slapd.d/cn=config/olcDatabase=\{0\}config.ldif

line 6: change

olcAccess:

{0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by * break

```
[root@ldap ~]# chown -R ldap. /etc/openldap/slapd.d
[root@ldap ~]# chmod -R 700 /etc/openldap/slapd.d
[root@ldap ~]# systemctl start slapd
[root@ldap ~]# systemctl enable slapd
```

```
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/core.ldif
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=core,cn=schema,cn=config"
```

```
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"
```

```
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"
```

```
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"
```

```
[root@dlp ~]# slappasswd
# generate encrypted password
```

```
New password:
# input any password
```

```
Re-enter new password:
{SSHA}xxxxxxxxxxxxxxxxxx
# remember
```

```
[root@dlp ~]# vi backend.ldif
```

```
# create new
```

```
# replace the section "dc=zmani,dc=net"
```

```
# replace the section "olcRootPW: ***" to your own password generated by slappasswd above
```

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib64/openldap
olcModuleload: back_hdb
```

```
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=server,dc=world
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=zmani,dc=net
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxxxxxx
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_ik_max_objects 1500
olcDbConfig: set_ik_max_locks 1500
olcDbConfig: set_ik_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcMonitoring: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=zmani,dc=net" write by anonymous auth by self write by
* none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=zmani,dc=net" write by * read
```

```
[root@dlp ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f backend.ldif
```

```
SASL/EXTERNAL authentication started
```

```
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

```
SASL SSF: 0
```

```
adding new entry "cn=module,cn=config"
```

```
adding new entry "olcDatabase=hdb,cn=config"
```

```
[root@dlp ~]# vi frontend.ldif
```

```
# create new
```

replace the section "dc=,dc=**" to your own suffix**

replace the section "userPassword: *" to your own password generated by slappasswd above**

```
dn: dc=zmani,dc=net
objectClass: top
objectClass: dcObject
objectclass: organization
o: zmani .net
dc: Server
```

```
dn: cn=admin,dc=zmani,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
userPassword: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
dn: ou=people,dc=zmani,dc=net
objectClass: organizationalUnit
ou: people
```

```
dn: ou=groups,dc=zmani,dc=net
objectClass: organizationalUnit
ou: groups
```

[root@dlp ~]# ldapadd -x -D cn=admin,dc=zmani,dc=net-W -f frontend.ldif

Enter LDAP Password:

admin password you set above

adding new entry "dc=zmani,dc=net"

adding new entry "cn=admin, dc=zmani,dc=net"

adding new entry "ou=people, dc=zmani,dc=net"

adding new entry "ou=groups, dc=zmani,dc=net"

Para configurar a un cliente hacemos lo siguiente:

[root@www ~]# [yum](#) -y install openldap-clients nss-pam-ldapd

ldapserver=(LDAP server's hostname or IP address)

ldapbasedn="dc=zmani.net"