



INFORME SPRINT VIII	
CODIFICACION:	DTI-ITC-2024-001
FECHA:	2024-10-10

Dirección de Tecnologías e Información

“Manual de habilitación de servidores Comunicaciones, Capacitaciones y WAF (Proxy 2024)”

Versión 1.0
Fecha de emisión: 10 de octubre de 2024
Quito – Ecuador



INFORME SPRINT VIII	
CODIFICACION:	DTI-ITC-2024-001
FECHA:	2024-10-10

Contenido

1. SERVIDOR RESPALDOS DE COMUNICACIONES.....	3
2. CAPACITACIONES – Moodle	4
3. WAF (Proxy 2024) - controla los subdominios	5
FIRMAS.....	9

A continuación, se describen los comandos para verificar o habilitar los daemons o servicios de algunos servidores en caso contingencia.

1. SERVIDOR RESPALDOS DE COMUNICACIONES

- Habilitar el servicio de firewallld
`sudo systemctl enable firewallld`
- Reiniciar el servicio de apache
`sudo systemctl restart httpd`
- Se realiza el montaje de disco sdb1 al data



Ilustración 1 Montaje de disco

- Se configura el servicio de Samba y su complemento para que se inicien automáticamente al arrancar el sistema.

`Sudo systemctl enable nmb`

`Sudo systemctl enable smb`

Complemento de Samba

- Se verifica el estado del servicio y se lo inicia.

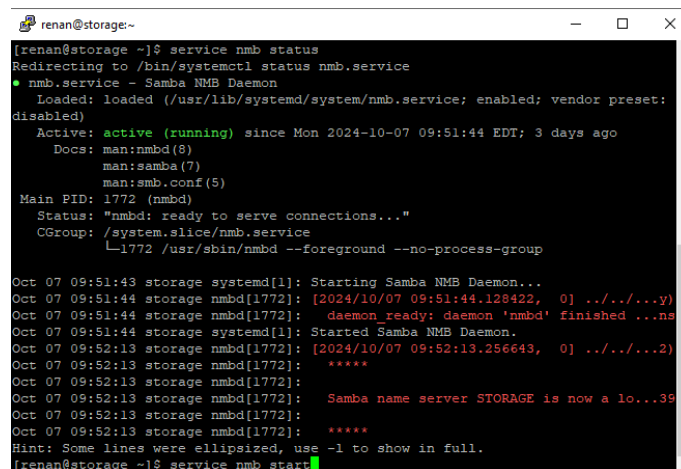
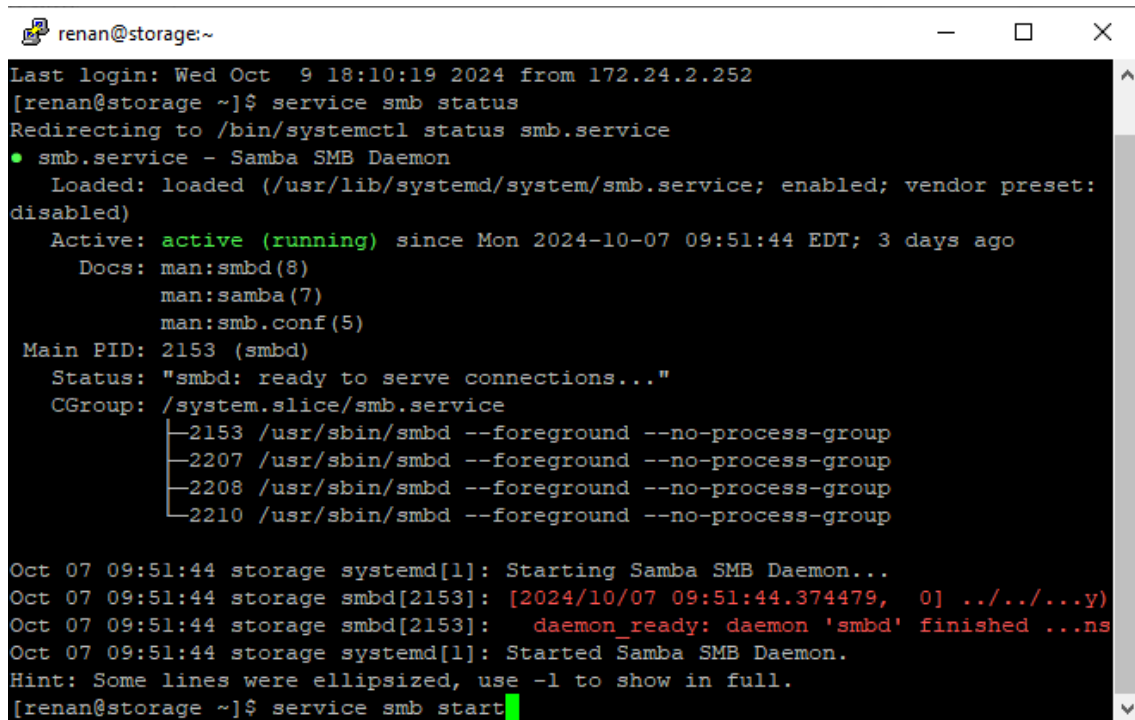


Ilustración 2 Complemento de Samba

Samba

- Se verifica el estado del servicio y se lo inicia.



```

renan@storage:~
Last login: Wed Oct  9 18:10:19 2024 from 172.24.2.252
[renan@storage ~]$ service smb status
Redirecting to /bin/systemctl status smb.service
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-10-07 09:51:44 EDT; 3 days ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Main PID: 2153 (smbd)
    Status: "smbd: ready to serve connections..."
   CGroup: /system.slice/smb.service
           └─2153 /usr/sbin/smbd --foreground --no-process-group
             └─2207 /usr/sbin/smbd --foreground --no-process-group
               └─2208 /usr/sbin/smbd --foreground --no-process-group
                 └─2210 /usr/sbin/smbd --foreground --no-process-group

Oct 07 09:51:44 storage systemd[1]: Starting Samba SMB Daemon...
Oct 07 09:51:44 storage smbd[2153]: [2024/10/07 09:51:44.374479, 0] ../../../../y)
Oct 07 09:51:44 storage smbd[2153]:  daemon_ready: daemon 'smbd' finished ...ns
Oct 07 09:51:44 storage systemd[1]: Started Samba SMB Daemon.
Hint: Some lines were ellipsized, use -l to show in full.
[renan@storage ~]$ service smb start

```

Ilustración 3 Servicio Samba

Nota: En caso de contingencia el servidor donde se encuentra el sitio web del Congope que se debe encender y que se encuentra en el Vcenter es:

 SITIO_WEB_2024

Ilustración 4 Máquina Virtual en Vcenter Sitio Congope

2. CAPACITACIONES – Moodle

- Iniciar el servicio de apache

```
sudo systemctl start httpd
```
- Reiniciar el servicio de apache

```
sudo systemctl restart httpd
```

- Iniciar el servicio de la base de datos

```
sudo systemctl start postgresql
```

Nota: En caso de contingencia el servidor Moodle Congope que se debe encender y que se encuentra en el Vcenter es:



Ilustración 5 Máquina Virtual en Vcenter Moodle

3. WAF (Proxy 2024) - controla los subdominios



Ilustración 6 Servidor WAF

- Iniciar el servicio de apache

```
sudo systemctl start httpd
```

```
sudo
```

- Reiniciar el servicio de apache

```
sudo systemctl restart httpd
```

- Se configura el servicio de Apache y Firewall para que se inicien automáticamente al arrancar el sistema.

```
sudo systemctl enable httpd
```

```
sudo systemctl enable firewallld
```

Nota: En caso de contingencia el servidor WAF que se debe encender y que se encuentra en el Vcenter es:


 WAF-2024 R1

Ilustración 75 Máquina Virtual en Vcenter WAF

- Redireccionamiento del subdominio soporte.gob.ec a la ip 172.24.5.87

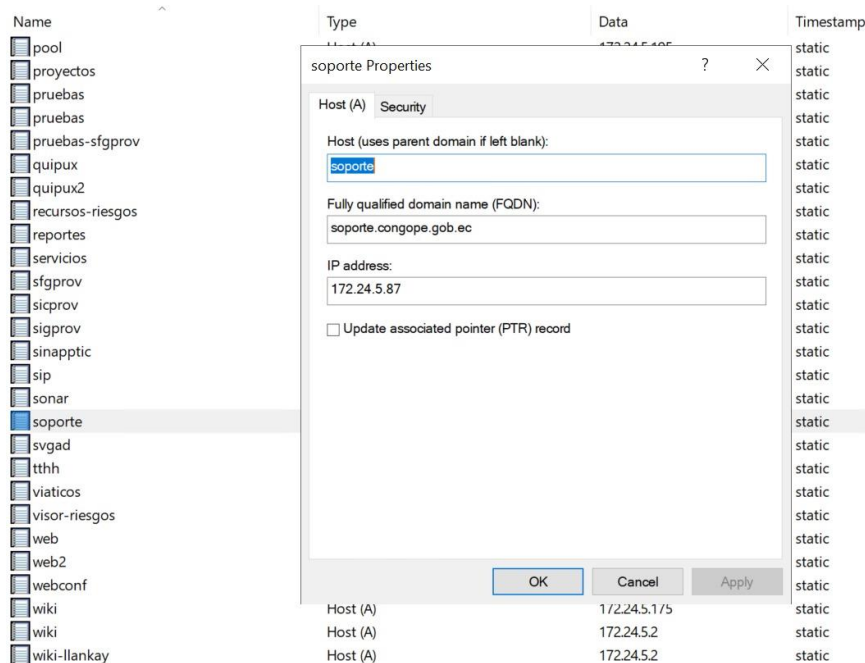


Ilustración 8 Redireccionamiento sitio web de soporte

- Configuración de certificado SSL

```
<VirtualHost 172.24.5.87:80>
  ServerName soporte.congope.gob.ec
  Redirect / https://soporte.congope.gob.ec/
</VirtualHost>
```

Ilustración 9 Certificado SSL

- Se muestra con certificado y sin certificado el subdominio.

```
<VirtualHost 172.24.5.87:443>
#DocumentRoot /var/www/myapp
ProxyPreserveHost On
ServerName soporte.congope.gob.ec
ServerAlias soporte
#SSLProxyEngine On
#RequestHeader set Front-End-Https "On"
#CacheDisable *
#ProxyHTML5Enable On

ProxyPass / http://172.24.5.80:8000/
ProxyPassReverse / http://172.24.5.80:8000/

ProxyPassReverseCookiePath / /
ProxyPassReverseCookieDomain 172.24.5.80:8000 soporte.congope.gob.ec

SSLEngine On
SSLProxyEngine On
ProxyRequests Off
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
SSLInsecureRenegotiation on
SSLProxyVerify none
SSLVerifyClient none

SSLCertificateFile "/etc/letsencrypt/live/soporte.congope.gob.ec/fullchain.pem"
SSLCertificateKeyFile "/etc/letsencrypt/live/soporte.congope.gob.ec/privkey.pem"

<IfModule mod_security2.c>
    SecRequestBodyAccess Off
    SecRuleRemoveById 200003
</IfModule>
</VirtualHost>
```

Ilustración 10 Certificado Subdominio

- Se visualiza reglas y versión de firewall

```
renan@waf2024-2:/etc/httpd/conf.d
[renan@waf2024-2 conf.d]$ sudo firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enol
sources:
services: cockpit dhcpv6-client ssh
ports: 80/tcp 443/tcp 8080/tcp 8443/tcp 8888/tcp 9999/tcp 8099/tcp
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[renan@waf2024-2 conf.d]$
```

Ilustración 11 Servicio de Firewall

- Se revisa la versión de apache.

```
renan@waf2024-2:/etc/httpd/conf.d
[renan@waf2024-2 conf.d]$ httpd -v
Server version: Apache/2.4.57 (Rocky Linux)
Server built: Aug 5 2024 00:00:00
[renan@waf2024-2 conf.d]$
```

Ilustración 12 Servicio Apache

- Se revisa la información de las direcciones IP, de las interfaces de red y redireccionamiento cast.

```
renan@waf2024-2:/etc/httpd/conf.d
[renan@waf2024-2 conf.d]$ ip a sh
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enol: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 2c:44:fd:1e:5f:b2 brd ff:ff:ff:ff:ff:ff
    altnam enp0s25
    inet 172.24.5.88/24 brd 172.24.5.255 scope global noprefixroute enol
        valid_lft forever preferred_lft forever
    inet 172.24.5.87/24 brd 172.24.5.255 scope global secondary noprefixroute enol
        valid_lft forever preferred_lft forever
    inet 172.24.5.2/24 brd 172.24.5.255 scope global secondary noprefixroute enol
        valid_lft forever preferred_lft forever
    inet 172.24.5.100/24 brd 172.24.5.255 scope global secondary noprefixroute enol
        valid_lft forever preferred_lft forever
    inet 172.24.5.12/24 brd 172.24.5.255 scope global secondary noprefixroute enol
        valid_lft forever preferred_lft forever
    inet6 fe80::b62f:6b48:de65:b670/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Ilustración 13 Información de dirección IP

- Se rastrea la ruta que siguen los paquetes de datos hasta el sitio web de soporte.

```
C:\Users\rguerrero>tracert soporte.congope.gob.ec

Trazo a la dirección soporte.congope.gob.ec [172.24.5.87]
sobre un máximo de 30 saltos:

 1    2 ms    1 ms    1 ms  172.24.2.254
 2    1 ms    1 ms    1 ms  172.24.5.87

Trazo completa.

C:\Users\rguerrero>
```

Ilustración 14 Tracert al sitio web de Soporte

- Se muestra un registro de los comandos que se ha ejecutado en la terminal.

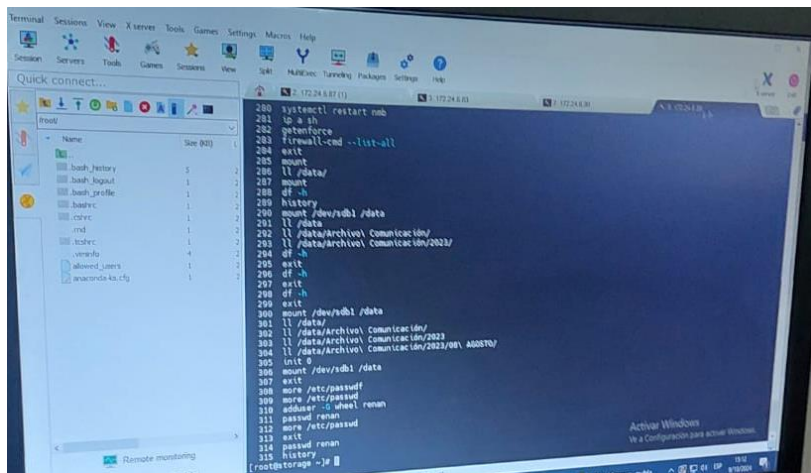


Ilustración 15 Historial de comandos ejecutados

FIRMA

	CARGO	FIRMA	FECHA
ELABORADO POR	Norma Arcos Profesional Contratado		2024-10-10