Servicio RSYNC SSL

- Instructivo para clientes
- Instructivo para administradores
- Instructivo para renovar certificado digital de Rsync-ssl

Instructivo para clientes

Uso de Rsync CSIRT Córdoba

Para utilizar el servicio rsync del CSIRT Córdoba siga atentamente los siguiente pasos:

1. Comunicar al CSIRT Córdoba (useremail@csirtcordoba.ar) la IP Address desde la cual se estará sincronizando. Para obtenerla, puede utilizar este servicio: https://ifconfig.me/

2. CSIRT Córdoba le entregará la siguiente información:

- USUARIO: Nombre de usuario con el que debe acceder al servicio.
- CONTRASEÑA: Contraseña asociada al nombre de usuario.
- CARPETA: Nombre de la carpeta que contiene la información de su interés.

3. Con esa información, debe ejecutar el siguiente comando, reemplazando los valores de USUARIO y CARPETA recibidos. DESTINO es la carpeta en su equipo en la cual desea que se alojen los datos.

```
$ rsync-ssl -avz USUARIO@rsync.csirtcordoba.ar::CARPETA DESTINO/
```

Se le pedirá la CONTRASEÑA y tras ingresarla correctamente, ya tendrá acceso a los datos.

Si no desea ingresar la contraseña en cada ocasión, puede generar un ARCHIVO de texto plano con la contraseña. Nadie más que el usuario logueado en el equipo debe tener privilegios de lectura y escritura sobre este ARCHIVO. Esto puede lograrse mediante el uso del siguiente comando:

```
$ chmod 600 ARCHIVO
```

Luego debe modificar el comando anterior por el siguiente:

```
$ rsync-ssl –password-file ARCHIVO -avz USUARIO@rsync.csirtcordoba.ar::CARPETA DESTINO/
```

Compartir con clientes

Instructivo para clientes.pdf

Instructivo para administradores

Al recibir la solicitud de acceso al servicio rsync, se debe proceder de la siguiente manera:

En el servidor rsync de la vlan7

Verificar que efectivamente existan datos correspondientes al cliente, de ser así, se deberá generar el directorio donde se almacenará la información correspondiente en el servidor de vlan 7, almacenar tales datos y sincronizarlos con el servidor externo.

En el servidor externo csirt-rsync-server

Solicitar al cliente la dirección ip desde la cual se conectará al servicio (debe ser fija).

1. Dentro del servidor externo csirt-rsync-server se debe modificar la configuración de rsync:

- Agregar el nuevo usuario con una contraseña segura al archivo /etc/rsyncd.secrets en una nueva línea. La sintaxis es usuario:contraseña.
- Editar el archivo /etc/rsyncd.conf y añadir un nuevo módulo. Dependiendo del tipo de dirección ip del cliente se deberá añadir **ipv6** o **::ffff:ipv4**.

```
[nombre_del_modulo]
path = /srv/csirt/directorio_del_cliente
auth users = usuario
hosts allow = ip_cliente
```

2. Reiniciar el servicio de rsync:

```
systemctl restart rsync.service
```

3. Añadir una excepción al firewall para la direccion del cliente:

- En primer lugar listar las reglas vigentes:

```
ufw status numbered
```

- Identificar el número de regla que bloquea el puerto 874:

```
...
[10] 874                   DENY IN     Anywhere
...
```

- Luego colocar la excepción en la misma posición para que la desplace hacia abajo. Se sugiere dejar un comentario que permita relacionar la regla con los clientes de rsync:

```
ufw insert 10 allow from ip_cliente to ip_server port 874 comment 'comentario'
```

Instructivo para renovar certificado digital de Rsync-ssl

Introducción

Los certificados son generados por el equipo de servicios y cargados en:

https://gitlab.unc.edu.ar/certificados/csirt.git

Normalmente en dicho repositorio hay 4 archivos:

- cert.pem: Es el certificado del sitio.
- chain.pem: Tengo entendido que es el certificado de la entidad de nivel superior que habilita el certificado del sitio.
- fullchain.pem: Es una concatenación de cert.pem y chain.pem.
- privkey.pem: Es la clave privada del sitio.

Procedimiento

Para el funcionamiento de haproxy, se requiere concatenar fullchain.pem con privkey.pem, por lo cual seguiremos los siguiente pasos:

1. Descargamos los archivos del repositorio en el servidor de rsync.

2. Concatenamos los archivos fullchain.pem con privkey.pem y lo guardamos en csirtcordoba.ar.pem:

```
cat fullchain.pem privkey.pem > csirtcordoba.ar.pem
```

3. Mover el archvio resultante a la carpeta /etc/letsencrypt/csirtcordoba.ar/ reemplazando el archivo anterior:

```
mv csirtcordoba.ar.pem /etc/letsencrypt/csirtcordoba.ar/csirtcordoba.ar.pem
```

4. Resetear el servicio de haproxy:

```
systemctl restart haproxy.service
```

Información

En caso de querer obtener informacion sobre el certificado, como por ejemplo la fecha de caducidad:

```
openssl x509 -in csirtcordoba.ar.pem -noout -text
```

Próxima fecha de vencimiento: Oct 12 07:02:22 2024