

# DMARC masivo — da\_dmarc\_bulk.sh

## Descripción

Script para crear registros `_dmarc` TXT en todos los dominios de un servidor DirectAdmin que no lo tengan. Usa la API local de DA (`CMD_API_DNS_CONTROL`), que propaga automáticamente los cambios a los miembros del cluster DNS (titrit/amazzal).

## Ubicación

```
/root/utilidades/directadmin/da_dmarc_bulk.sh
```

Repositorio: `~/utilidades/` (git)

## Uso

```
# Ver qué haría sin hacer cambios
./da_dmarc_bulk.sh --dry-run

# Ejecutar en todos los dominios
./da_dmarc_bulk.sh

# Solo un dominio específico
./da_dmarc_bulk.sh --domain ejemplo.com

# Con política quarantine en vez de none
./da_dmarc_bulk.sh --policy quarantine

# Con dirección RUA personalizada (%DOMAIN% se sustituye por el dominio)
./da_dmarc_bulk.sh --rua "postmaster@%DOMAIN%"
```

# Opciones

Opción	Descripción	Default
<code>--dry-run</code>	Muestra qué haría sin hacer cambios	—
<code>--policy</code>	Política DMARC: <code>none</code> , <code>quarantine</code> , <code>reject</code>	<code>none</code>
<code>--rua</code>	Email para reportes agregados. <code>%DOMAIN%</code> = placeholder	<code>dmarc@%DOMAIN%</code>
<code>--domain</code>	Procesar solo este dominio	todos

## Requisitos

- Root en servidor DirectAdmin
- `curl`, `dig`, `python3`
- DirectAdmin binary en `/usr/local/directadmin/directadmin`

## Cómo funciona

1. Obtiene credenciales API via `directadmin api-url`
2. Lista usuarios y dominios desde el filesystem (`/usr/local/directadmin/data/users/*/domains/*.conf`)
3. Para cada dominio, consulta `dig +short _dmarc.DOMAIN TXT @127.0.0.1`
4. Si no tiene DMARC, lo crea via `CMD_API_DNS_CONTROL` con impersonación (`admin|usuario`)
5. El cluster DNS sincroniza automáticamente

## Detalles técnicos

### API DirectAdmin para DNS

- **Endpoint:** `CMD_API_DNS_CONTROL?domain=DOMINIO&json=yes`
- **Impersonación obligatoria:** `admin|usuario:password` — el admin no puede modificar DNS de un dominio directamente, debe impersonar al usuario propietario
- **Formato del value TXT:** las comillas deben ir URL-encoded (`%22`) dentro del valor: `%22v%3DDMARC1...%22`
- **Propagación:** DA incrementa el serial de la zona y los slaves sincronizan via AXFR. Si no sincronizan inmediatamente, ejecutar `rndc notify DOMINIO` en el master

# Ficheros que NO son dominios

El script filtra automáticamente ficheros `.hotlink`, `.suspended` y `.letsencrypt` que DA almacena en el mismo directorio que los `.conf` de dominios.

## Dominios con DNS externo

Dominios cuyo DNS no está en el servidor DA (ej: Cloudflare) darán error `Domain does not belong to you` o `DNS controlled remotely`. Es esperado — esos DMARC hay que crearlos manualmente en el panel DNS externo.

## Ejemplo de salida

```
=====
DirectAdmin Bulk DMARC Creator
=====
Policy:  none
RUA:    dmarc@%DOMAIN%
=====

[OK] elayudante.es (user: elayudante) – DMARC created
[OK] fontaneriafontcal.com (user: ffontcal) – DMARC created
[SKIP] alufasa.com – DMARC already exists
[ERROR] status.castris.com (user: laravel): DNS controlled remotely

=====

Results
=====

Total domains:  91
Created:        87
Already exist:  3
Errors:         1
=====
```

## Ejecución inicial (2026-03-12)

Servidor	Total	Creados	Ya existían	Errores
----------	-------	---------	-------------	---------

kvm456	91	87	4	0
dar	19	15	4	0
srv120	276	275	0	1 (.hotlink)
srv121	139	76	62	1 (.hotlink)
amazsal	2	0	1	1 (DNS externo)
titrit	0	0	0	0

# Registro DMARC creado

```
_dmarc 1800 IN TXT "v=DMARC1; p=none; rua=mailto:dmarc@DOMINIO"
```

- **p=none** — modo monitorización (no rechaza ni pone en cuarentena). Recomendado como primer paso
- **rua** — dirección donde llegan los reportes agregados. Requiere que exista el buzón `dmarc@dominio` (o redirección)

# Licencia

AGPL-3.0 — GNU Affero General Public License v3.0

Revision #1

Created 2026-03-12 05:48:27 UTC by Abkrim

Updated 2026-03-12 05:48:27 UTC by Abkrim