Manejo de la plataforma MISP

Espacio en disco duro servidor MISP

Con la recepción contínua de eventos hacia la plataforma MISP y el almacenamiento ocupado en disco se requerirá periódicamente eliminar eventos antiguos que ya no representan información actualizada, para este propósito se ingresa a la base de datos de la plataforma desplegada.

Detener los servicios de Docker Compose
Una vez seguro de que la base de datos está en un estado consistente, se procede a detener los servicios de Docker Compose:

```
docker-compose down
```

Ingresamos a la consola del contenedor que almacena la base de datos

```
docker exec -it misp-docker-db-1 bash
```

Dentro de la instancia de base de datos se realizan los siguientes comandos:

```
USE misp;
DELETE FROM events WHERE date < '2020-01-01';
DELETE FROM attributes WHERE event_id NOT IN (SELECT id FROM events);
DELETE FROM objects WHERE event_id NOT IN (SELECT id FROM events);
DELETE FROM event_tags WHERE event_id NOT IN (SELECT id FROM events);
```

Reiniciar los servicios de Docker Compose

Antes de detener los servicios, verifica que la base de datos esté en un estado consistente. Puedes ejecutar consultas de verificación para asegurarte de que no queden referencias huérfanas:

```
SELECT * FROM attributes WHERE event_id NOT IN (SELECT id FROM events);
SELECT * FROM objects WHERE event_id NOT IN (SELECT id FROM events);
SELECT * FROM event_tags WHERE event_id NOT IN (SELECT id FROM events);
```

Se debe posicionar el terminal en el directorio que contiene el docker compose para poder reiniciarlo.

```
docker-compose up -d
```

Revision #7
Created 7 enero 2025 13:47:49 by Ricardo Alberto
Updated 3 abril 2025 12:30:23 by Ricardo Alberto