

Laboratorio de Sistemas Operativos y Redes



Trabajo Final: StreamVault



Alumnos: Cirilli, Ignacio
Greco, Gustavo Guido

Profesor: José Luis Di Biase

Guía completa para Instalar y Usar StreamVault (Passbolt) en Ubuntu con Nginx y MariaDB

Índice

1. **Introducción**
2. **Requisitos**
 - 2.1 Hardware de la máquina utilizada
 - 2.2 Requisitos del sistema
 - 2.3 Software necesario
3. **Instalación paso a paso**
 - 3.1 Actualizar el sistema
 - 3.2 Instalar PHP y dependencias
 - 3.3 Instalar MariaDB
 - 3.4 Crear base de datos
 - 3.5 Instalar Nginx
 - 3.6 Descargar e instalar Passbolt
4. **Cómo usar StreamVault**
5. **Casos de uso reales**
6. **Errores frecuentes**
7. **Consejos de seguridad adicionales**
8. **Conclusiones y recursos útiles**

1. Introducción

Bienvenido a esta guía pensada para personas que buscan una forma más segura, privada y organizada de compartir contraseñas con amigos, familiares o compañeros de equipo. El protagonista de este tutorial es **StreamVault**, una aplicación que toma como base **Passbolt**.

Passbolt es un gestor de contraseñas de código abierto diseñado específicamente para equipos y organizaciones que necesitan compartir credenciales de forma segura. A diferencia de herramientas como **LastPass**, **1Password** o **Bitwarden**, que están orientadas principalmente al uso individual (aunque tienen planes de equipo), Passbolt fue concebido desde sus cimientos para el trabajo colaborativo y la autogestión de seguridad.

Utiliza tecnologías como **GPG (GNU Privacy Guard)** para cifrar y descifrar contraseñas, lo que significa que cada usuario tiene su propia clave privada, garantizando así que solo quienes estén autorizados puedan acceder a las credenciales compartidas.

Además, a diferencia de otros servicios que operan en la nube de un proveedor, Passbolt permite ser instalado en tu propio servidor. Esto da un control total sobre la información almacenada y elimina la necesidad de confiar tus contraseñas a un tercero.

StreamVault es una instancia autohosteada de Passbolt pensada para resolver una necesidad muy concreta pero común: compartir contraseñas de plataformas como Netflix, HBO Max o Spotify entre varias personas de forma ordenada, segura y privada. Nada de pasarse claves por WhatsApp o anotarlas en papeles.

Esta guía tiene como objetivo ayudarte a instalar y configurar StreamVault en un servidor Ubuntu, utilizando **Nginx** como servidor web y **MariaDB** como base de datos. Está pensada para usuarios que no necesariamente tienen experiencia en programación, pero que desean tener una solución segura, privada y eficaz para compartir contraseñas en grupo.

Con StreamVault podés crear un servidor privado para guardar y compartir esas credenciales de manera **segura, cifrada y accesible desde cualquier navegador**, evitando malos entendidos y minimizando riesgos.

Esta guía te acompaña paso a paso para instalar StreamVault en un servidor Ubuntu utilizando **Nginx** como servidor web y **MariaDB** como base de datos, sin necesidad de programar ni escribir una sola línea de código.

2. Requisitos

Hardware de la máquina utilizada:

El equipo utilizado para la instalación de StreamVault cuenta con las siguientes características técnicas:

- Procesador: Intel Core i6-6200U a 2.50 GHz
- Memoria RAM: 8 GB
- Almacenamiento: 50 GB asignados para la máquina virtual (SSD en el host)
- Conectividad: Conexión a internet activa y estable
- Compatibilidad de virtualización: Soporte para virtualización habilitado (VT-x).

Requisitos del sistema

Antes de comenzar, asegurate de tener lo siguiente:

- Una PC o servidor con **Ubuntu 22.04 LTS** o superior instalado.
- Acceso a una terminal con permisos de administrador (**sudo**).
- Una conexión a internet activa.
- Ganas de experimentar y aprender algo nuevo :)

Software necesario

Vas a necesitar instalar algunos programas:

- **PHP 8.2** o superior (Passbolt no funciona con versiones menores).
- **Nginx** como servidor web.
- **MariaDB** como motor de base de datos.
- **GPG**, para generar claves de cifrado seguras.
- **Certbot** (opcional, pero recomendado para tener HTTPS con Let's Encrypt).

3. Instalación paso a paso

Paso I: Actualizar el sistema

Primero, abrí la terminal y ejecutá:

```
sudo apt update && sudo apt upgrade -y
```

Paso II: Instalar PHP 8.2 y sus dependencias

Passbolt requiere ciertos módulos de PHP:

```
sudo apt install -y php8.2 php8.2-cli php8.2-fpm php8.2-mysql php8.2-gd  
php8.2-xml php8.2-mbstring php8.2-curl php8.2-gnupg php8.2-imagick
```

Paso III: Instalar MariaDB

Esta base de datos va a guardar toda la información cifrada:

```
sudo apt install mariadb-server mariadb-client  
sudo mysql_secure_installation
```

Paso IV: Crear base de datos para StreamVault (Passbolt)

Ingresa a la consola de MySQL:

```
sudo mysql -u root -p
```

Y ejecutá estas consultas (reemplazá la contraseña por una segura):

```
CREATE DATABASE passbolt;  
CREATE USER 'passboltuser'@'localhost' IDENTIFIED BY 'Tu_Contraseña_Segura';  
GRANT ALL PRIVILEGES ON passbolt.* TO 'passboltuser'@'localhost';  
FLUSH PRIVILEGES;  
EXIT;
```

Paso V: Instalar Nginx

```
sudo apt install nginx
```

Paso VI: Descargar e instalar Passbolt

Ahora seguí las instrucciones oficiales para instalar Passbolt según tu versión de Ubuntu: [🔗 Guía oficial de instalación](#)

En este punto ya deberías tener todo lo necesario para iniciar tu servidor StreamVault.

4. Cómo usar StreamVault

Una vez finalizada la instalación:

1. Abrió tu navegador e ingresá la IP del servidor o el nombre de dominio que configuraste.
2. Vas a ver la pantalla de bienvenida de Passbolt. Creá tu usuario administrador.
3. Desde el panel, podés invitar a otros usuarios por email para que accedan al sistema.
4. Cada persona creará su clave GPG (la guía te ayuda con esto).

5. Una vez dentro, podés crear entradas de contraseñas, agruparlas por categoría y compartirlas con otros miembros.
 6. Configurar los permisos según el rol de cada usuario (solo lectura, edición, etc.).
 7. Si querés habilitar acceso desde internet, asegurate de tener configurado el HTTPS usando **Certbot**.
-

5. Casos de uso reales

StreamVault es ideal para:

- **Compartir una cuenta de Netflix** sin enviar la contraseña por WhatsApp. Simplemente la cargás en la app y compartís el acceso.
- **Organizar las contraseñas familiares:** un lugar seguro donde guardar las credenciales de todos los servicios que usan en casa.
- **Evitar confusiones** con usuarios y claves repetidas o cambiadas.
- **Tener control de acceso:** sabés quién ve qué información y podés revocar accesos en cualquier momento.

6. Errores frecuentes

Durante la instalación o el uso de StreamVault (Passbolt), es posible que te encuentres con algunos problemas comunes. Acá te dejamos una lista de los más frecuentes y cómo resolverlos:

✗ Error: *502 Bad Gateway en Nginx*

Causa: El servicio PHP-FPM no está corriendo o no está vinculado correctamente con Nginx.

Solución:

```
sudo systemctl restart php8.2-fpm
```

```
sudo systemctl restart nginx
```

✗ Error: *"Could not connect to the database"* en el navegador

Causa: Error en las credenciales de acceso a la base de datos o el servicio de MariaDB no está corriendo.

Solución:

- Asegurate de que MariaDB esté activo:

```
sudo systemctl status mariadb
```

- Verificá los datos en el archivo de configuración de Passbolt (`/etc/passbolt/passbolt.php`) y que coincidan con lo que creaste en MySQL.

✗ Error al enviar correos de invitación

Causa: No se configuró correctamente un servidor SMTP.

Solución:

Editá el archivo `/etc/passbolt/passbolt.php` y completá la sección `EmailTransport` con los datos de tu proveedor de correo (como Gmail, SendGrid, etc.). Asegurate también de que no esté bloqueado el puerto 587 o 465 si usás TLS o SSL.

✗ No carga el sitio con HTTPS

Causa: No se instaló el certificado SSL correctamente.

Solución:

Instalá Certbot y ejecutá:

```
sudo certbot --nginx
```

✗ Error: *GPG key not found* o problemas con claves

Causa: El usuario no tiene una clave GPG válida asociada.

Solución:

Pedile al usuario que genere su par de claves GPG desde la interfaz de Passbolt o usando terminal:

```
gpg --full-generate-key
```

7. Consejos de seguridad adicionales

Una vez que tengas StreamVault funcionando, es fundamental aplicar ciertas medidas para reforzar la seguridad de tu instalación. A continuación, te dejamos algunas recomendaciones clave:

🔒 1. Habilitá HTTPS

- Es imprescindible proteger las conexiones entre los usuarios y el servidor usando HTTPS. Podés hacerlo fácilmente con [Let's Encrypt](#) usando Certbot.

2. Actualizá regularmente

- Asegurate de mantener actualizado Passbolt, el sistema operativo, PHP, MariaDB y Nginx. Las actualizaciones corrigen vulnerabilidades que pueden ser explotadas.

3. Restringí el acceso al servidor

- Limitá el acceso SSH solo desde direcciones IP confiables.
- Usá claves SSH en lugar de contraseñas.

4. Hacé backups regulares

- Es recomendable automatizar respaldos de:
 - La base de datos de MariaDB.
 - Las claves GPG del servidor.
 - La configuración de Passbolt.
- Podés usar `cron` para ejecutar backups diarios o semanales.

5. Creá usuarios con el menor privilegio posible

- Solo los administradores deben tener acceso completo. Los usuarios normales deben tener permisos restringidos.
- Revisá periódicamente los permisos de los usuarios.

6. Activá la autenticación en dos pasos (2FA)

- Passbolt permite habilitar 2FA para mayor protección de las cuentas de usuario.
- Recomendá a tus usuarios que la configuren desde su perfil.

7. Monitoreá tu servidor

- Utilizá herramientas como `fail2ban`, `ufw`, `logwatch` o `netdata` para proteger, limitar accesos y monitorear actividad sospechosa.

8. Conclusiones y recursos útiles

Con StreamVault, no solo centralizás la gestión de contraseñas compartidas, sino que también aumentás significativamente la seguridad y el control sobre tus credenciales, evitando el uso de medios inseguros como mensajes o correos. Gracias a la potencia de Passbolt y su enfoque colaborativo, cualquier grupo de usuarios (familia, amigos o equipo de trabajo) puede acceder de forma ordenada, auditable y segura a las contraseñas que necesita.

Este tipo de soluciones autohosteadas permite una personalización total, mayor privacidad y reduce la dependencia de servicios de terceros. Si bien la configuración inicial puede parecer compleja, una vez en marcha, StreamVault se convierte en una herramienta liviana, robusta y confiable.

Recursos útiles

-  Documentación oficial de Passbolt:
<https://help.passbolt.com>
-  Repositorio en GitHub (Passbolt):
<https://github.com/passbolt>
-  Guía para instalar Certbot con Nginx:
<https://certbot.eff.org/instructions>
-  Tutorial de backups para MariaDB:
<https://mariadb.com/kb/en/mysqldump/>
-  Guía de buenas prácticas de seguridad para servidores Linux:
<https://www.cyberciti.biz/tips/linux-security.html>