Trabajo Final

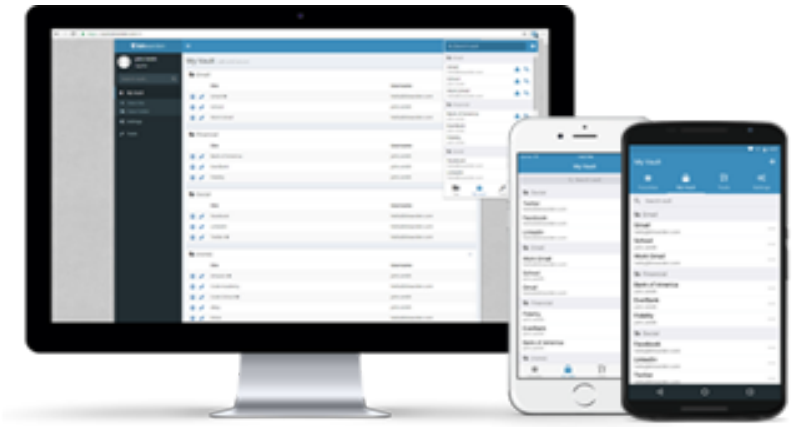
Bitwarden

Laboratorio de S. Operativos y Redes

Integrantes: Julián Bernal, Augusto Conti, Nicolás Pintos

Profesor: José Luis Di Biase

12 de julio de 2018



bitwarden

Resolvé tus problemas de administración de contraseñas.

Índice

Introducción

Bitwarden es la forma más fácil y segura para que individuos y equipos almacenen, compartan y sincronicen datos confidenciales.

Tu seguridad en línea está en riesgo.
El robo de contraseñas es un grave problema. Las páginas web y aplicaciones que usas están bajo ataque cada día. Las brechas de seguridad ocurren y tus contraseñas son robadas. Cuando usas la misma contraseña en diferentes aplicaciones o sitios web, los piratas informáticos pueden acceder fácilmente a tu correo electrónico, cuenta bancaria y otras cuentas importantes.

¿Cómo mantenerse seguro?
Los expertos en seguridad recomiendan que use una contraseña diferente, generada aleatoriamente para cada cuenta en línea que cree. Pero, ¿cómo se supone que vas a recordar y mantenerte al día con tantas contraseñas? Bitwarden te ayuda a crear y administrar contraseñas seguras.

¡Las funciones seguras de sincronización en la nube le permiten acceder a sus datos desde cualquier lugar, en cualquier dispositivo! Su bóveda está optimizada convenientemente para su uso en pc de escritorio, notebooks, tablets y celulares.

Dado que todos sus datos están completamente encriptados antes de que salgan de su dispositivo, solo usted tiene acceso a ellos. Ni siquiera el equipo de Bitwarden puede leer tus datos, incluso si quisiéramos. Sus datos están sellados con encriptación de extremo a extremo AES-256 bit, salted hashing, y PBKDF2 SHA-256.

Requerimientos mínimos

- Procesador: x64, 1.4GHz o más.
- Memoria: 2GB de RAM o más.
- Almacenamiento: 10 GB o más.
- Docker: Engine 1.8+ y Compose 1.17.1+

Instalación y uso

El proyecto Bitwarden Core contiene las APIs, base de datos y otros elementos de infraestructura necesarios para el "back-end" de todas las aplicaciones cliente de Bitwarden.

La infraestructura central está escrita en C# utilizando .NET Core con ASP.NET Core. La base de datos está escrita en T-SQL/SQL Server. El código base puede desarrollarse, compilarse, ejecutarse e implementarse multiplataforma en Windows, macOS y distribuciones Linux.

INSTALAR DOCKER

Bitwarden se implementará y ejecutará en su máquina utilizando una matriz de contenedores Docker . Bitwarden funcionará igualmente bien con las ediciones Docker Community (gratuita) y Enterprise. Debe evaluar qué edición es mejor para su instalación. Además, el despliegue de estos contenedores se orquesta mediante el uso de Docker Compose. Docker y Docker Compose deben instalarse primero en su máquina antes de comenzar una instalación de Bitwarden.

Instalar usando el repositorio

Antes de instalar Docker CE por primera vez en una máquina host nueva, debe configurar el repositorio Docker. Después, puede instalar y actualizar Docker desde el repositorio.

1. Actualice el índice apt del paquete:

```
$ sudo apt update
```

2. Instalar paquetes para permitir el `apt` uso de un repositorio a través de HTTPS:

```
$ sudo apt install apt-transport-https ca-certificates curl
  software-properties-common
```

3. Agregue la clave GPG oficial de Docker:

```
ubuntu@ubuntu-VirtualBox:~$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
OK
```

4. Verifique que ahora tiene la clave con la huella digital `9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88`, buscando los últimos 8 caracteres de la huella digital.

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-key fingerprint 0EBFCD88
pub   rsa4096 2017-02-22 [SCEA]
      9DC8 5822 9FC7 DD38 854A  E2D8 8D81 803C 0EBF CD88
uid           [desconocida] Docker Release (CE deb) <docker@docker.com>
sub   rsa4096 2017-02-22 [S]
```

5. .**Nota** : El comando `lsb_release -cs` retorna el nombre de su distribución de Ubuntu, como `xenial`.

```
ubuntu@ubuntu-VirtualBox:~$ sudo add-apt-repository \
>    "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
>    $(lsb_release -cs) \
>    stable"
```

Instalar Docker CE

1. Actualiza el índice `apt` del paquete.

```
$ sudo apt-get update
```

2. Instale la última versión de Docker CE

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt-get install docker-ce
```

3. El daemon Docker se inicia automáticamente.
4. Verifique que Docker CE esté instalado correctamente ejecutando la `hello-world` imagen.

```
ubuntu@ubuntu-VirtualBox:~$ sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
9db2ca6ccae0: Pull complete
Digest: sha256:4b8ff392a12ed9ea17784bd3c9a8b1fa3299cac44aca35a85c90c5e3c7afacdc
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.
```

Este comando descarga una imagen de prueba y la ejecuta en un contenedor. Cuando el contenedor se ejecuta, imprime un mensaje informativo y se cierra.

Instalar Docker-Compose

En Linux , puede descargar el binario Docker Compose desde la página de publicación del repositorio Compose en GitHub.

1. Descargar la última versión de Docker Compose:

```
sudo curl -L
https://github.com/docker/compose/releases/download/1.21.2/docker-compose-$(
uname -s)-$(uname -m) -o /usr/local/bin/docker-compose
```

2. Aplicar permiso de ejecutable al binario y comprobar la instalación:

```
ubuntu@ubuntu-VirtualBox:~$ sudo chmod +x /usr/local/bin/docker-compose
ubuntu@ubuntu-VirtualBox:~$ docker-compose --version
docker-compose version 1.21.2, build a133471
```

INSTALAR BITWARDEN

1. Descargue la secuencia de comandos principal de Bitwarden en su máquina en la ubicación deseada:

NOTA: Todos los activos de Bitwarden se instalarán en el directorio ./bwdata relativo al lugar donde se encuentra la secuencia de comandos principal de Bitwarden.

```
curl -s -o bitwarden.sh \
https://raw.githubusercontent.com/bitwarden/core/master/s
cripts/bitwarden.sh && sudo chmod u+x bitwarden.sh
```

2. Inicie el instalador:

```
./bitwarden.sh install
```

Nos pedirá:

- Dominio, si se deja vacío tomará “localhost”.
- ID y KEY de instalación (https://bitwarden.com/host).
- Si tenemos certificado SSL, si no, nos podrá generar uno.
- Usar puertos por defecto(80 y 443) y notificaciones push.

```
ubuntu@ubuntu-VirtualBox:~$ sudo ./bitwarden.sh install
 _     _ _                         _
| |__ (_) |___      ____ _ _ __ __| | ___ _ __
| '_ \| | __\ \ /\ / / _` | '__/ _` |/ _ \ '_ \
| |_) | | |_ \ V  V / (_| | | | (_| |  __/ | | |
|_.__/|_|\__| \_/\_/ \__,_|_|  \__,_|\___|_| |_|

Open source password management solutions
Copyright 2015-2018, 8bit Solutions LLC
https://bitwarden.com, https://github.com/bitwarden

=================================================

Docker version 18.03.1-ce, build 9ee9f40
docker-compose version 1.21.2, build a133471

(!) Enter the domain name for your Bitwarden instance (ex. bitwarden.company.com):
(!) Enter your installation id (get at https://bitwarden.com/host): 28f61f68[redacted]

(!) Enter your installation key: [redacted]

(!) Do you have a SSL certificate to use? (y/n): n

(!) Do you want to generate a self-signed SSL certificate? (y/n): y

Generating self signed SSL certificate.
Generating a 4096 bit RSA private key
......++
.....................................................++
writing new private key to '/bitwarden/ssl/self/localhost/private.key'
-----
Generating key for IdentityServer.
Generating a 4096 bit RSA private key
.....................................................................................
.......++
.....................................................................................++
writing new private key to 'identity.key'
(!) Do you want to use the default ports for HTTP (80) and HTTPS (443)? (y/n): y

(!) Is your installation behind a reverse proxy? (y/n): n

(!) Do you want to use push notifications? (y/n): n

Building nginx config.
Building docker environment files.
Building docker environment override files.
Building app settings.
Building FIDO U2F app id.
Building docker-compose.yml.

Setup complete

ubuntu@ubuntu-VirtualBox:~$
```

INICIAR BITWARDEN

Una vez que haya completado la instalación y configuración de su instalación de Bitwarden, puede iniciarla:

NOTA: La primera vez que inicie Bitwarden puede tomar algo de tiempo, ya que descarga todas las imágenes de Docker Hub.

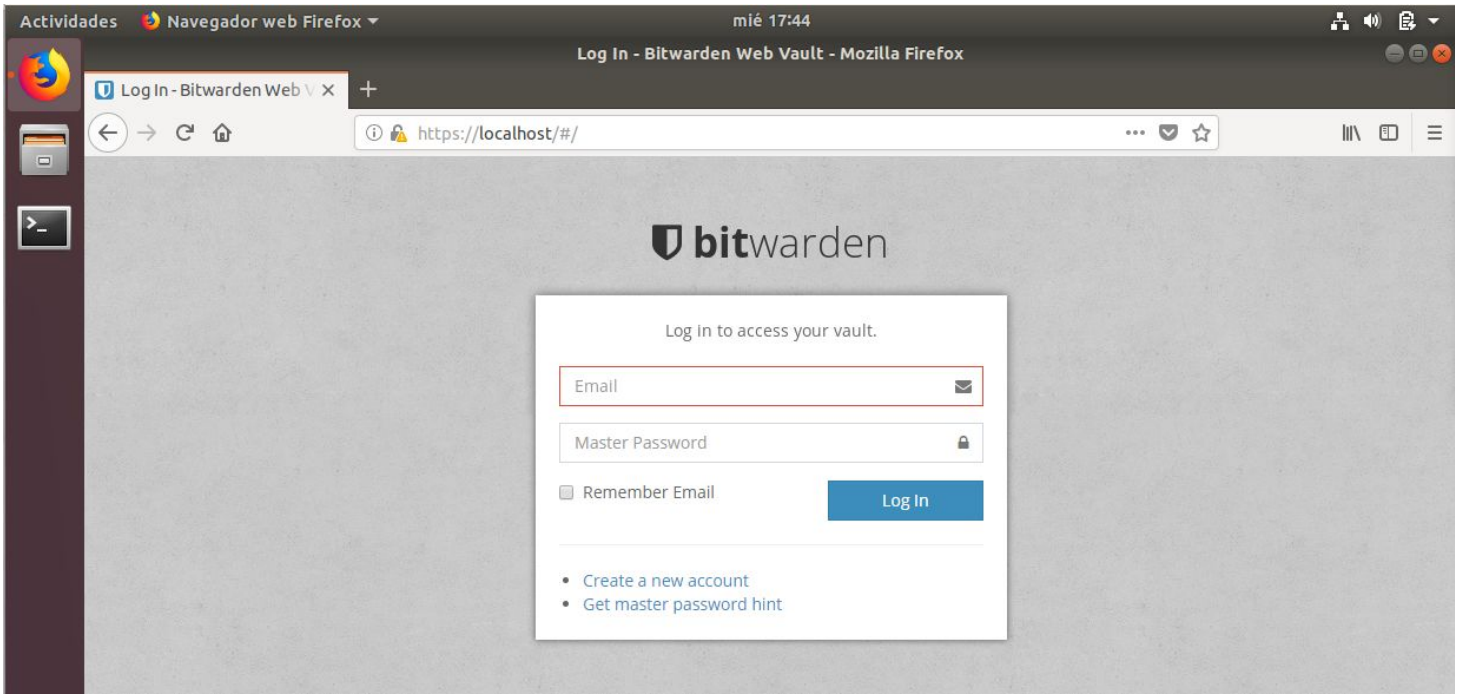
```
ubuntu@ubuntu-VirtualBox:~$ sudo ./bitwarden.sh start
 _     _ _                         _
| |__ (_) |___      ____ _ _ __ __| | ___ _ __
| '_ \| | __\ \ /\ / / _` | '__/ _` |/ _ \ '_ \
| |_) | | |_ \ V  V / (_| | | | (_| |  __/ | | |
|_.__/|_|\__| \_/\_/ \__,_|_|  \__,_|\___|_| |_|

Open source password management solutions
Copyright 2015-2018, 8bit Solutions LLC
https://bitwarden.com, https://github.com/bitwarden

=================================================

Docker version 18.03.1-ce, build 9ee9f40
docker-compose version 1.21.2, build a133471

Removing network docker_default
WARNING: Network docker_default not found.
Pulling mssql       ... done
Pulling web         ... done
Pulling attachments ... done
Pulling api         ... done
Pulling identity    ... done
Pulling admin       ... done
Pulling icons       ... done
Pulling nginx       ... done
Creating network "docker_default" with the default driver
Creating bitwarden-web         ... done
Creating bitwarden-api         ... done
Creating bitwarden-attachments ... done
Creating bitwarden-nginx       ... done
Creating bitwarden-mssql       ... done
Creating bitwarden-identity    ... done
Creating bitwarden-admin       ... done
Creating bitwarden-icons       ... done
Total reclaimed space: 0B
1.20.0: Pulling from bitwarden/setup
Digest: sha256:42c20f5c5aaf2ab90619ba41a100c7ac258ab412d439cbbf43185d573eadd35c
Status: Image is up to date for bitwarden/setup:1.20.0


Bitwarden is up and running!
=================================================

visit https://localhost
to update, run './bitwarden.sh updateself' and then './bitwarden.sh update'

ubuntu@ubuntu-VirtualBox:~$
```

Finalmente, necesitamos inicializar y actualizar la base de datos de Bitwarden:

```
ubuntu@ubuntu-VirtualBox:~$ sudo ./bitwarden.sh updatedb
 _     _ _                                  _
| |__ (_) |___      ____ _ _ __ __| | ___ _ __
| '_ \| | __\ \ /\ / / _` | '__/ _` |/ _ \ '_ \
| |_) | | |_ \ V  V / (_| | | | (_| |  __/ | | |
|_.__/|_|\__| \_/\_/ \__,_|_|  \__,_|\___|_| |_|

Open source password management solutions
Copyright 2015-2018, 8bit Solutions LLC
https://bitwarden.com, https://github.com/bitwarden

=================================================

Docker version 18.03.1-ce, build 9ee9f40
docker-compose version 1.21.2, build a133471

1.20.0: Pulling from bitwarden/setup
Digest: sha256:42c20f5c5aaf2ab90619ba41a100c7ac258ab412d439cbbf43185d573eadd35c
Status: Image is up to date for bitwarden/setup:1.20.0

Migrating database.
Beginning transaction
Beginning database upgrade
Fetching list of already executed scripts.
The [dbo].[Migration] table could not be found. The database is assumed to be at version 0.
Executing SQL Server script 'Bit.Setup.DbScripts.2017-08-19_00_InitialSetup.sql'
Creating the [dbo].[Migration] table
The [dbo].[Migration] table has been created
Executing SQL Server script 'Bit.Setup.DbScripts.2017-08-22_00_LicenseCheckScripts.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-08-30_00_CollectionWriteOnly.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-09-06_00_CipherDetails.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-09-08_00_OrgUserCounts.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-10-25_00_OrgUserUpdates.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-11-06_00_FamilyPlanAdjustments.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-11-13_00_IndexTuning.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-11-24_00_UpdateProcs.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2017-12-12_00_Events.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2018-02-28_00_LoginUris.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2018-03-12_00_FixLoginUris.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2018-03-21_00_AdminPortal.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2018-04-02_00_Org2fa.sql'
Executing SQL Server script 'Bit.Setup.DbScripts.2018-04-24_00_CipherQueryTuning.sql'
Upgrade successful
Migration successful.
Database update complete
ubuntu@ubuntu-VirtualBox:~$
```

Bitwarden ahora está funcionando en: *https://localhost*

Visite la bóveda web en su navegador para confirmarlo. Debemos registrar una nueva cuenta e iniciar sesión.



Preguntas Frecuentes

- *¿Puede el equipo de Bitwarden ver mis contraseñas?*

No.

Debido a que sus datos están totalmente encriptados y / o codificados antes de salir de su dispositivo local, nadie del equipo de Bitwarden puede ver, leer o realizar ingeniería inversa para acceder a sus datos reales. Los servidores de Bitwarden sólo almacenan datos cifrados y hash.

- *¿Cómo se transmiten y almacenan mis datos de manera segura en servidores Bitwarden?*

Bitwarden toma la seguridad muy en serio cuando se trata de manejar sus datos confidenciales. Sus datos nunca se envían a los servidores en la nube de Bitwarden sin encriptarse primero en su dispositivo local utilizando el cifrado AES de 256 bits. Puede leer más sobre el cifrado de Bitwarden aquí. Bitwarden nunca almacena datos significativos en sus servidores.

Cuando sus dispositivos se sincronizan con los servidores en la nube de Bitwarden, se descarga una copia de los datos encriptados y se almacena de manera segura en su dispositivo local. Cada vez que utilice las aplicaciones o extensiones de Bitwarden, sus datos se descifraran solo en la memoria, según sea necesario. Los datos nunca se almacenan en su forma descifrada en los servidores de Bitwarden remotos o en su dispositivo local.

Los servidores de Bitwarden se alojan y gestionan de forma segura en la nube de Microsoft Azure.

- *¿Qué encriptación se está utilizando?*

Bitwarden utiliza el cifrado AES de 256 bits y PBKDF2 para proteger sus datos.

AES es utilizado por el gobierno de los EE. UU. Y otras agencias gubernamentales de todo el mundo para la protección de datos secretos. Con la implementación adecuada y una fuerte clave de cifrado (su contraseña maestra), AES se considera irrompible.

PBKDF2 se utiliza para derivar la clave de cifrado de su contraseña maestra.

Bitwarden no escribe ningún código criptográfico. Bitwarden solo invoca criptografía de bibliotecas criptográficas populares y reputadas escritas y mantenidas por expertos en criptografía. Se usan las siguientes bibliotecas de cifrado:

- JavaScript (web, browser extension, desktop, and CLI vaults)
    - Forge
    - Web Crypto
    - Node.js Crypto
- C# (mobile vault)
    - CommonCrypto (iOS, Apple)
    - Javax.Crypto (Android, Oracle)
    - BouncyCastle (Android)

Bitwarden siempre cifra y / o mezcla sus datos en su dispositivo local antes de enviarlos a los servidores en la nube para su sincronización. Los servidores Bitwarden sólo se utilizan para almacenar datos cifrados. No es posible obtener los datos no encriptados de los servidores en la nube de Bitwarden.

- *¿Qué información es encriptada?*

Toda la información asociada con los datos almacenados de la bóveda está protegida con encriptación de extremo a extremo. Esto incluye:

- Folder names
- Collection names
- Item names
- Item notes
- Custom field names/values
- Login information
- Usernames
- Passwords
- URLs
- Authenticator keys (TOTP)
- Card information
- Cardholder names
- Numbers
- Brands
- Expirations
- Security codes
- Identity information
- Names
- Contact info (email, phone, etc)
- Password numbers
- License numbers
- SSNs
- Addresses
- Secure note information

- *¿Dónde están mis datos almacenados en la nube?*

Bitwarden procesa y almacena todos los datos de forma segura en la nube de Microsoft Azure utilizando servicios gestionados por el equipo de Microsoft. Bitwarden no administra ninguna infraestructura de servidor o seguridad directamente. Se realiza una copia de seguridad de todos los datos varias veces, utilizando nuevamente los servicios proporcionados por Microsoft Azure.

Referencias

A. https://bitwarden.com/
B. https://github.com/bitwarden/
C. https://help.bitwarden.com/article/install-on-premise/