Vaultwarden

Getting Started with Vaultwarden: The Ultimate Guide to Self-Hosted Password Management

In a world where digital security is paramount, managing and securing passwords efficiently is crucial. Vaultwarden (formerly known as Bitwarden_rs) offers a robust, self-hosted solution for password management. This article explores the features of Vaultwarden, provides Docker-Compose installation instructions, and guides you through the basic setup.

What is Vaultwarden?

Vaultwarden is an unofficial, open-source implementation of the Bitwarden password manager server. It is written in Rust and is designed to be lightweight and efficient, making it an ideal choice for self-hosting on resource-constrained devices such as Raspberry Pi.

Key Features of Vaultwarden

1. **Comprehensive Password Management**

- **Secure Storage**: Store and manage passwords, secure notes, credit card information, and identities in an encrypted vault.
- **End-to-End Encryption**: All data is encrypted locally before being sent to the server, ensuring that only you can decrypt and access it.

2. **Cross-Platform Compatibility**

- **Browser Extensions**: Available for major browsers like Chrome, Firefox, Safari, and Edge, enabling seamless password management across the web.
- **Mobile Apps**: Access your vault on the go with official Bitwarden mobile apps for iOS and Android.

- **Desktop Applications**: Native applications for Windows, macOS, and Linux.

3. **User Management and Sharing**

- **Organizations**: Create organizations to share vault items securely with team members or family.
- **User Roles and Permissions**: Assign roles and set permissions to control access within an organization.

4. **Two-Factor Authentication (2FA)**

- **2FA Support**: Enhance security with two-factor authentication, supporting TOTP, FIDO U2F, and Duo.
- **Authenticator Integration**: Generate and store TOTP codes within Vaultwarden, reducing the need for separate authenticator apps.

5. **Security and Compliance**

- **Audit Logs**: Keep detailed logs of all activities for security auditing and compliance.
- **Self-Hosting**: Full control over your data and infrastructure, reducing reliance on third-party services.

6. **API and Integration**

- **Bitwarden API Compatibility**: Fully compatible with the official Bitwarden API, allowing integration with various tools and services.
- **Webhooks**: Set up webhooks to trigger actions based on events in your Vaultwarden instance.

Installing Vaultwarden Using Docker-Compose

Deploying Vaultwarden with Docker-Compose simplifies the installation and management process. Follow these steps to get Vaultwarden up and running.

Step-by-Step Docker-Compose Installation

1. **Install Docker and Docker-Compose**
2. **Create a Docker-Compose File**
   Create a directory for your Vaultwarden setup and navigate to it. Create a `docker-compose.yml` file with the following content:

```
services:
  bitwarden:
    image: vaultwarden/server:latest
    container_name: vaultwarden
    restart: always
    ports:
      - ${HTTP_PORT}:80
    volumes:
      - ${DOCKER}/bitwarden/bw-data:/data
    environment:
      - PUID=${PUID}
      - PGID=${PGID}
      - TZ=${TZ}
      - WEBSOCKET_ENABLED='true' # Required to use websockets
      - SIGNUPS_ALLOWED='true'   # set to false to disable signups
```

3. **Start Vaultwarden**
   Open a terminal, navigate to the directory containing the `docker-compose.yml` file, and run the following command:

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

   This command will pull the Vaultwarden Docker image and start the container in detached mode.
4. **Access the Vaultwarden Web UI**
   Open your web browser and navigate to `http://localhost` to access the Vaultwarden web interface.

Basic Setup Instructions

Once Vaultwarden is running, follow these steps to configure your password manager.

Step 1: Register Your Account

- Access the Vaultwarden web UI at `http://localhost`.
- Click on **"Create Account"** and fill in your details to create a new account.

Step 2: Admin Panel Access

- Access the admin panel by navigating to `http://localhost/admin` and entering the admin token set in the Docker-Compose file.
- Use the admin panel to manage users, organizations, and other advanced settings.

Step 3: Set Up Two-Factor Authentication (2FA)

- Log in to your Vaultwarden account.
- Navigate to **"Settings"** > **"Two-step Login"** and set up your preferred 2FA method.

Useful Links

- Vaultwarden GitHub Repository – Explore the source code and contribute to the project.
- Vaultwarden Documentation – Access detailed setup guides and documentation.
- Bitwarden Official Site – Learn more about Bitwarden and its official applications.

Conclusion

Vaultwarden provides a secure, efficient, and flexible solution for self-hosted password management. Its comprehensive features, including cross-platform compatibility, robust security measures, and easy deployment with Docker-Compose, make it an excellent choice for individuals and organizations looking to maintain control over their digital security. By following the installation and setup instructions, you can quickly deploy Vaultwarden and start managing your passwords securely and efficiently.

Revision #4
Created 2024-07-01 06:57:17 UTC by thesabear
Updated 2024-09-17 18:30:41 UTC by thesabear