bitwarden | Article du Centre d'Aide

SELF-HOSTING

Kerberos Integration

Afficher dans le centre d'aide:
https://bitwarden.com/help/kerberos-integration/

Kerberos Integration

Kerberos integrated authentication allows Bitwarden users to use integrated AD authentication with external MSSQL databases.

> **Note**
> This guide assumes that you have already exported the required keytab file that will be used on the Bitwarden server to authenticate to the domain.

Keytab File

An exported `keytab` file is used by the Bitwarden server to authenticate the domain.

1. From the Windows Domain controller, enter the following code example (this may vary depending on your requirements):

```
Plain Text

ktpass /princ bitwarden@<EXAMPLE.DOMAIN> /mapuser "bitwarden" /pass super_secure_password_here /
out bitwarden.keytab /crypto all /ptype KRB5_NT_PRINCIPAL /mapop set
```

2. Once the file has been generated, copy the file to the Bitwarden server location in the next section.

Bitwarden Configuration

Next, create the Bitwarden configuration:

1. Create the Kerberos directory:

```
Plain Text

mkdir /opt/bitwarden/bwdata/kerberos
```

2. Place the two files in this directory
    1. The `keytab` file generated in the previous section
    2. the `krb5.conf` file (example below)
3. Create the `krb5.conf` file:

```
Plain Text

nano /opt/bitwarden/bwdata/kerberos/krb5.conf
```

Here is an example file.
Here is example TEST file.

Check that these values match your own and that the `kdc` and `admin_server` are accessible from the Bitwarden server.

> **Note**
> The ticket lifetime and renewal values are set in the `krb5.config` file using the `ticket_lifetime` and `renew_lifetime` variables. If both the ticket lifetime and ticket renewal expire, you will be unable to re-authenticate the ticket. For additional information, see the Kerberos documentation.

Update Bitwarden

global.override.env

In order to update Bitwarden, an additional environment variable will have to be added to the `global.override.env` file.

1. Access `global.override.env`:

```
Plain Text

nano ~/global.override.env/
```

2. Add the following variable to `global.override.env`:

```
Plain Text

globalSettings__kerberosUser=bitwarden
```

> **Note**
> This variable should be the AD user used to authenticate with the domain, and should match your domain user.

SQL connection string

Replace the SQL connection string to point to the external DB and use the integrated authentication. Change your SQL server `hostname` and `database` name:

```
Plain Text

globalSettings__sqlServer__connectionString="Data Source=tcp:example-sql-server.example.domain,1433;Initial Catalog=vault;Persist Security Info=False;Integrated Security=true;Multiple Active Result Sets=False;Connect Timeout=30;Encrypt=True;Trust Server Certificate=True"
```

Docker updates

Once the previous setup steps have been completed, the configuration file should exist on your host OS. Next, modify Bitwarden's Docker Compose configuration to add an additional volume mount to the relevant containers. This will ensure that the configuration is retained, following updates and changes to the main docker-compose file. Compose provides an `override` file that will merge your local changes to the standard Bitwarden configuration.

1. Create the override file:

```
Plain Text

nano /opt/bitwarden/bwdata/docker/docker-compose.override.yml
```

2. Include the following contents for a standard configuration:

```
Plain Text

services:
    admin:
        volumes:
            - ../kerberos:/etc/bitwarden/kerberos
    sso:
        volumes:
            - ../kerberos:/etc/bitwarden/kerberos
    identity:
        volumes:
            - ../kerberos:/etc/bitwarden/kerberos
    api:
        volumes:
            - ../kerberos:/etc/bitwarden/kerberos
    events:
        volumes:
            - ../kerberos:/etc/bitwarden/kerberos
```

3. If using SCIM, you will also have to include:

```
Plain Text

    scim:
        volumes:
            - ../kerberos:/etc/bitwarden/kerberos
```

4. Once completed, save the file.

Starting Bitwarden

Once setup has been completed, you may start Bitwarden. Restart the Bitwarden containers following the setup if you have not yet:

```
Plain Text

./bitwarden restart
```

The `admin` container will populate your new external MSSQL database. If you stored any information in the built-in `mssql` container, you will be required to migrate it to the new external database, with either databse backup and restore, or export/import.