

# Server Installation

Die Installation des Netbird Servers, über diesen können die Clients ihre Einstellungen beziehen und miteinander verbunden werden. Dieser muss als einziger Teilnehmer öffentlich erreichbar und auf einer festen Domäne sein.

Im folgenden wird die Anleitung der offiziellen Dokumentation von Netbird verwendet: [Netbird Advanced Guide](#)

## Code von GitHub laden

Bevor der Code heruntergeladen wird, empfiehlt es sich einen Ordner zu wählen, in dem später die Konfigurationsdateien und Daten gespeichert werden sollen. Anschließend in das Verzeichnis wechseln.

```
mkdir /pfad/zu/netbird
cd /pfad/zu/netbird
```

Dann laden wir uns Netbird samt Konfiguration von GitHub.

```
#!/bin/bash
# Die URL des Repositorys in einer Variable speichern
REPO="https://github.com/netbirdio/netbird/"
# Hiermit wird die neuste Version (latest) ermittelt und als Variable gesetzt
LATEST_TAG=$(basename $(curl -fs -o/dev/null -w %{redirect_url} ${REPO}releases/latest))
# Die Version ausgeben
echo $LATEST_TAG
# Das Repository von GitHub herunterladen
git clone --depth 1 --branch $LATEST_TAG $REPO
```

Es werden nicht alle heruntergeladenen Daten benötigt, also schieben wir uns die benötigten Dateien direkt passend ins Verzeichnis und löschen den Rest.

```
mv netbird/infrastructure_files/* .
rm -r netbird/
```

## Identitätsanbieter konfigurieren

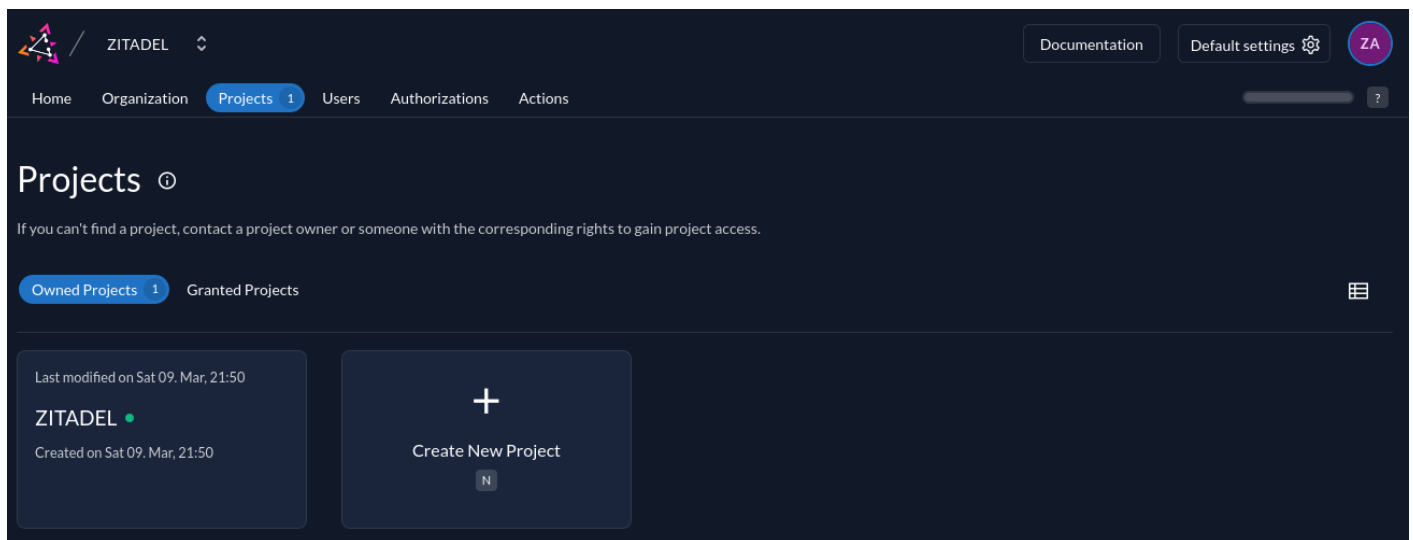
Der Identitätsanbieter kümmert sich um die Authentifizierung und Autorisierung der Benutzer. Hier setzt Netbird auf bereits etablierte Anbieter, die OpenSource und kostenlos für Self-Hosting zur Verfügung stehen. In diesem Fall wird Zitadel gewählt.

Anstelle von Zitadel könnten auch Keycloak oder Authentik verwendet werden. Alle 3 werden offiziell von Netbird unterstützt. Siehe hierzu: [Identity Providers](#)

Im folgenden wird davon ausgegangen, dass Zitadel bereits eingerichtet wurde und ausgeführt wird.

Eine Anleitung, wie Zitadel mit Docker bereitgestellt werden kann ist hier: [Buch Zitadel](#)

Zunächst wird ein neues Projekt erstellt. In der oberen Menüleiste auf *Projects* klicken und dann auf *Create New Project*.



Es wird nur ein Name für das Projekt abgefragt, hier z. B. Netbird eingeben, es kann selbst ein passender Name eingegeben werden. Nachdem der Name bestätigt wurde, erstellt Zitadel das Projekt und leitet direkt zu diesem weiter. Die Seite sieht in etwa wie folgt aus.

The screenshot shows the Netbird web interface. At the top, there's a navigation bar with 'ZITADEL' and 'Netbird' logos, and links for 'Documentation', 'Default settings', and a user profile 'ZA'. Below this is a secondary navigation bar with 'Home', 'Organization', 'Projects 2', 'Users', 'Authorizations', and 'Actions'. The main header area displays 'Netbird' and 'Owned Project' with an 'Actions' dropdown and a '+ ZA' button. A status bar shows 'Status: Active', 'Resource Id: 257705797541167118', 'Created on: 10. March 2024, 20:57', and 'Last modified on: 10. March 2024, 20:57'. The main content area is divided into three sections: 'General' (with links for Roles, Grants, and Authorizations), 'APPLICATIONS' (featuring a large blue '+ New' button), and 'LAST CHANGES' (showing a log of events for 10. Mar 2024, including 'Project member added' and 'Project added'). A 'Load more' button is present below the log. A 'SETTINGS' dialog box is open, showing a 'Branding Setting' as 'Unspecified' with an edit icon. It contains two checkboxes: 'Assert Roles on Authentication' and 'Check authorization on Authentication'. A tooltip for the first checkbox states: 'Role information is sent from Userinfo endpoint and depending on your application settings in tokens and other types.'

Hier wird nun unter *Applications* auf *New* geklickt, um eine neue Applikation anzulegen. Nun öffnet sich ein Dialog, um die Applikation zu erstellen. Als erstes wird ein Name vergeben und der Typ ausgewählt. Der Name kann frei gewählt werden und der Typ ist auf *User Agent* festzulegen. Die Konfiguration mit *Continue* bestätigen.

 / ZITADEL / 

Documentation

Default settings 

ZA

×

 CREATE APPLICATION 

Step 1 of 4

Enter Your Application Details Step by Step

Home Organization **Projects 2** Users Authorizations Actions

1

2

3

4

Name and Type Authentication Method Redirect URIs Overview

NAME OF THE APPLICATION

Name

Netbird

TYPE OF APPLICATION

WEB

Web

Regular Web applications like .net, PHP, Node.js, Java, etc.

OIDC

N

Native

Mobile Apps, Desktop, Smart Devices, etc.

OIDC

UA

User Agent

Single Page Applications (SPA) and in general all JS frameworks executed in browsers

OIDC

API

API

APIs in general

OIDC

SAML

SAML

SAML Applications

SAML

Continue

Danach wird der Typ noch spezifiziert, hier wird *PKCE* ausgewählt und wieder mit *Continue* bestätigt.

**ZITADEL** / Documentation / Default settings / ZA

Home Organization **Projects 2** Users Authorizations Actions

✕ CREATE APPLICATION Step 2 of 4

### Enter Your Application Details Step by Step

☐ I'm a pro. Skip this wizard.

1 ✓ Name and Type      2 Authentication Method      3 Redirect URIs      4 Overview

#### PKCE

PKCE

Use a random hash instead of a static client secret for more security

|                       |                    |
|-----------------------|--------------------|
| Response Types        | Code               |
| Grant Types           | Authorization Code |
| Authentication Method | None               |

recommended

#### IMP

Implicit

Get the tokens directly from the authorization endpoint

|                       |          |
|-----------------------|----------|
| Response Types        | ID Token |
| Grant Types           | Implicit |
| Authentication Method | None     |

not recommended

Back Continue

Im nächsten Dialog sind die Weiterleitungs-Adressen sowie die Logout-Adresse anzugeben.

Unter dem Punkt *Specify the URIs where the login will redirect to.* sind die folgenden beiden Adressen einzugeben (die Domäne durch die eigene ersetzen, Eingabe durch Klick auf das Pluszeichen bestätigen):

- <https://beispiel.de/auth>
- <https://beispiel.de/silent-auth>

Unter dem Punkt *This is the redirect URI after logout.* ist die folgende Adresse zu hinterlegen:

- <https://beispiel.de/>

ZITADEL

Documentation Default settings ZA

CREATE APPLICATION Step 3 of 4

Home Organization Projects 2 Users Authorizations Actions

Enter Your Application Details Step by Step

☐ I'm a pro. Skip this wizard.

1 Name and Type 2 Authentication Method 3 Redirect URIs 4 Overview

SPECIFY THE URIS WHERE THE LOGIN WILL REDIRECT TO.

☐ Development Mode

Redirect URIs

ex. <https://>

<https://beispiel.de/auth>

<https://beispiel.de/silent-auth>

THIS IS THE REDIRECT URI AFTER LOGOUT.

Redirect URIs must begin with <https://>. <http://> is only valid with enabled development mode.

Post Logout URIs

ex. <https://>

<https://beispiel.de/>

Back Continue

Abschließend wird die gesamte Konfiguration nochmal angezeigt. Diese gilt es zu bestätigen und danach ist die App eingerichtet. Das nun erzeugt, nur einmalig angezeigt Secret muss nicht gespeichert werden. Das Fenster kann einfach mit *Close* geschlossen werden.

Nun erscheint noch die OIDC Konfiguration. Bei dieser müssen unter *Grant Types* die folgenden Optionen angehakt werden:

- Authorization Code
- Device Code
- Refresh Token

Nachdem das ganze mit *Save* bestätigt wird, am besten direkt die *Client ID* kopieren, da sie später noch benötigt wird.

Navigation: ZITADEL / Netbird. Documentation, Default settings, ZA profile. Home, Organization, Projects 2, Users, Authorizations, Actions.

# Netbird

User Agent ⓘ Actions ▾

|        |                    |                       |                       |                            |
|--------|--------------------|-----------------------|-----------------------|----------------------------|
| Status | ID                 | Created               | Changed               | Client Id                  |
| Active | 257707395671654414 | 10. March 2024, 21:12 | 10. March 2024, 21:12 | 257707395671719950@netbird |

To configure roles, authorizations and more, navigate to the project. [Configure](#)

### Configuration

- Token Settings
- Redirect Settings
- Additional Origins
- URLs

### OIDC CONFIGURATION

**Custom** Your setting doesn't correspond to any other option. ✎

|                       |                             |                                                   |
|-----------------------|-----------------------------|---------------------------------------------------|
| Client ID             | Application Type            | Response Types                                    |
| 257707395671719950@r  | User Agent ▾                | Code ▾                                            |
| Authentication Method | Grant Types                 | <input checked="" type="checkbox"/> Refresh Token |
| None ▾                | Authorization Code, De... ▾ |                                                   |

☒ Authorization Code  
☐ Implicit  
☒ Device Code  
☒ Refresh Token

[Save](#)

### LAST CHANGES

10. Mar 2024

- ZA** OIDC Configuration added 21:12
- Application added 21:12

[Load more](#)

Im selben Fenster wird nun links in der Menüleiste auf *Token Settings* geklickt. Hier wird nun zuerst der *Auth Token Type* auf *JWT* geändert. Außerdem wird die Checkbos bei *Add user roles to the access token* angehakt. Die Einstellung wird mit *Save* gespeichert.

Configuration

Token Settings

Redirect Settings

Additional Origins

URLs

AUTHTOKEN OPTIONS

Auth Token Type

JWT

☒ Add user roles to the access token

If selected, the requested roles of the authenticated user are added to the access token.

☐ User roles inside ID Token

If selected, the requested roles of the authenticated user are added to the ID token.

☐ User Info inside ID Token

Enables clients to retrieve profile, email, phone and address claims from ID token.

ClockSkew

Enables clients to handle clock skew of OP and client. The duration (0-5s) will be added to exp claim and subtracted from iats, auth\_time and nbf.

Save

LAST CHANGES

10. Mar 2024

ZA

OIDC Configuration added  
21:12

Application added  
21:12

Load more

Nachdem Projekt und App konfiguriert sind, wird ein Dienstbenutzer für Netbird angelegt. Hierzu in der oberen Menüleiste *Users* auswählen, dann auf *Service Users* wechseln und auf *New* klicken. Durch die Auswahl der *Service Users* müssen z. B. keine Daten wie E-Mail oder Tel. eingegeben werden, da diese bei Dienstbenutzern nicht benötigt werden.

ZITADEL

Documentation

Default settings

ZA

Home

Organization

Projects

Users

Authorizations

Actions

Users

Create new users in your organization and manage existing ones.

Users

Service Users

Filter

+ New

|            | DISPLAY NAME | USER NAME | CREATED AT | LAST MODIFIED | STATUS |
|------------|--------------|-----------|------------|---------------|--------|
| No entries |              |           |            |               |        |

0 Total Results

Sunday 10. Mar 2024, 21:28

0 - 20

20

Die Felder können beliebig ausgefüllt werden, nur der *Access Token Type* muss auf *JWT* festgelegt werden.

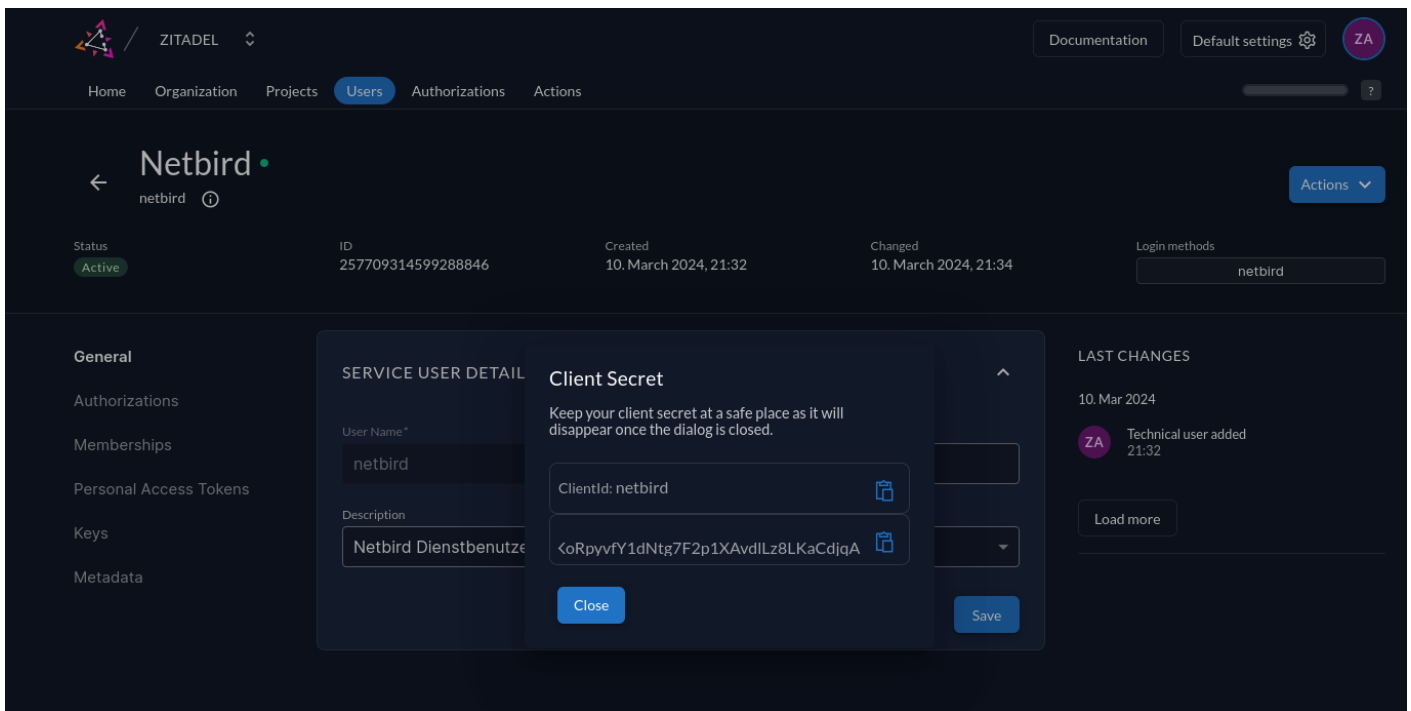
The screenshot shows the 'CREATE A NEW USER' form in the ZITADEL interface. The form has a dark blue background with white text and input fields. At the top, there is a navigation bar with links: Home, Organization, Projects, Users (highlighted), Authorizations, and Actions. Below the navigation bar, there is a close button (X) and the title 'CREATE A NEW USER'. The form contains four input fields: 'User Name\*' with the value 'netbird', 'Name\*' with the value 'Netbird', 'Description' with the value 'Netbird Dienstbenutzer', and 'Access Token Type\*' with a dropdown menu showing 'JWT'. At the bottom left, there is a blue 'Create' button.

Nach einem Klick auf *Create* wird der Benutzer erstellt und geöffnet. In diesem Menü wird nun rechts oben unter *Actions* auf *Generate Client Secret* geklickt.

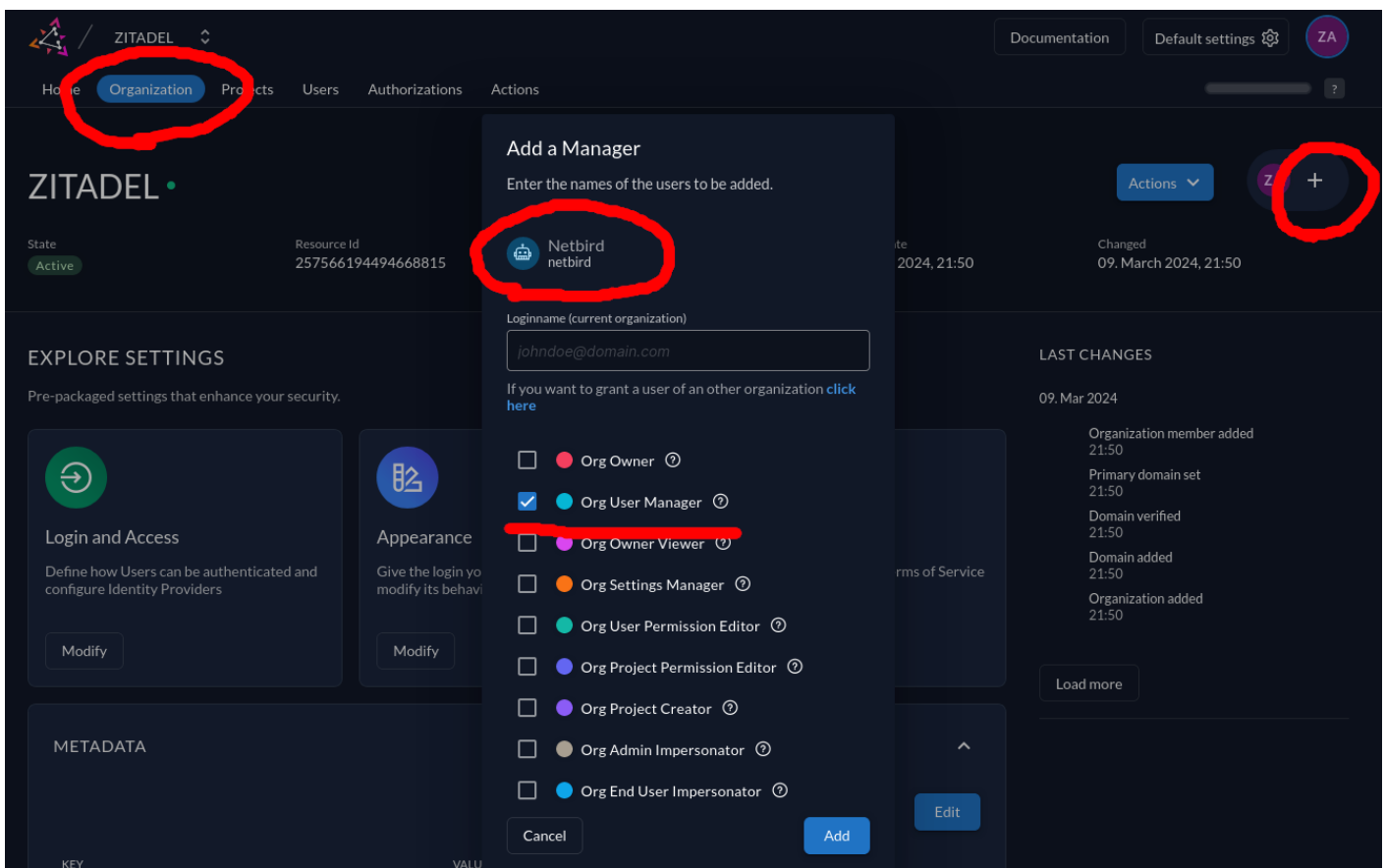
The screenshot shows the ZITADEL user management interface. At the top, there is a navigation bar with links: Home, Organization, Projects, Users (highlighted), Authorizations, and Actions. Below the navigation bar, there is a close button (X) and the title 'CREATE A NEW USER'. The form contains four input fields: 'User Name\*' with the value 'netbird', 'Name\*' with the value 'Netbird', 'Description' with the value 'Netbird Dienstbenutzer', and 'Access Token Type\*' with a dropdown menu showing 'JWT'. At the bottom left, there is a blue 'Create' button.

The screenshot shows the ZITADEL user management interface. At the top, there is a navigation bar with links: Home, Organization, Projects, Users (highlighted), Authorizations, and Actions. Below the navigation bar, there is a close button (X) and the title 'CREATE A NEW USER'. The form contains four input fields: 'User Name\*' with the value 'netbird', 'Name\*' with the value 'Netbird', 'Description' with the value 'Netbird Dienstbenutzer', and 'Access Token Type\*' with a dropdown menu showing 'JWT'. At the bottom left, there is a blue 'Create' button.

Daraufhin wird das *Client Secret* erzeugt und angezeigt. Dieses lässt sich später nie wieder anzeigen, als muss es sicher gespeichert werden. Es kann zwar jederzeit neu erzeugt werden, jedoch wird dadurch das vorherige Client Secret automatisch gelöscht.



Zum Schluss muss dem Dienstbenutzer nur noch die Rolle zum Verwalten von Benutzern zugewiesen werden. Dazu oben in der Menüleiste auf *Organizations* klicken, dann auf das Pluszeichen rechts oben neben *Actions*. Nun in das Suchfeld den Namen des Dienstbenutzers eingeben und diesen auswählen. Anschließend die Rolle *Org User Manager* zuweisen und das ganze mit *Add* bestätigen.



Konfigurationsdateien vorbereiten

Im nächsten Schritt werden die Konfigurationsdateien angepasst. Hier werden die Einstellungen für unsere Umgebung gesetzt.

Bei dieser Installation wird davon ausgegangen, dass bereits ein Reverse Proxy eingesetzt wird, sodass der Port 443 nicht verfügbar ist und stattdessen der Reverse Proxy sowie Netbird entsprechend konfiguriert werden müssen. Darauf geht die Anleitung später noch ein.

Die Datei `setup.env` definiert die Parameter, mit welchem später das Setup konfiguriert wird. Hierfür hat Netbird eine kommentierte Vorlage bereitgestellt, die im aktuellen Ordner liegt: `setup.env.example`

Am besten wird die einfach umbenannt und dann angepasst.

```
mv setup.env.example setup.env
# Optional: Direkt im Terminal im Texteditor nano öffnen:
nano docker-compose.yml.tpl
```

Für die Zitadel Konfiguration sind die folgenden Parameter in der `setup.env` anzupassen.

```
NETBIRD_AUTH_OIDC_CONFIGURATION_ENDPOINT="https://zitadel.beispiel.de/.well-known/openid-configuration"
NETBIRD_USE_AUTH0=false
NETBIRD_AUTH_CLIENT_ID="<CLIENT_ID>"
NETBIRD_AUTH_SUPPORTED_SCOPES="openid profile email offline_access api"
NETBIRD_AUTH_AUDIENCE="<CLIENT_ID>"
NETBIRD_AUTH_REDIRECT_URI="/auth"
NETBIRD_AUTH_SILENT_REDIRECT_URI="/silent-auth"

NETBIRD_AUTH_DEVICE_AUTH_PROVIDER="hosted"
NETBIRD_AUTH_DEVICE_AUTH_CLIENT_ID="<CLIENT_ID>"
NETBIRD_AUTH_DEVICE_AUTH_AUDIENCE="<CLIENT_ID>"

NETBIRD_MGMT_IDP="zitadel"
NETBIRD_IDP_MGMT_CLIENT_ID="netbird"
NETBIRD_IDP_MGMT_CLIENT_SECRET="<CLIENT_SECRET>"
NETBIRD_IDP_MGMT_EXTRA_MANAGEMENT_ENDPOINT="https://zitadel.beispiel.de/management/v1"
NETBIRD_MGMT_IDP_SIGNKEY_REFRESH=true
```

Konfigurationskript ausführen

Nachdem nun die Konfigurationsdateien vorbereitet wurden, muss noch das Skript ausgeführt werden, welches auf Basis der Konfigurationsdatei die eigentlichen Modifikationen vornimmt.

```
# Für das Skript wird jq benötigt, dieses ggf. mit folgendem Befehl nachinstallieren
sudo apt -y install jq
# Das eigentliche Skript ausführen
./configure.sh
```

Nach der Ausführung des Skripts wird ein neuer Ordner *artifacts* erstellt, in welchem alle notwendigen Konfigurationen abgelegt wurden. Einfach in diesen Ordner wechseln und die Docker Compose Konfiguration mit `sudo docker compose up -d` ausführen.

---

Version #4

Erstellt: 2024-03-07 21:17:22 CET von Marcel

Zuletzt aktualisiert: 2024-03-25 19:21:49 CET von Marcel