Contao Konferenz 2023

SSH-Keys

zum Server verbinden ohne Passwörter

SSH-Keys zum Server verbinden ohne Passwörter

Täglich verbinden wir uns mehrfach mit einem Server, um an einer Contao-Instanz zu arbeiten. Das, was uns dann immer als erstes "begrüßt", ist ein Login mit Benutzername und Passwort. Dieses soll(te) natürlich nicht zu einfach gewählt sein und auch nicht mehrfach verwendet werden. Wir müssen uns daher komplizierte und kryptische Passwörter merken oder immer neu aus dem Passwortmanager einkopieren. Das ist aufwändig und fehleranfällig. Der Vortrag gibt auch dazu Einblicke in die Arbeit bei trilobit, die auch als Denkanstöße oder Best Practices für andere dienen können.

Das habe ich heute vor

- Wer bin ich / trilobit GmbH
- Vorüberlegungen, Herausforderungen, Probleme
- Vorteile? (unsere) Ziele
- (unser) Weg
- auf dem Server
- neuer Weg
- SSH-Keys
- SSH-Config
- Vorteile! (unsere) Ziele
- The *trilobit* way of work

Wer bin ich?
trilobit GmbH

In eigener Sache

Wer bin ich / trilobit GmbH

- Peter Adelmann

- Erweiterungsentwicklung und Individual-Programmierung
- Aus dem Südwesten der Republik
- Familienvater & Coffeeholic

- Seit 2002 bei trilobit und damit ein Urgestein der Firma
- Ersten Schritte in Perl bevor es dann ab ~ 2010 mit TypoLight bzw Contao weiterging

trilobit
VIEL MEHR ALS INTERNET

Vorüberlegungen, Herausforderungen, Probleme

Vorüberlegungen, Herausforderungen, Probleme

- Wie verbinde ich mich aktuell mit einem Server?
- Mehrere Kunden
- Verschiedene Server/Quota/Projekte
- Projekt-Teams
- Sichere Passwörter
- Neue und ausscheidende Mitarbeitende


Vorteile?
(unsere)
Ziele

...das möchten wir erreichen...

- → Sichere Authentifizierung
- → Schutz vor Brute-Force-Angriffen
- → Verschlüsselte Kommunikation
- → Bequeme und sichere Anmeldung
- → Schnelle(re) Anmeldung

- Einfaches Management von Server-Logins → The *trilobit* way of work


(unser)
Weg /
IST-Stand

...bevor es los geht...

IST / SOLL Abgleich

- Welche Werkzeuge, Ressourcen stehen zur Verfügung?
- Welches Know-How steht zur Verfügung?
- Mit welchen Hosting-Paketen habe ich es zu tun?
- Welche Features stehen dort zur Verfügung?
- ... und meine Punkte aus ...
  - Vorüberlegungen, Herausforderungen und Probleme
  - Ziele


auf dem Server

auf dem Server

Verschiedene Möglichkeiten, auf dem Server zu arbeiten

1. Aus meiner Sicht nicht praktikabel
    - Contao: über die Dateiverwaltung und Templates
    - Dateizugriff über das Admin-Panel des Servers und/oder Hosting-Paketen
2. Besser
    - FTP - File Transfer Protocol
3. The *trilobit* way of work
    - SSH - Secure Shell

Was ist FTP?

zu 2. FTP - File Transfer Protocol

- FTP ist ein Netzwerkprotokoll zur Übertragung von Dateien
- 1985 spezifiziert
- Client ↗ Server ↘ Client
- Verzeichnisse und Dateien anlegen, umbenennen oder löschen

Was ist SSH?

zu 3. SSH - Secure Shell

- Kryptografisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten
- 1995 entwickelt (SSH-1)
- Lokal eine entfernte Kommandozeile verfügbar machen
- Sichere Remote-Verwaltung von Servern
- 1996 überarbeitete Version (SSH-2)
- Funktionen wie Datenübertragung per SFTP (SSH-2)


neuer Weg ♡♥

Arbeitsweisen

Die Merkmale von SSH bieten uns die Vorteile, die wir beim Arbeiten auf dem Server nicht missen möchten.

- Vorteile von SSH
  - "normales" Arbeiten auf dem Server
- Herausforderungen, Probleme
  - Zugangsdaten zum Server werden benötigt
  - SSH Client wird benötigt
- Lösung
  - Zum Server verbinden ohne Passwörter
  - Stichwort → SSH-Keys


SSH-Keys

Was sind SSH-Keys?

- Sicherheitsmechanismus für die Authentifizierung bei SSH-Verbindungen
- SSH-Keys bestehen aus einem Paar von kryptografischen Schlüsseln
  - Privater Schlüssel
  - Öffentlicher Schlüssel
- Privater Schlüssel
  - Geheim
  - Auf Client gespeichert
- Öffentlicher Schlüssel
  - Auf Server gespeichert

Authentifizierung

- Beim Verbinden mit einem Server überprüft dieser, ob der Client-Key gültig ist
- Passen privater und öffentlicher Schlüssel zusammen, wird ein Zugriff ohne Passwort gewährt

SSH-Keys

Schlüsselpaar erzeugen

```
ssh-keygen -a 100 -t ed25519
```

- Dadurch wird in diesem Beispiel ein Schlüssel nach dem Ed25519-Standard erstellt
- Das Schlüsselpaar wird (unter Linux) in der Regel im Ordner `~/.ssh` abgelegt

SSH-Keys

Ein paar Optionen...

- `-b` bits → Anzahl der Bits im zu erstellenden Schlüssel; Standardlänge beträgt 3072 Bit (RSA) oder 256 Bit (ECDSA)
- `-C` comment → benutzerdefinierten Schlüsselkommentar, der am Ende des öffentlichen Schlüssels angehängt wird
- `-p` Änderung der Passphrase einer privaten Schlüsseldatei anstatt einen neuen privaten Schlüssel zu erstellen
- `-t` Typ des zu erstellenden Schlüssels (z. B. RSA)

https://en.wikipedia.org/wiki/Ssh-keygen

https://man7.org/linux/man-pages/man1/ssh-keygen.1.html

SSH-Keys

Ausgabe Console

```
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/trilobit/.ssh/id_ed25519): mySshKeyName
Enter passphrase (empty for no passphrase): mySecret***
Enter same passphrase again: mySecret***
Your identification has been saved in /home/trilobit/.ssh/id_ed25519
Your public key has been saved in /home/trilobit/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:2qvAJzJZBoOLtXyYG/gQzdQGeNMc9T1O0vUVtpeNBoY trilobit@trilobit-HP-Z210-Workstat
The key's randomart image is:
+--[ED25519 256]--+
| .o=.o.    .+  oo|
|.=o =  . oEo o.o+|
|o.*o    o =   +oo|
|.* *     + . .  .|
|= * +   S .      |
| o O   o         |
|  * + o .        |
```

SSH-Keys

Ablage

```
~/.ssh/id_ed25519
~/.ssh/id_ed25519.pub
```

- Die Dateiablage des generierten Schlüsselpaars sieht wie folgt aus (Bspl)
- Die Datei `id_ed25519.pub` ist dabei der öffentliche Schlüssel

SSH-Keys

öffentlichen Schlüssel verteilen

```
ssh-copy-id -i ~/path/to/the/public/keyfile ssh-user@my-server.tld
```

oder

```
cat ~/path/to/the/public/keyfile | ssh-user@my-server.tld ↲
"mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

- An dieser Stelle wird jetzt einmalig das Passwort zum SSH-Benutzer benötigt

SSH-Keys

öffentlichen Schlüssel verteilen

Alternativ kann der öffentliche Schlüssel auch manuell auf den Server kopiert werden.

- Auf dem Server einloggen
- in das Verzeichnis `.ssh/` wechseln
- Mit einem Editor die Datei `authorized_keys` zum Bearbeiten öffnen
- Öffentlicher Schlüssel ergänzen

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKosxNXHui6Fh72ywhdk8DhMkMt3RTYx6zxHL/BGc410 tri
```

SSH-Keys

...einloggen...

Danach kann der passwortfreie Zugang zum Server getestet werden.

```
ssh -i ~/path/to/the/public/keyfile ssh-user@my-server.tld
```


A 54 Northwich, Chester
Middlewich, Holmes Chapel
NORTH WALES, Preston,
Manchester, Leeds
M6
18

SSH-Config

SSH-Config

- Das Login auf einen Server kann → muss noch einfacher werden
- Hierzu wird eine SSH-Config `~/.ssh/config` benötigt

```
mkdir -p ~/.ssh && chmod 700 ~/.ssh

touch ~/.ssh/config

chmod 600 ~/.ssh/config
```

SSH-Config

Konfiguration

```
Host nameForServerConnection
    HostName my-server.tld
    Port 22
    User ssh-user
    IdentityFile ~/path/to/the/private/keyfile
    IdentitiesOnly yes
```

Danach kann der vereinfachte Zugang zum Server getestet werden.

```
ssh nameForServerConnection
```


Vorteile!
(unsere)
Ziele

...das haben ♡♥ wir erreicht...

- ✓ Sichere Authentifizierung
- ✓ Schutz vor Brute-Force-Angriffen
- ✓ Verschlüsselte Kommunikation
- ✓ Bequeme und sichere Anmeldung
- ✓ Schnellere Anmeldung

- Einfaches Management von Server-Logins → The *trilobit* way of work


The
trilobit way of work

The *trilobit* way of work

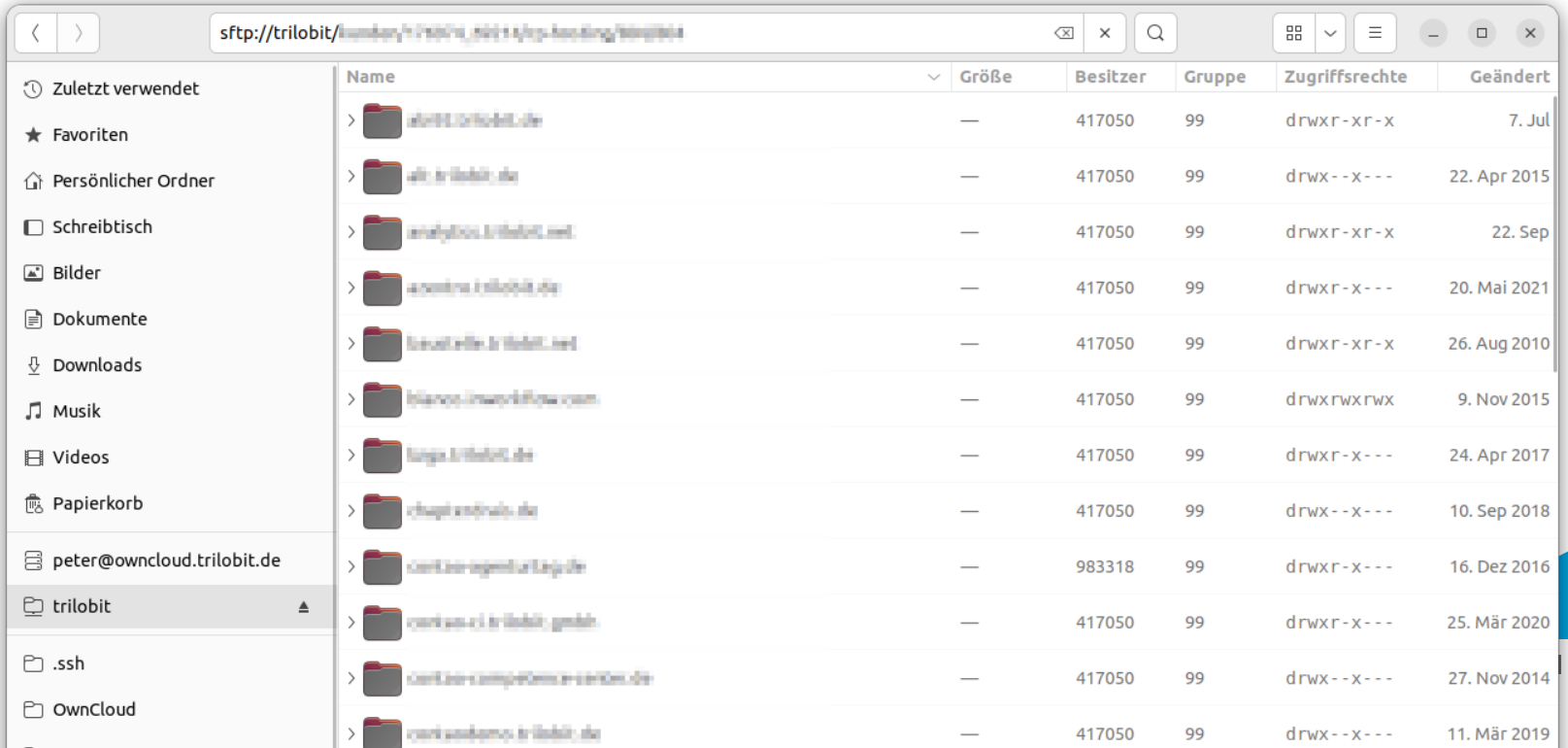
Mitarbeitende

- Jede(r) Mitarbeitende bekommt ein eigenes Schlüsselpaar
- Einfaches einbinden neuer bzw
- Deaktivieren ausgeschiedener Mitarbeitenden
- Personalisierter Zugang
- Server-Zugänge gezielt zuordnen und verteilen
- Berechtigungen zu verschiedenen Servern können einfach verwaltet werden

The *trilobit* way of work

An- und Einbindung

- Einfache Anbindung externer Tools (GitHub, GitLab, …) für CI, Depoyment, …
- Einfaches Einbinden z. B. als Laufwerk im Dateimanager



The *trilobit* way of work

Sicherheit und Automatisierung

- Passwörter der SSH-Benutzer können beliebig komplex und damit sicher werden
- Automatisierung für Erstellung und Verteilung → "SSH-Key-Manager"

The *trilobit* way of work

SSH-Key-Manager

- Neue Zugänge werden hier ergänzt
- Alte Zugänge einfach gelöscht
- Verteilung der Keys durch den SSH-Key-Manager
  - `authorized_keys` wird automatisiert verwaltet
  - Mitarbeitende: bekommen den privaten Schlüssel "persönlich" übermittelt

SSH-Key-Manager

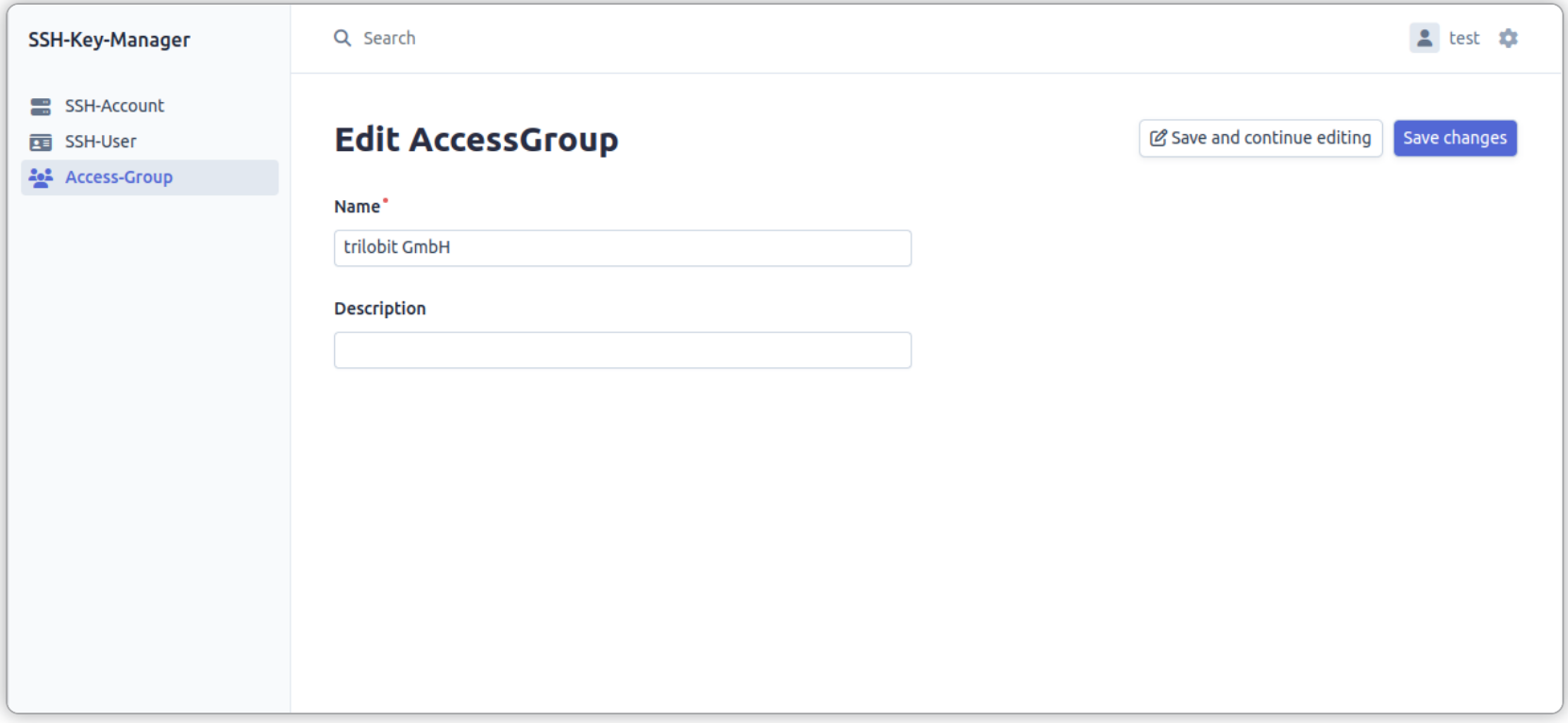
SSH-Key-Manager

Funktionen

- Verwaltung
  - Berechtigungsgruppen
  - Serverzugänge
  - Mitarbeitenden
- Individuelle SSH-Keys erzeugen
- Automatisches verwalten der öffentlichen Schlüssel
- Mitarbeitenden den privaten Schlüssel zur Verfügung stellen

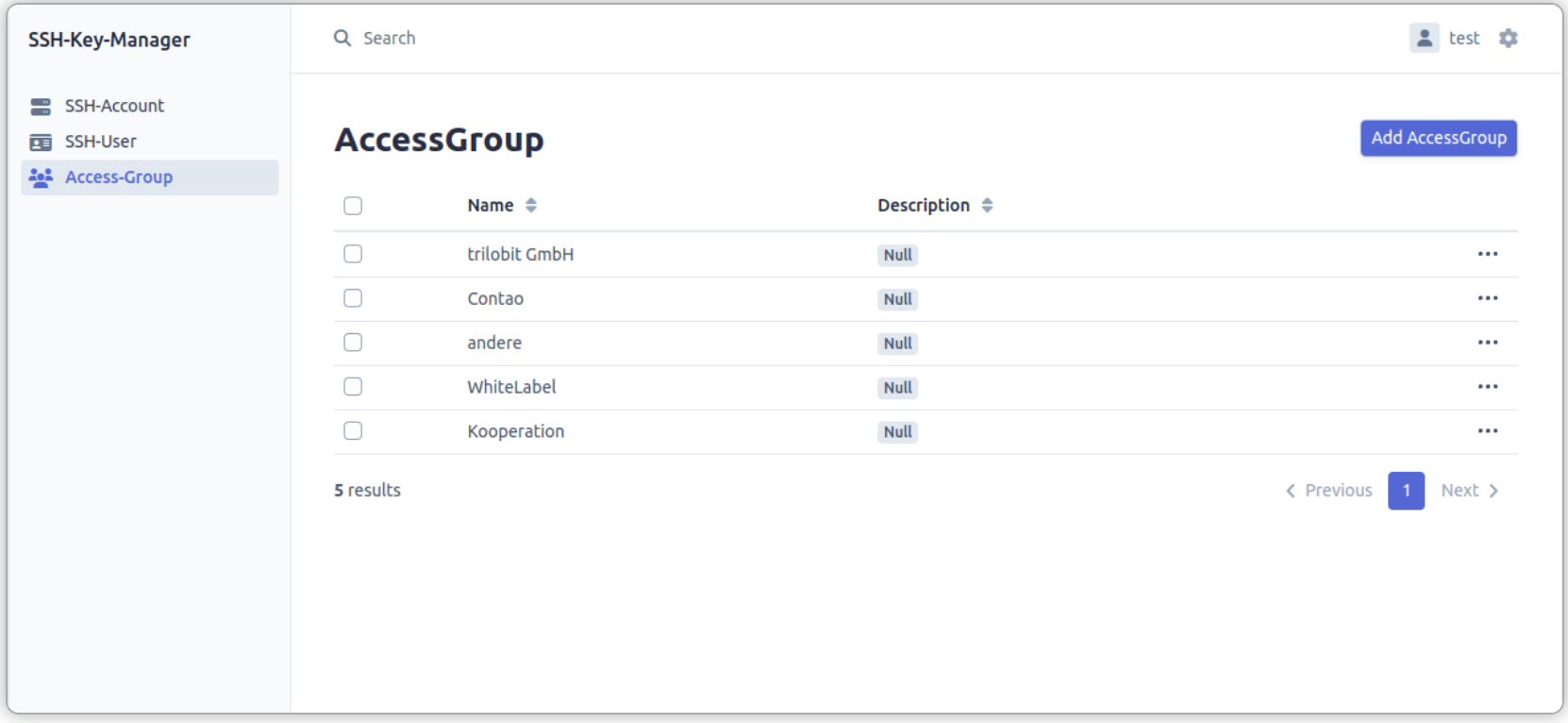
SSH-Key-Manager

Berechtigungsgruppen verwalten



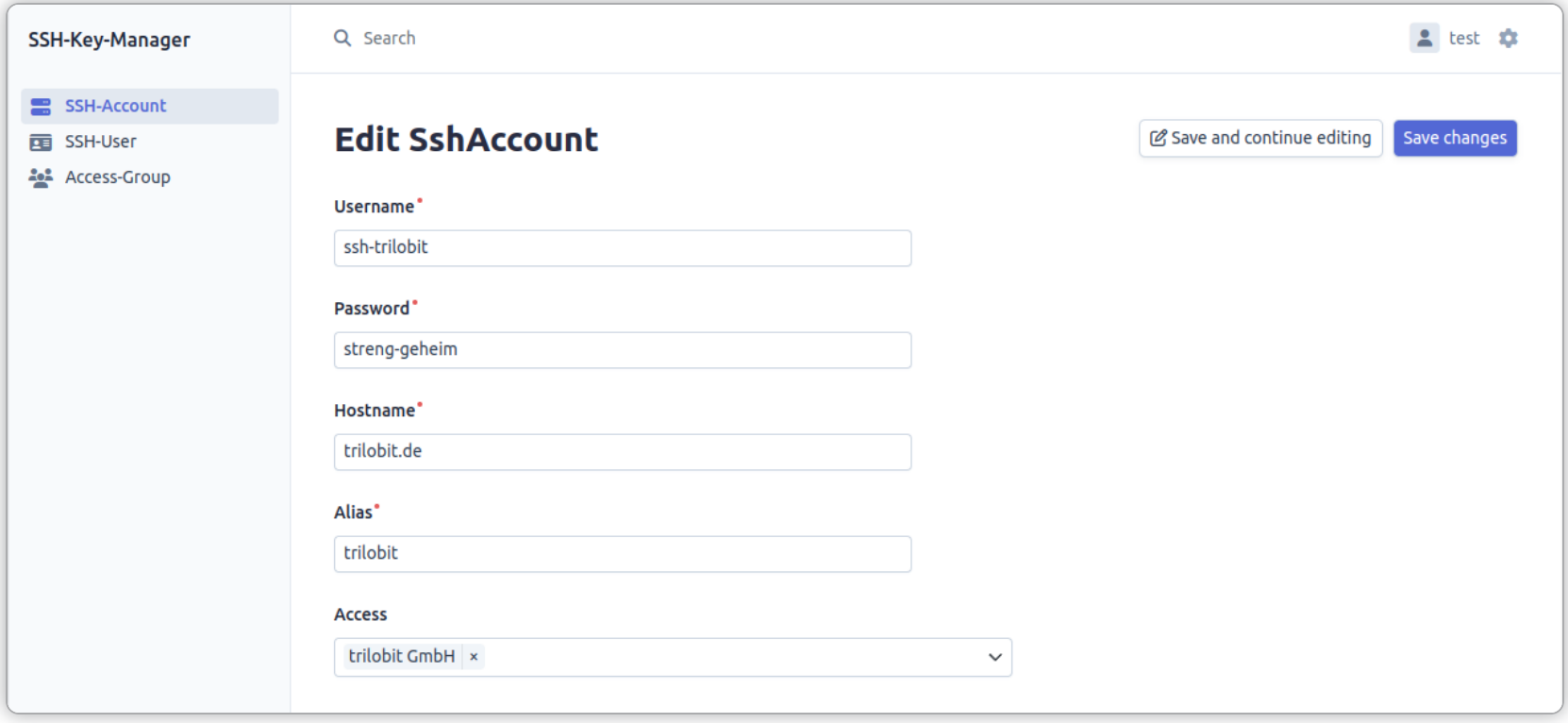
SSH-Key-Manager

Berechtigungsgruppen-Liste



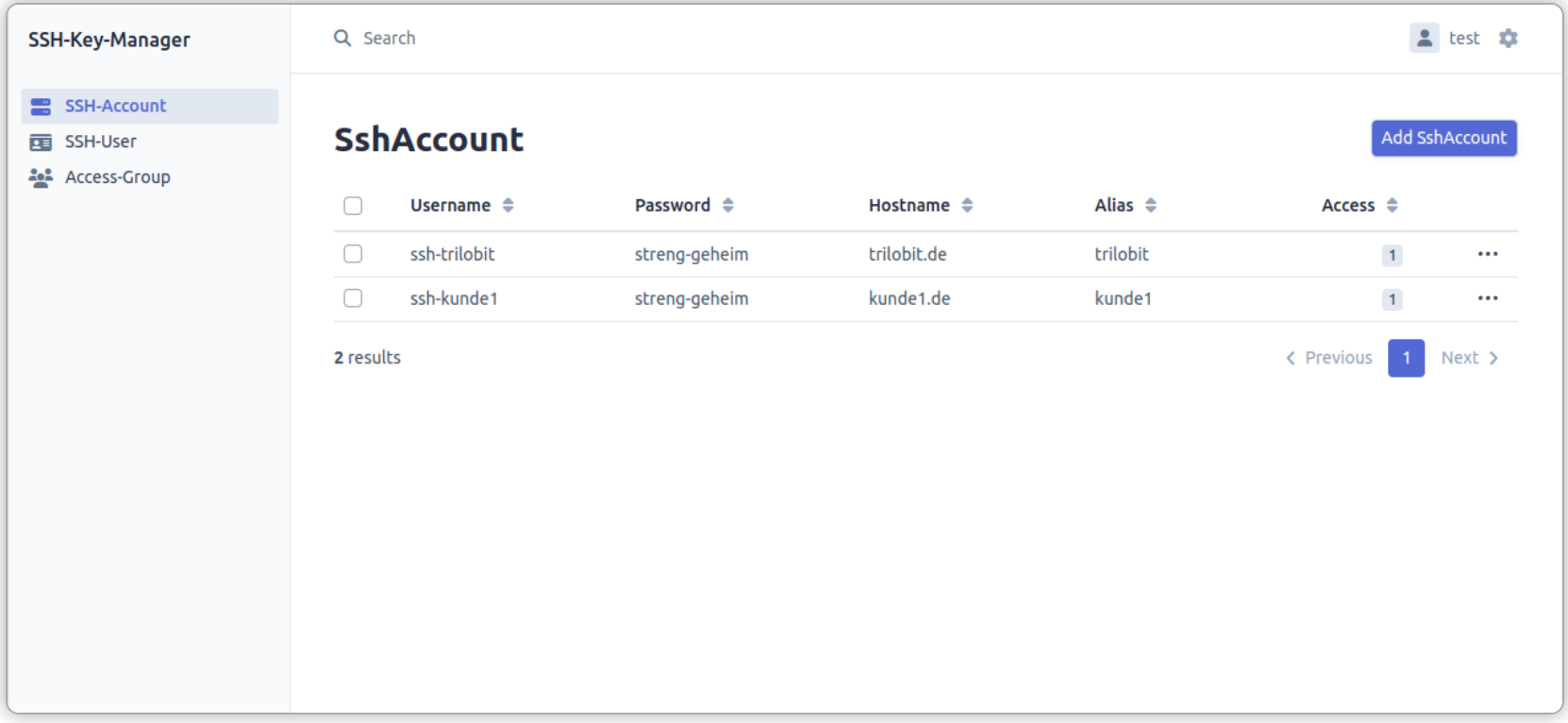
SSH-Key-Manager

Server verwalten



SSH-Key-Manager

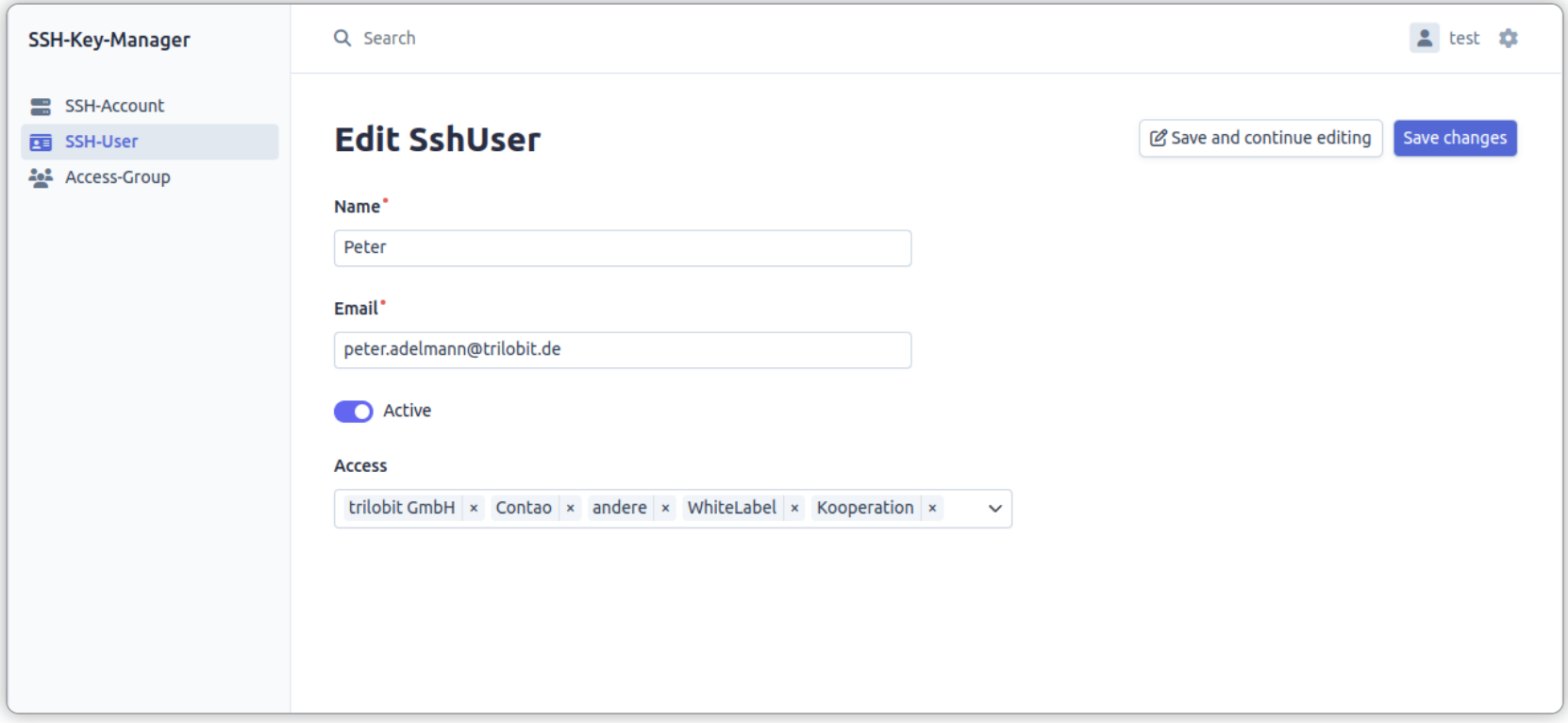
Server-Liste



trilobit
VIEL MEHR ALS INTERNET

SSH-Key-Manager

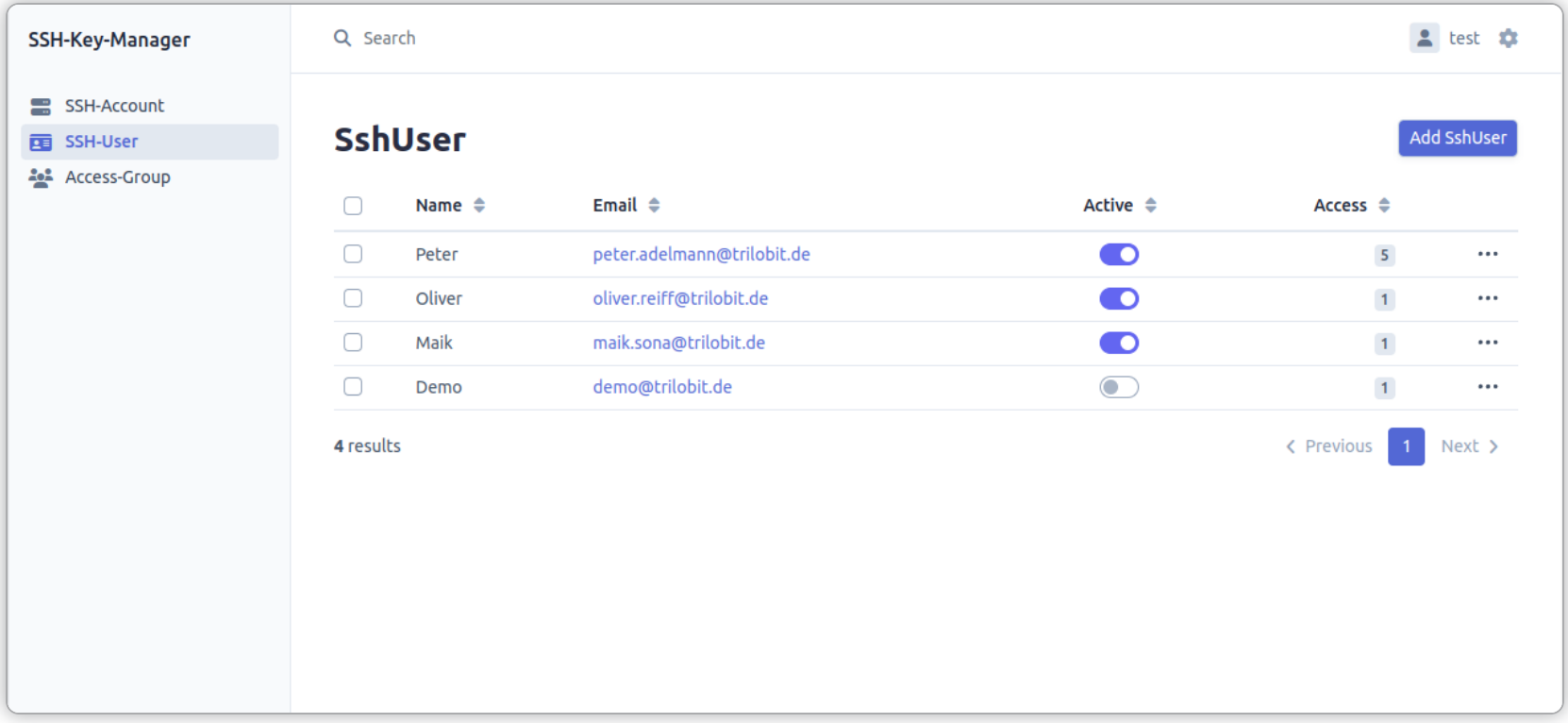
Mitarbeitenden verwalten



trilobit
VIEL MEHR ALS INTERNET

SSH-Key-Manager

Mitarbeitenden-Liste



The *trilobit* way of work

- ...


Software
Update / Nachtrag

Windows / Infos zu Rückfragen aus der Fragerunde ;-)

Software

- OpenSSH für Windows
  - https://learn.microsoft.com/de-de/windows-server/administration/openssh/openssh_overview
  - https://learn.microsoft.com/de-de/windows-hardware/manufacture/desktop/factoryos/connect-using-ssh?view=windows-11
- PuTTY
  - https://www.putty.org/
- SSH-Zugriff über Windows Dateimanager
  - https://konsumschaf.de/post/ssh-zugriff-ueber-windows-dateimanager/


Vielen DANK!

trilobit
VIEL MEHR ALS INTERNET

Optimiere ich die Seite für IE oder Netscape Navigator?

Wer sind die Spender von Kohl in der Spendenaffäre?

Könnt Ihr Internet?

Können wir uns Angestellte leisten?

Funktioniert mein Computerauch noch im Jahr 2000?

1999

Wer ist Dirk Nowitzki?

Wie verdiene ich im Internet Geld?

Nehme ich <marquee> oder <blink> dafür?

Wie beobachtet man die totale Sonnenfinsternis?

Was kommt nach Boris Becker und Steffi Graf?

„Mambo No. 5", „Buena Vista Social Club" oder doch lieber „Maschendrahtzaun"?

Wann kommt der Brexit
und kommt er überhaupt?

Können sich unsere Angestellten
die Karlsruher Mieten noch leisten?

Können wir
Internet?

Ist das auch
DSGVO-konform?

Wie verdiene ich im Internet Geld?

Was stellt Trump
schon wieder an?

2019

Gibt es dafür nicht schon
einen Microservice?

Beendet Dirk Nowitzki
seine Karriere?

Wird das nächste Projekt
vor dem Berliner Flughafen fertig?