

Technik

- [Diensteangebot](#)
 - [Softwerke-Account](#)
 - [Matrix-Chat](#)
 - [Cloud-Speicher](#)
 - [Passwort-Vault](#)
 - [Intern: E-Mail & Mailinglisten](#)
 - [Intern: Vereins-Homepage](#)
- [Infrastruktur-Dokumentation](#)
 - [Technologieplan](#)
 - [Infrastruktur der Softwerke](#)
 - [Backup-Server](#)
 - [Speicher-Server](#)
 - [Mail-Infrastruktur](#)
 - [DNS](#)

Dienstangebot

Allgemeine Hilfe & Infos zu unseren öffentlichen bzw. vereinsöffentlichen Diensten

Dienstangebot

Softwerke-Account

Dein Softwerke-Account ist der zentrale Login für all unsere Dienste. Du kannst deinen Account auf auth.softwerke.md registrieren & verwalten.

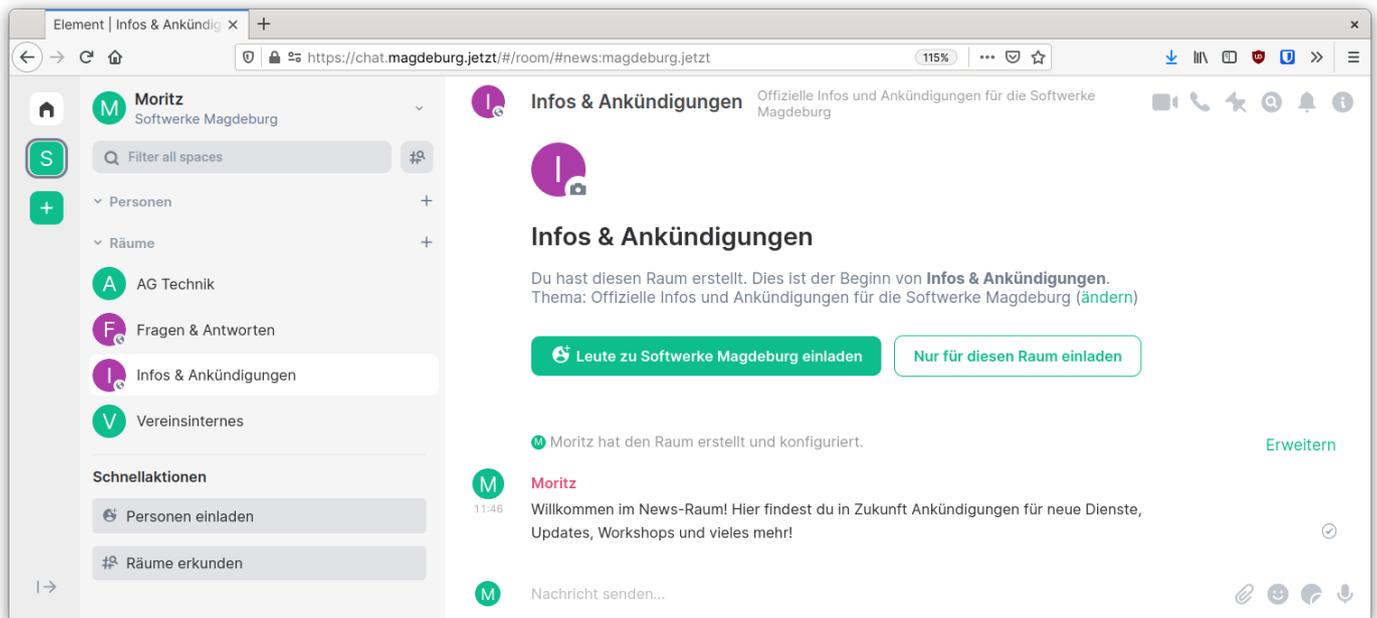
Die Erstellung eines Accounts ist kostenlos.

Um unseren Fortbestand und zu sichern kannst du uns mit einer Spende unterstützen oder direkt [hier](#) Mitglied werden.

Solltest du größere Projekte haben, bei denen unsere Dienste dir nicht ausreichen solltest, kontaktiere uns bitte unter vorstand@softwerke.md, damit wir eine Lösung finden können.

Matrix-Chat

Matrix ist ein verschlüsselter & föderierter Chat-Standard, bei dem du die Kontrolle über deine Daten hast. Tauche mit uns bei chat.magdeburg.jetzt in die Welt von Matrix ein, und kommuniziere sicher mit deinen Freunden!



Das technische Grundprinzip von Matrix ist ähnlich wie bei E-Mail: es gibt viele Server (bei E-Mail wird dieser durch den Teil hinter dem @ angegeben), und alle Menschen können sich darüber miteinander unterhalten, egal ob sie ihr Nutzerkonto z. B. bei Google, Mailbox.org oder ihrem Arbeitgeber haben. Auch bei Matrix ist die Adresse zweigeteilt (wenn auch in einem etwas anderen Format als bei E-Mail), mit einem [Softwerke-Account](#) mit dem Nutzernamen "max" heißt du bei Matrix `@max:magdeburg.jetzt`.

Der Nutzernamen für die Anmeldung bei Matrix muss in jedem Fall klein geschrieben werden! Ist der Nutzernamen deines [Softwerke-Accounts](#) also "Max" oder "MAX", dann heißt du bei Matrix trotzdem "max", also `@max:magdeburg.jetzt`

Ähnlich wie die Weboberfläche des E-Mail-Anbieters oder E-Mail-Programme oder -Apps gibt es auch bei Matrix sogenannte Clients - wir verwenden bei chat.magdeburg.jetzt die Software [Element](#), die du auch für deinen Computer oder für dein Handy [herunterladen](#) kannst. Weitere Clients sind [auf der Matrix-Homepage](#) aufgelistet, achte aber darauf dass bei vielen teils noch essentielle Funktionen fehlen.

Wenn du bereits einen Matrix-Account hast, kannst du evtl. [das Migrations-Tool von EMS](#) ausprobieren - wie gut dieses funktioniert müssen wir jedoch erst herausfinden.

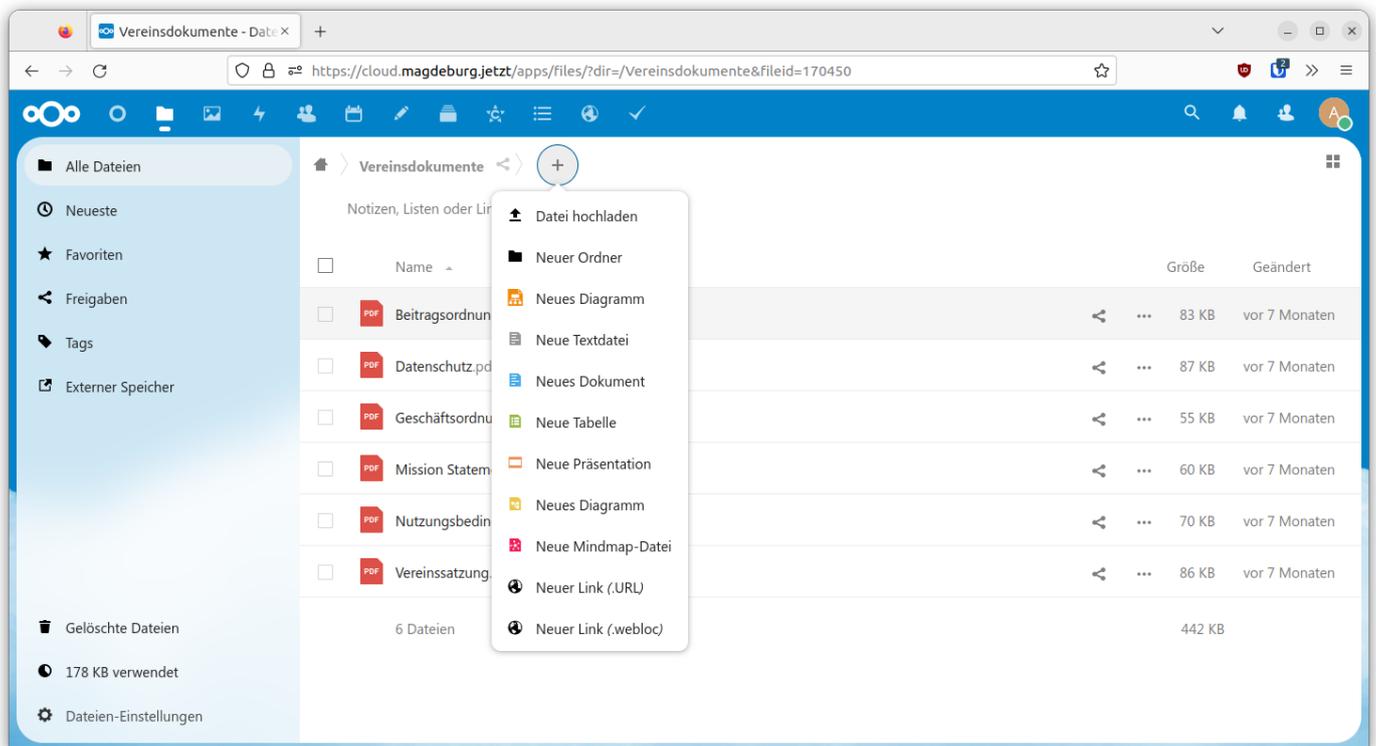
Cloud-Speicher

Unsere Nextcloud auf <https://cloud.magdeburg.jetzt/> ist ein Speicher für all deine Dateien, Fotos, Kontakte, Aufgaben & Kalender. Du kannst diese dort auch mit Freunden & Familie teilen und gemeinsam bearbeiten.

Bei uns bekommst du aktuell kostenlos bis zu **5 GB Speicherplatz** - das reicht für sehr viele Dokumente, sowie für Fotos aus dem einen oder anderen Urlaub.

Wenn du mehr brauchst, schreib' uns gern eine Mail an kontakt@softwerke.md mit einer kurzen Begründung.

Über jeden Antrag entscheiden wir separat und im Kontext unserer aktuellen Situation, jedoch freuen wir uns sehr, wenn wir unsere monatlichen Kosten von 33 € je 1000 GB auch regelmäßig durch deine Spenden decken können.



Kompatible Apps & Programme

Es gibt eine [offizielle Nextcloud-App](#) für Computer sowie für Android- & Apple-Handys, die aber vor allem auf Dateien fokussiert ist. Damit kannst du beispielsweise - wie du es vielleicht von Dropbox oder Google Drive kennst - einen Ordner auf deinem Computer mit der Cloud synchronisieren, damit du online und offline jeweils die gleichen Daten hast.

Andere Apps können genutzt werden, wenn sie entweder Nextcloud oder den **DAV-Standard** unterstützen (z.B. WebDAV für Dateien, CalDAV für Kalender oder CardDAV für Kontakte). Für **Kalender & Kontakte** gibt es hier beispielsweise für **Android die App [DAVx5](#)**, am Computer kannst du beispielsweise [Thunderbird](#) dafür nutzen.

Für DAV-Apps: App-Passwort erstellen

Um dich bei DAV-basierten Apps anzumelden, benötigst du ein Nextcloud-spezifisches App-Passwort.

Gehe dafür auf die Seite <https://cloud.magdeburg.jetzt/settings/user/security>, gib dort ganz unten einen Namen für die App und/oder das Gerät ein (damit du das Passwort später in der Liste erkennen kannst) und klicke daneben auf "Neues App-Passwort erstellen".

Du erhältst dann ein zufälliges Passwort, welches du in der App zusammen mit deinem Software-Benutzernamen nutzen kannst.

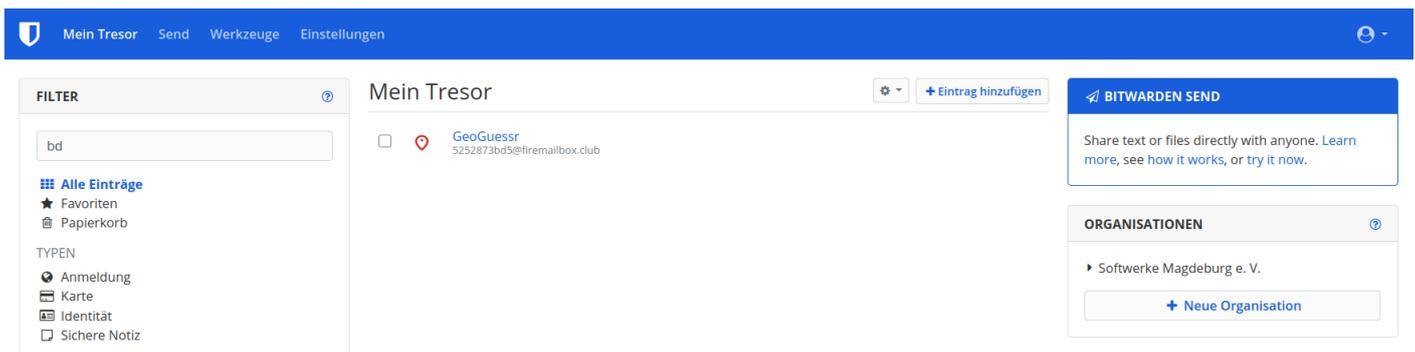
Passwort-Vault

Auf jeder Seite soll man ein einmaliges, sicheres Passwort verwenden, am besten ein schwer zu merkendes, und dann soll man sich alle merken? Das geht nicht - Abhilfe schaffen Passwort-Manager, bei denen man mit einem Master-Passwort (plus optional weitere Sicherheitsmaßnahmen) einen verschlüsselten Tresor aufschließen kann, in dem man dann alle seine Accounts und Passwörter verwaltet.

Die Softwerke bieten dafür [BitWarden](#) (bzw. technisch gesehen [bitwarden_rs](#)) an, du findest es unter [vault.magdeburg.jetzt](#).

Die Logindaten für deinen Tresor sind aus Sicherheitsgründen vollständig getrennt von deinem restlichen Softwerke-Account! Du benötigst jedoch einen Softwerke-Account mit der gleichen E-Mail-Adresse, um dich für den Tresor registrieren zu können.

Ohne deinem Master-Passwort kann niemand auf deine Passwörter zugreifen, merke es dir darum sehr gut! Im Idealfall merkst du dir nur dein Master-Passwort für den Tresor und änderst dein Passwort für den Softwerke-Account direkt auf ein im Tresor generiertes & gespeichertes zufälliges Passwort.



Einrichtung eines zweiten Faktors für mehr Sicherheit

In den Tresor-Einstellungen gibt es die Option "[Zwei-Faktor-Authentifizierung](#)" (2FA), wo du beispielsweise eine *Authentifizierungs-App* wie den [Aegis Authenticator](#) für Android oder den [Tofu Authenticator](#) für iOS als zweiten Faktor einrichten kannst. Sicherer sind jedoch *FIDO U2F-Sicherheitsschlüssel* - das sind kleine USB-Sticks (beispielsweise der [SoloKeys Solo V2](#) oder der [Nitrokey FIDO2](#)), die du zusammen mit deinem Passwort quasi wie einen klassischen "Schlüssel" zu deinem Tresor nutzen kannst.

Ein zweiter Faktor bedeutet, dass jemand der dein Passwort (den ersten Faktor) kennt, sich nur anmelden kann, wenn er auch Zugriff auf dein Handy oder deinen U2F-Schlüssel hat. Eine detailliertere Anleitung findest du unter "[Alles über Zwei-Faktor-Authentifizierung](#)".

Die Zwei-Faktor-Authentifizierung betrifft deinen Tresor nur logisch, nicht kryptografisch - das bedeutet, dass unsere AG Technik theoretisch trotz 2FA nur dein Master-Passwort benötigt, um deinen Tresor zu

entschlüsseln. Es schützt jedoch sehr gut gegen viele mögliche Angriffe von außen und ist darum unbedingt zu empfehlen.

Nutzung auf anderen Webseiten & am Handy

Um die Passwörter auf Webseiten und in Apps zu nutzen, gibt es [auf der Webseite von BitWarden Apps und Browser-Erweiterungen](#) für die meisten Geräte. Hierbei musst du bei der Anmeldung oben links das Zahnrad [Einstellungen](#) anklicken, und dort als "Server-URL" die Adresse `https://vault.softwerke.md` angeben: (vault statt tresor)

Schließen	Bitwarden	Speichern
SELBSTGEHOSTETE UMGEBUNG		
Server URL		
<code>https://tresor.softwerke.md</code>		
Bitte gib die Basis-URL deiner selbst gehosteten Bitwarden-Installation an.		

Sicherung und Backup

Exportiere regelmäßig deine Passwort-Datenbank und sichere sie in deinem Backup. Wir übernehmen keine Garantie, dass deine Passwörter nicht verloren gehen können. Im Team nutzen wir auch unsere Bitwarden-Instanz, daher haben wir aber selbst ein großes Interesse daran, dass nichts schief geht. Aber sichere so wichtige Sachen wie Passwörter bitte trotzdem nochmal unabhängig von uns ab.

Um deinen Tresor zu exportieren, kannst du [hier klicken](#) oder in Bitwarden im Tab "Werkzeuge" > "Tresor exportieren" deine Daten exportieren. Falls du dir unsicher bist, wähle am besten als Dateiformat *json (Encrypted)*, damit die Datenbank auch auf deiner Festplatte vor unbefugtem Zugriff geschützt ist (z.B. falls dein Laptop verloren geht).



WERKZEUGE
Generator
Daten importieren
Tresor exportieren

Tresor exportieren

PERSÖNLICHER TRESOR WIRD EXPORTIERT

Es werden nur persönliche Tresoreinträge exportiert, die mit hanneskuehn@posteo.de verbunden sind. Tresoreinträge der Organisation werden nicht berücksichtigt. Es werden nur Informationen der Tresoreinträge exportiert. Diese enthalten nicht die zugehörigen Anhänge.

Dateiformat

Exporttyp

Konto eingeschränkt

Verwende den Verschlüsselungscode deines Kontos, abgeleitet vom Benutzernamen und Master-Passwort, um den Export zu verschlüsseln und den Import auf das aktuelle Bitwarden-Konto zu beschränken.

Passwortgeschützt

Lege ein Dateipasswort fest, um den Export zu verschlüsseln und importiere ihn in ein beliebiges Bitwarden-Konto, wobei das Passwort zum Entschlüsseln genutzt wird.

Dateipasswort (erforderlich)

Dieses Passwort wird verwendet, um diese Datei zu exportieren und zu importieren

Dateipasswort bestätigen (erforderlich)

Format bestätigen

Intern: E-Mail & Mailinglisten

E-Mail wird von uns nur für Vereinsmitglieder für die offizielle Vereinskommunikation angeboten.

Wenn du einen Anbieter für deine persönliche E-Mail-Adresse suchst, schau doch einmal bei folgenden datenschutzfreundlichen Alternativen vorbei:

- **mailbox.org:** ab 1€/Monat
 - **Posteo:** ab 1€/Monat
 - **Tutanota:** vollverschlüsselt, kostenlose Version beschränkt Mail-Suche auf letzte 4 Wochen, sonst ab 1€/Monat
 - **ProtonMail:** vollverschlüsselt, kostenlose Version ebenfalls recht stark eingeschränkt, sonst ab 5€/Monat
- (*vollverschlüsselte* Anbieter sind etwas sicherer, aber nicht ganz so einfach und flexibel zu nutzen wie du das von anderen Anbietern kennst, du kannst z.B. nicht mehr beliebige Mail-Apps nutzen)

Für Vereins-E-Mails steht dir unter webmail.softwerke.md die Webmail-Oberfläche zur Verfügung. Anmelden kannst du dich ganz normal mit deinem Softwerke-Account, also Benutzername und Passwort.

Wenn du deine Vereins-Mails an deine private Adresse weiterleiten möchtest, kannst du im Webmail in den Einstellungen unter "Filter" eine Weiterleitung erstellen (neuer Filter mit Aktion "Weiterleiten nach").

Jeder kann E-Mails von den, dem jeweiligen Konto zugewiesenen, Aliassen verschicken, sowie der eigenen Adresse. Das heißt, wenn `alias1@softwerke.md` auf `nutzer1@softwerke.md` weiterleitet, kann Nutzer1 sowohl von `alias1@` also auch von `nutzer1@` verschicken. Das ganze funktioniert auch mit verketteten Aliassen.

Der Vorstand kann über unsere Server E-Mails von jeder Adresse `@softwerke.md` verschicken, alle anderen nur unter ihrer Vereins-E-Mail-Adresse oder unter explizit freigeschalteten Aliassen. Im Webmail kannst du dafür in den Einstellungen deine Identitäten verwalten.

Wenn du einen externen E-Mail-Client nutzen willst, nutze dafür folgende Daten:

	IMAP (Empfang)	SMTP (Versand)
Server	<code>mail.softwerke.md</code>	<code>mail.softwerke.md</code>
Port & Sicherheit	<code>993</code> (TLS/SSL) oder <code>143</code> (StartTLS)	<code>465</code> (TLS/SSL) oder <code>587</code> (StartTLS)
Benutzername	<code>accountname@softwerke.md</code>	
Passwort	Dein Softwerke-Passwort	

Mailinglisten

Das beschriebene Setup für Mailinglisten ist nicht korrekt, und wird angepasst, sobald die Listmonk-Umstellung abgeschlossen ist.

Für Mailinglisten verwenden wir [Schleuder](#), du findest dafür die Weboberfläche auf verteiler.softwerke.md. Die Administration erfolgt ansonsten hauptsächlich über E-Mail-Befehle, mehr Informationen dazu findest du [in der Schleuder-Dokumentation](#).

Aktuell gibt es folgende Mailinglisten:

- (noch nicht eingerichtet)

Für neue Mailinglisten und weitere Fragen kontaktiere bitte die AG Technik (admin@softwerke.md).

Mailrouting

Alias	?	Ziel	Bemerkung
accounts@	?	AG Technik & Vorstand	Adresse für Accounts
admin@	?	AG Technik	
finanzen@	?	AG Finanzen	
kontakt@	?	vorstand@	
pr@	?	AG Öffentlichkeitsarbeit	
verein@	?	Alle Vereinsmitglieder	Kann nur vom Mitgliedern benutzt werden.
vorstand@	?	Vorstand	

Intern: Vereins-Homepage

Dieser Artikel betrifft die Vereins-Webseite, die von Mitgliedern der AG für Öffentlichkeitsarbeit verwaltet wird.

Wenn du einen Anbieter für deine persönliche Homepage suchst, schau doch einmal bei folgenden datenschutzfreundlichen Alternativen vorbei:

- **hosting.de**: ab 2,90€/Monat, klassisches Webhosting
- **uberspace.de**: zahl-was-du-willst, für technisch versierte Nutzer

Die Vereinshomepage softwerke.md wird über ProcessWire verwaltet und kann von allen Mitgliedern der AG Öffentlichkeitsarbeit bearbeitet werden.

Die Adminoberfläche ist über <https://softwerke.md/processwire/> zu erreichen.

Caching

Bei Bedarf kann der Cache der Website unter Module ? Core ? PageRender geleert werden. Das ist zum Beispiel notwendig, um einen Refresh der Vereinsdokumente zu erzwingen.

Infrastruktur-Dokumentation

Die technische Seite der Technik, hauptsächlich intern von der AG Technik genutzt.

Technologieplan

“ Willkommen in unserem Technologieplan!

Hier sammeln wir zukünftige Pläne und Ideen aus drei Perspektiven in drei Kategorien: aus der Perspektive der **Benutzenden unseres Angebots**, der **Vereinsmitglieder** sowie der **AG Technik** gibt es jeweils, die Softwerke-Infrastruktur betreffend, **Schmerzpunkte** (die einen regelmäßig nerven), **Wünsche** (die ein Problem dieser Perspektive direkt lösen würden) sowie ungenutztes **Potenzial** (also Ideen die das Leben einfacher machen könnten).

Am Anfang jeder Idee steht der Monat, in dem sie dieser Liste hinzugefügt wurde. Die AG Technik wird sich bemühen, sich insbesondere zeitlich an die Reihenfolge der Kategorien und das Alter der Ideen zu halten.

Wenn du einen neuen Punkt für diese Liste hast, schreibe am besten einfach einen Kommentar zu diesem Wiki-Artikel, damit wir die Idee entsprechend ausformulieren und einordnen können.

Perspektive der Benutzenden

Schmerzpunkte

Wünsche

2022/08 Es gibt noch keine Mobilizon-Instanz.

2022/05 Die Webseite ist bisher nur auf Deutsch verfügbar, eine Englische Version oder auch eine Version in leichter Sprache ist sinnvoll.

Potenzial

2022/08 Erstregistrierung bei Vaultwarden erfolgt nicht intuitiv über den Softwerke-Account.
Aktuell braucht man effektiv jemandem der einem zeigt wie es funktioniert.

2021/12 Synchronisation von Nextcloud Circles zu anderen Diensten wäre cool.
Beispielsweise LDAP/Authentik-Gruppen, Vaultwarden-Organisationen, Matrix-Spaces, etc.

Perspektive der Mitglieder

Schmerzpunkte

2022/08 Der Schlüssel für die Vorstands-Mailadresse im WKD ist nicht aktuell. -> Mailserver!

Wünsche

2022/08 Generell sollten verschlüsselte Mails für alle einfach nutzbar sein.

2024/02 Ein Link-Shortener wäre schön für so Dinge wie den Plenums-Links, QR-Codes etc.; es gibt auch schon eine Domain.

2024/02 Eine einfach einzurichtende Spielwiese für Neumitglieder
Das kam aus der Roadmap.

Potenzial

2022/08 Mehr Motivation für Spenden von Nichtmitgliedern.
Über Authentik sollte es möglich sein, einen monatlichen Spendenbetrag zu verwalten. Dieser könnte dann als einfachster Weg genutzt werden, um entsprechend unserer Unkosten automatisch die Limits des Accounts anzupassen.
Zu klären: ist das dann eine geschäftsmäßige Tätigkeit oder dürften wir diesen Betrag auch als zweckungebundene Spende behandeln wenn wir gemeinnützig wären?

Perspektive der AG Technik

Schmerzpunkte

2022/02 Die Dokumentation ist optimierbar.

Das macht es nicht besonders einfach, neue Leute an Bord zu holen

2024/02 Wir haben immer noch keinen ordentlichen Onboarding-Prozess

2024/02 Blackbox nervt, wir sollten auf git-crypt umsteigen.

2024/02 InfluxDB macht immer Probleme mit dem RAM.

Es gibt Alternativen zu Influx, oder wir müssen den Server upgraden. Tunen kann man da wenig.

Wünsche

Potenzial

Infrastruktur der Softwerke

Der gesamte Code der für den Betrieb unserer Infrastruktur notwendig ist, ist auf <https://codeberg.org/softwerke-magdeburg/infrastructure> zu finden.

Server, DNS & mehr

Unsere Server laufen bei <https://netcup.de>. Das Passwort zum CCP kann im Passwort-Manager nachgeschlagen werden; das SCP ist nur über das CCP erreichbar.

Domains, DNS und Speicherplatz (als Object Storage) laufen bei <https://ovh.de>.

CoreOS als Betriebssystem

CoreOS wurde gewählt, weil es sich selbst updated und kaum Wartung benötigt. Für Updates ist ein Neustart notwendig, dafür wurde als Wartungszeitfenster 05:30 bis 06:25 gewählt.

Die Ignition-Konfiguration kann immer nur bei der (Neu)Installation von CoreOS verwendet werden - kleinere Änderungen dürfen manuell erledigt werden, ansonsten ist eine Neuinstallation meist empfehlenswert.

Für das Deployment von CoreOS ist eine `.env`-Datei notwendig (im `coreos`-Verzeichnis dieses Repositories), deren Inhalt im Passwort-Manager zu finden ist.

Mehr Informationen zum Deployment neuer Server ist in der [coreos/README.md](#) zu finden.

Docker Swarm + Docker Stack

Docker Swarm kann mehrere Systeme zu einem Cluster zusammenschließen, ist dabei aber deutlich weniger flexibel als Kubernetes.

Docker Stack kann Projekte auf ein Docker-System oder einen Swarm-Cluster deployen, und zwar mit den bekannten [Compose-Dateien](#).

Die Projekte sind im Ordner `services` zu finden und können mit `swarm-make <service>.up clean` gestartet und mit `swarm-make <service>.down clean` gestoppt werden - dafür ist ein erstmaliges Setup erforderlich, wie in der [services/README.md](#) beschrieben ist. Ebenfalls ist eine zweite `.env`-Datei erforderlich, die ebenfalls im Passwort-Manager zu finden ist..

Zur Konfiguration der Dienste werden statt Volumes `configs` genutzt, da diese automatisch im Cluster verteilt werden.

Backup-Server

Der [Borg Backup](#)-Server ist eine Schnittstelle zwischen dem Internet sowie dem - nur intern erreichbaren - Backup-Speicher bei [Scaleway](#) (als Block Storage).

Einrichtung

Erstellung in Scaleway

Der Server wurde mit folgender Konfiguration erstellt:

```
scw instance server create \  
  type=STARDUST1-S \  
  zone=nl-ams-1 \  
  image=rockylinux_8 \  
  root-volume=l:10G \  
  additional-volumes.0=b:25G \  
  name=backup.s.softwerke.md \  
  ip=none \  
  project-id=869d0909-f443-424a-8a6d-08c21ed750a8
```

Durch diese Konfiguration ist der Server nicht per IPv4 sondern nur per IPv6 erreichbar (das spart etwas über 1 € im Monat).

In der zugehörigen Security Group (namens `Backup`) wird dann ausschließlich SSH-Verkehr aus dem Internet zugelassen und alle anderen eingehenden TCP- und UDP-Verbindungen verworfen.

Aktuell hängt noch eine IP am Server da IPv6 auf unserem Hauptserver noch nicht wirklich funktioniert.

Einrichtung per Ansible

Zu beachten ist, dass (Stand Oktober 2021) bei Rocky Linux 8.4 nur OpenSSH 8.0 verfügbar ist, also noch keine Hardware-Schlüssel unterstützt werden.

Der Server kann über [Ansible](#) mithilfe des Playbooks im Ordner `backup-server` des Infrastruktur-Repos eingerichtet werden - dies erfolgt mit dem folgenden Befehl:

```
ansible-playbook playbook.yml
```

Vergrößerung des Speicherplatzes

Wenn der Block Storage vergrößert wird, kann die Partitionstabelle sowie das Dateisystem mit folgendem Befehl vergrößert werden:

```
{ printf 'w\nY\nY\n' | gdisk /dev/sda; } && \  
{ printf "d\nn\n$(cat /sys/block/sda/sda1/partition)\n$(cat  
/sys/block/sda/sda1/start)\n\n8300\nw\nY\n" | gdisk /dev/sda; } && \  
partprobe && \  
resize2fs /dev/sda1
```

Backups & Borg-Repositories

Repository erstellen

Ein verschlüsseltes Backup-Repository wird (auf dem jeweiligen Quellserver) wie folgt erstellt:

```
borg init \  
  --encryption authenticated-blake2 \  
  --append-only \  
  backup@backup.s.softwerke.md:/mnt/REPONAME
```

Backup manuell erstellen

Ein Backup kann dann folgendermaßen durchgeführt werden:

```
BORG_PASSPHRASE='...' \  
borg create \  
  --progress \  
  "backup@backup.s.softwerke.md:/mnt/REPONAME:: {now:%Y-%m-%d--%H-%M-%S}" \  
  /var/lib/docker/volumes
```

Automatische Backups per systemd-Timer

/etc/systemd/system/backup.service

```
[Unit]  
Description=Backup  
After=syslog.target network.target  
  
[Service]  
Type=oneshot  
ExecStart=/usr/bin/borg create --progress  
"backup@backup.s.softwerke.md:/mnt/REPONAME:: {now:%Y-%m-%d--%H-%M-%S}"  
/var/lib/docker/volumes  
Environment=BORG_PASSPHRASE=...
```

/etc/systemd/system/backup.timer

```
[Unit]  
Description=Run backup every 3 hours  
  
[Timer]  
OnCalendar=*-*-* 00,03,06,09,12,15,18,21:00:00  
  
[Install]  
WantedBy=timers.target
```

Monitoring

TODO: wir sollten (jeweils mit Benachrichtigung) prüfen ob einerseits im Repo die Backups ankommen, und andererseits der "borg create"-Befehl mit erfolgreichem Exit-Code abschließt.

Speicher-Server

Der Speicher-Server stellt die NextCloud zur Verfügung - dafür würde sich zwar theoretisch auch ein Docker-Container mit der NextCloud-S3-Anbindung eignen, letztere ist jedoch unglaublich langsam. Unsere Zwischenlösung ist darum ein RAID-0 aus Block Storage Volumes, wodurch ausschließlich vertikale Skalierung möglich ist. Langfristig ist die NextCloud wohl der Dienst wo sich am ehesten die Anschaffung eigener Hardware in Kombination mit einem GlusterFS-Dateisystem lohnt, hoffentlich ist bis dahin aber OwnCloud Infinite Scale an einem Punkt angekommen, wo das obsolet ist.

Einrichtung

Erstellung in Scaleway

Der Server wurde mit folgender Konfiguration erstellt:

```
scw instance server create \  
  type=DEV1-S \  
  zone=fr-par-2 \  
  image=rockylinux_8 \  
  root-volume=1:20G \  
  name=speicher.s.softwerke.md \  
  ip=new \  
  project-id=473e8c4a-83a4-41f6-a7de-9dd6aa2a3247
```

Einrichtung per Ansible

Zu beachten ist, dass (Stand Oktober 2021) bei Rocky Linux 8.4 nur OpenSSH 8.0 verfügbar ist, also noch keine Hardware-Schlüssel unterstützt werden.

Der Server kann über [Ansible](#) mithilfe des Playbooks im Ordner `speicher-server` des Infrastruktur-Repos eingerichtet werden - dies erfolgt mit dem folgenden Befehl:

```
ansible-playbook playbook.yml
```

Mail-Infrastruktur

// TODO

Postfix

- MTA
- Senden und empfangen von Mails
 - routing, rewriting, restrictions und bedingungen

Rspamd

- spamfilter

Dovecot

- MDA
- Mailboxen

LDAP

DNS

Momentan haben wir folgende DNS-Zonen

magdeburg.jetzt, softwerke.md

für die Erreichbarkeit von Diensten

s.softwerke.md

für Server

swarm.softwerke.md

Docker Swarm ist bei uns legacy und wird mit dem Server-Umzug abgelöst

für Docker Swarm