Shibboleth IdP und eduMFA containerisiert betreiben

David Hübner

Support: Pascal König, Aleyna Nasher Taher

DAASI International GmbH

Agenda

- Vorteile und Herausforderungen
- DAASI Shibboleth IdP-Image
- Beispiel 1:
  Betrieb eines containerisierten IdP inkl. Config mit docker compose
- eduMFA-Image
- Beispiel 2:
  Betrieb in Kubernetes mit Helm-Charts
- Ausblick

Motivation

- Config auf verschiedenen Umgebungen synchron halten
- Einheitliches Deployment-Modell
- Reproduzierbare Setups v.a. für CI
- Verfügbarkeit & Skalierung

DAASI International

Vorteile eines containerisierten Betriebs

- **Einfaches Setup**
  - Reproduzierbare Installation
  - Vorkonfigurierte Umgebung
  - Schneller Start, insbesondere auch für Entwicklungsumgebungen
- **Unabhängig des Betriebssystems**
  - Einheitliche Laufzeitumgebung inklusive Java und Tomcat
  - Aktuelle Tomcat Version (keine Abhängigkeiten zur Updateversorgung der Distribution)
  - Weniger Abhängigkeiten vom Host-System
- **Config-Management (via Git)**
  - Versionierte Konfiguration
  - Nachvollziehbare Änderungen
  - Reproduzierbare Deployments

DAASI International

Vorteile eines containerisierten Betriebs

- **Automatisierung**
  - Automatisierte Deployments (z.b. bei Konfigurationsänderungen im Git)
- **Updates & Rollback**
  - Kontrollierter Wechsel zwischen Image-Versionen
  - Schnelle Rückkehr zur vorherigen Version
  - Unterbrechungsfreie Updates bei passender Architektur und Deployment-Strategie
- **Skalierbarkeit**
  - Zusätzliche Instanzen bei Bedarf
  - Lastverteilung
  - Ausfallsicherheit
  - Flexible Ressourcenzuweisung

DAASI International

Vorteile eines containerisierten Betriebs

- **Modern**
  - Standardisierte Bereitstellung
  - Portable Images
  - Gute Integration in Cloud- und Plattformumgebungen
- **Security-Strategie**
  - Unpriviligierter Betrieb mit minimalen Berechtigungen
  - Gezielte Volume-Freigaben
  - Klare Benutzer- und Rechteverwaltung
- **Logs, Reports & Metriken**
  - Zentralisierung von Logs, Reports und Metriken
  - Transparente Betriebszustände
  - Dashboards und automatische Alarmierung
  - z.B. mit Loki, Grafana und Prometheus

DAASI International

Reporting Beispiele

Authentifizierungsmethoden pro Service Provider

Service Provider ↑	Anzahl Logins	Authentifizierungsmethode
https://accounts.meet.daasi.de/auth/realms/opentalk	2	https://refeds.org/profile/mfa
https://accounts.meet.daasi.de/auth/realms/opentalk	2	password
https://cor[redacted].daasi.de/auth/external/saml/metadata	1	https://refeds.org/profile/mfa
https://gitlab.daasi.de	1	https://refeds.org/profile/mfa
https://login.computer[redacted].de/shibboleth	288	password
https://monitoring.daasi.int/shibboleth	578	password
https://testsp3.aai.dfn.de/shibboleth	1	https://refeds.org/profile/mfa
https://testsp3.aai.dfn.de/shibboleth	1	urn:de:zedat:fudis:SAML:2.0:ac:classes:CR

Fehlerhafte Logins pro Benutzer und IP-Adresse

IP Adresse	userid	Anzahl
134.[redacted].71	[redacted]	1
212.71.[redacted].105	Hallo-DFN-BT	1
84.[redacted].2	pl[redacted]er	1
93.[redacted].147	0815	1
93.[redacted].147	asdfg	2
93.[redacted].147	leider.vertippt	1

Dashboards: https://gitlab.daasi.de/didmos2/didmos2-grafana/-/tree/develop/dashboards?ref_type=heads

DAASI International

Logs Beispiele

Shibboleth IdP ERROR Events

```
2026-09-30 11:46:39,886 - 47.[redacted]252 - ERROR [org.opensaml.profile.action.impl.DecodeMessage:97] - Profile Action DecodeMessage: Unable to decode incoming request
2026-09-30 11:46:39,886 - 47.[redacted]252 - ERROR [org.opensaml.profile.action.impl.DecodeMessage:97] - Profile Action DecodeMessage: Unable to decode incoming request
2026-09-30 11:46:14,524 - 47.[redacted]216 - ERROR [org.opensaml.profile.action.impl.DecodeMessage:97] - Profile Action DecodeMessage: Unable to decode incoming request
2026-09-30 11:46:14,524 - 47.[redacted]216 - ERROR [org.opensaml.profile.action.impl.DecodeMessage:97] - Profile Action DecodeMessage: Unable to decode incoming request
2026-09-30 11:27:01,124 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
2026-09-30 11:27:01,068 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
2026-09-30 11:27:01,124 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
2026-09-30 11:27:01,068 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
2026-09-30 11:27:00,895 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
2026-09-30 11:27:00,844 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
2026-09-30 11:27:00,793 - 20.[redacted].163 - ERROR [org.opensaml.saml.metadata.resolver.impl.AbstractDynamicMetadataResolver:841] - FunctionDrivenDynamicHTTPMetadataResolver dfn_aai_mdq_prod: Error fetching metadata from origin source
```

Shibboleth IdP Lockout Management Events

```
INFO 2026-09-30 12:51:10,629 - 93.[redacted].147 - INFO [net.shibboleth.idp.authn.impl.StorageBackedAccountLockoutManager:380] - Lockout threshold reached for '0815!93.[redacted]147', invalid count is 5
INFO 2026-09-30 12:49:36,014 - 93.[redacted].147 - INFO [net.shibboleth.idp.authn.impl.StorageBackedAccountLockoutManager:380] - Lockout threshold reached for 'leider.vertippt!93.[redacted].147', invalid count is 3
INFO 2026-09-30 12:46:30,973 - 93.[redacted].147 - INFO [net.shibboleth.idp.authn.impl.StorageBackedAccountLockoutManager:380] - Lockout threshold reached for '0815!93.[redacted].147', invalid count is 4
INFO 2026-09-30 12:46:28,949 - 93.[redacted].147 - INFO [net.shibboleth.idp.authn.impl.StorageBackedAccountLockoutManager:380] - Lockout threshold reached for '0815!9[redacted]147', invalid count is 3
```

Dashboards: https://gitlab.daasi.de/didmos2/didmos2-grafana

Herausforderungen eines containerisierten Betriebs

- **Know-how**
  - Einarbeitung in Containerisierung & Orchestrierung (K8s)
  - Komplexeres Netzwerksetup
- **Betriebskomplexität**
  - Zusätzliche Komponenten für Deployment
  - Monitoring und Verwaltung
- **Datenpersistenz**
  - Datenhaltung außerhalb des Containers
  - Backup und Wiederherstellung von Volumes

DAASI International

Herausforderungen eines containerisierten Betriebs

- **Permissions & Users**
  - Zugriffsrechte (UID/GID) zwischen Container und Host
- **Security**
  - Regelmäßiges Update von Images
  - Schwachstellen prüfen
  - Secrets sicher verwalten
- **Fehlersuche**
  - Analyse über mehrere Instanzen
  - Zentrale Logs und Metriken sinnvoll

DAASI International

Herausforderungen eines containerisierten Betriebs

- **Ressourcenmanagement**
  - CPU- und RAM-Limits
  - Skalierung
  - Engpässe frühzeitig erkennen
- **Rollbacks**
  - Datenbank-Rollbacks
    - konsistente Wiederherstellung kann komplexer sein im Vergleich zu VM-basiertem Snapshot Rollback

DAASI International

DAASI Shibboleth IdP Baseimage

Link zum DAASI Gitlab
Dokumentation &
source code

- **Image Basics**
  - Rocky Linux 10.1 Basisimage
  - openjdk-21
  - Aktuelle Tomcat 11 Version *(durch DAASI paketiert für Rocky 10)*
  - Versionierung
    - Prefix v5.2.3 = Shibboleth IdP Version
    - Suffix = Datumsstempel des Release
    - Immutable Tags: v5.2.3-20260930
    - Dynamic Tags: v5.2.3 oder v5.2
    - Weekly Rebuild mit Sicherheitsupdates mit Immutable Tag + Update der Dynamic Tags

DAASI International

DAASI Shibboleth IdP Baseimage

Link zum DAASI Gitlab Dokumentation & source code

- **Image Content**
  - Aktuelle Shibboleth IdP Version *(ohne Config & Credentials)*
  - Integrierte Plugins *(ohne Config)*
    - jdbc
    - nashorn
    - OIDC OP / Config / Common
    - OIDC RP
    - Fudiscr
  - Healthcheck / liveness probes
  - Entrypoint-Skript

DAASI International

DAASI Shibboleth IdP Baseimage

Link zum DAASI Gitlab Dokumentation & source code

- **Entrypoint Funktionen**
  - Validierung der IdP Config & Gesamtsetup
    - Config Integration + Shibboleth Basissetup in Working directory
    - sealer.jks Validierung
      - Auto create wenn nicht vorhanden
    - DB Connection Check
      - für mariadb / mysql u. postgresql
      - Automatische Initialisierung der DB

```
============ CHECK SEALER AVAILABILITY ============
INFO: sealer parts available, use existing sealer.jks & kver


============ CHECK DATABASE AVAILABILITY ============
INFO: mysql/mariadb database driver found, trying to connect now
INFO: Check DB Connection
INFO: Databases found:
Database
information_schema
shibboleth
INFO: validate credentials now
Detected MariaDB → using CREATE INDEX IF NOT EXISTS for index creation
INFO: db connect successful, create tables for Shibboleth IDP if not existent
INFO: Create Index of shibpid table if not existent
```

DAASI International

DAASI Shibboleth IdP Baseimage

Link zum DAASI Gitlab
Dokumentation &
source code

- **Entrypoint Funktionen**
  - LDAP Connection Check
  - Import CA-Certs in Java Keystore *(z.B. f. http data-connector)*
  - Tomcat Config *(RemoteIpValve)*
    - Anpassungen von http header & internalProxies über Variablen

```
============ CHECK LDAP AVAILABILITY ============
INFO: Detected 1 configured ldap systems, trying to connect now


LDAP CONNECTION CHECK (1/1)
INFO: ldap connection to ldap://ldap.daasi.de successful established after 1 retries, trying connect to next ldap server if more configured


============ CHECK CUSTOM (CA) CERTS ============
INFO: file(s) found in java-cacerts-addon directory. Prepare cacerts file location, checking file type's and going forward to import if content is a (ca) certificate
INFO: daasi-ca.crt looks like a certificate, check now
INFO: daasi-ca.crt is a certificate, import now into cacerts
INFO: test.crt looks like a certificate, check now
ERROR: test.crt is not a valid certificate (errorlevel: 1), skip import
```

DAASI Shibboleth IdP Baseimage

- **Entrypoint Funktionen**
  - Build des Shibboleth IdP Servlet *(idp.war)*
  - Installation zusätzl. Shibboleth Plugins
    - Dateibasiert
    - URL-basiert auf der Roadmap

Link zum DAASI Gitlab
Dokumentation &
source code

```
============ CHECK CUSTOM (CA) CERTS ============


============ TOMCAT CONFIGURATION ============

INFO: No custom proxy addresses detected. Add container networks to tomcat11 configuration as internalProxies
INFO: Set tomcat webapps directory: /var/lib/tomcat/webapps
INFO: ROOT webapps directory not available, copy directory from /usr/src/tomcat11/webapps


============ BUILDING SHIBBOLETH IDP SERVLET ============


============ INSTALLING CUSTOM SHIBBOLETH PLUGINS ============
INFO: custom-plugin dir is present but empty
```

DAASI International

DAASI Shibboleth IdP Baseimage

Link zum DAASI Gitlab
Dokumentation &
source code

- **Konfiguration des Image**
  - Steuerung des Containers per Umgebungsvariablen
    - STAGE → steuert Umgebung (z.B. DEV | STAGING | PROD)
    - LOGLEVEL → entrypoint
    - PROXY_IP → Proxy IP f. Tomcat *(Single IP o. CIDR; multivalue)*
    - REMOTE_IP_HEADER → Header mit Client IP *(default x-forwarded-for)*
    - JAVA_PARAMS → Steuerung der Java Parameter und Ressourcen

Weitere Parameter sind in der README im DAASI Gitlab dokumentiert.

DAASI Shibboleth IdP Baseimage

- Shibboleth Identity Provider Konfigurationsaufbau (stages)
- Annahme: Großteil der Konfig ist stage-übergreifend (hier nicht gezeigt)

```
.
├── conf
│   ├── env.properties -> /opt/shibboleth-idp/stages/DEV/conf/env.properties
│   ├── metadata-providers.xml -> /opt/shibboleth-idp/stages/DEV/conf/metadata-providers.xml
├── credentials
├── edit-webapp
├── flows
├── messages
├── metadata
│   ├── idp-metadata.xml -> /opt/shibboleth-idp/stages/DEV/metadata/idp-metadata.xml
│   └── oidc-clients.xml -> /opt/shibboleth-idp/stages/DEV/metadata/oidc-clients.xml
├── stages
│   ├── DEV
│   │   ├── conf
│   │   │   ├── env.properties
│   │   │   └── metadata-providers.xml
│   │   ├── metadata
│   │   │   ├── idp-metadata.xml
│   │   │   └── oidc-clients.xml
│   │   └── static
│   │       └── openid-configuration.json
│   ├── STAGING
│   ├── PROD
├── static
│   └── openid-configuration.json -> /opt/shibboleth-idp/stages/DEV/static/openid-configuration.json
└── views
```

DAASI Shibboleth IdP Baseimage

- **IdP Implementierung der Konfiguration**
  - Image Overlay basierend auf DAASI Baseimage
    - Kopieren der Config in das Baseimage (ohne secrets/credentials)

```
FROM docker.gitlab.daasi.de/shibboleth-identity-provider/shibboleth-identity-provider-baseimage:v5.2

USER tomcat:tomcat
COPY --chown=tomcat:tomcat conf /usr/src/shibboleth-idp-addon/conf
COPY --chown=tomcat:tomcat edit-webapp /usr/src/shibboleth-idp-addon/edit-webapp
COPY --chown=tomcat:tomcat flows /usr/src/shibboleth-idp-addon/flows
COPY --chown=tomcat:tomcat messages /usr/src/shibboleth-idp-addon/messages
COPY --chown=tomcat:tomcat metadata /usr/src/shibboleth-idp-addon/metadata
COPY --chown=tomcat:tomcat stages /usr/src/shibboleth-idp-addon/stages
COPY --chown=tomcat:tomcat views /usr/src/shibboleth-idp-addon/views

COPY --chown=tomcat:tomcat edit-webapp/error/generic-error.html
/usr/src/tomcat10/webapps/ROOT/error/generic-error.html
```

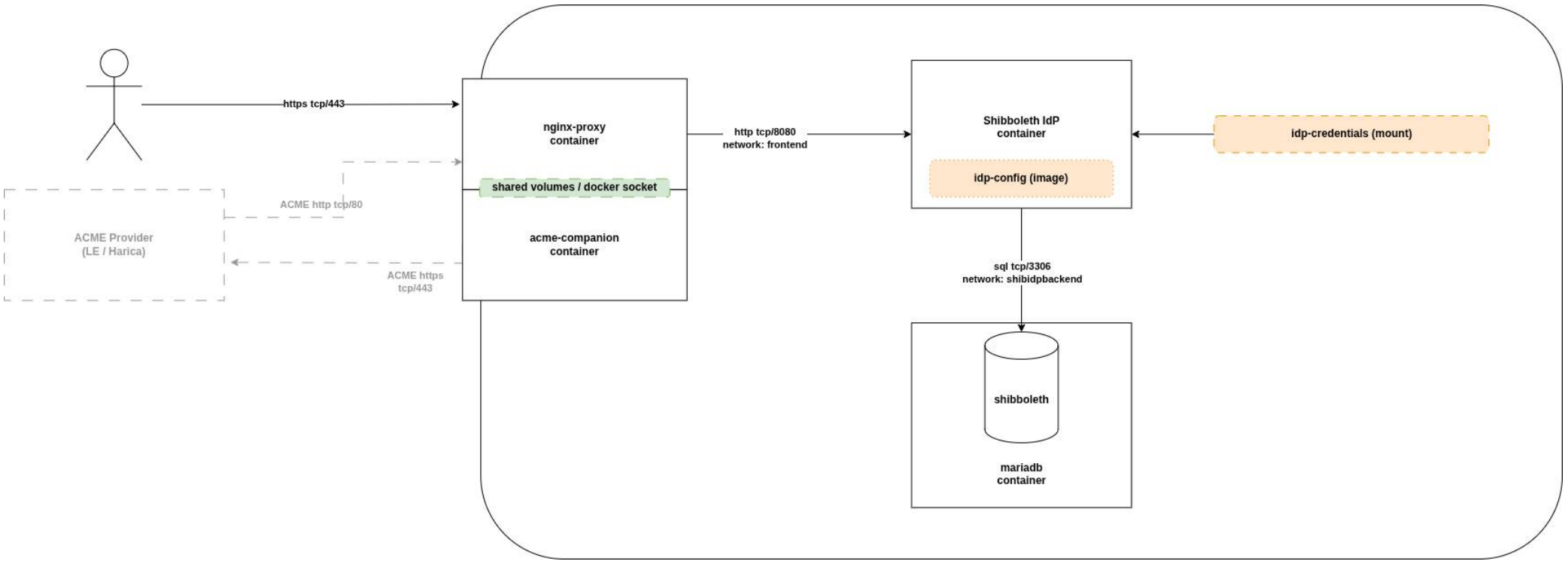
DAASI Shibboleth IdP Baseimage

- **IdP Implementierung der Konfiguration**
  - per filemount in docker / podman

```
- "shibidp-var:/var/shibboleth-idp/metadata"
- "shibidp-logs:/var/log/shibboleth-idp"
- "./shibidp-config:/usr/src/shibboleth-idp-addon"
- "./shibidp-certs:/usr/src/java-cacerts-addon" #optional: cert import into java keystore (entrypoint)
```

DAASI International

Beispiel 1: Betrieb eines containerisierten Shibboleth IdP (docker)



Betrieb eines containerisierten Shibboleth IdP

- Beispiel docker-compose.yml IdP + MariaDB siehe Git
- Mit oder ohne Reverse Proxy

Link zum DAASI Gitlab Dokumentation & source code

```
# docker compose -f docker-compose-nginx-acme.yaml up -d
[+] up 5/5
 ✓ Container proxy                Running                                  0.0s
 ✓ Container nginx-acme           Running                                  0.0s
 ✓ Network docker_shibidpbackend  Created                                  0.1s
 ✓ Container shibboleth-idp-db    Healthy                                 10.5s
 ✓ Container shibboleth-idp       Started                                 10.8s
#
```

Betrieb eines containerisierten IdP inkl. Config mit docker-compose

- Setup Übersicht

```
# docker ps --format "table {{.Image}}\t{{.Ports}}\t{{.Names}}\t{{.Status}}"
IMAGE                                                                                  PORTS                                                                   NAMES               STATUS
docker.gitlab.daasi.de/shibboleth-identity-provider/shibboleth-identity-provider-baseimage:v5.2   8080/tcp                                                                shibboleth-idp      Up 6 minutes (healthy)
mariadb:lts                                                                            3306/tcp                                                                shibboleth-idp-db   Up 6 minutes (healthy)
nginxproxy/acme-companion                                                                                                                                      nginx-acme          Up 19 hours
nginxproxy/nginx-proxy:latest                                                          0.0.0.0:80->80/tcp, [::]:80->80/tcp, 0.0.0.0:443->443/tcp, [::]:443->443/tcp   proxy               Up 19 hours
#
```

```
# docker stats
CONTAINER ID   NAME              CPU %     MEM USAGE / LIMIT     MEM %     NET I/O           BLOCK I/O         PIDS
ed419d41edb2   shibboleth-idp    0.23%     603.5MiB / 7.569GiB   7.79%     57.8kB / 54.1kB   717kB / 143MB     67
b2f6271176bd   shibboleth-idp-db 0.01%     124MiB / 7.569GiB     1.60%     41.5kB / 38.7kB   4.24MB / 70.7kB   21
1dff5e7bb29a   nginx-acme        0.23%     14.77MiB / 7.569GiB   0.19%     13MB / 6.99MB     2.13MB / 26.5MB   15
f3f7a40d0e12   proxy             0.23%     47.69MiB / 7.569GiB   0.62%     1.55MB / 807kB    1.61MB / 13.9MB   26
```

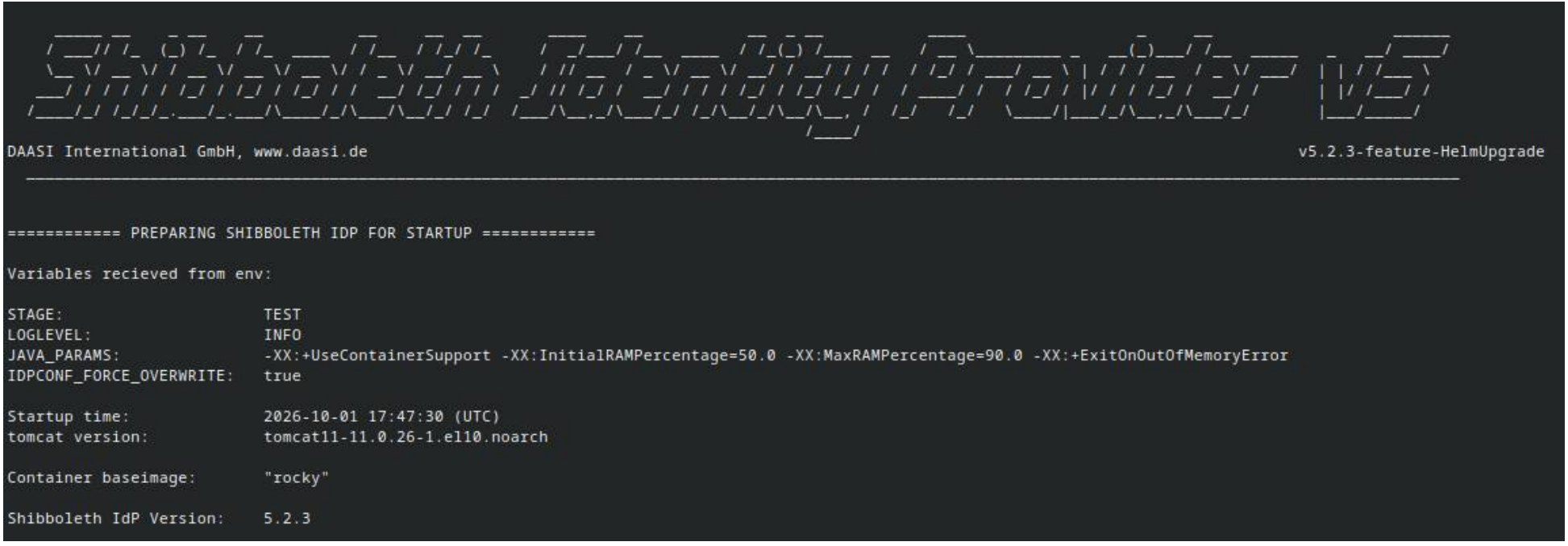
Betrieb eines containerisierten IdP inkl. Config mit docker-compose

- **Alle Logs nach stdout**
  - Entrypoint
  - Tomcat
  - Shibboleth IdP (idp-process.log)
    - Eigener Log Appender benötigt (zusätzlich zu File)

DAASI International

Betrieb eines containerisierten IdP inkl. Config mit docker-compose

- **Entrypoint Logs**



Betrieb eines containerisierten IdP inkl. Config mit docker-compose

- **Tomcat Startup Logs**

```
============ STARTING TOMCAT ============
17:48:20.643 [main] INFO net.shibboleth.idp.conf.impl.SpringConfigServletContextInitializer -- Setting init parameters and instal
ling Spring listener
17:48:20.690 [main] INFO net.shibboleth.idp.conf.impl.ServletConfigServletContextInitializer -- Registering primary IdP servlet
17:48:20.698 [main] INFO net.shibboleth.idp.conf.impl.ServletConfigServletContextInitializer -- Registering RemoteUser authentica
tion servlet
17:48:20.701 [main] INFO net.shibboleth.idp.conf.impl.ServletConfigServletContextInitializer -- Registering X.509 authentication
servlet
17:48:20.702 [main] INFO net.shibboleth.idp.conf.impl.ServletConfigServletContextInitializer -- Registering metadata endpoint ser
vlet
17:48:20.703 [main] DEBUG net.shibboleth.idp.conf.impl.RegisterFilterChainServletContextInitializer -- Attempting to register fil
ter 'ShibbolethFilterChain'
17:48:20.708 [main] INFO net.shibboleth.idp.conf.impl.RegisterFilterChainServletContextInitializer -- Registered the filter 'Shib
bolethFilterChain'.
```

Betrieb eines containerisierten IdP inkl. Config mit docker-compose

- **idp-proccess.log**

```
2026-10-01 17:48:33,831 - IP: n.a. - INFO [de.zedat.fudis.shibboleth.idp.plugin.authn.fudiscr.profile.spring.impl.FudisCrConfigurationBeansServiceCreationStrategy:102] - Serviceable co
 name 'fudismfareminder.RemindMfaSetupPredicate' could not be found.
2026-10-01 17:48:33,833 - IP: n.a. - INFO [net.shibboleth.shared.spring.service.ReloadableSpringService:395] - Service 'fudiscr.ConfigurationBeansService': Completed reload and swapped
2026-10-01 17:48:33,833 - IP: n.a. - INFO [net.shibboleth.shared.spring.service.ReloadableSpringService:402] - Service 'fudiscr.ConfigurationBeansService': Reload complete
2026-10-01 17:48:34,634 - IP: n.a. - INFO [net.shibboleth.idp.admin.impl.ReportUpdateStatus:149] - No upgrade available from 5.2.3
2026-10-01 17:48:34,635 - IP: n.a. - INFO [net.shibboleth.idp.admin.impl.ReportUpdateStatus:160] - Version 5.2.3 is current
2026-10-01 17:48:36,428 - IP: 0:0:0:0:0:0:0:1 - ERROR [org.apache.velocity.loader:355] - ResourceManager: unable to find resource 'status.vm' in any resource loader.
2026-10-01 17:56:02,579 - IP: n.a. - INFO [net.shibboleth.oidc.metadata.cache.impl.BatchMetadataCache:418] - Metadata Cache DefaultUnregisteredClientPolicyCache-cache: Metadata has not
2026-10-01 17:56:02,580 - IP: n.a. - INFO [net.shibboleth.oidc.metadata.cache.impl.BatchMetadataCache:463] - Metadata Cache DefaultUnregisteredClientPolicyCache-cache: Next refresh cyc
json]' will occur on '2026-10-01T21:56:02.580406876Z' ('2026-10-01T21:56:02.580406876Z[UTC]' local time)
2026-10-01 17:56:02,700 - IP: n.a. - INFO [net.shibboleth.oidc.metadata.cache.impl.BatchMetadataCache:418] - Metadata Cache DefaultProfileMetadataPolicyCache-cache: Metadata has not ch
2026-10-01 17:56:02,701 - IP: n.a. - INFO [net.shibboleth.oidc.metadata.cache.impl.BatchMetadataCache:463] - Metadata Cache DefaultProfileMetadataPolicyCache-cache: Next refresh cycle
on '2026-10-01T21:56:02.701429397Z' ('2026-10-01T21:56:02.701429397Z[UTC]' local time)
2026-10-01 18:03:30,170 - IP: n.a. - INFO [net.shibboleth.shared.service.AbstractReloadableService:258] - Service 'shibboleth.AttributeFilterService': Reloading service configuration
```

Betrieb eines containerisierten IdP inkl. Config mit docker-compose

- **Admin Tools im Container**
  - idplogreload → IdP Logging Service reload
  - idpmetadatareload → IdP Metadata Resolver Sercivice reload
  - idpreload → IdP Servlet reload *(touch war/idp.war)*
  - idpstatus → Ausgabe der Statusseite /idp/status[1]

Join in den Container: `docker exec -it shibboleth-idp bash`

[1] *benötigt jstl und jstl-api Java Bibliotheken unter edit-webapp/WEB-INF/lib/*

eduMFA Image

- **DAASI pflegt derzeit eigenes eduMFA Image**
  - Migration von privacyIDEA Image (damals kein offizielles Image existent)
  - Do not use... Ablösung in Arbeit
- **Vorteile des offiziellen eduMFA Image**
  - kein eigener Reverse-Proxy
  - Konfiguration ohne Config-File mit Umgebungsvariablen
  - Betrieb ohne Persistenz/Volume möglich
  - Beispiel docker-compose.yml und Config-Referenz siehe eduMFA-Doku

eduMFA Image

- **eduMFA Konfiguration**
  - Import git-basierter Policies, System- und Realm/Resolver-Konfigurationen etc.
    - Implementierung durch config-Script
    - Kann in eduMFA Images eingebunden werden
    - Overlay Image mit config-Script & parameterisierter Konfigurationsdateien
    - Steuerung der Parameter mit Umgebungsvariablen

```
services:
 edumfa:
   image: ghcr.io/edumfa/edumfa:2.9.5
   restart: unless-stopped
   volumes:
     - edumfa-keys:/etc/edumfa/:rw
     - ./mfa-config/config.sh:/opt/edumfa/user-scripts/config.sh:ro
     - ...
    environment:
     EDUMFA_ADMIN_USER: admin
     EDUMFA_ADMIN_PASS: [CHANGEME]
     EDUMFA_PAGE_TITLE: eduMFA Demo DAASI
     ...
```


DAASI International

eduMFA Image

- **eduMFA Konfiguration**
  - Import git-basierter Policies, System- und Realm/Resolver-Konfigurationen etc.
    - Beispiel einer Gesamtstruktur des Repositories:

```
├── mfa-config
│   ├── authentication-policy.json
│   ├── config.sh
│   ├── disablelogin-policy.json
│   ├── email-identifier.json
│   ├── emailtemplate-otp.html
│   ├── enrollment-policy.json
│   ├── idp-admin-policy.json
│   ├── policy.json
│   ├── resolver.json
│   └── smtp-server.json
```

eduMFA Image

- **eduMFA Konfiguration**
  - Beispiel Resolver config.sh Script für den Import
    - envsubst & sponge: Befüllen der Umgebungsvariablen in die JSON

```
# LDAP resolver import
envsubst < /opt/edumfa/userscripts/resolver.json | sponge /tmp/resolver.json
edumfa-manage resolver create <realm name> ldapresolver /tmp/resolver.json
```


DAASI International

eduMFA Image

- **eduMFA Konfiguration**
  - Inhalt resolver.json

```
{
  'LDAPURI': '${LDAP_URL}',
  'LDAPBASE': '${MFA_BASE_DN}',
  'START_TLS': False,
  'BINDDN': '${MFA_BIND_DN',
  'BINDPW': '${MFA_BIND_PW}',
  'LOGINNAMEATTRIBUTE': 'uid',
  'LDAPSEARCHFILTER': '(uid=*)(objectClass=inetOrgPerson)',
  'USERINFO': '{ "phone" : "telephoneNumber", "mobile" : "mobile", "email" : "mail", "surname" : "sn", "givenname" : \
                "givenName", "description" : "uid" }',
  'UIDTYPE': 'entryUUID',
  'AUTHTYPE': 'Simple',
  'NOREFERRALS': True,
  'TIMEOUT': 5,
  'SIZELIMIT': 5000,
  'CACHE_TIMEOUT': 10,
  'NOREFERRALS': False,
  'NOSCHEMAS': False
}
```

eduMFA Image

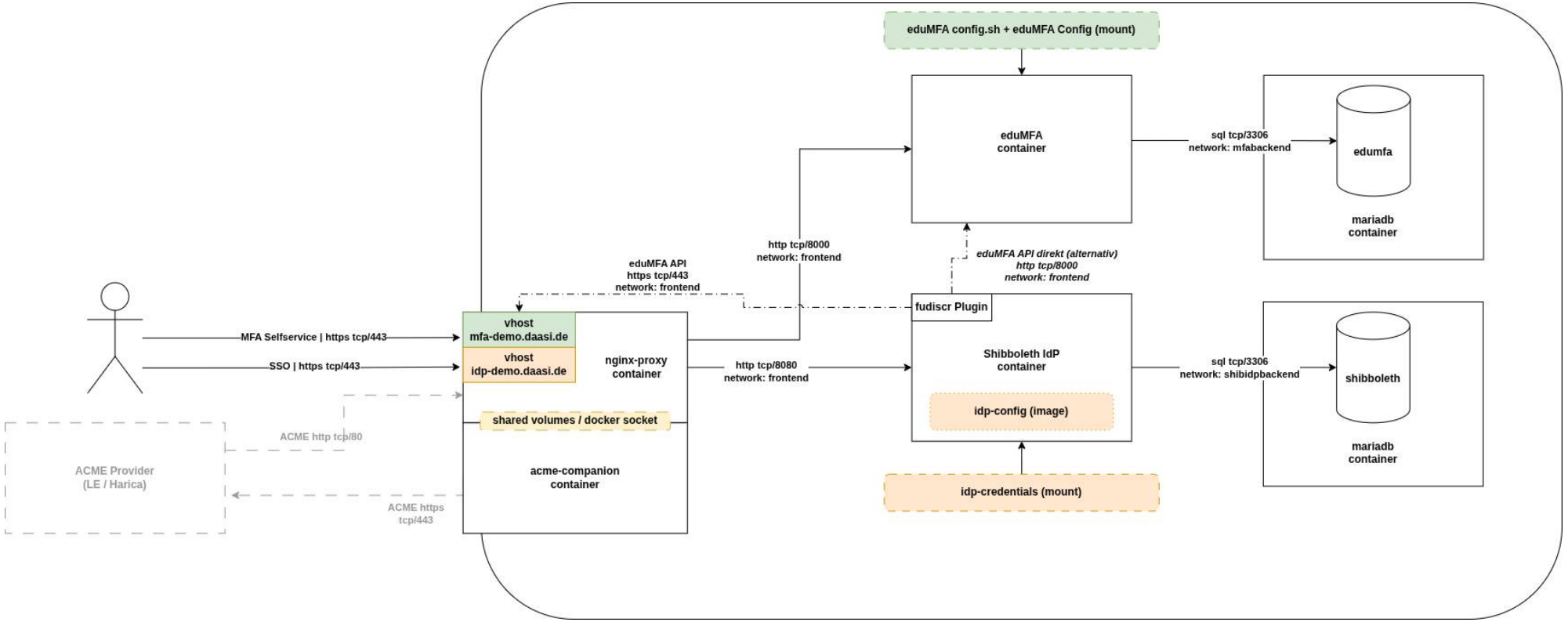
- **eduMFA inkludiert in das bestehende IdP-Setup**
  - EduMFA Container
  - mariadb

```
# docker ps --format "table {{.Image}}\t{{.Ports}}\t{{.Names}}\t{{.Status}}"
IMAGE                                                                                PORTS                                                                                 NAMES               STATUS
nginxproxy/acme-companion                                                                                                                                                  nginx-acme          Up 2 minutes
ghcr.io/edumfa/edumfa:2.9.5                                                          8000/tcp                                                                              docker-edumfa-1     Up About a minute (healthy)
nginxproxy/nginx-proxy:latest                                                        0.0.0.0:80->80/tcp, [::]:80->80/tcp, 0.0.0.0:443->443/tcp, [::]:443->443/tcp          proxy               Up 2 minutes
docker.gitlab.daasi.de/shibboleth-identity-provider/shibboleth-identity-provider-baseimage:v5.2   8080/tcp                                                                              shibboleth-idp      Up About a minute (healthy)
mariadb:12.3                                                                         3306/tcp                                                                              docker-mfa-mariadb-1   Up 2 minutes (healthy)
mariadb:lts                                                                          3306/tcp                                                                              shibboleth-idp-db   Up 2 minutes (healthy)
#
```

```
# docker stats
```

CONTAINER ID	NAME	CPU %	MEM USAGE / LIMIT	MEM %	NET I/O	BLOCK I/O	PIDS
b5b356f25285	docker-edumfa-1	3.46%	95.64MiB / 7.569GiB	1.23%	1.31kB / 252B	0B / 0B	8
11f37409db07	docker-mfa-mariadb-1	0.02%	129.7MiB / 7.569GiB	1.67%	4.43kB / 126B	11.7MB / 21.2MB	11
2bfd43ffe185	shibboleth-idp	0.28%	702.4MiB / 7.569GiB	9.06%	226kB / 289kB	0B / 144MB	68
98e4d451976a	shibboleth-idp-db	7.00%	137.4MiB / 7.569GiB	1.77%	151kB / 108kB	4.23MB / 69.1kB	27
1dff5e7bb29a	nginx-acme	0.42%	15.45MiB / 7.569GiB	0.20%	13.1MB / 7.03MB	2.13MB / 26.6MB	15
f3f7a40d0e12	proxy	0.33%	48.43MiB / 7.569GiB	0.62%	1.7MB / 973kB	1.61MB / 14.3MB	26

Finales Setup Shibboleth IdP + eduMFA



Shibboleth IdP & eduMFA in Kubernetes

Link zum DAASI Gitlab
Dokumentation &
source code

- **Helm Charts – Shibboleth IdP**
  - Siehe Git im Verzeichnis k8s
  - Besteht aus mehreren Subcharts
  - shibidp → Shibboleth IdP Chart
    - Statefulset
    - Configmap
    - Service
    - Ingress
    - Secrets

DAASI International

Shibboleth IdP & eduMFA in Kubernetes

- **Helm Charts – Shibboleth IdP**
  - Steuerung der Parameter (z.B. replicas, Hostname) per values.yaml
  - Steuerung der Secrets (primär IdP secrets Ordner) per credentials.yaml

DAASI International

Shibboleth IdP & eduMFA in Kubernetes

- **Helm Charts – eduMFA**
  - Public in https://github.com/eduMFA/helm-charts
  - benötigt externe Datenbank
  - Secrets können initial mit `uv` oder per `edumfa-manage` erzeugt werden
  - Doku siehe Git
  - Integrierte Cronjobs für regelmäßige Tasks (z.B. Audit-Log-Rotation)

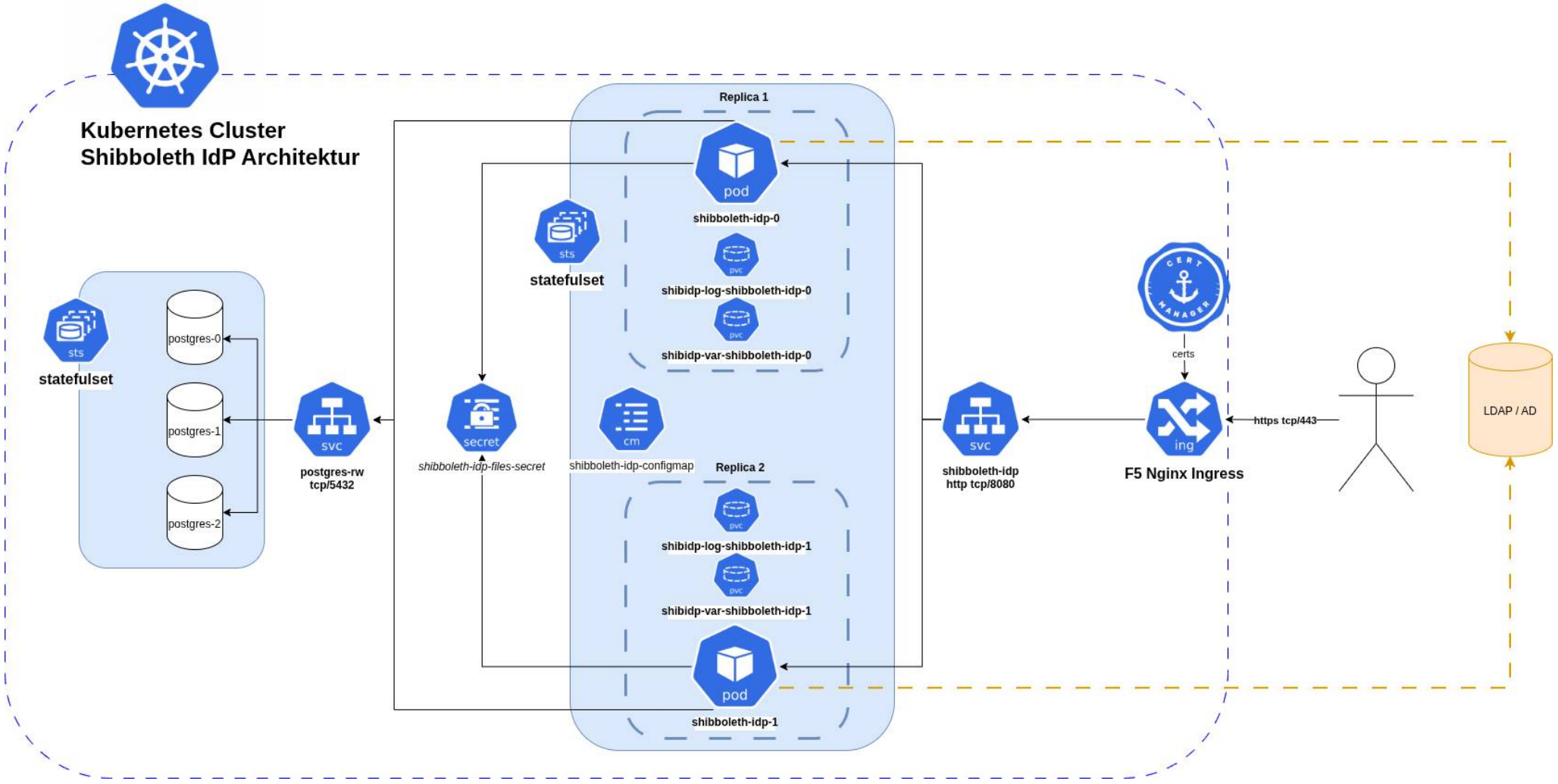
Shibboleth IdP & eduMFA in Kubernetes

- **K8s Deployment – Requirements**
  - Ingress / API Gateway → Zugang vom Internet
    - F5 NGINX Ingress Controller
    - APISIX API Gateway
  - certmanager → ACME-basierte Zertifikate (LE / Harica etc.)
  - Datenbank → extern oder im K8s Cluster
    - CloudNativePG (postgresql)
    - MariaDB Operator
    - Percona Operator (mysql)

Shibboleth IdP & eduMFA in Kubernetes

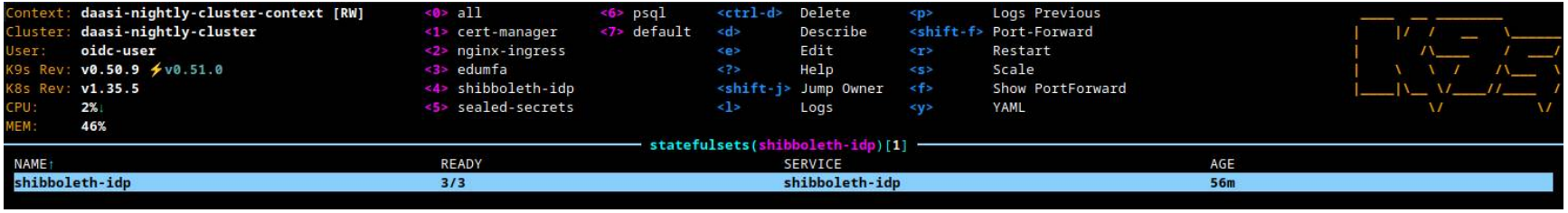
- **K8s Deployment – Requirements**
  - Secure Secrets → optional
    - HashiCorp Vault
    - Mozilla SOPS
    - (bitnami sealed-secrets)

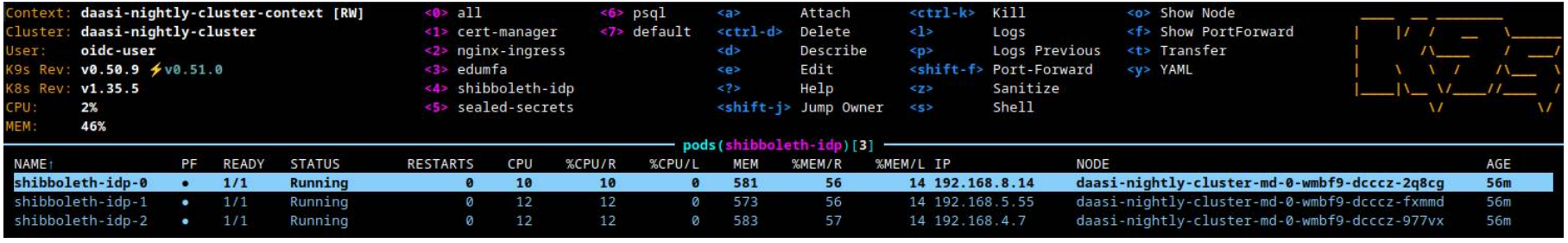
DAASI International


Kubernetes Cluster
Shibboleth IdP Architektur
Replica 1
pod
shibboleth-idp-0
sts
statefulset
pvc
shibidp-log-shibboleth-idp-0
pvc
shibidp-var-shibboleth-idp-0
sts
statefulset
postgres-0
postgres-1
postgres-2
svc
postgres-rw
tcp/5432
secret
shibboleth-idp-files-secret
cm
shibboleth-idp-configmap
Replica 2
pvc
shibidp-log-shibboleth-idp-1
pvc
shibidp-var-shibboleth-idp-1
pod
shibboleth-idp-1
svc
shibboleth-idp
http tcp/8080
CERT MANAGER
certs
ing
F5 Nginx Ingress
https tcp/443
LDAP / AD

Shibboleth IdP & eduMFA in Kubernetes

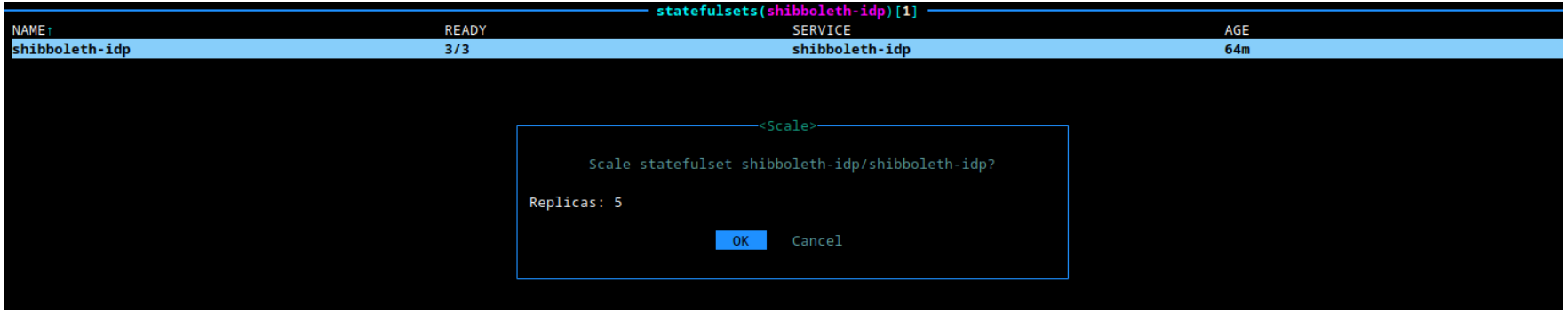
- **Shibboleth IdP in K9s**





Shibboleth IdP & eduMFA in Kubernetes

- **Shibboleth IdP in K9s**



Shibboleth IdP & eduMFA in Kubernetes

- **Shibboleth IdP in K9s**

pods(shibboleth-idp)[5]

NAME↑	PF	READY	STATUS	RESTARTS	CPU	%CPU/R	%CPU/L	MEM	%MEM/R	%MEM/L	IP	NODE	AGE
shibboleth-idp-0	•	1/1	Running	0	31	31	1	610	59	14	192.168.8.14	daasi-nightly-cluster-md-0-wmbf9-dcccz-2q8cg	68m
shibboleth-idp-1	•	1/1	Running	0	19	19	0	603	58	14	192.168.5.55	daasi-nightly-cluster-md-0-wmbf9-dcccz-fxmmd	68m
shibboleth-idp-2	•	1/1	Running	0	25	25	1	609	59	14	192.168.4.7	daasi-nightly-cluster-md-0-wmbf9-dcccz-977vx	68m
shibboleth-idp-3	•	0/1	Running	0	0	0	0	0	0	0	192.168.5.8	daasi-nightly-cluster-md-0-wmbf9-dcccz-fxmmd	16s
shibboleth-idp-4	•	0/1	Running	0	0	0	0	0	0	0	192.168.4.52	daasi-nightly-cluster-md-0-wmbf9-dcccz-977vx	16s

pods(shibboleth-idp)[5]

NAME↑	PF	READY	STATUS	RESTARTS	CPU	%CPU/R	%CPU/L	MEM	%MEM/R	%MEM/L	IP	NODE	AGE
shibboleth-idp-0	•	1/1	Running	0	10	10	0	591	57	14	192.168.8.14	daasi-nightly-cluster-md-0-wmbf9-dcccz-2q8cg	76m
shibboleth-idp-1	•	1/1	Running	0	10	10	0	584	57	14	192.168.5.55	daasi-nightly-cluster-md-0-wmbf9-dcccz-fxmmd	76m
shibboleth-idp-2	•	1/1	Running	0	12	12	0	588	57	14	192.168.4.7	daasi-nightly-cluster-md-0-wmbf9-dcccz-977vx	76m
shibboleth-idp-3	•	1/1	Running	0	18	18	0	2388	233	58	192.168.4.4	daasi-nightly-cluster-md-0-wmbf9-dcccz-977vx	2m39s
shibboleth-idp-4	•	1/1	Running	0	38	38	1	2173	212	53	192.168.5.52	daasi-nightly-cluster-md-0-wmbf9-dcccz-fxmmd	2m39s

Shibboleth IdP & eduMFA in Kubernetes

- **Shibboleth IdP in K9s - PVC**

persistentvolumeclaims(shibboleth-idp)[10]

NAME↑	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
shibidp-log-shibboleth-idp-0	Bound	pvc-3d007398-de29-4de6-8992-ca515bd979e2	5Gi	RWO	csi-cinder-sc-delete	69m
shibidp-log-shibboleth-idp-1	Bound	pvc-24d92397-1c00-4a64-9101-63dd7c6d9743	5Gi	RWO	csi-cinder-sc-delete	15h
shibidp-log-shibboleth-idp-2	Bound	pvc-53285436-0c94-4c34-a4b8-300a385e3380	5Gi	RWO	csi-cinder-sc-delete	69m
shibidp-log-shibboleth-idp-3	Bound	pvc-5945a16e-1412-42d7-a562-c0130825c274	5Gi	RWO	csi-cinder-sc-delete	2m13s
shibidp-log-shibboleth-idp-4	Bound	pvc-f20998d9-9c68-4a5b-b08e-90862d04d105	5Gi	RWO	csi-cinder-sc-delete	2m13s
shibidp-var-shibboleth-idp-0	Bound	pvc-dd039010-453c-4e7d-922f-de9f5d90d491	1Gi	RWO	csi-cinder-sc-delete	69m
shibidp-var-shibboleth-idp-1	Bound	pvc-96e236a6-5f89-4d4e-8342-7b377b72c2df	1Gi	RWO	csi-cinder-sc-delete	15h
shibidp-var-shibboleth-idp-2	Bound	pvc-f9b33c68-80c2-425d-9e93-bcb31a413efa	1Gi	RWO	csi-cinder-sc-delete	69m
shibidp-var-shibboleth-idp-3	Bound	pvc-06adec07-7d43-4a3a-872d-14e64769a78d	1Gi	RWO	csi-cinder-sc-delete	2m13s
shibidp-var-shibboleth-idp-4	Bound	pvc-fd6ff1de-a316-4147-85e9-65ee493c7558	1Gi	RWO	csi-cinder-sc-delete	2m13s

DAASI International

Shibboleth IdP & eduMFA in Kubernetes

- **Shibboleth IdP in K9s – Secrets**
  - Inhalt secrets.properties in K8s Secret:

```
Name:         shibboleth-idp-files-secret
Namespace:    shibboleth-idp
Labels:       app.kubernetes.io/managed-by=Helm
Annotations:  meta.helm.sh/release-name: shibboleth-idp
              meta.helm.sh/release-namespace: shibboleth-idp

Type:  Opaque

Data
====
sealerKeystore:     500 bytes
jwkEncryptionRSA:   1694 bytes
jwkSigningES:       239 bytes
sealerKver:         46 bytes
secrets:            860 bytes
jwkSigningRSA:      1695 bytes
ldapservercrt:      53 bytes
oidcClientSecrets:  29 bytes
saml2privKey:       2454 bytes
saml2pubKey:        1483 bytes
```

```
secrets: # Access to internal AES encryption key
idp.sealer.storePassword                    = CHANGEME
idp.sealer.keyPassword                      = CHANGEME

# Default access to LDAP authn
idp.authn.LDAP.bindDNCredential             = secret
idp.attribute.resolver.LDAP.bindDNCredential = %{idp.authn.LDAP.bindDNCredential:undefined}

# Salt used to generate persistent/pairwise
# IDs, must be kept secret
idp.persistentId.salt                       = CHANGEME

idp.persistentId.salt                       = CHANGEME
idp.oidc.subject.salt                       = CHANGEME
postgres.password                           = CHANGEME

fudiscr.edumfa.authorization_token          = CHANGEME
```


DAASI International

Shibboleth IdP & eduMFA in Kubernetes

- **Shibboleth IdP in K9s – Secrets**
  - Das „secrets“ Secret wird als Datei im statefulset gemountet

```
volumeMounts:
  - mountPath: /var/shibboleth-idp/credentials/secrets.properties
    name: {{ .Values.global.shibidp.name }}-files-secret
    subPath: secrets.properties
```

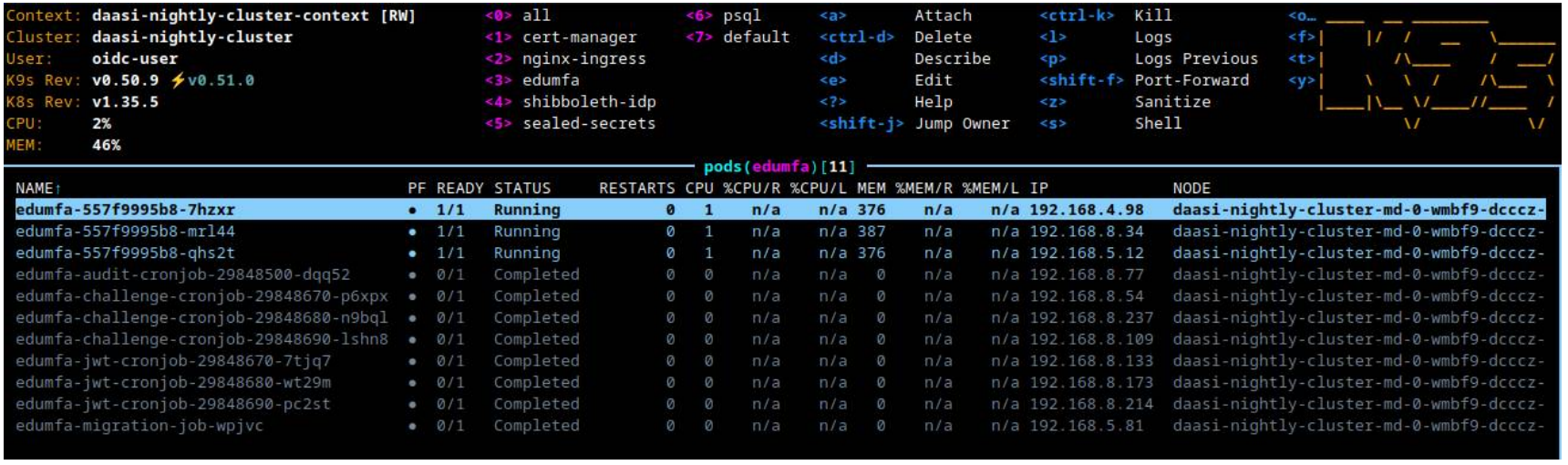
  - Und als Volume definiert

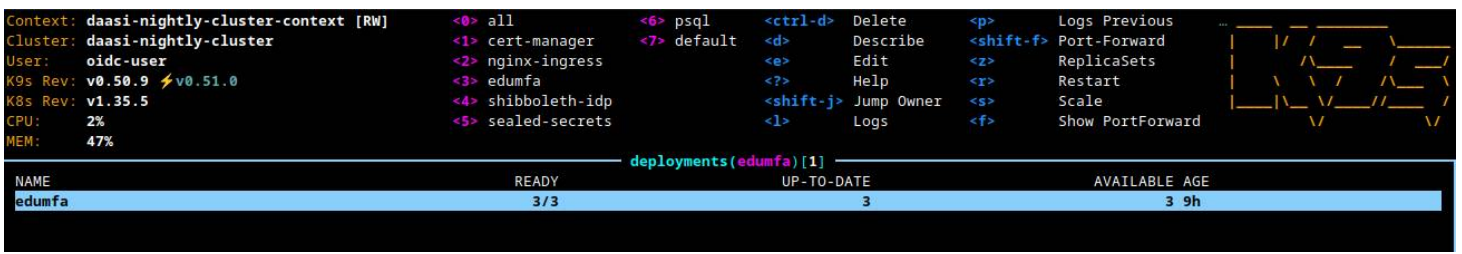
```
volumes:
  - name: {{ .Values.global.shibidp.name }}-files-secret
    secret:
      secretName: {{ .Values.global.shibidp.name }}-files-secret
      items:
      - key: "secrets"
        path: "secrets.properties"
```

  - /opt/shibboleth-idp/credentials verweist nach /var/shibboleth-idp/credentials
    → symlink im container

Shibboleth IdP & eduMFA in Kubernetes

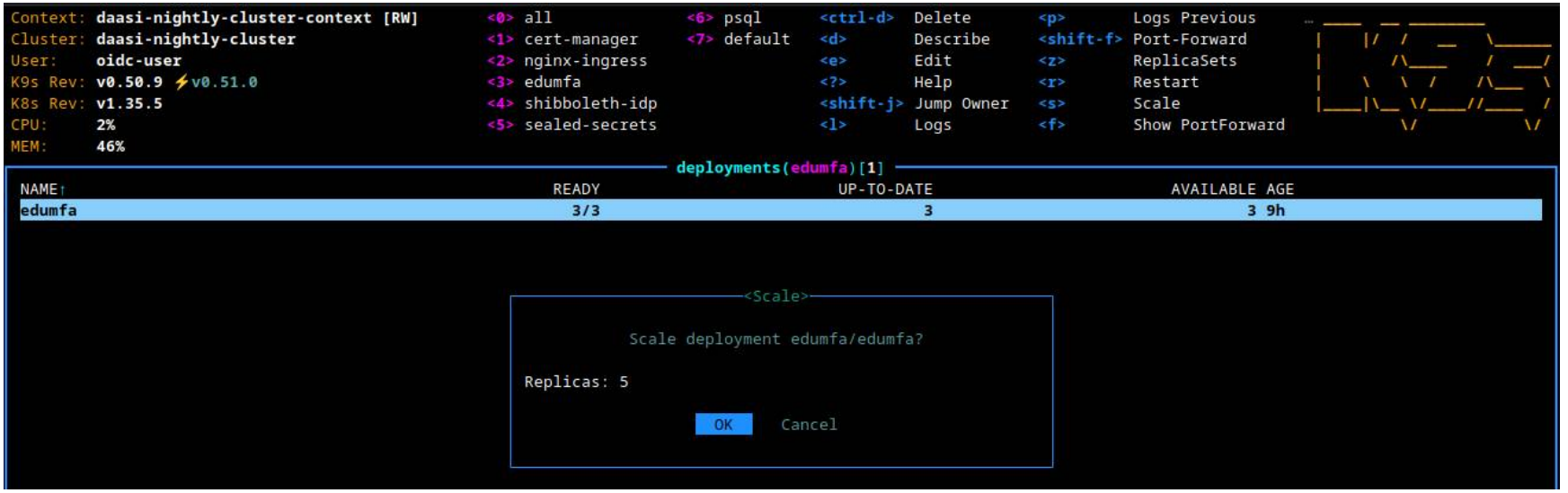
- eduMFA in K9s





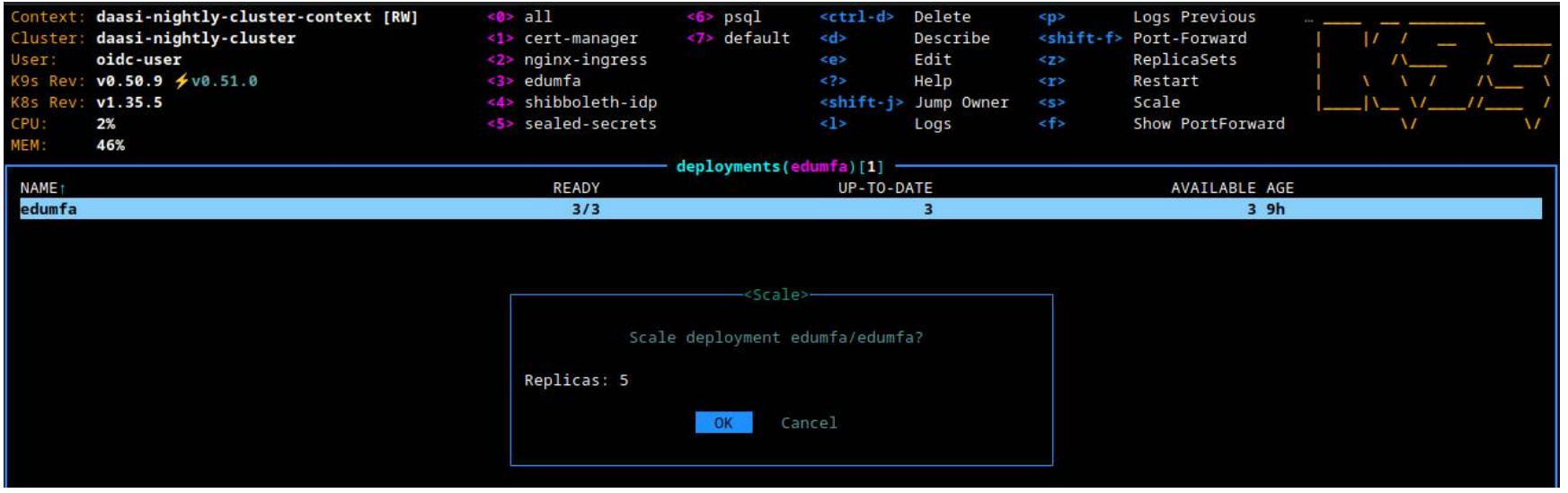
Shibboleth IdP & eduMFA in Kubernetes

- **eduMFA in K9s – manuelles Scaling**
  - Scaling von 3 → 5 Pods



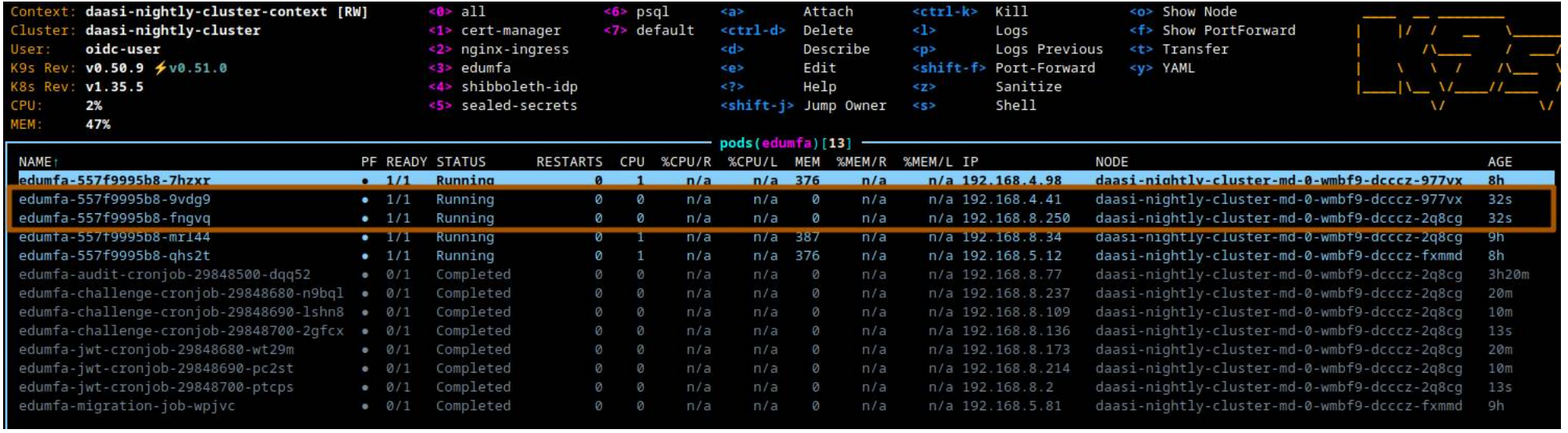
Shibboleth IdP & eduMFA in Kubernetes

- **eduMFA in K9s – manuelles Scaling**



Shibboleth IdP & eduMFA in Kubernetes

- **eduMFA in K9s – manuelles Scaling**



Shibboleth IdP & eduMFA in Kubernetes

- **eduMFA in K9s – Secrets**
  - Existierende secrets

secrets(edumfa)[7]

NAME↑	TYPE	DATA	AGE
edumfa-secrets	**Opaque**	**5**	**10h**
mfa-secret	Opaque	2	9h
mfa-tls	kubernetes.io/tls	2	9h

  - secrets defaults

```
Name:         edumfa-secrets
Namespace:    edumfa
Labels:       <none>
Annotations:  <none>

Type:  Opaque

Data
====
enckey:       96 bytes
pepper:       48 bytes
private.pem:  1675 bytes
public.pem:   451 bytes
secret_key:   48 bytes
```

  - secrets Erweiterung

```
Name:         mfa-secret
Namespace:    edumfa
Labels:       <none>
Annotations:  <none>

Type:  Opaque

Data
====
ADMIN_PASSWORD: secret
DB_PASSWORD: CHANGEME
```


DAASI International

Shibboleth IdP & eduMFA in Kubernetes

- **Fazit**
  - (+) Aufwandsarme Implementierung, insb. mit Docker-Compose
  - (+) Einfache Skalierung und Redundanz, insb. mit Kubernetes
  - (+) Versionierung, Rollbacks, Updates
  - (+) Weniger VM Maintenance
  - (+) / (-) Anderer Technologiestack im Vergleich zu VM-Deployment
  - (+) / (-) Schnelle Änderungen an der Config i.d.R. schlechter möglich
  - (-) Komplexität beim Debugging, insb. mit mehreren Replicas
  - (-) Deploymentmodell der Config & Secrets muss bedacht werden

DAASI International

Ausblick

Shibboleth IdP Image

- Credentials Initialisierung
  - Scriptbasierte Erstellung basierend auf Umgebungsvariablen
- IdP Config Initialisierung (optional)
  - Config aktuell losgelöst vom Image
  - Template-Basis
  - sed replacements basierend auf Umgebungsvariablen?
- URL-basierte Plugin Installation
  - inkl. Override-Option z.B. für fudiscr-beta Version Tests
- didmos-Plugin
  - Schnittstelle zum DAASI-eigenen didmos IAM per SCIM
- K8s Auto Scaling (Horizontal Pod Autoscaler)

DAASI International

Ausblick

eduMFA Image

- rootless Image
- Refactoring Image auf Basis Zendis hardened Images
- edumfa-radius standalone Image

Github: edumfa-radius

eduMFA Helm Chart

- Bis Release 2.10.0 noch flexibel änderbar: Feedback erwünscht
  → eduMFA Mailinglist
- User-Scripts (Import Policy etc.)
- User-defined-Cronjobs (Token Janitor f. Token Cleanup etc.)

DAASI International

Vielen Dank für die Aufmerksamkeit

DAASI International

Tel.: 07071 407109-0

E-Mail: info@daasi.de

Web: www.daasi.de

Fragen?

david.huebner@daasi.de

Shibboleth IdP:

pascal.koenig@daasi.de

eduMFA:

aleyna.nashertaher@daasi.de
edumfa-users@listserv.dfn.de