

2. HDF AAI Meeting -- Demo Slides

Steinbuch Centre for Computing
Marcus Hardt



Introduction

■ HDF Proposal:

- 6 Helmholtz Centres (AWI, DESY, DKFZ, FZJ, GSI, KIT), 10 M€/a
- Focus on **hardware**, to “satisfy the additional resource needs of a wide spectrum of scientific domains covering the Helmholtz research fields Energy, Earth and Environment, Health, Key Technologies and Matter”...
- ...“**data centres will be federated**”...
- ...“the federation is open and **extensible for additional data centres from Helmholtz, universities and other research institutions in Germany**”...
- ...“Links to European and international research data and supercomputing **infrastructures like EUDAT, EU-T0, WLCG, PRACE and NDS** will be established”...
- ...“**enable** a better **cooperation** of scientists in Germany with their **international colleagues and ESFRIs**”...

Goals

1. Extensible Federated Authentication and Authorisation Infrastructure
2. Compatible with international initiatives
3. Resources mainly in Germany, but international users

■ Derived / technical Goals:

1. Be in line with **European activities** focusing around the European Open Science Cloud **EOSC**
2. Enable the **participating centres to connect services** to federated infrastructure
 - Including non-web services
3. **Enable Principal Investigators / Virtual Organisations**
 - => **allocate resources** on behalf of their group
 - => **manage membership and authorisation** for their groups
4. Enable **global researchers** to use services provided by Centres
(Given they are properly authorized and their identity is adequately understood)
5. Ensure that **federated users are well known**, based on **solid authentication**
 - => **Policies**
6. Proof of Concept Demonstrator:
 - Example services
 - Deployment
7. Policies

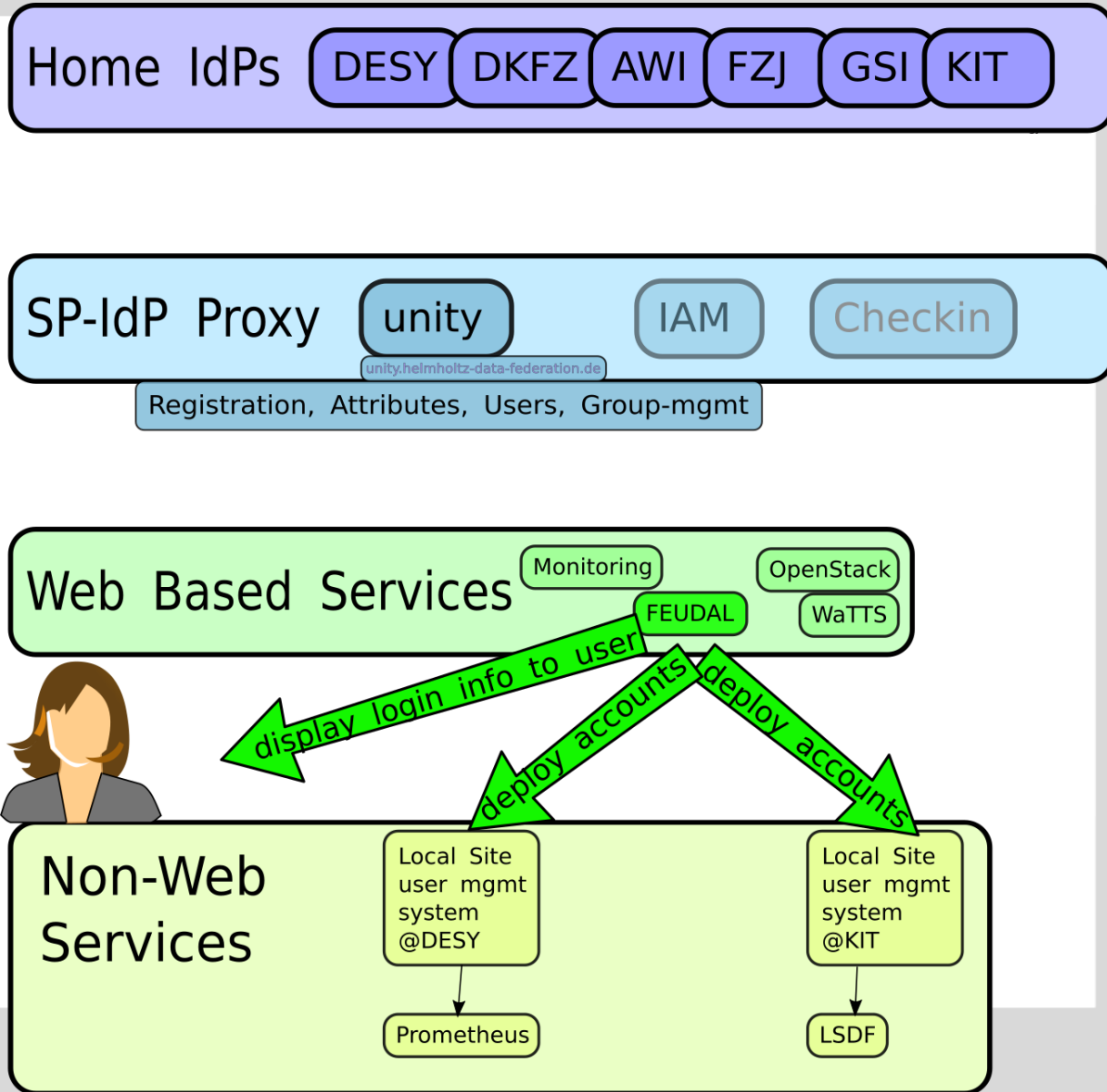
General Plan in HDF-AAI

- Unity is the SP-IdP-Proxy
 - <http://unity.helmholtz-data-federation.de>
- Use OIDC to integrate services
- Group based access control
 - Services filter access by group membership
- Delegated Group Management
 - E.g. Communities can self manage their membership
 - Centres can provide services for selected communities
- Delegated Authentication / Identity verification
 - **Services trust other centres to do their thing right**

Architecture

- Based on existing solutions
 - DFN-AAI Federation for IdPs (each HDF Partner already operates one)
 - Based on international developments: AARC Blueprint Architecture (BPA)
 - SP-IdP Proxy: Unity
- This allows
 - Users with home-account
 - Authenticate to
 - SAML services (Web-portals)
 - OpenID Connect services (Web, REST-APIs, Unicore-Grid)
 - X.509 services (EGI-Grid)
 - Commandline services (e.g. SSH)
 - Data Storage Services
 - All using Single Sign On (SSO)

Architecture model



Demos

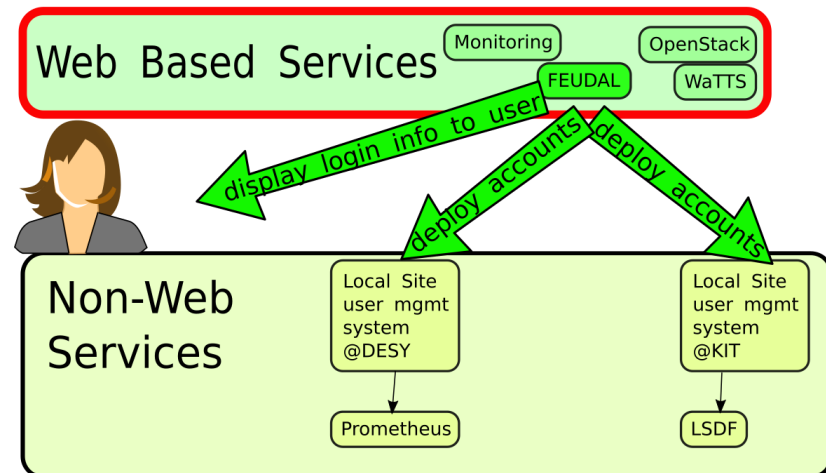
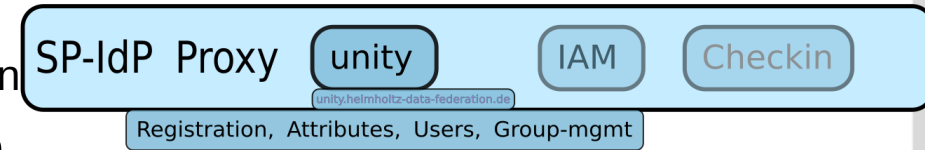
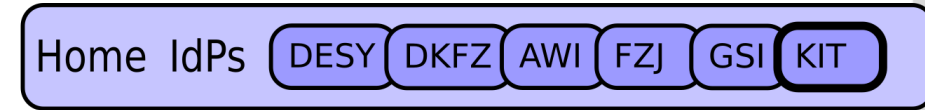
- Goals
 - Demonstrate current capabilities
 - Motivate additional services to make use of HDF AAI
- Demos
 - 1: Login for a known user
 - 2: Single sign on for additional services
 - 3: Access cmdline-based services
- Services that are available for demo:
 - Unity
 - Icinga Monitoring
 - WaTTS token translation
 - OpenStack
 - dCache / Prometheus
 - Adding users via FEUDAL
 - LSDF Storage

Demo – Login

■ Prerequisites

- User has a home-account in DFN-AAI
- User is already known to infrastructure
- User is member of the
“MyExampleCollab” Virtual Organisation

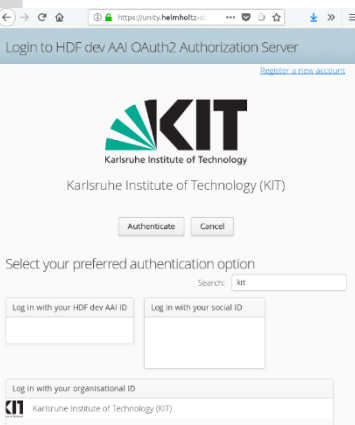
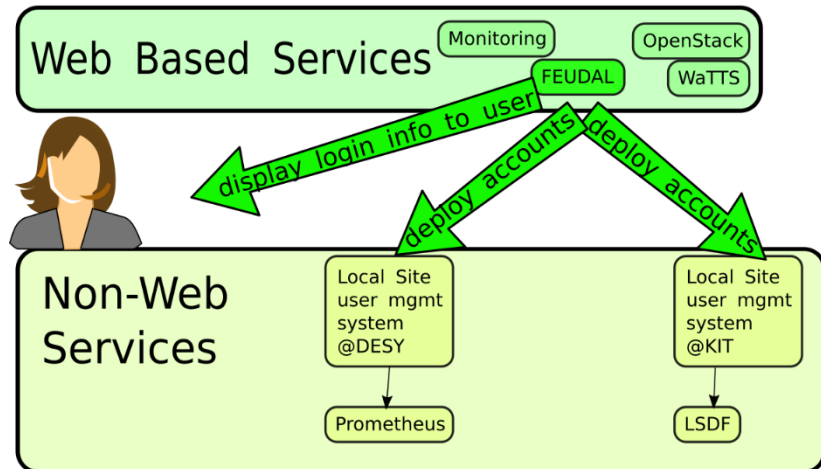
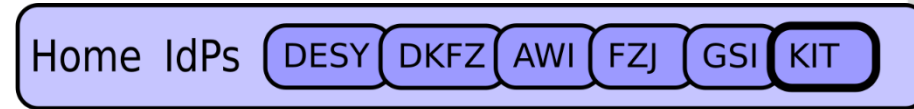
■ User goes to a service of his choice



Demo – Login

■ Prerequisites

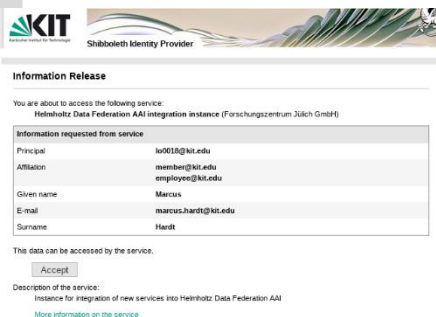
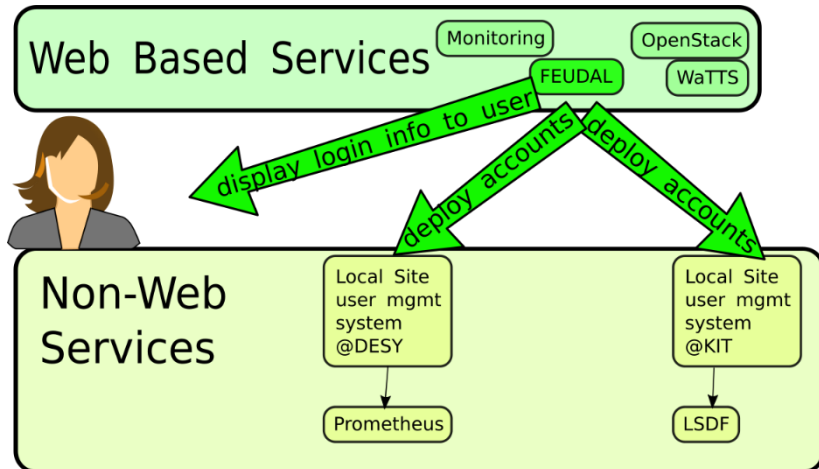
- User has a home-account in DFN-AAI
- User is already known to infrastructure
- User is member of the “MyExampleCollab” Virtual Organisation
- User goes to a service of his choice
- Service redirects user to unity
 - Choose home-IdP



Demo – Login

■ Prerequisites

- User has a home-account in DFN-AAI
- User is already known to infrastructure
- User is member of the “MyExampleCollab” Virtual Organisation
- User goes to a service of his choice
- Service redirects user to unity
- Choose home-IdP
- Unity redirects user to home-IdP



Demo – Login

■ Prerequisites

- User has a home-account in DFN-AAI
- User is already known to infrastructure
- User is member of the
“MyExampleCollab” Virtual Organisation

■ User goes to a service of his choice

■ Service redirects user to unity

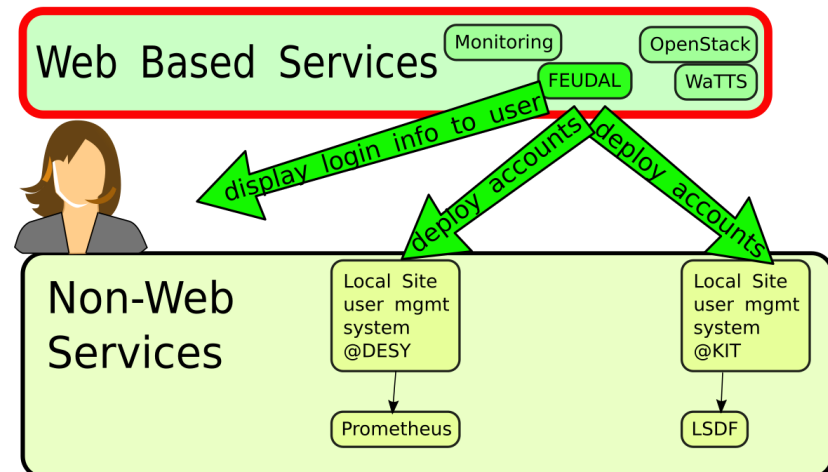
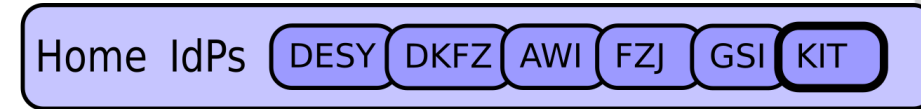
- Choose home-IdP

■ Unity redirects user to home-IdP

■ Double redirect

- Home-IdP => unity => service

=> User can use the service



Demo Single Sign On (SSO)

- Now we will use a different service...
- ...just a bit later on the same day

Demo – SSO

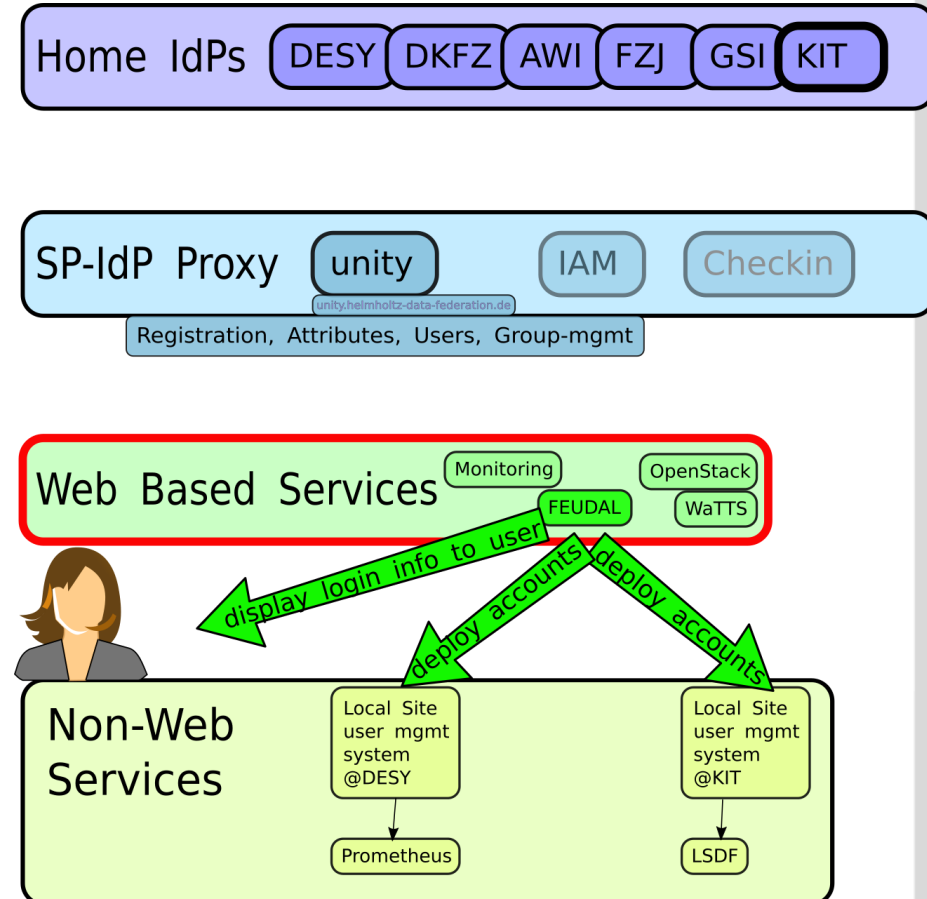
■ Prerequisites

- User was already logged in to another service (i.e. less than 4h ago)

■ User goes to a different service of his choice

- User chooses “HDF” to login
- Redirects happen quickly, in the background, without the user noticing
- Sessions live between 10min and 1h

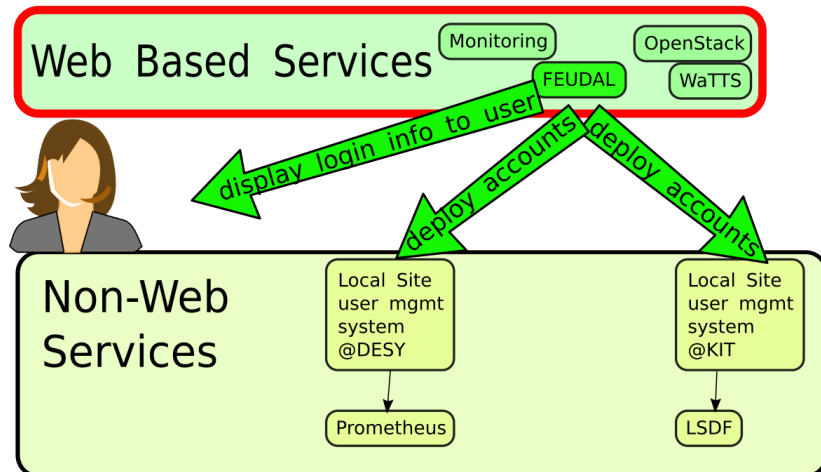
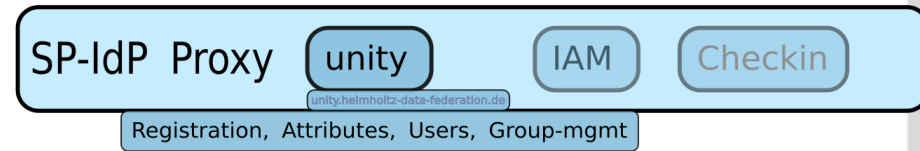
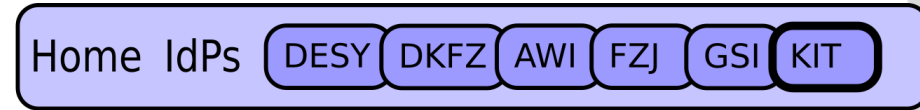
■ User is immediately logged in



Demo Commandline Based Services

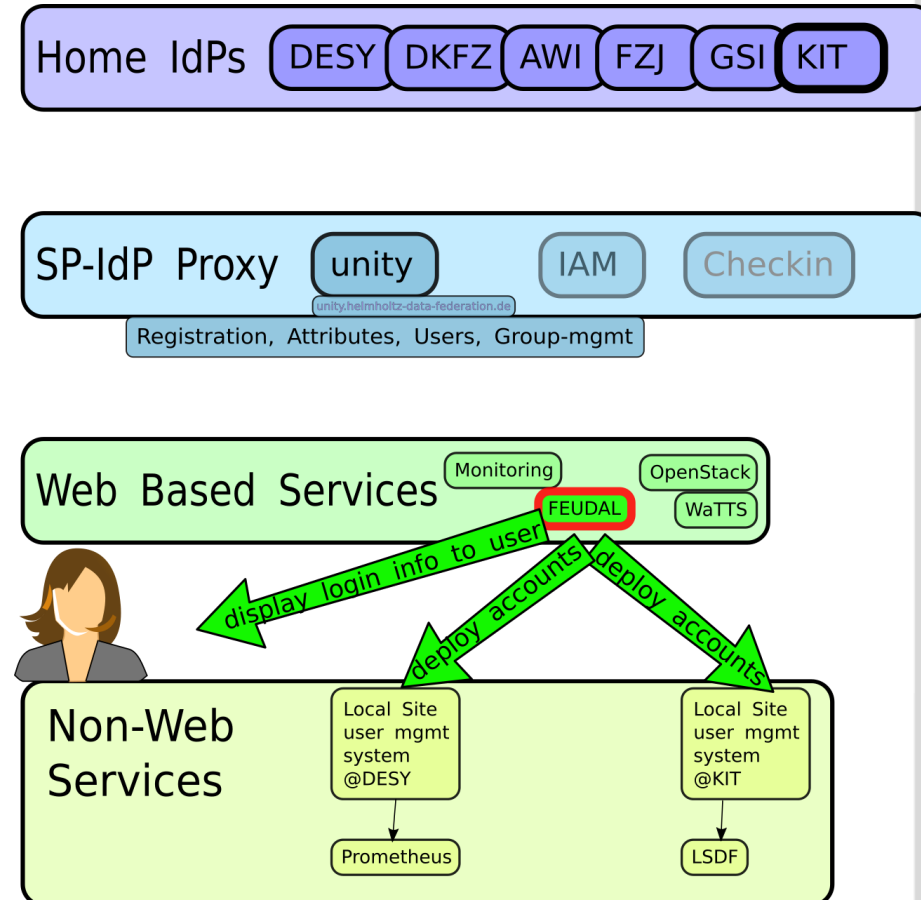
Demo – Services that require deployment

- Some services require deployment of a user account prior to the user logging in
 - Examples: ssh, prometheus
- User visits the “FEUDAL” service



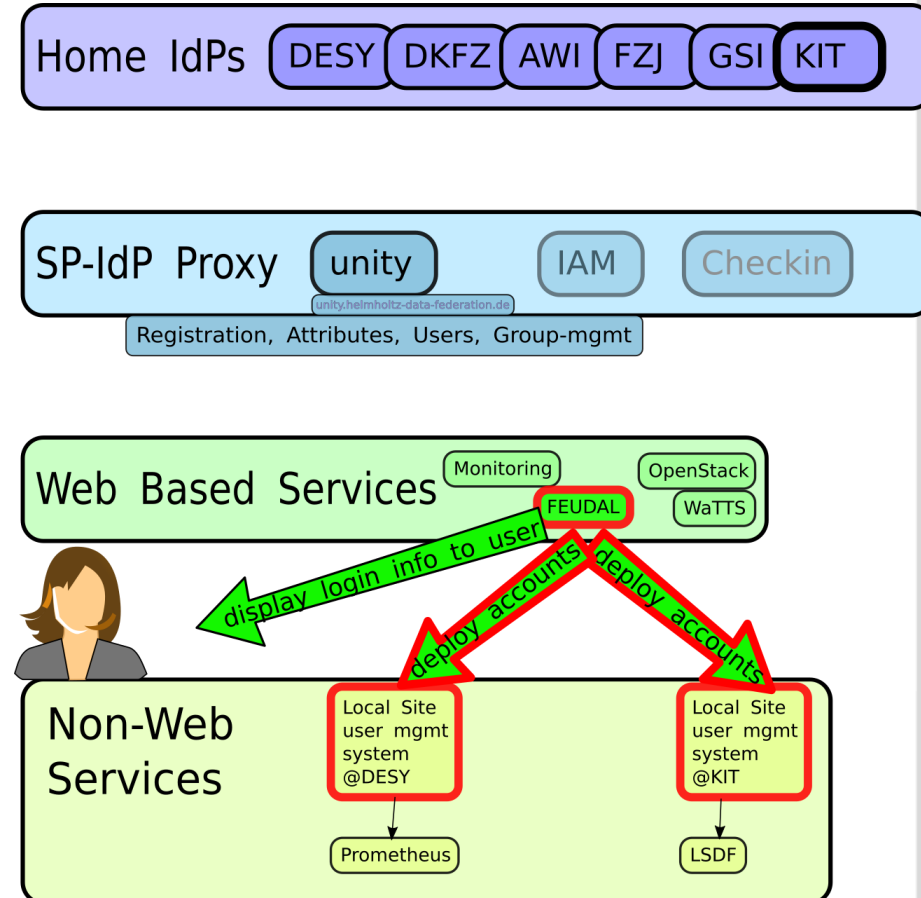
Demo – Services that require deployment

- Some services require deployment of a user account prior to the user logging in
 - Examples: ssh, prometheus
- User visits the “FEUDAL” service
 - Provides ssh-key as a credential
 - Chooses services (or VOs) to which he needs to be deployed



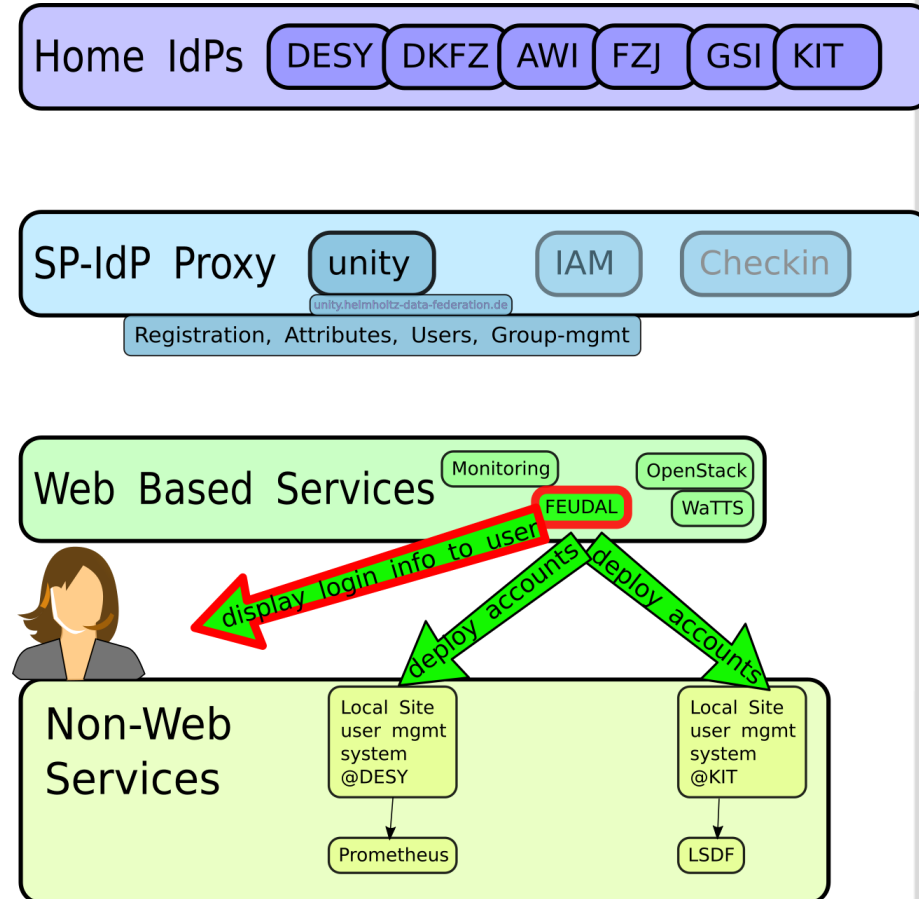
Demo – Services that require deployment

- Some services require deployment of a user account prior to the user logging in
 - Examples: ssh, prometheus
- User visits the “FEUDAL” service
 - Provides ssh-key as a credential
 - Chooses services (or VOs) to which he needs to be deployed
 - User account is deployed into site-local systems



Demo – Services that require deployment

- Some services require deployment of a user account prior to the user logging in
 - Examples: ssh, prometheus
- User visits the “FEUDAL” service
 - Provides ssh-key as a credential
 - Chooses services (or VOs) to which he needs to be deployed
 - User account is deployed into site-local systems
 - User is shown login information



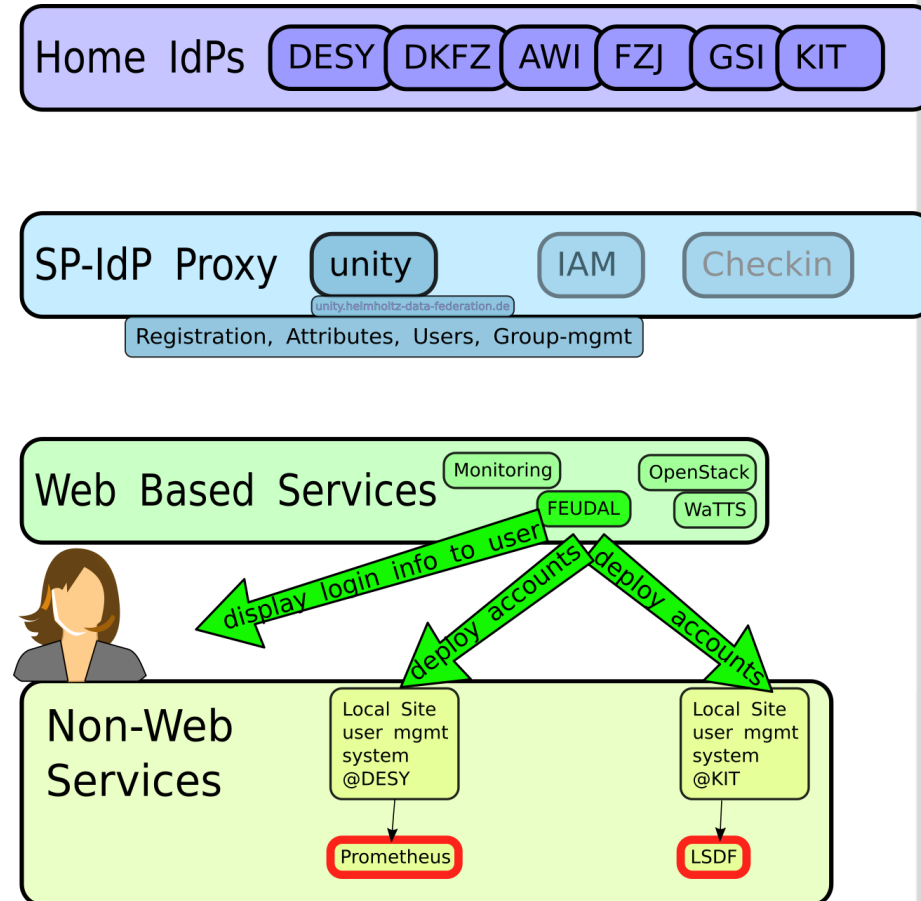
Demo – Services that require deployment

- Some services require deployment of a user account prior to the user logging in

- Examples: ssh, prometheus

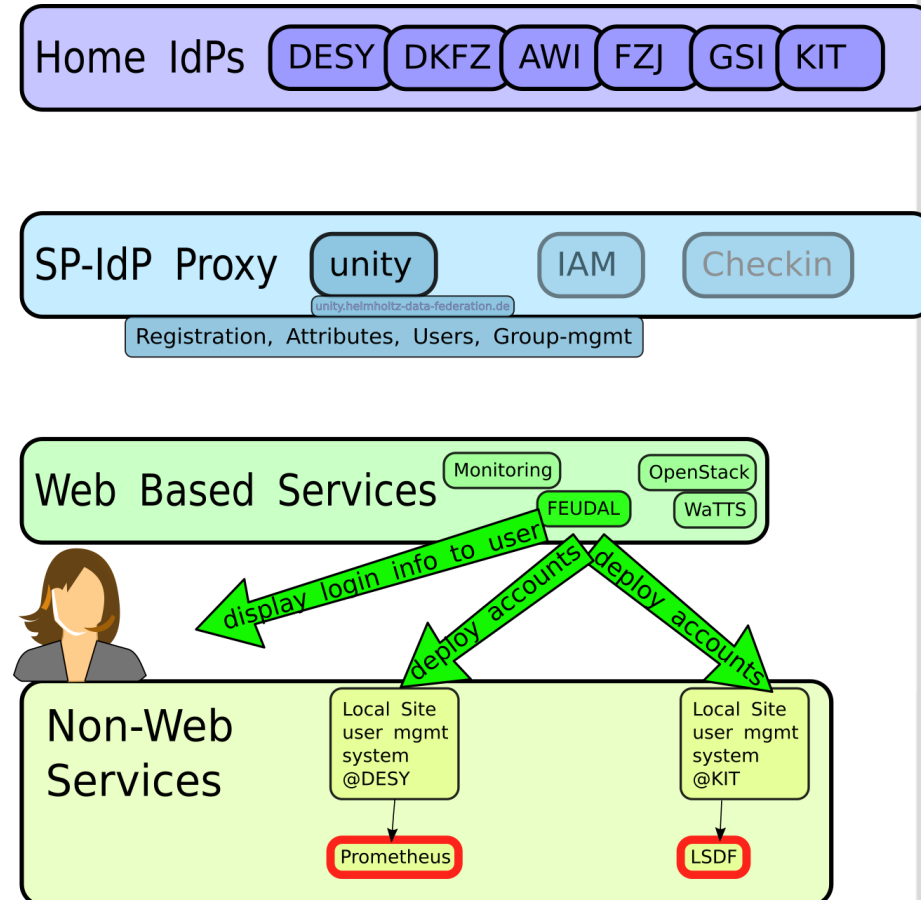
- User visits the “FEUDAL” service

- Provides ssh-key as a credential
 - Chooses services (or VOs) to which he needs to be deployed
 - User account is deployed into site-local systems
 - User is shown login information
 - User can login straight into the end service



Demo – Services that require deployment

- Some services require deployment of a user account prior to the user logging in
 - Examples: ssh, prometheus
- User visits the “FEUDAL” service
 - Provides ssh-key as a credential
 - Chooses services (or VOs) to which he needs to be deployed
 - User account is deployed into site-local systems
 - User is shown login information
 - User can login straight into the end service
- Deprovisioning
 - Remove user credentials (e.g. security incident, ...)



Additional Demos

- OpenStack
- WaTTS

Wrap Up

- HDF AAI Works:
 - Single Sign On
 - Web and non-web services
 - Virtual Organisation / 3rd party group management: in progress
 - A large range of services can be integrated
 - Policy framework is in place

- Future work:
 - Observe the uptake of the AAI Infrastructure
 - Observe the uptake of the policy framework
 - Additional (minor) developments:
 - Support for AAI in REST APIs
 - Enhanced support for cmdline
 - Extend VO management capabilities