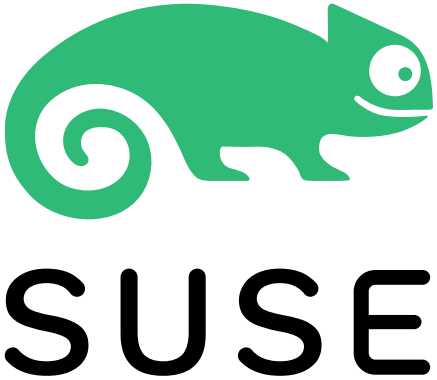

SUSE

SUSE

SUSEID

Open by design,
sovereign by choice



How did we get here?

A brief history of SUSE

Who is SUSE?

- Founded in 1992
- The first company to market Linux for enterprise
- SUSE was acquired by Novell in 2003
- Novell was acquired by the Attachmate Group in 2011
- Attachmate Group ~~merged with~~ was acquired by Microfocus in 2014
- In 2019 SUSE becomes an independent company.

Can you see the pattern?

SUSE

SUSE

But... who are you?

– Audience member

José Gómez

Full-stack Engineer

6-7 Years @ SUSE

- 5 Years in SUSE Customer Center
- 1 year SUSE IT Platform Engineering

In a nutshell:

SUSE

Disclaimer

Disclaimer

We’re not here to sell you any product (whether SUSE or not).

We will speak about how the organization is working towards a better IAM landscape.

The products in this presentation are mentioned without any marketing sponsorship involved.

SUSE

How did we get here?

Who is SUSE?

- Founded in 1992
- The first company to market Linux for enterprise
- SUSE was acquired by Novell in 2003
- Novell was acquired by the Attachmate Group in 2011
- Attachmate Group ~~merged with~~ was acquired by Microfocus in 2014
- In 2019 SUSE becomes an independent company.

Can you see the pattern?

SUSE

How did we get here?

The authentication roller coaster

- Multiple password providers:
  - $SaaS$
  - LDAP'ses
  - YP/NIS
- Multiple addons and bridges:
  - 2FA Addons
  - ActiveDirectory bridges/connector
  - LDAP-to-OIDC bridges
  - RADIUS servers

SUSE

How did we get here?

The authentication roller coaster

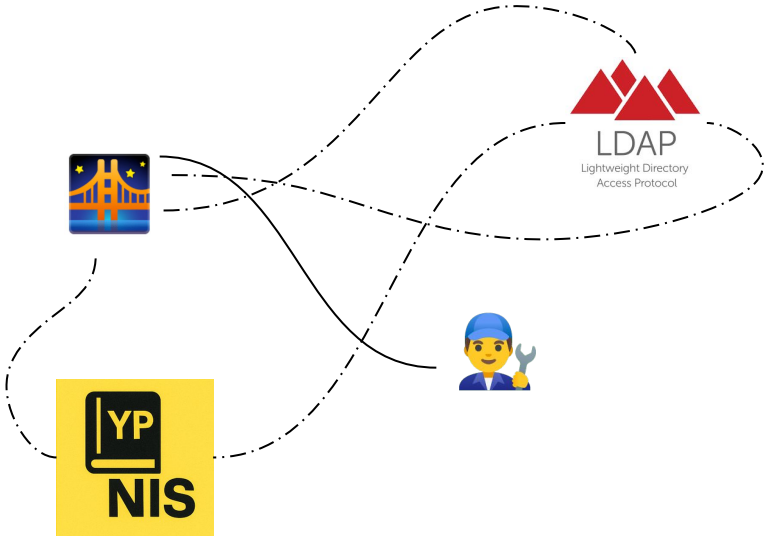
TL;DR:

How did we get here?

The authentication roller coaster

Why are we doing this?

- Authentication integrations across the company is not fully standardized.



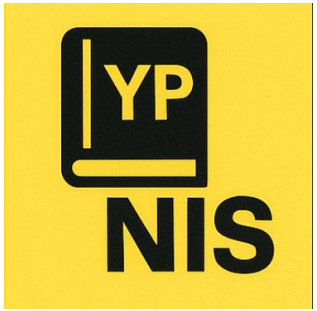
How did we get here?

Motivation

Why are we doing this?

- As of time of writing the vast majority of employees need at minimum two identities in order to work effectively.

$SaaS Product$



How did we get here?

Motivation

Security & Compliance Concerns

- Challenging Identity and Access Management (IAM) governance.
- Inconsistent MFA implementation.
- No standardized source of truth for identity and access.

How did we get here?

Motivation

Administration

- Multiple tools require manual changes for single requests

- Custom integrations increase the maintenance overhead.

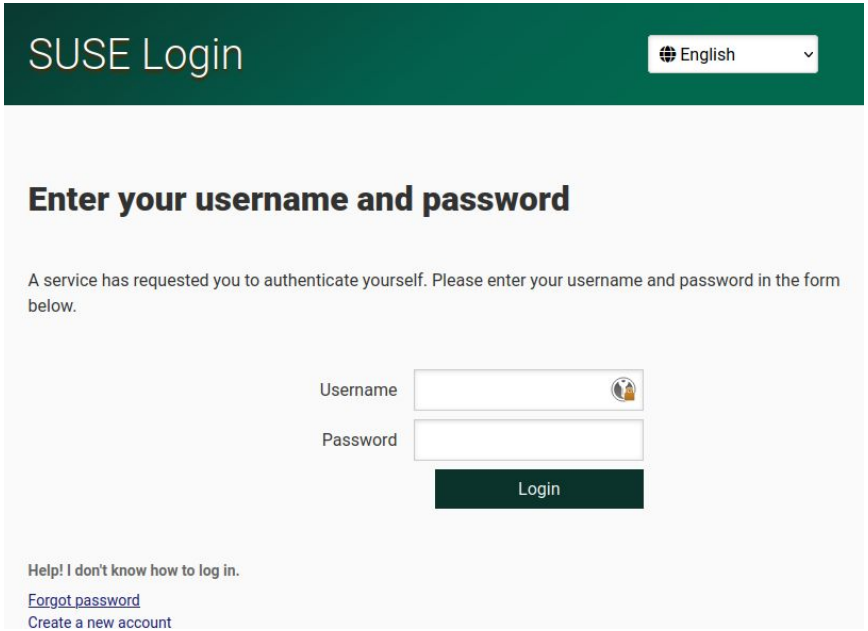
SUSE

The ride for an average SUSE Employee/Partner

The ride for an average SUSE Employee/Partner

Open JIRA

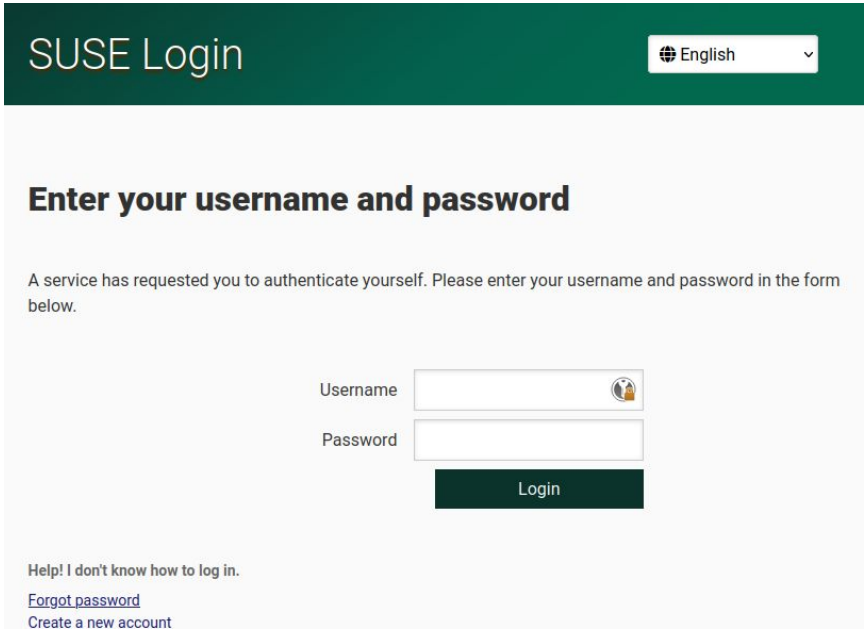
Authenticate...



The ride for an average SUSE Employee/Partner

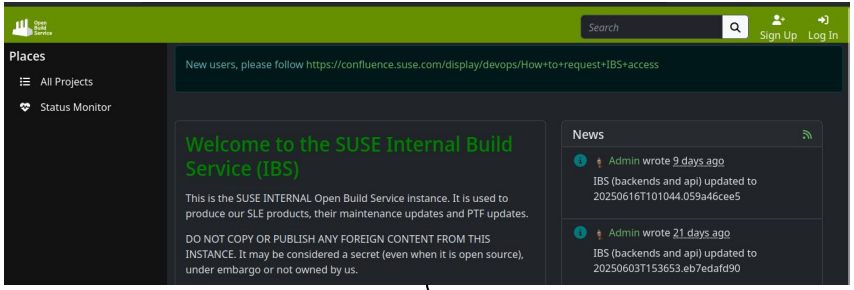
Open Confluence

Authenticate...

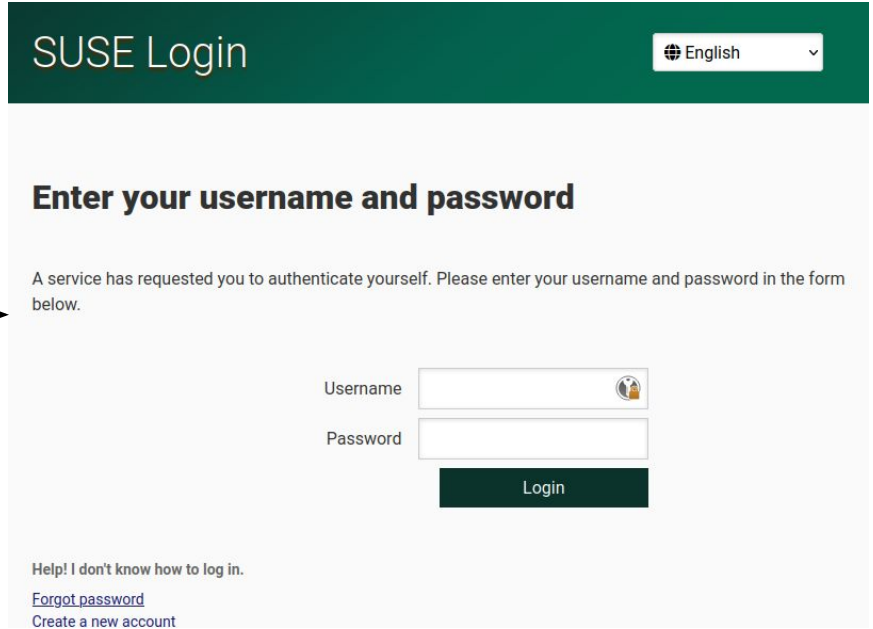


The ride for an average SUSE Employee/Partner

Open Internal Build Service

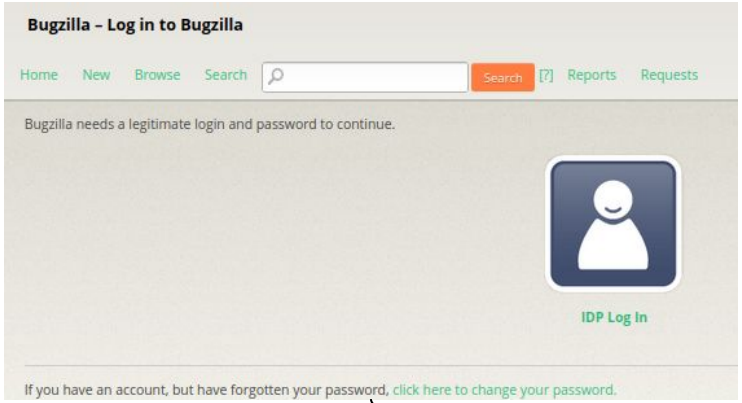


Authenticate...

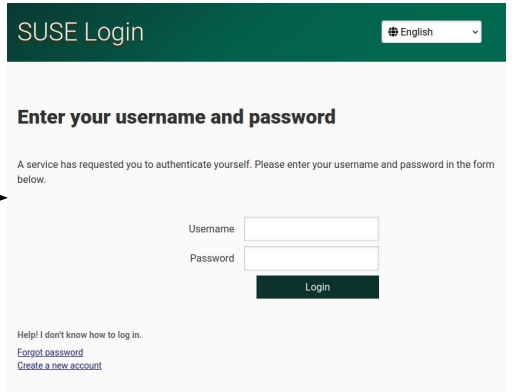


The ride for an average SUSE Employee/Partner

Bugzilla? Guess what?

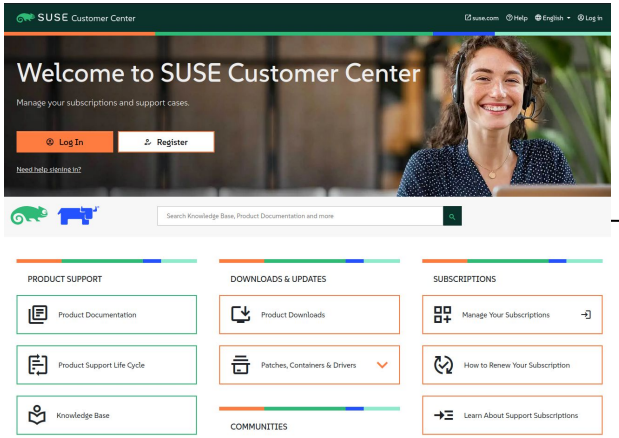


Authenticate...

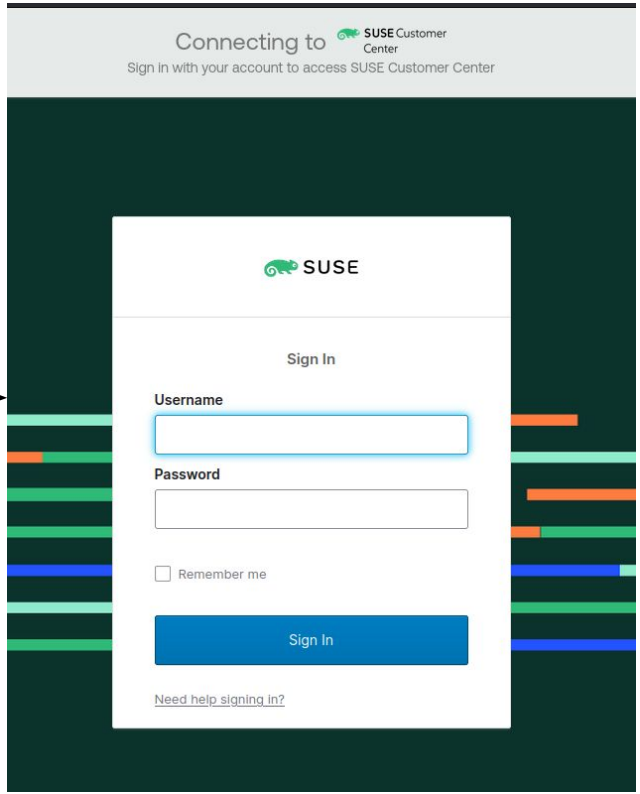


The ride for an average SUSE Employee/Partner

Wanna double check your subscriptions in SCC?

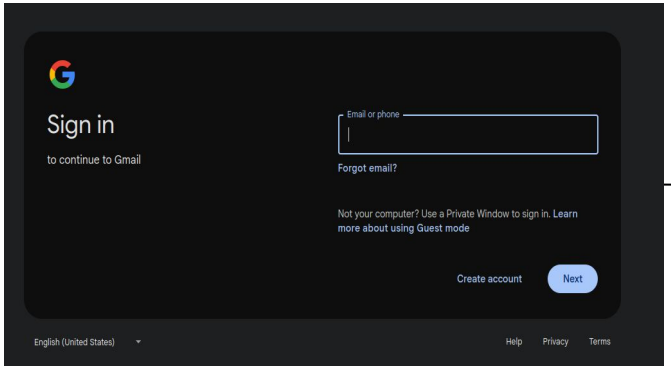


Authenticate...

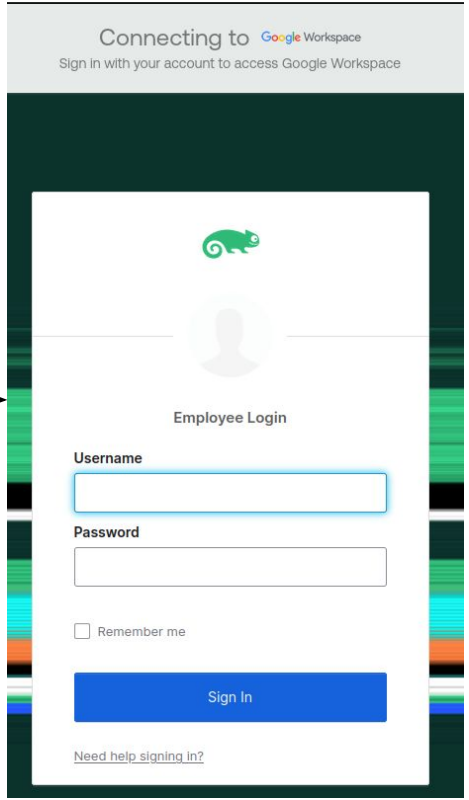


The ride for an average SUSE Employee/Partner

Corporate email?



Authenticate...



Our day-to-day summarized

Why not move it all to $yet another SaaS$ / $Cloud service$ / $Third Party Service Provider$?

– https://xkcd.com/927/

Why not move it all to $third party$?

Why not move it all to $third party$?

Security Compliance and Digital Sovereignty are our goals

Framework	Key Requirements
GDPR	✔ Data Protection by Design (Art. 25) ✔ Minimize 3rd-party processors (Art. 28) ✔ Data localization concerns
NIS2	✔ Risk-based access control and identity management (Art. 21) ✔ Supply chain security (Annex I)
DORA	✔ Secure and resilient Information and Communications Technology (ICT) Services ✔ In-house or contractually-bound IAM providers (Art. 5, 9, 10)

There’s always a catch

Security Compliance and Digital Sovereignty are our goals

- Self hosting will enable us to comply with more regulations, be in control of our data and be an exemplar of Digital Sovereignty.

- However *there ain't no such thing as a free lunch*. Every new solution comes with new problems.

SUSE

There's always a catch

Security Compliance and Digital Sovereignty are our goals

- At the expense of every benefit we'll get in the long term, we incur in new costs in the short term:
    - OPS
    - DC
    - Data handling
    - Security & Hardening
    - 24/7 SRE
    - Front-line support

SUSE

There’s always a catch

Security Compliance and Digital Sovereignty are our goals

- In our case:
  - ✅ We have multiple DCs and personnel for it
  - ✅ We have multiple departments with Support Crew
  - 🆕 Ops Staff (SRE)
  - 🆕 Data Handling
  - 🆕 Security & Hardening

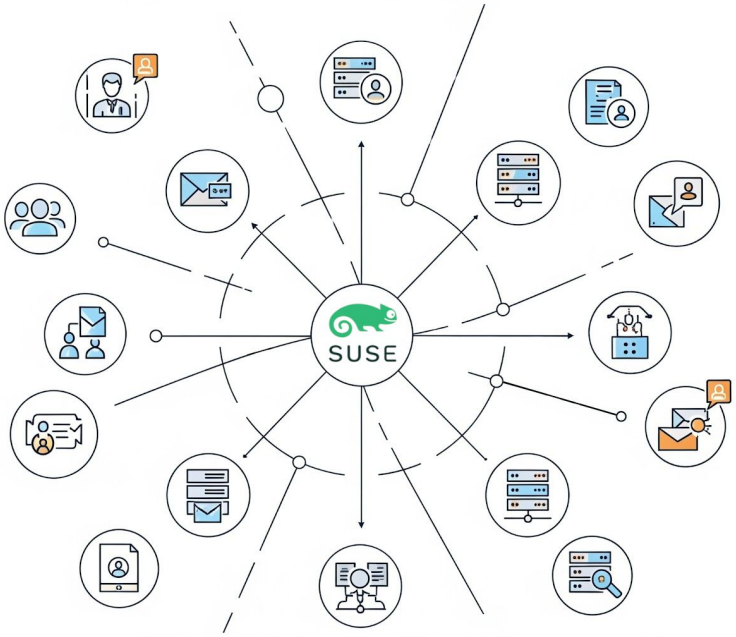
SUSE

Enough!

Show me the real diagrams, again

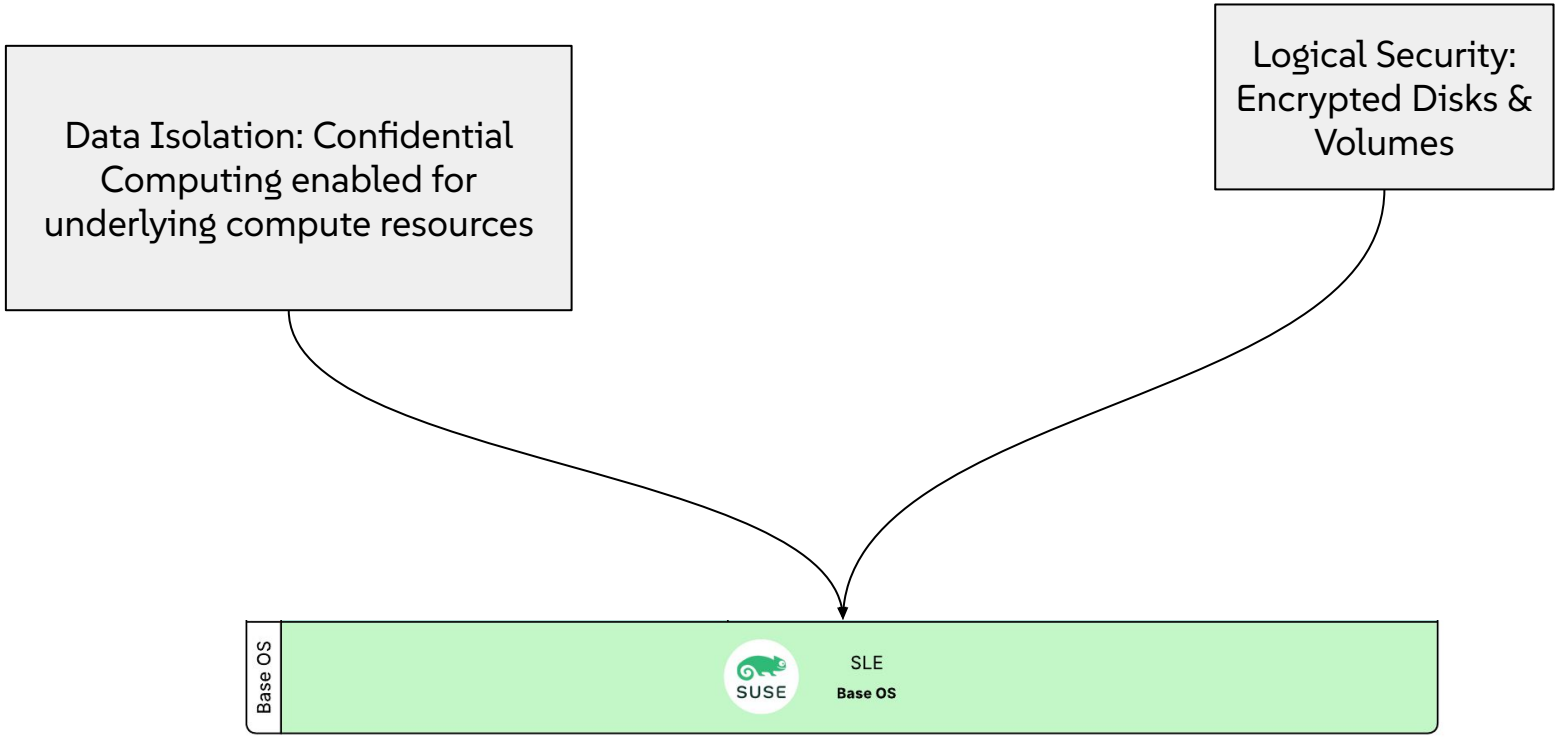
Architecture Overview

Our design goal



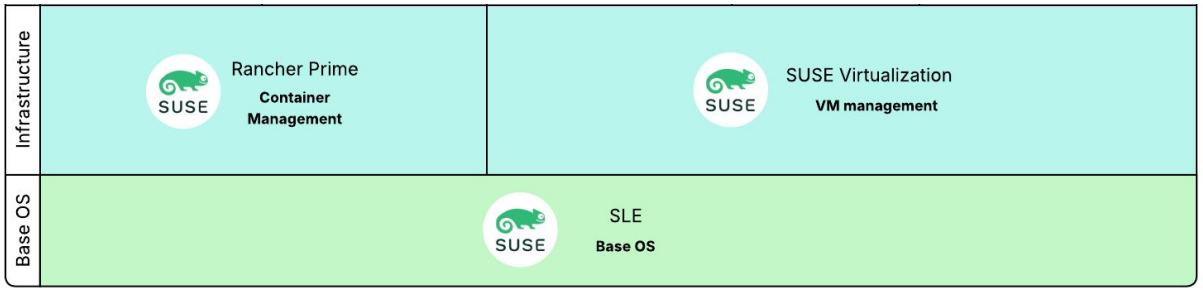
Architectural Overview

Software components



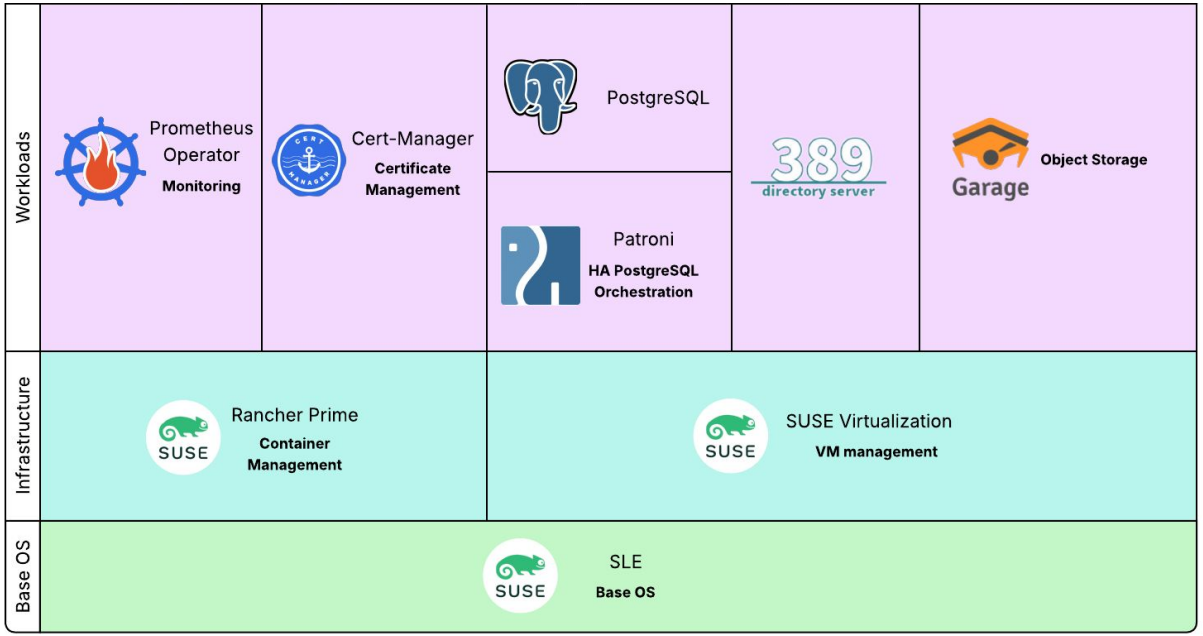
Architectural Overview

Software components



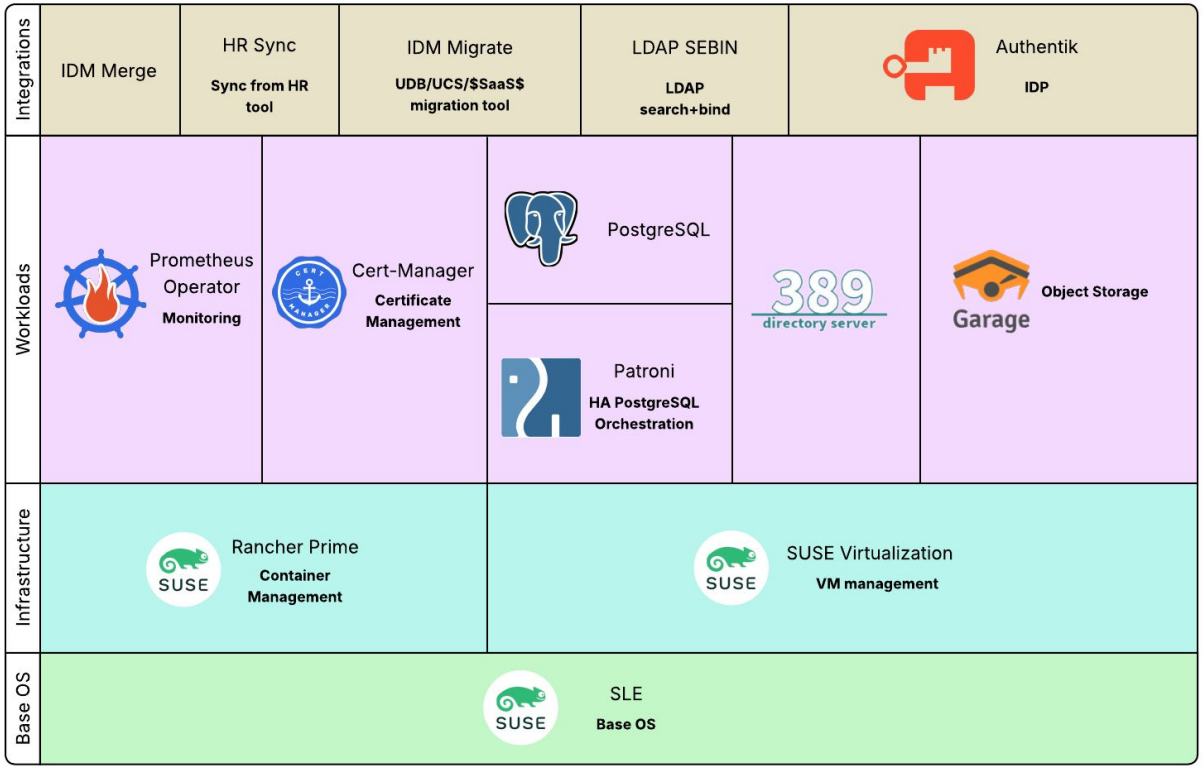
Architectural Overview

Software components



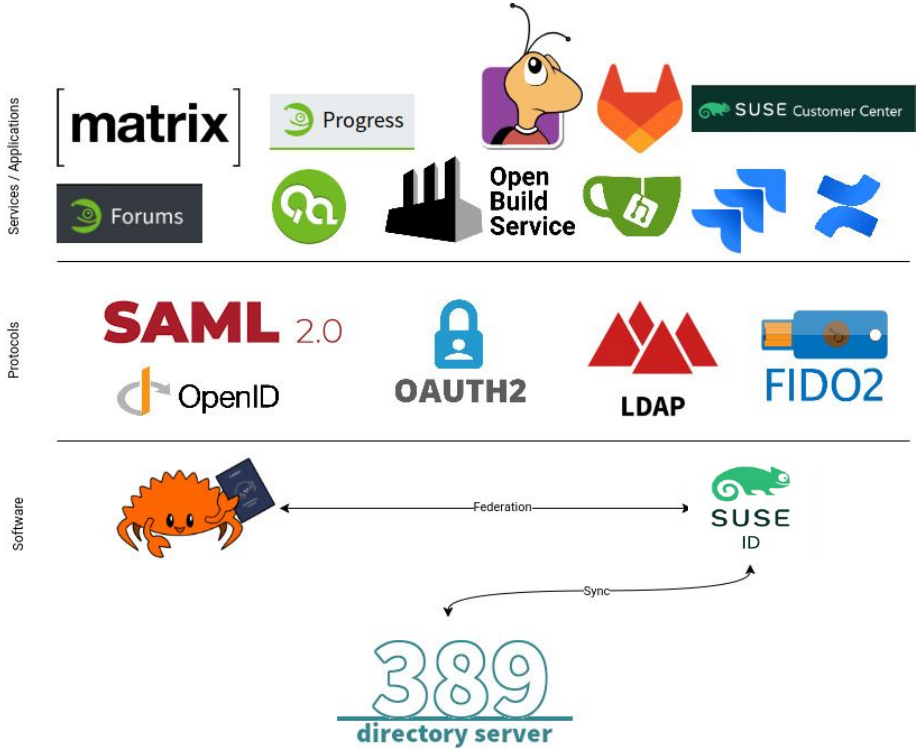
Architectural Overview

Software components



Architectural Overview

SUSEID + Community



OSS Contributions

Until today and still counting...

Existing projects:

- Authentik
- Saltstack
- smallstep/certificates
- Django-python-ldap
- KanIDM
- Podman-py
- go-ldap/ldif

New projects born during the project (to be public soon):

- Stepdance: Client Certificates made Easy
- LDAP SEBIN: LDAP **Se**arch+**Bin**d
- IDM Merge: Identity Aggregator & De-duplicator

Q&A


SUSE