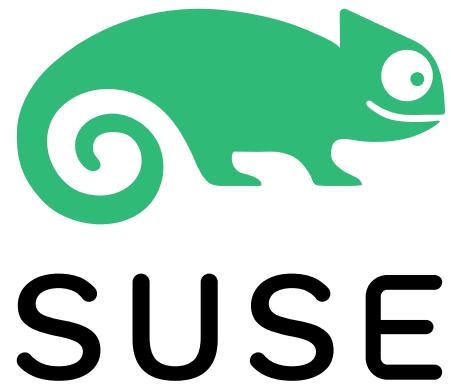


SUSE



SUSEID

Open by design,
sovereign by choice



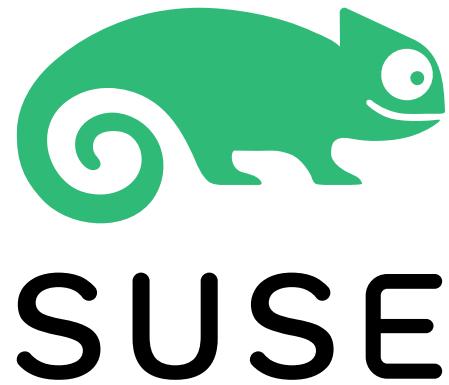
How did we get here?

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?



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:



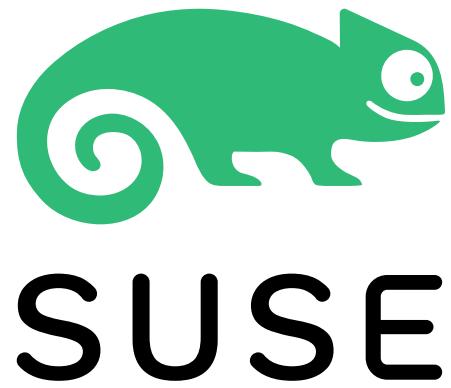
Disclaimer

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.



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?

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

How did we get here?

The authentication roller coaster

TL;DR:



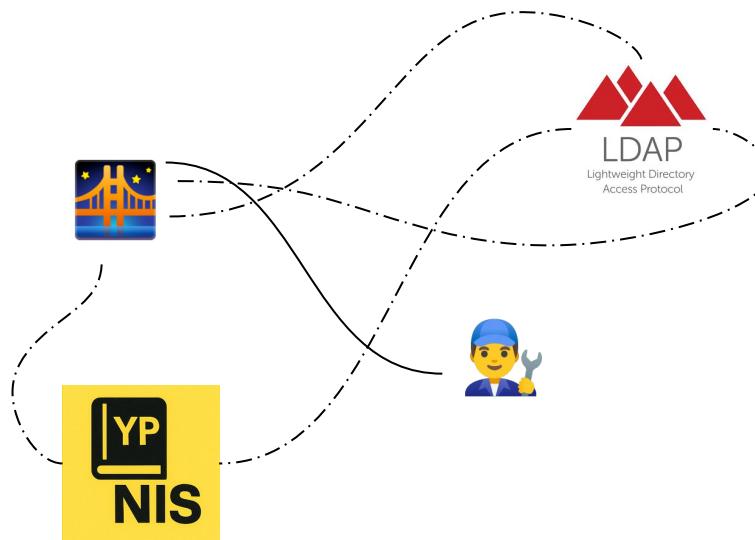
How did we get here?

The authentication roller coaster



Why are we doing this?

- Authentication integrations across the company is not fully standardized.



How did we get here?

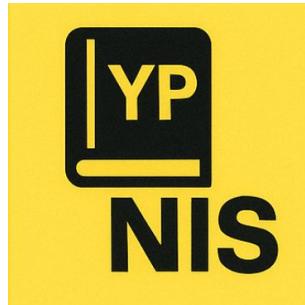
Motivation

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?

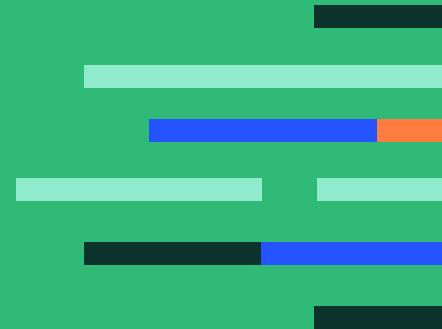
Motivation

Administration

- Multiple tools require manual changes for single requests
- Custom integrations increase the maintenance overhead.

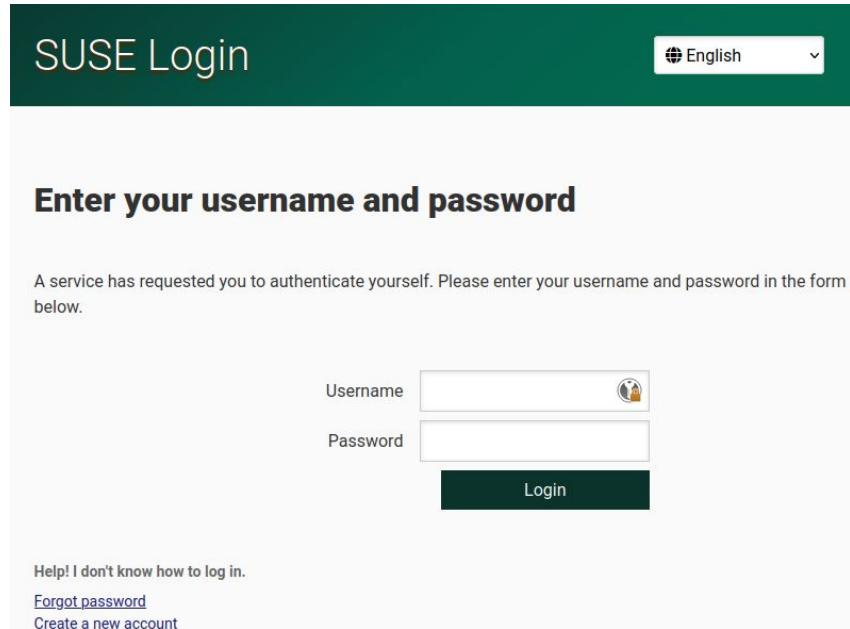


The ride for an average
SUSE Employee/Partner



The ride for an average SUSE Employee/Partner

[Open JIRA](#)



The screenshot shows the SUSE Login page. At the top, a dark green header bar displays the text "SUSE Login" on the left and a "English" dropdown menu on the right. The main content area has a light gray background. In the center, the text "Enter your username and password" is displayed in a bold, dark font. Below this, a message reads: "A service has requested you to authenticate yourself. Please enter your username and password in the form below." To the left of the form, the text "Authenticate..." is visible. The form itself consists of two input fields: "Username" and "Password", each with a small icon to its right. Below these fields is a dark green "Login" button. At the bottom of the page, there is a link "Help! I don't know how to log in.", a "Forgot password" link, and a "Create a new account" link.

SUSE Login

English

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Authenticate...

Username

Password

Login

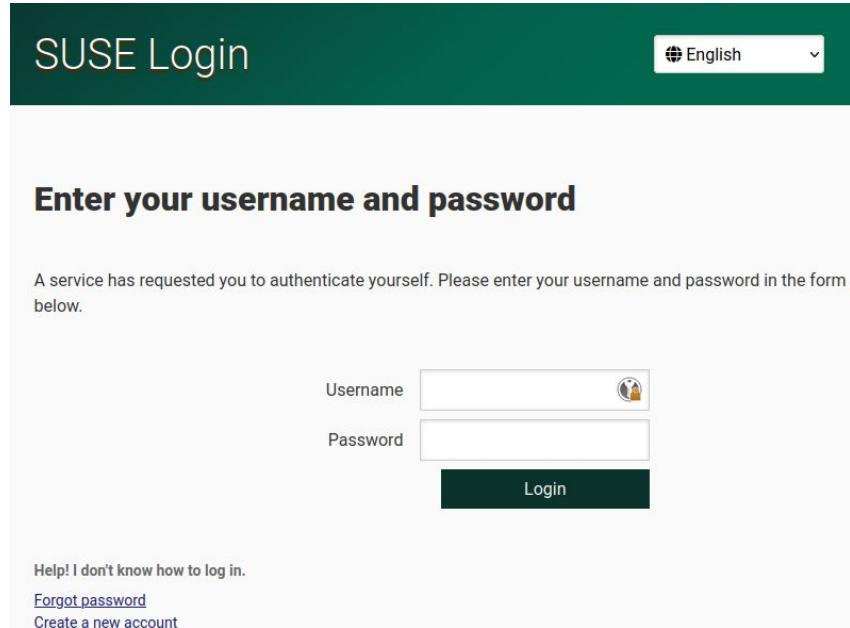
Help! I don't know how to log in.

[Forgot password](#)

[Create a new account](#)

The ride for an average SUSE Employee/Partner

[Open Confluence](#)



The screenshot shows the SUSE Login page. At the top, a dark green header bar displays the text "SUSE Login" on the left and a "English" dropdown menu on the right. The main content area has a light gray background. In the center, the text "Enter your username and password" is displayed in a bold, dark font. Below this, a message reads: "A service has requested you to authenticate yourself. Please enter your username and password in the form below." To the left of the form, the text "Authenticate..." is visible. The form itself consists of two input fields: "Username" and "Password", each with a small icon to its right. Below these fields is a dark green "Login" button. At the bottom of the page, there is a link "Help! I don't know how to log in.", a "Forgot password" link, and a "Create a new account" link.

SUSE Login

English

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Authenticate...

Username

Password

Login

Help! I don't know how to log in.

[Forgot password](#)

[Create a new account](#)

The ride for an average SUSE Employee/Partner

Open Internal Build Service



Welcome to the SUSE Internal Build Service (IBS)

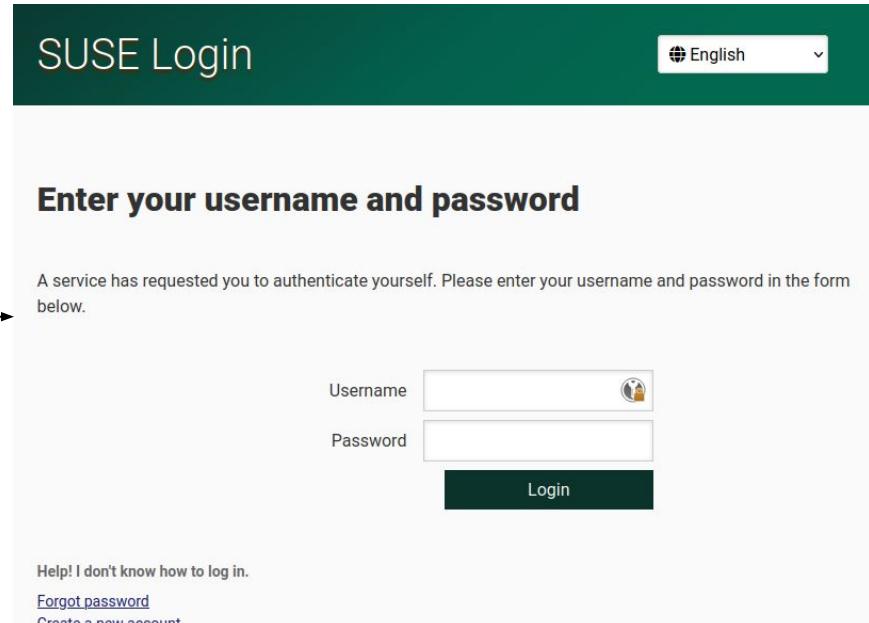
This is the SUSE INTERNAL Open Build Service instance. It is used to produce our SLE products, their maintenance updates and PTF updates.

DO NOT COPY OR PUBLISH ANY FOREIGN CONTENT FROM THIS INSTANCE. It may be considered a secret (even when it is open source), under embargo or not owned by us.

News

- Admin wrote 9 days ago
IBS (backends and api) updated to 20250616T101044.059a46cee5
- Admin wrote 21 days ago
IBS (backends and api) updated to 20250603T153653.eb7edad90

Authenticate...



SUSE Login

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username

Password

Login

Help! I don't know how to log in.
[Forgot password](#)
[Create a new account](#)

The ride for an average SUSE Employee/Partner

Bugzilla? Guess what?

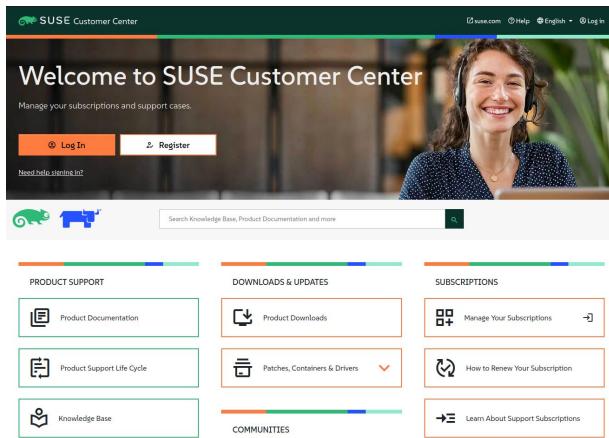


Authenticate...

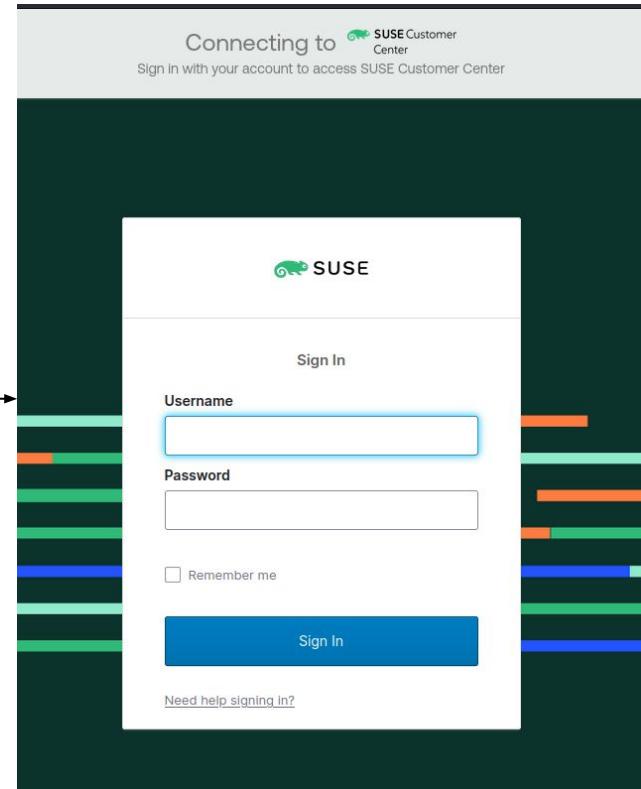
A screenshot of the SUSE Login page. The title bar says "SUSE Login" and has a language dropdown set to "English". Below it is a section titled "Enter your username and password". A message says "A service has requested you to authenticate yourself. Please enter your username and password in the form below." There are two input fields: "Username" and "Password", and a "Login" button. At the bottom, there are links for "Help! I don't know how to log in.", "Forgot password?", and "Create a new account".

The ride for an average SUSE Employee/Partner

Wanna double check your subscriptions in SCC?

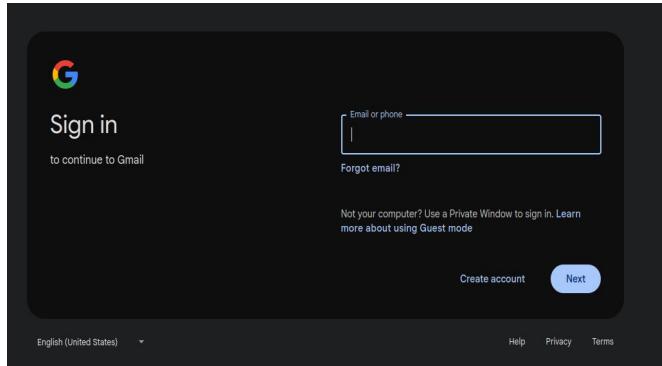


Authenticate...

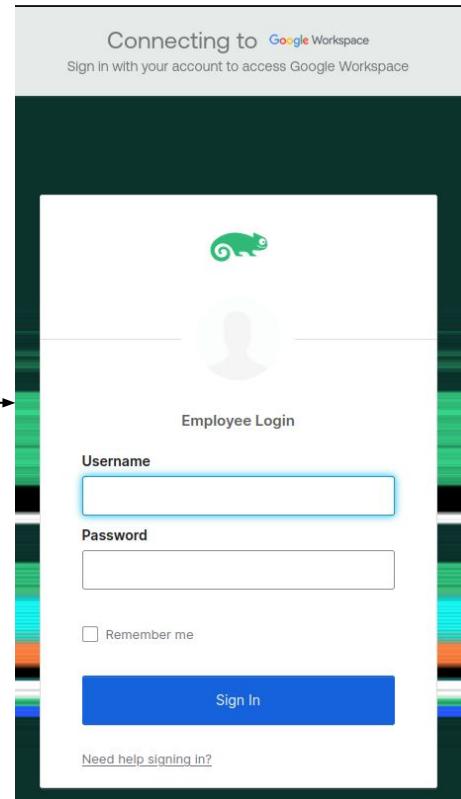


The ride for an average SUSE Employee/Partner

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	<ul style="list-style-type: none">✓ Data Protection by Design (Art. 25)✓ Minimize 3rd-party processors (Art. 28)✓ Data localization concerns
NIS2	<ul style="list-style-type: none">✓ Risk-based access control and identity management (Art. 21)✓ Supply chain security (Annex I)
DORA	<ul style="list-style-type: none">✓ 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.

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

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
 - NEW Ops Staff (SRE)
 - NEW Data Handling
 - NEW Security & Hardening

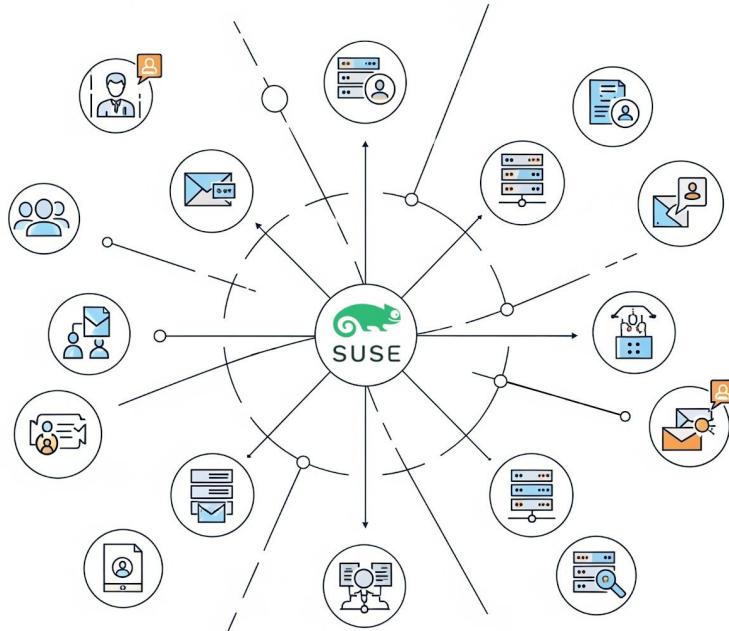


Enough!

Show me the real diagrams, again

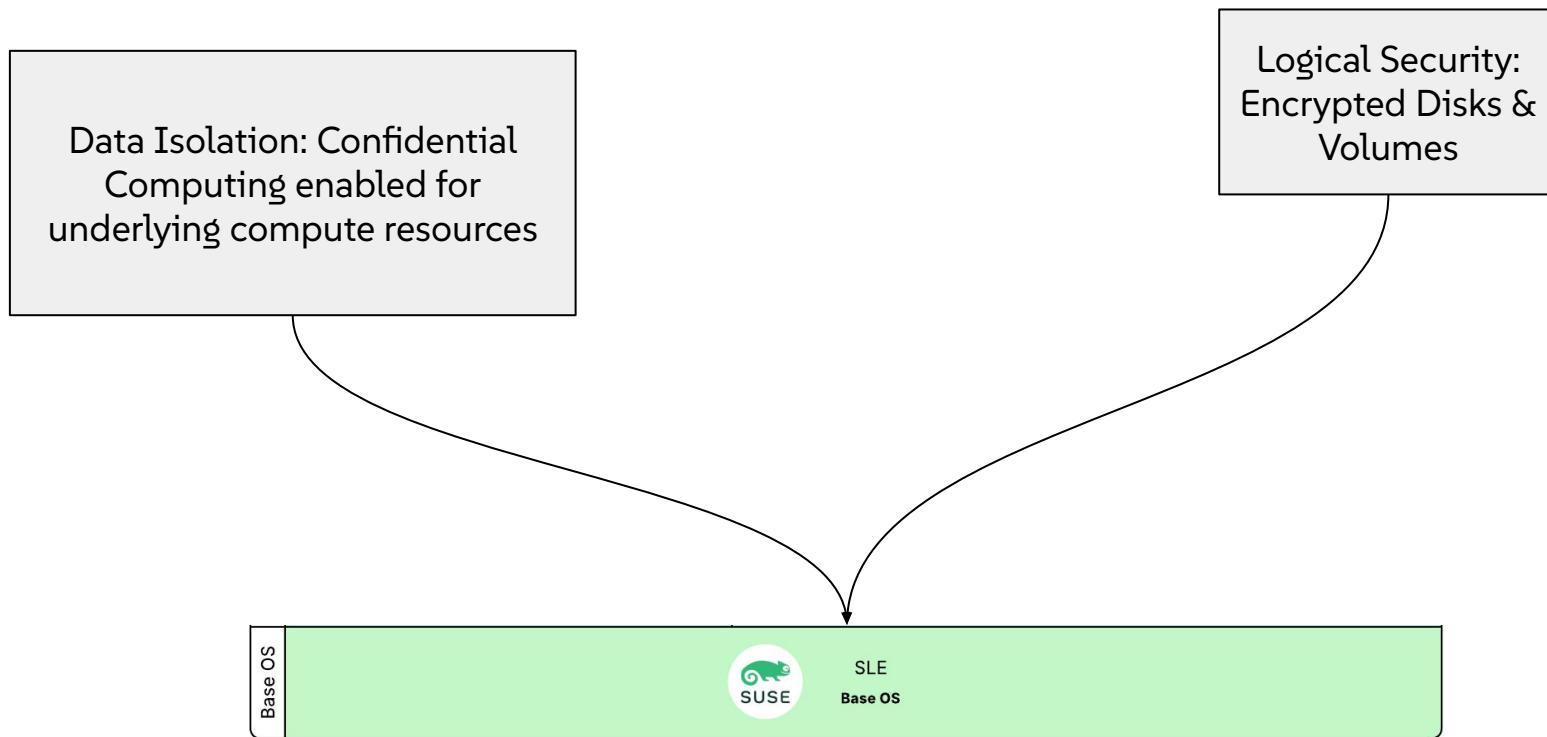
Architecture Overview

Our design goal



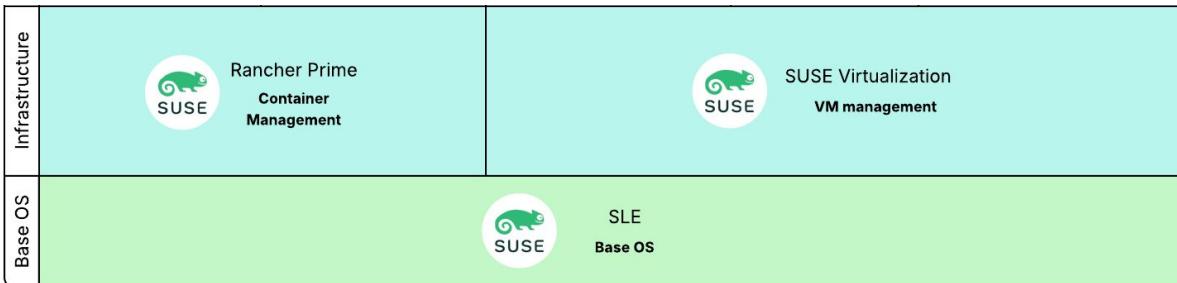
Architectural Overview

Software components



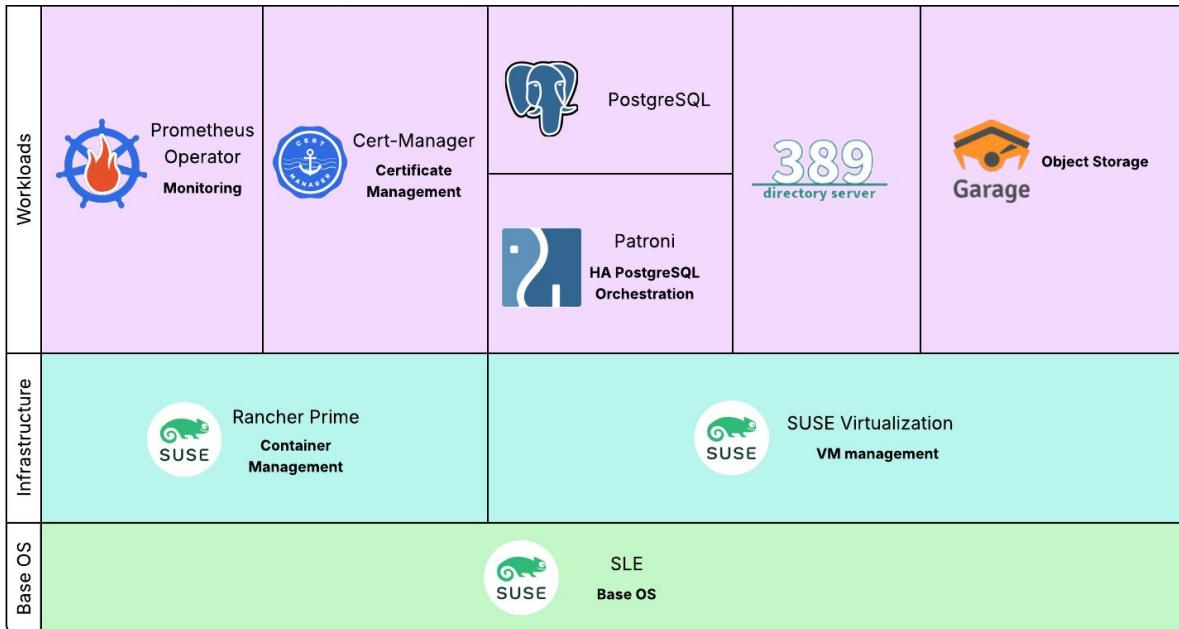
Architectural Overview

Software components



Architectural Overview

Software components



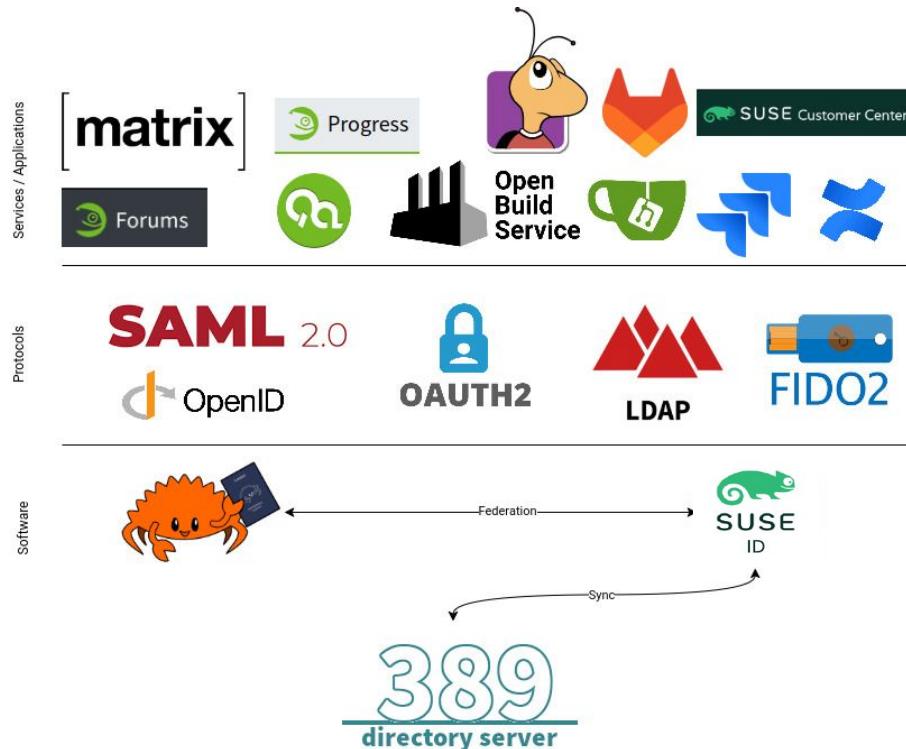
Architectural Overview

Software components

Integrations	IDM Merge Sync from HR tool	HR Sync Sync from HR tool	IDM Migrate UDB/UCS/\$SaaS\$ migration tool	LDAP SEBIN LDAP search+bind	 Authentik IDP
Workloads	 Prometheus Operator Monitoring	 Cert-Manager Certificate Management	 PostgreSQL	 389 directory server	 Garage Object Storage
Infrastructure	 Rancher Prime Container Management		 Patroni HA PostgreSQL Orchestration	 SUSE Virtualization VM management	
Base OS	 SLE Base OS				

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 **Search+Bind**
- IDM Merge: Identity Aggregator & De-duplicator

Q&A

