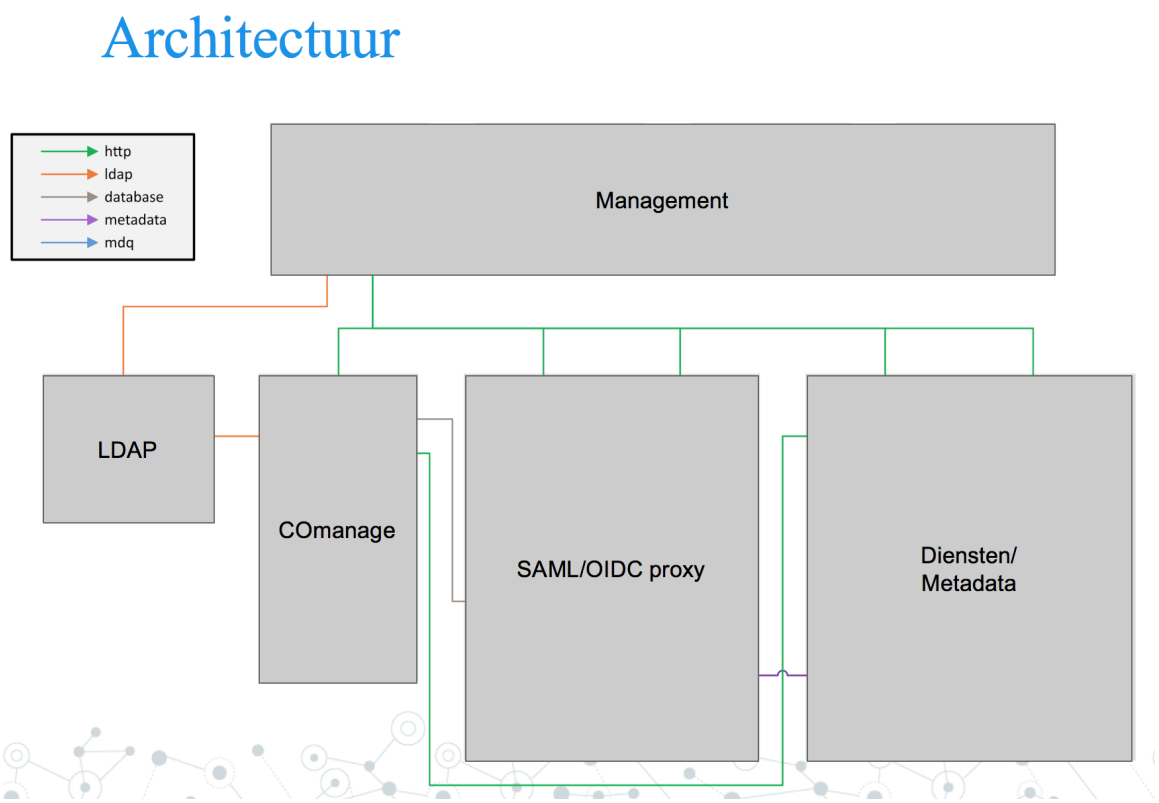
Technical overview of SCZ

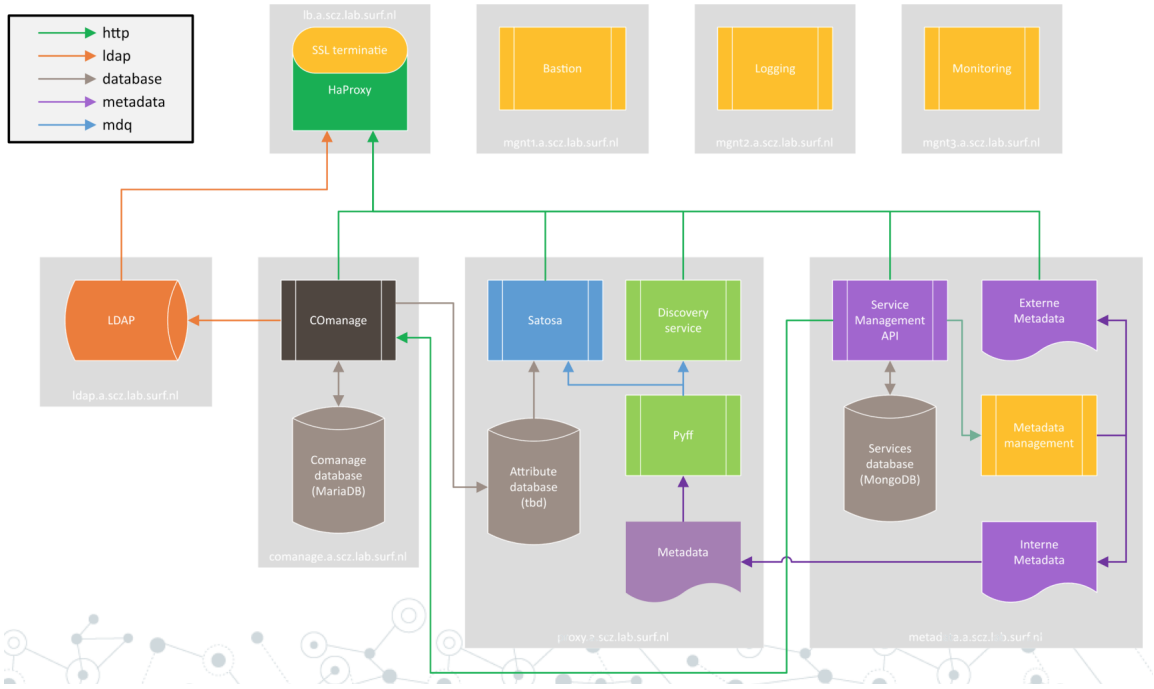
This page shows the components we use for the SCZ infrastructure. Wherever possible, proven technology is used. We analyse existing, often open source, components for fit for our purpose, and change code when necessary to have all components work together and deliver the functionality we need.

Architecture in 2 images



and one level deeper:

Architectuur



More info about the 'happy flow' for a user trying to access a SP while authenticating via the SCZ environment can be found in Userflow .

Used components

A brief description of modules and principles we use:

- A Membership Management Service (MMS)
  For this, currently, we use COmanage, an Internet2 initiative started some years ago an which has also been tested within AARC. Of the available solutions for group management, invites and attribute management we think this is the most future proof. SURF has direct connections with the developers of COmanage. Alternatives are Hexaa, Perun and, based on feedback on COmanage from the Dutch pilot partners, a self-built Collaboration Management System.
- A Proxy & Identity Hub
  The Proxy is an SP-IdP Proxy. It can connect SAML Identity Providers, OIDC Providers, SAML Service Providers and OIDC Resource Providers, thus enabling teams to use their preferred identity sources and services regardless of the authentication protocol. The Proxy is responsible for aggregating the user attributes from various identity sources, enforcing community and platform wide policies and providing one persistent user identifier and a harmonised set of attributes to the connected services. For this, we currently use SATOSA ("A configurable proxy for translating between different authentication protocols such as SAML2, OpenID Connect and OAuth2") is used in the current phase to technically connect services so authentication requests can be managed. SUNET has been instrumental in development of SATOSA.
- A Metadata Service (MDS)
  The Metadata Service aggregates the metadata of all the SAML Identity and Service Providers that are connected to the platform. It does so by aggregating the metadata feed of eduGAIN, while allowing the platform administrators to configure also other local or remote metadata sources. The MDS is an essential component of the platform directly connected to the eduTEAMS Proxy. For this we currently use pyFF, python Federation Feeder. pyFF also provides the WAYF. NORDUnet has been instrumental in development of PyFF.
- Discovery Service (DS)
  The Discovery service provides a web interface for users to search and select their preferred identity provider. pyFF in SCZ also provides for the Discovery Service.
- Besides those components, we also use the following to software and components to complete SCZ:
  - CMService
    For showing and managing Consent
  - LDAP
    Together with the membership management service like COmanage, and SATOSA, LDAP provides the technical basis for SCZ. In the LDAP database we store application specific passwords (ASP), public ssh/pgp keys, grid certificates etc, so non-web applications can retrieve them.

- LSC-project: LSC, which "*main goal is to provide a simple and efficient way of synchronizing any data source to a LDAP directory quickly*", enables us to do fine graned syncing between our LDAP and that of SP's.

Functionalities also provided by the above components:

- Federated authentication and non-web resources (like SSH and webDAV)
  For web applications providing federated access, with protocols like SAML and OIDC, is pretty straight forward. But researchers often use tools from the command prompt, where SAML and OIDC don't provide a solution for. SCZ will provide a way to connect the federated way of working with access to these 'non-web' resources (the LDAP and PAM play an important role in this).
- Non edu ('guest') usage
  SURF has extensive knowledge of supporting people without an edu account, for instance as it is needed for the SURFconext service (currently OneGini is used to provide a 'guest IdP' in SURFconext). SURF-employees where involved in several AARC projects focuses on the question how to provide access for people without an edu-account.
- Account Linking
  Most people have several online identities, each of which has it's own value. Some people have multiple institutional accounts, some have a national identity, a bankId etc. Within the SCZ context there is a need to link those accounts together, also to prevent someone loosing access to all resources, just because one account has been revoked.

We also plan to add shortly, based on user requirements:

- Strong 2 step Authentication
  Many services projected to be connected to the SCZ infrastructure deal with sensitive or special personal data, which needs strong authentication for an extra layer of protection, sometimes required as either the client or service provider needs to adhere to standards like NEN 7510. The SCZ project can leverage the experience SURF has with providing strong authentication.

During the project we also are testing:

- Containerization
  Within the SCZ project we will test whether using containers provides advantages in scalability, management, stability, availability etc.

If you're interested in similar technology: AARC in 2015/2016 listed components that fit the AARC architecture in 'Existing AAI and available technologies for federated access'.