AKKA

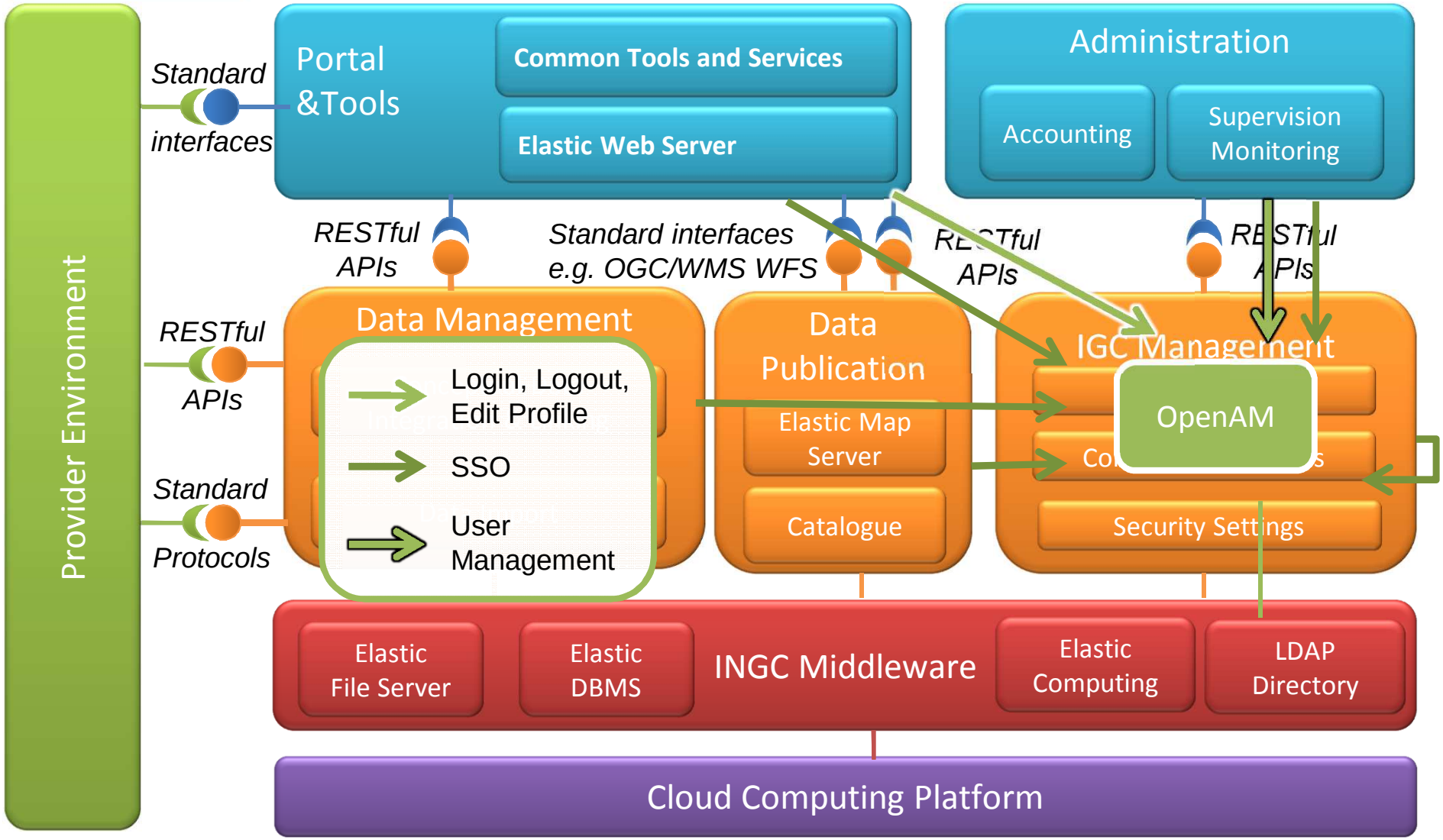
Insights into the Technical Aspects of the InGeoCloudS platform

USER MANAGEMENT
AUTHENTICATION
AUTHORIZATION

Experts Workshop

Nov. 21st, 2013

Authentication & Authorization



Why SSO ?

- Multiple software used during a user session
  - User should not connect more than once in the system

- Classic HTTP authentication modes are not enough secured
  - E.g. with basic HTTP, passwords are sent in clear (Base64)

➢ With SSO, a token is associated to user session
  - User connect once to get a token,
  - Token is encrypted and valid only for the session,
  - Browser pass the token with each request,
  - Applications use the token to control access.

Authentication

- SSO integration in Web applications
  - Ingeoclouds API,
  - Portal (Sitools),
  - Geonetwork,
  - Data providers' applications.

- No SSO for other applications:
  - LDAP authentication for system users,
  - Dedicated authentication for database,
  - Applications and tools delegating authentication to system: GlusterFS, FTP, etc.

Authentication

- User can authenticate on the portal
  - Sitools redirects the user on the OpenAM login page,
  - Other applications must not authenticate the user.
- User can authenticate using REST services
  - Provided by OpenAM,
  - Useful for automatic or batch process.
- User session is valid for 2 hours
  - And invalid after 30 minutes of inactivity.

Authorization

- Ingeoclouds platform does not manage authorizations
  - But defines primary roles.
- Applications rely on the SSO token
  - To check the user session is valid,
  - To retrieve the user profile, including the user roles,
- Applications check the user session and retreive user profile
  - Using REST services or SDKs for Java or C applications provided by OpenAM.

Authorization

- Applications build permissions from the user roles
  - To customize the behaviour of the application (e.g. mail on event),
  - To control access,
  - To filter results displayed on the application GUI.

- Each software component of the platform control access to its own resources
  - Sitools filter the accessible applications,
  - API filter access to RESTful services,
  - Geonetwork console features depend on the connected user,
  - OpenAM console is only accessible for administrators.

Authorization

- Public (anonymous user):
  - user allowed to access the public part of the portal and of the data provider applications.
- Registered user:
  - user allowed to access a data provider application with specific behavior or additional features.
- Data provider:
  - user allowed to access all the resources and services of the platform, except the administration services.
- Administrator:
  - user allowed to access all the administration services and resources.

User Management

- User management is centralized
  - OpenAM manages all users.

- User management API is provided by Ingeoclouds
  - Data providers management (accessible by Administrators)
  - Registered users management (accessible by Data Providers)

- OpenAM console (accessible by Administrators)

LDAP Directory

- OpenDJ as LDAP Directory
  - Because OpenLDAP not officially supported,
  - Unfortunately, OpenDJ is less efficient,
  - We plan to migrate to OpenLDAP.
- LDAP authentication for system users
  - Configured to use OpenDJ.
- LDAP directory backed up every night