IdPnube: RedIRIS approach to IdP as a service

José-Manuel Macías / IdPnube Team
idpnube@rediris.es

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

Topics

- Objectives
- Short IdPnube history
- Components
- Some IdPnube Internals
- Current and future developments

Objectives

- Created with security in mind
- Flexible enough to support several use cases
- Fast deployment for new organizations
- Able to scale up to hundreds of organizations
- Easy to use for staff with minimal training
  - For end users, no training at all
- Support for organization branding
- SAML IdP… and eduroam IdP, too

IdPnube = eduGAIN + eduroam

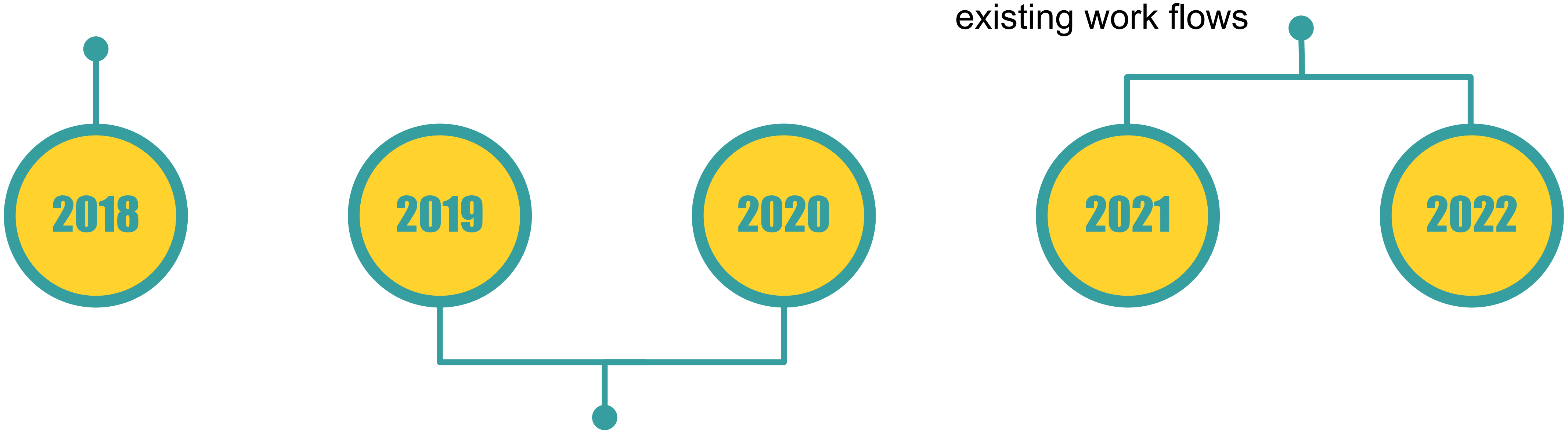
IdPnube history

survey

- small organizations interested
- orgs low in dedicated staff
- service perceived as complex to setup
- interest in having eduroam, too

new developments / production

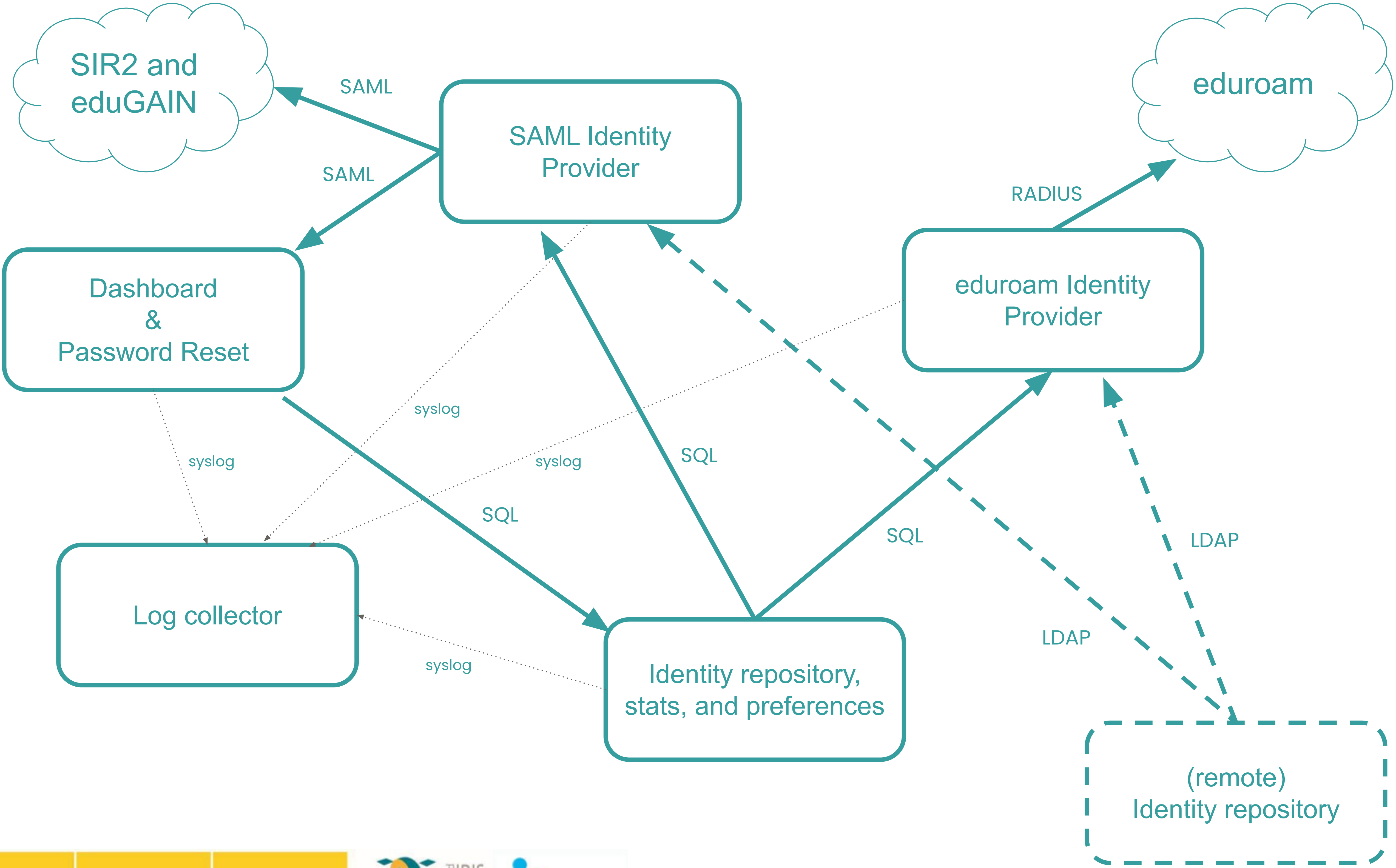
- new organizations added
- improvements in the different elements
- work started on “bespoke IdPnube”
- Start partial code rewriting and improvement of existing work flows



initial development and pilot

- focus in Unique Science and Technology Infraestructures (ICTS)
- Below 250 users
- Included ~10 organizations initially
- a training was held in fall 2019
- several use cases covered
- gathered new requirements from organizations feedback
- different use cases to cover (new functionalities)

Components


SIR2 and eduGAIN
SAML
SAML Identity Provider
SAML
eduroam
RADIUS
Dashboard & Password Reset
eduroam Identity Provider
syslog
syslog
syslog
SQL
SQL
SQL
LDAP
Log collector
LDAP
syslog
Identity repository, stats, and preferences
(remote) Identity repository

Components: solutions used

SAML Identity Provider

simpleSAMLphp

Dashboard, IdM, & Password Reset

internal development

eduroam Identity Provider

freeRADIUS

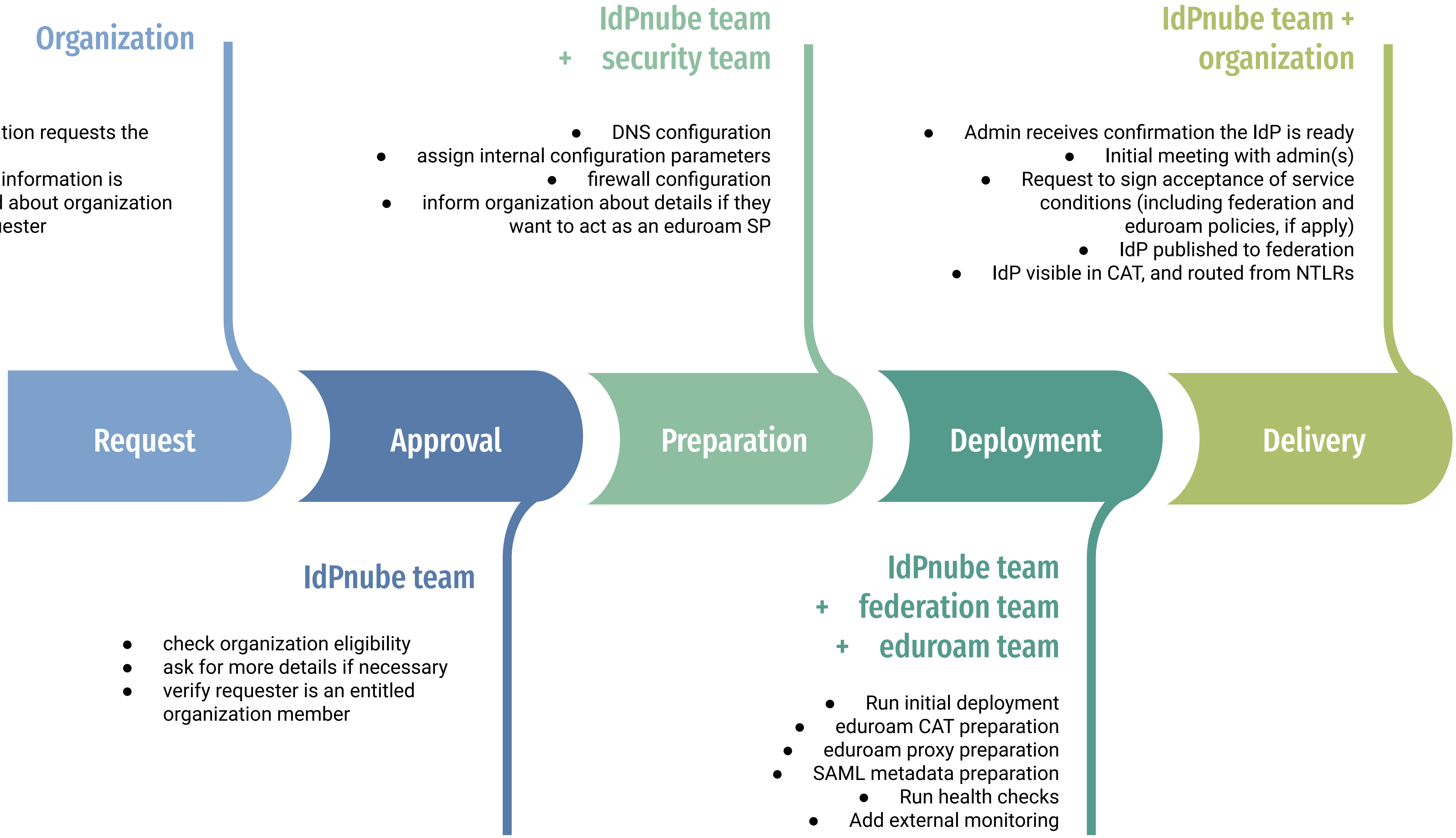
Log collector

rsyslog

Identity repository, stats, and preferences

MariaDB

From request to delivery



Request

Organization

- organization requests the service
- minimal information is gathered about organization and requester

Approval

IdPnube team

- check organization eligibility
- ask for more details if necessary
- verify requester is an entitled organization member

Preparation

IdPnube team
+ security team

- DNS configuration
- assign internal configuration parameters
- firewall configuration
- inform organization about details if they want to act as an eduroam SP

Deployment

IdPnube team
+ federation team
+ eduroam team

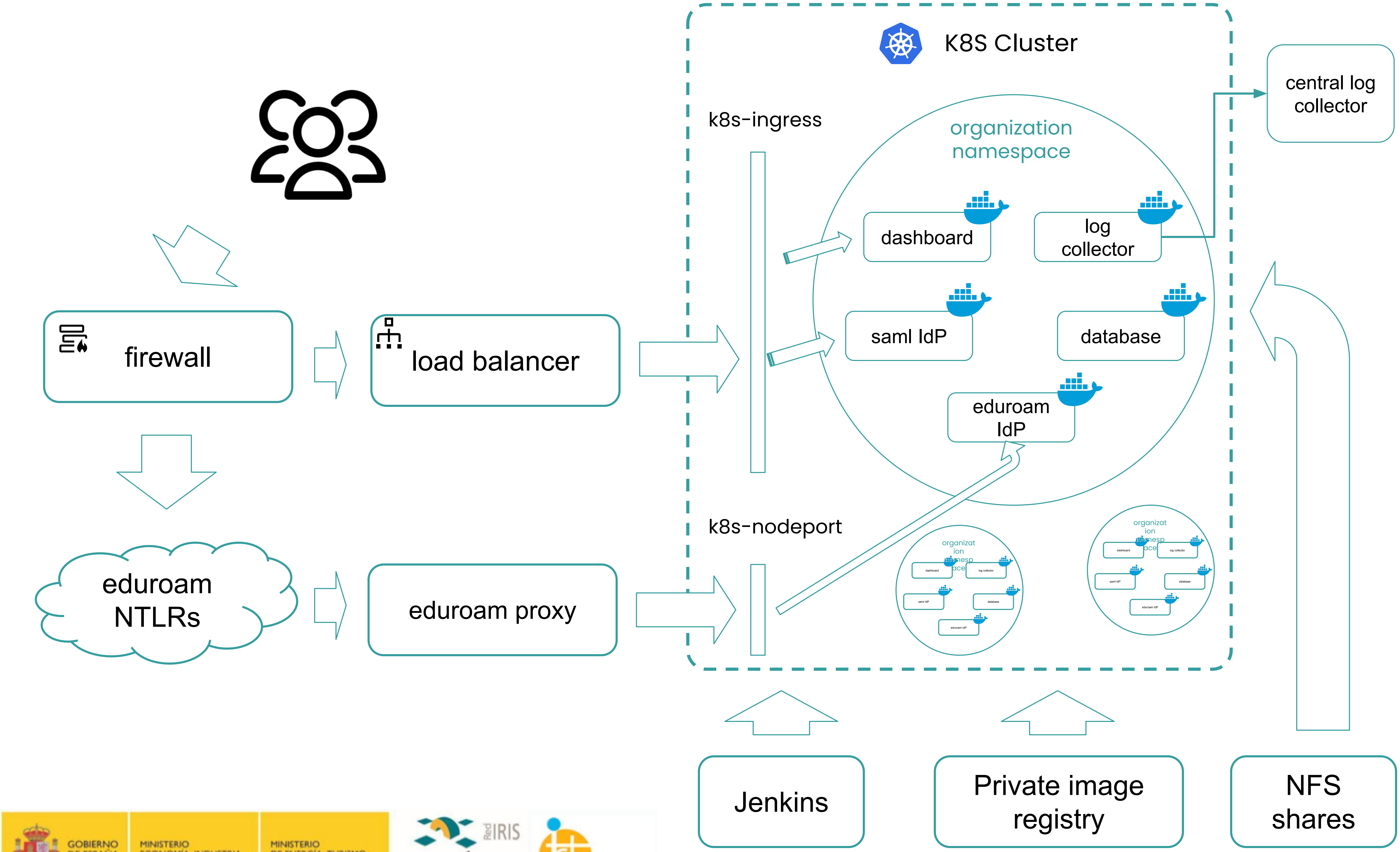
- Run initial deployment
- eduroam CAT preparation
- eduroam proxy preparation
- SAML metadata preparation
- Run health checks
- Add external monitoring

Delivery

IdPnube team + organization

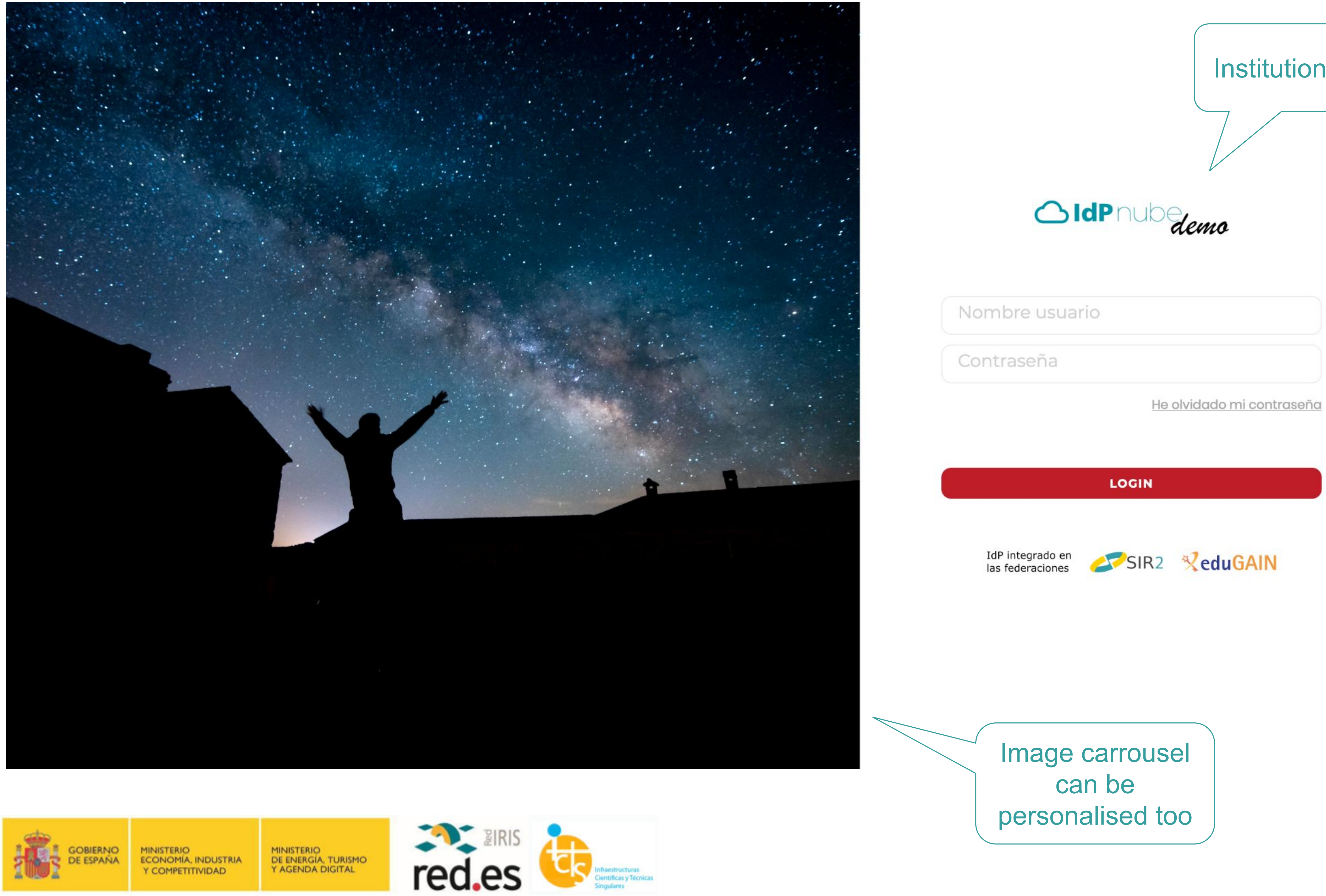
- Admin receives confirmation the IdP is ready
- Initial meeting with admin(s)
- Request to sign acceptance of service conditions (including federation and eduroam policies, if apply)
- IdP published to federation
- IdP visible in CAT, and routed from NTLRs

Architecture



GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

SAML IdP



IdPnube demo

Nombre usuario

Contraseña

He olvidado mi contraseña

LOGIN

IdP integrado en las federaciones SIR2 eduGAIN

GOBIERNO DE ESPAÑA

MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Red IRIS red.es

Infraestructuras Científicas y Técnicas Singulares

Institution logo

Image carrousel can be personalised too

Dashboard details (IdM)

Home Page

IdM (this page)

Stats (SSO & eduroam)

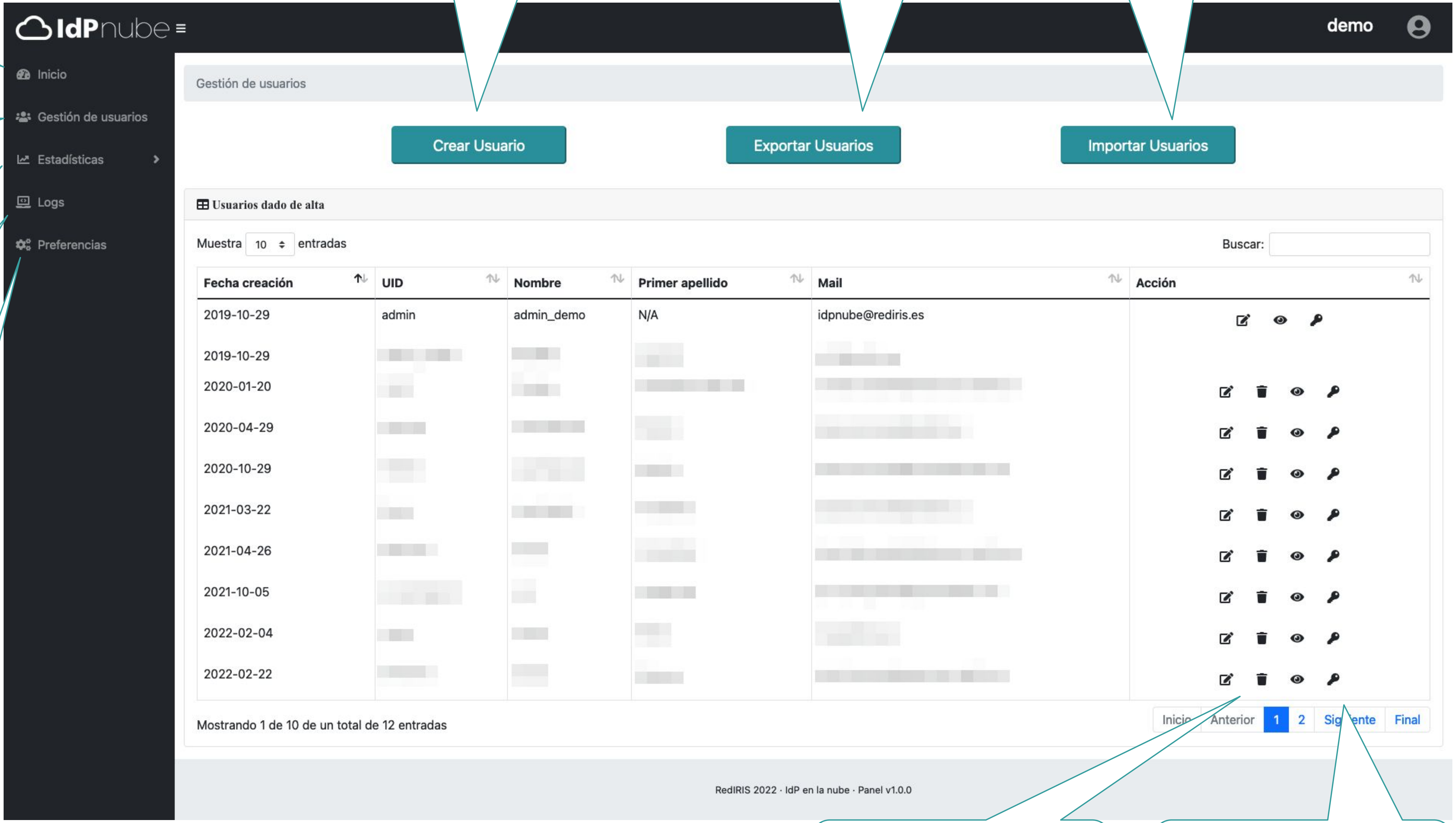
Log visualizer

Organization Preferences

Create individual user

Export users (CSV)

Import users (CSV)



Gestión de usuarios

Usuarios dado de alta

Muestra 10 entradas

Buscar:

Fecha creación	UID	Nombre	Primer apellido	Mail	Acción
2019-10-29	admin	admin_demo	N/A	idpnube@rediris.es	
2019-10-29	[redacted]	[redacted]	[redacted]	[redacted]	
2020-01-20	[redacted]	[redacted]	[redacted]	[redacted]	
2020-04-29	[redacted]	[redacted]	[redacted]	[redacted]	
2020-10-29	[redacted]	[redacted]	[redacted]	[redacted]	
2021-03-22	[redacted]	[redacted]	[redacted]	[redacted]	
2021-04-26	[redacted]	[redacted]	[redacted]	[redacted]	
2021-10-05	[redacted]	[redacted]	[redacted]	[redacted]	
2022-02-04	[redacted]	[redacted]	[redacted]	[redacted]	
2022-02-22	[redacted]	[redacted]	[redacted]	[redacted]	

Mostrando 1 de 10 de un total de 12 entradas

Inicio Anterior 1 2 Siguiente Final

RedIRIS 2022 · IdP en la nube · Panel v1.0.0

Usual CRUD operations

Force password reset

GOBIERNO DE ESPAÑA

MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

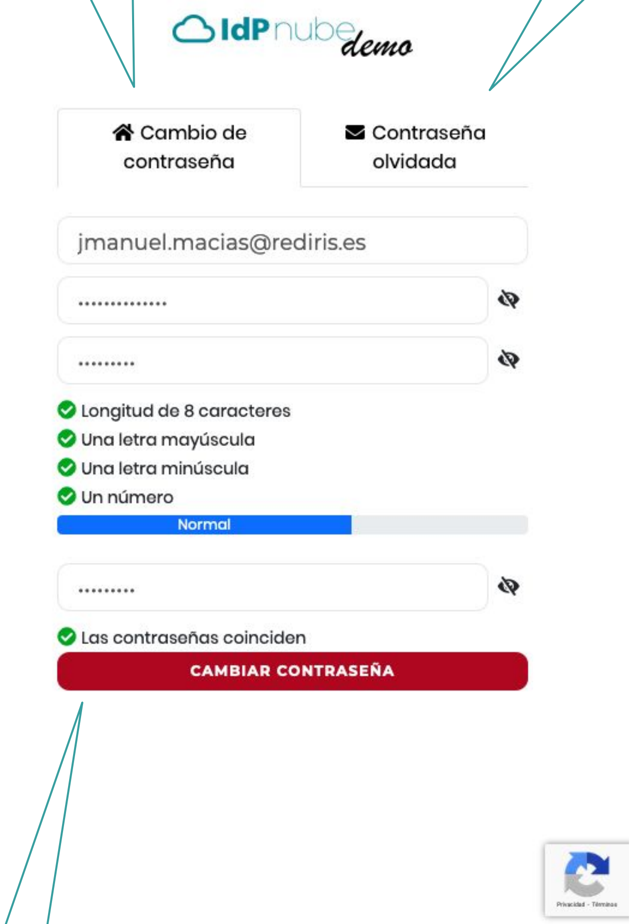
RedIRIS red.es

Infraestructuras Científicas y Técnicas Singulares

Password Reset

Reset knowing previous password

Reset by token via email



IdPnube demo

🏠 Cambio de contraseña

✉ Contraseña olvidada

jmanuel.macias@rediris.es

....

....

✓ Longitud de 8 caracteres

✓ Una letra mayúscula

✓ Una letra minúscula

✓ Un número

Normal

....

✓ Las contraseñas coinciden

CAMBIAR CONTRASEÑA

Fixed password complexity policy

Recaptcha to avoid messing with password reset

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

Some IdP details

- We decided to use passwords, but
  - Use a strong hashing algorithm (argon2)
  - Passwords never known by admins
  - Fixed minimum complexity forced
  - Reset via emailed token
- SQL authsource module used as basis for SAML IdP
  - had to add support for argon2
- eduroam authentication possibilities limited
  - TTLS-PAP used
  - decided to use FreeRADIUS `rlm_rest` for authentication
- No passwords stored if remote repository is used
- Plans to get rid of passwords…
- We use F-TICKS for stats in both IdPs

Current and future work

- Dashboard being rewritten using the Laravel framework
- Implement the *groups* functionality
- Implement SCIM (server)
- Improvement CI/CD workflows
- Improve resilience of the K8S cluster
- Better handling of secrets
- Marketing actions

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

Current and future work

- *Bespoke* IdPnube
  - Testing Packer+ansible playbooks for:
    - deployment over organization own infrastructure
    - containerised IdPs, too
- Also, we want to explore
  - WebAuthn instead of passwords
  - Introduce MFA + assurance
  - EAP-TLS for eduroam
    - *Let's WiFi + get eduroam* probably a good solution

Thanks for your attention!

Questions?