ISTI: migrazione dei servizi come occasione per l'introduzione di automazione e integrazione

Andrea Dell’Amico <andrea.dellamico@isti.cnr.it>

ISTI-CNR

Laboratorio InfraScience

Servizio Infrastruttura Informatica ISTI e Supporto ai Servizi (S2I2S)

Responsabile: *Franca Debole*

Componenti:

- *Tommaso Piccioli*
- *Andrea Dell'Amico*

Philosophical choices

- Free software everywhere

Architectural choices

SMTP: Load balancer vs DNS

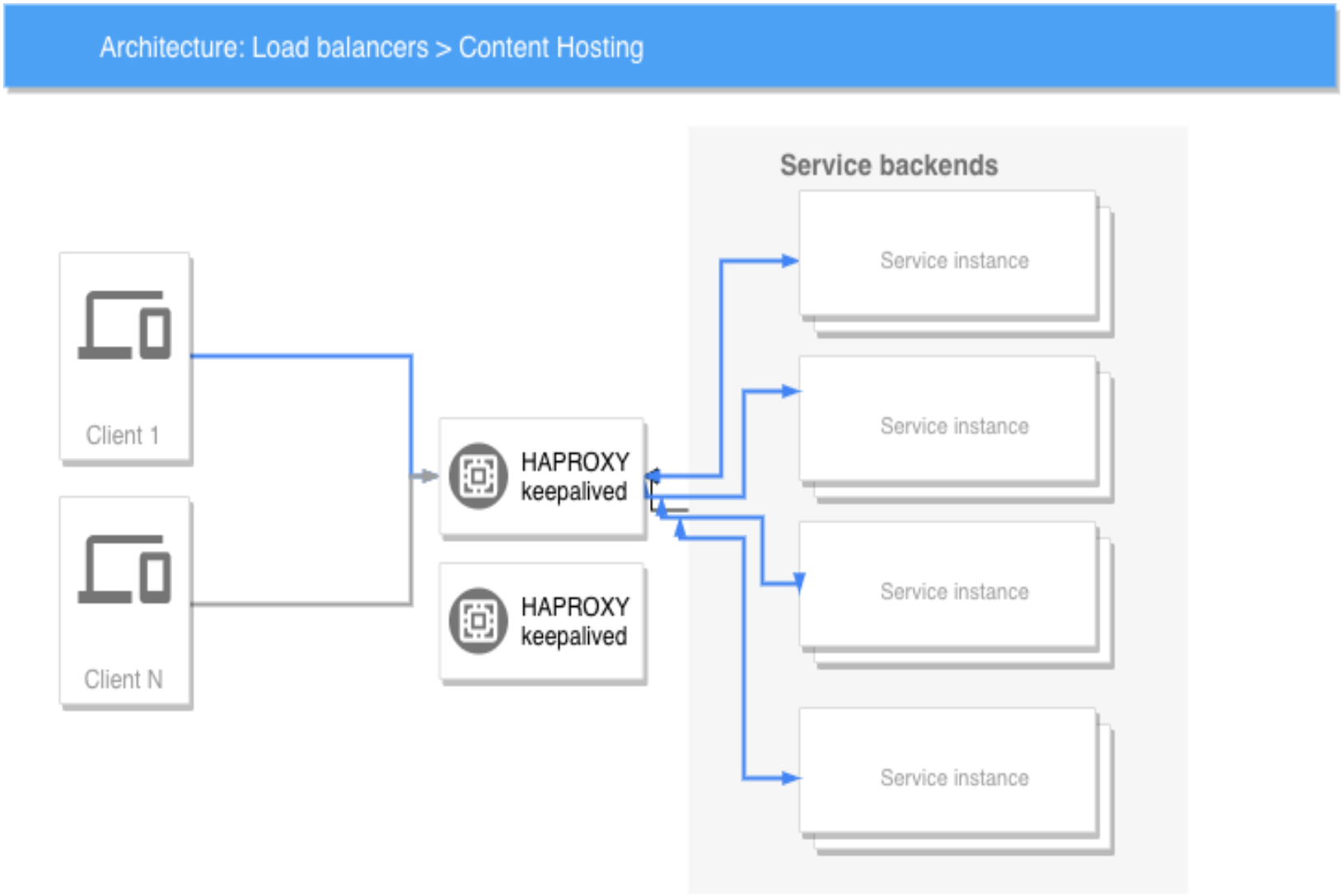
- Load balancer: single endpoint that distributes the requests to N backends
- DNS: more than one MX record, or more than one IP address associated to a hostname

Why a load balancer:

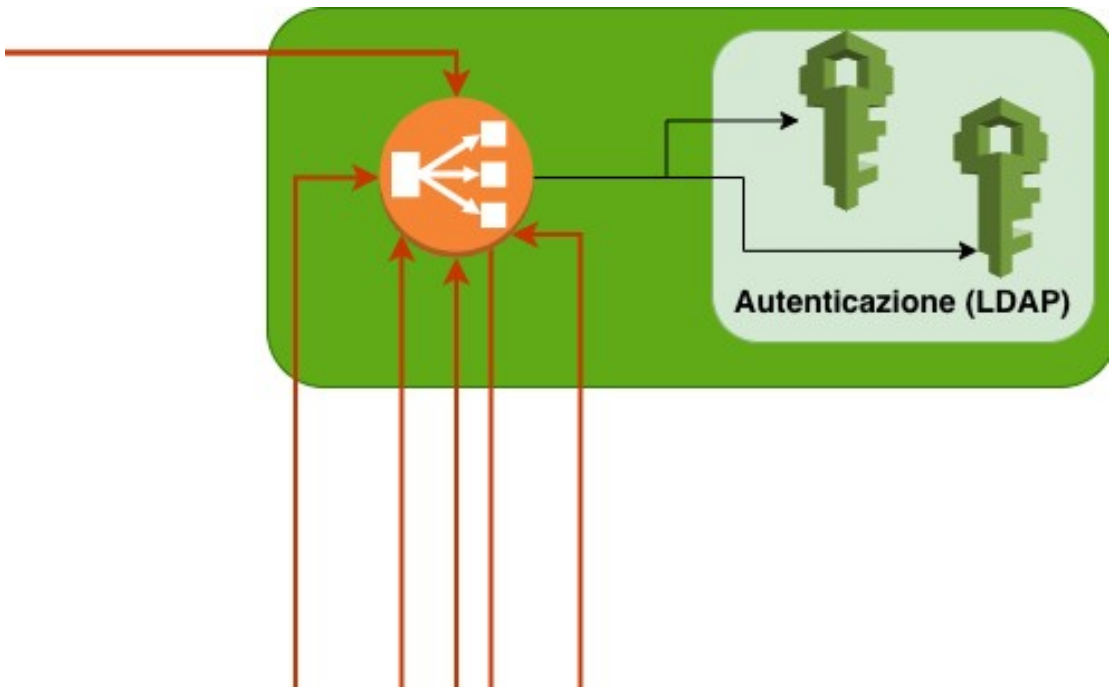
- Backend servers can be added or removed transparently to the user
- Email clients cannot be easily configured with more than one SMTP server for one email address
- The web services can be proxied by a load balancer without changes to the application, when a single instance is involved

Load balancers architecture

- 2 Virtual Machines
- 1 floating IP
- Services running on every VM:
  - HAPROXY
  - Keepalived, for HA and floating IP management

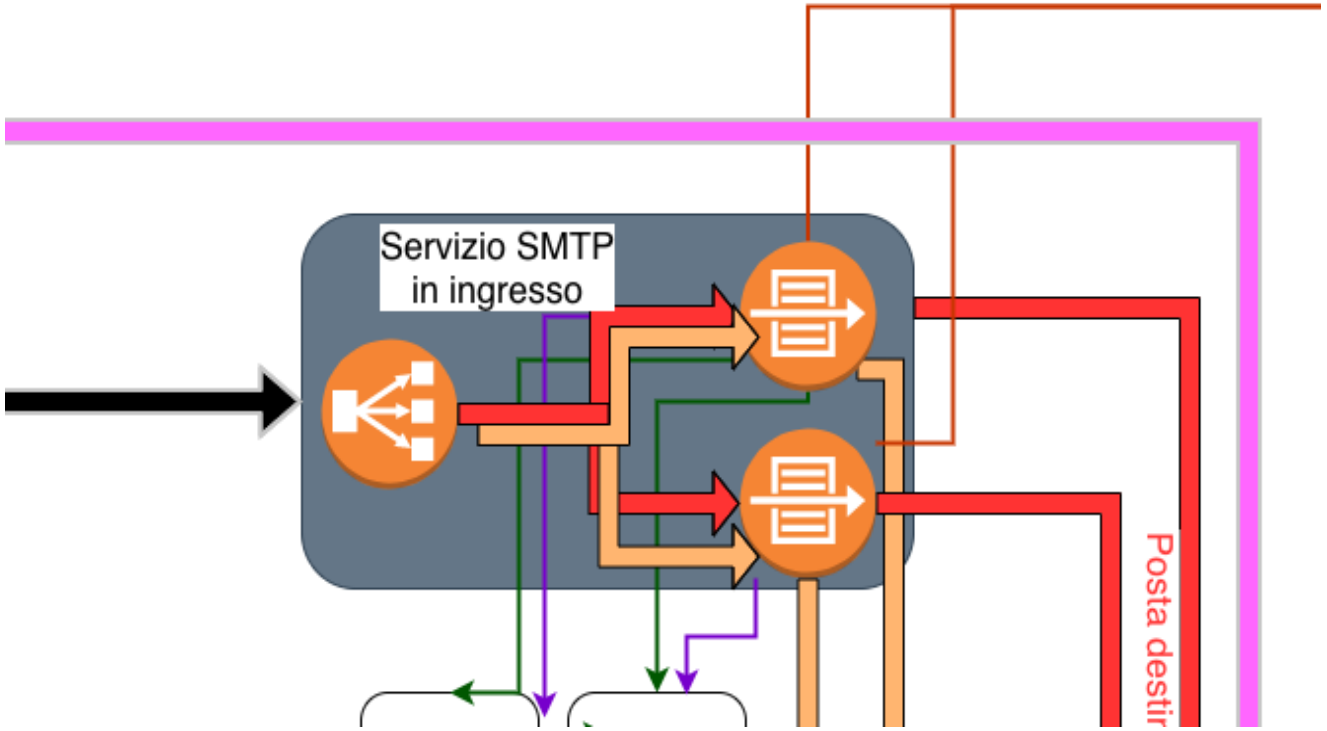


Email system: authentication (FreeIPA)



- Incoming SMTP: check of the recipient's email address
- SMTP delivery: find the recipient's username
- POP/IMAP, webmail: user authentication
- Outgoing SMTP: user authentication, authorize the sender's email address

Incoming SMTP

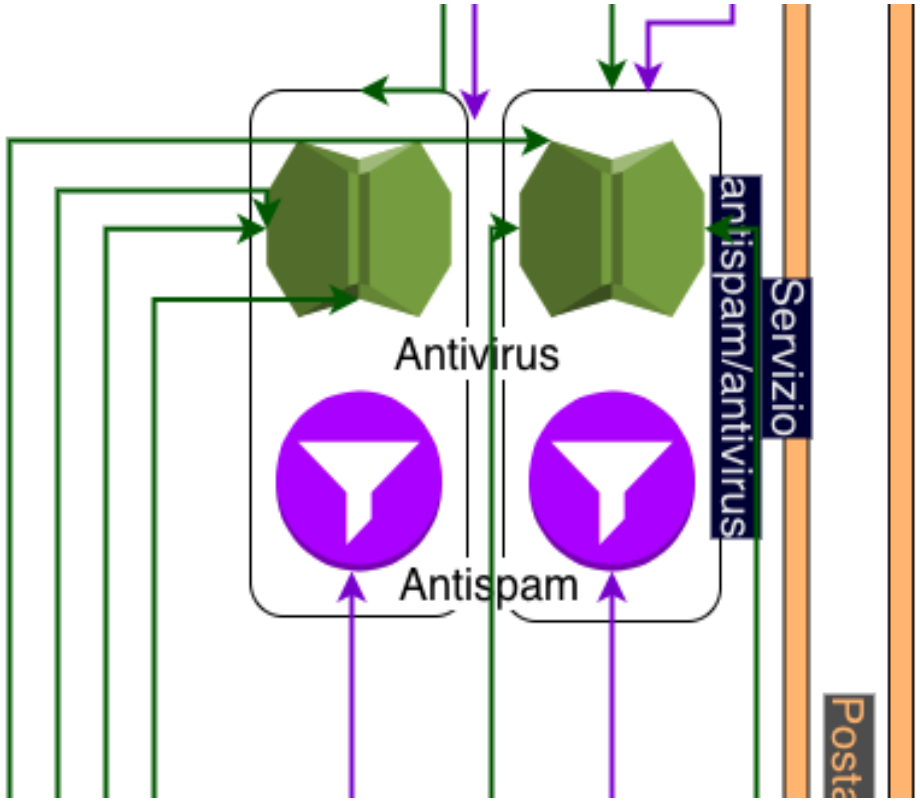


- Two servers behind the load balancers
- Before the delivery
  - RBL check (SpamHaus ZEN)
  - DBL check (SpamHaus)
  - Antivirus check
  - Antispam check
- Different route for the mailing lists
- Delivery via LMTP

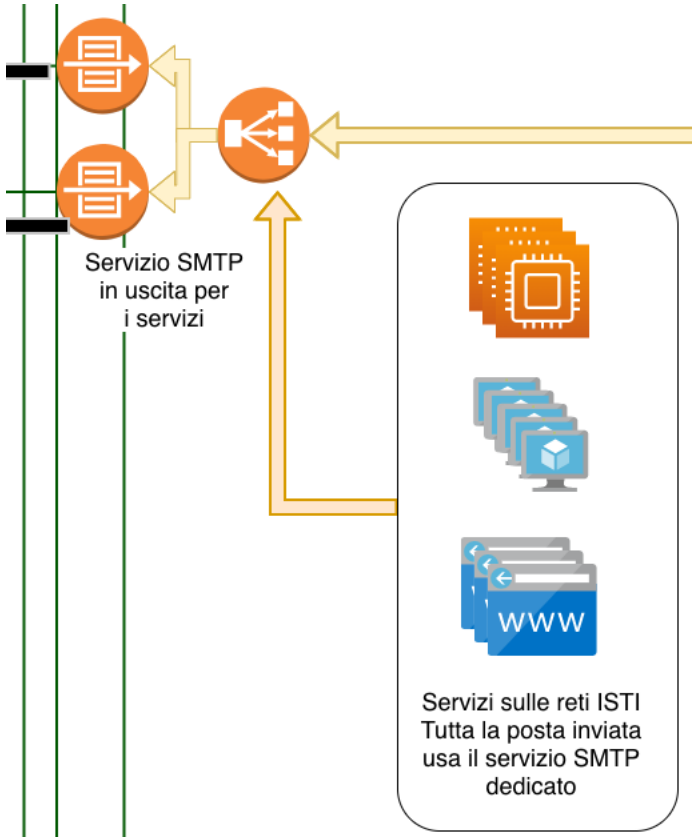
Antispam and antivirus

Two VMs, each running both the antivirus and the antispam service

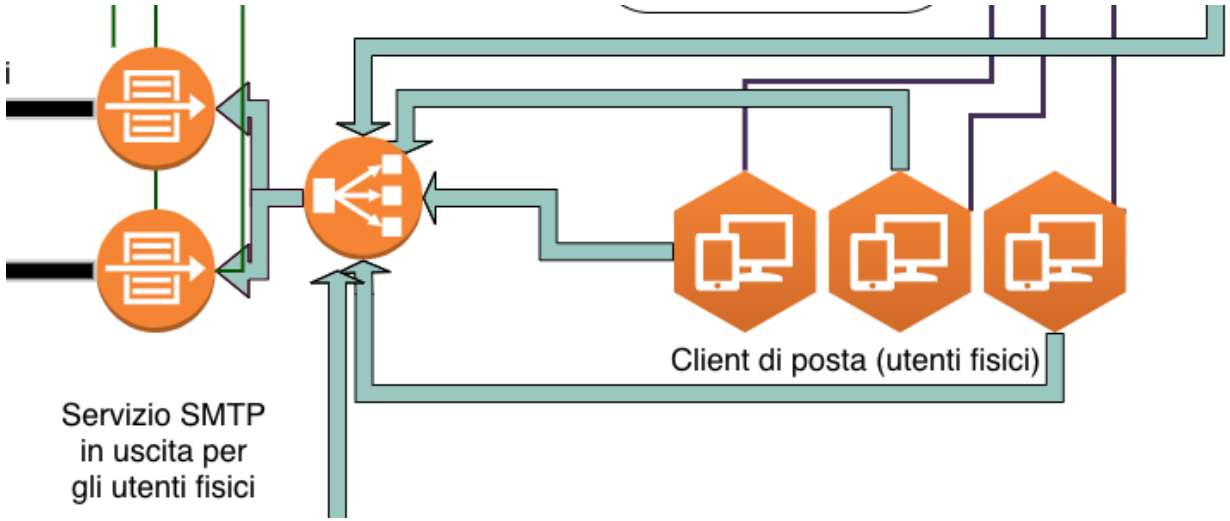
- The antivirus rejects the emails immediately
- Every antispam rule assign points (positive or negative). Over 5 (default) an email is marked as SPAM



Outgoing SMTP service



- Services and physical users use two different SMTP servers
- Both servers check the outgoing emails for viruses
- The SMTP server used by the physical users checks the sender's email address
- The delivery rules will diverge in future, between services and users



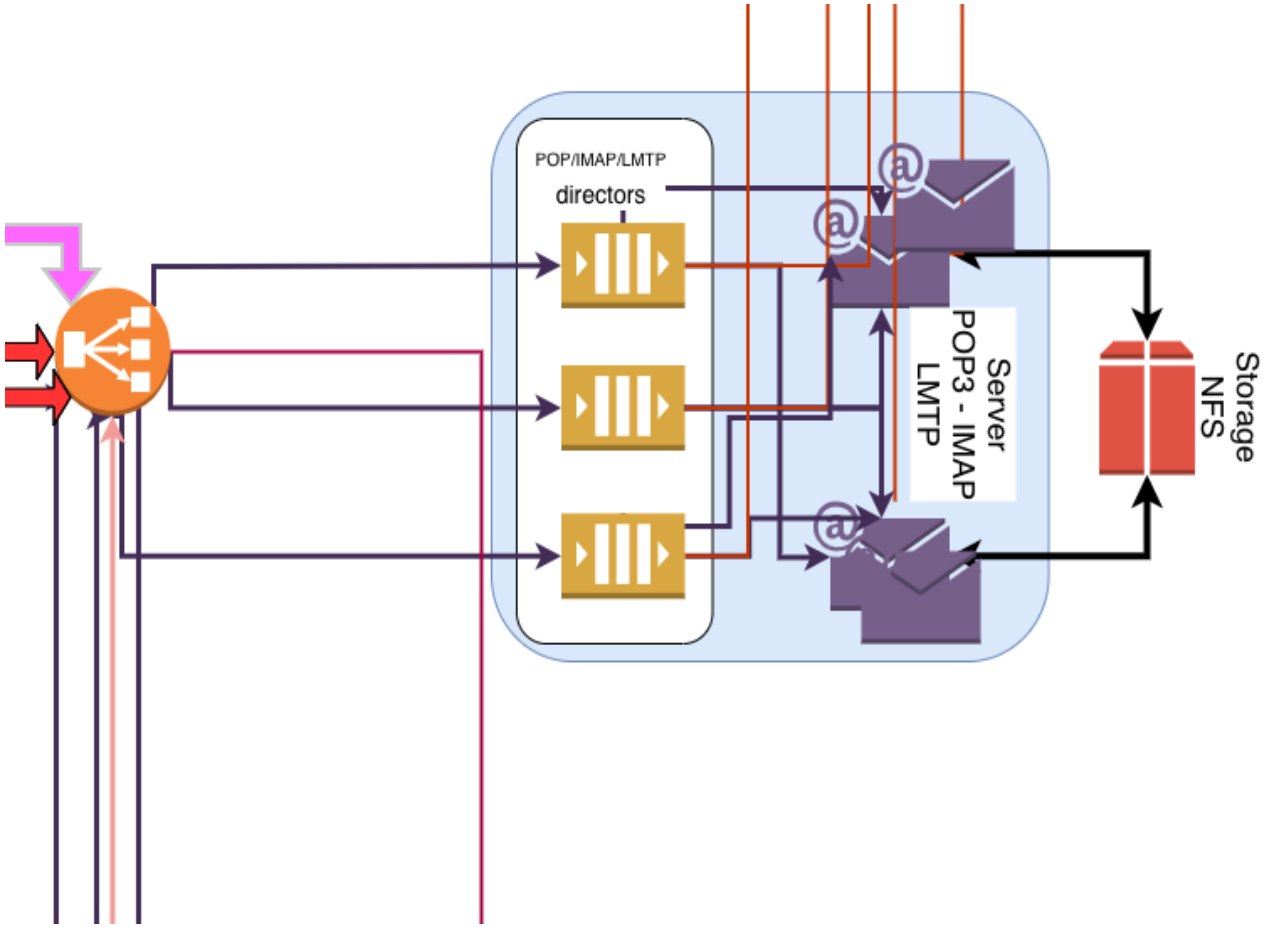
SMTP: Reputation policies

- SPF enabled and enforced: only the IP address of our SMTP servers are allowed by the policy, with one exception

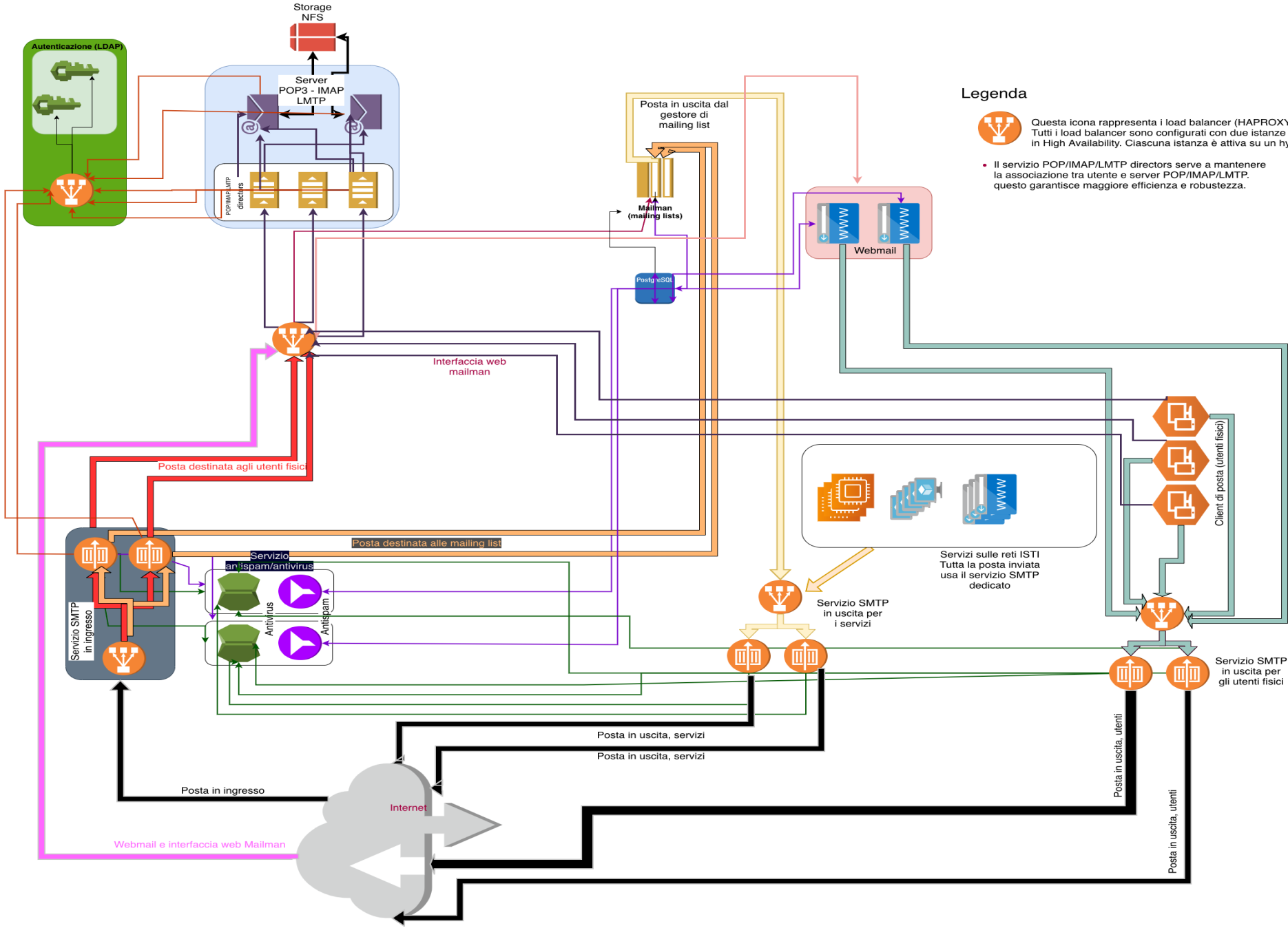
In the near future

- DKIM
- DMARC
- MTA-STS

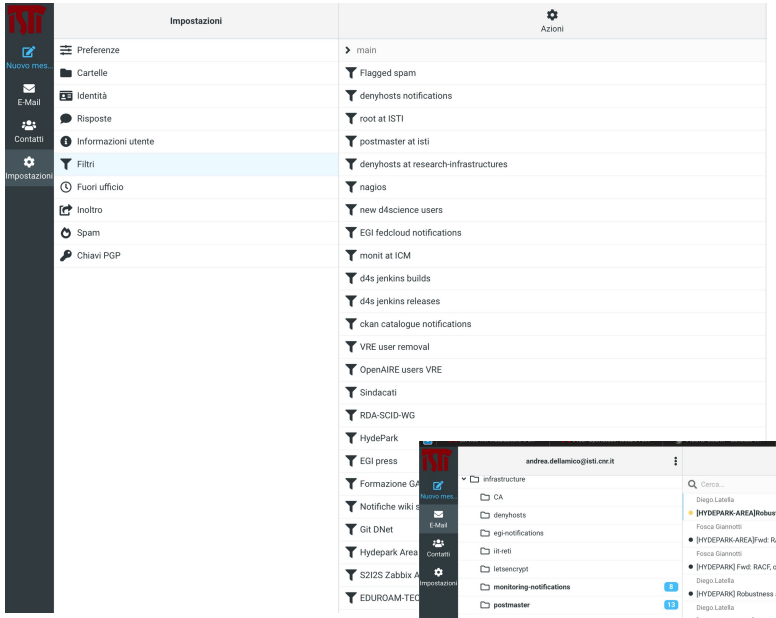
IMAP and POP service

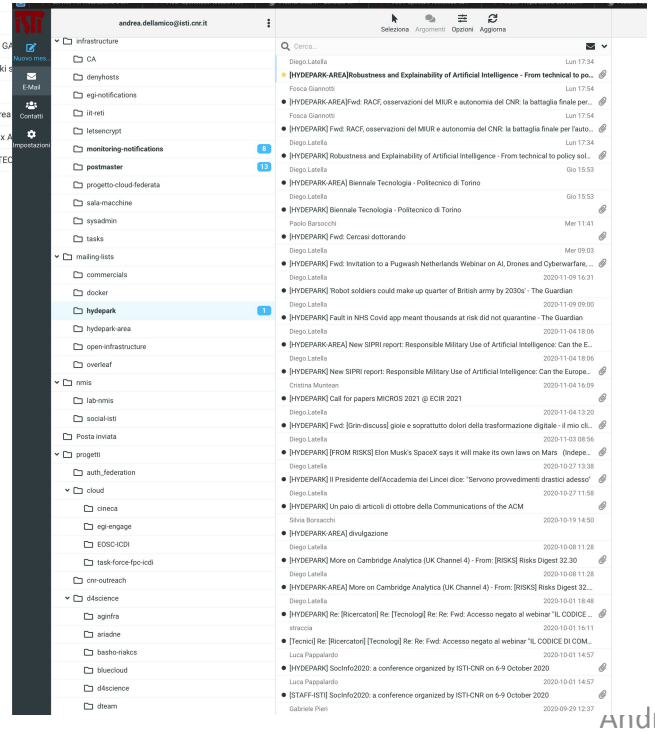


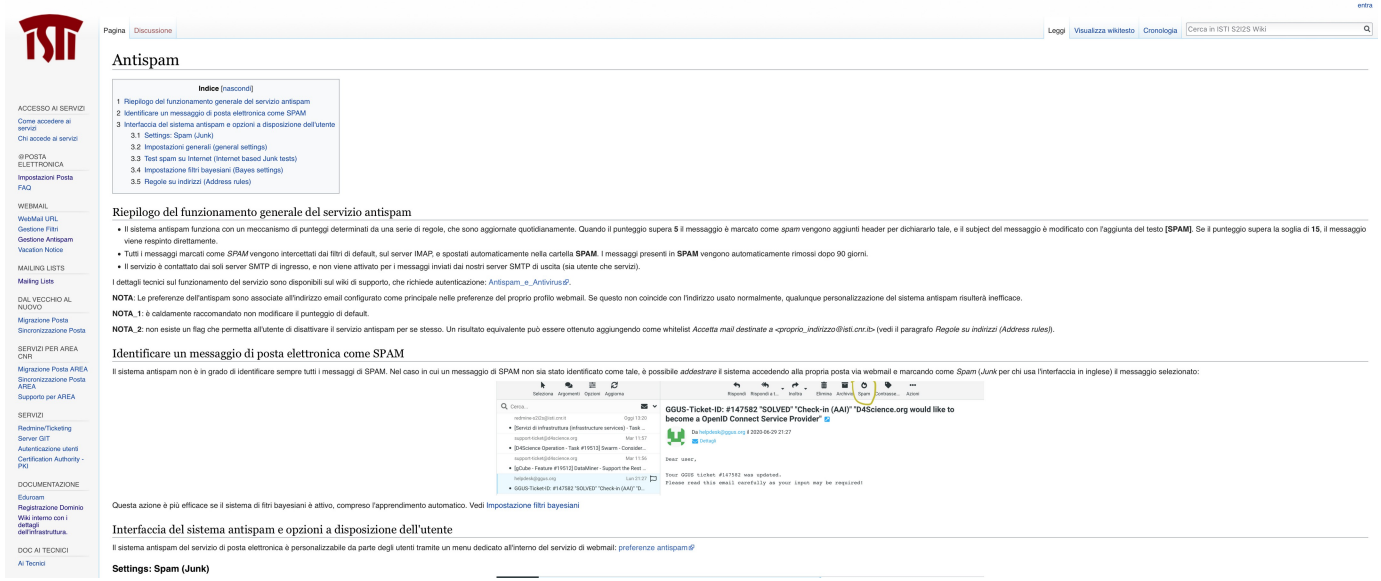
- Three *director* servers behind the load balancers
- Four POP/IMAP servers
- The NFS server exports the same volume to all the POP/IMAP servers (SPoF)

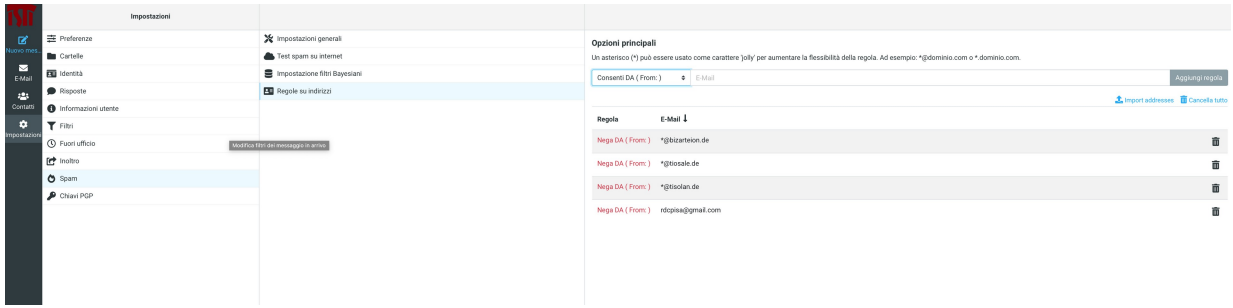

Storage NFS
Autenticazione (LDAP)
Server POP3 - IMAP LMTP
POP/IMAP/LMTP directors
Posta in uscita dal gestore di mailing list
Mailman (mailing lists)
Webmail
PostgreSQL
Interfaccia web mailman
Posta destinata agli utenti fisici
Posta destinata alle mailing list
Servizio antispam/antivirus
Antivirus
Antispam
Servizio SMTP in ingresso
Servizi sulle reti ISTI
Tutta la posta inviata usa il servizio SMTP dedicato
Servizio SMTP in uscita per i servizi
Servizio SMTP in uscita per gli utenti fisici
Client di posta (utenti fisici)
Posta in uscita, servizi
Posta in uscita, servizi
Posta in ingresso
Internet
Webmail e interfaccia web Mailman
Posta in uscita, utenti
Posta in uscita, utenti
Legenda
Questa icona rappresenta i load balancer (HAPROXY).
Tutti i load balancer sono configurati con due istanze separate, in High Availability. Ciascuna istanza è attiva su un hypervisor differente
Il servizio POP/IMAP/LMTP directors serve a mantenere la associazione tra utente e server POP/IMAP/LMTP. questo garantisce maggiore efficienza e robustezza.

Filters, antispam, vacation, forward settings are accessible from inside the webmail interface.
Their use is documented at https://mediawiki-s2i2s.isti.cnr.it/









Operations

- Everything over TLS (not limited to https)
  - Letsencrypt is being used not only for web certificates
  - Certificates renewals are automatic
- Firewall rules on every VM

  (or: *is it zero trust?*):
  - Minimal set of open ports
  - Services that are not public are limited to the allowed clients
- No direct root access
- Use of the VPN is mandatory

Problem

- A lot of very old clients still in use ➔ we cannot remove support for tls < 1.2 yet

Operations: everything is a ticket, at https://redmine-s2i2s.isti.cnr.it

Task #28

Edit Unwatch Copy Delete

Attivazione di un nuovo sistema di posta elettronica per l'ISTI

Added by Andrea Dell'Amico over 1 year ago. Updated 24 days ago.

Status:	In Progress	**Start date:**	11 Feb 2020
Priority:	High	**Due date:**	10 Jun 2020
Assignee:	s2i2s	**% Done:**	20%
Category:	Migrazione servizi ex Gennai	**Estimated time:**	(Total: 0:00 h)

Description Quote

Questo vuole essere il task padre di tutte le attività, che comprendono parecchi servizi. Task dettagliati verranno aperti in seguito.

Una descrizione di come dovrebbe essere strutturata tutta l'architettura, compresa anche la posta elettronica, è definita in https://docs.google.com/document/d/1kcCn_jGdi6uhfGxRwHqWzlyxFDK4qIIsqefJ7pEk2G8/edit?usp=sharing
Una copia PDF del documento è disponibile su nextcloud: https://nextcloud-s2i2s.isti.cnr.it/s/5A9rExkfLHoPw6K

Subtasks Add

~~Task #147~~: Installare e configurare tre server che ospiteranno il servizio di posta, in attesa dell'infrastruttura definitiva	Closed	s2i2s	
~~Service #37~~: VM sulla quale installare imapsync e una interfaccia web che collezioni i dati di accesso degli utenti	Closed	s2i2s	
~~Task #153~~: Configurare KVM sui due server di calcolo del piano B	Closed	s2i2s	
~~Task #154~~: Configurare lo storage server del piano B	Closed	s2i2s	
~~Task #196~~: Installare due VM che funzioneranno da load balancer per i server pop/imap e per webmail	Closed	s2i2s	
~~Task #197~~: Installare le due VM che funzioneranno da server pop/imap	Closed	s2i2s	
~~Task #198~~: Configurare NFS tra lo storage server e le macchine del servizio pop/imap	Closed	s2i2s	
~~Task #199~~: Installare e configurare due VM per postgresql	Closed	s2i2s	
~~Task #200~~: Installare e configurare due macchine sulle quali installare il servizio webmail	Closed	s2i2s	
~~Task #203~~: VM col servizio SMTP, che distribuisca a pop/imap	Closed	s2i2s	
~~Task #207~~: Modificare il record SPF per il dominio isti.cnr.it	Closed	s2i2s	
~~Task #231~~: Servono 6 VM da usare come load balancer per i server SMTP in uscita e in ingresso	Closed	s2i2s	
~~Task #232~~: Due VM per gestire il servizio SMTP in uscita da parte dei client	Closed	s2i2s	
~~Task #233~~: Due VM per gestire il traffico SMTP in uscita generato da servizi	Closed	s2i2s	
~~Task #234~~: Due VM per il traffico SMTP in ingresso	Closed	s2i2s	
~~Task #244~~: 3 VM con dovecot configurato in modalità 'director'	Closed	s2i2s	
~~Task #248~~: Chiedere allo IIT di aprire il firewall ai nostri servizi di posta	Closed	s2i2s	
~~Task #268~~: Aggiungere due VM, CentOS based, sulle quali installare i servizi antivirus	Closed	s2i2s	
~~Task #303~~: SMTP per gestire il traffico in uscita dai nodi dovecot	Closed	s2i2s	
~~Incident #304~~: I server SMTP per il delivery non hanno ricevuto posta per alcune ore	Closed	s2i2s	
~~Task #254~~: DOC:Documentare la configurazione necessaria per usare il nuovo server imap.	Closed	s2i2s	
~~Task #255~~: DOC:Documentare l'uso dei filtri di posta sul server imap (via webmail)	Closed	s2i2s	
~~Task #263~~: Lista di questioni aperte relative al 'vecchio' sistema di posta	Closed	s2i2s	
~~Task #270~~: DOC:Disegnare l'architettura del nuovo sistema di posta	Closed	s2i2s	
Task #271: DOC:Documentare le caratteristiche tecniche del sistema di posta	New	s2i2s	
~~Task #286~~: Utente per i test di vacation e forward	Closed	s2i2s	
~~Task #294~~: webmail: aggiungere la possibilità di cambiare i temi	Closed	s2i2s	
~~Task #295~~: Record MX per testare i server SMTP in ingresso	Closed	s2i2s	
~~Task #296~~: Interfaccia che permetta agli utenti di gestire la configurazione dell'antispam	Closed	s2i2s	
~~Task #575~~: Modificare il ruolo ansible di roundcube per la gestione del plugin sauserspref	Closed	Andrea Dell'Amico	
~~Task #605~~: webmail: pyzor attivo di default	Closed	s2i2s	
Task #306: Gestione Utenti di MailboxManager	In Progress	s2i2s	
~~Task #210~~: Alias degli utenti di posta	Closed	Franca Debole	
~~Task #688~~: Migrazione degli alias su Mailman3	Closed	Franca Debole	
~~Documentation #749~~: ProceduraMigrazioneAliases	Closed	s2i2s	
~~Task #214~~: Forward degli utenti di posta	Closed	s2i2s	
~~Feature #266~~: Gestione degli utenti che spediscono e leggono mail e sono legati ai servizi, su freeipa	Closed	s2i2s	
Task #307: Gestione degli utenti associati a servizi	Feedback	s2i2s	
~~Task #308~~: Utenti di servizi-KDD	Closed	Vittorio Romano	
~~Task #309~~: Utenti di servizi-SI	Closed	Marco Tampucci	
~~Task #310~~: Utenti di servizi-DIR	Closed	Enrico Fantini	
~~Task #606~~: Gestione Utenti di CONDIVISI-DIR	Closed	s2i2s	
~~Task #311~~: Utenti di servizi-NEMIS	Closed	Tommaso Piccioli	
~~Task #394~~: Utenti di Servizi-MMS	Closed	Daniele Pellegrini	
~~Task #395~~: Utenti di servizi-SSE	Closed	Alessandro Coco	
~~Task #396~~: Utenti di servizi-SEDC	Closed	Antonello Calabrò	
~~Task #397~~: Utenti di servizi-FMT	Closed	Gianluca Trentann	
~~Task #398~~: Utenti di servizi-SB	Closed	Caterina D'Angelo	
~~Task #399~~: Utenti di servizi-SAL	Closed	Giovanni Lombard	
~~Task #400~~: Utenti di servizi-SFDL	Closed	Luciano Anselmo	
~~Task #401~~: Utenti di servizi-VC	Closed	Federico Ponchio	
Task #402: Utenti di servizi-WN	Feedback	Francesco Potortì	
~~Task #414~~: Utenti di servizi-HTIS	Closed	Marco Manca	

Task	77	227	304
Service	5	15	20
Feature	21	50	71
Hardware resource	3	6	9
Bug	9	36	45
Incident	2	52	54
Documentation	4	8	12

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated	Due date
993	Possibili evoluzioni	Feature	New	Normal	SIEM: attivare una infrastruttura di logging e report compatibile SIEM	s2i2s	02 Nov 2020 04:37 PM	
936	Possibili evoluzioni	Feature	New	Normal	Plugin nextcloud per la webmail	s2i2s	05 Oct 2020 08:12 PM	
774	Possibili evoluzioni	Service	New	Normal	Autodiscovery per la configurazione della posta	s2i2s	24 Jun 2020 01:07 PM	
684	Possibili evoluzioni	Feature	New	Normal	Attivare DNSSEC sulle nostre zone	s2i2s	20 May 2020 02:39 PM	
635	Possibili evoluzioni	Service	New	Normal	Servizio che permetta di gestire newsletter	s2i2s	20 Apr 2020 02:11 PM	
609	Possibili evoluzioni	Feature	New	Normal	Recupero password self service su freeipa	s2i2s	15 Apr 2020 08:25 PM	
549	Possibili evoluzioni	Service	New	Normal	Zulip come chat collaborativa	s2i2s	16 Mar 2020 08:24 PM	
413	Possibili evoluzioni	Feature	New	Normal	Form per la richiesta di registrazione dei domini	s2i2s	12 Feb 2020 10:36 AM	
313	Possibili evoluzioni	Service	New	Normal	Look dell'interfaccia web dell'autenticazione dell'IdP	s2i2s	21 Feb 2020 11:55 AM	
288	Possibili evoluzioni	Feature	New	Normal	Soluzione per il Disaster recovery	s2i2s	27 Dec 2019 05:01 PM	
287	Possibili evoluzioni	Feature	New	Normal	Sistema di backup con cifratura	s2i2s	27 Dec 2019 06:42 PM	
243	Possibili evoluzioni	Service	New	Normal	Ricerca server side per le email	s2i2s	29 Nov 2019 07:55 PM	
240	Possibili evoluzioni	Service	New	Normal	Mailbox sull'object storage	s2i2s	29 Nov 2019 07:47 PM	
239	Possibili evoluzioni	Service	New	Normal	Notifiche push per l'email	s2i2s	29 Nov 2019 07:46 PM	
238	Possibili evoluzioni	Feature	New	Normal	Mailbox cifrate sul server imap	s2i2s	29 Nov 2019 07:44 PM	
206	Possibili evoluzioni	Feature	New	Normal	Valutare l'introduzione di DNS over HTTPS	s2i2s	29 Nov 2019 07:44 PM	
205	Possibili evoluzioni	Feature	New	Normal	Valutare 'LetsMapYourNetwork'	s2i2s	29 Nov 2019 07:44 PM	

(1-17/17)

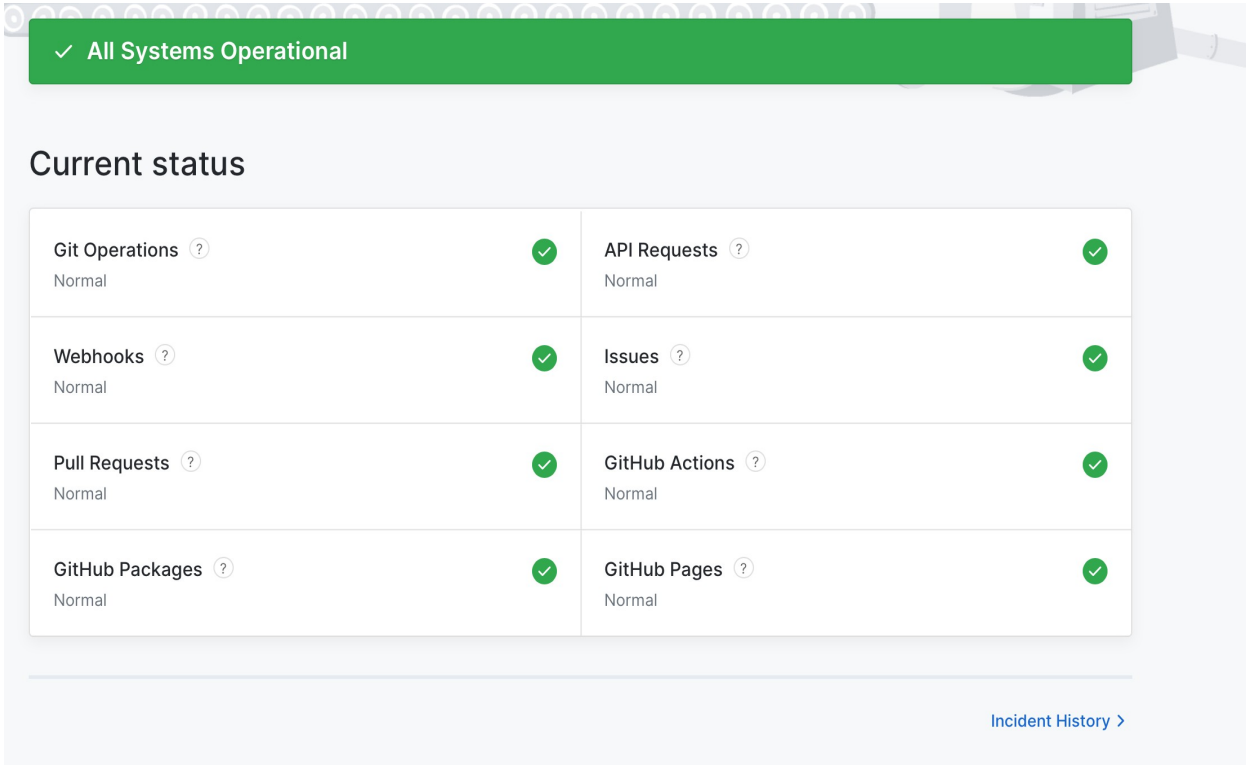
Operations: monitoring

What we have (Zabbix)

- Hardware status
  - Disk space
  - Free memory
  - Load average
  - Disk I/O activity
  - Is the server alive?

What we are going to have

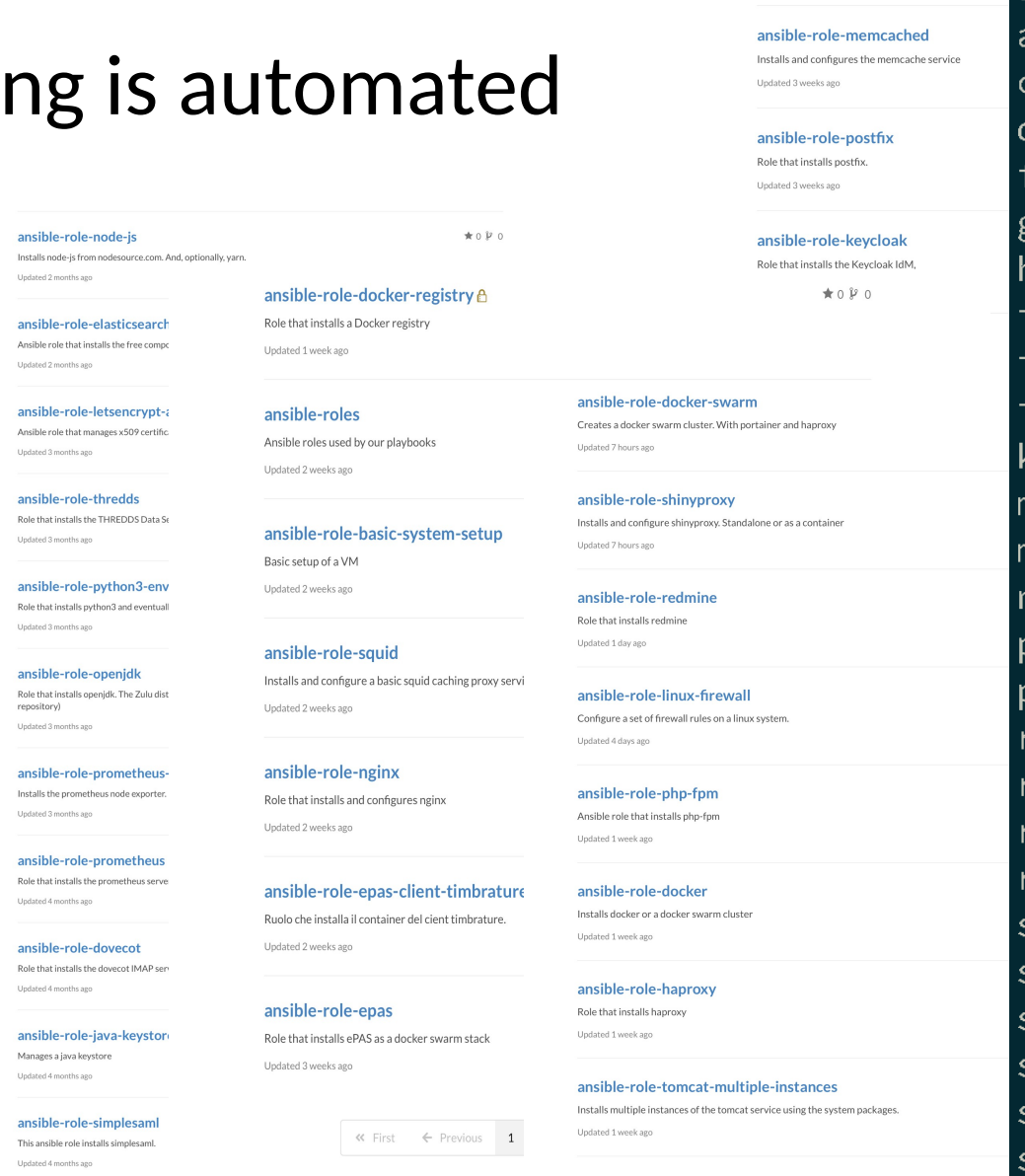
- Observability (Prometheus + Grafana)
- Services status
- Services behaviour
- Status dashboard
- Incident history



Deployment: everything is automated (mostly)

Ansible is the provisioning tool used to configure all the servers and all the services.

- All the servers share a basic configuration set (language, ssh access, timezone, firewall, dns resolver, NTP, …)
- No manual editing of configuration files
- A new instance of a server can be ready in a matter of minutes




```
antivirus-servers.yml
authoritative_dns.yml
ca.yml
dhcp-server.yml
freeipa.yml
git-server.yml
haproxy-frontend.yml
imap-director.yml
imap-pop-server.yml
imap-sync.yml
kvm_hosts.yml
mailman.yml
mediawiki.yml
nextcloud-fileserver.yml
postgresql-server.yml
powerdns_admin.yml
radius.yml
redmine.yml
resolvers.yml
roundcube-webmail.yml
san_plan_b.yml
simplesaml.yml
smtp-servers-in.yml
smtp-servers-out.yml
squid.yml
syslog-collector.yml
vm_templates_setup.yml
vpn-service.yml
zabbix-monitoring.yml
```

Ansible: a brief introduction

Essentials https://docs.ansible.com

- No client/server model. Remote hosts accessed using SSH
- Python based. A basic python setup is required on the target nodes
- Modules can be written in whatever language, but python is easier
- Components: playbooks, tasks, roles, modules, inventory, collections

Ansible concepts: control and managed nodes, inventory, collections, modules, tasks, playbooks

- Ansible runs *playbooks*
- A playbook is a set of tasks, often grouped into roles.
- Tasks use modules. Most modules guarantee idempotency (exceptions: command, shell)
- Playbooks are run on the control node and execute on the managed nodes

Ansible: a brief introduction (2)

A playbook

- A playbook usually lives on the control node
- Its execution is influenced by variables
- Variables can be associated to hosts, host groups, roles, or loaded from files
- Files that define variables, and also files that must be transferred into the managed nodes, can be encrypted

```
---
- hosts: smtp_avs_servers
  serial: 1
  roles:
    - { role: pgsql-db-management }
    - { role: ../library/bootstrap-roles/centos-common, when: ansible_distribution_file_variety == "RedHat" }
    - { role: user_services_perms }
    - ../library/roles/ssh-keys
    - clamav
    - spamassassin
```

Ansible: variables

```
---
letsencrypt_acme_install: False
letsencrypt_acme_sh_install: '{{ letsencrypt_acme_install }}'
letsencrypt_acme_sh_git_install: True
letsencrypt_update_acme_distribution: True
letsencrypt_acme_sh_git_url: https://github.com/acmesh-official/acme.sh.git
letsencrypt_acme_sh_default_ca: 'letsencrypt'
letsencrypt_acme_user: acme
letsencrypt_acme_sh_user: '{{ letsencrypt_acme_user }}'
letsencrypt_acme_user_home: /var/lib/acme
letsencrypt_acme_git_dest_dir: '{{ letsencrypt_acme_user_home }}/acme_sh_dist'
letsencrypt_acme_sh_user_home: '{{ letsencrypt_acme_user_home }}'
letsencrypt_acme_sh_base_data_dir: '{{ letsencrypt_acme_sh_user_home }}/acme_data'
letsencrypt_acme_sh_certs_data_prefix: '{{ letsencrypt_acme_sh_certificates_install_dir }}'
letsencrypt_acme_sh_certs_data_path: '{{ letsencrypt_acme_sh_base_data_dir }}/certs/{{
  letsencrypt_acme_sh_certs_data_prefix }}'
letsencrypt_acme_sh_certificates_install_dir: '{{ ansible_fqdn }}'
letsencrypt_acme_sh_certificates_install_base_path: '{{ letsencrypt_acme_sh_user_home }}/live'
letsencrypt_acme_sh_certificates_install_path: '{{ letsencrypt_acme_sh_certificates_install_base_path }}/{{
  letsencrypt_acme_sh_certificates_install_dir }}'
letsencrypt_acme_sh_log_dir: /var/log/acme
letsencrypt_acme_sh_install_cron: False
letsencrypt_acme_sh_log_enabled: True
letsencrypt_acme_sh_auto_upgrade: False
letsencrypt_acme_sh_install_options: '--install'
letsencrypt_acme_sh_test_request: False
letsencrypt_acme_sh_use_syslog: True
letsencrypt_acme_sh_syslog_level: 6     You, a year ago • Letsencrypt acme-sh-client has its own repository
```

Ansible: tasks

ansible-tasks.yml

```yaml
---
- import_tasks: acmetool_deb.yml
  when: ansible_distribution_file_variety == "Debian"

- import_tasks: acmetool_rh.yml
  when: ansible_distribution_file_variety == "RedHat"

- block:
  - name: Create the letsencrypt acme user
    user: name={{ letsencrypt_acme_sh_user }} home={{ letsencrypt_acme_sh_user_home }} createhome=no shell=/usr/sbin/nologin system=yes
    tags: ['letsencrypt', 'letsencrypt_user']

  - name: Create the letsencrypt acme home, if it does not exist already. In a separate step because it could be already there.
    file: dest={{ letsencrypt_acme_sh_user_home }} owner={{ letsencrypt_acme_sh_user }} group={{ letsencrypt_acme_sh_user }} state=directory recurse=yes

  - name: Install the acme.sh environment variables file
    template: src=acme_sh_request_env.j2 dest=/etc/default/acme_sh_request_env owner=root group=root mode=0444
    register: acme_sh_issue

  - name: Install a daily cron job to renew the certificates when needed. It runs as root
    cron:
      name: "Letsencrypt certificate renewal"
      day: '{{ letsencrypt_acme_cron_day_of_month }}'
      hour: '{{ letsencrypt_acme_cron_hour }}'
      minute: '{{ letsencrypt_acme_cron_minute }}'
      job: "/usr/local/bin/acme-sh-cron-script > {{ letsencrypt_acme_sh_log_dir }}/acme-cron.log 2>&1"
    tags: ['letsencrypt', 'letsencrypt_cron', 'letsencrypt_acme_sh', 'letsencrypt_acme_sh_scripts']

  - name: Remove the daily cron job that run as acme user.
    cron:
      name: "Letsencrypt certificate renewal"
      day: '{{ letsencrypt_acme_cron_day_of_month }}'
      hour: '{{ letsencrypt_acme_cron_hour }}'
      minute: '{{ letsencrypt_acme_cron_minute }}'
      job: "/usr/local/bin/acme-sh-cron-script > {{ letsencrypt_acme_sh_log_dir }}/acme-cron.log 2>&1"
      state: absent
    tags: ['letsencrypt', 'letsencrypt_cron', 'letsencrypt_acme_sh']

  become: True
  become_user: '{{ letsencrypt_acme_sh_user }}'
  when: letsencrypt_acme_sh_install | bool
  tags: ['letsencrypt', 'letsencrypt_acme_sh']
```

Ansible: play run

`ansible-playbook --vault-password-file=<LOL>' ca.yml -i inventory/hosts -t letsencrypt`

```
PLAY [certification_authority] *************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
Thursday 14 October 2021  20:39:56 +0200 (0:00:00.150)       0:00:00.150 ******
Thursday 14 October 2021  20:39:56 +0200 (0:00:00.150)       0:00:00.150 ******
ok: [ca.isti.cnr.it]

TASK [postfix-client : Create the acme hooks directory if it does not exist] ***************************************
Thursday 14 October 2021  20:40:00 +0200 (0:00:03.788)       0:00:03.938 ******
Thursday 14 October 2021  20:40:00 +0200 (0:00:03.788)       0:00:03.938 ******
skipping: [ca.isti.cnr.it]

TASK [postfix-client : Install a hook for letsencrypt] *************************************************************
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.064)       0:00:04.003 ******
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.064)       0:00:04.002 ******
skipping: [ca.isti.cnr.it]

TASK [letsencrypt-acme-sh-client : Install the socat utility, needed when using the http protocols to request the certificates] **
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.048)       0:00:04.051 ******
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.048)       0:00:04.050 ******
skipping: [ca.isti.cnr.it]

TASK [letsencrypt-acme-sh-client : Install the git client if we are installing using git] *************************
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.044)       0:00:04.095 ******
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.044)       0:00:04.095 ******
skipping: [ca.isti.cnr.it]

TASK [letsencrypt-acme-sh-client : Install the socat utility, needed when using the http protocols to request the certificates] **
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.047)       0:00:04.142 ******
Thursday 14 October 2021  20:40:00 +0200 (0:00:00.047)       0:00:04.142 ******
changed: [ca.isti.cnr.it]

TASK [letsencrypt-acme-sh-client : Install the git client if we are installing using git] *************************
Thursday 14 October 2021  20:40:07 +0200 (0:00:06.162)       0:00:10.305 ******
Thursday 14 October 2021  20:40:07 +0200 (0:00:06.162)       0:00:10.305 ******
changed: [ca.isti.cnr.it]

TASK [letsencrypt-acme-sh-client : Activate the firewalld rule for the http, if we require certificates using the http protocol] *
Thursday 14 October 2021  20:40:31 +0200 (0:00:24.652)       0:00:34.957 ******
Thursday 14 October 2021  20:40:31 +0200 (0:00:24.652)       0:00:34.957 ******
changed: [ca.isti.cnr.it] ⇒ (item={'domain': 'ca.isti.cnr.it', 'standalone': True})
```

Evolution of the ISTI infrastructure

The technical buzzwords

- Servers consolidation
- Cloud computing, on premise
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Managed Software as a Service (MSaaS)
  - Functions as a Service (FaaS)
  - Object storage
  - Distributed block storage
  - Distributed Posix File system
  - Containers Orchestrator (Kubernetes, Docker Swarm)

What does it even mean?

- Contribute hardware to the infrastructure
- Everything runs in the same infrastructure (when possible)
- Resources available to each laboratory, based on the contributions and the needs
- Federated SSO
- Federated resources, potentially

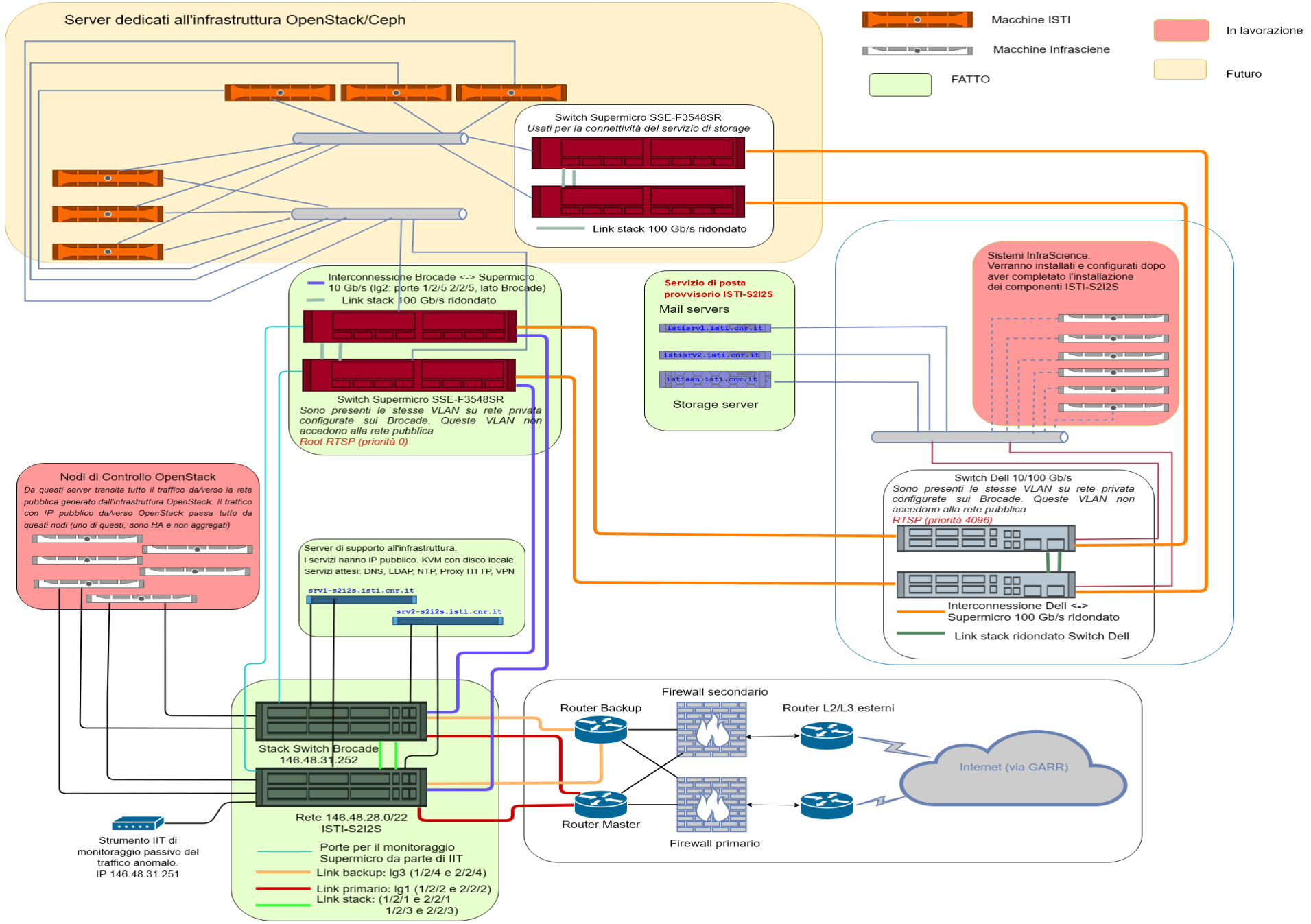
ISTI Services: next steps

- IAM, to enable SSO between all services
  - 2FA, with both applications (Google authenticator, for example) and hardware keys: yubikeys, solo keys, feitian, etc (they cost money)
- Nextcloud general availability, and
  - OnlyOffice integration
  - Draw.io integration
  - Integration with the webmail
- Git server general availability

Security (see the aGID guidelines):

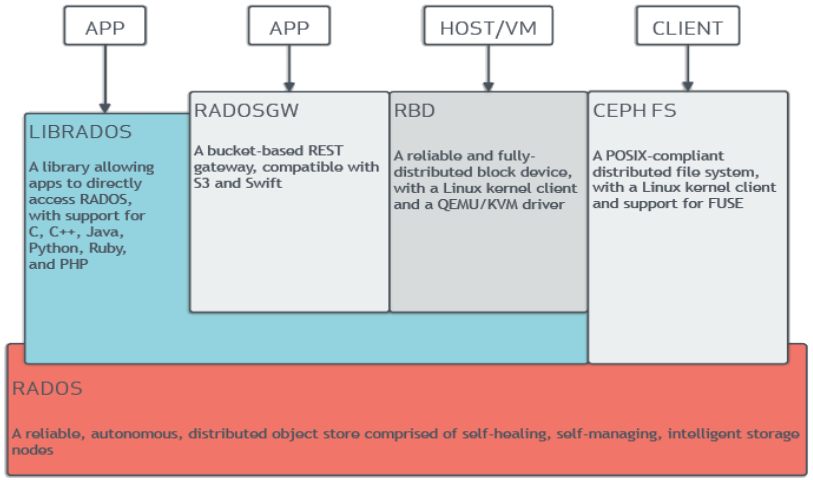
- Logs centralization
- Alerting based on log patterns
- A SIEM system

#	Project	Tracker	Status	Priority	Subject
1019	Possibili evoluzioni	Service	New	Normal	Istanza condivisa di Overleaf (sharelatex)
993	Possibili evoluzioni	Feature	New	Normal	SIEM: attivare una infrastruttura di logging e report compatibile SIEM
936	Possibili evoluzioni	Feature	New	Normal	Plugin nextcloud per la webmail
774	Possibili evoluzioni	Service	New	Normal	Autodiscovery per la configurazione della posta
684	Possibili evoluzioni	Feature	New	Normal	Attivare DNSSEC sulle nostre zone
635	Possibili evoluzioni	Service	New	Normal	Servizio che permetta di gestire newsletter
609	Possibili evoluzioni	Feature	New	Normal	Recupero password self service su freeipa
549	Possibili evoluzioni	Service	New	Normal	Zulip come chat collaborativa
539	Possibili evoluzioni	Service	New	Normal	Sistema free (open source) di videoconferenza
413	Possibili evoluzioni	Feature	New	Normal	Form per la richiesta di registrazione dei domini
313	Possibili evoluzioni	Service	New	Normal	Look dell'interfaccia web dell'autenticazione dell'IdP
288	Possibili evoluzioni	Feature	New	Normal	Soluzione per il Disaster recovery
287	Possibili evoluzioni	Feature	New	Normal	Sistema di backup con cifratura
243	Possibili evoluzioni	Service	New	Normal	Ricerca server side per le email
240	Possibili evoluzioni	Service	New	Normal	Mailbox sull'object storage
239	Possibili evoluzioni	Service	New	Normal	Notifiche push per l'email
238	Possibili evoluzioni	Feature	New	Normal	Mailbox cifrate sul server imap
206	Possibili evoluzioni	Feature	New	Normal	Valutare l'introduzione di DNS over HTTPS
205	Possibili evoluzioni	Feature	New	Normal	Valutare 'LetsMapYourNetwork'

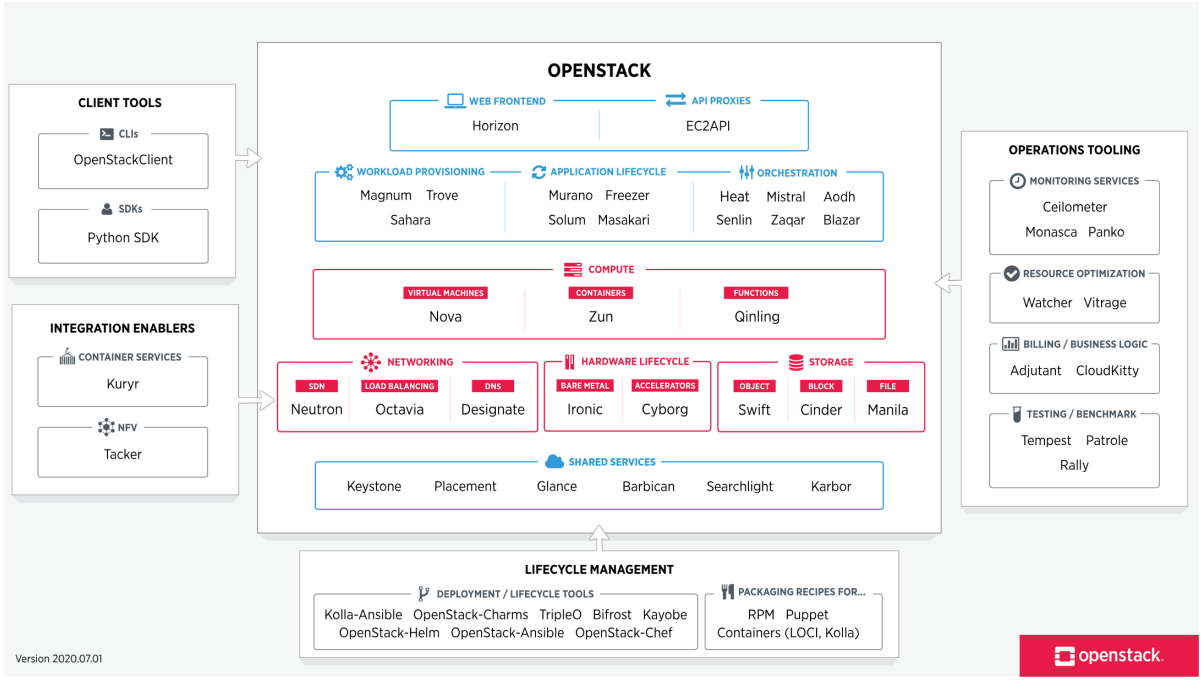

Server dedicati all'infrastruttura OpenStack/Ceph
Macchine ISTI
Macchine Infrasciene
FATTO
In lavorazione
Futuro
Switch Supermicro SSE-F3548SR
Usati per la connettività del servizio di storage
Link stack 100 Gb/s ridondato
Interconnessione Brocade <-> Supermicro
10 Gb/s (lg2: porte 1/2/5 2/2/5, lato Brocade)
Link stack 100 Gb/s ridondato
Switch Supermicro SSE-F3548SR
Sono presenti le stesse VLAN su rete privata configurate sui Brocade. Queste VLAN non accedono alla rete pubblica
Root RTSP (priorità 0)
Servizio di posta provvisorio ISTI-S2I2S
Mail servers
istisrv1.isti.cnr.it
istisrv2.isti.cnr.it
istisxn.isti.cnr.it
Storage server
Sistemi InfraScience.
Verranno installati e configurati dopo aver completato l'installazione dei componenti ISTI-S2I2S
Switch Dell 10/100 Gb/s
Sono presenti le stesse VLAN su rete privata configurate sui Brocade. Queste VLAN non accedono alla rete pubblica
RTSP (priorità 4096)
Interconnessione Dell <-> Supermicro 100 Gb/s ridondato
Link stack ridondato Switch Dell
Nodi di Controllo OpenStack
Da questi server transita tutto il traffico da/verso la rete pubblica generato dall'infrastruttura OpenStack. Il traffico con IP pubblico da/verso OpenStack passa tutto da questi nodi (uno di questi, sono HA e non aggregati)
Server di supporto all'infrastruttura.
I servizi hanno IP pubblico. KVM con disco locale.
Servizi attesi: DNS, LDAP, NTP, Proxy HTTP, VPN
srv1-s2i2s.isti.cnr.it
srv2-s2i2s.isti.cnr.it
Stack Switch Brocade
146.48.31.252
Rete 146.48.28.0/22
ISTI-S2I2S
Strumento IIT di monitoraggio passivo del traffico anomalo.
IP 146.48.31.251
Porte per il monitoraggio Supermicro da parte di IIT
Link backup: lg3 (1/2/4 e 2/2/4)
Link primario: lg1 (1/2/2 e 2/2/2)
Link stack: (1/2/1 e 2/2/1
1/2/3 e 2/2/3)
Router Backup
Firewall secondario
Router L2/L3 esterni
Router Master
Firewall primario
Internet (via GARR)

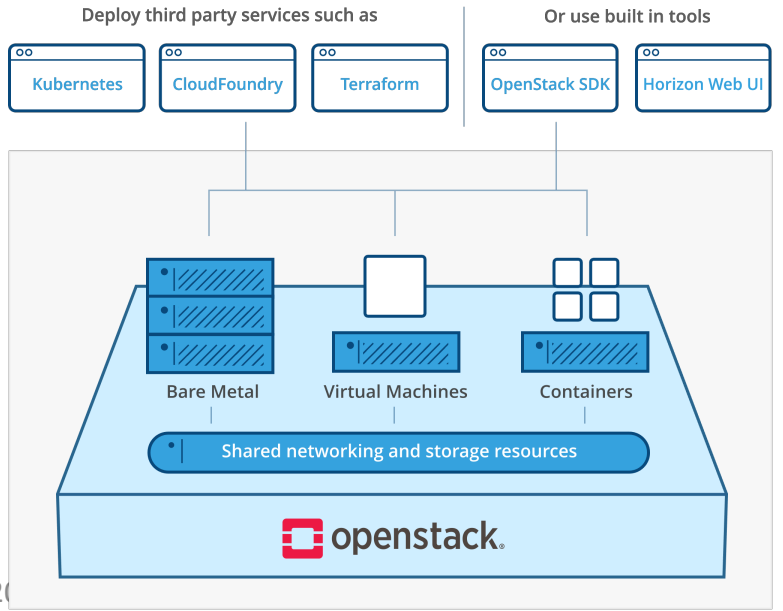
Infrastructure: next steps

- Fix the wiring between switches and servers
- Start the OpenStack installation (hyperconverged)
- Test the functionalities
- Test at least one live upgrade of the OpenStack distribution
- Start migrating the ISTI and InfraScience (D4Science) services



Hyperconverged: each server is used for both computing and distributed storage





Una infrastruttura complessa: *perché tanto odio?**

(* cit. https://fr.wikipedia.org/wiki/Édika)

L'impegno per la realizzazione di una infrastruttura così complessa è giustificato dalla necessità di fornire servizi sofisticati

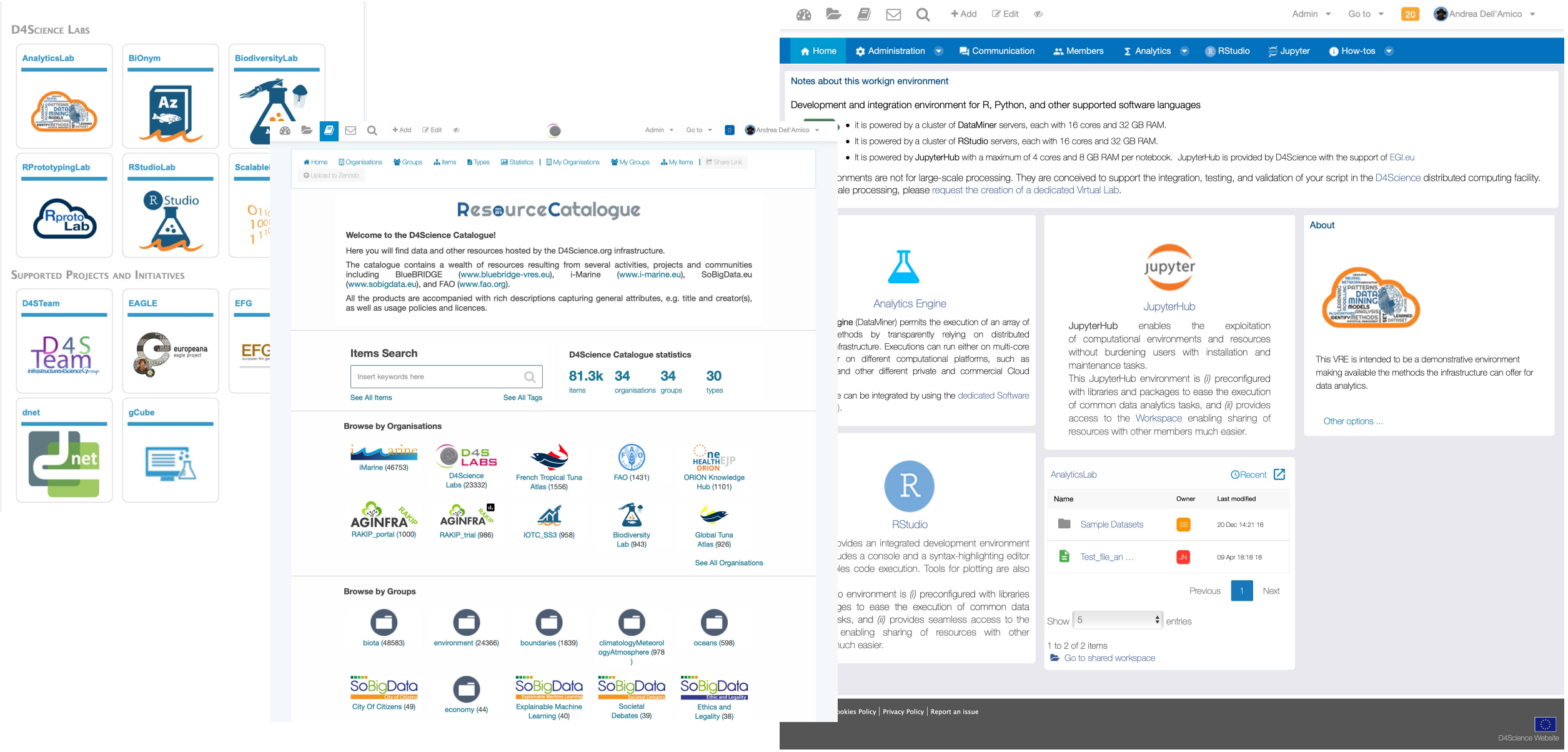
Servizi specifici per l'istituto

- Posta elettronica
- DNS
- Autenticazione
- Supporto agli utenti
- Wiki
- Git
- Cloud storage (nextcloud)
- (eccetera)

Supporto alla ricerca (D4Science, OpenAIRE): VRE, Virtual Research Environments

- VRE (Virtual Research Environment): storage, messaggistica, social
- Autenticazione federata (soggetta all'accettazione di Terms of Use)
- Servizi gestiti, disponibili ai ricercatori (JupyterHub, Rstudio, Shinyproxy, OverLeaf, catalogo CKAN-based, Geoserver, Geonetwork, Hadoop...)
- Esecuzione di esperimenti con workflow FAIR (Analytics Engine, prossimamente container based)

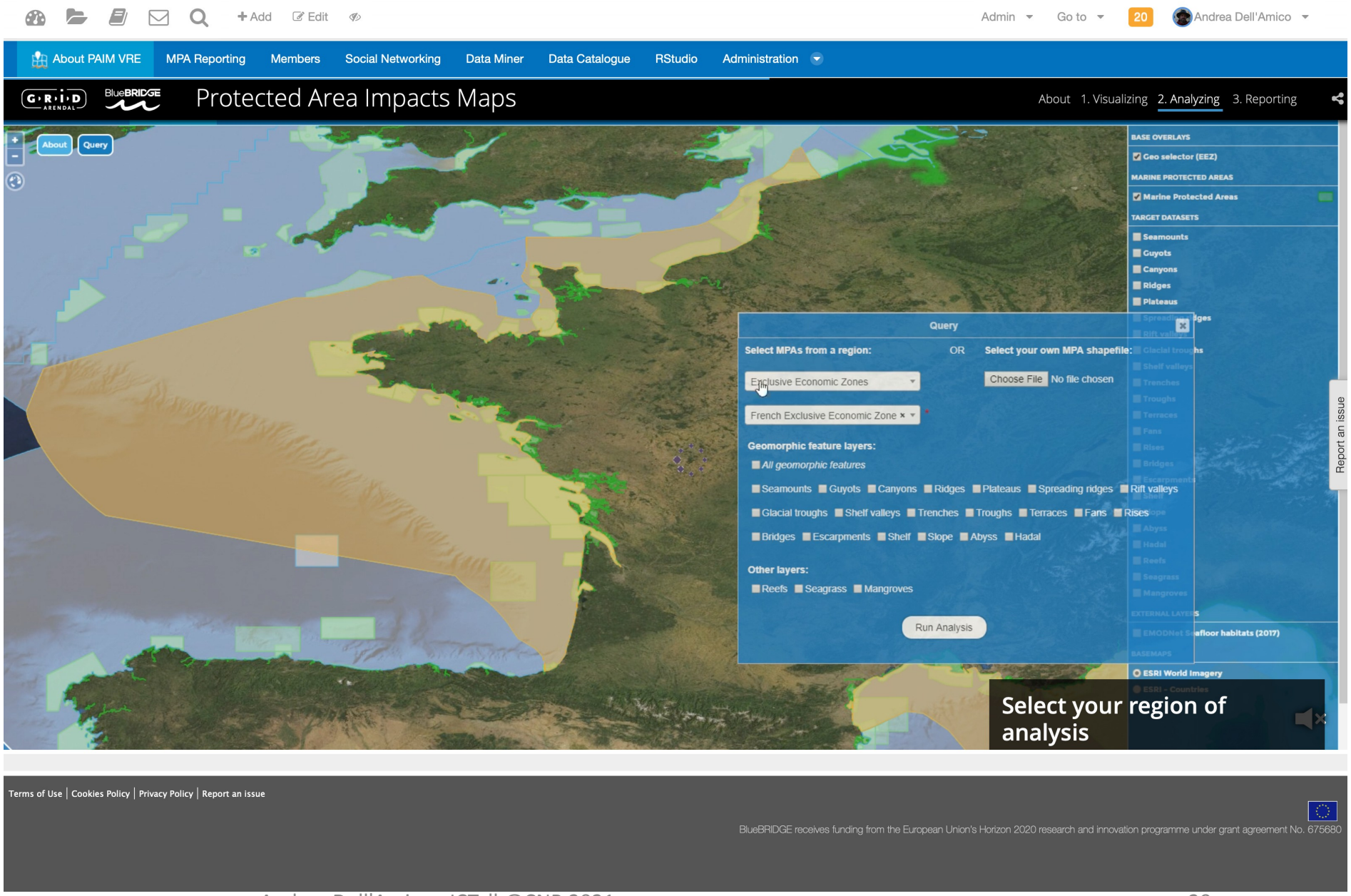
Main D4Science gateway: https://services.d4science.org



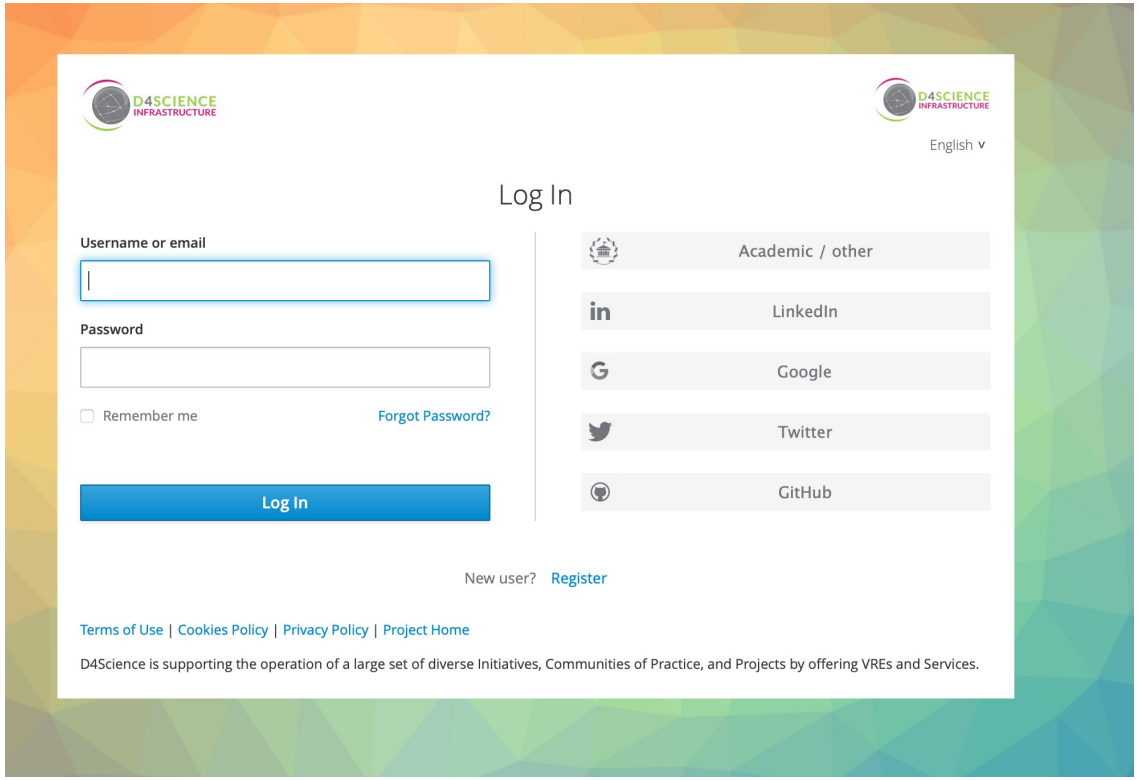
Use case: Protected Area Impacts Maps
https://i-marine.d4science.org/web/protectedareaimpactmaps

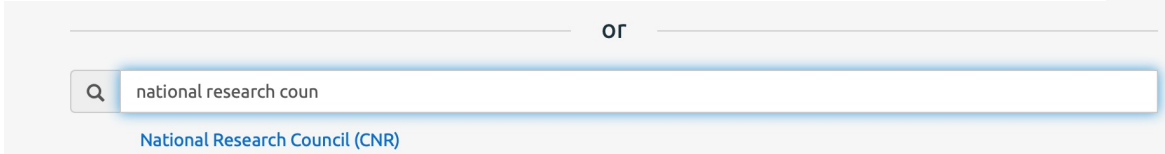
Involved services and resources:

- (Authentication)
- (Authorization)
- Static web application
- Dataminer (Analytics engine)
- Geoserver
- Workspace
- FAIR

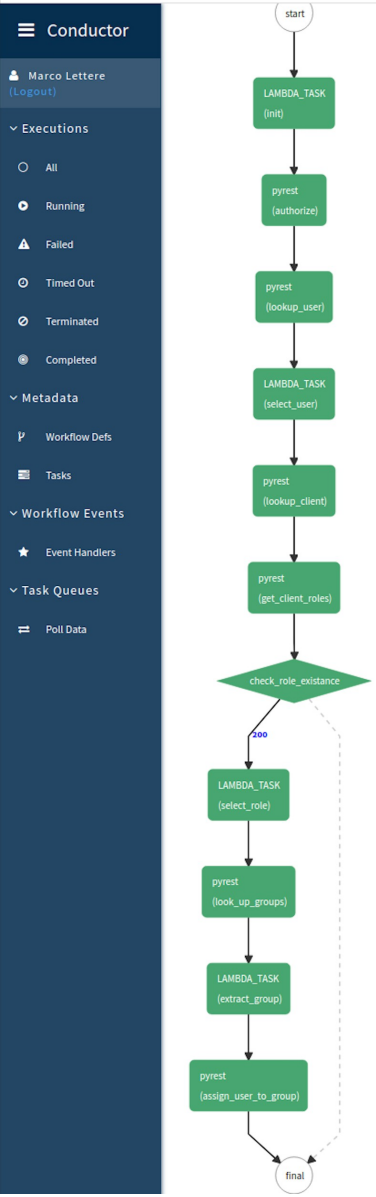


D4Science authentication and authorization flow (Keycloak, OIDC, federation)





D4Science authentication and authorization flow (Keycloak, orchestrator, VRE and users setup)



Name * Default Permission

Description

esource Type OFF

Resources * Default Resource

Apply Policy Select existing policy...

Name	Description
VO-Admin_policy	
VRE-Manager_policy	
Catalogue-Admin_policy	
Data-Manager_policy	
Infrastructure-Manager_policy	
Accounting-Manager_policy	
DataMiner-Manager_policy	
Data-Editor_policy	
VRE-Designer_policy	
Catalogue-Editor_policy	
Member_policy	

sion Strategy Affirmative

Save Cancel

Clients

Lookup

Search...

Client ID
%2Fd4science.research-infrastructures.eu
%2Fd4science.research-infrastructures.eu%2FD4OS
%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_AggregationMgmt
%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_Lab
%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_Mappings
%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_Project
%2Fd4science.research-infrastructures.eu%2FD4OS%2FArcheomar
%2Fd4science.research-infrastructures.eu%2FD4OS%2FArianna
%2Fd4science.research-infrastructures.eu%2FD4OS%2FBlue-CloudLab
%2Fd4science.research-infrastructures.eu%2FD4OS%2FBlue-CloudProject
%2Fd4science.research-infrastructures.eu%2FD4OS%2FDisseminationEventsCollaboratory
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCCollaboratory
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillar4AgriFood
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillar4EarthScience
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarITServiceRegistry
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarOS4SSCH
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarOSTA
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarResDataCtlg
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarServiceRegistry
%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarTrainingAndSupport

First Page Previous Page Next Page

The end
Grazie!

Any questions?