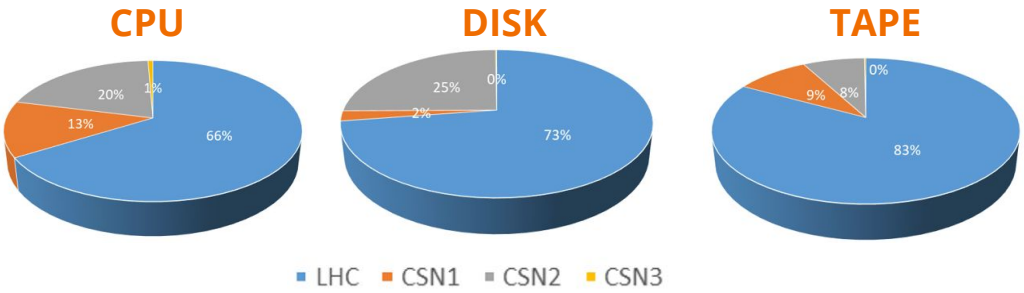
IAM @ INFN-T1

Lucia Morganti

Experiments @INFN-T1

- INFN-T1 supports 44 experiments
- LHC experiments use about
  - 65% of CPU resources
  - 70% of disk space
  - 80% of tape space



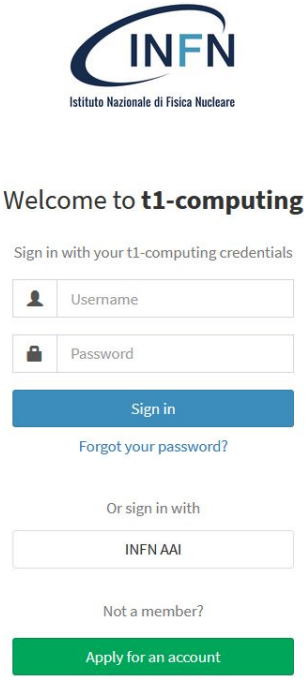
Moving beyond X.509 certificates

- Complaints about handling X.509 certificates: not immediate, not flexible, too complex
- Typically, non-LHC users are interested in the opportunity of navigating data with browsers, and VOMS does not work in browsers

- Also, a gradual transition away from X.509 and towards token-based authn/authz is foreseen in the context of DOMA WGs
- As a result: even if most users currently use VOMS-based authn/authz, there is increasing interest in IAM from many experiments and user communities, not only small ones but also Virgo, CTA, Juno, BelleII...

IAM @INFN-T1: a catch-all instance

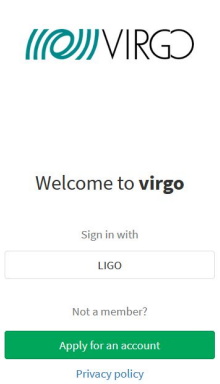
- For collaborations “allergic” to certificate/VOMS, and typically interested in Web data browsability and/or data access from cloud resources
- Login integrated with INFN AAI
- Users assigned to groups
- New users can apply for an account and for group membership (admin-moderated flow)

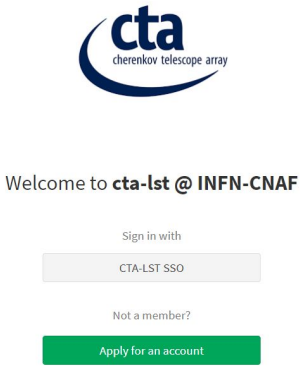


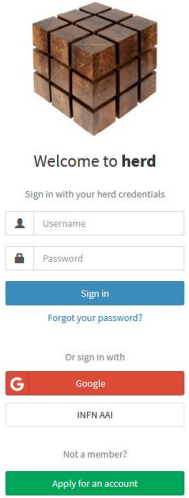
IAM @INFN-T1: dedicated instances

- Depending on the size of the experiment and/or on specific requirements for the IAM instance (e.g. usability by other sites, support of specific IdP), dedicated IAM instances have been configured, e.g.
  - CTA-LST, connected to a Keycloak instance @PIC
  - VIRGO, with LIGO credentials
  - HERD
  - …

…







IAM @INFN-T1: support at storage level

IAM integration is supported at storage level with StoRM WebDAV

- StoRM WebDAV supports OpenID connect authn/authz on storage areas.
- StoRM WebDAV supports fine-grained authorization targeting specific authenticated groups of users
- Data access via browser, following the OIDC login
- Data access via command line using OIDC-agent, a set of tools to manage OpenID Connect tokens from cli
  - OIDC-agent is currently installed on the UIs at INFN-T1
  - User support provides documentation and training on how to configure and use OIDC-agent to get token and access the storage
  - Some complaints: client registration is not immediate, not always possible to install OIDC-agent, token expiration

Next step: IAM integration at HT Condor level

- The stable version of HTCondor is used at INFN-T1
  - Tokens are supported in testing version of HTCondor (8.9.x) and HTCondor-CE (4.x),
  - As soon as the support for tokens will be provided in stable releases, we'll offer that
- Planning to setup a HTCondor testbed for tests in March 2021