MetaCentrum

MetaCentrum – the Czech computational grid

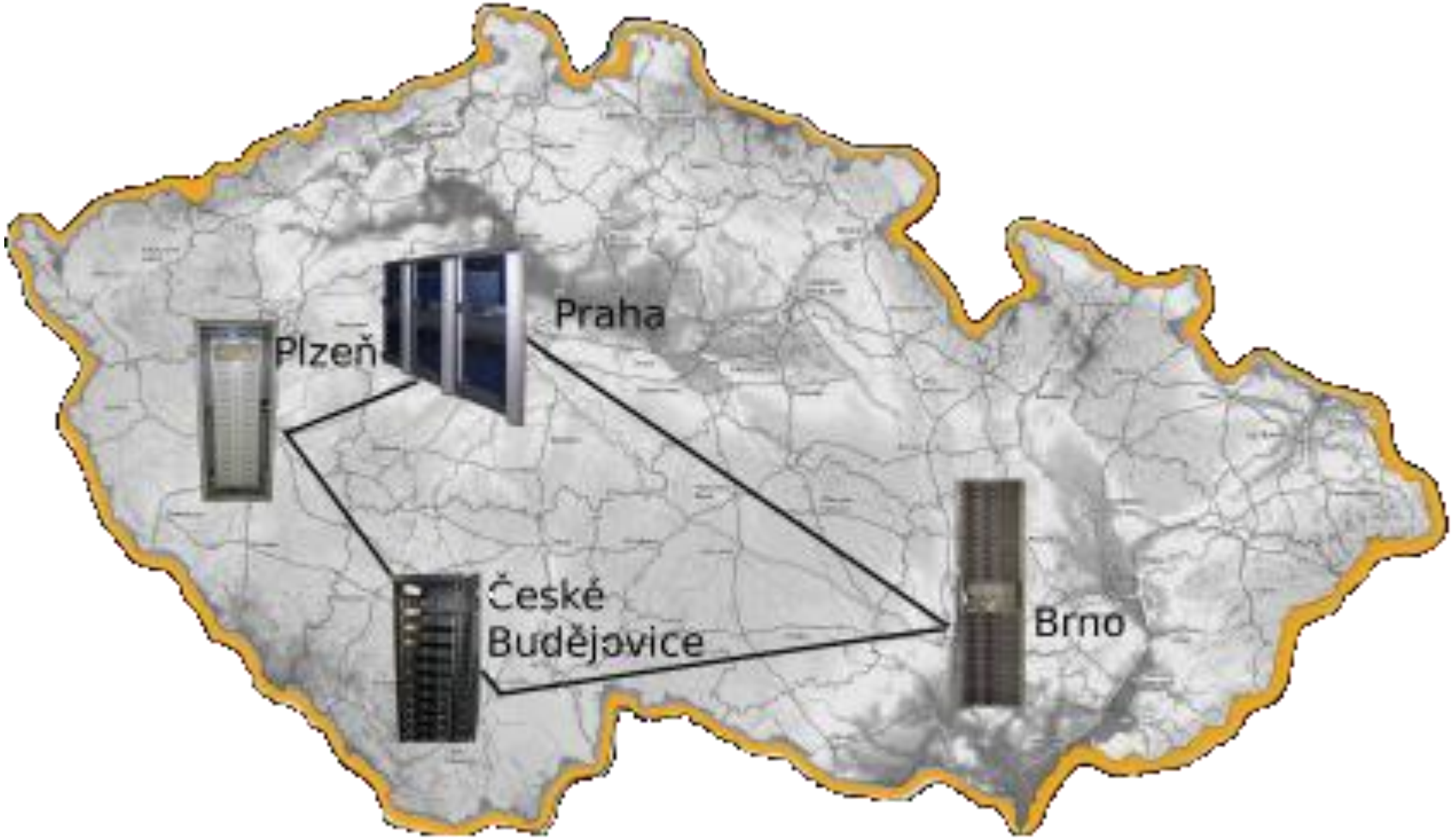
Martin Kuba
CESNET and Masaryk University
Brno, Czech Republic

Highlights

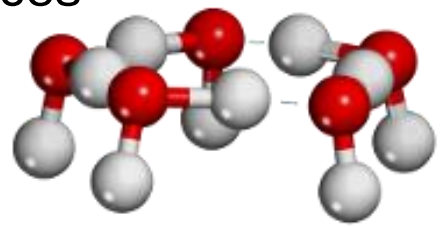
- MetaCentrum is a computing infrastructure pooling resources contributed by several universities, using AFS and Kerberos
- the mod_auth_kerb module for the Apache http server is maintained by Dan Kouřil of MetaCentrum
- Kerberos support for Firefox/Mozilla was developed in MetaCentrum

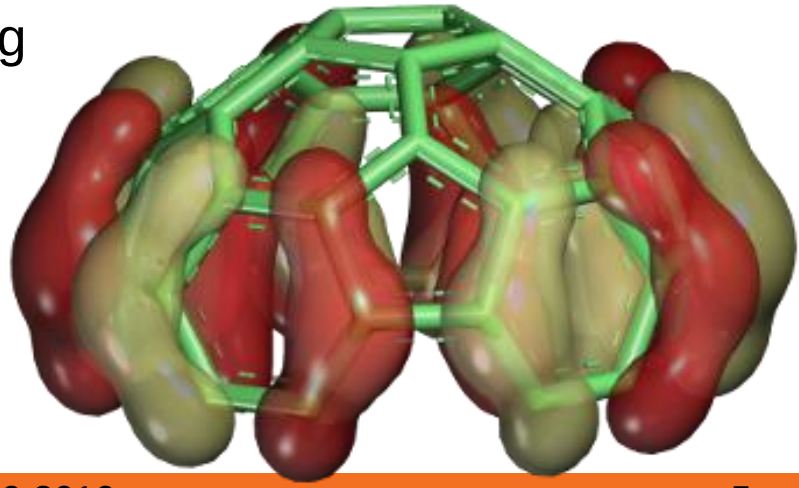
- MetaCentrum was established in 1996 as a supercomputing meta-center consisting of
  - Supercomputing Center at Masaryk University in Brno
  - Supercomputing Center at University of West Bohemia in Plzeň
  - Supercomputing Center at Charles University in Prague
- later included
  - CESNET – operator of the Czech NREN (academic network)
  - University of South Bohemia in České Budějovice (Budweis)
  - University of Technology in Brno
- now connects 15 computer clusters consisting of 290 machines with 1500 CPUs, located in six geographical locations

MetaCentrum map



- MetaCentrum is open and free for the Czech academic community
- users can be scientists or students from
  - 26 public universities
  - 57 institutes of the Czech Academy of Sciences
- challenges in establishing user identity
- users run applications for
  - computational chemistry
  - structural biology, protein engineering
  - material and structural simulations
  - liquid and gas flow simulations
  - mathematics, number theory
  - speech recognition and generation





- MetaCentrum was involved in the DataGrid, EGEE I,II,III and EGI Design Study projects
- the coming **European Grid Infrastructure** (EGI) is organized in National Grid Infrastructures (NGIs)
- MetaCentrum is now transforming into the Czech NGI, its free resources will be one of many VOs (Virtual Organizations)

Infrastructure

- clusters of linux x86-compatible machines
  - strongest machines have 8x quadcore Opteron (32 cores), 256GB
- user accounts are maintained by own system Perun
  - Oracle database holding users, machines, accounts, etc.
  - master-slave architecture, generating local config files on changes
- several file systems (local,NFSv3,NFSv4,AFS)
- single sign-on using Kerberos
  - first access using Kerberos PAM module
  - Kerberized ssh, telnet, ftp, rsh (MPI needs)
- workload management system PBSPro, moving to Torque
  - Kerberized, own ticket renewal system for long running jobs
- web portal, supports Kerberos, SSL certs, Shibboleth, ...

File systems

- several file systems for various needs
  - fast, but small and not shared – local HDD or SSD
  - large and shared, but slower - NFSv4 on all machines (100TB)
  - home directories shared by NFSv3 on local clusters
  - software installed on AFS with multiple read-only copies
  - experiments with Lustre for shared network scratch
- for shared FS we need Kerberos authN (not trusting admins of clients), thus NFSv4 or AFS
- both can be installed on user workstations from standard SUSE/Debian/Ubuntu repositories
- AFS is slow compared to NFSv4
- both support ACL, AFS only directories, NFSv4 also files
- AFS supports multiple read-only copies

- users can come from many of institutions
- ways of establishing user identity on web portal
  - paper application with boss' signature (slow and too much work)
  - SSL client certificates (complicated, needs visit to RA)
  - eduroam (Wi-Fi federation)
  - access to local ID system (WebAuth, LDAP, Kerberos)
  - SAML (Shibboleth) identity federation eduId.cz
- after establishing identity, MetaCentrum account is created, annual renewal in exchange for report of activities
- authN to MetaCentrum machines
  - Kerberos
  - username/password translated to Kerberos
  - One Time Passwords translated to Kerberos

User authentication to web portal

- users manage their account through web portal
- authentication in web browser
  - username/password (HTTP basic auth) to mod_auth_kerb
    - creates Kerberos ticket on the web server
    - mod_auth_kerb maintained by Daniel Kouřil of MetaCentrum
    - used by majority of users
  - Negotiate – GSSAPI Kerberos
    - needs negotiation support in browser (MSIE and Konqueror have)
    - support for Firefox/Mozilla was created as bachelor thesis in MetaCentrum and later included into the Firefox sources
    - used only by our security experts ☺
  - SSL client X509 certificates from grid Certification Authorities
    - grid certificates have unique Distinguished Names
    - best method, no typing or clicking, but used by few
- created new **mod_ssl_preauth** to have SSL client certs and other auth modules on one URL

USB tokens

- we tried USB token (Rainbow iKey 3000) for storing private key and certificate
- PKCS11 device
- encrypts and signs internally, never gives out the private key
- unsuccessful experiment
  - connector damaged after weeks
  - many applications do not support
  - problems with drivers
  - uncomfortable, must be connected to computer during work

Real authentication in MetaCentrum

- typical user authentication:
  - account created after authentication using identity federation
    - user selects username and password
  - first login using username/password to frontend machine
    - kerberos ticket and AFS tokens on the frontend machine
  - jobs submitted using kerberized PBSPro
    - delegates kerberos ticket and AFS tokens
  - login to computing machines using kerberized ssh
    - delegates kerberos ticket and AFS tokens
  - long running jobs have Kerberos tickets renewed
    - using krb525
- MetaCentrum maintains its own accounts in Kerberos
  - Shibboleth identity federation so far works only on web
  - no dependence on external services

Thank you

- http://www.MetaCentrum.cz/
- Thank you for your attention
- Questions ?