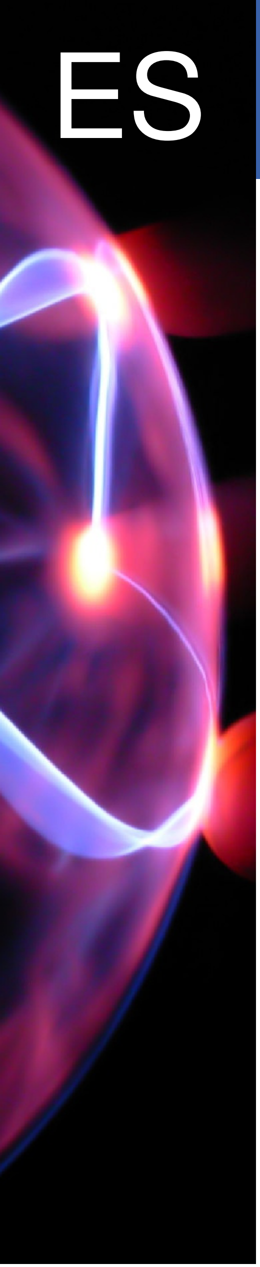
ATLAS Central Services and Computing Security

Flavia Donno

CERN/IT-ES-VOS

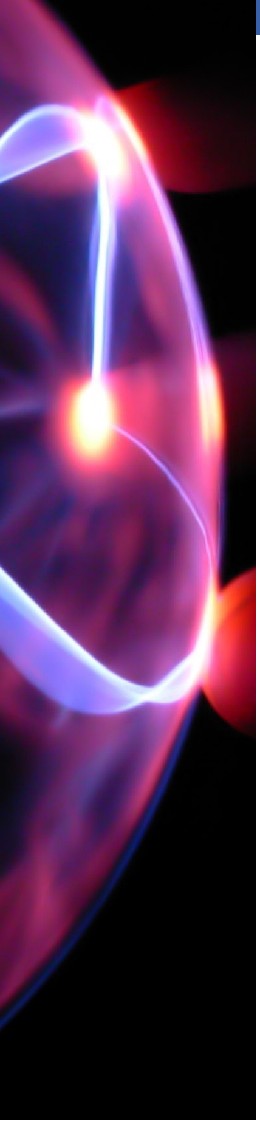


Outline

- ***Security in ATLAS: can this model be exported to other LHC experiments?***
  - Why we do it
  - How we do it: policies and measures

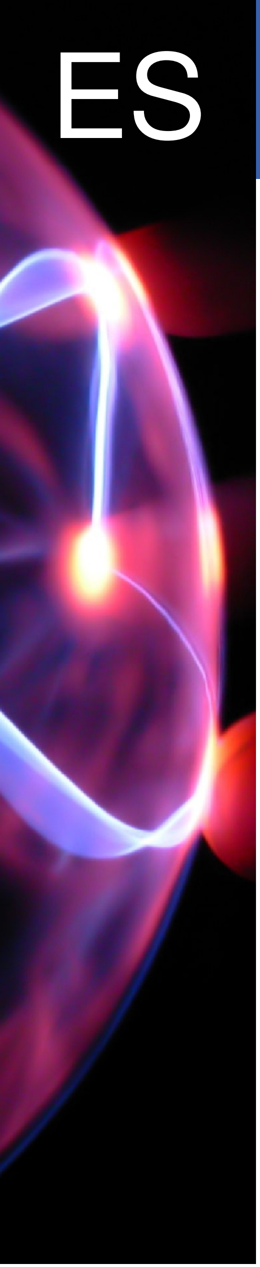
- ***The ATLAS Central Services Operations Team. Can we share procedures, experiences, tools?***
  - What we do
  - Some details: service inventory and the web redirector
  - Better interface and documentation to CERN/IT available tools.

ATLAS Security: The Goal



- ***Minimize ATLAS central services unavailability*** during data taking, mitigating vulnerability and improving operation and management of ATLAS services.

- ***Preserve ATLAS reputation worldwide***.
  - The focus is on security
  - Security cannot be enforced without good service management practices → ***Policies***
  - Strategy: increase robustness and availability of critical services while containing vulnerabilities of less critical ones → ***Plan***



ATLAS Security: references

- Various CERN IT and wLCG/EGEE documents define policies and good practices:
  - VOBox Service Level Agreement (CERN-IT/FIO-FS)
    - https://twiki.cern.ch/twiki/pub/FIOgroup/FsSLA/sla-v1.2.1.pdf
  - VOBox Security Recommendations and Questionnaire (wLCG Joint Security Policy Group)
    - https://edms.cern.ch/file/639856/0.6/VO-Box-security-policy-0-6.pdf
  - GRID system administrators best practice and guidelines (EGEE security group)
    - http://rss-grid-security.cern.ch/glite.php?display=1

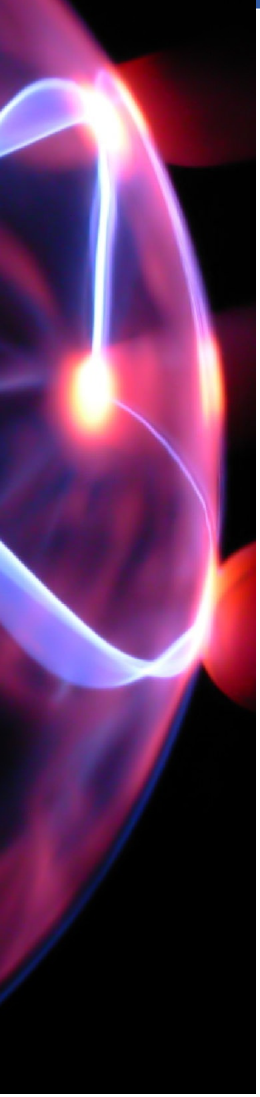
SECURITY POLICIES AND PLAN FOR CERN ATLAS CENTRAL SERVICES

https://twiki.cern.ch/twiki/pub/Atlas/ATLASInternalSecurityPlan/ATLAS_Security_PlanV20.pdf

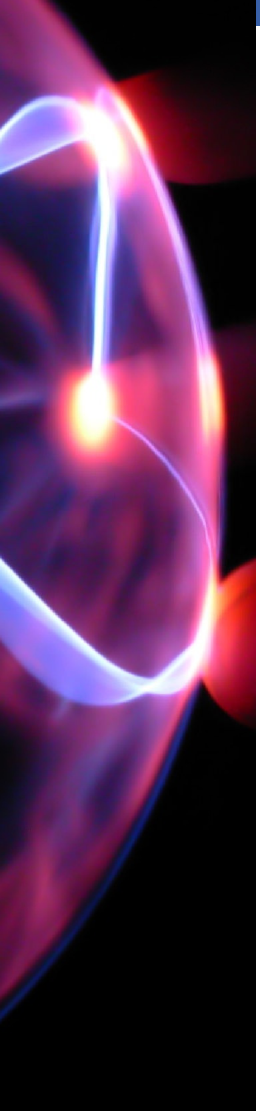
–Special thanks to **Sebastian Lopienski, Romain Wartel** and **Stefan Lueders**

The policies

- The policies can be summarized in the following points:
  - All hardware, software and configuration requests go through the ATLAS Central Services Operations Team
  - Services are catalogued through a standard Service Documentation Card (contacts, network configurations, files footprints, draining procedures, recovery procedures, etc.)
  - All service machines are quattorized, with alarms, exceptions and actuators in place (services are distributed via rpms and configured via SINDES)



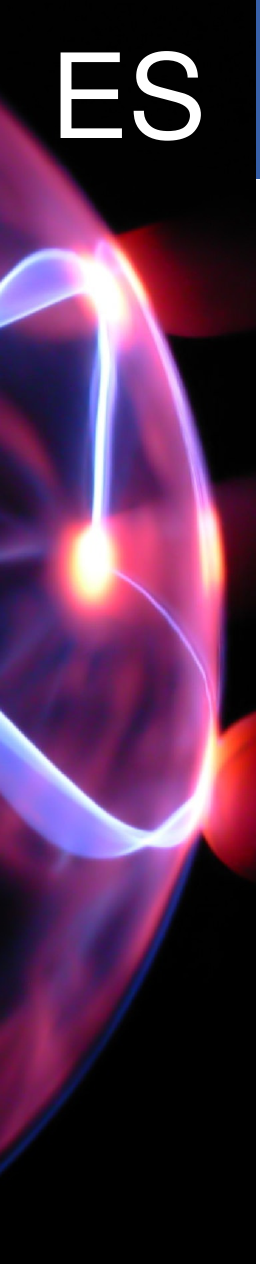
The security measures

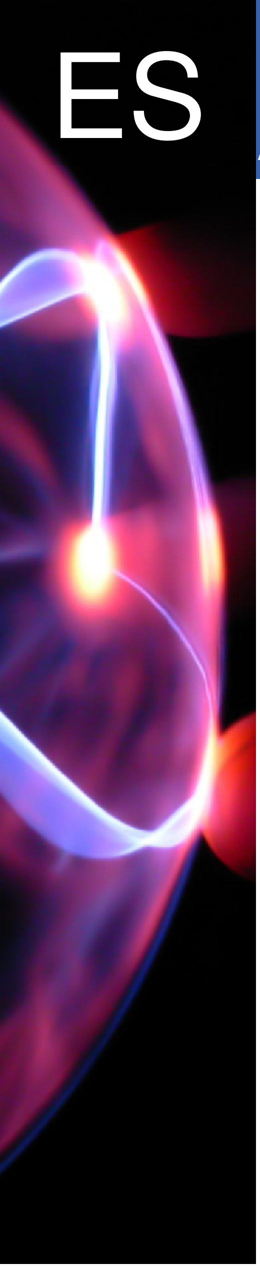


- Service inventory completed with service documentation cards
- Network services reduced to the necessary
- Restricted incoming/outgoing connections (local firewall)
- Limited interactive/root/sudo access
- Security patches
- Security scan campaigns
- Procedures for handling a security incident
- Training

What can we share?

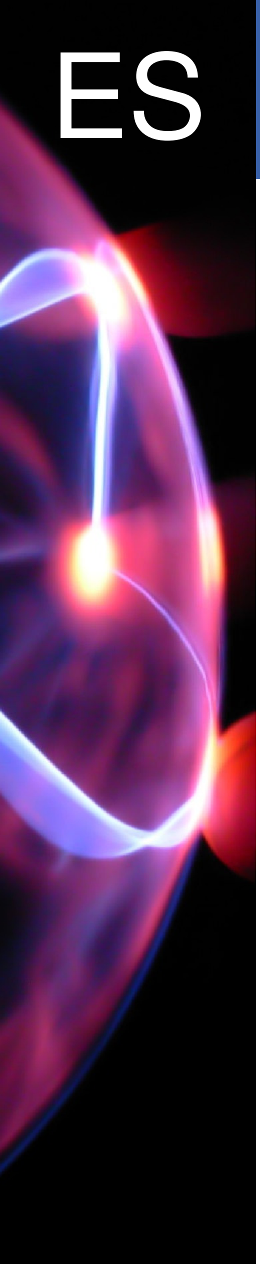
- ***Service inventory DB? Service documentation card ?***
- ***Security patches for software used by the experiments***
- ***Procedures***
- ***Experience – Common support team***
  - Vulnerabilities discovered on commonly used software?
  - Network scan results
  - …





ATLAS Central Services Team

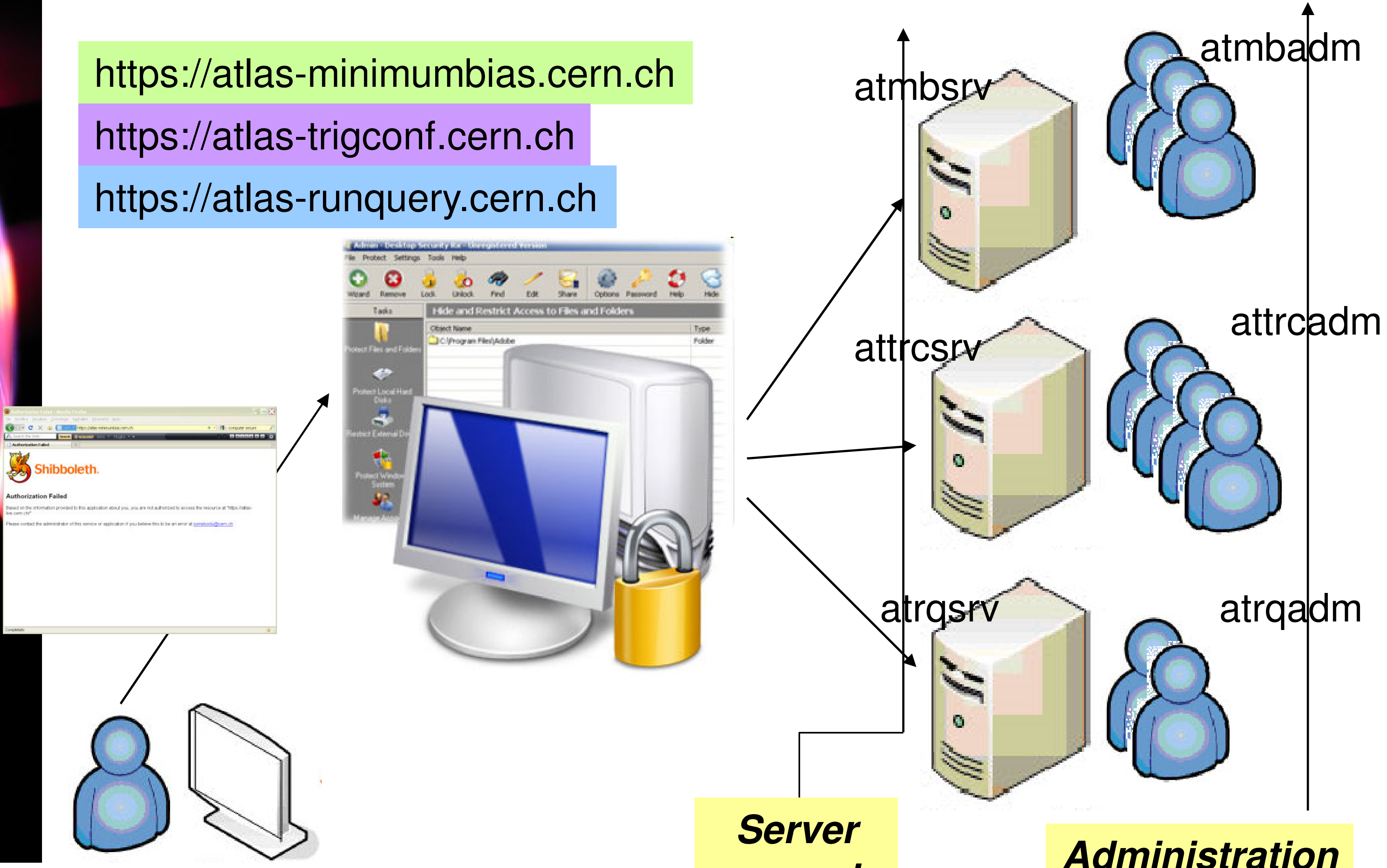
- ***ATLAS VOC*** for CERN/IT (Alarm Tickets, security, etc.)
- ***Management of ATLAS Central Services*** according to the SLA between CERN-IT and ATLAS (hardware requests, quattor, best practices, etc.)
- ***Providing assistance*** with machine, software and service management to ATLAS service developers and providers (distribution, software versions, rebooting, etc.)
- ***Provision of general frameworks***, tools and practices to guarantee availability and reliability of services (squid/frontier distribution, web redirector, hot spares, sensors, better documentation, etc.)
- ***Collection of information*** and operational statistics (service inventory, machine usage, etc.)
- Enforcing the application of ***security*** policies
- ***Training*** of newcomers in the team
- Spreading knowledge among service developers and providers about the ***tools available within CERN/IT*** (Shibboleth2, SLS, etc.)



Availability in ATLAS

- Normal operations are complemented by the following actions to ensure availability of services:
  - ***Every ~6 months*** the ATLAS VOC will exercise ***rebooting and moving*** of some critical, load-balanced services on hot spares in order to be prepared for emergencies.
  - In coordination with the Security Team the ATLAS VOC performs ***regular checks*** on the existing services ***for signaled vulnerabilities***.
  - The ATLAS VOC makes available web framework (such as the ***ATLAS web redirector***) services to AM/SM. Such frameworks ensure a secure and CERN supported environment where to run web services (Shibboleth, CERN approved software packages, safe services etc.). In case the web redirector cannot be used, recommendations will be given to avoid common problems.
  - The ATLAS VOC advices and provides ***support on specific software packages and their versions*** to be used on specific platforms (Python 2.6, emacs, mod_python, mod_wsgi, Django, etc.).
  - The ATLAS VOC ***provides sensors*** for most common alarm needs.
  - Better ***documentation*** on Quattor tools.

The web redirector



https://atlas-minimumbias.cern.ch

https://atlas-trigconf.cern.ch

https://atlas-runquery.cern.ch

Authorization Failed - Mozilla Firefox

https://atlas-minimumbias.cern.ch

Shibboleth.

Authorization Failed

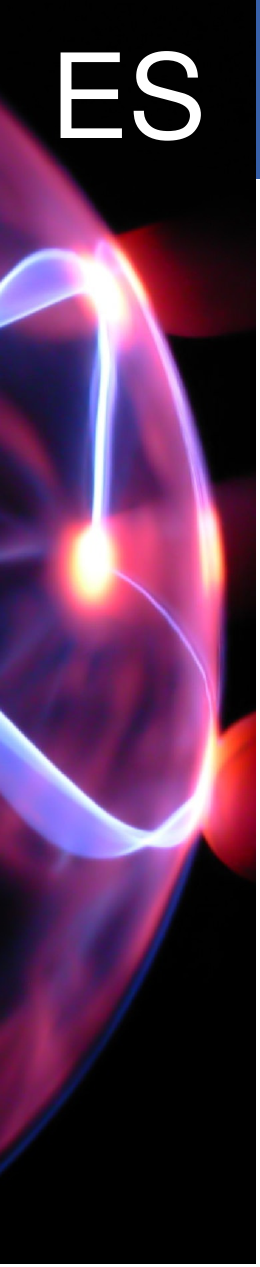
Based on the information provided to this application about you, you are not authorized to access the resource at "https://atlas-live.cern.ch/"

Please contact the administrator of this service or application if you believe this to be an error at somebody@cern.ch

Admin - Desktop Security Rx - Unregistered Version
File Protect Settings Tools Help
Wizard Remove Lock Unlock Find Edit Share Options Password Help Hide
Tasks
Hide and Restrict Access to Files and Folders
Object Name
Type
C:\Program Files\Adobe
Folder
Protect Files and Folders
Protect Local Hard Disks
Restrict External Dev
Protect Windows System
atmbsrv
atmbadm
attrcsrv
attrcadm
atrqsrv
atrqadm

Server accounts

Administration accounts



Possible area of collaboration

- ***Better documentation and examples on CERN available tools (Quattor family, SSO, SLS, etc.)***
- ***Shared rpm repository***
- ***Shared Lemon metrics repository***
- ***Web redirectors and other tools (SINDES?)***
- ***Common support team***
- ***Training***

… ***comments/suggestions ?***

Please, send e-mail to
Flavia.Donno@cern.ch