Role Based Access Control System in the ATLAS Experiment

Introduction

The complexity of the ATLAS [1] experiment motivated the deployment of an integrated Access Control System in order to guarantee safe and optimal access for a large number of users to the various software and hardware resources. Such an integrated system was foreseen since the design of the infrastructure and is now central to the operations model. In order to cope with the ever growing needs of restricting access to all resources used within the experiment, the Roles Based Access Control (RBAC) previously developed [2] has been extended and improved.

The access control system regulates the operations that can be executed on data and resources to be protected. Its goal is to control operations executed by subjects in order to prevent actions that could damage or steal data and resources.

System design

The Role Based Access Control (RBAC) system used in the ATLAS experiment takes the access decision for an individual user based on the roles the user possesses. The role determines which resources can be accessed and permission is being granted only if the user has the required role enabled. The core components of the RBAC system are:

- **users**: computing accounts associated with human beings or automated agents;
- **roles**: job functions or job titles which defines an authority level;
- **resources**: object which supports a set of possible actions;
- **permissions**: approvals to perform an action.

Implementation

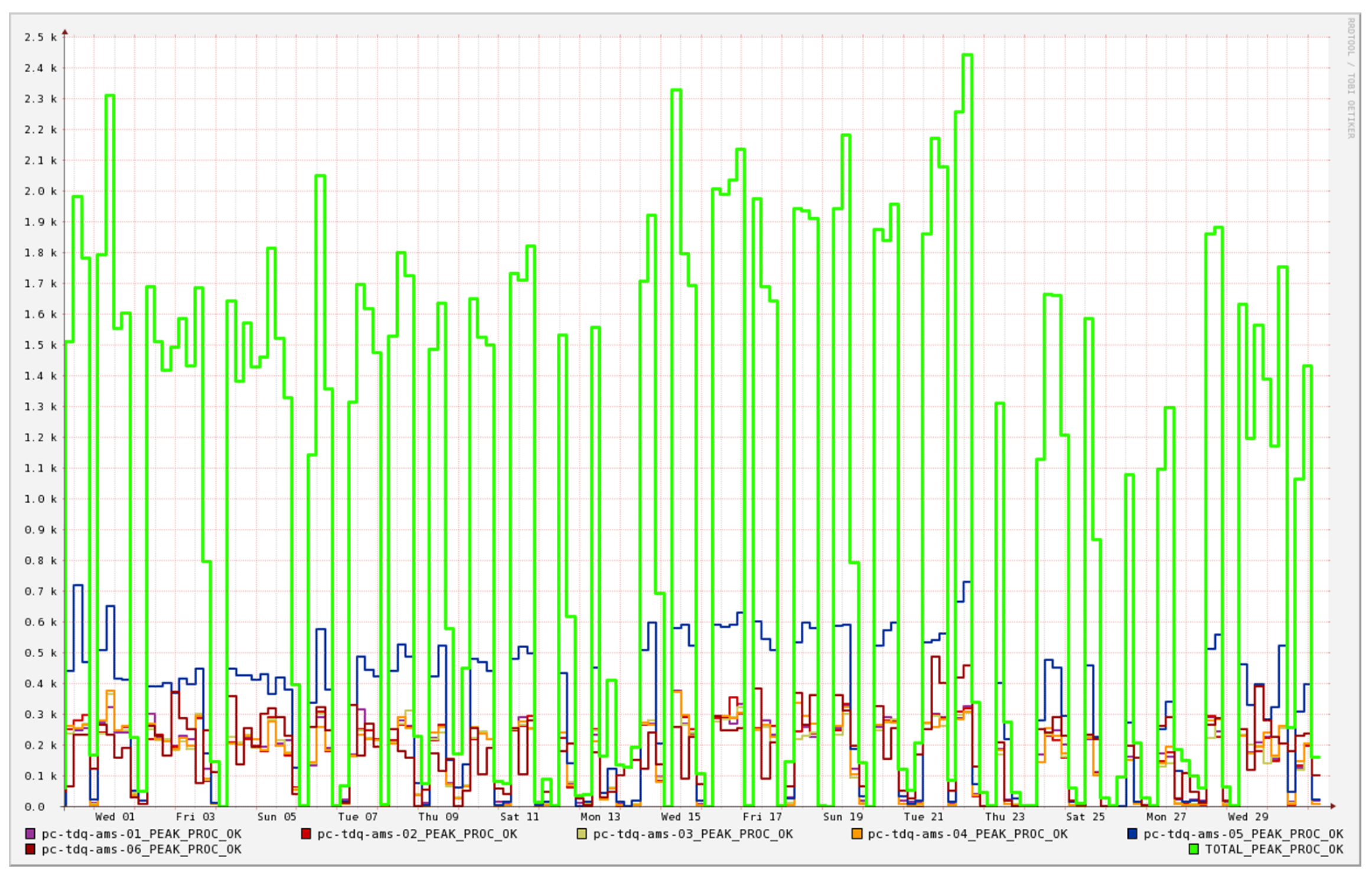
Inside ATLAS a simplified RBAC model was implemented. Roles have been designed to have both an organizational (ATLAS subsystem or project) and a functional component (reflecting the expertise levels within a subsystem).

Permissions are attached to roles located at the bottom of a role hierarchy (like a task based organization). The roles assigned directly to users are at the top of hierarchy. The two classes of roles are connected via intermediary roles, allowing for a fine grained and flexible permission allocation.

Global base roles are used as building blocks. These are not directly assignable to users and generic access policies are defined for them. More specific roles are assignable to users, inherit other roles including base roles not assignable to users and can get additional permissions.

Roles are defined in LDAP (Lightweight Directory Access Protocol) as NIS (Network Information Service) netgroups. This approach offers several advantages, including the ability to model a hierarchical structure and integration at the operating system / application level [3].

The Access Manager [4] is the component that implements the access management for Trigger and Data Acquisition (TDAQ) software. It has a client-server architecture and has been designed as a highly scalable system, capable of handling hundreds of requests in parallel.



Number of requests served by the Access Manager servers

References

[1] The ATLAS Collaboration, G. Aad et al., "The ATLAS Experiment at the CERN Large Hadron Collider", JINST 3 S08003, 2008

[2] M.C. Leahu, M. Dobson, G. Avolio, "Access Control Design and Implementations in the ATLAS Experiment", IEEE Trans. Nucl. Sci., vol 55, pp. 386-391, Feb. 2008

[3] A Adeel-Ur-Rehman et al, "System administration of ATLAS TDAQ computing environment", J. Phys.: Conf. Ser. 219 022048, 2010

[4] J. E. Sloper, M. Leahu, M. Dobson, G. Lehmann, "Access management in the ATLAS TDAQ," IEEE Trans. Nucl. Sci., vol. 53, no. 3, pp. 986-989, Jun. 2006.

[5] KDE e.V., Darmstadt, Germany, "KIOSK," [Online], available: http://techbase.kde.org/KDE_System_Administration/Kiosk/Introduction

Integration of the RBAC system

In order to have a consistent security policy across all ATLAS subsystems a synchronization mechanism was implemented to integrate the RBAC policies with various other security components, including:

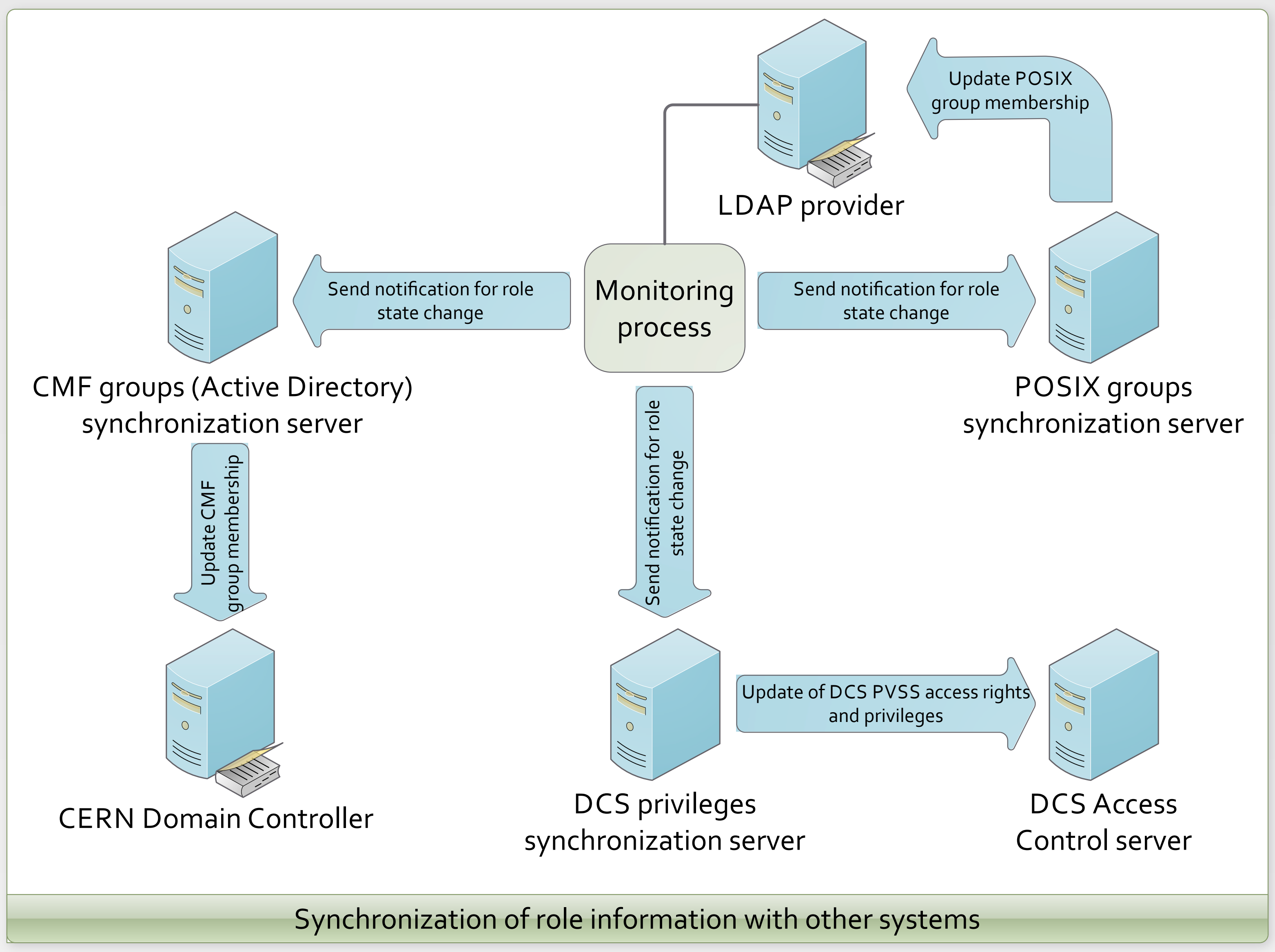
- the Detector Control System (DCS) Access Control
- login restrictions to Windows machines
- POSIX groups used at the filesystem level

The synchronization mechanism is based on a monitoring process running on the LDAP provider server which sends notification to several synchronization processes whenever a role to user relation changes. After receiving a trigger the listener process connects to one of the LDAP servers, gets the updated user to role relationships and performs the required changes.

The full list of user enabled DCS-related roles (explicit and inherited) is passed to the DCS Access Control system to avoid the need for duplicating and synchronizing the whole role hierarchy.

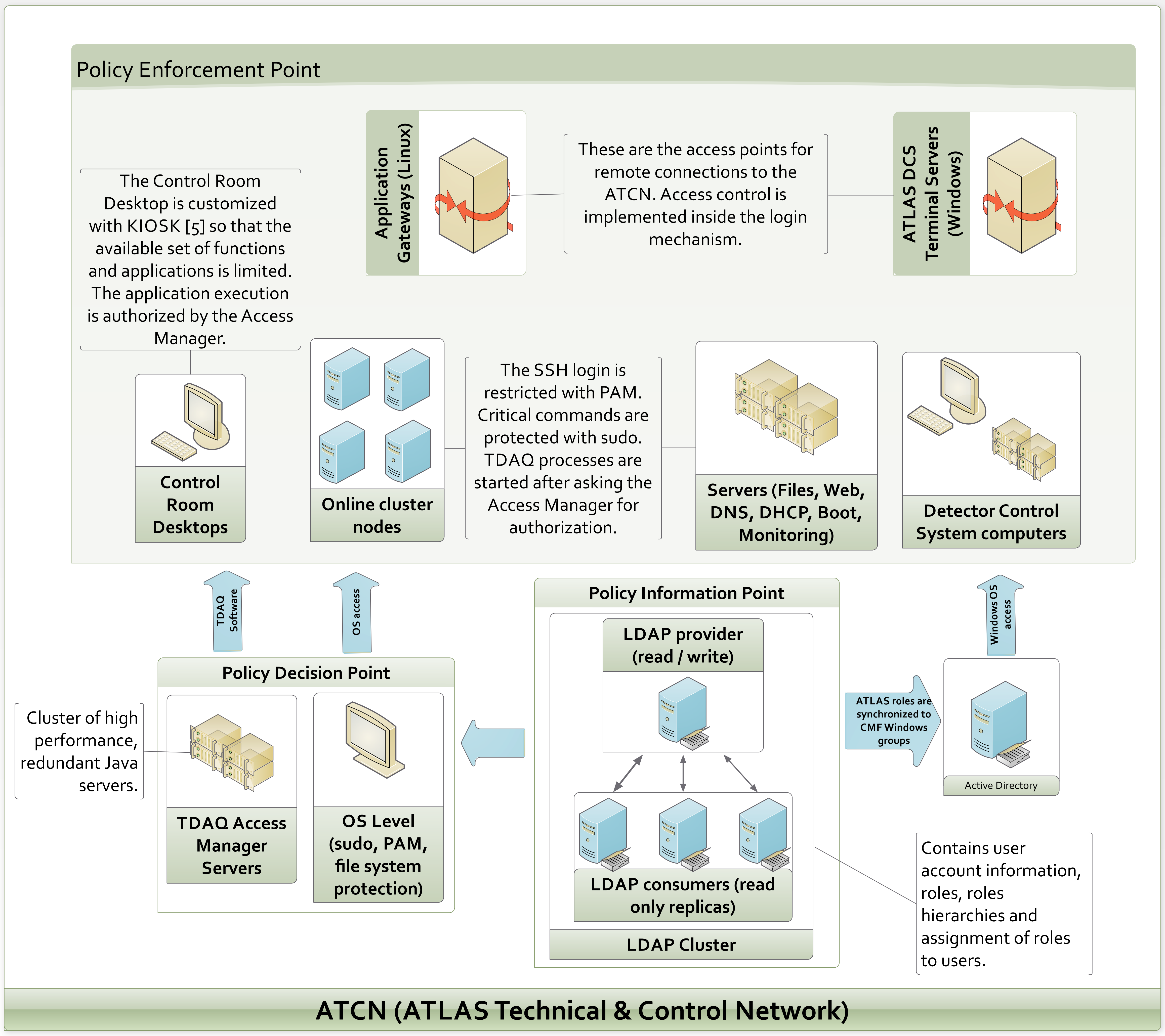
List of authors

M. L. Valsan	Politehnica University Bucharest, Romania
M. Dobson	CERN, Switzerland
G. Lehmann Miotto	CERN, Switzerland
D. A. Scannicchio	University of California at Irvine, USA
S. Schlenker	CERN, Switzerland
V. Filimonov	Petersburg Nuclear Physics Institute, Russia
V. Khomoutnikov	Petersburg Nuclear Physics Institute, Russia
I. Dumitru	Politehnica University Bucharest, Romania
A. S. Zaytsev	Budker Institute of Nuclear Physics, Russia
A. A. Korol	Budker Institute of Nuclear Physics, Russia
A. Bogdantchikov	Budker Institute of Nuclear Physics, Russia
G. Avolio	University of California at Irvine, USA
S. Ballestrero	University of Johannesburg, South Africa
G. L. Darlea	Politehnica University Bucharest, Romania
M. Twomey	University of Washington, USA
F. Bujor	Politehnica University Bucharest, Romania
C. Caramarcu	National Institute of Physics and Nuclear Engineering, Romania



LDAP provider
Update POSIX group membership
Monitoring process
Send notification for role state change
Send notification for role state change
CMF groups (Active Directory) synchronization server
POSIX groups synchronization server
Update CMF group membership
Send notification for role state change
CERN Domain Controller
DCS privileges synchronization server
Update of DCS PVSS access rights and privileges
DCS Access Control server

Synchronization of role information with other systems



Policy Enforcement Point
Application Gateways (Linux)
ATLAS DCS Terminal Servers (Windows)
Control Room Desktops
Online cluster nodes
Servers (Files, Web, DNS, DHCP, Boot, Monitoring)
Detector Control System computers
TDAQ Software
OS access
Windows OS access
Policy Decision Point
TDAQ Access Manager Servers
OS Level (sudo, PAM, file system protection)
Policy Information Point
LDAP provider (read / write)
LDAP consumers (read only replicas)
LDAP Cluster
ATLAS roles are synchronized to CMF Windows groups
Active Directory

These are the access points for remote connections to the ATCN. Access control is implemented inside the login mechanism.

The Control Room Desktop is customized with KIOSK [5] so that the available set of functions and applications is limited. The application execution is authorized by the Access Manager.

The SSH login is restricted with PAM. Critical commands are protected with sudo. TDAQ processes are started after asking the Access Manager for authorization.

Cluster of high performance, redundant Java servers.

Contains user account information, roles, roles hierarchies and assignment of roles to users.

ATCN (ATLAS Technical & Control Network)

CERN - ATLAS TDAQ SysAdmins

Poster designed by Mihai Liviu Valsan <Liviu.Valsan@cern.ch>, ATLAS TDAQ SysAdmin Team, CERN, Sep 2010