

Abstract

ATLAS (A Toroidal LHC Apparatus), cel mai mare experiment de la CERN, este un detector dedicat studierii interacțiunii particulelor la energii înalte în acceleratorul Large Hadron Collider (LHC). Sistemul de achiziție de date al detectorului este compus dintr-un număr considerabil de echipamente hardware, aplicații software și personal uman care supraveghează funcționarea experimentului. Protecția acestora împotriva daunelor provocate de utilizarea incorectă precum și optimizarea exploatarei prin evitarea conflictelor de acces la resurse sunt cerințe esențiale în ATLAS. Astfel se impune necesitatea unui mecanism de control al accesului pentru a proteja resursele software ale experimentului.

Această teză prezintă contribuția noastră la analiza, proiectarea, implementarea și instalarea soluției de control al accesului la resurse software pentru protecția ATLAS Online cluster și a software-ului TDAQ ce rulează pe el. Soluția reprezintă un pas înainte de la modelul bazat pe conturi de grup folosit în experimentele anterioare la CERN către modelul caracterizat de conturi de utilizator individuale și de atribuire a permisiunilor utilizatorilor prin intermediul unor roluri și ierarhii de roluri. Astfel, soluția de control al accesului la ATLAS Online cluster este centrată pe modelul de control al accesului bazat pe roluri (RBAC), ce permite îndeplinirea cerințelor de protecție în ATLAS, trasabilitatea acțiunilor utilizatorilor și adaptabilitatea la un număr mare de utilizatori. Contribuția originală a acestei teze constă în proiectarea unei soluții unitare de control al accesului pornind de la modelul RBAC: se abordează într-un mod coerent protecția de la nivelul administrării de sistem a cluster-ului (accesul de la distanță, conectarea la nodurile cluster-ului, restricționarea execuției programelor) până la nivelul software-ului TDAQ (protejarea funcționalităților critice în componentele TDAQ). Integrarea cu alte sisteme software ale experimentului este facilitată de o aplicație în linie de comandă cât și de interfețe de programare în limbajele Java și C++. Lucrarea se concentrează pe autorizarea acțiunilor utilizatorului pe baza politicilor de control al accesului, faza de autentificare fiind în sarcina serviciilor specifice administrării de sistem a cluster-ului. Principiile RBAC sunt aplicate la nivelul administrării de sistem cu mecanismele de securitate Linux pentru o integrare facilă cu Scientific Linux CERN instalat pe nodurile din cluster. Pentru nivelul aplicațiilor, am dezvoltat un serviciu dedicat TDAQ Access Manager (AM) care administrează politicile de acces și ia deciziile de autorizare. Acest serviciu l-am construit cu ajutorul standardului OASIS XACML acordând o atenție deosebită aspectelor critice într-un sistem de lucru în timp real: disponibilitate, performanță, scalabilitate, monitorizare.

Soluția de control al accesului în ATLAS Online cluster a fost instalată în toamna anului 2008 când a fost inaugurat LHC-ul. Configurația soluției constă într-o suită de 6+1 servere ce rulează serviciul TDAQ AM pentru ~3800 de utilizatori și ~440 de roluri. Fiecare server procesează ~800 de cereri de autorizare/secundă deservind astfel software-ul TDAQ ce rulează pe cele ~3000 de noduri din cluster. TDAQ AM este integrat cu platforma de monitorizare a cluster-ului pentru supravegherea permanentă a performanței și disponibilității serviciului. Serviciul funcționează astfel de 4 ani asigurând o achiziție de date stabilă și eficientă în ATLAS ce a condus către prima descoperire majoră: bosonul Higgs.

ATLAS (A Toroidal LHC Apparatus) is a general-purpose detector for studying high-energy particle interactions: it is the largest particle detector experiment at CERN and it is built around one of the interaction points of the proton beams accelerated by the Large Hadron Collider. This experiment comprises a significant number of hardware devices, software applications and human personnel to supervise its operation. Their protection against damages as a result of misuse and their optimized exploitation by avoiding the conflicting accesses to resources are key requirements for the successful running of ATLAS. In order to achieve this, an access control mechanism must be set up in ATLAS.

This thesis presents our contribution to the analysis, design, implementation and deployment of the access control solution for the protection of ATLAS Online cluster and the Trigger and Data Acquisition (TDAQ) software running on it. The access control solution we worked on is a step forward from the model based on group accounts used in past experiments at CERN to the model characterized by individual user accounts and permissions assignment to users by means of roles and roles hierarchy. Hence the access control solution for the ATLAS Online cluster revolves around the Role Based Access Control (RBAC) model which fulfills the ATLAS experiment's requirements for action traceability and accountability and offers the flexibility to accommodate the high number of users. The original contribution of this thesis consists in designing a solution on top of RBAC model to address in a coherent way the protection needs from the cluster system administration level (remote access, login on the nodes, restrict access to tools execution on the nodes) to the TDAQ software level (TDAQ components protecting their functions). At the same time, the solution is open for integration with other experiment systems through the command line client and Application Programming Interface offered in Java and C++. Our work focuses on the authorization of user actions based on the access control policies, while the user authentication function is handled by the system administration specific services. The RBAC concepts are applied at system administration level with Linux traditional security mechanisms for seamless integration in the Scientific Linux CERN running on the cluster nodes. At the application level, we developed a dedicated service (TDAQ Access Manager) to serve the TDAQ Software components in managing the access control policies and to take the authorization decisions. The service is built on top of the OASIS XACML industry standard while paying special attention to the critical non-functional aspects like availability, performance, scalability and monitoring.

We finished the deployment in production in time for the first beam accelerated in LHC in autumn 2008. The setup currently consists in a high availability cluster of 6+1 nodes running the TDAQ Access Manager Service for ~3800 user accounts and ~440 roles. The service is able to handle ~800 authorization requests per second from TDAQ software running on the ~3000 nodes of the ATLAS Online cluster. It is integrated with the system administration monitoring system for continue surveillance of service availability and performance. This production setup has run successfully in the last 4 years and has allowed ATLAS to take data steadily, leading to the first major discovery: the Higgs boson.