그리드 사용자 계정 관리 시스템 설계

장택수[0], 홍필두, 노남수, 이용우
서울시립대학교 전자전기컴퓨터공학부
{wichid iamhpd, topnons}@metalab.uos.ac.kr, ywlee@uos.ac.kr

A Design of the User Account Management System in Grid

Taek-Soo Jang[0], Pil-Du Hong, Nam-Su No, Yong-Woo Lee
Faculty of Electrical & Computer Engineering, The University Of Seoul

요 약

그리드 컴퓨팅을 실현하기 위해서는 Virtual Organization을 구성하는 개인, 기관, 그리고 자원 등의 동적인 집합에 대해 유연하고 안정적이며 통합된 자원의 공유를 구현해야 한다. 이를 위해 해결해야 할 많은 과제들 중에는 인증과 권한 부여가 있으며 이 두 가지는 단일시스템의 계정관리에 속한다. 현재 그리드 컴퓨팅을 실현하기 위한 많은 middleware들 중에서 확고한 위치를 차지하고 있는 Globus Toolkit은 grid-mapfile을 이용하여 정적인 사용자 계정관리를 하기 때문에 동적 특성을 가진 그리드 컴퓨팅에는 적합하지 않다. 따라서 본 논문에서는 그리드 컴퓨팅을 위한 사용자 계정관리시스템에 대한 기존의 연구를 토대로 그리드 사용자 계정관리시스템을 Globus Toolkit 3.2를 기반으로 설계하였다.

1. 서 론

그리드 컴퓨팅(Grid Computing)은 VO(Virtual Organization)들 사이에 흩어져 있는 다양한 자원들의 통합된 사용과 공유를 실현하고자 하는 새로운 컴퓨팅 기법이다[1]. 그리드 컴퓨팅을 실현하기 위해서는 VO를 구성하는 개인, 기관, 그리고 자원 등의 동적인 집합에 대해 유연하고 안정적이며 통합된 자원의 공유를 구현해야 하며 이를 위해 인증(authentication), 권한부여(authorization), 자원 접근 및 발견(resource access and discovery) 등 해결해야 할 많은 문제점들이 존재한다[2].

이러한 동기로 현재 그리드 컴퓨팅을 위한 많은 middleware들이 개발되었다[3]. 여러 Grid middleware들 중에서 Metacomputing Infrastructure Toolkit으로 출발하여 현재 그리드 컴퓨팅을 위한 middleware로서 확고한 위치를 차지하고 있는 GT(Globus Toolkit)[4][5]은 컴퓨팅 파워, 데이터베이스, 그리고 다른 툴들을 지리적 위치나 관리 영역에 관계없이 사용할 수 있는 환경을 제공한다. GT에서 분산된 자원에서의 계산작업에 대한 인증과 권한부여에 대한 문제점을 해결하기 위하여 다음과 같은 방법을 사용하고 있으며 인증과 권한부여는 계정관리에 속한다.

GT에서 사용자와 자원에 대한 인증을 위하여, X.509 인증서를 사용한다. 그리고 권한부여를 위하여, 로컬시스템의 grid-mapfile에 사용자의 DN(Distinguished Name)과 매핑될 로컬 계정을 추가하고 로컬 계정에 대한 부가적인 권한(authorization) 설정을 하게 된다[1][5].
그러나 GT의 계정관리시스템을 그리드 컴퓨팅에 적용할 때 발생하는 문제들에 대한 많은 지적과 해결책들이 제시되었다[6][7][8][9][10][11][12][13]. 하지만 이 해결책들 역시 동적이고 확장성 있는 VO를 구성하는 경우 문제를 일으킨다.

본 연구에서는 GT 사용자 계정관리시스템에 대한 관련 연구와 문제점에 대해 알아보고 그 해결책으로서 GT3를 기반으로 하는 그리드 환경에 적합한 계정관리시스템을 설계하였다.

2. 관련 연구

현재 GT는 안정적인 버전의 GT3.2.1(이하 GT3)과 GT4의 beta release가 있다.

우선 GT3의 계정관리시스템을 간단히 소개하면 다음과 같다. 서론에서 언급한 것과 같이 GT3에서 사용자와 자원에 대한 인증은 X.509 인증서를 사용하며, 권한부여를 위해 grid-mapfile을 사용하고 각각의 계정에 대한 부가적인 권한 설정을 한다[1][5]. GT4의 계정관리시스템도 GT3와 거의 유사하나 사용자가 원격지에 작업을 실행시킬 수 있는 여러 개의 로컬 계정을 가진 경우 RSL 파일을 이용하여 하나의 로컬 계정을 지정할 수 있도록 기능을 추가하였다[5].

그러나 grid-mapfile을 이용해 로컬시스템의 사용자 계정을 매핑하는 경우 그리드 사용자는 장래에 사용 가능성이 있는 모든 로컬 자원상의 grid-mapfile에 자신의 DN과 매핑될 로컬 계정을 추가해야 한다. 또한 로컬 자원 관리자는 사용 권한을 가진 모든 사용자들에게 하나 이상의 계정을 할당하고 이를 관리해야 한다.

이러한 계정 할당 방법에 대한 문제점을 해결하는 방법으로서 Michigan 대학의 Thomas J. Haker와 Brian D. Athey는 "Account Templates"라는 계정 할당 방법을 제안했다[6]. 이 방법은 로컬 시스템을 사용 중에 있는 모든 그리드 사용자에게 독립적인 로컬 계정을 일시적으로 바인딩(binding)함으로써 여러 사용자들이 하나의 로컬 계정을 사용함으로써 발생하는 사용자 프로세스들 간의 간섭을 제거하고 사용자의 잘못된 사용으로 시스템 및 다른 사용자에게 끼치는 손해에 대한 책임 규명을 할 수 있게 하였다. 또한 각각의 사용자들이 자신만의 유일한 로컬 계정으로 매핑되도록 계정을 할당할 경우 발생하는 사이트 관리자와 사용자의 계정관리 부담을 줄였다.

"Account Templates"는 사용자 계정을 할당하는 방법에 대한 하나의 해결책을 제시하였으나 사용자의 권한 설정에 있어서는 해결책을 제시하지 못하였다.

이후 그리드 컴퓨팅을 위한 사용자 권한 설정에 대한 중요성 인식과 더불어 많은 해결책들이 제시되었다. 그 중에서 X.509 Attribute Certificate를 이용하여 사용자 권한 설정에 대한 해결책을 제시한 PRIMA[7]와 PERMIS[8]가 있다. 이 두 가지 모델은 작은 수의 사용자 community들에는 잘 적용되나 많은 수의 community에서는 관리자의 부담을 가중시켜 적절하지 않다.

또 다른 모델로 Shibboleth[9]와 VOMS[10]가 있는데 이 두 모델은 권한 요청을 전달하는(passing) framework만을 포함하고 policy engine이 없다는 문제점을 가지고 있다. 이 외에 CAS(Community Authorization Server)[11]와 SAZ(Site Authorization Service)[12] 등이 있는데, CAS의 경우 자원 소유주가 community 관리자에게 자원 관리 권한을 위임하여야 한다는 단점을 가지고 있고 SAZ의 경우는 사용자의 DN을 데이터베이스에 저장하여 2단계 보안체크만을 하였다는 단점이 있다.

지금까지 소개한 여러 가지 모델들의 단점을 보완하고 장점을 살린 새로운 모델을 제시한 MGRID 프로젝트가 있다. 이 모델은 "Walden"이라 부르며 기존의 캠퍼스 인증 및 권한부여 메커니즘과 GT를 통합하여 Michigan 대학 내의 사용자 인증과 권한 관리를 하는 새로운 접근법이다[13]. 이 방법은 GT2.4의 grid-mapfile을 이용한 정적인 사용자 계정 매핑 방식을 kx509와 secure LDAP에 기반한 새로운 접근법으로 교체하여 자원 관리자와 사용자의 계정 관리 부담을 제거하였다. 또한 XACML[14]에 기반한 권한 모델 이용하여 로컬 자원에 대한 사용자 그룹의 세부적인 권한 설정을 할 수 있도록 함으로써 캠퍼스 전역적이고 효율적인 계정관리시스템을 제안하였다. 그러나 이 계정관리시스템은 Michigan 대학의 구성원들이 사용하던 기존의 로컬 계정을 그대로 사용하기 때문에 기존의 단일 시스템의 계정관리 방식에서 크게 벗어나지 못하고 있으며, Michigan 대학의 특성에 맞추어 계정관리시스템을 설계 및 구현하였다. 또한 Attribute Authority에서 검색되는 Attribute들은 사용자 개개인이 아닌 사용자 그룹 또는 역할(role-based)에 따른 Attribute들이므로 사용자 개개인에 대한 세부적인 권한 설정을 보장하지 못한다.

결론적으로 그리드 컴퓨팅에 적합한 계정관리시스템은 다음의 사항을 고려해서 설계되어야 한다. 첫째, 모든 사용자가 작업을 실행하게 될 로컬 머신에는 대부분 자신의 계정이 없으며, 설사 있다고 할지라도 작업을 실행할 모든 로컬 머신에 동일한 UID을 가지고 있지는 않을 것이다. 둘째, 자원 제공자가 신뢰하는 인증서를 소유한 사용자는 자원을 사용할 최소한의 권한을 가진다.

다음 장에서는 이 두 가지를 고려하여 본 논문에서 설계한 사용자 계정관리시스템에 대해 세부적으로 기술하겠다

3. 사용자 계정 관리 시스템 설계

본 논문에서 설계한 사용자 계정관리시스템은 GT3를 기반으로 하였으며, GT 자원관리(Resource Management) Component의 GRAM(Grid Resource Allocation and Management)에 속한다. GRAM은 클라이언트가 원격지 자원상에서 계산 작업을 실행, 관리, 모니터링할 수 있는 기능과 로컬 자원을 사용하는 사용자에 대한 인증 및 권한부여 기능을 제공한다[1].

본 논문에서는 사용자 계정관리시스템의 설계에 있어서 다음과 같은 요구사항을 반영하였다.

1) Scalability & Security

grid-mapfile을 이용한 정적인 사용자 계정 매핑방식에서 Template Accounts와 같은 계정 매핑 방식으로 변경하여 자원 관리자와 사용자의 부담을 줄이고 권한 정보 관리에 있어서 표준화된 인터페이스와 확장성 있는 시스템을 사용함으로써 사용자 수에 대한 관리 부담을 최소화한다. 또한 사용자와 로컬 계정의 일시적인 매핑으로 발생하는 사용자의 transaction과 자원 사용에 대한 부인을 방지하도록 한다.

2) Extensibility

로컬자원을 사용하는 사용자에 대한 권한부여에 있어서 세부적인 권한설정 방법을 지원하고 장래에 부가적인 권한 설정이 용이하도록 지원한다.

3) Resource Ownership & Autonomy

각 자원의 소유자가 자원제공정책을 설정할 수 있도록 하고, 이러한 자원제공정책에 따른 사용자 권한부여를 함으로써 자원의 소유권을 보장함과 동시에 관리의 자율성을 보장한다.

이러한 요구사항을 반영하여 설계한 사용자 계정관리시스템은 아래 그림과 같다.

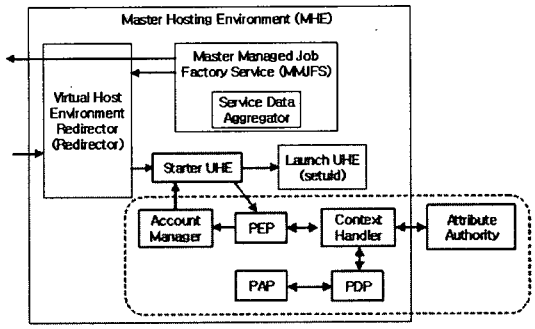

그림 1 계정관리시스템 설계도

위 그림의 GT3의 GRAM의 MHE(Master Hosting Environment)에 본 논문에서 설계한 사용자 계정관리시스템(진한 파란색 점선 영역)을 적용한 것이다. PEP (Policy Enforcement Point), PDP(Policy Decision Point), PAP(Policy Administration Point), Context Handler는 XACML[14]의 시스템 개체(System Entity)로서, XACML 명세서에 정의된 것과 같이 동작하므로 용어를 그대로 사용하였다. 그러나 Attribute Authority는 XACML의 PIP에 해당하지만 단순한 정보 제공의 기능뿐만 아니라 정보 관리의 기능도 포함하기 때문에 Attribute Authority라고 명명하였다. 사용자계정관리시스템이 동작하는 과정을 간단히 설명하면 다음과 같다.

1. Redirector가 Starter UHE를 호출하고 Starter UHE는

로컬 계정을 얻기 위해 PEP에 요청한다.

2. PEP는 Starter UHE로부터 받은 정보를 이용하여 Context Handler에 요청한다. Context Handler는 권한 결정에 필요한 Attribute들이 더 필요한지를 PDP와 PAP를 통해 알아낸 후 필요한 Attribute들이 있으면 Attribute Authority로부터 얻는다.
3. 이 정보들을 이용하여 Context Handler는 PDP에 해당 사용자의 자원 사용에 대한 결정 요청(decision request)를 보내고 PDP는 정책(Policy)에 따라 이에 대한 응답(reponse)을 Context Handler에 보낸다.
4. Context Handler는 이를 변환하여 PEP에 보내고, PEP는 다시 Account Manager에 정보를 보냄으로써 사용자의 권한에 맞게 로컬 계정을 설정하고 매핑하도록 한다. 이때 사용되는 로컬 계정은 자원관리자가 그리드 사용자를 위해 만들어 놓은 계정이고 자원관리자가 지정한 사용자 수를 초과하지 않는 범위에서 동작한다.

본 논문의 사용자 계정관리시스템에서 Account Manager는 사용자 권한에 따라 로컬 계정의 환경설정(파일시스템 한도와 프로세스 자원 한도 등등)을 하는 기능과 사용자의 로컬자원 사용기록을 위한 정보를 기록하는 기능을 가지도록 설계하였다. 그러나 Account Manager에 특정 파일에 대한 접근 통제는 모든 사용자가 한 시점에 같은 계정을 사용하지 않으므로 설계에서 제외하였다. Attribute Authority는 그리드 사용자의 DN과 권한 결정에 필요한 Attribute들을 Database에 저장 및 관리하도록 설계하였다. 이는 사용자의 DN이 각각의 사용자를 구별할 수 있다는 특성을 이용하였다. 그리고 XACML에서 접근 질의(Access Query)에 연관된 두 agent인 PEP와 PDP를 PAP와 함께 로컬시스템에 배치함으로써 자원제공자의 자율적인 자원제공정책 설정을 보장하였다.

4. 결론 및 향후 과제

본 논문에서 설계한 사용자계정관리시스템은 인증을 위해서는 기존의 GT가 사용하던 X.509 인증서를 사용하며 XACML과 Database를 사용하여 사용자의 권한을 결정하고 그에 따라 Account Manager가 로컬계정의 권한 설정을 하도록 하였다.

이 시스템은 기존에 설계 및 구현되었던 사용자 계정관리시스템과 다음과 같은 차이점을 갖는다. 첫째, 기존의 정적인 사용자 계정할당 방식(grid-mapfile을 이용)이나 Template Account 방식과 정적인 사용자 계정할당 방식의 조합과는 달리, Template Account 방식만을 이용해 완전한 동적 사용자 계정할당 방식을 지원함으로써 기존의 시스템보다 더욱 유연한 자원의 제공 및 사용을 가능하게 하였다. 둘째, X.509 인증서의 사용자 DN은 다른 사용자들과 구별되는 특성을 가지기 때문에 Database를 이용하여 모든 사용자의 권한 정보를 세밀하게 저장하도록 설계였고 계정관리에 있어서 자원 제공자와 사용자의 부담을 최소화하였다. 셋째, XACML을 이용하여 로컬자원에 대한 사용자의 권한을 판단하는 기능을 제공함과 동시에 사용자의 권한에 따라 로컬 사용자 계정의 권한을 설정하는 기능을 설계하였다.

향후 본 논문에서 설계한 사용자 계정관리시스템을 구현하고 그리드 환경에 적용하여 제반 문제점을 파악하고 개선할 것이다.

5. 참고문헌

[1] Welch V., Siebenlist F., Foster I., Bresnahan J., Cajkowski K., Gawor J., Kesselman C., Meder S., Pearlman L., Tuecke S., "Security for Grid Services", HPDC, 2003.

[2] Foster I., Kesselmann C., Tuecke S., "The Anatomy of the Grid", Intl J. Supercomputer Application, 15(3), 2001

[3] Grid Computing Info Centre, http://www.gridcomputing.com/

[4] Foster I., Kesselman C, "Globus: A Metacomputing Infrastructure Toolkit", International Journal of Supercomputing Applications, 11(2):115-128, 1997

[5] Globus Alliance, http://www.globus.org

[6] Thomas J. Hacker, Brian D. Athey, "A Methodology for Account Management in Grid Computing Environments", Lecture Notes In Computer Science Vol. 2242, 2001

[7] Lorch M., Adams D., Kafura D., Koneni M.S.R, Rathi A., Shah S., "The PRIMA System for Privilege Management, Authorization and Enforcement in Grid Environments", 4th Int. Workshop on Grid Computing - Grid 2003, 2003

[8] D. W. Chadwick and A. Otenko, "The PERMIS X.509 role based privilege management infrastructure,"Future Generation Computer Systems, vol. 19, no. 2, pp. 277289, Feb. 2003.

[9] Internet2. (2004) Shibboleth project. [Online]. Available: http://shibboleth.internet2.edu

[10] R. Alfieri, R. Cecchini, V. Ciaschini, L. Dell'Agnello, A. Frohner, A. Gianoli, K. Lorentey, and F. Spataro, "VOMS, an authorization system for virtual organizations," in First European AccessGrids Conference, Santiago, Chile, Feb. 2003.

[11] L. Pearlman, C. Kesselman, V. Welch, I. Foster, S. Tuecke, "The Community Authorization Service: Status and Future", Computing in High Energy and Nuclear Physics(CHEP03), La Jolla, CA, USA, 2003

[12] D. Skow, I. Mandrichenko, V. Sekhri, "Site Authorization Service (SAZ)", Computing in High Energy and Nuclear Physics(CHEP03), La Jolla, CA, USA, 2003

[13] Beth A. Kirschner, Thomas J. Hacker, William A. Adamson, Brian D. Athey, "Walden: A Scalable Solution for Grid Account Management", 5th IEEE/ACM International Workshop on Grid Computing - Grid 2004, 2004

[14] OASIS XACML TC, http://www.oasis-open.org/committees/workgroup.php?wg_abbrev=xacml