http://dx.doi.org/10.7840/kics.2015.40.5.860

Inter-Cloud 환경을 위한 IAM 클러스터링 아키텍처

김 진 욱•, 박 정 수*, 박 민 호**, 정 수 환°

IAM Clustering Architecture for Inter-Cloud Environment

Jinouk Kim•, Jung Soo Park*, Minho Park**, Souhwan Jung°

요 약

본 논문에서는 Inter-Cloud 환경에서 효율적인 사용자 인증 및 권한 인가를 위한 새로운 형태의 IAM 클러스터링 아키텍처를 제안한다. 제안하는 클러스터링 아키텍처는 사전 Access Agreement를 통하여 사용자가 자신이 등록되지 않은 어떤 서비스도 간단하게 이용할 수 있도록 인증 및 접근 권한을 제공한다. 본 논문에서는 IAM 클러스터링 아키텍처의 구성요소 및 인증 프로토콜을 설명한다.

Key Words : IAM Clustering, Inter-Cloud, Access Agreement, Authorization, Authentication

ABSTRACT

In this paper, we propose a new type of IAM clustering architecture for the efficiency of user authentication and authorization in the Inter-Cloud environment. clustering architecture allows users to easily use un-registered services with their registered authentication and access permissions through pre-Access Agreement. through this paper, we explain our authentication protocol and IAM clustering architecture components.

Ⅰ. 서 론

최근 클라우드 컴퓨팅의 급격한 성장으로 인하여 서비스 사업자들은 확장성, 비용 감소, 효율성 등의 장점을 가진 클라우드 서비스의 형태로 이동하고 있다[1,2]. 본 논문은 클라우드 서비스를 이용할 때, 사용자가 이용하고자 하는 서비스에 계정 등록을 할 필요 없이 기존 등록된 서비스 계정 정보를 이용하여 원하는 서비스에 접근하고 자원을 이용할 수 있는 IAM 클러스터링 아키텍처를 제안한다. 본 논문에서 제안하는 아키텍처는 시스템에 새로운 서비스를 추가할 경우 기존 서비스와 연동을 위하여 기존 서비스를 수정할 필요 없이 단순히 Access Agreement (AA) 추가만으로 기존 IAM System과 연결을 할 수 있다.

Ⅱ. 제안하는 아키텍처

2.1 IAM 클러스터링 아키텍처 구성

그림 1과 같이 IAM 클러스터링 아키텍처는 클라우드 서비스와 IAM System 간에 통신하는 Authentication Agent, IAM System 내의 Authentication Gateway와 Authorization Manager로 구성된다. 아래에 Access Agreement의 의미와 IAM 클러스터링 아키텍처 구성요소에 대한 자세한 설명이 있다.

2.1.1 Access Agreement (AA)

본 논문에서는 상호 연동에 대한 사전 협약을 맺고 있는 클라우드 서비스들로 대상을 제한한다. AA는 이러한 서비스 간의 리소스 접근에 대한 협약(Agreement)으로 정의한다. AA는 사용자의 권한에 맞는 리소스를 접근할 수 있도록 미리 정의하는 것으로 서비스와 시스템 연동 단계에서 수행한다. 표 1은 AA의 예를 보여준다. 표에서 R_1^A의 위첨자는 속해있는 클라우드 서비스를 의미하고 아래 첨자는 사용자 권한 레벨을 의미한다. 따라서 R_1^A은 A에 속한 레벨 1의 리소스를 의미하고, U_3^B는 B에 속한 레벨 3의 사용자를 의미한다. 이러한 AA에 의해 R_1^A는 레벨 1 이

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 IT연구센터육성 지원사업의 연구결과로 수행되었습니다(IITP-2015-H8501-15-1008).
• First Author : Soongsil University, School of Information and Telecommunication Engineering, ouk92@ssu.ac.kr, 학생회원
° Corresponding Author : Soongsil University, School of Electronic Engineering, souhwanj@ssu.ac.kr, 종신회원
* Soongsil University, School of Information and Telecommunication Engineering, ddukki86@ssu.ac.kr, 학생회원
** Soongsil University, School of Electronic Engineering, mhp@ssu.ac.kr, 정회원
논문번호 : KICS2015-03-056, Received March 20, 2015; Revised April 9, 2015; Accepted April 16, 2015

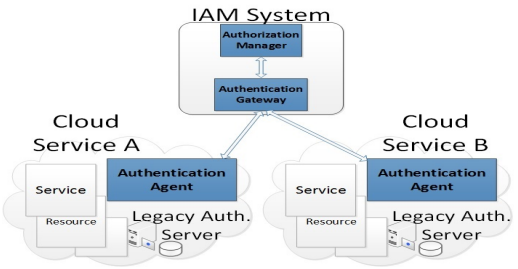

그림 1. Inter-Cloud IAM 아키텍처 구성도
Fig. 1. Inter-Cloud IAM Architecture Diagram

상 권한을 가진 모든 사용자가 접근할 수 있으며, R_2^B는 레벨 2 이상의 권한을 가진 모든 서비스의 사용자가 접근할 수 있다.

2.1.2 Cloud Service

1) Authentication Agent

각 클라우드 서비스와 IAM System 간 통신을 위하여 클라우드 서비스에 설치하는 Agent로, 안전한 채널을 통하여 사용자의 인증 정보를 IAM System의 Authentication Gateway에 전달하고 Access Token을 Authorization Manager로부터 획득한다.

2) Service

클라우드 서비스 사용자가 로그인하여 이용하고자 하는 기능 및 자원을 의미한다. 사전에 정의한 AA를 기반으로 사용자는 자신의 접근 권한에 따라 자원에 접근할 수 있다.

2.1.3 IAM System

1) Authentication Gateway

Authentication Agent, Authorization Manager와 통신을 한다. 클라우드 서비스에 등록된 사용자가 Service A의 계정정보로 Service B에 접근하려고 할 때, Authentication Gateway는 Service B로부터 요청을 받고, 사용자에게 Service A의 로그인 페이지를 Redirect 한다. 이러한 방법은 Service가 추가될 경우 모든 Service 마다 Redirect Page를 추가하지 않고 중앙에서 한 번의 추가로 손쉽게 관리 할 수 있는 장점이 있다. 또한, Authentication Gateway는 클라우드 서비스로부터 사용자 정보를 받아 Authorization Manager에게 전달한다.

2) Authorization Manager

사전에 협약 된 Access Agreement(AA)를 관리한다. Authentication Gateway에서 사용자 정보를 받아 사용자의 AA를 확인한 후 해당 사용자 권한에 맞는 Access Token을 만들어서 사용자가 접근하고자 하는 서비스의 Agent로 발급한다.

표 1. Access Agreement 예시
Table 1. Example of Access Agreement

Resource	User Authorization	Resource	User Authorization
R_1^A	U_1^*, U_2^*, ...	R_1^B	U_1^*, U_2^*, ...
R_2^A	U_2^*, U_3^*, ...	R_2^B	U_2^*, U_3^*, ...
. . .	. . .	. . .	. . .

2.2 인증 프로토콜

제안하는 IAM 클러스터링 아키텍처의 인증 프로토콜은 그림 2와 같다. Cloud Service A에 등록된 User와 Cloud Service A, Cloud Service B 그리고 IAM System의 Authentication Gateway, Authorization Manager가 있다. User와 User가 등록된 Cloud Service A는 User의 Key K_u를 가지고 있고 K_u는 User가 이용하고자 하는 서비스와 User 간의 인증과 세션을 형성하는 데 이용된다.

그림 2의 프로토콜을 순서에 따라 설명한다.

① Service A에 등록된 User가 Service B에 접근을 요청한다.

② Cloud B의 Authentication Agent를 통하여 IAM System의 Authentication Gateway로 “User가 Service A의 계정정보를 이용하여 Service B에 접근을 희망한다.”는 요청을 보낸다.

③ Authentication Gateway는 User의 Service A 계정 정보를 받기 위하여 User에게 Service A의 로그인 페이지를 Redirect 한다.

④ User는 자신의 Service A 계정정보를 이용하여 로그인한다. 그리고 Service A는 User에게 입력받은 계정정보가 Service A에 등록된 User 정보와 일치하는지 확인한다.

⑤ Service A는 Authentication Gateway에게 User의 정보와 User가 Service A 사용자임을 증명하는 서명과 해시 된 User A의 Key $h(K_u)$를 전송한다.

⑥ IAM System 내부에서 Authentication Gateway는 Authorization Manager에게 User의 정보를 전송한다. 그리고 Authorization Manager는 User의 레벨 정보를 바탕으로 사전에 Agreement 된 User의 권한 정보를 확인한 후 해당하는 Access Token을 생성한다.

⑦ Authorization Manager는 생성된 Access Token과 해시 된 User의 Key $h(K_u)$를 Service B에게 전송한다. Service B는 Access Token을 확인하여 User의 정보를 확인한다.

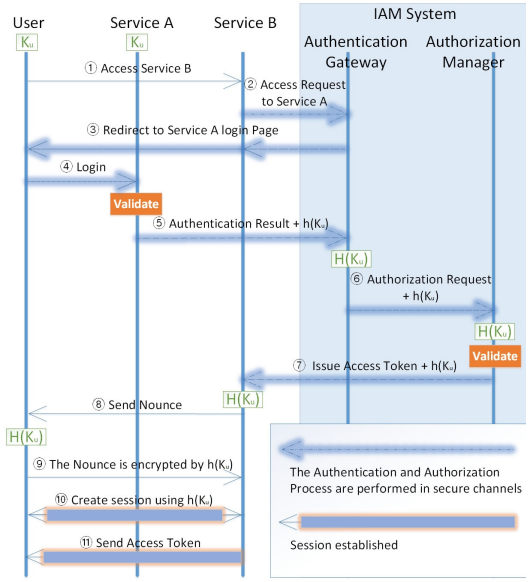

그림 2. Inter-Cloud 인증 플로우
Fig. 2. Authentication Flow for Inter-Cloud

⑧ Service B는 Access Token을 발급하기 전에 User를 확인하기 위하여 nounce를 전송한다.

⑨ User는 자신의 Key를 해시하고 nounce를 $h(K_u)$로 암호화하여 $[nounce]h(K_u)$를 Service B에게 전송한다. 그리고 Service B는 User로부터 수신한 $[nounce]h(K_u)$와 $h(K_u)$로 nounce를 암호화한 값이 일치하는지 확인한다.

⑩ 서로를 확인한 User와 Service B는 $h(K_u)$를 이용하여 세션을 형성한다.

⑪ Service B는 형성된 세션을 이용하여 Access Token을 $h(K_u)$로 암호화하여 User에게 전송한다.

Ⅲ. 성능 및 보안 평가

본 논문에서 제안하는 아키텍처는 사용자의 계정정보를 클라우드 서비스마다 등록하지 않고 기존에 등록된 서비스와의 인증을 통하여 다른 서비스들을 이용할 수 있게 함으로써 개인정보 유출 위험성을 줄일 수 있다. 그리고 암/복호화 및 인증 등 기존 보안 기법으로 대부분의 공격 유형은 보호할 수 있지만, 새롭게 제안하는 아키텍처는 중간자 공격이 취약하므로 본 논문에서는 중간자 공격에 대한 보안성을 평가한다. IAM 클러스터링 아키텍처는 안전한 채널을 이용하여 통신하므로 중간자 공격에 안전하다.

3.1 성능

IAM 클러스터링 아키텍처는 Authentication Server (AS)가 아닌, AS를 연결하는 역할을 한다. 따라서 AS에 맞춰서 표준화할 필요 없이 어떠한 클라우드 서비스도 IAM System과 쉽게 연결할 수 있다. 또한, 기존 N개의 서비스가 있을 때, 새로운 서비스를 추가하기 위해 N개의 서비스를 수정하는 것이 아닌 IAM System과 단 한 번의 연결을 하므로 확장성이 좋다.

3.2 보안 평가

1) Cloud Server - IAM System

Cloud Server의 Authentication Agent와 IAM System은 인증서를 이용한 상호 인증을 한다.

2) User - User registered Cloud Server

User와 User가 등록된 Cloud A는 인증서를 이용한 상호 인증을 한다.

3) User - User unregistered Cloud Server

User와 User가 이용하고자 하는 Cloud B는 사용자의 해시된 Key $h(K_u)$를 이용하여 세션을 형성하고 이를 통해 정보를 주고받는다.

Ⅳ. 결 론

본 논문에서는 기존 IAM과 다른 새로운 패러다임의 IAM 클러스터링 아키텍처를 제안했다. 제안된 아키텍처와 인증 프로토콜을 이용하여 사용자는 많은 서비스에 가입할 필요 없이 하나의 계정으로 어떤 서비스라도 접근할 수 있다. 또, 새로운 서비스가 추가될 경우 서비스들과 연동하기 위해서 기존 서비스를 수정할 필요 없다. 사용자의 개인 정보를 서버마다 저장하지 않아도 되고 중간자 공격에 안전한 IAM 클러스터링 아키텍처를 이용하여 기업, 국가 행정부처 등에서 효율적인 접근 제어가 가능할 것으로 예상한다.

References

[1] D.-H. Choi, H.-N. You, T.-S. Park, K.-H. Do, and M.-S. Jun, "A design of security structure in bare metal for virtualized internal environment of cloud service," *J. KICS*, vol. 38B, no. 07, pp. 526-534, Jul. 2013.

[2] L. Qian, Z. Luo, and Y. Du, L. Guo, "Cloud computing: An overview," *iFirst Int. Conf., CloudCom 2009,* pp. 626-631, Beijing, China, Dec. 2009.