Authority Management Infrastructure for the Virtual Server Integrated Environment

OGAWA Ryuichi, MAENO Yoshiharu, NAKAE Masayuki

Abstract

In the virtual server integrated environment, users from different organizations must share resources correctly via various types of software, so illegal access and information leak will be prevented in advance. In the cloud computing environment where dynamic placement of resources and creation/deletion of services occur frequently, however, managing and setting access control correctly is a large burden to the operation. To solve this issue, we have developed the integrated access control management technology supporting multi-layer and multi-vendor software. This paper introduces the overview of the technology developed and the proposal for its international standardization.

Keywords

virtual server, role-based access control, authority management
resource model, automatic setup, DMTF standardization

1. Introduction

In recent years, virtual server integrated environments that consolidate multiple servers belonging to different organizations into a server using the virtualization technologies have been spreading. In such environments, users from different organizations must share resources correctly via various types of software, so illegal access and information leak will be prevented in advance. In the cloud computing environment where dynamic placement of resources and creation/deletion of services occur frequently, however, managing and setting access control correctly is a large burden to the operation.

As the infrastructure technology to solve this issue, we have developed the integrated access control management technology. Its technical characteristics are as follows:

(1) Access control in the virtual machine (VM) layer through the application (AP) layer is managed in an integrated manner by extending role-based access control (RBAC: Role-Based Access Control) that is widely used in authority management.

(2) Through automation of access control setup linked with ID management and resource management, changes in the organizations, resource configuration, and services are properly supported.

(3) Standardization of the access control management system has been offered to the DMTF (Distributed Management Task Force) and its diffusion has been promoted as an international standard.

This paper introduces the overview of the technology developed and the proposal of its international standardization.

2. Integrated Access Control Management System

2.1 Necessity of Integrated Access Control Management

The server integrated environment attained through virtualization is a critical cloud computing infrastructure in terms of cost reduction through resource consolidation. To let various users share resources securely in this environment, access control management is required to prevent illegal access and information leak.

Although traditional access control management has achieved measures for respective software such as automation of authority setup for business applications and file sharing on particular operating systems, integrated authority management must be performed for multi-layer and multi-vendor software in cloud computing. Two important requirements are:

- Authority management must integrate various access targets (resources) for respective software layers such as VM and OS (multi-layer support).
- In each layer, authority setup for different software must

be easy (multi-vendor support).

The integrated access control management infrastructure to solve these issues is described in detail below.

2.2 Integrated Access Control Management Infrastructure (IAM)

The IAM (Integrated Access control Manager) is the infrastructure software that manages access control to various types of software on the virtual server in an integrated manner.

Fig. 1 illustrates its overview. The IAM is located on the management server and collaborates with the integrated ID management feature. An agent is located on the virtual server to be controlled for communication with the IAM. The IAM consists of the following three elements:

(1) Policy Generation

The RBAC access description (RBAC policy) corresponding to the role (user attributes such as the post and title) acquired from the integrated ID management server is generated. The RBAC policy consists of three elements; the role, resource, and resource operation right, and is stored in the database in the format of the international standard XACML (eXtensible Access Control Markup Language).

(2) Resource Management

Necessary resource information for policy creation is managed. Resource information such as the guest VM, file, and table is collected from the agent on the controlled server and stored in the database with the structure based on the international standard management model CIM (Common Information Model) [1), 2)] . Further, to manage the resource group explained later, the hierarchical resource management model is employed.

(3) Policy Distribution

The RBAC policy is distributed to the access control software on the specified virtual server. Before distribution, the RBAC policy in the XACML format is automatically converted into the setup file format of the software and automatically set via the agent [3)] .

We have developed - first in the world - the technology that sets the common RBAC policy automatically for the multi-layer and multi-vendor software group. The following sections will introduce the technology as a basis.

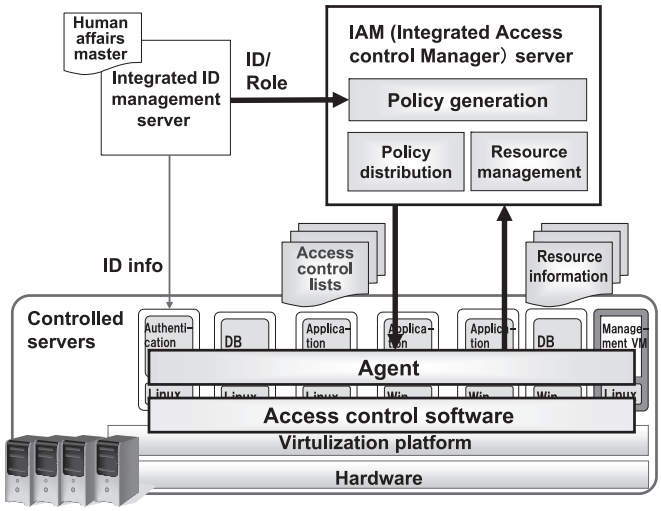

Fig. 1 Integrated access control management infrastructure.

2.3 Simple Description of the RBAC Policy Using a Resource Group

With the traditional RBAC policy, the access target is designated in a fine-grained manner using the file name, etc. Therefore, description is very cumbersome in the server integrated environment. The IAM has extended the RBAC policy to designate access control totally using a resource group [2), 3)] .

There are a variety of access target resources such as the guest VM, file, database table, etc., for which different operations are available. To represent various operation authorities in a common format, resource management employs the extended CIM model, based on which the relationship between the resource and operation authority is managed. As a result, policy description supporting the multi-layer and multi-vendor software becomes very simple.

Fig. 2 illustrates an example. Through standardization of the format between the resource group and operation authority, highly abstract RBAC policies such as “Only the staff in the accounting section can edit documents in the section” or “Only the manager in the accounting section can manage the server in the section” can be created without recognition of the setting target software layer and type.

2.4 Automatic Setup of the RBAC Policy Reflecting the Latest ID/Resource Information

The RBAC policy created in policy generation can be automatically distributed and set up by designating the distribution destination virtual server and distribution schedule in advance using the GUI. **Fig. 3** illustrates the process flow in this case.

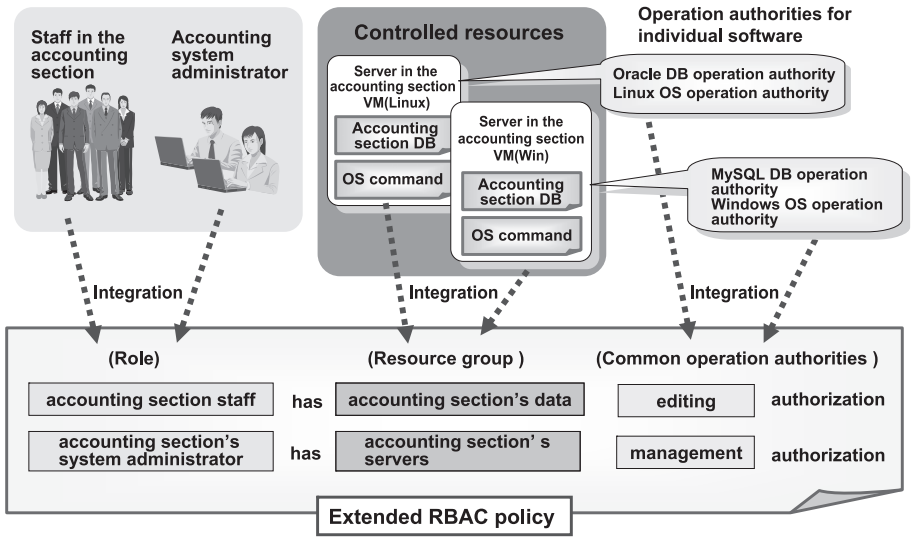

Fig. 2 Simple description of the RBAC policy using a resource group.

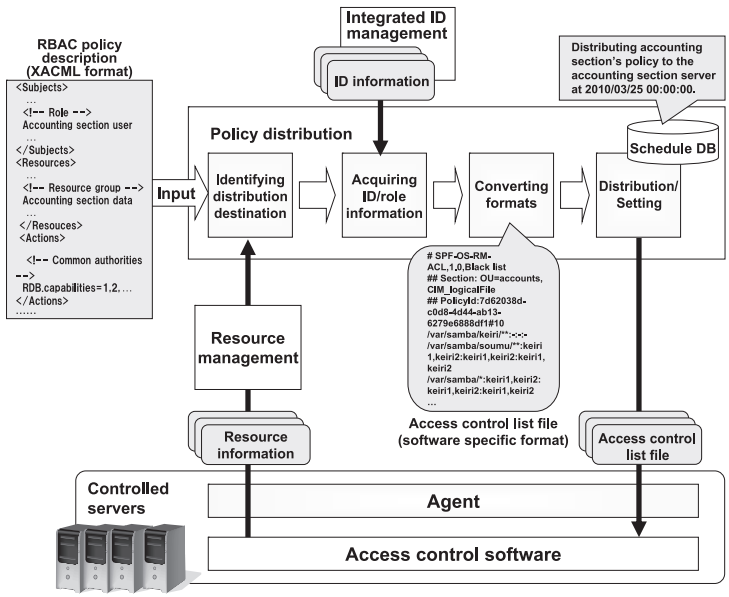

Fig. 3 Policy distribution/setup process flow.

1) Resource information is acquired from the resource management feature and the distribution destination virtual server contained in the resource group is identified. For example, even though the virtual server has been moved through migration after policy creation, the correct distribution destination is determined as a result of updating the resource management database.

2) To convert the role described in the RBAC policy into the ID/role on the distribution destination virtual server, the integrated ID management feature is queried and the ID/role

information is acquired.

3) Using the acquired ID/role information and resource information, the RBAC policy is converted into the setup file format meeting the software on the distribution destination virtual server. **Fig. 4** illustrates the preview screen showing conversion of the common RBAC policy into the file setting format at the distribution destination. In this way, the setup file (access control list file) based on the latest information can be automatically generated using the common RBAC policy. Therefore, inadequacy due to incomplete updates and incorrect input is eliminated.

4) The converted file is distributed to the agent on the distribution destination virtual server and set in various access control software. In this case, the distribution schedule can be designated according to routine maintenance, etc.

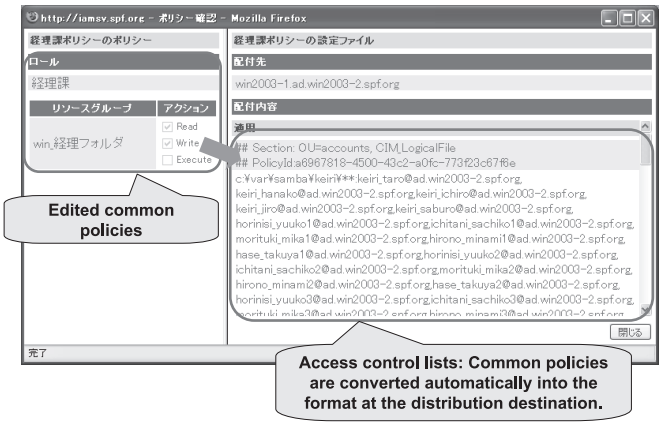

Fig. 4 Setup file format conversion preview screen.

3. Implementation of the Integrated Access Control Management System and Performance Demonstration

The IAM server has been implemented in the Java language and its operation in RedHat Enterprise Linux 5 has been verified. As the virtulization platform software, Xen allowing for easy linkage with the guest VM management feature has been employed. For communication with the agent, WS-Management as an international standard operation management protocol has been adopted. Through development of the adaptor for the following software, authority setup has been automated:

- VM layer:Xen guest VM management software (libvirt)
- OS layer:Linux, Windows
- DB layer:MySQL, Oracle
- AP layer:Provides the adaptor development SDK for user applications

To validate the effectiveness of the IAM server developed, a demonstration test was conducted for three months from November 2009. In this test, a case of integrating the human affairs/accounting system in a company with 3,000 users was assumed. An environment in which the business server actually used by the company was virtualized was built. Management cost evaluation and scalability performance evaluation through pseudo operation were performed. **Fig. 5** illustrates the

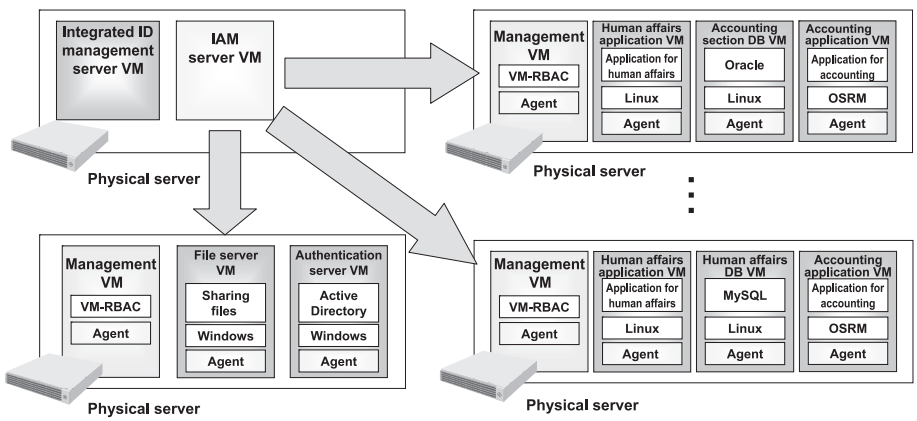

Fig. 5 Overview of the demonstration test system.

overview of the demonstration test system. The scale of this environment is as follows:

- **Number of physical servers: 6**

(connected via 1Gb-Ethernet)

- **Number of guest VMs: 15**

(12 business AP/DB servers, 2 file servers, 1 authentication server)

- **Number of business applications: 3**

(2 for human affairs, 1 for accounting)

The demonstration test resulted in the following:

(1) Up to 80% of the Authority Management Cost Reduced

As a result of measuring the working hours required for setup of the ID/access control setup for changes in system administrators in the virtual server environment, reduction of up to 80% compared with the traditional system using manpower was verified. The rate of reduction will further increase if the number of guest VMs increases.

(2) Sufficient Scalability Reserved for Business System Authority Management in a Company with 10,000 Users

In the business server integrated environment with 10,000 users and 200 VMs, it was verified that ID/access control package setup could be implemented within the routine maintenance hours (up to 5 hours).

On the other hand, the following issues were identified:

- Integration know-how for migration of the existing system is insufficient.
- Role design and policy design are difficult.

Against these issues, enhancement of the adaptor development SDK, establishment of the simple design approach, and enhancement of the collaboration with system's unique authority management will be studied.

4. International Standardization of the Integrated Access Control Management System

In the resource management system, it is indispensable to newly specify software attributes relating to multi-layer access control setup and extend the existing CIM model.

In a large-scale virtual server integrated environment such as cloud, it is considered that interoperability of multi-vendor products relating to access control collective management and package setup is essential for efficient operation. Therefore, to spread the resource management system and policy distribution system employed for the IAM as an international standard, we made a proposal for the DMTF, a multi-vendor system operation standardization organization. **Fig. 6** illustrates the overview of the proposal (IAM profile).

Fig. 7 illustrates the class diagram representing the extended CIM model in the IAM profile. This figure is represented in the implementation-independent system model language (UML). The following two specifications form the core of the IAM profile:

- Definition of the access control feature for the software needing access control setup (ReferenceMonitor class in Fig. 7)
- Definition of the access control feature target resource and its resource operation authority (RMTargetSettingData class in Fig. 7)

After approval by the DMTF, this proposal was announced as a Work in Progress (standardization scheduled) in February 2010 [4]. We will continue the activities to complete standardization in 2010. Through standardization by the DMTF, access control collective management and package setup in a multi-vendor environment will be easily achieved.

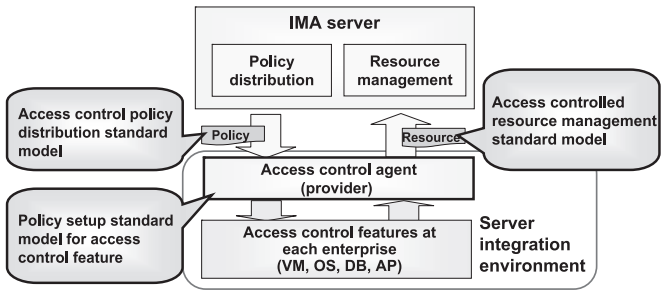

Fig. 6 Overview of the proposal for standardization by the DMTF.

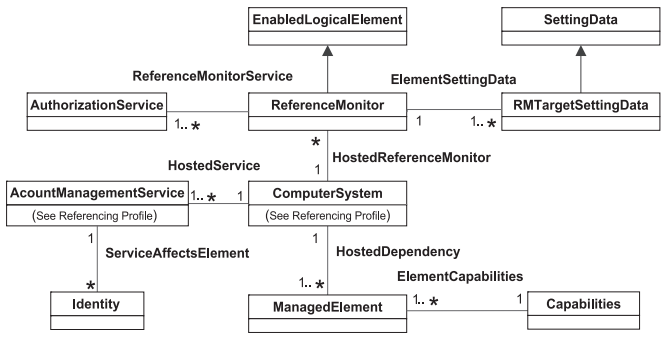

Fig. 7 Class diagram specified by the IAM profile (partial).

5. Conclusion: Issues in Application to the Cloud Service

With the IAM, authorities in the virtual server integrated environment can be managed in an integrated manner and illegal access and information leak can be prevented. On the other hand, there are issues in applying the IAM to the cloud service.

First, management of not only the software in the VM layer and AP layer but also management of the network layer is important. The RBAC policy relating to the management operation of the physical/virtual network must be supported. Further, multitenant supporting authority management and the technical scheme locating the responsibility in the event of illegal access or information leak are important.

We will develop an integrated access control management system that solves these issues. This system will be applicable to the private cloud used within a particular enterprise as well as the public cloud used by a large indefinite number of companies.

A part of this research is the result of "2007 Secure Platform Project" commissioned by the Ministry of Economy, Trade and Industry to the Association of Super-Advanced Electronics Technologies (ASET).

References

1) K. Tadano et al., "Automatic Cache Update Control for Scalable Resource Information Service with WS-Management," in Proceedings of DMTF SVM'09, 2009.

2) K. Tadano et al., "Research and Development of Secure Platform (3) Resource Information Management for Integrated Access Control," in Proceedings of FIT2009, September 2009.(in Japanese)

3) Y. Morita et al., "Research and Development of Secure Platform (2) Access Control Policy Composition and Distribution to Server Consolidated Environment," in Proceedings of FIT2009, September 2009. (in Japanese)

4) DMTF DSP1106, "Integrated Access Control Policy Management Profile," February 2010.

Authors' Profiles

OGAWA Ryuichi
Senior Principal Researcher
Service Platforms Research Laboratories

MAENO Yoshiharu
Principal Researcher
Service Platforms Research Laboratories

NAKAE Masayuki
Principal Researcher
Service Platforms Research Laboratories