

ROLE-BASED PRIVILEGE MANAGEMENT

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to an improved data processing system and, more specifically, to a computer implemented method, an apparatus, and a computer program product for role-based privilege management.

2. Description of the Related Art

Various systems used today represent authorization policy using role-based access control (RBAC) semantics. While a role may span many domains, for example, membership of the application admin role may confer administrative privileges for the operating system, a database, and an application server, there is no general way to represent the privileges conveyed by a role membership in a single way. Role-based privileges may vary from system to system, causing privileges to be relative to an install location of particular files on a system, particular universal resource locator (URL), Web resources, or operating system type.

The representation of the role-based access control policies has become complex and varied. Having to deal with various implementations of similar, yet different, role scenarios across multiple systems, subsystems, and applications typically leads to administration inefficiencies, confusion, and possible errors.

BRIEF SUMMARY OF THE INVENTION

According to one embodiment of the present invention, a computer implemented method for role-based privilege management is provided. The computer implemented method receives a transformation request from a requester to form a received request and identifies a target environment of the received request. The computer implemented method determines whether the target environment matches a predefined environment in a set of role-based privileges and, responsive to a determination that the target environment matches a predefined environment in the set of role-based privileges, maps the parameterized privileges from the set of role-based privileges to the target environment and performs the request.

In another illustrative embodiment, an apparatus in the form of a data processing system for role-based privilege management is provided. The data processing system comprises a bus, a memory connected to the bus, wherein the memory comprising computer-executable instructions, a communications unit connected to the bus, a display unit connected to the bus, a processor unit connected to the bus, wherein the processor unit executes the computer-executable instructions in the memory to direct the data processing system to receive a transformation request from a requester to form a received request, identify a target environment of the received request, determine whether the target environment matches a predefined environment in a set of role-based privileges, respond to a determination that the target environment matches a predefined environment in the set of role-based privileges, to map parameterized privileges from the set of role-based privileges to the target environment, and perform the request.

In yet another illustrative embodiment, a computer program product for role-based privilege management is provided. The computer program product comprises computer-readable, recordable-type medium tangibly embodying computer-executable instructions. The computer-executable instructions comprising, computer-executable instructions for receiving a transformation request from a requester to

form a received request, computer-executable instructions for identifying a target environment of the received request, computer-executable instructions for determining whether the target environment matches a predefined environment in a set of role-based privileges, computer-executable instructions responsive to a determination that the target environment matches a predefined environment in the set of role-based privileges, for mapping parameterized privileges from the set of role-based privileges to the target environment, and computer-executable instructions for performing the request.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. 1 is a pictorial representation of a network of data processing systems in which illustrative embodiments may be implemented;

FIG. 2 is a block diagram of a data processing system is shown in which illustrative embodiments may be implemented;

FIG. 3 is a block diagram of components of a privilege manager in accordance with illustrative embodiments;

FIG. 4 is a block diagram of a privilege management system in accordance with illustrative embodiments;

FIG. 5 is a text representation of a general format of a privilege template, in accordance with illustrative embodiments;

FIG. 6 is a text representation of an example of a privilege template with a role definition, and an inherited role example, in accordance with illustrative embodiments;

FIGS. 7A-7B are a text representation of a generalized role specification, in accordance with illustrative embodiments; and

FIG. 8 is a flowchart of a process using the privilege manager of FIG. 3, in accordance with illustrative embodiments.

DETAILED DESCRIPTION OF THE INVENTION

As will be appreciated by one skilled in the art, the present invention may be embodied as a system, method, or computer program product. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, the present invention may take the form of a computer program product embodied in any tangible medium of expression having computer-usable program code embodied in the medium.

Any combination of one or more computer-usable or computer-readable medium(s) may be utilized. The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electro-magnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples (a non-exhaustive list) of the computer-readable medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CDROM), an optical storage device, a transmission media such as those supporting the Internet or an intranet, or a magnetic storage device. Note that the computer-usable or computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance,