

13

apparatus that can contain, store, communicate, propagate, or transport the program for use by, or in connection with, the instruction execution system, apparatus, or device.

The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device), or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk, and an optical disk. Current examples of optical disks include compact disk-read only memory (CD-ROM), compact disk-read/write (CD-R/W), and DVD.

A data processing system suitable for storing and/or executing program code will include at least one processor coupled directly, or indirectly, to memory elements through a system bus. The memory elements can include local memory employed during actual execution of the program code, bulk storage, and cache memories which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution.

Input/output or I/O devices (including but not limited to keyboards, displays, pointing devices, etc.) can be coupled to the system either directly or through intervening I/O controllers.

Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems, remote printers or storage devices through intervening private or public networks. Modems, cable modems and Ethernet cards are just a few of the currently available types of network adapters.

The description of the present invention has been presented for purposes of illustration and description, and is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art. The embodiment was chosen and described in order to best explain the principles of the invention, the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

What is claimed is:

1. A computer implemented method for role-based privilege management, the computer implemented method comprising:

receiving a request from a requester for an allocation of privileges associated with a role in a target environment; identifying the target environment of the request and the role requested;

identifying, using a processing unit, a set of privilege templates referenced by the role, wherein the set of privilege templates includes parameters for a plurality of environments;

determining whether the target environment is one of the plurality of environments referenced by the parameters in the set of privilege templates;

responsive to determining that the target environment is one of the plurality of environments referenced by the parameters in the set of privilege templates, mapping values from the parameters that are specific to the target environment to the target environment; and

conveying to the requester the privileges associated with the role in the target environment;

wherein identifying the set of privilege templates referenced by the role comprises:

identifying a plurality of privileges associated with the role; and

14

searching a database for a privilege template for an individual privilege in the plurality of privileges, wherein the privilege template includes a first set of parameters for assigning the individual privilege in a first system having a first operating system and a second set of parameters for assigning the individual privilege in a second system having a second operating system.

2. The computer implemented method of claim 1 further comprising:

responsive to determining that the target environment is one of the plurality of environments referenced by the parameters in the set of privilege templates, raising an error; and

notifying the requester.

3. The computer implemented method of claim 1, wherein identifying the target environment of the request comprises:

identifying an operating system of a computer system that the request was received from as the target environment; and

wherein mapping values from the parameters that are specific to the target environment to the target environment comprises:

selecting a set of parameters from the set of privilege templates that are specific to the operating system of the computer system.

4. The computer implemented method of claim 1, wherein identifying the set of privilege templates referenced by the role comprises:

searching a database for a set of role-based privileges for the role, wherein the set of role-based privileges include one or more privileges for the role; and

identifying a privilege template for each privilege in the set of role-based privileges to form the set of privilege templates referenced by the role, wherein the set of role-based privileges comprises a data structure having a hierarchical structure having a set of attributes of a first type to define a specific environment to which the set of role-based privileges apply, and a set of attributes of a second type to define privileges to be conveyed in the specific environment.

5. The computer implemented method of claim 1, wherein providing the requester with the allocation of privileges associated with the role in the target environment comprises:

providing the requester with the allocation of privileges only upon mapping values from the parameters that are specific to the target environment.

6. A data processing system for role-based privilege management, the data processing system comprising:

a bus;

a memory connected to the bus, wherein the memory comprising program code;

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 is configured to execute the program code;

receive a request from a requester for an allocation of privileges associated with a role in a target environment; identify the target environment of the request and the role requested;

identify a set of privilege templates referenced by the role, wherein the set of privilege templates includes parameters for a plurality of environments;

determine whether the target environment is one of the plurality of environments referenced by the parameters in the set of privilege templates;