

Enabling Dell OpenManage Applications for Microsoft Active Directory **User Authentication**

Many enterprises have implemented security policies that require user authentication for directory services such as Microsoft® Active Directory® directory service. Certain components of the Dell™ OpenManage™ systems management suite—Dell OpenManage Server Administrator, Dell OpenManage IT Assistant, and Dell Remote Access Controller 4—have been enabled for Microsoft Active Directory user authentication. This article describes Dell’s approach to the security integration of these components and provides implementation examples.

BY MARCOS PALACIOS, PH.D.

Related Categories:

Authentication

Dell OpenManage

Dell PowerEdge servers

Directory services

Microsoft Active Directory

Microsoft Windows

Systems management

Visit www.dell.com/powersolutions for the complete category index to all articles published in this issue.

A directory is a repository used to store information about a set of relevant objects. For example, a telephone directory stores information about telephone service subscribers in a given locale. In a server’s file system, the directory stores information about files on the server and their respective locations and attributes. In a typical distributed enterprise computing system, many types of relevant objects need to be stored in a directory—including user account names, application servers, Web servers, printers, fax servers, and other objects. End users want to easily and quickly find the objects they need, while IT administrators are concerned with managing and securing access to the various objects to comply with their organization’s security and usage policies.

Directory service capabilities and features

A robust directory service is one of the most important components of an extended computer system. Users and

administrators frequently do not know the exact names of the objects they need to access. They may, however, know one or more attributes of these objects.

A directory service allows a user to find any object based on one or more of its attributes by querying the directory to obtain a list of objects that match the attributes. For example, an administrator might pose the query: “Find all duplex printers in building 26.” In addition, a directory service can perform the following actions:

- Enforce security defined by administrators to help keep information safe from intruders
- Distribute a directory across several computers in a network
- Replicate a directory to make it available to more users and to keep it highly available
- Partition a directory into multiple stores to allow the storage of very large numbers of objects

Microsoft Active Directory is the directory service included with Microsoft Windows® 2000 Server and Windows Server™ 2003 operating systems. It extends the functionality of previous Windows-based directory services and introduces additional features. Active Directory is secure, distributed, partitioned, replicated, and highly scalable. It is designed to work well in any size installation, from a single server hosting a few hundred objects to thousands of servers hosting millions of objects. Active Directory's feature set helps ease navigation and management of large amounts of information—helping to save time and improve productivity for both administrators and end users.

Active Directory is a distributed database. The rules for the database are defined by the database schema, which is a collection of attributes and classes. An example class is the User class. Examples of attributes from the User class are First Name, Last Name, and Phone Number.

Dell OpenManage support for Microsoft Active Directory

Several products in the Dell OpenManage suite now support Active Directory user authentication: Dell OpenManage Server Administrator (OMSA), Dell OpenManage IT Assistant (ITA), and the Dell Remote Access Controller 4 (DRAC 4). A major advantage of Dell's support for Active Directory is that supported Dell products use the same authorization and authentication schemas and associated security configuration user interfaces as Active Directory, which enhances the end user's experience by helping to reduce the complexity associated with directory services security. Figure 1 shows how the applications comprising the Dell OpenManage suite can integrate with Microsoft Active Directory directory services security.

Dell schema extensions for Active Directory enablement

Dell has extended the Active Directory schema by adding attributes and classes to represent Dell OpenManage objects. By doing so, Dell has tailored Active Directory to meet Dell OpenManage user authentication and authorization needs.

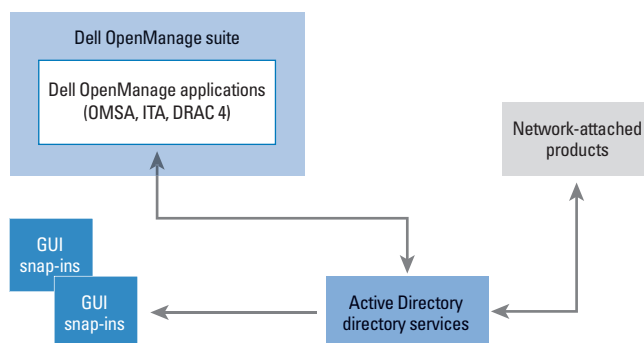


Figure 1. Dell OpenManage integration with Microsoft Active Directory security

Dell has defined a group of Active Directory objects that can be configured depending on an organization's IT environment: an Association object, a Device object, an Application object, and a Privilege object.

- **Association object:** Links together users or groups possessing a specific set of privileges to one or more Dell OpenManage devices or applications
- **Device object:** Represents a Dell remote access controller (RAC) device
- **Application object:** Represents either a Dell OMSA application or a Dell ITA application
- **Privilege object:** Lists which privileges are granted to users depending on the Dell OpenManage application or device

One Application object or Device object must exist in the Active Directory database for each Dell OpenManage application or device to be managed. Administrators can create as many Privilege objects as there are levels of users in the organization. Similarly, administrators can create as many Association objects as there are relationships between users and the applications or devices to be implemented in the environment.

To help administrators modify the Active Directory schema, Dell provides both a wizard installation utility—called the Schema Extender Utility—and a command-line Lightweight Directory Access Protocol (LDAP) Data Interchange Format (LDIF) configuration file for each Dell OpenManage application and device to be Active Directory enabled. The Schema Extender Utility walks the administrator through the process of extending the schema. When executed, the utility is designed to display the results of each of the attributes and classes added to the schema and a message acknowledging that the Active Directory objects have been successfully added. If another administrator has already run the Schema Extender Utility and made the changes to the schema, then the utility generates a message indicating that the Active Directory objects already exist.

The LDIF configuration file is for advanced Active Directory administrators who want to see the specific modifications that they have configured before these changes are made to the Active Directory schema. Microsoft Windows operating systems provide a utility called `ldifde.exe` that is used to run the LDIF configuration file.

Extension to the Microsoft Management Console snap-in

After extending the schema, administrators must extend the Microsoft Management Console (MMC) Active Directory Users and

A robust directory
is one of the most
important components
of an extended
computer system.

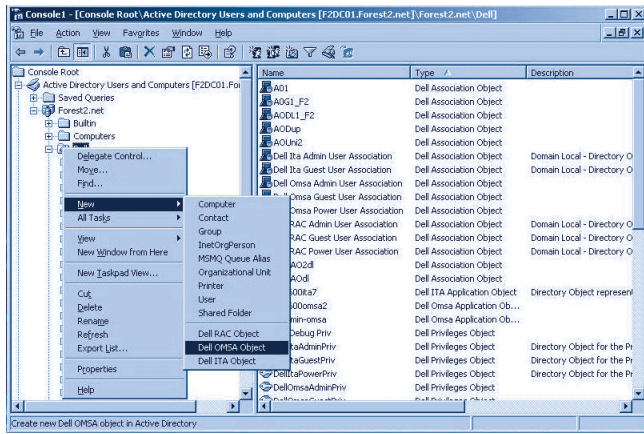


Figure 2. Adding an Application object to the Microsoft Active Directory database

Computers snap-in. This allows administrators to create the Active Directory objects needed to manage RAC devices, OMSA applications, and ITA applications. Dell provides a wizard installation application that walks administrators through modifying the MMC snap-in. Administrators must install this utility on each server that is used to access the MMC Active Directory Users and Computers snap-in utility.

Every Active Directory domain contains a set of containers that are created during the installation of Active Directory. Organizational units are Active Directory containers into which administrators can place users, groups, computers, and other organizational units. From the menu associated with a container or organizational unit in the Active Directory Users and Computers console, the snap-in extensions allow administrators to create Active Directory objects by selecting either New > Dell RAC Object; New > Dell OMSA Object; or New > Dell ITA Object (see Figure 2). Administrators can add these objects by right-clicking on the container or organizational unit to which they want to add the object. The menu structure shown in Figure 2 appears if the container or organizational unit supports Dell objects.

Dell OpenManage and Active Directory integration

Once the extensions are installed in the Active Directory database, new Active Directory objects for Dell OpenManage integration can be added. Administrators can add a Device object, for example, using the following steps to create each device and application:

1. Select New > Dell RAC Object from the Active Directory console menu, and a dialog box similar to the one shown in Figure 3 is displayed.

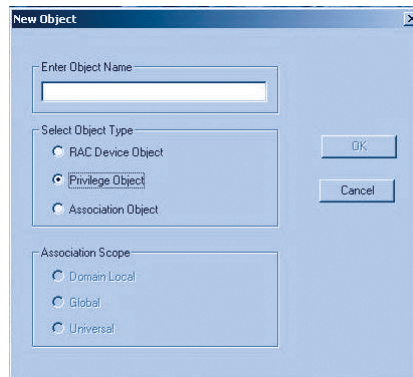


Figure 3. Adding a Device object to the Active Directory database

2. Choose the object name, type of object, and scope characteristics of the object. The object will then be created and added to the container from which the command was initiated.

To create an Association object, administrators must choose the association scope that applies to the type of object added. The association scope is the security group type that the association object will have. The Association object is derived from a security group and must contain a group type. Universal Association objects can be created only when the Active Directory domain is functioning in native mode or higher.

Dell has tailored Active Directory to meet Dell OpenManage user authentication and authorization needs.

By right-clicking on an Association object's Properties page, administrators can add the desired users or groups, a Privilege object, and Dell products to the association. Figure 4 shows a user called Administrator being added to an Association object.

Similarly, by clicking on the Privilege Object tab, administrators can add the Privilege object to the association that defines the user's or group's privileges when authenticating to a RAC device or Dell OpenManage application. *Note:* Only one Privilege object can be added to an Association object. Additionally, by clicking on the Products tab, administrators can add one or more Dell products to the association. These products specify the RAC devices or Dell OpenManage applications that are available for the defined users or groups. Administrators can add multiple Dell products to an Association object by using the Add button.

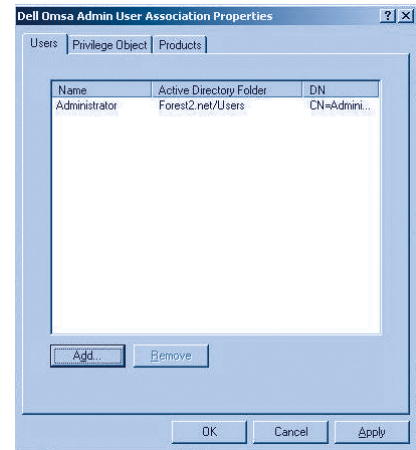


Figure 4. Adding a user called Administrator to the Association object

Active Directory configuration parameters for Dell products

The final step in establishing communication with the Active Directory servers is to configure the individual RAC devices and Dell OpenManage applications with specific parameters. Administrators must configure the following Active Directory settings across devices and applications using their respective interfaces:

- **Active Directory Dell product name:** This is a unique string representing the name of the Dell product. The same name should be used both for creating the Dell product in the Active Directory environment and adding the Dell product to the Dell Association object.
- **Active Directory domain name:** This is the Active Directory root domain name—for example, mydomain.com.
- **Active Directory Certificate Authority (CA) certificate:** This certificate is created from the organization's Active Directory certification authority. The certificate is downloaded to a file and then uploaded to the server where the Dell product is located.
- **Dell product certificate:** This certificate allows the Dell product to communicate securely with the Domain Name System (DNS) server to authenticate a user in the Active Directory database. The Dell product certificate is downloaded to a file and then uploaded to the Active Directory domain being accessed.

IT management advantages of Active Directory support

By delivering support for Microsoft Active Directory authentication in Dell OpenManage applications and RAC devices, Dell has enabled IT administrators to seamlessly integrate management of Dell products into the directory service that they are already using to manage other objects in their enterprise. The benefits of this standards-based approach include maximum flexibility for IT administrators in controlling access to Dell OpenManage applications, granular assignment of privileges based on the type of Dell OpenManage application being accessed, and consolidation of security processes in a central Active Directory repository rather than having to distribute these security processes among local devices. 

Marcos Palacios, Ph.D., is a software quality engineer on the Dell OpenManage development team. Prior to joining Dell, he worked for BMC Software, where he specialized in software test processes and methodologies. Marcos has a Ph.D. from Texas Tech University.

FOR MORE INFORMATION

Dell OpenManage systems management:
dell.com/openmanage