

Using Microsoft Active Directory Authentication with the DRAC 4

With the release of the Dell™ Remote Access Controller 4 (DRAC 4), administrators can now take advantage of their existing Microsoft® Active Directory® directory service environments for security implementations. This article explains the advantages of DRAC 4 and provides a step-by-step configuration process to enable Active Directory authentication and authorization.

BY JON MCGARY AND BRADLEY BRANSOM

Microsoft Active Directory provides a directory service that allows organizations to administer their networked resources. In addition, it offers a scalable management solution and supports open standards for Lightweight Directory Access Protocol (LDAP) and other query interfaces. One of the goals of a directory service is to maintain a common database of all information needed for controlling user access, computers, printers, and other network resources. The Dell Remote Access Controller 4 (DRAC 4) allows administrators to manage remote access controller (RAC) users and devices from within existing Active Directory environments. The DRAC 4 supports Active Directory authentication for all user interfaces such as the RAC graphical user interface (GUI) login and remote `racadm` commands over serial and Telnet interfaces.

Understanding Active Directory schema extensions

Active Directory data can be conceptualized as a distributed database of attributes and classes. The Active Directory schema comprises the set of rules for what data can be added or included in the database. For example, a user class may include attributes such as the user's first name, last name, and phone number. Companies can extend the Active Directory database by

adding their own unique attributes and classes to address environment-specific needs. Dell has extended the Active Directory schema to include the necessary changes to support remote management authentication and authorization.

Every attribute or class that is added to Active Directory must be defined with a unique ID. Microsoft maintains a database of Active Directory object identifiers (OIDs) to help ensure that the extensions that companies add to the schema will be unique and will not conflict with each other. To extend the schema in Microsoft Active Directory, Microsoft provided Dell with a unique OID, a unique prefix, and unique linked-attribute IDs for the attributes and classes that Dell added into the directory service:

- Dell prefix: dell
- Dell base OID: 1.2.840.113556.1.8000.1280
- RAC LinkID range: 12070 to 12079

Working with Dell schema extensions

To help enable flexibility for a multitude of customer environments, Dell provides a group of objects that can be configured by administrators depending on the desired results. Dell has extended the schema to include Association, RAC Device, and Privilege objects (see Figure 1).

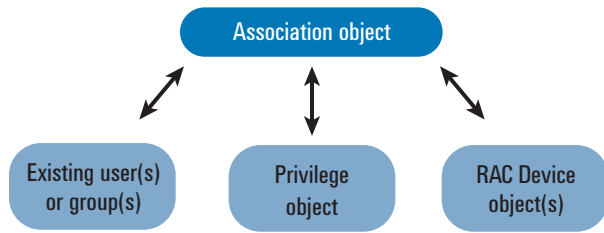


Figure 1. Association, RAC Device, and Privilege objects

The Association object is used to link together users or groups that have a specific set of privileges to one or more RAC devices. This model provides administrators with the flexibility to address different combinations of users or groups, privileges, and RAC devices on the network without adding much complexity.

Each organization's Active Directory environment can be configured differently; however, at least one Association object must exist, and one RAC Device object must exist for each of the RACs on the network to which the user wants to connect. The Association object enables the privileges to be granted to the assigned users on the RAC devices.

Tools to modify the schema extensions

To help administrators modify and extend the Active Directory schema, Dell provides both a step-by-step installation application and a command-line LDAP Data Interchange Format (LDIF) file. When executed, the installation application—called the Dell Schema Extension utility—displays the results of each attribute and class that is added to the schema.¹ If the Dell Schema Extension utility has already been run and the changes to the schema have been made, then a message is generated indicating that the objects already exist.

The LDIF file is for advanced Active Directory users who want to view the specific modifications before they are made to the Active Directory schema. Microsoft Windows® operating systems provide a utility called `ldifde.exe` that can be used to run the .ldf configuration file that Dell provides.

An example LDIF script is as follows:

```
c:\ldifde -i -k -c dc=dell,dc=com
dc=mydomain,dc=com -f dellschemaextension.ldf
```

where `dc=dell,dc=com` is the domain listed in the .ldf file and `dc=mydomain,dc=com` is the target domain where the Active Directory extensions will be installed.

Prerequisites for changing the Active Directory schema are as follows:

- The system registry entry `\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Schema Update Allowed` must be set to "1."
- The logged in user must have schema administrator rights on the domain controller being modified.
- The domain must be the schema Flexible Single Master Operations (FSMO) role owner of the Active Directory forest.

Extension to the Microsoft Management Console snap-in

After extending the schema, an administrator must extend the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in utility. This will allow the administrator to manage users or groups, Privilege objects, RAC Device objects, and Association objects just like any other resource in the system. Dell provides an installation application that installs the Dell extensions to the MMC snap-in.² Administrators must install this utility on all the clients and servers that are used to manage the Dell objects through the Active Directory Users and Computers MMC snap-in utility.

Using predefined Active Directory objects

RAC privileges provided by the Active Directory schema modifications include nine user capabilities. These capabilities can be combined as needed by administrators when the Privilege object is created:

- RAC Login User
- RAC Card Configuration Admin
- RAC User Configuration Admin
- RAC Log Clear Admin
- RAC Server Reset and Power-On/Off User
- RAC Console Redirect User
- RAC Virtual Media User
- RAC Test Alert User
- RAC Debug Command Admin

To create generic authorization levels, Dell provides three recommended groupings of these privileges, as shown in Figure 2.

When administrators use the Dell Schema Extender utility to install the schema, this utility creates an organizational unit in Active Directory containing three predefined Privilege objects and three Association objects. Administrators who do not require all the granularity available for RAC privileges can simply use the following predefined objects:

- RAC Guest User Privilege object
- RAC Admin User Privilege object
- RAC Power User Privilege object

¹The Dell Schema Extension utility and LDIF file are located on the Dell OpenManage™ application CD in the `Support\OMActiveDirectory Tools\RAC4` directory and can be run directly from the CD. There is no need to install the utility.

²The MMC snap-in is located on the Dell OpenManage application CD. Administrators can install the MMC snap-in by selecting `Management Station Software > Active Directory Snap-In`.

RAC Guest User	RAC Power User	RAC Administrator
RAC Login User	RAC Login User	RAC Login User
	RAC Log Clear Admin	RAC Log Clear Admin
	RAC Server Reset and Power-On/Off User	RAC Server Reset and Power-On/Off User
	RAC Console Redirect User	RAC Console Redirect User
	RAC Virtual Media User	RAC Virtual Media User
	RAC Test Alert User	RAC Test Alert User
	RAC Debug Command Admin	RAC Debug Command Admin
		RAC Card Configuration Admin
		RAC User Configuration Admin

Figure 2. Dell-recommended groupings of RAC privileges

- RAC Guest User Association object
- RAC Admin User Association object
- RAC Power User Association object

Creating a new Dell object

The Active Directory Users and Computers snap-in extension allows administrators to create new Dell objects by selecting New > New Dell Object from a menu associated with a container or organizational unit (see Figure 3). Administrators may add RAC objects to a container or organizational unit by right-clicking on the container to which they want to add the RAC objects. If the container or organizational unit supports RAC objects, the menu appears. New Dell objects are created just like any other objects that administrators would create using the Active Directory Users and Computers MMC snap-in utility.

After an administrator selects New Dell Object, a dialog box similar to that shown in Figure 4 is displayed. The administrator can enter the object name and select the type of object and Association object scope characteristics of the object. The object will then be created and added to the container from which the command was initiated.

When creating a Dell Association object, administrators must choose the Association object scope that applies to the type of object they intend to add. The association scope is the security group type that the Association object will be. The Association object is derived from a group and must contain a group type. Universal Association objects are available only when the Active Directory domain is functioning in native mode or higher.

Associating users, groups, Privilege objects, and RAC Device objects to the Association object

By right-clicking on the Association object and selecting Properties, an administrator can associate the desired users or groups, Privilege object, and RAC Device objects to the Association object in the Dell RAC Power User Association Properties dialog box (see Figure 5).

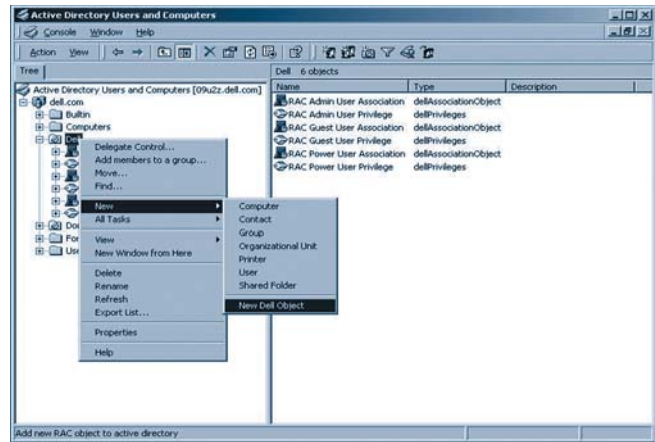


Figure 3. Active Directory Users and Computers MMC snap-in GUI

By clicking on the Privilege Object tab, an administrator can add the Privilege object to the Association object that defines the user’s or group’s privileges when authenticating to a RAC device.

In the example in Figure 5, the DellRACPowerPriv object has been added to the Association object. Note that only one Privilege object can be added to an Association object. By right-clicking on the Privilege object and selecting Properties, an administrator can modify the nine privilege attributes assigned to the object.

By clicking on the Products tab, an administrator can add one or more RAC Device objects or groups of RAC Device objects to the Association object. These objects specify the RAC devices connected to the network that are available to the defined users or groups. Multiple RAC Device objects or groups of RAC Device objects may be added to an Association object.

Configuring Active Directory parameters in the RAC GUI

The last configuration step is to configure the individual DRAC 4 device using the RAC GUI (see Figure 6). Administrators must configure the following Active Directory settings:

- **Enable Active Directory:** By default this is disabled. Select this check box to enable the DRAC 4 to use Active Directory for user authentication.

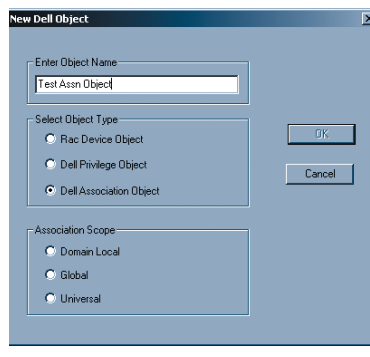


Figure 4. New Dell Object dialog box

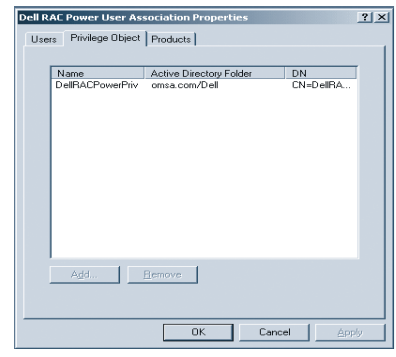


Figure 5. Dell RAC Power User Association Properties dialog box

- **DRAC 4 name:** This is a unique string representing the name of the RAC Device object. This name should be the same name used for the RAC Device object created in the Active Directory environment and added to the Dell Association object. (Refer to the section “Associating users, groups, Privilege objects, and RAC Device objects to the Association object” in this article.) By default, this value is null. A valid RAC Device object name must be between 1 and 256 characters in length and cannot contain any spaces.
- **Root domain name:** This value is null by default. A valid domain name must be between 1 and 256 characters in length, cannot contain any spaces, and must contain a valid domain classification such as com, edu, gov, int, mil, net, or org. For example, dell.com is a valid Active Directory root domain name.
- **DRAC 4 domain name:** This is the Domain Name System (DNS) name of the domain in which the Active Directory RAC Device object is a member (for example, dell.com). This value is null by default. A valid domain name must be between 1 and 256 characters in length, cannot contain any spaces, and must contain a valid domain classification such as com, edu, gov, int, mil, net, or org.
- **Active Directory Certificate Authority (CA) certificate:** This is an X509 version 3 base64–encoded certificate that is created from an organization’s Active Directory environment. It allows the DRAC 4 to communicate securely with the DNS server to authenticate a RAC user in the Active Directory database.³
- **DRAC 4 server certificate:** This certificate allows the DRAC 4 to communicate securely with the DNS server to authenticate a RAC user in the Active Directory database. The RAC certificate is downloaded to a file and then uploaded to the Active Directory domain being accessed.⁴
- **Dynamic Host Configuration Protocol (DHCP) or static DNS server:** The DRAC 4 device can be configured to use either DHCP or a static IP address to connect to the DNS server. The DNS server contains the Active Directory database information that allows the RAC to authenticate the Active Directory request. The DHCP DNS feature can be enabled or disabled by selecting or unselecting the check box located on the Network page, which is accessible from the Configuration tab. The static preferred and alternate DNS server IP addresses can be entered in the fields provided.

Authenticating valid Active Directory usernames

Once the Active Directory environment has been modified and the various objects configured, the user can log in. A valid Active Directory RAC username can be authenticated in several formats. In the User Name field, enter either a DRAC 4 username as *username*,

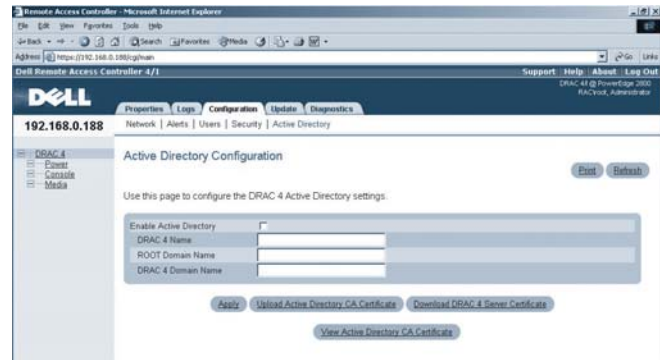



Figure 6. Active Directory Configuration screen

or an Active Directory user name as *domain\username*, *domain/username*, or *user@domain*.

The DRAC 4 username for local users is case sensitive; the Active Directory username is not case sensitive. Examples of an Active Directory user name are: *dell.com\john_doe* or *john_doe@dell.com*. The domain and username should be between 1 and 256 characters in length and cannot contain any spaces or special characters.

Supporting existing Microsoft Active Directory environments

Support for Microsoft Active Directory is one of the many useful features of the DRAC 4. If this feature is enabled, whenever a user enters a domain name and attempts to log in to the RAC device, the Active Directory server will be used to authenticate the RAC user and obtain the user’s authorization information for the targeted RAC device. With minimal configuration, administrators can help optimize network security implementations by integrating the DRAC 4 remote management functionality into their existing Active Directory environments. 

Jon McGary is a senior software developer in the Dell OpenManage Remote Management Group. Prior to joining Dell, Jon was employed by Tandem Computers and specialized in remote management of fault-tolerant computers. He has a B.S. from Texas A&M University.

Bradley Bransom is a senior software developer in the Dell OpenManage Enabling Technologies Group. Prior to joining Dell, Bradley was employed by AMD, 3COM, and Texas Instruments. He has a B.S. from Texas A&M University.

FOR MORE INFORMATION

Active Directory in Windows 2000 Server:

<http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp>

Active Directory in Windows Server 2003:

<http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.msp>

^{3,4}For additional information about these certificates, refer to the *Dell Remote Access Controller 4 User's Guide* on the Systems Management documentation page of the Dell support Web site (<http://support.dell.com>).