Configuring iDRAC6 for Directory Services

Instructions for Setting Up iDRAC6 with Active Directory, Novell, Fedora, OpenDS and OpenLDAP Directory Services.

A Dell Technical White Paper

Dell | Product Group

Babu Chandrasekhar, Arulnambi Raju

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

March 2011

Contents

iDRAC6 and Directory Services

Integrated Dell Remote Access Controller 6 (iDRAC6) can use industry standard directory services for user authentication and privilege control. Active Directory (AD) is the most commonly-used directory service. In addition to AD, iDRAC6 supports generic LDAP-based directory services and has been validated with OpenLDAP, OpenDS, Novell eDirectory and Fedora Directory Services.

This white paper describes the needed setup in the directory services and in the iDRAC user interface.

The article also explains how iDRAC can be set up to use single sign-on with Active Directory user accounts.

In general, if an organization already has existing directory services set up, the only additional configuration needed is on the iDRAC6 side. However, if the organization wants to use AD Dell extended schema, then additional configuration is needed on the AD server side.

Configuring Active Directory Server

Details about the AD setup can be found in the iDRAC6 user guide at **http://support.dell.com/support/edocs/software/smdrac3/idrac/index.htm**

Microsoft documentation for deploying AD can be found at **www.microsoft.com/windowsserver2008/en/us/active-directory.aspx**

The prerequisites for directory service usage are the domain controller, Public Key Infrastructure (PKI), and Secure Socket Layer (SSL) on the domain controller. These services are part of Microsoft AD. Refer to the Microsoft documentation or the iDRAC6 user guide for details.

AD installation in Windows servers is done using an application called **dcpromo.exe**. In the dcpromo application, select the following options:

1. **Create a new domain in a new forrest**.
2. Enter a fully-qualified domain name (FQDN).
3. Choose **Windows 2008** as the **Forrest Functional Level**.
4. Provide folder locations to store the database and log files.
5. Once this installation is completed, Windows will restart for the settings to take effect.

After the AD setup, download the Certification Authority (CA) certificate. You will use this file during the iDRAC configuration. (Refer to Configuring iDRAC6 for Active Directory.)

For AD, you can configure iDRAC6 to use standard schema or Dell-customized extended schema. With extended schema, access control objects are maintained in the AD server.

Standard schema makes use of standard AD users and groups. No additional configuration is needed in AD server to use standard schema.

Refer to Installing Dell Extended Schema for AD for details.

Installing Dell Extended Schema for AD

Note: *You can skip this section if you plan to use only standard schema.*

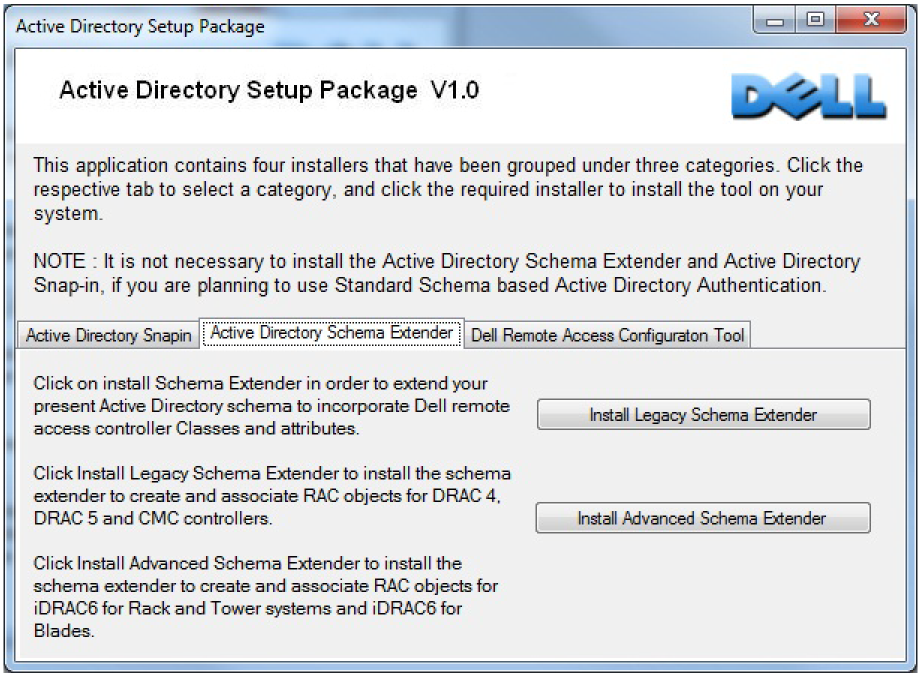
The Dell extended schema is available with the following Dell applications, 1) Dell OpenManage software and 2) Dell Remote Access Configuration Tool (RACT). Both of these applications can be obtained from http://support.dell.com. From the Dell Support website, select the PowerEdge server model number to search for available downloads. The needed applications are listed under the category **Systems Management** for Microsoft server operating systems.

Usage of OpenManage software is explained in the iDRAC6 user guide.

The RACT installation package contains the following applications:

- Active Directory Schema Extender
- Active Directory Snap-in
- Dell Remote Access Configuration Tool (RACT)

Figure 1. AD Schema Extender Installation from Dell Remote Access Configuration Tool


Active Directory Setup Package
Active Directory Setup Package V1.0
DELL
Active Directory Snapin
Active Directory Schema Extender
Dell Remote Access Configuraton Tool
Install Legacy Schema Extender
Install Advanced Schema Extender

This application contains four installers that have been grouped under three categories. Click the respective tab to select a category, and click the required installer to install the tool on your system.

NOTE : It is not necessary to install the Active Directory Schema Extender and Active Directory Snap-in, if you are planning to use Standard Schema based Active Directory Authentication.

Click on install Schema Extender in order to extend your present Active Directory schema to incorporate Dell remote access controller Classes and attributes.

Click Install Legacy Schema Extender to install the schema extender to create and associate RAC objects for DRAC 4, DRAC 5 and CMC controllers.

Click Install Advanced Schema Extender to install the schema extender to create and associate RAC objects for iDRAC6 for Rack and Tower systems and iDRAC6 for Blades.

The AD Schema Extender is used to install the Dell-provided extended schema on the AD server (select the **Install Advanced Schema Extender** option for iDRAC6). The schema extender tool will be used only once during schema installation and is not needed later for maintenance. Refer to the iDRAC6 user guide section *Using Active Directory Service* for details about extended schema (http://support.dell.com/support/edocs/software/smdrac3/idrac/index.htm).

Note: *Advanced users may extend the schema by using the LDIF script files provided with this utility.*

Creating Device and Association Objects

Note: *You can skip this section if you plan to use only the standard schema.*

You can use the AD snap-in tool with RACT or use the Dell MMC Console from the OpenManage DVD to create extended iDRAC objects in the AD server.

To create users using the extended schema, perform the following steps:

1. Create an iDRAC6 device object.
2. Create a privilege object.
3. Create an association object.
4. Add objects to the association object.
5. Associate users or user groups, privilege objects, and iDRAC6 devices to the association object.

Note that only one privilege object can be added to a single association object, but you can add multiple iDRAC devices and iDRAC users to the same association object. For multiple privileges, you must create separate association objects.

Refer to the iDRAC6 user guide section *Using Active Directory Service* for details on creating AD objects for extended schema.

Configuring Novell® eDirectory™

Novell documentation to configure eDirectory is available at http://www.novell.com/documentation/edir88/.

You can download the eDirectory installation packages from the Novell website. The following software versions were used during iDRAC 3.20 validation:

- Novell eDirectory v8.8 Service pack 5 (eDirectory_88SP5_Linux_x86_64.iso)
- Novell iManager v2.7.3 and plug-ins (eDir_88_iMan27_Plugins.npm, iman27_sp3.npm, iman273_FTF3.npm)

Administrators can install eDirectory by performing the following steps:

1. Mount the ISO image eDirectory_88SP5_Linux_x86_64.iso and run the **nds-install** application from the setup directory.
2. Select both option 1 to install Novell eDirectory and option 2 to install Administration Utilities.
3. Unzip **iMan_27_linux.tgz** and locate the directory for the Novell iManager plug-in files **eDir_88_iMan27_Plugins.npm**, **iman27_sp3.npm** and **iman273_FTF3.npm**.
4. Run **iManagerInstallLinux.bin** from **iManager/installs/linux** directory. Provide the path for iManager plug-ins when prompted.
5. Run the **/sbin/ldconfig** command to regenerate the library cache to resolve possible library errors.
6. Reboot the system, and then run the **ndsconfig** command to create a directory tree. The utility will ask for "server context" options. Provide the domain name and administrator credentials as required. Optionally, you can provide the "-i" option, which will create a new tree and ignore any existing one with the same name.

7. Create users and groups by logging into the iManager console by entering the eDirectory URL from a web browser, for example, `https://<IP Address>:8443/nps/`. Alternatively, an administrator can use standard LDAP command line utilities to add objects to the directory services. Refer to Creating LDAP Objects in Directory Services for details.
8. From the iManager console, create and assign a server certificate for the eDirectory Server.
9. Download the CA certificate and keep it for later uploading into iDRAC.

Configuring Fedora Directory Service

RedHat directory server 8.2 installation information is available at http://docs.redhat.com/docs/en-US/Red_Hat_Directory_Server/8.2/html/Administration_Guide/

Before installing Fedora DS, access the EPEL (Extra Packages for Enterprise Linux) repository. Use yum to install Fedora DS instead of picking up individual packages and installing one after another.

Following are the steps to install Fedora DS.

1. Download the repository packages **epel5.3.repo** and **rhel5.3.i386.repo** and install the Fedora DS and base packages using yum.

   ```
   # yum install 389-ds
   ```

2. Update NSS (network security service) by running the following command, if needed.

   ```
   # yum update nss
   ```

3. After Fedora DS has been installed, create a user and group ‘fds’ and then configure the DS server by running the following command:

   ```
   # /usr/sbin/setup-ds-admin.pl
   ```

4. After configuring the DS server, the directory services will automatically start.
5. Create users and groups by using the command **389-console**. Alternatively, an administrator can use standard LDAP command line utilities to add objects to the directory services. Refer to Creating LDAP Objects in Directory Services for details.
6. Create a folder for private CA files and copy the SSL configuration file to the private CA folder, for example,

   ```
   #mkdir /etc/pki/FedoraCA/
   ```

7. Create an SSL configuration file for the directory services by editing the **openssl.cnf** file.
8. Use the following command to generate the Certificate of Authority:

   ```
   #openssl req –new –x509 –days 3650 –extensions v3_ca –keyout
   private/cakey.pem –out cacert.pem –config /etc/pki/FedoraCA/openssl.cnf
   ```

9. Use the 389 console to create a certificate signing request (CSR) and generate a server certificate from CA server.
10. From the 389 console, upload the server certificate.

Configuring OpenDS

The latest OpenDS directory service installation information is available at https://docs.OpenDS.org/2.2/page/InstallationGuide

Since the OpenDS directory service is completely developed in Java, a Java Run time Environment must be installed prior to installing the OpenDS directory service.

OpenDS 2.2.0 (Zip file not JNLP file) is available at http://www.OpenDS.org/.

To install OpenDS, perform the following steps:

1. Copy the OpenDS installation file (**OpenDS-2.2.0.zip**) to a folder where you want to install OpenDS. Unzip the installation file and start installation. In the following example, we are installing OpenDS under the **Home** folder.
   ```
   # cp OpenDS-2.2.0.zip /home
   # cd /home
   # unzip OpenDS-2.2.0.zip
   # cd OpenDS-2.2.0
   # ./setup
   ```
2. On the **Welcome** screen, click **Next**.
3. Specify the OpenDS server FQDN (Hostname.domainname) for the **hostname** field. (`OpenDS-Server.example.com`, in this example.)
4. Keep the default settings for **LDAP Listener Port**, **Administrator Connection Port**, and **Root User DN**.
5. Enable LDAP secure access by clicking on **Configure…**
   a. Click the **Enable SSL on Port** check box.
   b. Use default port number 636.
   c. Use the default for **Generate Self-Signed Certificate (recommended for testing only, later this has to be removed with valid CA certificate)**.
   d. Click **OK**.
6. Specify the appropriate OpenDS administrator password for Directory Manager.
   Note: *This Directory Manager will be used to add objects to the OpenDS server. Therefore, this password is required while adding and modifying user and group objects using standard LDAP client tools.*
7. On the **Topology Options** page, use the default of **This will be a standalone server**.
8. On the **Directory Data** page, customize the following and click **Next**:
   Directory Base DN: dc=example,dc=com
9. On the **Review** page, click **Finish**.
10. Check the **Progress** page for any error message.
11. On the **Finished** page, check for any messages, then click **Close**.
    NOTE: You can modify the OpenDS configuration at any time by launching the control panel from bin folder of the OpenDS installation folder.
12. Key manager providers are ultimately responsible for providing access to the certificate that should be used by the directory server when performing SSL or StartTLS negotiation. Use the **keytool** utility to generate a certificate and certificate signing request. Use the openssl tool to sign the certificate using the CA certificate. Use the **keytool** utility to import the CA certificate and the server certificate into the keystore files. For more information on enabling a secure connection, refer to: https://docs.OpenDS.org/2.2/page/ConfiguringSecurity

After the directory services installation is complete, you can add LDAP objects for iDRAC6 users and groups by using standard LDAP command line utilities. Refer to Creating LDAP Objects in Directory Services for details.

Configuring OpenLDAP

The OpenLDAP directory service installation information is available at http://www.OpenLDAP.org/software/download/

To install and configure OpenLDAP, perform the following steps:

1. Install the following packages on your LDAP server machine:
   - `openldap`
   - `openldap-clients`
   - `openldap-devel`
   - `nss_ldap`
   - `openldap-servers`
2. The LDAP server's daemon is named **slapd** and its configuration file is named **/etc/openldap/slapd.conf**.
   a. A database of the default type `bdb` using the domain suffix “example.com” made up of domain components (DCs) `example` and `com`.
   b. The LDAP admin user with a common name (CN), or nickname, of Manager who, as expected, is part of the `example` and `com` DCs. This user can read and write everything to the LDAP database.
   c. The encrypted version of the LDAP admin password (use the **slappasswd** tool to generate an encrypted password) as well as the location of the LDAP database.

   The configuration file syntax to do this is:

```
database        bdb

suffix          "dc=example,dc=com"

rootdn          "cn=Manager,dc=example,dc=com"

rootpw          {SSHA}v4qLq/qy01w9my60LLX9BvfNUrRhOjQZ

directory       /var/lib/ldap/openldap.com
```

3. To enable SSL on the LDAP server, install a CA authority and sign the server certificate with this CA. Use the following steps to enable SSL:
   a. Configure TLS parameters on the ldap configuration file.
      Edit the **/etc/OpenLDAP/slapd.conf** file and configure the TLS parameters as follows:

```
TLSCACertificateFile /etc/pki/CA/cacert.pem

TLSCertificateFile /etc/pki/openLdapCA/openldap_server_cert.pem

TLSCertificateKeyFile /etc/pki/openLdapCA/private/openldap_pkey.pem
```

   b. Restart the LDAP Service:

```
service ldap stop

service ldap start
```

After the directory services installation is complete, LDAP objects for iDRAC6 users and groups can be added by using standard LDAP command line utilities. Refer to Creating LDAP Objects in Directory Services for details.

Creating LDAP Objects in Directory Services

Standard LDAP commands require user objects to be available in the LDIF format. This process is common for all directory services including AD (if standard schema is used). Use the **ldapadd** command to add the object to the directory's database.

The LDAP administrator username and password can be used to add or modify an object on the LDAP server. (In the following example, admin user: "cn=Manager,dc=example,dc=com" password: "password" are used).

Creating an Organizational Unit (OU) on the LDAP Server

Create a file named **createOU.ldif** with the following content for creating an organizational unit called **iDRAC** on the LDAP server machine:

```
dn: ou=iDRAC,dc=example,dc=com

objectclass: organizationalunit

ou: iDRAC
```

Run the following command to create an organization unit on the LDAP server using this .ldif file:

```
# ldapadd -x -D "cn=Manager,dc=example,dc=com" -W password -f createOU.ldif
```

Creating a User on the LDAP Server

Create a file named **createUser.ldif** with the following content for creating a user called **iDracAdmin** on the LDAP server machine.

```
dn: uid=iDracAdmin,ou=iDRAC,dc=example,dc=com

objectClass: person

objectClass: inetorgperson

objectClass: organizationalperson

cn: iDracAdmin

sn: surname

description: This is a generic description

uid: iDracAdmin

userPassword: pass
```

Run the following command to create this user on the LDAP server.

```
# ldapadd -x -D "cn=Manager,dc=example,dc=com" -W password -f createUser.ldif
```

Creating a Group with a Member

Create a file named **createGroup.ldif** with the following content for creating a group called **iDracAdminGroup**.

```
dn: cn=iDracAdminGroup,ou=iDRAC,dc=example,dc=com

objectclass: groupOfUniqueNames

cn: iDracAdminGroup

uniqueMember: uid=iDracAdmin,ou=iDRAC,dc=example,dc=com
```

Run the following command to create a group on LDAP server.

```
#ldapadd -x -D "cn=Manager,dc=example,dc=com" -W password -f createGroup.ldif
```

Note: *To add more members (users) to this group, use the* ***ldapmodify*** *tool.*

Configuring iDRAC6 for Active Directory

There are three primary user interfaces that an administrator could use to configure Active Directory: iDRAC web GUI, RACADM command line, and Dell Remote Access Configuration Tool (RACT).

The options to configure AD with the web GUI are:

1. Login to iDRAC with administrator privilege.
2. Navigate to **System -> Remote Access -> Network/Security -> Directory Service**.

3. Select the **Microsoft Active Directory** check box and click **Apply**.
4. Options to upload keytab, test settings, and configure AD are available in this page. Click **Configure Active Directory**.
5. This will bring up step 1 of the AD configuration. Select the certificate validation option (optional), and if certificate validation is selected, upload the CA certificate to iDRAC6.
6. On the next page (step 2), select **Enable Active Directory**. Fill in the remaining AD configuration options as needed, and click **Next**.
7. On step 3, select extended or standard schema.
8. If standard schema is used, configure the role groups and global catalog server options in the subsequent pages.
9. If extended schema is used, provide the iDRAC6 name and the iDRAC6 domain name.

After completing this setup, go to **Test Settings** in step 4 to verify the settings with the AD server.

Configuring iDRAC for Generic Directory Services

To configure iDRAC6 for a basic LDAP login, perform the following steps:

1. Log in to iDRAC with administrator privilege.
2. Navigate to **System -> Remote Access -> Network/Security -> Directory Service**.
3. Select the **Generic LDAP Directory Service** check box and click **Apply**.
4. On the **Generic LDAP Configuration and Management** page, click **Configure Generic LDAP**.
5. Select the **Enable Certificate Validation** check box and upload the valid CA certificate which is used to sign the respective LDAP server certificate (The certificate validation is optional. IDRAC will be functional without enabling this option). Click **Next**.
6. Specify the following settings on this page and click **Next**.

Attribute	Value
Enable Generic LDAP	***Checked***
Use Distinguished Name to Search Group Membership	***Checked***
LDAP Server Address	***Server IP or FQDN***[(Note 1)]. To specify multiple, redundant LDAP servers that serve the same domain, provide the list of all servers separated by a comma.
LDAP Server Port	***636*** (Default secure port)

Attribute	Value	
Bind DN	***cn=Manager,dc=example,dc=com***	*Optional, but required if anonymous bind is not supported by the directory server*. Specify the distinguished name and password of a user used to bind to the server when searching for the login user's DN. If not provided, an anonymous bind will be used
Bind Password	***Password***	
Base DN to Search	***dc=example,dc=com*** The DN of the branch of the directory where all searches should start from.	
Attribute of User Login	`Uid` *Optional*. This is the attribute to search for. If not configured, the default is to use `uid`. It is recommended to be unique within the chosen baseDN, otherwise a search filter must be configured to ensure the uniqueness of the login user. If the user DN cannot be uniquely identified by search the combination of attribute and search filter, the login wil fail with an error.	
Attribute of Group Membership	`Uniquemember` *Optional.* Specify which LDAP attribute is used to check for group membership. This should be an attribute of the group class. If not specified, then firmware uses the member and uniquemember attributes.	
Search Filter	`(objectClass=*)` *Optional*. A valid LDAP search filter. This is used if the user attribute cannot uniquely identify the login user within the chosen baseDN. If not provided, this defaults to (objectClass=*), which will search for all objects in the tree. The **Search Filter** only applies to userDN search, not the group membership search(Note2).	

7. Click **Role Group1** (At least one role group must be configured for user authorization).
8. Specify "Group DN" and "Role Group Privilege Level" and then click **Apply**.

Attribute	Value
Group DN	`cn=iDracAdminGroup,ou=iDRAC,dc=example,dc=com` Specify the distinguished name (DN) of LDAP groups whose members are allowed access to the device.
Role Group Privilege Level	`Administrator` Specify the privileges associated with each configured group.

9. Click **Finish**.

Note 1: *FQDN or IP must match the server certificate's common name if certificate validation is enabled.*

Note 2: *The user-configured search filter will be applied as it is without any further modification during the LDAP directory search.*

10. To test the LDAP configuration, perform the following steps:
    a) On the **Generic LDAP Configuration and Management** page, click **Test Settings**.
    b) Specify Username as `iDracAdmin` and Password as `pass` and click **Start Test**.
    c) Log out from the iDRAC GUI and log back in with username `iDracAdmin` and password `pass`.

Configuring iDRAC to Enable Single Sign-on

The single sign-on feature is available only if the iDRAC is configured for AD authentication.

To enable single sign-on, navigate to **iDRAC Settings->Network/Security->Directory Services** and select **Microsoft Active Directory**. Click **Apply**. On the next page, there is an option to upload the keytab file. Refer to the user guide for information about the keytab file. The **single sign-on** check box is available at step 2 of the **Configure Active Directory** pages.

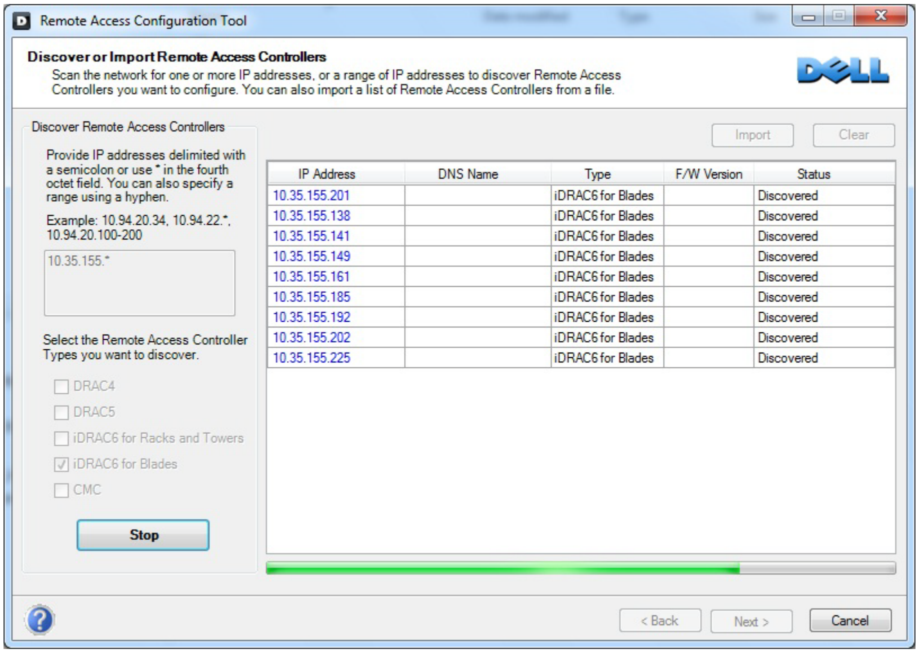
The single sign-on feature is only available with workstations using the Internet Explorer browser. This feature uses the same ActiveX plug-in which is used for smart card logins. On certain Windows versions, the ActiveX plug-in requires the installation of Microsoft Visual C++ 2005 Redistributable package.

Configuring Multiple DRACs for AD with the Dell RAC Tool

The RACT utility allows one-to-many configuration of DRAC AD settings to multiple DRAC's at the same time. It allows configuring different generations of DRACs including DRAC4, DRAC5, iDRAC and iDRAC6. It starts with discovering all the DRACs in the selected network and then checks the logon credentials, followed by options to do a firmware update and directory service deployment (refer to screenshots).

Discovery is performed by the user providing a range of DRAC IP addresses using the available wildcard selection options. You can then select the login credentials to verify authentication with the selected DRACs. The next screen allows you to identify the already-configured schema options or to select a new schema option to configure. Follow through these GUI options to provide the required AD settings for all the selected DRACs. The following are the screenshots from RACT utility.

Figure 2. DRAC Discovery Page in the RACT Utility



Remote Access Configuration Tool

Discover or Import Remote Access Controllers

Scan the network for one or more IP addresses, or a range of IP addresses to discover Remote Access Controllers you want to configure. You can also import a list of Remote Access Controllers from a file.

Discover Remote Access Controllers

Provide IP addresses delimited with a semicolon or use * in the fourth octet field. You can also specify a range using a hyphen.

Example: 10.94.20.34, 10.94.22.*, 10.94.20.100-200

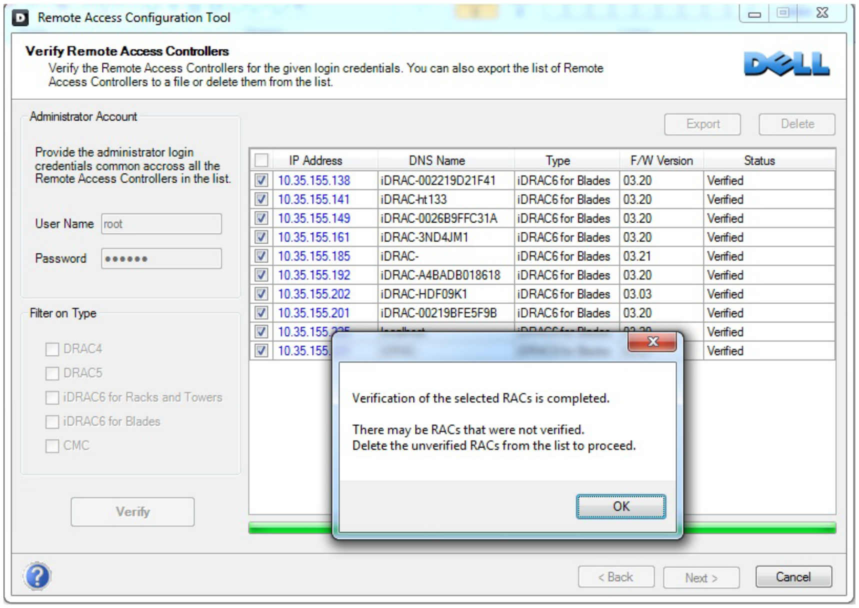
10.35.155.*

Select the Remote Access Controller Types you want to discover.

- □ DRAC4
- □ DRAC5
- □ iDRAC6 for Racks and Towers
- ☑ iDRAC6 for Blades
- □ CMC

IP Address	DNS Name	Type	F/W Version	Status
10.35.155.201		iDRAC6 for Blades		Discovered
10.35.155.138		iDRAC6 for Blades		Discovered
10.35.155.141		iDRAC6 for Blades		Discovered
10.35.155.149		iDRAC6 for Blades		Discovered
10.35.155.161		iDRAC6 for Blades		Discovered
10.35.155.185		iDRAC6 for Blades		Discovered
10.35.155.192		iDRAC6 for Blades		Discovered
10.35.155.202		iDRAC6 for Blades		Discovered
10.35.155.225		iDRAC6 for Blades		Discovered

Figure 3. DRACT User Interface, After Discovering the DRACs in the Network.



Remote Access Configuration Tool

Verify Remote Access Controllers

Verify the Remote Access Controllers for the given login credentials. You can also export the list of Remote Access Controllers to a file or delete them from the list.

Administrator Account

Provide the administrator login credentials common accross all the Remote Access Controllers in the list.

User Name: root

Password: ●●●●●●

Filter on Type

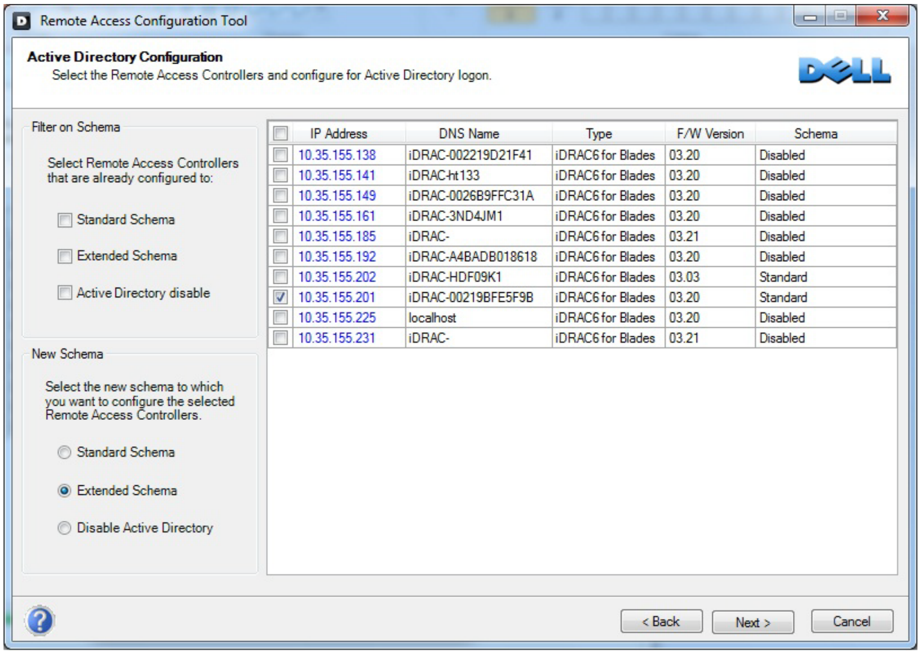
- □ DRAC4
- □ DRAC5
- □ iDRAC6 for Racks and Towers
- □ iDRAC6 for Blades
- □ CMC

□	IP Address	DNS Name	Type	F/W Version	Status
☑	10.35.155.138	iDRAC-002219D21F41	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.141	iDRAC-ht133	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.149	iDRAC-0026B9FFC31A	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.161	iDRAC-3ND4JM1	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.185	iDRAC-	iDRAC6 for Blades	03.21	Verified
☑	10.35.155.192	iDRAC-A4BADB018618	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.202	iDRAC-HDF09K1	iDRAC6 for Blades	03.03	Verified
☑	10.35.155.201	iDRAC-00219BFE5F9B	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.225	localhost	iDRAC6 for Blades	03.20	Verified
☑	10.35.155.[illegible]	[illegible]	[illegible]	[illegible]	Verified

Verification of the selected RACs is completed.

There may be RACs that were not verified.
Delete the unverified RACs from the list to proceed.

Figure 4. Schema Selection Option in RACT



Active Directory Configuration

Select the Remote Access Controllers and configure for Active Directory logon.

Filter on Schema

Select Remote Access Controllers that are already configured to:

□ Standard Schema

□ Extended Schema

□ Active Directory disable

New Schema

Select the new schema to which you want to configure the selected Remote Access Controllers.

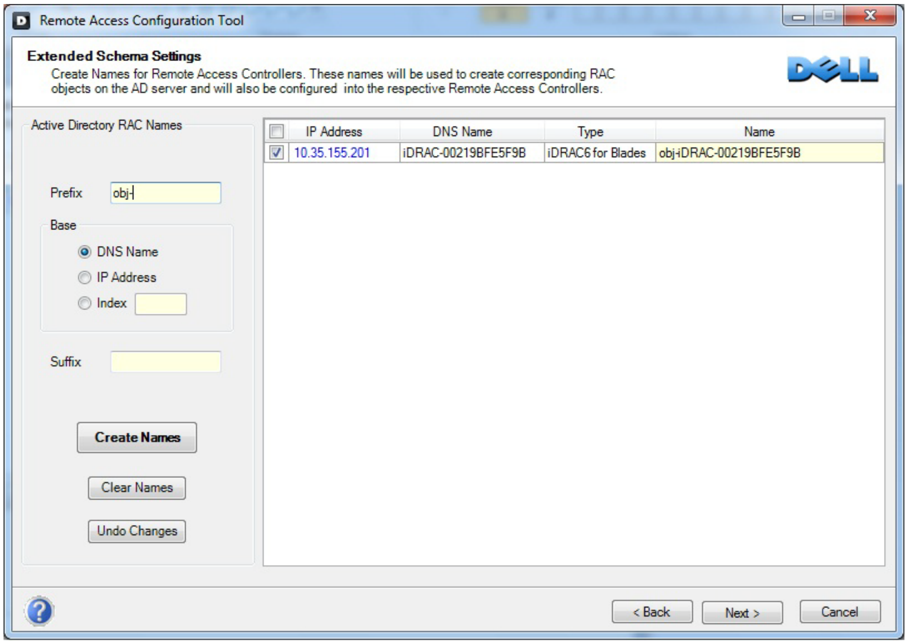
○ Standard Schema

● Extended Schema

○ Disable Active Directory

□	IP Address	DNS Name	Type	F/W Version	Schema
□	10.35.155.138	iDRAC-002219D21F41	iDRAC6 for Blades	03.20	Disabled
□	10.35.155.141	iDRAC-ht133	iDRAC6 for Blades	03.20	Disabled
□	10.35.155.149	iDRAC-0026B9FFC31A	iDRAC6 for Blades	03.20	Disabled
□	10.35.155.161	iDRAC-3ND4JM1	iDRAC6 for Blades	03.20	Disabled
□	10.35.155.185	iDRAC-	iDRAC6 for Blades	03.21	Disabled
□	10.35.155.192	iDRAC-A4BADB018618	iDRAC6 for Blades	03.20	Disabled
□	10.35.155.202	iDRAC-HDF09K1	iDRAC6 for Blades	03.03	Standard
☑	10.35.155.201	iDRAC-00219BFE5F9B	iDRAC6 for Blades	03.20	Standard
□	10.35.155.225	localhost	iDRAC6 for Blades	03.20	Disabled
□	10.35.155.231	iDRAC-	iDRAC6 for Blades	03.21	Disabled

Figure 5. iDRAC AD Configuration Using RACT



Extended Schema Settings

Create Names for Remote Access Controllers. These names will be used to create corresponding RAC objects on the AD server and will also be configured into the respective Remote Access Controllers.

Active Directory RAC Names

Prefix: obj-

Base

● DNS Name

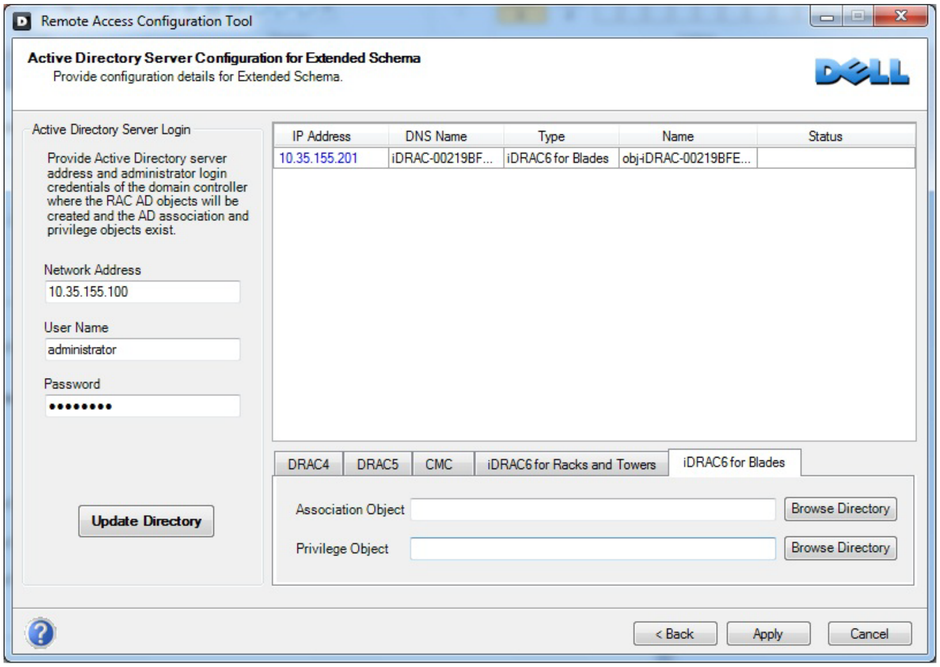
○ IP Address

○ Index

Suffix

□	IP Address	DNS Name	Type	Name
☑	10.35.155.201	iDRAC-00219BFE5F9B	iDRAC6 for Blades	obj-iDRAC-00219BFE5F9B

Figure 6. iDRAC AD Configuration Using RACT



Remote Access Configuration Tool

Active Directory Server Configuration for Extended Schema

Provide configuration details for Extended Schema.

Active Directory Server Login

Provide Active Directory server address and administrator login credentials of the domain controller where the RAC AD objects will be created and the AD association and privilege objects exist.

Network Address: 10.35.155.100

User Name: administrator

Password: ••••••••

IP Address	DNS Name	Type	Name	Status
10.35.155.201	iDRAC-00219BF...	iDRAC6 for Blades	obj-iDRAC-00219BFE...	

Association Object:

Privilege Object:

Summary

This white paper provides a quick overview and instructions on installing and configuring the supported directory services for iDRAC6. The steps are the same for Modular and Monolithic Dell servers using iDRAC6 Enterprise version, with slight variations in the iDRAC web GUI layout (based on firmware versions). The examples and DRAC web page links referenced in this article are for Modular iDRAC6 firmware version 3.20. For specific details about a particular directory service, always refer to the documentation from the directory services provider's website, links to which are provided in each subsection. iDRAC6-specific details, including command line options and frequently asked questions, are available in the iDRAC6 user guide, which is available at **http://support.dell.com/support/edocs/software/smdrac3/idrac/index.htm**