DELL™ Remote Access Configuration Tool

A Dell Technical White Paper

Dell | Product Group

Austin Cherian

Table of Contents

Executive Summary

This white paper provides an overview of the features and benefits of using the Dell Remote Access Configuration tool (DRACT) as a one-to-many configuration deployment application for enterprise remote access controllers (RACs). This paper also serves as a guide for administrators who would want to deploy configuration baselines across a large number RACs that vary in generation (type) and current configuration.

Introduction

There are always costs for provisioning and maintaining enterprise remote access controllers (RACs). For IT administrators who need to maintain system uptime using RACs, this would mean constantly monitoring current device configurations to make sure they are up-to-date with the latest configuration baseline, ensuring accessibility to these devices during disaster recovery scenarios and business continuity.

As the maintenance task becomes more complex and the number of devices to manage increases, IT administrators typically resort to customized scripts to get the job done. These scripts, although considered a one-time effort, have costs in maintenance as product lines change and new features are added to older products.

The Dell Remote Access Configuration Tool (DRACT) alleviates the system administrator's challenges by automating some of the common repetitive tasks that would otherwise require scripting or individual configuration. DRACT provides a central console to discover and configure RACs for all systems on your network. The first version of the tool automates the Active Directory™ (AD) authentication configuration across a selected set of RACs. The table below summarizes the DRACT key features:

Provides a convenient and simple-to-use GUI to apply common configuration baselines across multiple RACs of different generations, thus avoiding cumbersome one-to-one maintenance tasks; ensures business continuity through uninterrupted access to RACs.
Discover RAC IP addresses on the network – allows you to scan your network and discover the IP addresses of all the RACs regardless of their type / generation. You can also export the discovered IPs to a file.
Update firmware for selected RAC IP addresses – can update the firmware on multiple RACs at the same time, minimizing the cost of keeping RACs up to date. DRACT allows for both host-based and TFTP firmware updates.
Configure standard- or extended-schema based AD settings – allows you to apply the same standard or extended AD configuration across multiple RACs to ensure successful AD authentication.

Create RAC objects on the AD server for extended schema-based AD login – remotely configures the AD server by creating and associating DRAC objects and avoiding manual object creation and enables ESAD-based AD authentication.

Migrate from one AD schema to another – can be used as a schema migration tool to migrate multiple RACs that are using one AD schema type to another AD schema type.

Supported RACs and Operating Systems

DRACT supports the following RAC types that support RACADM commands:

- Dell Remote Access Controller 4 (DRAC 4)
- Dell Remote Access Controller 5 (DRAC 5)
- Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for blade servers
- Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for rack and tower servers
- Chassis Management Controller (CMC)

NOTE: DRACT does not support iDRAC6 installed on 10th generation PowerEdge™ systems.

You can install DRACT only on 32-bit Microsoft® Windows® operating systems like Windows XP, Windows Vista®, Windows 7, and Windows Server® 2008.

Installing DRACT

There are a few DRACT install prerequisites:

- Install the .Net Framework version 2.0 SP1 (or later)
- A user account with installation and execution privileges.

DRACT is available as a Windows installer package (.msi), as well as part of the AD setup package (ADSP), that can be downloaded from the Dell Support Website at **support.dell.com.**

When using the .msi Installer, standard msi installation procedures should be followed to install DRACT using both the msi GUI as well as the CLI installation methods. To install DRACT using the AD setup package see the ADSP product ReadMe file available on the Dell Support Website at **support.dell.com/manuals**.

Discovering RAC IP Addresses

You can use DRACT to discover the RAC IP addresses for the different RAC types on your network. You can either specify an IP address to be discovered, or specify an IP range. DRACT also provides the choice to only discover particular RAC types/generations by selecting the RAC types to be discovered. Once the RAC IPs are displayed, you can click on a RAC IP address

link to launch the Web-based GUI. You can also sort the entries in ascending or descending order for each column, by clicking on the column heading. In this way DRACT proves to be an invaluable tool to keep tabs on the enterprise RACs, and could be used in a variety of scenarios to check for controller accessibility.

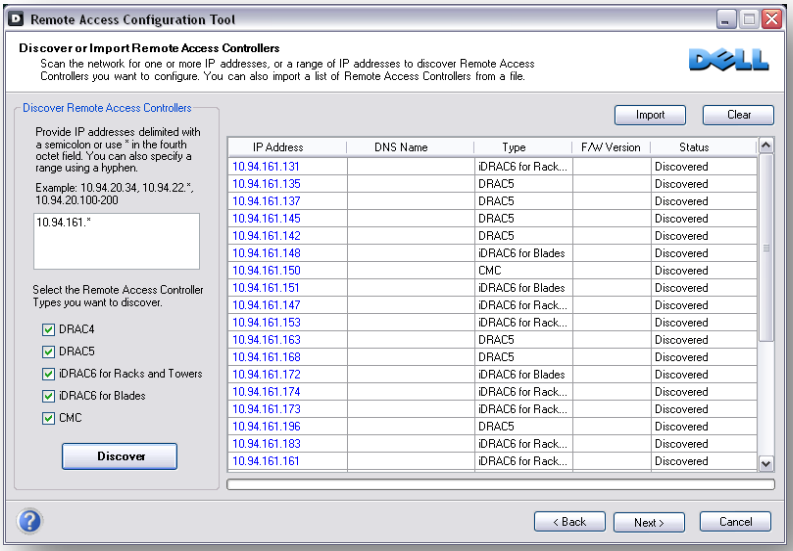

Figure 1 – DRAC IP Discovery

DRACT also supports importing a CSV file containing the RAC IP addresses that have been discovered, so as to eliminate the discovery process if it has already completed or if it is prohibited in your environment. In addition, the discovery process could compliment the imported list RAC IPs in that DRACT will append the imported list of RAC IP addresses to the ones it discovers.

Since changing RAC configuration information requires authentication, user credentials that have the RAC configuration privilege are required by DRACT to ensure that it can configure the RAC. To check if DRACT will be able to use a specified user credential, it has an additional verification step for the supplied credential against the RACs selected for configuration.

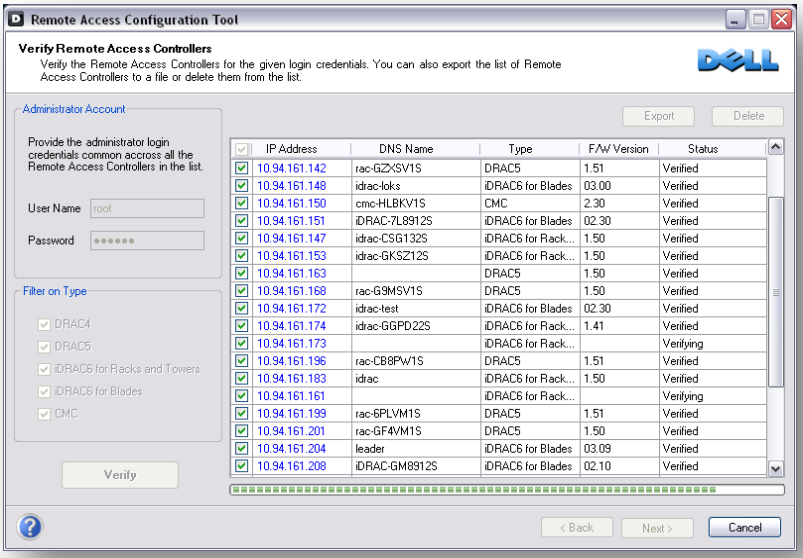

Figure 2 – DRAC IP Verification

The user can provide credentials that are either local RAC credentials or AD credentials. These credentials are then verified for the selected RACs when the user clicks Verify. It is assumed that the credentials provided are common across all the RACs selected; only verified RACs will be considered for further configuration. For a single configuration session, only one set of credentials will be utilized. If there are RAC IPs in the list that have different user credentials, DRACT will have to be run again with the RAC-specific credentials to configure them.

On the verification screen the user can also export the IPs and other related information, such as DNS name and RAC type, to a CSV file by clicking **Export**. The CSV file can then later be used to eliminate rerunning the discovery process.

During the verification process, DRACT collects data from the RACs such as the current DNS name, the current firmware version, the type of schema that is configured, and so on; this information is required to complete RAC configuration.

Update Firmware

It is recommended that users have the latest firmware image installed on their RACs before applying configuration settings. DRACT can be used to perform firmware updates on multiple RACs using one of the two RAC firmware update mechanisms: local image firmware update or TFTP image based firmware update.

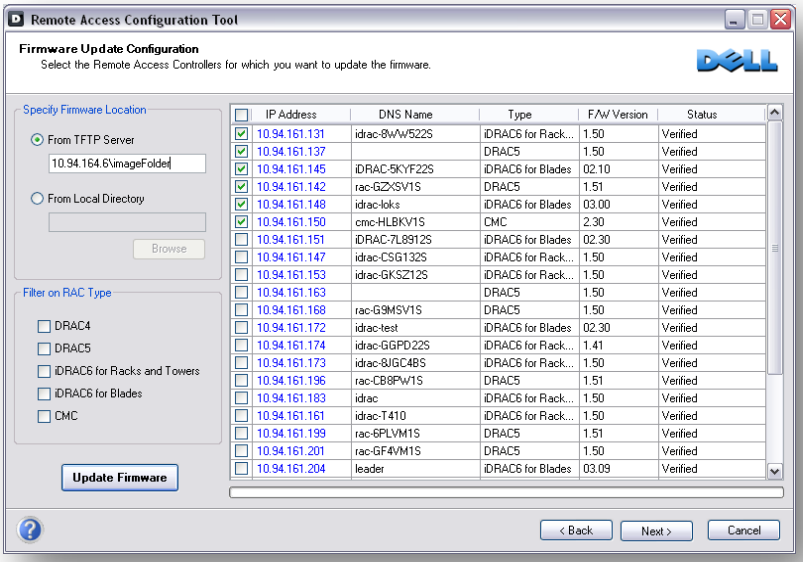

Figure 3 – DRACT Firmware Update

The local image firmware update allows for a remote firmware update when the firmware image file is located on a local host where the DRACT application is running. Simply browse to the folder that contains all of the firmware images for the different RACs; DRACT will automatically apply the correct firmware image to a particular controller depending on its type. The TFTP mechanism of remote firmware update involves having all the firmware images on a TFTP server. If the TFTP server IP address is provided to DRACT, it can direct specific controllers to download the image from the TFTP server and perform a self update.

Configure AD Settings

One of the principal DRACT 1.0 features is to configure multiple RACs to enable AD login across all the RACs. Using DRACT, the user should be able to configure RACs to have either extended or standard-schema based AD login. DRACT automatically applies the proper device-dependant schema settings based on the schema selected and the RAC type.

In the case of extended-schema AD configuration, DRACT also completes the AD configuration by configuring the AD servers with the new DRAC objects that are required for extended-schema authentication. The list below contains the different AD schema operations that DRACT allows:

Configure RACs to use AD standard schema for AD authentication.
Configure RACs to use AD extended schema for AD authentication.
Disable AD standard or extended schema for RACs. For more information, see "Disabling AD Standard or Extended Schema for RACs."
Migrate from standard schema to extended schema and vice versa.

DRACT can recognize the presence of the AD schema configuration on each of the RACs after completion of the verification process described above. You can select all the RACs that have a particular schema by selecting one, or a combination of, filter options under the **Filter on Schema** section. You can then select the new schema by selecting the desired options under the **New Schema** section. You can also disable AD for selected RACs by selecting the **Disable Active Directory** option under the New **Schema** section.

Figure 4 – AD Schema Configuration

Common Configuration Settings

DRACT's AD configuration pages are similar to the AD configuration pages found on a RAC's Web interface. Figure 5 below shows the DRACT common settings page that maps to the RAC's common settings page on the Web interface. From this page you could upload the AD servers CA SSL certificate, and provide other AD configuration information that is common for standard, as well as extended, schema AD configuration.

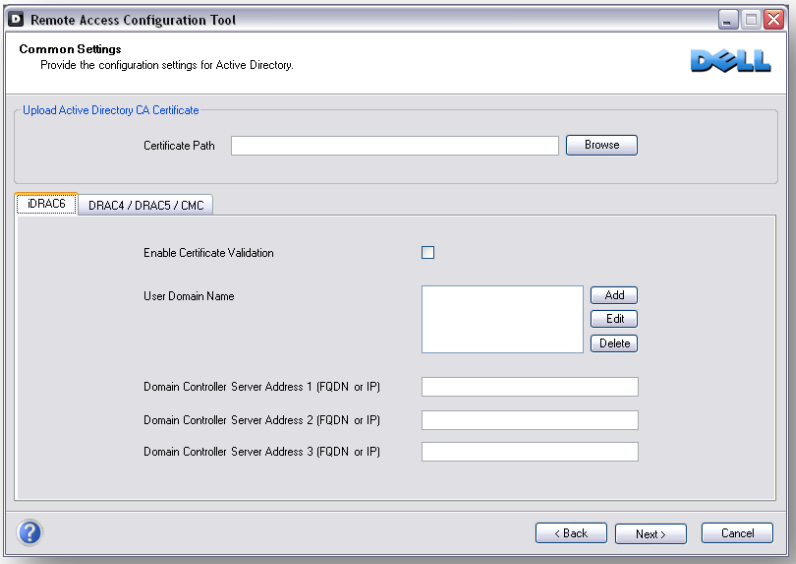

Figure 5 – Active Directory Common Configuration Settings

Configuring RACs to use AD Standard Schema

In regard to standard-schema AD configuration, a standard group object is used as an AD server role group. A user who has RAC access is a member of the role group. To provide access to a specific RAC for a certain user, the role group name and its' domain name must be configured on the specific RAC.

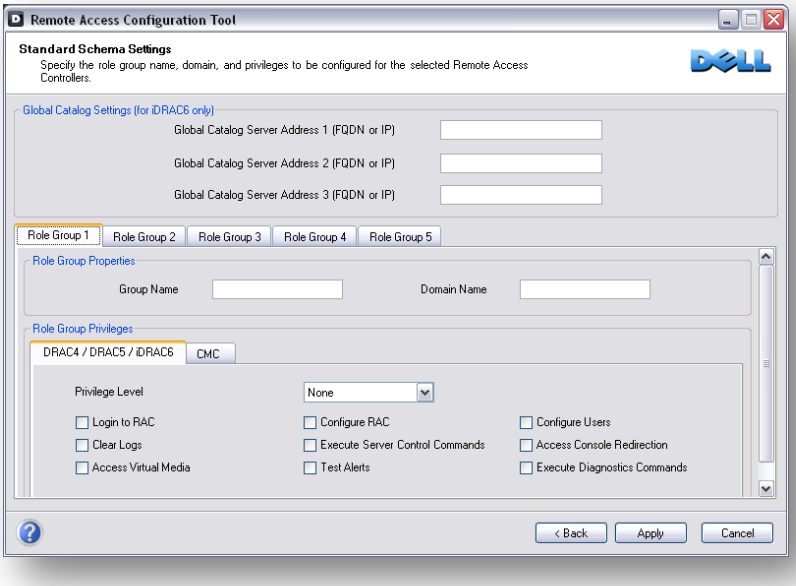

Figure 6 – Active Directory Standard Schema Configuration

You must specify an existing role group name that is available on the AD server. The role and the privilege level is defined on each RAC. You can configure up to five role groups, and associate a role and a set of privilege levels with each of the five role groups. For iDRAC6 it is necessary to specify the global catalog server address (GCSA) as part of the standard-schema configuration and you can specify up to three GCSAs. After entering the relevant information and clicking **Apply,** DRACT will start RAC configuration. DRACT will apply the correct RAC configuration settings depending on the RAC type; for example, DRACT configures the GCSAs only for iDRAC6 RACs and not for the other RAC types.

Creating RAC Objects and Configuring RACs to use AD Extended Schema

Using the Dell extended-schema AD architecture, you can extend the AD schema to include Dell specific association, device, and privilege objects. The association object is used to link together the users or groups with a specific set of privileges to one or more RAC device objects. For more information on Dell extended schema AD objects, see the extended schema AD section of the User Guides listed in the “Where to go for more information” section of this document.

DRACT has the capability to connect to an AD server and create the RAC device objects for each individual DRAC. The extended schema settings screen shown in Figure 7 allows users to construct or specify the RAC device names that will have a corresponding RAC device object created on the AD server. The RAC device name is also configured on the corresponding RAC, as part of the extended schema configuration settings.

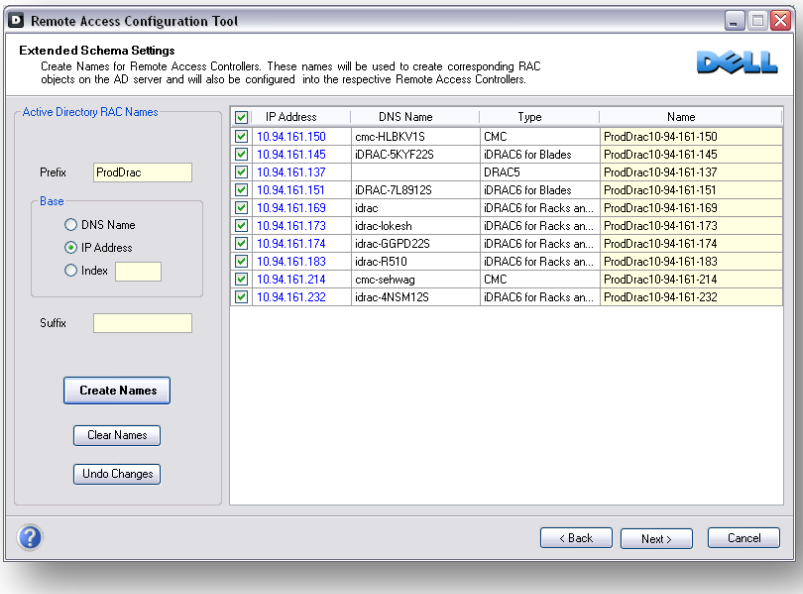

Figure 7 – AD Extended Schema DRAC Objects Creation

You need to specify the AD server login credentials in order for DRACT to:

Connect to the AD server
Create the RAC device objects
Associate the RAC device objects and the corresponding privilege objects to a specified association object

DRACT also allows you to browse to a connected AD server, and select the association and privilege objects that are needed to complete the association task.

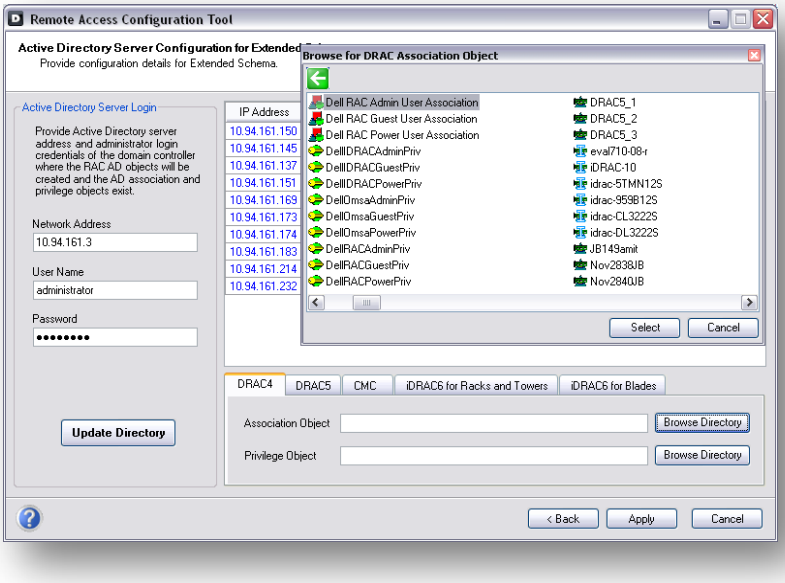

Figure 8 – AD Extended Schema Configuration and AD Server Browser

You can have multiple association objects, and each association object can be linked to as many users, groups of users, or RAC device objects as required. For more information on the Dell extended schema AD objects see the extended-schema AD section of the User Guides listed in the “Where to go for more information” section of this document.

AD Schema Migration

There are often maintenance scenarios where it will be required to configure all, or a subset of, RACs to migrate from using standard-schema to extended-schema based AD login and vice versa. DRACT can be used to migrate selected RACs from using standard schema to using extended schema for AD login, or vice versa, in a convenient and efficient manner.

On the DRACT AD schema selection page shown in Figure 4, you can select all or a subset of DRACs that match the selection criteria by entering a combination of options under the **Filter on Schema** group; DRACT will select the RACs from the list that match the selection criteria. You can then simply select the schema to be applied by entering the appropriate option under the **New Schema** group, and clicking **Next** to provide details for the new schema. DRACT applies the new schema settings on the selected / filtered list of RACs.

In this manner, you can migrate a list of DRAC's from using one schema type to using another in a few steps; DRACT applies the applicable schema settings based on the DRAC type.

Context Sensitive Help

DRACT provides context sensitive help information on all its pages. To access the help content, click the question mark symbol located on the bottom right corner of the page and the help content specific to that page will appear in a new window.

Where to go for more information

For more information on DRACT, and information on configuration of specific controller types, you can reference the following guides on the Dell Support Website at **support.dell.com/manuals**.

• The *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* provides information about configuring and using an iDRAC6 for blade servers to remotely manage and monitor your system and its' shared resources through a network.

• The *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* provides complete information about configuring and using an iDRAC6 for tower and rack servers to remotely manage and monitor your system and its' shared resources through a network.

• The *Dell Remote Access Controller 5 User's Guide* provides complete information about installing and configuring a DRAC 5 controller and using DRAC 5 to remotely access an inoperable system.

• The *Dell Remote Access Controller 4 User's Guide* provides complete information about installing and configuring a DRAC 4 controller and using DRAC 4 to remotely access an inoperable system.

• The *Dell Chassis Management Controller (CMC) User's Guide* provides information about using the controller that manages all modules in the chassis containing your PowerEdge server.

Conclusion

DRACT is an application that can be used to remotely automate common tasks to ensure uninterrupted access to a RAC during disaster recovery scenarios, and ensure system uptime.

Most importantly, the tool provides a one-to-many push point to perform common repetitive maintenance operations on a multitude of RACs that vary in generation and current configuration baselines. The first version of this tool can be used also to update RAC firmware and perform AD configuration. This makes it a useful tool for large enterprise customers that typically have hundreds or thousands of servers and RACs.