Active Directory Configuration Setup on 12G Servers Using Lifecycle Controller

Zhan Liu

This document 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.

January 2013| Rev 1.0

Contents

Introduction

Active directory (AD) simplifies the process of user account and privilege management. With AD setup, the credentials of AD will be used for all iDRACs, and it is not necessary to configure each credential for every iDRAC. These credentials can be used for iDRAC GUI, SSH login, and for running both WSMAN and RACADM commands from the CLI.

Integrated Dell Remote Access Controller v7 (iDRAC7) with Lifecycle Controller (LC) provides the capability to programmatically and remotely configure Active Directory (AD) for Dell PowerEdge 12th generation servers.

This Whitepaper [1] describes the tasks to manually set up the AD and give other useful information about setting up AD. This paper will not repeat those contents, but concentrate on remotely setting up AD with LC.

iDRACCard profile [3], provides the explanation about the iDRAC card attributes, including all AD–related attributes. For more information about the correct attributes of WSMAN commands, see iDRACCard profile [3],

This document describes the AD workflow by using the remote API that is exposed by the LC capability of Dell PowerEdge 12th generation servers. The goal of this paper is to provide clear steps to set up Microsoft AD on Dell 12G servers by using WS-MAN commands.

This document assumes that the customers are familiar with AD, Domain Controller, IP, DNS, DHCP, and Certification Service for Windows and AD manually set up for iDRACs. For more information about manually setting up AD for PowerEdge 12G servers, see Appendix B and C.

Active Directory Configuration Workflow

1. The Structure of the Active Directory Environment

The whole AD environment composes the following systems and services

Active Directory Server: A server that is running Microsoft Windows Server 2008 Enterprise with DNS, DHCP, Active Directory Domain Services, and Active Directory Certificate Service, which provides AD, DNS, and DHCP services.

Server(s): Dell PowerEdge server(s) (for example, R820) with iDRAC7. In which, iDRAC AD setup should be configured.

Client: A system that is running Microsoft Windows 7 with Internet Explorer 9 and winrm, on which, the winrm commands are run to configure **Server(s)**.

Router: Connect the above three systems in a private network.

2. Standard Schema or Extended Schema

On the basis of application, two different schemas—standard and extended, can be chosen. The followings are the pros and cons for each schema. For more information about Schema, see [1].

Standard Schema:

Pros: Not having to extend the Active Directory schema

Cons: Active Directory group credentials must be entered for each iDRAC

Extended Schema:

Pros: Must configure only the Active Directory group credentials once for all iDRACs on the domain controller

Cons: An extension to the Active Directory schema, which is irreversible, is required.

3. Set up Active Directory Service

Before configuring the Active Directory for iDRAC, Active Directory service must be set up and the **Enterprise License** must be present. Check **Enterprise License** by following Appendix A. Active Directory service setup steps can be found in Appendix B and C. Dell strongly suggests to follow all the steps in Appendix B and Appendix C to setup the system, manually test it, and make sure it works before trying to use the WSMAN commands provided in this paper to setup AD. In this way, you can be sure the system is a working system. Then customer can try remotely setting up the iDRAC with the procedure stated in this paper.

If Windows Server 2008 is used and the following is the setup for Active Directory service.

- **Domain name: ci.local**
- **FQDN: SCCM.ci.local**
- **Group Name: iDRACAdministrators**
- **DNS IP address: 192.168.0.100**
- **iDRAC IP address: 192.168.0.120**
- **User Name: admin**

If the customers select to use

- Standard Schema
- Static IP address

4. Set up the AD Attributes

The following attributes must be set.

a. `NIC.1#DNSRegister = Disabled`

b. `NIC.1#DNSDomainName = ci.local`

c. `IPv4.1#Enable = Enabled`

d. `IPv4Static.1#Address = 192.168.0.120`

e. `IPv4.1#DHCPEnable = Disabled`

f. `IPv4.1#DNSFromDHCP = Disabled`

g. `IPv4Static.1#DNS1 = 192.168.0.100`

h. `IPv4Static.1#DNS2 = 0.0.0.0`

i. LDAP.1#Enable = Disabled

j. ActiveDirectory.1#CertValidationEnable = Enabled

k. ActiveDirectory.1#Enable = Enabled

l. UserDomain.1#Name = ci.local

m. ActiveDirectory.1#DomainController1 = SCCM.ci.local

n. ActiveDirectory.1#Schema = Standard Schema

o. ActiveDirectory.1#GlobalCatalog1 = SCCM.ci.local

p. ADGroup.1#Name = iDRACAdministrators

q. ADGroup.1#Domain = ci.local

r. ADGroup.1#Privilege = 511

The values are shown for-example only. Customer must change to the values, which is appropriate to their system. For more information and the corresponding winrm commands, See **"Appendix E: Sample WINRM Commands and Mapping to iDRAC GUI Display Names".**

1. Before running the configuration wirnm commands, make sure that LC is ready and delete all pending jobs and pending values (refer to [4] section 33.2.3 and 33.2.4) as they may prevent further configuration changes,

2. By running the **SetAttributes()** method on the **DCIM_IDRACCardService** class, set up the above attributes. This can be done with one **SetAttributes()** command or multiple **SetAttributes()** commands.

3. An iDRAC Card job needs to be created in order for the changes to be committed. This can be done by using the **CreateTargetedConfigJob()** method on the **DCIM_iDRACCardService** class.

4. Start the system and wait for the job status to change to completion. After the job is 100% completed, upload the Certification to iDARC by using the **SetPublicCertificate()** method on the **DCIM_LCService** class to upload the certification created by customer when they set up their certification service.

For all the winrm commands, see **"Appendix E: Sample WINRM Commands and Mapping to iDRAC GUI Display Names"**

5. Check the Setting

The following sample WSMAN command can be run to check the values that customer just set in the above section. Before running this command, change the IP address to customer's iDRAC IP address, and then use the credential of iDRAC.

winrm enumerate "cimv2/root/dcim/DCIM_iDRACCardAttribute" -r:https://192.168.0.120/wsman -u:root -p:calvin -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic -format:pretty

All the AD–related attributes can be found in this output. Search for the **AttributeName** that the customer is interested in. For example, **CertValidationEnable,** a sample output is given here.:

DCIM_iDRACCardEnumeration

AttributeDisplayName = Certificate Validation Enable

AttributeName = CertValidationEnable

CurrentValue = Enabled

…

Check the current value (**CurrentValue**),which is **Enabled**. Therefore, the Certificate Validation is Enabled, which is the correct value we try to set. Therefore, Certificate Validation has been successfully enabled.

Similarly, customer can check if other attributes have been set correctly.

6. Test the Setting

To test if the setting works and the user group has the corresponding privilege, see Appendix D.

If the test is passed, customer can log in to iDRAC by using the AD credential. Customer can also try SSH, WSMAN, and RACADM command with the AD credential.

7. Summary:

This White paper provides the workflow to set up the AD for 12G PowerEdge servers with iDRAC 7 LC . It also provides the WSMAN commands used for the workflow and the mapping of GUI name to the Attribute Name and Display Name for the AD–related attributes.

This paper uses Standard Schema and static IP address as an example to show customer the workflow, and winrm commands for setting up AD. For using Extended Schema and/or DHCP, the workflow and winrm commands are the same. Only the corresponding attributes value must be changed accordingly.

Appendix A : Confirming the iDRAC7 has an Enterprise License Installed

To use Active Directory authentication, you must have an Enterprise License installed on your iDRAC7.
To check the license you have:
1. Browse through to **https://<idrac_ip_address>**, and then log in to iDRAC as an administrative user (the default username is `root`, and password is `calvin`.)

2. Go to **Overview > Server > Licenses**.

3. To view the license information, expand the "+" in the left pane. . However, if only Basic or Express is displayed, and the plus (+) symbol is not displayed, it implies that you cannot use the Active Directory feature. However, you can quickly upgrade to an Enterprise License electronically, by using the License Self-Service Portal (linked on the Licensing page) or by contacting your Dell Sales representative.

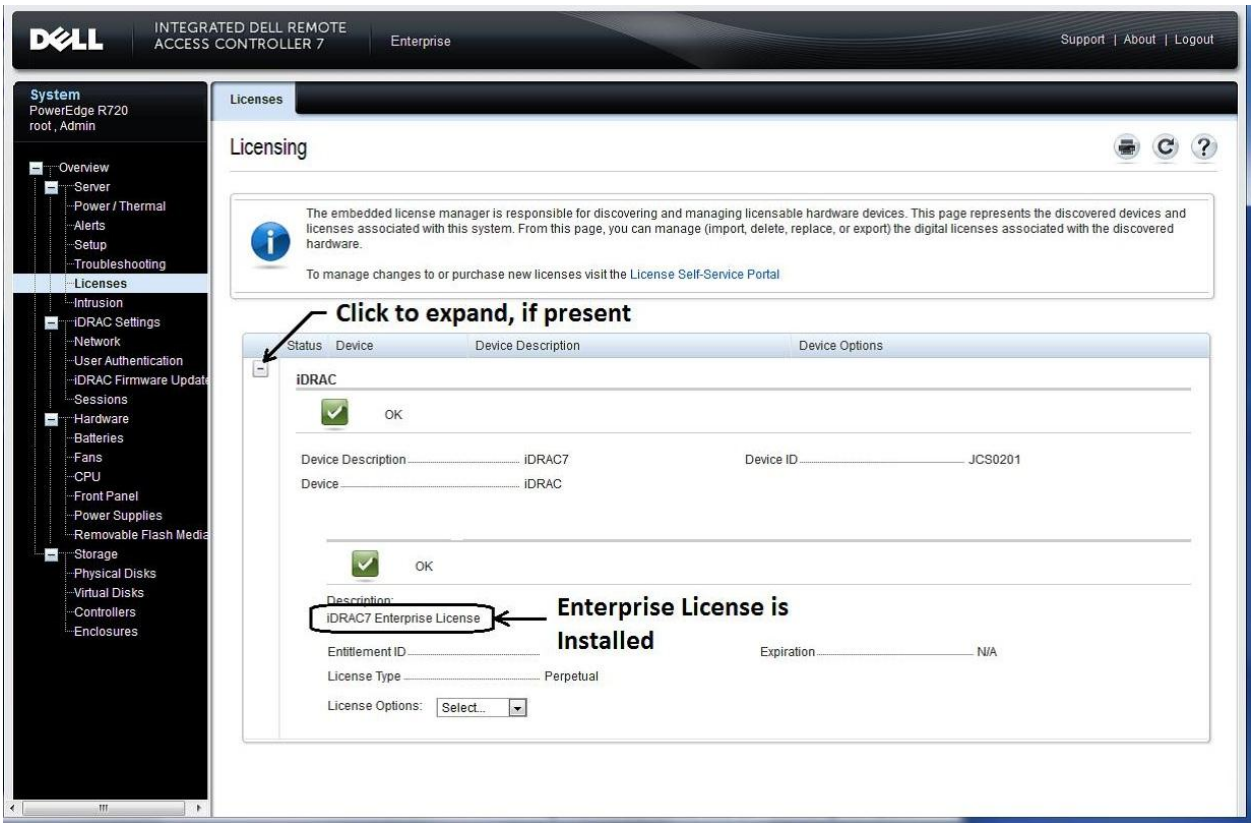

Figure 1. Viewing the License.

Appendix B : Build Active Directory Server

Building the Domain Controller

All tasks in this section are automatically performed on the server that is used as the **Active Directory Server**.

1. Install a supported Windows Server operating system, such as Windows Server 2008 Enterprise.
2. Make sure the date, time, and time zone on the server are correct. This is critical for Active Directory authentication with iDRAC.
3. Configure a static IP address (recommended as it also is the DNS server).
4. If desired, change the Windows computer name of the Domain Controller before running the next steps.

Promoting the Server to a Domain Controller and Installing DNS

The procedural steps are from Windows Server 2008 Enterprise. Tasks for other Windows Server supported operating systems are similar.

1. Promote the server to a Domain Controller. Click **Start** > **Run** > **dcpromo**.
2. In the **Active Directory Domain Services Installation Wizard**, click **Next**.

Figure 2. Active Directory Domain Services Installation Wizard.

3. On the Operating System Compatibility page, click **Next**.

4. Select the **Create a new domain in a new forest option,** and then click **Next**.

5. Enter the **FQDN of the forest root domain** (for example, **`ci.local`**).

6. For both Forest and Domain functional levels, select either **Windows Server 2003** or **Windows Server 2008**, click Next, and then click **Next**.

If DNS is not already installed, you are asked to install it. Accept the default options and install DNS.

7. Accept the default locations for the Database, Log files, and SYSVOL, and then click **Next**.

8. Assign a **Directory Services Restore Mode Administrator Password,** and then click **Next**.

9. On the **Summary** page, click **Next**.

10. Allow the installation to complete and restart the system when prompted.

11. Your system is now a Domain Controller that is running DNS.

Note: If DHCP is not already running on your network, you can optionally install it on the Domain Controller ,or use static IP addresses on your network.

Installing and Configuring Active Directory Certificate Services

Installing Certificate Services as an Enterprise Root CA

1. Open **Server** Manager, go to **Roles** > **Add Roles,** and then click **Next.**

2. Select **Active Directory Certificate Services,** and then click **Next.**

3. Click **Next.**

4. Select the **Certification Authority** option.

5. Click **Next** > **Enterprise** > **Next** > **Root CA** > **Next** > **Create a New Private Key** > **Next.**

5. Accept the default values of CSP, key character length, hash algorithm, and then click **Next.**

6. Accept the default CA name, and then click **Next.**

7. Select the default validity period, and then click **Next.**

8. Select the default database and log locations, and then click **Next.**

9. Click **Install**.

When installation is complete, you should get an Installation Succeeded message as shown in the screen host here.

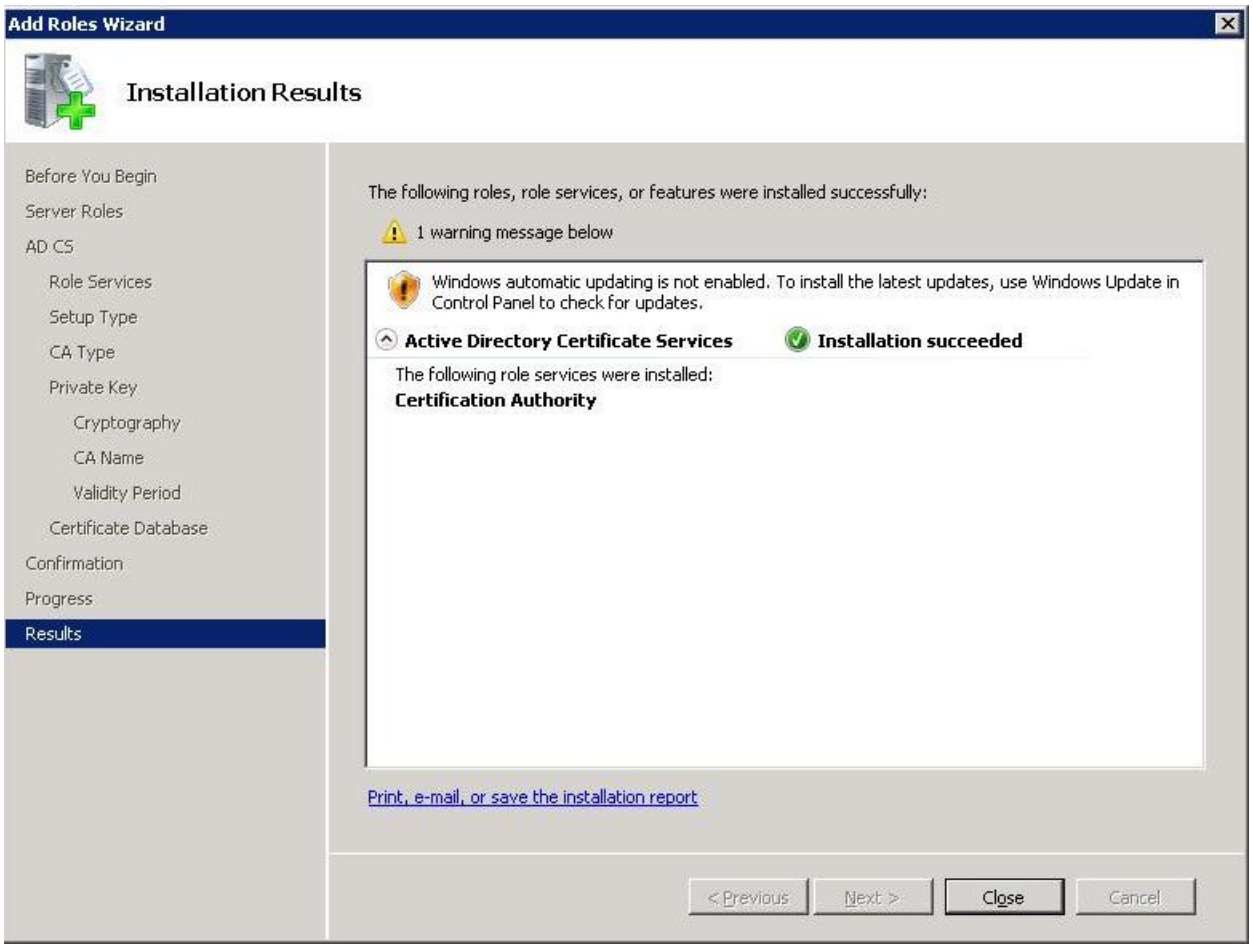

Figure 3. Installation Succeeded Message Screen.

Adding the certificates snap into Microsoft Management Console

1. Click **Start** > **Run** > **MMC** > **OK**.

2. On the **Console 1** page, click **File** > **Add/Remove Snap-in** > select **Certificates** > **Add** > select **Computer Account** > **Next** > **Local Computer** > **Finish** > **OK**.

It is recommended that you save **Console1.msc** to your local hard disk drive. You will use this console for other snap-ins later in this document.

Installing the CA certificate for Client Authentication to the Domain Controller

1. Open **Console1,** expand **Certificates**, expand **Personal**, and then click **Certificates**.

2. Right click **Certificates**, and then click **All Tasks** > **Request New Certificate.**

3. In the **Certificate Enrollment** wizard, click **Next**.

4. Select **Domain Controller**, and then click **Enroll** > **Finish**.

1. 5. The **Certificate Enrollment** page is displayed as shown in the screen host here.

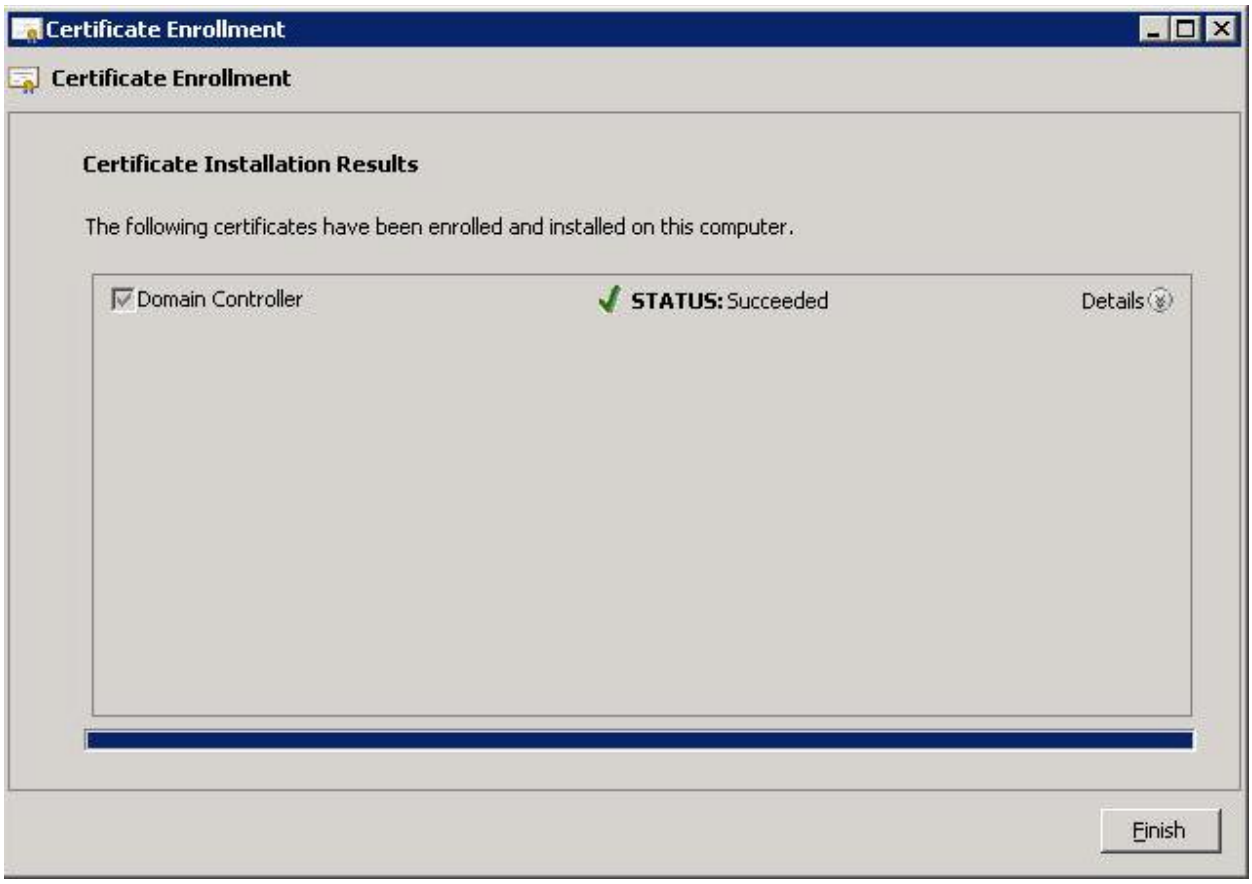

Figure 4. Certificate Enrollment Success Message.

The contents of your certificate folder should now look similar to the following, with the newly-created certificate.

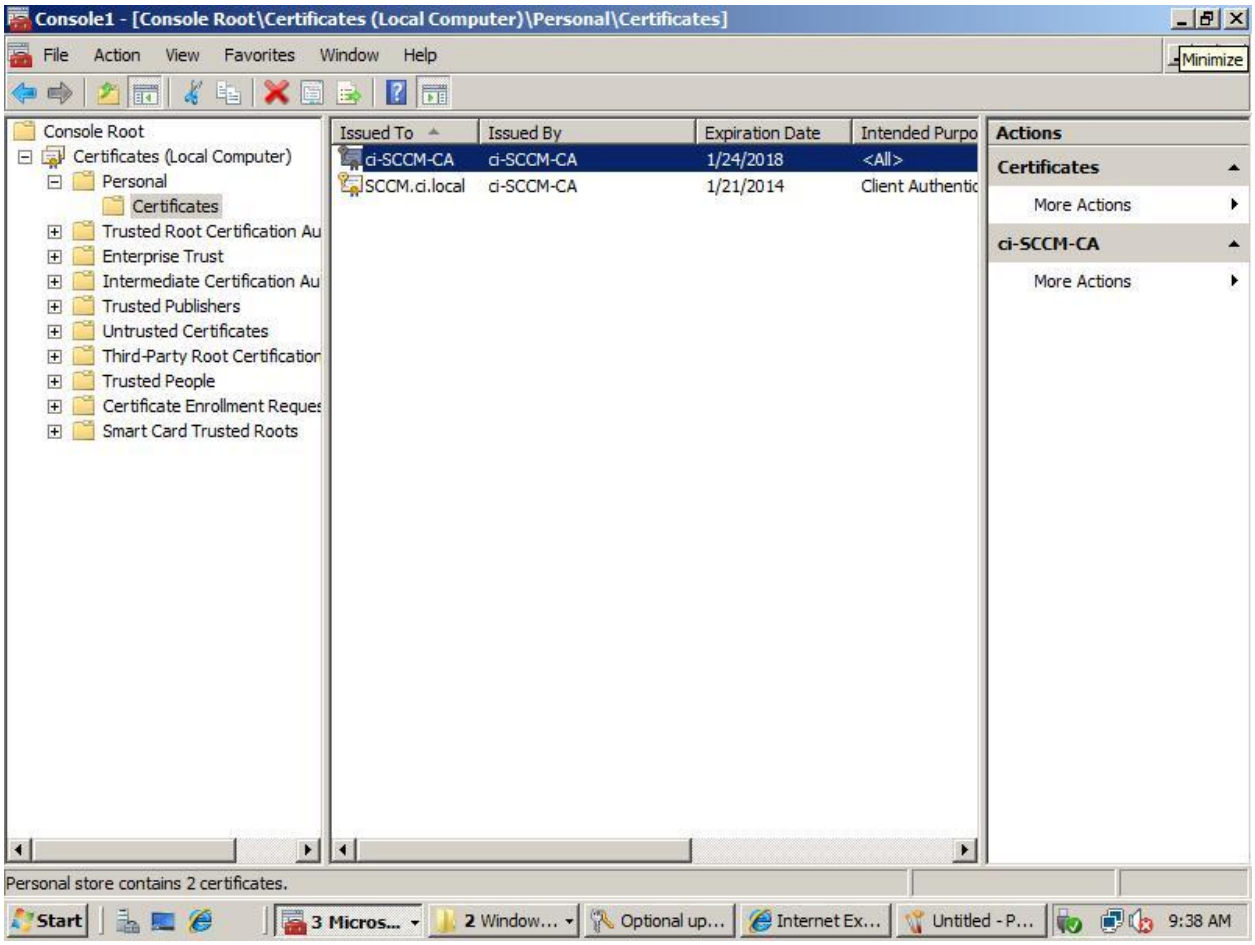

Figure 5. Certificate Folder Contents.

Exporting the CA Certificate (You will install this certificate on iDRAC Server(s) later).
1. Locate the **CA** certificate. This is the certificate issued to your CA, (named **ci-SCCM-CA** in this example).

2. Right click **CA Certificate** and select **All Tasks** > **Export.**

3. In the **Certificate Export Wizard**, click **Next** > **No, do not export the private key**, and then click **Next.**

4. Select **Base-64 encoded X.509 (.CER)**, and then click **Next.**

5. Browse through to the appropriate file location, enter a file name (For example, `root.cer`), and then click **Next.**

Figure 6. Completing the Certificate Export Wizard.

6. Click **Finish**.

7. View the success message, and then click **OK**.

Creating iDRAC Users and Groups

1. In the left pane of **Server Manager**, expand **Roles** > **Active Directory Domain Services** > **Active Directory Users and Computers** > your domain name (**ci.local**).

2. In the **Users** container, create users that will be provided to the three different iDRAC privilege levels. (Right click **Users** and select **New** > **User**). For example, create three users and name them:

- admin
- operator
- readonly

Note: usernames must be an ASCII string of 1–256 bytes. White space and special characters (such as \, /, or @) cannot be used in the user name.

• Assign each user a password and clear the **User must change password at next logon option** as each user is created.

• In addition, in the **Users** container, create groups on the basis of iDRAC privilege levels that the iDRAC users belong to (Right click **Users** and select **New > Group**). Keep the default group type of **Global, Security**. For example, create three groups and name them:

- iDRACAdministrators
- iDRACOperators
- iDRACReadOnlyUsers

After successful completion, the list looks like the screen shot given here.

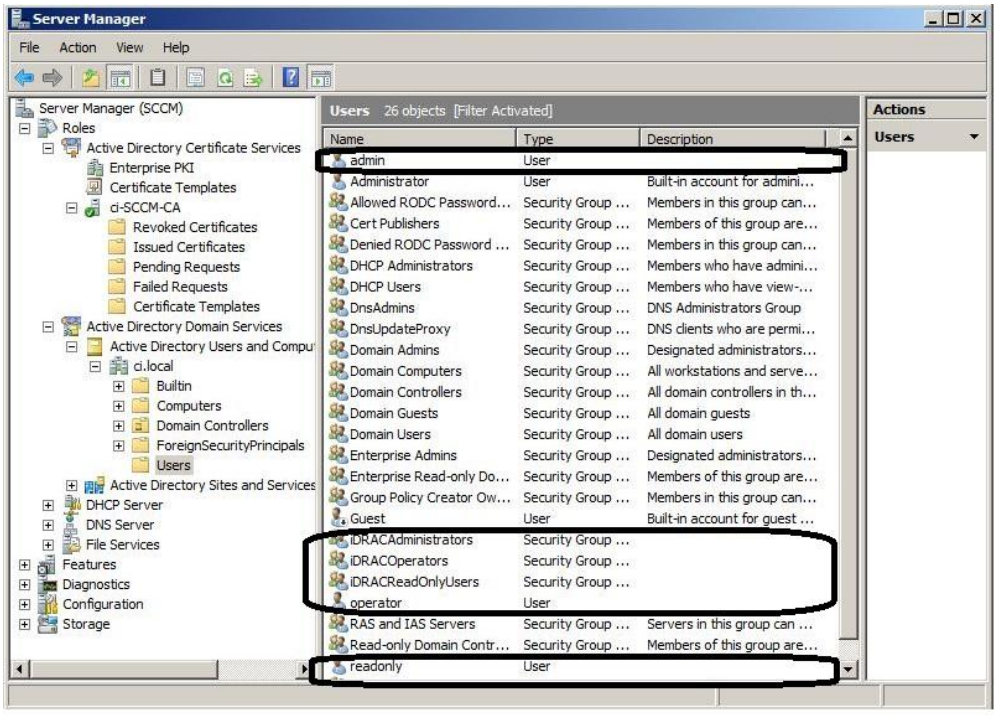

Figure 7. iDRAC Users and Groups

Assigning the users to their corresponding groups

1. Double click the **admin** user, click the **Member Of** tab, and then click **Add.**

2. Under **Enter the object names to select,** type `iDRAC` (or part of the group name you used) > **Check Names** > select the **iDRACAdministrators** group, click OK, click OK, and then click OK

3. Repeat for the **operator** and **readonly** users. (Assign them to **iDRACOperators** and **iDRACReadOnly** groups respectively.)

Appendix C : Configure iDRAC for use with Active Directory Standard Schema

At the **Server(s)**, in your Internet Explorer or Firefox web browser, browse through to **https://<idrac_ip_address>** and log in to the iDRAC GUI of your system as an administrator (the default username is **root**, and password is **calvin**.)

Configure the iDRAC Network Settings

1. On the iDRAC GUI, go to **iDRAC Settings** > **Network** > **Common Settings.**

• **Register DRAC on DNS** (unchecked, optional)

• **DNS DRAC name** (optional), the default is **idrac-<Dell service tag #>**

• **Auto config domain name (not checked).** (Select the option only if your DCHP server provides the domain name).
• **Static DNS Domain Name -** Enter the FQDN of your domain, for example **`ci.local`**, if the **Auto config domain name** option is not selected.

• Click **Apply**.

2. On the same page under **IPv4 Settings:**

3. • Select **Enable IPv4**.

• **DHCP enabled** - (optional, depending on your network configuration). Do not select this option.

• **Use DHCP to obtain DNS server address** - Select this option only if you are using a DHCP server and it is configured to point to the Active Directory Server that is running a DNS. This option is not selected for this experiment.

• **Static Preferred DNS Server** - Specify the IP address of your domain controller that is running DNS, if the **Use DHCP to obtain DNS server address** option was not selected. For this experiment, it is `192.168.0.100`.

• **Alternate DNS server** - Optional, can leave at 0.0.0.0.

• Click **Apply**.

The screen shot given here displays the **Common Settings** page after you enter all the data.

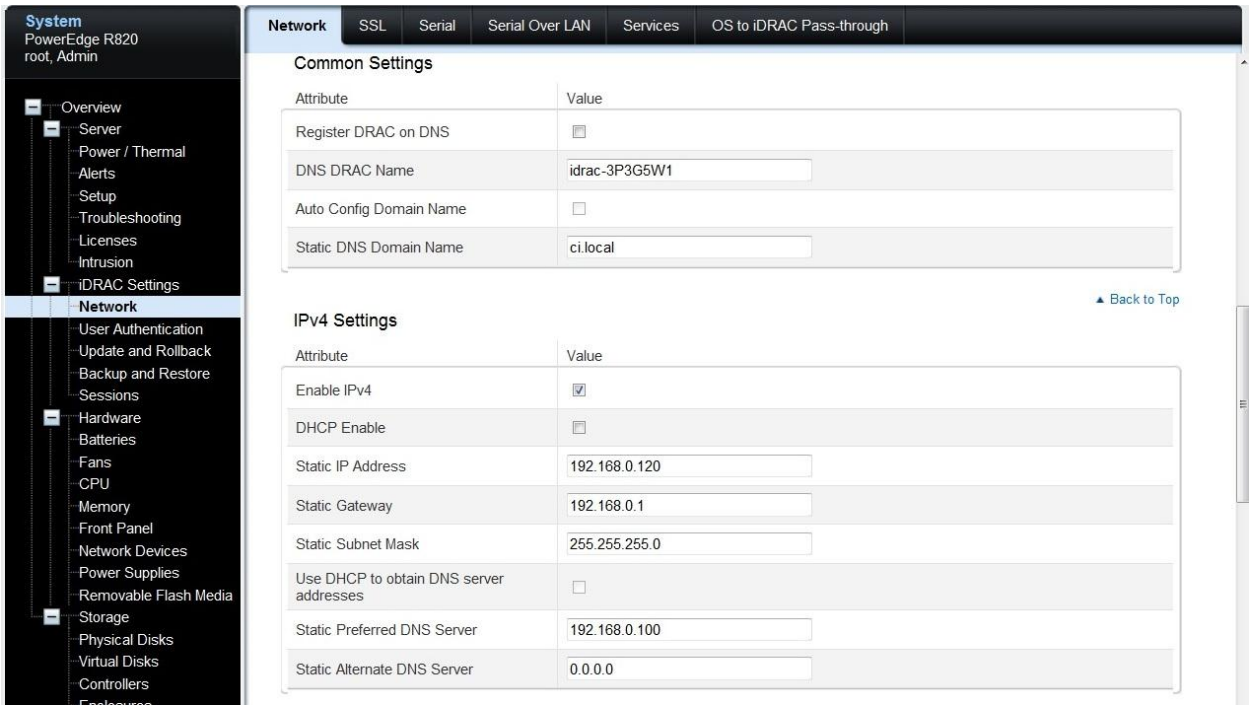

Figure 8. iDRAC Network Settings.

Configure the iDRAC Directory Services Settings

1. Go to **iDRAC Settings** > **User Authentication** > **Directory Services** (Reminder that an Enterprise License is required to get the Directory Services option).

• Select **Microsoft Active Directory,** and then click **Apply**.

• On the **Active Directory Configuration and Management** page, scroll through to the bottom of page and click **Configure Active Directory**.

• Select **Enable Certificate Validation**.

• Upload the **Directory Service CA Certificate** - Upload the certificate file generated earlier (named **root.cer** in this example) to iDRAC. Copy this file from the **Active Directory Server** to your **Client**. In the iDRAC Web GUI, next to **Upload Directory Service CA Certificate**, click **Browse**, point to the file, and then click **Upload**.

A message is displayed as shown in the sample screen shot here.

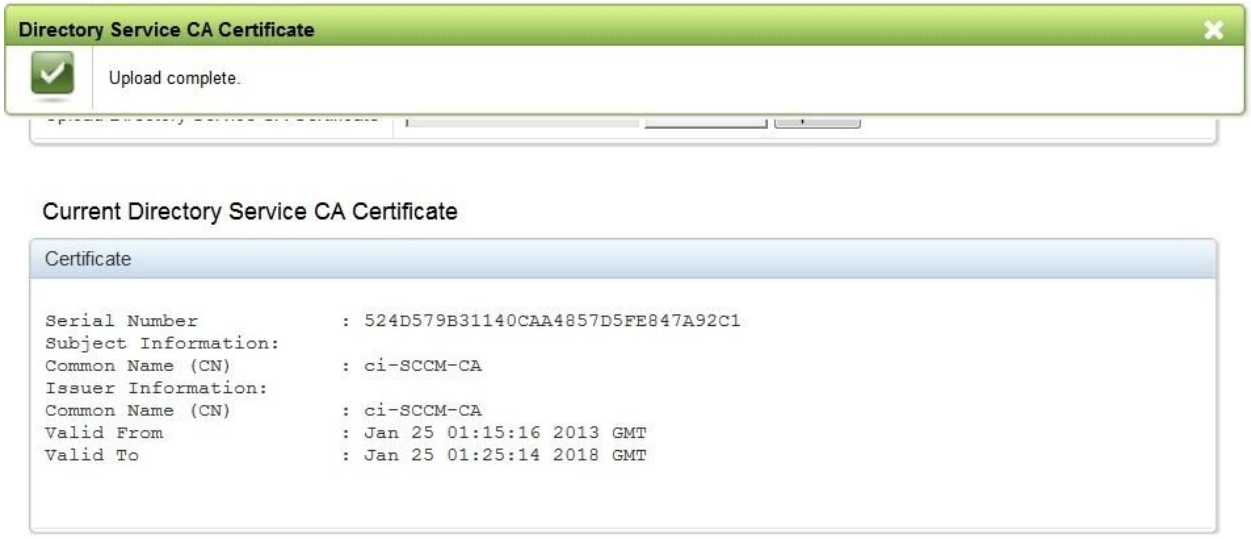

Figure 9. Upload Complete and the Certificate.

If you get a message indicating that the Certificate is not valid, there may be a date/time discrepancy between your CA and the iDRAC. Make sure the date and time on the iDRAC match the date and time on the CA (the **Active Directory Server** in this document) and retry.
Note: If the certificate was issued from a *newly-created CA*, it may continue to be reported as not valid, even though the iDRAC and CA server dates and times match. This is because the iDRAC treats its time as UTC (Coordinated Universal Time). For example, if your CA server was created today at 2:00 P.M. Central Standard Time, the iDRAC views this as 2:00 P.M. *UTC*, a difference of 6 hours. As a result, the "valid from" timestamp on the certificate is not considered valid by the iDRAC until 8:00 P.M. on the day the CA was created. Alternatively, you can temporarily move the time on the **Server(s)** containing the iDRAC ahead by the appropriate amount for your time zone and reset the iDRAC, or wait until the time has passed. Dell is aware of this issue and is developing a resolution for a later release.
2. After you receive the **Upload complete** message, click **OK**.

3. Click **Next**.

4. Select **Enable Active Directory**.

5. Clear **Enable Single Sign-on**.

6. **User Domain Name**. Click **Add** and enter the FQDN of your domain. For example, **ci.local,** and click **OK**.

7. Select **Specify Domain Controller Addresses** and enter the FQDN of your Domain Controller for **Domain Controller Server Address 1** (For example, **SCCM.ci.local**).

8. Click **Next**.

9. Select **Standard Schema.**

10. Click **Next.**

11. Select **Specify Global Catalog Server Addresses** and enter the **FQDN of your Domain Controller** for **Global Catalog Server Address 1** (For example, **SCCM.ci.local**).

12. Click **Role Group 1**.

• For the **Group Name**, enter **iDRACAdministrators** (Note: all group names must be an exact match to the group names you created earlier in **Active Directory Server**).

• **Group Domain** - enter your domain name. For example, **ci.local**.

• **Role Group Privilege Level** - Select **Administrator** from the drop-down menu. Note that all the nine privilege options are selected. Even though these privileges can be customized, it is recommended that you keep the default options selected for the Administrator and Read-only users. "Operator" is the correct user level to make customized privilege selections.

• Click **Apply.**

13. Click **Role Group 2.** • **Group Name** - iDRACOperators

• **Group Domain** - **ci.local** for example

• **Privilege Level** - Select **Operator** from the drop-down menu. Note that seven of the nine options are selected. This is where customized privileges (if any) should be made by selecting or clearing appropriate options.

• **Click Apply.**

14. Click **Role Group 3.** • **Group Name** - iDRACReadOnlyUsers

• **Group Domain** - **ci.local** for example

• **Privilege Level** - Select **Read Only** from the drop-down menu.

• Click **Apply**

• **Click Finish**. The Active Directory Configuration and Management page is displayed.

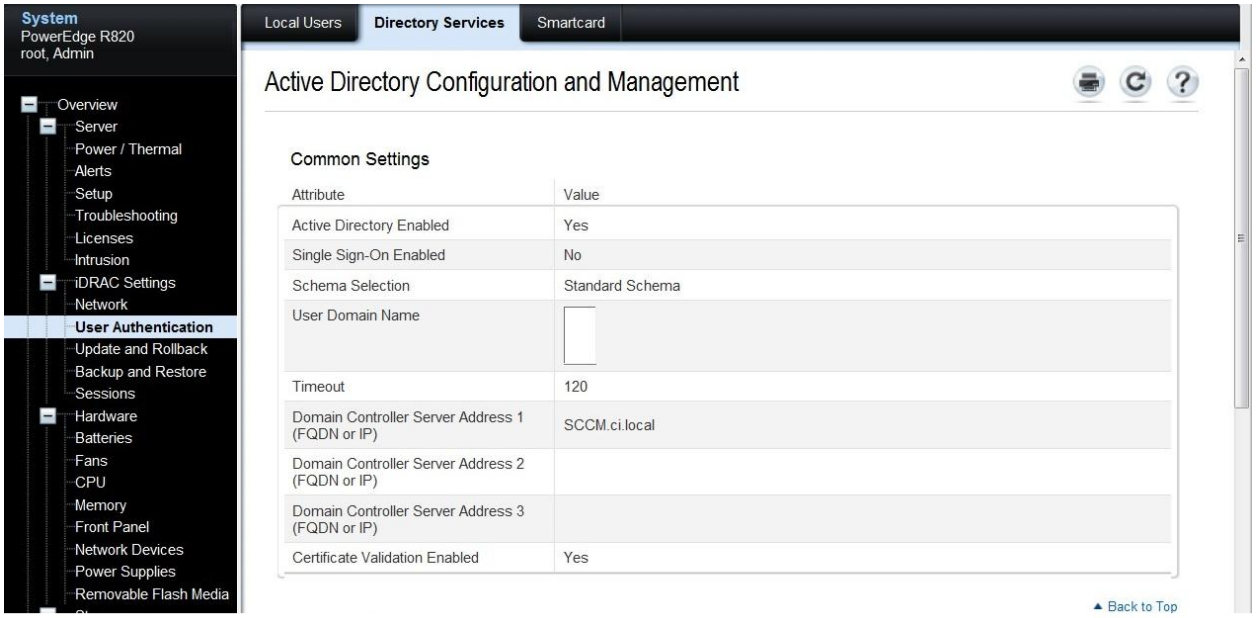

Figure 10. Directory Services Summary

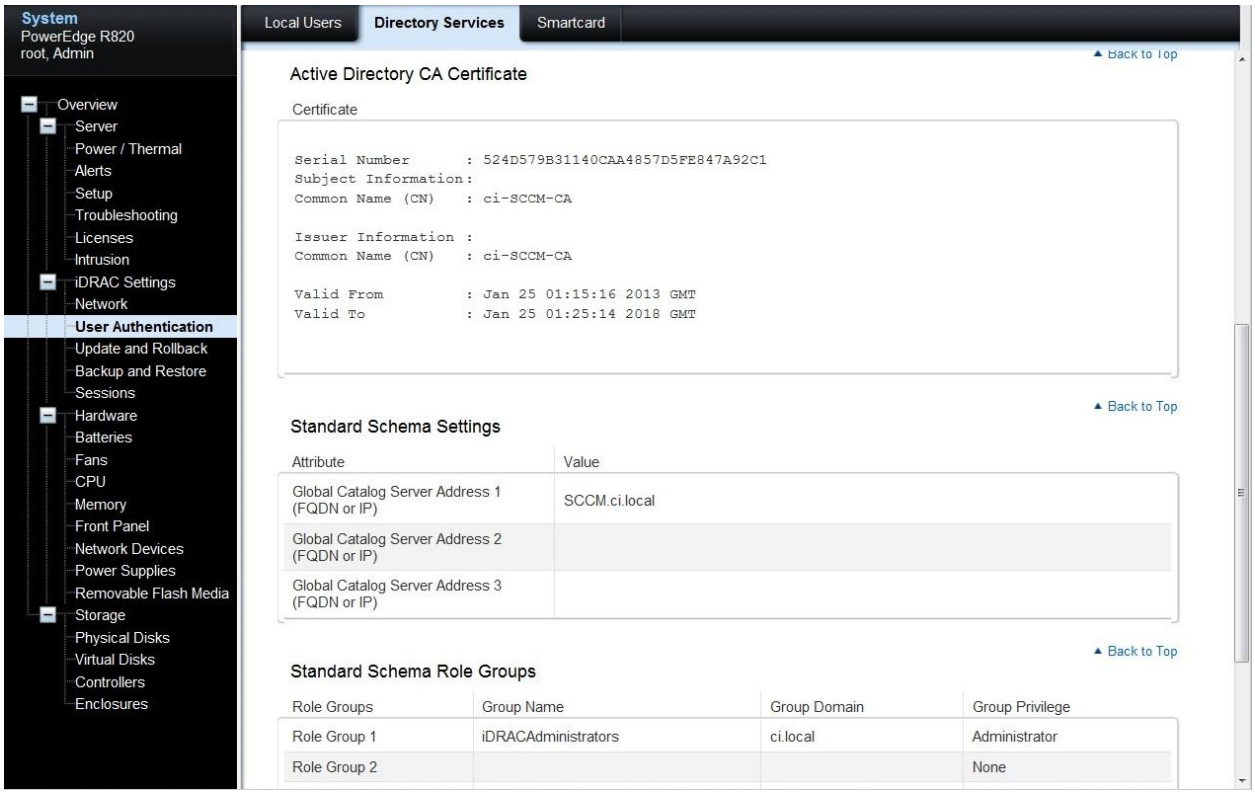

Figure 11. Directory Services Summary (continue)

Appendix D : Test your Standard Schema Configuration

1. Click the **Test Settings** button in the lower-right corner of the screen.

2. In the **Test User Name** text box, type your administrator credentials in the `username@domain.com` format. For example, **admin@ci.local**.

3. In the **Test User Password** text box, type the user's password for the domain.

4. Click **Start Test.**

5. At the top of the results page, all tests must pass (including Certificate Validation) or be marked Not Applicable or Not Configured.
6. The **Test Log** at the bottom of page should have no errors and list all nine privileges in the **Cumulative privileges gained** section as shown here.

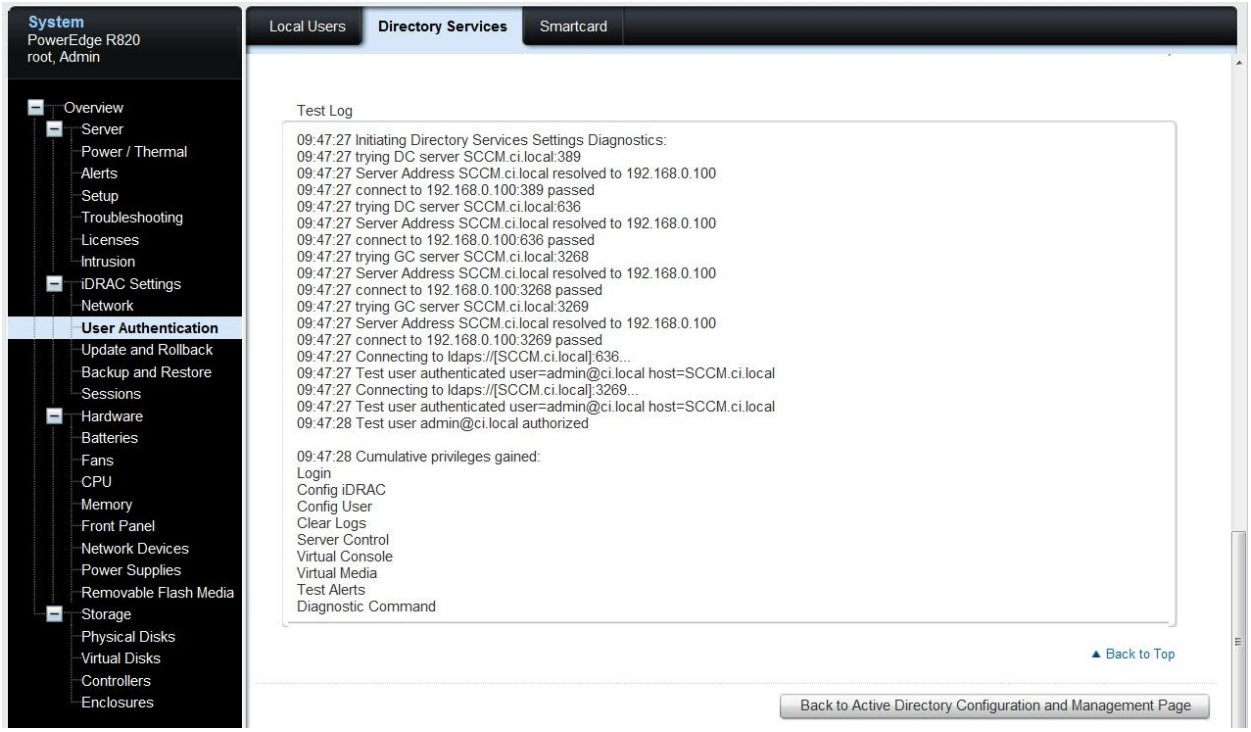

Figure 12. Administrative User Test Results.

You can repeat the test with the other users you've created.

Appendix E : Sample WINRM Commands and Mapping to iDRAC GUI Display Names

For the convenience of knowing the set command for each attribute, the commands are listed individually. Dell suggests customers to use one command for **SetAttributes()** to setup all the attributes together.

Before running the commands, customers must change the IP address to their iDRAC IP address and use the iDARC username and password.

In the following commands, the name is the iDRAC GUI display name, the value is the value this attribute should be set to, and the WSMAN command is the corresponding command to set the value of the attribute.

Name: Register DRAC on DNS
Description: unchecked
Value: Disabled
Winrm command:

```
 winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpgloomo



<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>NIC.1#DNSRegister</p:AttributeName>
  <p:AttributeValue>Disabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Static DNS domain name
Value: your domain name. in this example, ci.local
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
```

```
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpveyu4z

<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>NIC.1#DNSDomainName</p:AttributeName>
  <p:AttributeValue>ci.local</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Enable IPv4
Value: Enabled:
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmp2x0r4s


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>IPv4.1#Enable</p:AttributeName>
  <p:AttributeValue>Enabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Static IP address
Value: the IP address of your iDRAC, in this example, 192.168.0.120

Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmphekkld


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>IPv4Static.1#Address</p:AttributeName>
  <p:AttributeValue>192.168.0.120</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: DHCP
Value: Disabled
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpapfm6v


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>IPv4.1#DHCPEnable</p:AttributeName>
  <p:AttributeValue>Disabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
```

```
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Use DHCP to obtain DNS server address
Value: disabled
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpcm7yd5


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>IPv4.1#DNSFromDHCP</p:AttributeName>
  <p:AttributeValue>Disabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Static Preferred DNS Server
Value : IP address of the DNS server, in this example: 192.168.0.100
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmptg8ijl


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>IPv4Static.1#DNS1</p:AttributeName>
```

```
  <p:AttributeValue>192.168.0.100</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Alternate DNS server
Value: no alternate DNS server is used in this example, therefore, 0.0.0.0
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpocfxcl


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>IPv4Static.1#DNS2</p:AttributeName>
  <p:AttributeValue>0.0.0.0</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Microsoft Active Directory
Description: Check this option. Disable LDAP will enable Microsoft active directory
Value: Disabled
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpvi8who


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>LDAP.1#Enable</p:AttributeName>
  <p:AttributeValue>Disabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Enable Certificate Validation
Value: Enabled
Winrm command:

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmp1shize


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">

<p:AttributeName>ActiveDirectory.1#CertValidationEnable</p:AttributeNam
e>
  <p:AttributeValue>Enabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
```

```
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Enable Active Directory
Value: Enabled
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpuen1af


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>ActiveDirectory.1#Enable</p:AttributeName>
  <p:AttributeValue>Enabled</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: User Domain Name
Value: the domain name, in this example, ci.local
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmp1mdouj
```

```
<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>UserDomain.1#Name</p:AttributeName>
  <p:AttributeValue>ci.local</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Select Specify Domain Controller Addresses
Description: The domain controller addresses, in this example, : SCCM.ci.local
Value: SCCM.ci.local
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpmyzfaf


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">

<p:AttributeName>ActiveDirectory.1#DomainController1</p:AttributeName>
  <p:AttributeValue>SCCM.ci.local</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Standard Schema
Value: Standard Schema
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpccwahb


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>ActiveDirectory.1#Schema</p:AttributeName>
  <p:AttributeValue>Standard Schema</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Specify Global Catalog Server Addresses
Description: The FQDN of your Domain Controller for Global Catalog Server Address1, in this example, SCCM.ci.local
Value: SCCM.ci.local
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpb27flk


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>ActiveDirectory.1#GlobalCatalog1</p:AttributeName>
  <p:AttributeValue>SCCM.ci.local</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>
```

```
SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Role Group1 Group Name
Description: The group name of group1, in this example, iDRACAdministrators
Value: iDRACAdministrators
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmp88bua0


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>ADGroup.1#Name</p:AttributeName>
  <p:AttributeValue>iDRACAdministrators</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Name: Role Group1 Group Domain
Description: The domain name, in this example, ci.local
Value: ci.local
Winrm command

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
```

```
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpqjgepl


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>ADGroup.1#Domain</p:AttributeName>
  <p:AttributeValue>ci.local</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
  RebootRequired = No
  ReturnValue = 0
 SetResult = Set PendingValue
```

Name: Role Group1 Privilege Level
Description: The privilege level for group 1, in this example, the privilege is Administrator
Value: 511
Winrm command

The attribute value 511 has the highest privilege, which is an “administrator”. By changing the attribute value, you can assign different privileges to the users (user group). This command can also be used to set “Role Group2 Privilege Level” and “Role Group3 Privilege Level”.

```
winrm invoke SetAttributes
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty -file:c:\users\zhan_liu\appdata\local\temp\tmpwxb3lt


<p:SetAttributes_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_IDRACCardService">
  <p:AttributeName>ADGroup.1#Privilege</p:AttributeName>
  <p:AttributeValue>511</p:AttributeValue>
  <p:Target>iDRAC.Embedded.1</p:Target>
</p:SetAttributes_INPUT>


SetAttributes_OUTPUT
  Message = The command was successful
  MessageID = RAC001
```

```
  RebootRequired = No
  ReturnValue = 0
  SetResult = Set PendingValue
```

Notes: For group 2 (group 3, …), run the commands for **Role Group1 Group Name, Role Group1 Group Domain and Role Group1 Privilege Level** by using ADGroup.2 (ADGroup3, …) instead of ADGroup1, and then change the corresponding group name and privilege level to the value you choose. You can setup a maximum of five groups.

After setting up the attributes, run the following command to actually make the changes effective and poll the system until it is ready for use again.

"Create Configuration Job"

```
winrm invoke CreateTargetedConfigJob
"cimv2/root/dcim/DCIM_IDRACCardService?SystemCreationClassName=DCIM_Com
puterSystem+CreationClassName=DCIM_iDRACCardService+SystemName=DCIM:Com
puterSystem+Name=DCIM:iDRACCardService"
@{ScheduledStartTime="TIME_NOW";Target="iDRAC.Embedded.1";UntilTime="20
211111111111"} -r:https://192.168.0.120:443/wsman -u:root -p:****** -
SkipCNcheck -SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic
-format:pretty


CreateTargetedConfigJob_OUTPUT
  Job
    EndpointReference
      Address =
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
      ReferenceParameters
        ResourceURI = http://schemas.dell.com/wbem/wscim/1/cim-
schema/2/DCIM_LifecycleJob
        SelectorSet
          InstanceID = JID_596502937751
          __cimnamespace = root/dcim
  ReturnValue = 4096
```

"Poll Job for completion"

```
winrm get
"cimv2/root/dcim/DCIM_LifecycleJob?InstanceID=JID_596502937751" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty
```

```
DCIM_LifecycleJob
  ElapsedTimeSinceCompletion
  InstanceID = JID_596502937751
  JobStartTime = TIME_NOW
  JobStatus = Ready For Execution
  JobUntilTime = 20211111101111
  Message = NA
  MessageArguments = NA
  MessageID = NA
  Name = iDRACConfig:iDRAC.Embedded.1
 PercentComplete = 0


 Until: JobStatus != Completed  [['Ready For Execution']]

winrm get
"cimv2/root/dcim/DCIM_LifecycleJob?InstanceID=JID_596502937751" -
r:https://192.168.0.120:443/wsman -u:root -p:****** -SkipCNcheck -
SkipCAcheck -SkipRevocationCheck -encoding:utf-8 -a:basic -
format:pretty


DCIM_LifecycleJob
  ElapsedTimeSinceCompletion = 0
  InstanceID = JID_596502937751
  JobStartTime = TIME_NOW
  JobStatus = Completed
  JobUntilTime = 20211111101111
  Message = Job successfully completed.
  MessageArguments = NA
  MessageID = JCP007
  Name = iDRACConfig:iDRAC.Embedded.1
  PercentComplete = 100
```

Name: Upload Certification
Description: The Directory Service CA Certificate you generated when setup the certification service. See page p7 of [1]
Value: see the content of *SetDirectoryCACert.xml* below
Winrm command

```
winrm i SetPublicCertificate http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_
LCService?SystemCreationClassName=DCIM_ComputerSystem+CreationClassName
=DCIM_LCS
ervice+SystemName=DCIM:ComputerSystem+Name=DCIM:LCService -u:root -
p:calvin -r:h
ttps://192.168.0.120/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -
a:basic -f
ile:SetDirectoryCACert.xml
```

```
SetPublicCertificate_OUTPUT
    ReturnValue = 0
```

Sample xml file content (SetDirectoryCACert.xml**)**

```
<p:SetPublicCertificate_INPUT
xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/root/dcim/DCIM_LCService">
<p:Type>directoryCA</p:Type>
<p:Certificate>
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIQUk1XmzEUDKpIV9X+hHqSwTANBgkqhkiG9w0BAQUFADBA
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEjAQBgoJkiaJk/IsZAEZFgJjaTETMBEG
A1UEAxMKY2ktU0NDTS1DQTAeFw0xMzAxMjUwMTE1MTZaFw0xODAxMjUwMTI1MTRa
MEAxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDESMBAGCgmSJomT8ixkARkWAmNpMRMw
EQYDVQQDEwpjaS1TQ0NNLUNBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAkU7Ec3P9KJCW9HRPIbS/yWcjmxluZqv2MSfzb2DFMBwmjr/PZ+inadDQKsAR
lnoWceLiEZy9qLmPi3HXQpFYwM+dl+s95TGrH7cxaHXIsmraXb1gbvn9FwGerg/P
pJkGMq0LVzCuo8RBPPSlh3Ua/0WTPAnkbKq1wE5UrdkP8xnPSgMNCPieTixasndO
kj4IJOLUWYoh4AN3IYab33hhCINipr0xjx5wvFd49HOTI17WfEb79S5BiTl0hen/
uV3Lar5yxlXXk1Qxh3e/Iddbtn6fv5JDo4Lx/frRjmuCytRKQll5CLhja5vB4nFI
WQcLLAzQkREkqr0OkL1/S9rJ4wIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0T
AQH/BAUwAwEB/zAdBgNVHQ4EFgQU1TNEWKRBOeg05hzuKHoQE+kkNTYwEAYJKwYB
BAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQADggEBAFwBI4HIthr3CIAjpOZSrJy8
/a4E2CS94k39uD3VUthmuMHBk42KaU4faiKoYnvwPNF5GV3t5bGDhCePnUbXnHje
1zNJuSoytRhW4McLUQ3Y6WWx09n9np/NOEP5YUcM1ELs16V2DJS/ruN742tElGsz
GmoJoaQCuaQ4BeZpjO+keh2vbeJyJDFArICw31sG/9lLEu/b01ywMu877ourD22B
1XB4RUGOkAqlY+AxEh0acGSOtJjinyeBJbpJqkpmPFxq2RDF96idDU5uUedZ00eO
aLcCjujbiZiqZMs32cdzsVy0WiTL5Csanx3rDbTxQFYVPcR6e97DuMjb4CXUDC8=
-----END CERTIFICATE-----
</p:Certificate>
```

References

[1] Integrating iDRAC 7 with Microsoft Active Directory
http://en.community.dell.com/techcenter/extras/m/white_papers/20078288/download.aspx

[2] http://moss.dell.com/sites/softdevwiki/Wiki%20Pages/PKCS12.aspx

[3] Dell iDRACCard Profile 1.3
http://en.community.dell.com/techcenter/extras/m/white_papers/20263520/download.aspx

[4] LC Integration Best Practices
http://moss.dell.com/sites/MASER/Console_Integration/Shared%20Documents/Best%20Practices/LC%20Integration%20Best%20Practice.pdf

Glossary

Acronym	Description
FQDN	Fully Qualified Domain Name
LC	Lifecycle Controller
AD	Active Directory
iDRAC	Integrated DELL Remote Access Controller
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
GUI	Graphical User Interface