HOL-0903-01 - iDRAC9 7.00.X FOR PowerEdge Servers
# Table of Contents

Lab Overview - iDRAC9 GUI Overview ................................................................. 4
Lab Guidance ........................................................................................................ 5

Module 1 - iDRAC9 Getting Started ................................................................. 7
  Module 1 - iDRAC9 Getting Started ............................................................... 8
  Getting Started / Did you Know? ................................................................. 9
  Lesson 1 - iDRAC9 Login screen ............................................................... 10
  Lesson 2 - iDRAC9 Dashboard ................................................................. 13
  Lesson 3 - iDRAC9 Maintenance ............................................................... 16
  Lesson 4 - iDRAC9 Storage ................................................................. 24
  Module 1 Conclusion ............................................................................... 31

Module 2 - iDRAC9 Configuration ................................................................. 32
  Module 2 - iDRAC9 Configuration ........................................................... 33
  iDRAC9 Configuration / Did you Know? .................................................. 34
  Lesson 1 - iDRAC9 BIOS settings ......................................................... 35
  Lesson 2 - iDRAC9 Alerts ...................................................................... 38
  Lesson 3 - iDRAC9 Server Configuration Profile .................................. 41
  Lesson 4 - iDRAC9 Virtual Console options ....................................... 45
  Module 2 Conclusion .............................................................................. 47

Module 3 - iDRAC9 Security ........................................................................... 48
  Module 3 - iDRAC9 Security ................................................................. 49
  iDRAC9 Security / Did you Know? ......................................................... 50
  Lesson 1 - iDRAC9 System Lockdown mode .......................................... 51
  Lesson 2 - iDRAC9 Settings and Security ............................................. 55
  Lesson 3 - iDRAC9 Web Security .......................................................... 61
  Module 3 Conclusion .............................................................................. 64

Module 4 - iDRAC9 Datacenter ..................................................................... 65
  Module 4 - iDRAC9 Datacenter ............................................................... 66
  iDRAC9 Datacenter / Did you Know? ..................................................... 67
  Lesson 1 - iDRAC9 Datacenter Telemetry Streaming ......................... 68
  Lesson 2 - iDRAC9 Datacenter Multi Vector Cooling ....................... 72
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesson 3 - iDRAC9 Datacenter Automatic Certificate Enrollment</td>
<td>75</td>
</tr>
<tr>
<td>Module 4 Conclusion</td>
<td>77</td>
</tr>
<tr>
<td>Module 5 - iDRAC9 RedFish</td>
<td>78</td>
</tr>
<tr>
<td>Module 5 - iDRAC9 Redfish</td>
<td>79</td>
</tr>
<tr>
<td>iDRAC9 Redfish / Did you Know?</td>
<td>80</td>
</tr>
<tr>
<td>Lesson 1 - Redfish GET requests</td>
<td>81</td>
</tr>
<tr>
<td>Lesson 2 - Redfish PATCH requests</td>
<td>85</td>
</tr>
<tr>
<td>Lesson 3 - Redfish POST requests</td>
<td>88</td>
</tr>
<tr>
<td>Module 5 - Conclusion</td>
<td>92</td>
</tr>
<tr>
<td>Conclusion</td>
<td>93</td>
</tr>
<tr>
<td>Conclusion</td>
<td>94</td>
</tr>
</tbody>
</table>
Lab Overview - iDRAC9 GUI Overview
Lab Guidance

iDRAC9 GUI Overview

About this lab:

It will take approximately 45 - 90 minutes to review the basic features of this lab. The modules are independent of each other, so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

This lab will cover many of the highlights of the iDRAC9 7.00.00.00. This includes several features of the Datacenter license. This lab is designed to touch on a few key items but will not cover every possible option. You are encouraged to explore as you wish.

Please note that while in demo mode, it is not possible to "apply changes" to the system. Doing so may result in an error; an example may be "RAC0508: An unexpected error occurred." If this happens, simply click "OK" and return to the page. Also, some features such as virtual console and Group Manager are not available in demo mode.

Navigation - text in **Bold** indicate an action and the image will have red box outline. Items in an image with a yellow box outline point out items of interest.

iDRAC9

The integrated Dell Remote Access Controller 9 (iDRAC9) delivers advanced agent-free, local and remote server administration. iDRAC9 provides additional security and control to help IT admins monitor and manage their PowerEdge Servers. This lab will cover a few of the key features such as dashboard, alerts, system lockdown, BIOS, server configuration profile, and more.

Lab Module List

- **Module 1** - Introduction
  - Lesson 1 - Log in (5 minutes) - Basic - This lesson will walk you through an overview of the information available and security features on the initial log in screen
  - Lesson 2 - Dashboard (5 minutes) - Basic - This lesson will cover the key information located on the dashboard.
  - Lesson 3 - Maintenance (5 minutes) - Basic - This module will provide an overview of logs, job queue, and troubleshooting options
  - Lesson 4 - Storage (10 minutes) - Basic - This module will showcase the deep level information available for drives, controllers, and enclosures

- **Module 2** - Configuration
  - Lesson 1 - BIOS settings (10 minutes) - Basic - This lesson will demonstrate how to view BIOS information while the server is running as well as stage any changes.
  - Lesson 2 - Alerts (10 minutes) - Basic - This lesson will showcase how to set and view alerts
  - Lesson 3 - Server Configuration Profile (10 minutes) - Basic - This module will provide a high level overview on how to create, export, and import a custom-tailored template of a server for various uses
  - Lesson 4 - Virtual Console (10 minutes) Advanced - This module will cover the new eHTML5 access to the virtual console.
• Module 3 - Security
  • Lesson 1 - System Lockdown mode (5 minutes) - Advanced - This lesson will show how to enable System Lockdown mode, and cover the effects and benefits of doing so.
  • Lesson 2 - iDRAC settings and security (10 minutes) - Advanced - This module give an understanding of the configuration options for connectivity, services such as RSA SecurID, AD/LDAP, users, and the iDRAC Connection View
  • Lesson 3 - Web security settings (10 minutes) - Advanced - This module will showcase how and why to select advanced security settings to access the iDRAC, including Cipher Select.

• Module 4 - iDRAC9 Datacenter
  • Lesson 1 - Telemetry Streaming (10 minutes) - Advanced - This modules shows the various previously set parameters and reports this server can stream telemetry data.
  • Lesson 2 - Thermal Manage (10 minutes) - Advanced - This modules provides an overview of many options available to fine tune the cooling options for your server.
  • Lesson 3 - Automatic Certificate Enrollment (5 minutes) - Advanced - This lesson gives a quick overview on how to set up the initial CA certificate as well and continual renewal of the same.

• Module 5 - Redfish
  • Lesson 1 - Overview of "Get" (3 minutes)
  • Lesson 2 - Overview of "Post" (3 minutes)
  • Lesson 3 - Overview of "Patch" (3 minutes)
Module 1 - iDRAC9 Getting Started
Module 1 - iDRAC9 Getting Started

Module 1 - iDRAC9 Getting Started (30 minutes) - Basic - This module will provide an introduction to the iDRAC9 web interface.

This module contains the following lessons:

1. Lesson 1 - The Log in screen
   1. Learn about the additional information found on the log in page

2. Lesson 2 - The Dashboard
   1. Review of the key information available on the dashboard when you first log in to the iDRAC

3. Lesson 3 - Maintenance
   1. Overview of logs, job queue, and troubleshooting options

4. Lesson 4 - Storage
   1. View deep level information about drives, controllers, and enclosures
Getting Started / Did you Know?

Log in Screen

The iDRAC9 Log in screen has links to several key pages such as manuals, user guides, white papers and more. There is also a customizable "warning banner" that can be tailored to the exact needs of your company.

Dashboard

Just like the dashboard on your car, the iDRAC dashboard provides key server information the moment you log in. From there, the most widely used features such as virtual console (requires iDRAC Enterprise or Datacenter,) access to logs, and easy navigation to other tabs.

Maintenance

All the detailed activity of the server can be seen in the Lifecycle log. This log can hold over 5 years of average server data events. The log includes SEL events as well as other informational events such as log ins and firmware and configuration changes.

This provides you and tech support with an incredible amount of detail as to what has been occurring on your server. And the SupportAssist Collection can be run quickly and without the need to make changes or power down the server.

All in an effort to keep your PowerEdge servers running in top performance.

Storage

With iDRAC9, quick access to all your storage is at your fingertips. No need to install an agent in the operating system, or take the server offline to add a drive. This means more uptime for production servers, and more time you can spend on other datacenter tasks.
Lesson 1 - iDRAC9 Login screen

Lesson 1 - iDRAC Login screen (5 minutes) - Basic - Overview of the information available and security features on the initial log in screen

The iDRAC9 log in screen provides a great deal of information - even before you log in. The key features specific to this module are the key identifiers about the server you are about to access, the customizable security banner, and the links for additional information regarding manuals and other help.

Launch iDRAC9 Simulator

From the Desktop, launch the iDRAC9 Simulator

Log in Screen

At this point, you will be presented with the initial login screen

Note the server model and iDRAC license installed on the server
Review the **security banner**. This is configurable via Racadm commands.

Notice the links at the bottom of the screen. Select the "Help" to bring up the embedded Help Guide. Other links will connect to Dell support pages, which may not be available in Demo mode.

For the purposes of this lab, the username/password combination is set to **root/calvin**. Press "**log in**" to continue.
Lesson 2 - iDRAC9 Dashboard

Lesson 2 - iDRAC9 Dashboard (5 minutes) - Basic - Introduction to the key information found on the dashboard.

The iDRAC9 dashboard offers a great deal of key information as soon as you log in to the server. High level health status and the most used short cuts and functions are found on the home page.

Dashboard

The initial landing page after logging in with correct credentials is the iDRAC9 Dashboard. This screen shows an overview of the system health, system information and recent events in the log.

From this screen there are a number of tasks that can be performed:

• Control power options
• Find and navigate to pages via the "Search" box
• View and access pending and past jobs in "Task Summary"
• Turn on/off System Lockdown Mode (This will be covered in a later module)
• Navigate to other sub menus within the iDRAC interface

Key information available at log in

• Server system and storage health
• System information
• Recent log events

Also available on the Dashboard (requires iDRAC Enterprise or Datacenter) but not available in Demo mode:

• Virtual Console
• Group Manager

Take some time to navigate around the dashboard
Accessing help and other resources

The same information located on the log in screen is also located in the top right hand corner of the iDRAC9 web interface. Click on the small white circle containing a question mark. This will bring up the various help options. Next, click on "Help" and a new window will pop up. Review content and close the Help window.

Using the Search box

The Search box helps you find and navigate quickly to pages within the iDRAC. Simply type in a word, and pages with that key word will appear. Then, you can move your mouse down and click on the page you wish.

Locate the "Search box," type in the word "Alert" to see the options.
Task Summary

The Task Summary is a quick way to view any pending or previous jobs scheduled, running, or performed on the server. This can be very useful when checking status for pending jobs before rebooting the server.
Lesson 3 - iDRAC9 Maintenance

Lesson 3 - iDRAC Maintenance (10 minutes) - Basic - Overview of logs, job queue, and troubleshooting options.

There are times when as a server admin, you want to see what happened to the server – perhaps a critical error occurred or tracking down when an update was installed. Or you need to work with Tech Support to resolve an issue. All of this and more can be done from both the Dashboard and the maintenance tab.

Checking Server and Storage health from the Dashboard

Should any server component or storage device have an issue (warning or critical) the "Health Information" box will change from green to yellow or red to match the issue. Note that for the demo this system has no issues. If there were an issue, click "Details" to go to directly the System tab

System Overview page

This page will show the health status of key server components. iDRAC9 4.xx and forward monitors items such as GPU's and FPGA's, as well as SFP network cards. Take a moment to click on a few of the components in the server, such as "Accelerators" to view the GPU card installed. New categories include Removable Media, Voltages, and extended details have been added to PCIe slots. All the pertinent information you need as well as extensive details just a click away.

When done, take a look at the details provided in Cooling. Click on the "Cooling" tab and expand "Temperatures"
Review the data provided. When done, click on the "expander arrow" to minimize.

**Navigate to Maintenance Tab**

After viewing the information about the Accelerators, click on the "Maintenance" tab

The main page for Maintenance will appear, and the Lifecycle Log will be displayed. The Lifecycle Log includes all the events for the server, including events such as log in, jobs scheduled, SEL Events, and more.
The Lifecycle Log can also be filtered and exported. Click the "Filter" option in the top right corner.

This will bring up the various filter options such as severity, log type, date ranges, or you can enter a specific keyword or IP address or event.

Next, navigate to the "Troubleshooting" tab
The Troubleshooting tab displays the last 3 boot captures. iDRAC Enterprise and Datacenter also offer the option to view an OS crash screen; this feature requires the iDRAC Service Module (iSM) to be installed in the OS / hypervisor.

Note that these features (boot capture, video player, last crash screen) are not available in demo mode.

Click on the "Diagnostics" tab

On this page, you can remotely reset the iDRAC (note that you can do this as well on the Dashboard.) One key feature on this page is the option to run diagnostic commands. Click the "?" icon in the top right corner to display the command options in the "Help"
Also available on this page are options to gather Serial Data Logs for better diagnostics, along with the option to set frequency for BIOS Live Scanning.
Next, click on the “SupportAssist” tab

This page can be used to run your own report, view previous collections, and offer links to check the warranty for the server.

Should you have to contact Tech Support for an issue, they will direct you to this page to run a detailed report on the server. Click the "Start a Collection" to initiate the report.

The next page will show the various areas of collection. Some options require the installation of the iDRAC Service Module. **Mouse over the blue and yellow icons** for details for each particular option. Then click "Cancel" to return to the previous page.
Next, review the Collection Log to see the previous report data. On this page you can view last collection date, status, and more. Note that the actual Collection Log is not available in demo mode.

Next, scroll up the page on click on "Check Warranty"

This feature allows you to quickly check the warranty status of your server.
While this feature isn't active in Demo mode, it would allow you to open a tab on your browser and view the warranty information associated with this service tag.

Next, take note on the "Visit Support Portal". Note that this feature is not available in demo mode. This would open a new tab in your browser taking you to the Dell Support page.

This concludes the Maintenance lesson.
Lesson 4 - iDRAC9 Storage

Lesson 4 - iDRAC Storage (10 minutes) - Basic - View deep level information about drives, controllers, and enclosures. Plus a brief overview of drive security options.

The latest version of iDRAC9 helps keep IT admins informed on drive status, but also provides extensive details about the drives, controllers, and any associated enclosures.

For a more in depth walk through of iDRAC9 storage features, see the "iDRAC9 Interactive Demo."

Navigate to the Storage tab

From any page, select the "Storage" tab

The main page for storage will appear.

The storage tab provides information about the locally attached storage controllers, physical disks, virtual disks and enclosures.

A number of additional features have been added to the iDRAC 9 in regards to storage.

- Online Capacity Expansion
- Raid Level Migration
- Virtual Disk wizard
- View and edit SSD wear thresholds
- Secure erase of SEDs (Self Encrypting Drives)
- Variety of filters to sort/view drives

The Summary screen provides the status of all physical disks attached to the system in both a graphical system view as well as a pie chart format. Other details are displayed, such as a text list of physical disks, virtual disks and hot spares configured, both global and dedicated. At the bottom of the screen, recent storage events from the log file are displayed.
The front view of the server shows the drives populated in the server. Note that there are only 2 drives in this server. Mouse over the first drive to see information for this drive.

Clicking the "Controllers" tab lists all PERC and SAS HBA modules installed in the system. Note that the PowerEdge RAID Controller (PERC) H745 is installed on this system. Click the "+" to expand this section.

Take a moment to review the extensive amount of information available; you may need to scroll down to see it all. When done, click the "-" to return to the previous screen.
Open the "Physical Disks" tab to see all disks attached to the system.

High level information is provided for both PCIe SSD's and physical disks. Extensive information about a drive can be seen by expanding the "+"

After reviewing the details, click the "-" to return the last screen
Take a look at the filter options. Click on "Filter Options" and then "Advanced Filter".

This block allows you to choose what drives you're looking for. There are several drop down options as well as custom fields. When done, click on "Cancel."
Scroll to the top and click the "Virtual Disks" tab lists all disks attached to the system.

Just like the physical disk tab, high level information is provided for the virtual disk. As you can see, no virtual disks have been created. While it is not possible to create a virtual disk in demo mode, you can see how to create a virtual disk in the "iDRAC9 Interactive Demo."

Next, the "Enclosures" tab lists all enclosures attached to the system.

There is no Enclosure attached to the server in Demo mode. However, this screen will also provide information about the backplane in the system. Expand the "+" to see the drives from the viewpoint of the enclosure.
Now, take a look at some of the security options available for drives. Navigate to "iDRAC Settings" the "Services" and then "iDRAC Key Management."

The iDRAC Key Management features are available with iDRAC Enterprise or Datacenter. There are 2 types of licenses for storage - local and external. Local is the iDRAC Local Key Manager, or iLKM and is a key between the iDRAC, PERC, and the drives. The external solution called "Secure Enterprise Key Manager (SEKM) has all the elements of iLKM, but also adds a check to an external Key Management Interoperability Protocol (KMIP) server. SEKM is not available in Demo mode.
Take a moment to explore the various iLKM settings. See also the "?" in the top right corner.

This concludes the Storage lab.
Module 1 Conclusion

Congratulations on completing Module 1.

In Lesson 1 - Log in

- You were shown the many different links for additional information.
- You logged in with the legacy password "calvin" but also know the default is the random password located on the pull out information tag on the front of the server.

In Lesson 2 - Dashboard

- You discovered the key items available on log in and the easy access to other key functions of the iDRAC9.

In Lesson 3 - Maintenance

- You were able to view the detailed information kept in the Lifecycle Log. You were also able to view where any of the crash screen captures would be stored. Other options, such as diagnostics and how to capture a SupportAssist log were also shown.

In Lesson 4 - Storage

- You were able to view the detailed information for physical disks, virtual disks, controllers, and enclosures.

For additional information on iDRAC9, please see the “white papers” [www.dell.com/support/idrac](http://www.dell.com/support/idrac)
Module 2 - iDRAC9 Configuration
Module 2 - iDRAC9 Configuration

Module 2 - iDRAC Configuration (30 minutes) - advanced - This module will cover a few of the key tools that can be used to provision a bare metal server, or make changes to already configured servers.

This module contains the following lessons:

1. Lesson 1 - BIOS settings
   1. View BIOS information while the server is running as well as stage any changes

2. Lesson 2 - Alerts
   1. Understand how to view and set alerts

3. Lesson 3 - Server Configuration Profile
   1. How to create, export, and import a custom-tailored template of a server for various uses
iDRAC9 Configuration / Did you Know?

BIOS Settings

iDRAC9 allows you to view and edit BIOS settings while the server is running - meaning more server uptime. BIOS changes can implemented right away, or they can be scheduled for the next server reboot.

Alerts

With iDRAC9 you can easily set up alerts with a few mouse clicks. "Quick Alerts" groups alerts for easy configuration. If a more granular process is required to set alerts, the full option is still available. Quick Alerts allows you to spend less time setting up your server, while still providing key information alerts.

Server Configuration Profile

With a Server Configuration Profile (SCP) you can import and export a set template to a server to easily provision a bare metal server. But an SCP can do more than just hardware settings. An SCP can be as simple as a single attribute, such as changing an iDRAC password or few BIOS settings. Or it can be as complex as any and every setting you can make on a server. An SCP can be expanded to updated firmware. An SCP can even deploy an operating system. Server Configuration Profiles can be created and consumed by the iDRAC9 GUI as well as consoles such as OpenManage Enterprise or Dell integrations with partner consoles such as VMware vCenter or Microsoft System Center.

The iDRAC9 GUI provides very easy to follow steps for exporting and importing a Server Configuration Profile. Server Configuration Profiles can be used by any IT admin - whether you have 5, 50, 500 or more servers. Using a Server Configuration Profile sets up a server quickly and correctly saves time and removes the possibility for human error.
Lesson 1 - iDRAC9 BIOS settings

Lesson 1 - iDRAC9 BIOS settings (10 minutes) - Advanced - View BIOS information while the server is running as well as stage any changes.

There are times when as a server admin, you want to see what the current BIOS settings are but you don’t want to power down the server just to see the attributes. Or, you may be needing to make a change to BIOS settings, but you don’t want to reboot the server at that moment. iDRAC9 offers the option to both view and stage changes to the BIOS – without having to take the server offline and boot to F2.

Navigate to the BIOS Settings tab

From any page, click the "Configuration" tab and then choose the "BIOS Settings" tab

Locate and expand "Processor Settings." Scroll down as needed.
Make changes to any / all of the possible settings. Two possible options are shown below. Next, scroll to the bottom of the section (not the page) and select "apply". Then click "OK" when the success box appears.
Review the column to the right of the current values; this will show all the pending values you have selected.

Explore the other tabs available, and make changes if you wish. When done, scroll to the bottom of the page, and decide when or if you want to apply the changes.

Note that no changes will be made in demo mode.

This concluded the BIOS settings lesson.
Lesson 2 - iDRAC9 Alerts

Lesson 2 - iDRAC Alerts (10 minutes) - Advanced - Understand how to set and view alerts.

The iDRAC9 offers two ways to configure alerts. You can choose from a few categories, or make very granular choices; whichever suits your needs.

Note that alerts are not set up by default. But with a few clicks and defining destination options like an SNMP trap location, you can be done in minutes. Simply navigate to the "Systems Settings" page, and expand the "Alert Configuration" section. The new Quick Alert Configuration box appears. Three options to configure – which categories, what severity, and where to send alerts. It’s that easy. Plus, the Alerts Configuration Summary gives you a very quick, easy to see list of what alerts have been set.

Navigate to the Alerts tab

From any screen, select "Configuration" and then "System Settings" and the "Alerts" is the first option.

Note that for new servers from the factory, alerts have not been enabled. Move the slider to toggle alerts on/off. Notice that this server however *does* have alerts enabled.
Review the "Alerts Configuration" Summary. These are alerts currently set for the server. You can scroll through each category - Critical, Warning, and Informational.

Now review the "Quick Alert Configuration" option. This is a great way to choose the alerts you want with just a few mouse clicks.

Next, make changes to the alerts. If you only care about critical and warning events, and only for system and storage, you would make the following selections. Next choose how you want to receive notifications; for example Redfish Events and SNMP alerts. Note that "Apply" does not functional in demo mode. Click "Discard" to continue.
If a more granular selection of alerts is required, choose the standard “Alert Configuration” option. This tab allows you to choose a wide variety of options in regards to what alerts are sent, and how they are sent.

This concludes the Alerts section.
Lesson 3 - iDRAC9 Server Configuration Profile

Lesson 3 - iDRAC Server Configuration Profile (10 minutes) - Advanced - How to create, export, and import a custom-tailored template of a server for various uses.

Setting up a server “just the way you want it” takes time. And if you want several servers to be set up the same way – 3 servers, 300, or even 3000 – iDRAC provides a quick and simple way to “copy and paste” all the settings from one server to another. Server Configuration Profiles have been in use since the 12th generation of PowerEdge Servers. With iDRAC9, importing and exporting a server configuration profile is as simple as a few mouse clicks.

Admins can export a Server Configuration Profile to a location of their choice, and import that profile 1 by 1, or use tools such as OpenManage Enterprise or scripting tools like Racadm or the RESTful API Redfish to install on as many servers as they wish.

Navigate to the Server Configuration Profile tab

From any page, click on "Configuration" and then "Server Configuration Profile"

Expand the "Export" tab

Here, you can choose **where** you want your profile stored, and give it a **name**. Next, select what **items** you want to be part of your profile. Remember, the Server Configuration Profile can include any/all...
settings and passwords, or it can be limited. An example of a limited profile would be changing the iDRAC password for all the iDRACs in the datacenter.

Next choice to make is the type of file you want. The blue "i" provides a quick overview of the choices. Some of the settings in a profile are classified as "destructive" - meaning these settings will override any previous settings. However, if you are creating a "clone" template to set up bare metal servers, this is helpful to ensure all settings are set the way you want them.

Then choose the format you prefer -- JSON or XML - as you can edit profiles as needed once you create one. Also note that any passwords part of the profile will be shown in plain text. Acceptable in test/dev labs, but if the profile will be used for production systems and will be stored on a share, security best practices would be to check the "Password Hash Values" box to ensure that passwords are hashed and unreadable in the profile.

Normally, the next step would be to click "Export" and your Server Configuration Profile would be ready to use. You could then go to another server of the same model & components and "Import" the file and reboot the server.

However, the "Export" is not available in demo mode. If you do click "Export" you will get the RAC0508 error as noted at the beginning.
Next, navigate away from the "Export" tab by clicking "Custom Defaults."

An alert will appear. This helps prevent leaving any pending changes in limbo should you accidentally move to another section or page before committing the changes. For this exercise, select "Discard."

When the warning is gone, you will see the "Custom Defaults" tab. This can be a custom Server Configuration Profile. Otherwise, you can use the option to "Reset to Factory Defaults" as discussed in Maintenance > Diagnostics.
Now that you've made an SCP, you can now use it as a template for other like servers. Or, you can use the profile on the same server - perhaps some random changes were made in a dev/test environment, and you wanted to get back to your starting point. From the "Configuration" page, click on "Import."

The rest is basically the same steps as Export, but with the added step for shut down, so that the changes can be applied.

Server Configuration Profiles can be exported and imported using the GUI, Racadm, Redfish, OpenManage Enterprise, and any combination of these.

This concludes the SCP lesson.
Lesson 4 - iDRAC9 Virtual Console options

Lesson 4 - iDRAC9 Virtual Console options (10 minutes) - Advanced - Explore and understand the various options for access to the Virtual Console.

One of the key features for iDRAC Enterprise and Datacenter is the option to remotely access the operating system of a server using the Virtual Console. For many years, users were required to choose between ActiveX or Java to connect to the virtual console. In the spring of 2016, iDRAC introduced the option of HTML5 as a means to access the virtual console. iDRAC 7.00 firmware no longer offers Java or ActiveX as an option to access virtual console or connect virtual media. Instead, iDRAC9 uses "enhanced HTML5" or "eHTML5." Code has been optimized for security and speed.

The HTML5 access version of the virtual console is full featured, but cannot be accessed in demo mode. For more information on virtual center, see the iDRAC9 Interactive demo.

Navigate to the Virtual Console tab

From any page, click on "Configuration" and then "Virtual Console"

View the various options on the page. Note the multiple security related options.
This is the end of the vConsole session. See the iDRAC9 Interactive Demo for more information.
Module 2 Conclusion

Congratulations on completing Module 2.

In Lesson 1 - BIOS Settings

• You were shown the option to view the server BIOS settings in real time while the server was up and running.
• You made configuration changes, took notice of the pending changes, and shown how to commit changes.

In Lesson 2 - Alerts

• You first navigated to the Alerts page, enabled alerts, and the reviewed the Quick Alerts options.
• You also looked at the more detailed options to configure alerts.

In Lesson 3 - Server Configuration Profile

• You were shown how to create, save, and import a server configuration. This template, known as a Server Configuration Profile (SCP) can exported and imported in the GUI. For larger scale, this template can be used in consoles such as OpenManage Enterprise, or can be selected for use by Command Line tools such as Racadm or the RESTful API Redfish.

In Lesson 4 - Virtual Console

• You learned about the eHTML5 access to the virtual console for faster, more secure connectivity. For more details on vConsole, see the iDRAC9 Interactive Demo.

For additional information on iDRAC9, please see the “white papers” tab at www.dell.com/support/idrac
Module 3 - iDRAC9 Security
Module 3 - iDRAC9 Security

Module 3 - iDRAC Security (30 minutes) - Advanced

This module will provide an overview of the various security options and settings available. These settings will help you better control access to your iDRAC in terms of users, control points, and other security "best practices" for your iDRAC.

NOTE: Check out the iDRAC9 Security Configuration Guide on www.dell.com/idracmanuals. It has an extensive overview of many of the security best practices available in iDRAC9.

This module contains the following lessons:

- Lesson 1 - System Lockdown Mode
  - How to enable System Lockdown mode, and the effects and benefits of doing so

- Lesson 2 - Web Security settings
  - How and why to select advanced security settings to access the iDRAC, including RSA SecurID

- Lesson 3 - iDRAC Settings
  - Understanding the configuration options for connectivity, services such as AD/LDAP, users, and the iDRAC Connection View
There are many security features in iDRAC that go unused by IT admins. Dell has consolidated these "best practices" in one paper - the iDRAC9 Security Configuration Guide. To access the guide, start at www.dell.com/idracmanuals. It covers the following features, plus many more.

System Lockdown Mode

- iDRAC9 allows IT Admins to quickly restrict users from making any configuration changes to the server. This feature provides IT admins with an added level of security. While the server is in System Lockdown mode, no configuration changes can be made via the iDRAC. This includes CLI tools such as Racadm, RESTful APIs like Redfish, BIOS, and consoles such as OpenManage Enterprise.

Web Security settings

- The iDRAC9 is built on SELinux, and continually adds new security features. iDRAC9 offers several security features not available from other vendors, such as the ability to select and limit the ciphers negotiated by iDRAC. This and other security control options -- 2FA/MFA, Active Directory/LDAP, RSA SecurID integration, and other options like IP Range blocking -- result in tighter security when it comes to interacting with your iDRAC.

iDRAC settings

- This tab has many options to help you fine tune the access to your iDRAC. In addition, this page has a feature no other remote access controller offers - iDRAC9's "Connection View." Connection View provides you with the MAC address of the port, as well as the switch, to which the iDRAC is connected. Connection View also provides the same information for select LOM's and PCIe cards. This saves you from having to make a trip to the hot aisle of the datacenter to see if a server is connected as planned.
Lesson 1 - iDRAC9 System Lockdown mode

Lesson 1 - iDRAC System Lockdown mode (10 minutes) - Advanced - How and why to select many of the advanced security settings, including access to the iDRAC.

Prevent changes to your server with one click by enabling System Lockdown mode. System Lockdown mode is a feature of iDRAC Enterprise or Datacenter, and requires the user to have "Administrator" privileges. To put it simply, System Lockdown mode prevents server configuration changes. This will prevent any changes to the server, such as Dell updates, BIOS changes, and much more.

iDRAC9 System Lockdown is dynamic - there is no need to reboot the server to enable and disable this feature. Other competitors force you to power down the system to enable/disable this feature. This adds time/risk that many IT admins cannot afford.

System Lockdown mode prevents configuration "drift" from multiple interfaces such as the GUI, consoles like OpenManage Enterprise, and commands from Racadm or the RESTful API Redfish.

Note that while a server is in System Lockdown mode, the server can still be powered on/off, and storage can be added or removed, as these are not considered "configuration" changes.

System Lockdown Mode can be enabled/disabled 2 ways. One is via the Dashboard, and the other is via the icon in the header bar at the top of every page. System Lockdown can also be enabled using command line tools like Redfish and Racadm.

Again, it is key to note that it is possible to enable and disable System Lockdown mode without having to halt server operations. This allows IT admins to "bookend" scripts with 'unlock' and 'lock' when applying updates for example.

Navigate to the Dashboard

From any page, click on "Dashboard"

Under the "More Actions" tab, click on "Turn on System Lockdown Mode"
Once enabled, a gold banner will appear at the top of the page.

The warning banner will clear after five (5) seconds. At that time, the lock icon in the top right will change from 'open' to 'closed' and change from white to yellow. At this point, no configuration changes can be made to the system and the 'lock' icon in the top right side of the header is now "locked" and gold.

Navigate to the BIOS Settings page (Configuration > BIOS Settings.) As you navigate between tabs you will notice the gold bar reminder that the system is in lockdown mode. Next, expand the tab for "Processor settings" and see that all of the settings are greyed out and no longer configurable.
To disable System Lockdown mode, you have two choices. One is to return to the Dashboard tab, and under "More Actions" click on "Turn off System Lockdown mode." Or, for this exercise, go to the header bar at the top and click on the gold "lock". Then click the 'disable' option. Notice that the lock will turn white and be in the open position.

Now, all the options under "Processor Settings" can be modified.
System Lockdown can be enabled/disabled in the UI, as well as command line tools such as Racadm or Redfish.

This concludes the lesson on System Lockdown.
Lesson 2 - iDRAC9 Settings and Security

Secure remote access to the server is every bit as important as secure physical access to the server. Every iDRAC offers a wide variety of security controls, and iDRAC9 Enterprise/Datacenter offer additional tools such as integrating with Microsoft’s Active Directory as well as LDAP.

Navigate to the iDRAC Settings tab

From any page, click on "iDRAC Settings"

Another feature unique to iDRAC9 is "Connection View"

Once enabled, iDRAC will make an LLDP call to the top of rack switch, and will display the port and switch information. LLDP must be configured on the switch.
Also, certain LOM and PCIe NIC’s will also display Connection View information; this can be found in the tab System > Network Devices.

Connection view details can also be retrieved via Racadm commands.

An additional step to increase security and limit access to the iDRAC can be done by enabling IP range blocking and adjusting log in attempts to mitigate against DoS attacks.

To access this information, click on "Connectivity" then "Network" and then "Advanced Network Settings"

In the Advanced Network Settings tab, you’ll see 4 key options: IP Ranges, IP blocking, 802.1x Security, and Federal Information Processing Standards (FIPS.)

The first option, IP Ranges, allows admins to set up to five IP ranges to restrict the incoming access points into the iDRAC.

IP Blocking allows you to customize fail counts and "lockout time" for failed attempts.

802.1x provides new security certificate options; FIPS is often used by US Federal customers.
Options can be found in the “?” in the upper right corner.

Take a moment to expand each of these sections.

![Advanced Network Settings]

One critical task is setting up User accounts to access iDRAC. Not just who can access, but what tasks they can perform once logged in.

To add/delete users, change passwords or privileges, navigate to the "Users" tab and expand "Local Users." Take a few moments to explore the Local Users tab. Note that no changes will be saved while in demo mode.

![iDRAC Settings]

Next, expand the "Directory Services" tab. If you use either the Microsoft Active Directory or the LDAP Directory Service software, you can configure the software to provide access to iDRAC. This allows you to add and control the iDRAC user privileges to your existing users in your directory service.

Active Directory and LDAP features are available with either the iDRAC Enterprise or Datacenter license.

Click on "Edit" to edit domain information and other items such as Extended Schema settings; hit "close" to return to the previous screen.
This will open a 4-step wizard to configure Active Directory. Click "Next" or "Close" to return.

Now, expand the "Global User Settings" and the "Password Settings" tab. The 'Default Password Warning' will suppress the warning on the log in page if your server was ordered with 'calvin' from the factory. 'Policy Settings' allows you to choose the strength variables for your passwords. See the "?" icon in the top right for more details and suggestions.
For those customers who are using RSA SecurID in their environment, the iDRAC9 Datacenter license provides a simple means to set up this solution. RSA SecurID is a two-factor authentication (2FA) technology. RSA SecurID can be used on local users, and Active Directory and LDAP users. To view and configure RSA SecurID, navigate to "Settings" and expand "RSA SecurID Configuration."

In this section, you can view, upload, and test RSA SecurID settings.
This concludes the iDRAC Security and Settings.
Lesson 3 - iDRAC9 Web Security

Lesson 3 - iDRAC9 Web Security Settings (10 minutes) - Advanced - How and why to select advanced web security settings to access the iDRAC

Web based attacks are a common datacenter concern, and iDRAC9 has many settings to further control web access parameters to help mitigate security risks.

iDRAC7/8/9 is the only solution which offers the option to further control access by limiting the ciphers negotiated by iDRAC.

Navigate to the Web Server tab

From any page, click "iDRAC Settings" then "Services" and then "Web Server" and expand "Settings"

iDRAC9 offers a plethora of editable fields such as number of sessions, timeout limits that the amount of time a session can remain idle. HTTP/s port numbers are also configurable to provide additional levels of security.
The next area to review are encryption bit strength and TLS settings. By increasing these to the maximum settings, only most secure ciphers and the highest level of encryption between the server and the client are enforced. Dell Security best practices recommend keeping SSL Encryption to "256-Bit or higher", and changing the TLS protocol to "TLS 1.3 only." TLS 1.3 offers faster handshakes and fewer ciphers.

However, for some datacenters may not have adopted the full TLS 1.3 solution, but still need more security with TLS 1.2. iDRAC offers the option to remove or allow only specific cipher suites. Using OpenSSL Cipher String Syntax, IT admins can pare down even further the ciphers negotiated by iDRAC. Click "Set Cipher String" to view screen.

After reviewing the information, click "cancel" to return to the previous screen.
This is the end of the iDRAC9 web security lesson.
Module 3 Conclusion

Congratulations on completing Module 3.

In this module, you explored several security features of iDRAC9. You were able to quickly place a server in configuration lockdown, and were shown the Connection View information about the switch and port to which iDRAC is connected. You reviewed ways to integrate various user control tools such as AD, LDAP, and RSA SecurID. You also reviewed the options that provide tighter controls over the ciphers allowed to communicate with the iDRAC.

For additional information on iDRAC9, please see the “Security Configuration Guide” at www.dell.com/idracmanuals
Module 4 - iDRAC9
Datacenter
Module 4 - iDRAC9 Datacenter

Module 4 - iDRAC Datacenter (10 minutes) - Advanced - This module will provide an overview of the various features available only with the iDRAC9 Datacenter license. The Datacenter license is an upsell license that has all the advantages and features of iDRAC Enterprise, plus several other features that can help drive datacenter efficiencies.

This module contains the following lessons:

1. Lesson 1 - Telemetry Streaming
   1. Where to view which reports and settings for Telemetry Streaming have been set via Racadm or Redfish.

2. Lesson 2 - Multi Vector Cooling
   1. How and why to select advanced cooling settings for the server.

3. Lesson 3 - Automatic Certificate Enrollment
   1. How to set up your iDRAC9 to connect to your CA server to obtain a new certificate, as well as a renewal when the existing license expires.
iDRAC9 Datacenter / Did you Know?

Telemetry Streaming

• iDRAC9 Datacenter provides IT managers the option to integrate advanced server hardware operation telemetry into their existing analytics solutions like Splunk or ELK Stack. Telemetry is provided as granular, time-series data that is continually streamed, compared to inefficient, legacy polling methods. The advanced agent-free architecture in iDRAC9 provides over 180 data metrics that are related to server and peripherals operations. Metrics are precisely timestamped and internally buffered to allow highly efficient data stream collection and processing with minimal network loading. This comprehensive telemetry can be fed into analytics tools to predict failure events, optimize server operation, and enhance cyber resiliency.

Multi Vector Cooling

• With increasing server densities and the desire to maximize compute power per unit area at the datacenter level, there is an increasing need for better telemetry and controls related to power and thermals to manage and optimize data center efficiency.
• Multi Vector Cooling, part of the iDRAC Datacenter license, provides key thermal controls that facilitate deployment and customization challenges.

iDRAC9 Automatic Certificate Enrollment

• Previously, creating and renewing iDRAC SSL/TLS certificates required a mostly manual, time-consuming effort. Monitoring approaching expiration dates and arranging for new certificates to be generated from a CA authority is just one aspect. IT admins then had to update scripts to deploy the certificates to embedded devices like the iDRAC.
• This feature can be used not only to renew existing iDRAC SSL/TLS certificates but also installs TLS certificates on bare-metal servers. The new certificates can be generated from a CA authority.
Lesson 1 - iDRAC9 Datacenter Telemetry Streaming

Lesson 1 - iDRAC9 Datacenter Telemetry Streaming (10 minutes) - Advanced - How to view Telemetry Streaming reports previously set by Racadm or Redfish commands.

Beginning with iDRAC9 firmware 4.00 and forward, you can have iDRAC9 stream 2.9 million data points every day to the ingress tools such as Splunk or ELK Stack. All reports are DMTF Redfish compliant, and all settings can be done either via Racadm or Redfish commands.

Some of the metrics iDRAC9 can provide telemetry metrics are:

- CPU performance
- Memory statistics
- Storage Drive SMART logs
- Sensors: voltage, temp, power, connectivity, intrusion
- GPU and FPGA statistics
- Much more!

Combine the data from the hardware with any OS/application data to better understand the cause/effect to optimize performance. Or track performance or hardware irregularities before they become an issue.

Navigate to the Telemetry Streaming tab

To see if Telemetry Streaming is enabled, or to view the reports selected, select "Configuration" then "System Settings", then "Telemetry Configuration" and open the "Telemetry Streaming" tab.

"Telemetry Data Stream" allows the iDRAC to send (stream) data. If needed for troubleshooting purposes, data streaming can be disabled.

It is possible to configure two Remote Syslog (RSyslog) servers to receive data. The "Telemetry Subscriptions" are read only fields. Click the "?" icon in the top right corner for "Help" on this topic.
Next, scroll down and click on the "Metric Report Definition." Metric Reports Definitions can be imported/exported as needed and can be included in a Server Configuration Profile (SCP). Use the "scroll bar" to move see the full list of available metric reports. Expand the section "CPUMemMetrics"

Review the various metric in this report. Then, expand the "Actions" tab and click "Edit Report Properties."
Note the many different options available to get the data you need at a frequency that best suits your business needs. When done, click "Cancel." Note, the "Save" option is not available in Demo mode.

Next scroll down and open the "Triggers" tab. Triggers allow you to dictate when a report is sent. A report can be send continually, or it can be sent only if an event ‘triggers’ the report. And like the Metric Reports, Triggers can get exported/imported with the Server Configuration Profile. Telemetry triggers are a means to generate and stream reports that are based on an error or warning condition. These reports are predefined based on Lifecycle Log events for error or warming conditions. If
configured, a new report is generated before the scheduled report interval when a trigger occurs. The default configuration includes the triggers that are relevant for a report. You can modify the trigger association. “Linked MRD” shows the associated Metric Report Definition.

![Image of Triggers interface]

As you can see, iDRAC9 offers a wide range of detail and options to fine tune data coming from the iDRAC to the ingress tool of your choice. See www.dell.com/support/idrac for white papers and videos on all aspects of Telemetry Streaming with iDRAC9 Datacenter. Telemetry Streaming can be configured by the GUI as well using tools such as Racadm and Redfish.

This ends the Telemetry Streaming lesson.
Lesson 2 - iDRAC9 Datacenter Multi Vector Cooling

Lesson 2 - iDRAC9 Datacenter Multi Vector Cooling (10 minutes) - Advanced - How and why to select settings to better control airflow, cooling and overall power consumption in the datacenter via granular controls available via Multi Vector Cooling.

Multi Vector Cooling allows customers to customize the thermal operation of their PowerEdge servers with the following benefits:

- Optimize server-related power and cooling efficiencies across their datacenters.
- Integrates seamlessly with OpenManage Enterprise Power Manager for optimized management experience.
- Provides a state-of-the-art PCIe cooling management dashboard

Navigate to the iDRAC Cooling Configuration page

From any page, click on "Configuration" and "System Settings". Then, expand "Hardware Settings" and "Cooling Configuration"

Take a moment to explore the detailed information on this page. You can hover over the "i" icons for more information. See drop down options as well. iDRAC9 offers a 'Sound Cap' option as a Thermal Profile which can be used to limit an acoustic profile, but this has an impact on performance.
Remember to click the "?" help icon in the tool bar at the top right for additional information for items on this page.

Scroll down to the section "**PCIe Airflow Settings.**" These settings control the airflow over a specific PCIe slot. iDRAC will default to the 'automatic' settings for the device in the PCIe slot. However, there are times when the airflow (measured in Linear Feet per Minute, or LFM) needs to be adjusted to allow for custom cooling based on usage.

To modify these settings, change the LFM Mode from "Automatic" to "Custom" and modify the LFM. This setting is useful when increased thermal margin is wanted for custom high-power PCIe cards. Only third-party PCIe cards can be customized for reduce, or increased fan speeds based on your requirement. Note that this feature is not available in Demo mode.
This is the end of the Multi Vector Cooling lesson.
Lesson 3 - iDRAC9 Datacenter Automatic Certificate Enrollment

Lesson 3 - iDRAC9 Datacenter Automatic Certificate Enrollment (5 minutes) - Advanced - How to configure iDRAC9 to access initial and subsequent access to the CA server.

iDRAC9 Datacenter license offers a fully automated process for iDRAC SSL certificate enrollment and renewal. Previously, tracking iDRAC SSL certificates meant a lot of administration overhead -- maintaining spreadsheets, setting reminders, or regularly checking the certificate authority. With iDRAC9 Datacenter, all of these tasks are automated.

This feature can be configured in the GUI, via Racadm, and once set, can be configured as part of the Server Configuration Profile (SCP). This lesson will show the options to configure via the GUI.

Navigate to the SSL Certificate tab

From any page, click "iDRAC Settings", "Services", "Web Server", and expand the "SSL/TLS Certificate Signing Request" tab.

On this tab you will see two options - one for the manual process to request and download a Certificate Signing Request (CSR) and one for the Automatic Certificate Enrollment. For servers without the Datacenter license, only the manual option is available. You would be required to fill out the required information, generate, and then upload the CSR.

First, enable "Automatic Certificate Enrollment." Mouse over the "i" icon to review the information and options. Starting with 7.00, users can choose to use ACME or SCEP protocol. Next, you would
choose the enrollment action and enter the address of the CA servers. However, this feature is not available in demo mode. When finished, click the 'discard' option.

But if the process does complete, the iDRAC is now connected to the CA server. So when the current CSR expires, the iDRAC will automatically contact the CA server for a new license.

For more information on automatic certificate enrollment, see the white papers at www.dell.com/support/idrac.

This completes the lesson on Automatic Certificate Enrollment.
Module 4 Conclusion

Congratulations on completing Module 4.

In this module, you explored several features included in iDRAC9 Datacenter. You learned how to view settings and wide variety of reports for Telemetry Streaming, how to configure advanced cooling option in Multi Vector Cooling, and how to "set and forget" iDRAC SSL certificates via Automatic Certificate Enrollment.

For additional information on iDRAC9, see the “white papers” at www.dell.com/support/drac

For a 30 day eval license of iDRAC9 Datacenter, visit the Trial License page

https://www.dell.com/support/kbdoc/000176472/
Module 5 - iDRAC9 RedFish
Module 5 – iDRAC9 Redfish

Module 5 – iDRAC9 Redfish (10 minutes) - Advanced - This module will provide an overview of the Redfish URIs and various operations - GET (read), PATCH update), POST (create/action).

According to the DMTF, Redfish® is a standard designed to deliver simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). Both human readable and machine capable, Redfish leverages common Internet and web services standards to expose information directly to the modern tool chain.

Redfish requests can be carried out using any API platforms such as Postman or Talend API tester. For this lab, you will use the Talend API tester (Chrome extension) to invoke, discover, and test REST APIs. This module contains the following lessons:

Lesson 1 - Redfish GET requests

• How to perform GET operation on Redfish URIs
  • GET allows you to retrieve information, such as users, passwords, hardware inventory, and more

Lesson 2 - Redfish PATCH requests

• How to perform PATCH operation on Redfish URIs
  • PATCH is always for updating a existing resource, such as updating a password

Lesson 3 - Redfish POST requests

• How to perform POST operation on Redfish URIs
  • POST is always for creating a resource (does not matter if it was duplicated) such as adding an entirely new parameter suite or feature set
iDRAC9 Redfish / Did you Know?

Redfish is a standard that uses RESTful interface semantics to access a schema based data model to conduct management operations.

- It is suitable for a wide range of devices, from stand-alone servers, to composable infrastructures, and to large-scale cloud environments.
- The initial Redfish scope targeted servers. DMTF and its alliance partners expanded that scope to cover most data center IT equipment and other solutions, and both in- and out-of-band access methods.
- Redfish is easy to use (human readable format versus the IPMI hexadecimal format).
- Inherently more secure than IPMI as it uses HTTPs connections.
- Dell offers a comprehensive API spec for a wide variety of Dell and EMC solutions at https://developer.dell.com
Lesson 1 – Redfish GET requests

Lesson 1 - iDRAC9 Redfish GET operations (10 minutes) - Advanced - How to perform GET operations on Redfish URIs

Let’s say you want to find out basic information on the system set up. In Redfish terms, to find this information you’ll use the “Get” command.

The GET operation retrieves resources from a Redfish service. Clients make a GET request to the individual resource URI.

The root URL for Redfish services is /redfish/v1/.

For the demo, you’ll be using an API tester. The API tester is pre-loaded in the browser; click on "second tab."

Note: If you do go back to the iDRAC tab, you will need to log in again with root/calvin.

GET request on root URI

In order to perform GET operation on root URI, choose GET as a method and type basic URI i.e to get started. The URI along with status code will appear on left panel to traverse through the history.

Note: In demo mode, authentication credentials are not used. They are required in a normal environment.

First, click on "GET request for root URI" and click "Open Request"
Click on **Send** to observe the output of retrieving the resources from Redfish client. Next, view the information. Explore the various options on the page.

When finished viewing, click **“Get request for Account Service URI”**

Follow the same steps as before to see the information about "Account Service."
When finished viewing, click "Get request for Chassis URI"

Follow the same steps as before to see the information about the chassis.
This concludes the lesson on Redfish "GET" commands.
Lesson 2 – Redfish PATCH requests

Lesson 2 - iDRAC9 Redfish PATCH operations (10 minutes) - Advanced

In this lesson, we'll show how to perform PATCH operations using Redfish URIs

To update a resource's properties, use the PATCH method. The request body defines the changes to update one or more properties.

The PATCH request can only make changes to existing properties. To add a new property, you would use POST.

To perform PATCH operations on Redfish URI, you need to first perform GET on a specific URI to obtain the present value for each attribute. Then, use PATCH (update) to change an attribute's value.

For this exercise, we'll toggle the Indicator LED on/off.

Select "GET" as a request with Systems URI, click on "Send" to observe the response obtained from Systems URI. Note the the LED is currently on.

As you can see, the current value is "Lit" but you want to turn it off. To find the allowable values, you could use the Redfish API tool on https://developer.dell.com. Note that this link may not be available in Demo mode.

From this home page, you would select "Explore APIs"
Then, you would select “Servers” and “iDRAC9 Redfish API”

Then you would find the Chassis / Chassis Settings Instance

Next, you’d scroll down to see the entry for “indicatorLED” and to right, hover over “more” to see the valid options.

Now, choose "PATCH" as a method. For this demo, the field has been pre-populated with the new parameter from off. Click "Send" to post.
To see the change in attribute's value after PATCH operation, perform "GET" operation on the same URI. You can now see the value has changed from "lit" to "off."

This is the end of the PATCH lesson.
Lesson 3 – Redfish POST requests

Lesson 3 - iDRAC9 Redfish POST operations (10 minutes) - Advanced

In this lesson, you’ll see how to use Redfish POST requests. There are 2 basic types of POST requests:

- POST (create) : To create a resource, services support the POST method on resource collections.
- POST (action) : To request actions on an existing resource, send the HTTP POST method to the URI of the action.

The URI of the action is in the format: <ResourceURI>/Actions/<QualifiedActionName> :

- <ResourceURI> is the URI of the resource that supports the action.
- Actions is the name of the property that contains the actions for a resource.
- <QualifiedActionName> is the qualified name of the action and includes the resource type.

To start, click "POST (create) request on AccountService URI" under Redfish POST requests.

Then, choose "GET", click "Send"
Take a look at the Session Count. In the demo GET command, the session count was 3, as shown below. The session count with POST is much higher.

To see the UserName and Password provided while performing a POST operation, you first need to click on the session links in the response. For this demo, click on "Session 2"

Then, perform a "GET" operation on that link by clicking on "Send."

The link provides the details of newly created user with specific UserName and Password.
Next, let's take a look at a POST (action) command. In this exercise, you will be changing the power state of the server. Note that in demo mode, no action will be taken. Click "POST (action) request on Systems URI"

Click on "Send" to see the response from Redfish client.
To see the possible values for changing power state, expand the section. Simply view the possible choices. If you were to make changes, it would follow the same process as PATCH. But since this changes the state for multiple parameters, this is a POST job.

This concludes the lesson on Redfish "POST" commands.
Module 5 – Conclusion

Congratulations on completing Module 5.

In this module, you explored few Redfish RESTful API operations such as GET, PATCH, and POST.

- GET operation is used to retrieve resources from a Redfish service.
- To create or request actions on a resource, PATCH operation is suggested.
- To update a resource's properties, POST operation is performed.

Redfish is a powerful API that let's you take full advantage of all iDRAC capabilities.

For more information on Redfish on Dell and EMC, see https://developer.dell.com
Conclusion
Conclusion

This lab was designed to provide some basic hands-on experience using the iDRAC9, firmware 7.00.00.00 and higher. It covered many of the basic tasks to automate your daily server management tasks. iDRAC9 can perform end to end server lifecycle management, including monitoring, updates, configuration and bare-metal deployment.

For additional documentation, manuals, and white papers on iDRAC9 visit www.dell.com/support/idrac