Behind the Report:

Dell Technologies vs. HPE: Who Leads in Server Management?

This methodology report outlines Prowess Consulting's approach to comparing server management features and tools for security, ease-of-use, analytics, and sustainability metrics between Dell™ and HPE® servers.

Methodology Overview

Prowess Consulting's engineers utilized systems in a lab to compare and validate claims in our **technical research report** regarding server management features. For our testing, we compared features and tools for Integrated Dell™ Remote Access Controller 10 (iDRAC10) and HPE® Integrated Lights-Out (iLO) 7. We also compared Dell™ OpenManage™ Enterprise (OME) to HPE® OneView, in addition to comparing Dell™ AIOps with HPE® Compute Ops Management (COM).

Our comparisons focused on assessing security, ease of use, and analytics features and obtaining sustainability metrics. This methodology document is organized by server management interface, as shown in Table 1. Each section contains steps for validating specific feature claims.

Table 1 | Summary of Dell Technologies and HPE server management tools

	Dell Technologies	HPE
Embedded/remote server management	Integrated Dell™ Remote Access Controller 10 (iDRAC10)	HPE® Integrated Lights-Out (iLO) 7
One-to-many device management console	Dell™ OpenManage™ Enterprise (OME)	HPE® OneView
Cloud-based monitoring	Dell™ Artificial Intelligence for IT Operations (Dell™ AIOps)	HPE® Compute Ops Management (COM)

Verifying iDRAC/HPE® iLO Claims

This section outlines the steps taken to verify individual claims relating to the iDRAC10 and iLO 7 systems. The starting point for each procedure assumes that the user is currently logged in to the respective interface.

Dynamic Front USB

This section outlines the steps taken to change the enabled or disabled status of the front USB ports on a server, including the number of clicks and the time required to complete these processes.

iDRAC Steps

1. From the left-hand menu, select **Configuration**.
2. Select **System Settings**.
3. Click the **Hardware Settings** tab.
4. Click the **Front Ports** tab.
5. In the **Front USB Port** dropdown, select either **Enable** or **Disable**.
6. Click **Apply**.
7. Click **OK** to confirm the change.

iLO Steps

1. From the left-hand menu, select **Host**.
2. On the resulting page, click the tile for **BIOS**.
3. In the search field, enter **USB**.
4. From the resulting options, click the **USB control** dropdown.
5. Click the new choice:
   a. **All USB Ports Enabled**
   b. **All USB Ports Disabled**
   c. **External USB Ports Disabled**
6. Click **Save Draft**.
7. Click **Review Draft and Apply**.
8. Note that the change to be made is correct, and then select the **Apply and Reboot Now** radial option choice.
9. Click **Yes Proceed**.
10. Wait while the system reboots and applies the configuration change.
11. Optionally, open an HTML console to monitor the progress of the feature application and reboot processes.

System Lockdown

This section outlines the steps taken to enable the system lockdown mode. This assumes that the user has access to the iDRAC system and that the password fingerprint has already been created for the iLO system. The click counts and timings are measured from live system to live system for this test.

iDRAC Steps

1. In the top right corner, click the **Lock** icon.
2. Select **Enable**.

iLO Steps

1. In the lower left corner, click the **Virtual Console** icon.
2. Click the **Launch** button.
3. In the top right corner, click the **Power** icon.
4. Select **Reset**.
5. Click **Confirm Reset**.
6. Observe system POST and press **F9** to enter the BIOS when prompted.
7. Select **System Configuration**.
8. Select **BIOS/Platform Configuration (RBSU)**.
9. Select **Server Security**.
10. Select **Server Configuration Lock Settings**.
11. Select **Server Configuration Lock Options**.
12. Enable **Server configuration lock**.
13. Press **F12** to save and exit.
14. Click **Yes** to confirm the save.
15. Click **Reboot** to confirm the reboot action.
16. Allow the system to reboot.

HTML5 Remote Console

This section outlines the steps taken to compare the various HTML consoles. Each button and menu of the console was explored and documented. The total number of features available was then used as the score.

iDRAC Steps

1. Click the **Virtual console** icon to open the virtual console.
2. Make note of the features available:
    a. **One-time boot device:** Click the **Boot** button, and then choose your desired option for the next system boot device.
    b. **Power controls:** Click the **Power** button, and then choose from **Graceful Shutdown, Power Off System, Reset System (warm boot)**, and **Power Cycle System (cold boot)**.
    c. **Virtual console simultaneous user chat:** Click the **Chat** button to open the chat interface, and then use the text box and **Send** button to send messages.
    d. **Virtual keyboard:** Click the **Keyboard** button to access a full virtual keyboard.
    e. **Alternate keyboard layouts for virtual keyboard:** Click the keyboard selection dropdown in the top left corner to choose from six available formats.
    f. **Screen image capture:** Click the **Screen Capture** button to capture and download a screenshot of the virtual console output.
    g. **Full screen mode:** Click the **Full Screen** button to see the console output on the full screen (this hides virtual console control buttons; press **Esc** to return to the normal view).
    h. **Console Refresh:** Click the **Refresh** button to refresh the virtual console window.
    i. **Disconnect View:** Click the **Disconnect Viewer** button to disconnect the virtual console and close the window.
    j. **Virtual media controls:** Click the **Virtual Media** button to open the virtual media controls window to confirm the following features:
        i. **Connect Virtual ISO Image:** Click the **Connect Virtual Media** button to map a CD/DVD or a removable media device from an .iso file.
        ii. **Map External Device:** Click the **Connect Virtual Media** button, and then select the external device to mount externally bootable devices.
        iii. **Virtual Media Statistics:** Click the **Virtual Media Statistics** tab to view connected virtual media device information and transfer rates.
        iv. **Create ISO from folder:** Click the **Create Image** tab, and then select a folder to upload to generate an .iso file from a folder on the local system.
    k. **Console Controls:** Click the **Console Controls** button to confirm the following features:
        i. **Keyboard macros:** On the **General** tab, select the key combination via the **Keyboard Macros** dropdown, and then click **Apply** to send the virtual keystrokes.
        ii. **Aspect ratio lock:** On the **General** tab, select the **Maintain** or **Don't maintain** value via the **Aspect Ratio** dropdown, and then click **Apply** to activate the selection
        iii. **Touch mode:** On the **General** tab, select the **Direct** or **Relative** value via the **Touch Mode** dropdown, and then click **Apply** to activate the selection.
        iv. **Virtual Clipboard:** Select the **Virtual Clipboard** tab to access a text box into which data can be pasted and a **Send Clipboard to Host** button.
        v. **KVM Statistics:** Select the **KVM Statistics** tab to view the frame and packet rate, in addition to bandwidth and compression statistics.
        vi. **Video Quality Controls:** Select the **Performance** tab to access a slider to choose between the video quality and speed priority.
        vii. **User List:** Select the **User List** tab to view the users currently connected to the virtual console.

iLO Steps

1. Click the **Virtual Console** icon.
2. Click the **Launch** button.
3. Make note of the features available:
    a. **Power controls:** Click the **Power** icon, and then choose from **Graceful Shutdown, Force Power Off, Reset**, and **Power Cycle**.
    b. **Virtual keyboard:** Access to the Alt, Shift, Ctrl, and Super keys can be found in the lower left-hand corner of the console. Additional keys can be found via the shortcut keys button.
    c. **Alternate Keyboard Layout:** From the dropdown in the lower right corner, select either **EN 101** or **JP 106/109**.
    d. **Screen image capture:** Click the **Capture Screen** button to open a new tab containing an image of the virtual console output.
    e. **Full screen mode:** Click the **Full Screen** button to see the console output on the full screen (this maximizes the window, but controls are still visible; press **Esc** to exit).
    f. **Virtual media controls:** Click the **Virtual Media** icon to access the following features:
        i. **Mount Folder**: Click the **Connect** button next to the mount folder to mount a local folder to the system.
        ii. **Mount Floppy image:** Click the **Connect** button next to **Floppy** to mount an .img file.
        iii. **CD/DVD:** Click the **Connect** button next to the **CD/DVD** option to mount an .iso file.
    g. **Hotkeys keys**: Click the **Hotkeys** button in the lower right to send or modify preset key combinations.
    h. **Aspect ratio lock:** Click the **Lock Aspect Ratio** button to enable or disable the feature.
    i. **Playback recording:** Click **Screen Recording** to start the capture, and then click **Stop Recording** to stop the recording and access the **Save As** dialog.
    j. **Playback prior recordings:** Click the **Play** button and select a previously saved screen recording to play the video in the virtual console window. Click **Stop** and **Exit** to return to the base console window.
    k. **Logout:** Click the **User** icon in the top right, and then select **Logout** to log out of the virtual console and iLO interface.
    l. **System information:** Click the **Information** icon in the top right to view the server and product name, in addition to the iLO firmware, hostname, and time.

Connection View

This section contains the steps used to validate the display of the switch and switch port information.

iDRAC Steps

On iDRAC systems, one can view the link status, but also the link speed, connected switch, and port, on the switch the system is connected to with the following steps:

1. Navigate to **System**.
2. Select **Overview**.
3. Select **Components**.
4. Select **Network Devices**.
5. Select the tab for the network interface controller (NIC) to be viewed.
6. View the row associated with a given port and confirm:
    a. **Link Status**
    b. **Link Speed**
    c. **Connected Switch**
    d. **Connected Switch Port**

iLO Steps

1. Navigate to **Host > Hardware > Network**.
2. In the **Ports** section, view the **Link state**.
3. Confirm that **physical switch wiring info** is not available.

Telemetry Streaming

This section compares platforms that offer sensor data, thermal levels, and log files, which can be streamed into analytics tools and leveraged by AIOps for AI analysis.

iDRAC Steps

1. From the left-hand menu, select **Configuration > System Settings**.
2. From the tabs at the top of the page, select **Telemetry Configuration > Metric Report Definition**.
3. Select each report to view associated metrics.
4. Manually count available reports and metrics.
5. Confirm the presence of:
    a. 32 reports across 12 categories
    b. 230 Dell™ PowerEdge™ server–based metrics

iLO Steps

iLO 7 documentation for Redfish® is not yet public. We used a short script to pull the metric report definitions to validate what was available.

1. From a local windows system (other than the server) that has access to the management network of the system under test, create the following PowerShell® script, replacing “iLO management IP,” “USER NAME,” and “PASSWORD” with their relevant values. (Note: telemetry streaming can be sent to another system, but the management port is not accessible from the public internet.)

```
Sd

$iloIP = “iLO management IP”

$username = “USER NAME”

$password = ‘PASSWORD’

[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]::Tls12

[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}

# Create session

$body = @{“UserName” = $username; “Password” = $password} | ConvertTo-Json

$sessionResponse = Invoke-WebRequest -Uri “https://$iloIP/redfish/v1/SessionService/Sessions/” -Method
POST -Headers @{“Content-Type” = “application/json”} -Body $body -UseBasicParsing

$token = $sessionResponse.Headers[‘X-Auth-Token’]

$headers = @{“X-Auth-Token” = $token}

# Get report definitions

$reportDefs = (Invoke-WebRequest -Uri “https://$iloIP/redfish/v1/TelemetryService/MetricReportDefinitions/”
-Headers $headers -UseBasicParsing).Content | ConvertFrom-Json

# Process each report

$output = @()

foreach ($member in $reportDefs.Members) {

    $report = (Invoke-WebRequest -Uri “https://$iloIP$($member.’@odata.id’)” -Headers $headers
-UseBasicParsing).Content | ConvertFrom-Json

    # Extract metric names from paths

    $metrics = @()

    foreach ($prop in $report.MetricProperties) {

        if ($prop -match ‘#([^/]+)$’) { $metrics += $matches[1] }

        elseif ($prop -match ‘/([^/]+)$’) { $metrics += $matches[1] }

    }
    # Store report data
    $output += “Report: $($report.Id)”
    $output += “Metrics: $($metrics -join ‘, ‘)”
    $output += “”
}
# Save to file
$output | Out-File “ilo_metrics_$(Get-Date -Format ‘yyyyMMdd_HHmmss’).txt”
```

2. Run the freshly created script.
3. Review the resulting **ilo_metrics-date.txt** file.
4. Confirm the presence of:
    a. Six base reports
    b. Three categories (CPU, memory, and power)
    c. 19 unique metrics

Verifying Dell™ OpenManage™ Enterprise and HPE® OneView Claims

This section outlines the steps we took to validate claims related to the OME and OneView interfaces. These steps assume that you are already logged into the respective interface.

Scalability

We verified the maximum number of servers that can be managed via documentation.

OpenManage Enterprise Steps

1. Open the OpenManage Enterprise Support Matrix.
2. Locate Table 2 under **Hardware Requirements**.
3. Identify the **Large Deployment Configuration** row.
4. Confirm support for up to 8,000 devices.

OneView Steps

1. Open the HPE OneView 10.2 Support Matrix.
2. Locate Table 1 under **Server Hardware**.
3. Identify the **Maximum** value in the **Total number of servers’** row.
4. Confirm support for up to 2,500 devices.

Addressing System Alerts

This section outlines the steps we took to validate the actions needed to handle multiple alerting systems.

OpenManage Enterprise Steps

OME allows for configuring an alert policy, which addresses a specific alert and all future occurrences of that alert without further action.

1. In the top menu, click **Alerts**.
2. Click **Alert Policy**.
3. Click the **Create** button.
4. Enter a **Name** for the policy.
5. Enter a **Description** for the policy.
6. Leave the **Enable Policy** box selected.
7. Click **Next**.
8. Select the **Category of Alert** to monitor.
9. Click **Next**.
10. Select **Message IDs** and enter the ID to monitor.
11. Click **Next**.
12. Click **Select Devices**.
13. Specify instances to monitor, and then click **OK**.
14. Click **Next**.
15. Confirm **Active Date Ranges**, and then click **Next**.
16. Specify **Severity** by selecting the relevant checkboxes.
17. Click **Next**.
18. Specify **Action to Take** by selecting the relevant checkboxes.
19. Click **Next**.
20. Review the **Summary** page.
21. Click **Finish**.

OneView Steps

Within the OneView environment, each alert is addressed manually, rather than by a configured policy. Additional alerts require repeating these steps for each alert.

1. Click **Active Alerts** to view current alerts.
2. Select an alert to view its summary.
3. Click **Event Details** to view alert details.
4. Enter a note in the **Notes** field (optional).
5. Click the **Resource Name** to open the instance.
6. On the **Server Hardware** page, click **Actions**.
7. Select the action to perform (for example, **Power off**).

Faster Deployment

This section outlines the steps we took to validate the deployment steps for deploying one or multiple servers.

OpenManage Enterprise Steps

1. Click **Configuration**.
2. Select **Templates**.
3. Select a **Pre-existing Template**.
4. Click **Deploy Template**.
5. Click **Select** to open the server selection window.
6. Choose one or more **System Groups** or **Devices**.
7. Click **OK**.
8. Select the checkbox for **Graceful Reboot Fallback**.
9. Click **Next**.
10. Leave **Boot to Network Settings** as-is, and then click **Next**.
11. Leave **iDRAC Management IP Selection** as-is, and then click **Next**.
12. Leave **Target Attributes** as-is, and then click **Next**.
13. Choose **Run Now** or **Enable Schedule**.
14. Click **Finish**.
15. Click **Yes** to confirm.

OneView Steps

1. In the left-hand menu, expand **Servers**.
2. Select **Server Profile Templates**.
3. Choose a template.
4. Click **Actions**.
5. Select **Create Server Profile**.
6. Enter a **Name** for the server.
7. Enter a **Description** for the server.
8. Select a single server from the hardware search box.
9. Review other settings (no changes needed).
10. Click **Create** + to add an additional server or **Create** if this is the last server being added.
11. Repeat steps 6 through 10 as needed.

Heterogeneous Server Monitoring

This section outlines the steps we took to validate the ability to monitor servers outside of the manufacturer's ecosystem, or the lack thereof.

OpenManage Enterprise Steps

OME supports the discovery and monitoring of third-party servers via the following steps:

1. In the top menu, click **Monitoring**.
2. Click **Discovery**.
3. Click the **Create** button.
4. Enter a **Discovery Job Name**.
5. From the **Device Type** dropdown, select **Server**.
6. In the popup, select **Non-Dell Servers (via OOB)**.
7. Choose one of **HP iLO, Lenovo XClarity,** or **Other**.
8. Click **OK**.
9. Specify **IP/Hostname/Range**.
10. Enter a **Username**.
11. Enter a **Password**.
12. Choose **Run Now** or schedule.
13. Click **Finish**.

OneView Steps

OneView does not currently support monitoring of third-party servers.

1. Export all topics of the OneView User Guide.
2. Navigate to pages 13–16.
3. Review the list of **Explicitly Supported Hardware**.
4. Confirm that **Third-Party Monitoring** is not supported.

Dedicated Mobile App

This section outlines the steps taken to confirm mobile app support. These claims were verified via documentation rather than app installation.

OpenManage Enterprise Steps

1. Refer to the **Dell OpenManage Mobile Support Page**.
2. Confirm support for:
   a. Remote management via console
   b. Direct server access
   c. At-the-server management via Quick Sync
   d. Push notifications
   e. Inventory and alert monitoring
   f. Server provisioning
   g. Event logs
   h. SupportAssist integration
   i. Virtual console access
   j. Script and command-line interface (CLI) support

OneView Steps

1. Review HPE documentation and blog archives.
2. Confirm that OneView 10.2 does not have a mobile administration app.
3. Note that the only older iLO versions that mention apps in their user guides (iLO 3/4/5) are deprecated.

Report Builder with Customization

This section contains the steps we used to validate the report-related claims.

OpenManage Enterprise Steps

1. Click **Monitoring**.
2. Select **Reports**.
3. In the lower right corner, note the number of total reports (51).
4. Click **Create** to build a custom report.
5. Enter a **Name and Description**.
6. Click **Next**.
7. Choose a **Category** and **Device Group**.
8. Select **Columns** from available metrics.
9. Click **Finish** to create the report.
10. Select a built-in or custom report.
11. Choose **Run** to view the report.
12. Click **Download** to download the report.
13. Select from **HTML, CSV, PDF**, or **XLS** formats.

OneView Steps

1. In the left-hand menu, click **Appliance > Reports**.
2. Choose from one of 10 default report types.
3. Click **Actions > Download**.
4. Select **.CSV** or **.XLSX** format.
5. Note the lack of a customizable report option.

Power Usage Metrics

This section outlines the steps we took to validate the power usage metrics available via OpenManage Enterprise and OneView.

OpenManage Enterprise Steps

1. Click the **Devices** tab.
2. Select a device from the list.
3. Click the **Monitoring Metrics** tab.
4. Review metrics displayed:
   a. **Power**
   b. **Thermal**
   c. **Carbon Emission**
   d. **System Usage**
   e. **CPU Utilization**
   f. **Memory Bandwidth Utilization**
   g. **I/O Utilization**
   h. **System Airflow History**
   i. **Overall CPU Power Consumption**
   j. **Overall Memory Power Consumption**
   k. **Fan Power Consumption**
   l. **Storage Power Consumption**
   m. **FPGA Power Consumption**
   n. **Grid A Current**
   o. **Grid B Current**
   p. **System Current**
   q. **Power Supply – Current (PSU)**
   r. **Power Supply – Thermal (PSU)**
   s. **CPU Socket – Thermal**
5. Review the **OpenManage Enterprise user guide**, page 280, for metrics that are supported, but that might not apply to a given system, such as:
   a. GPU statistics
   b. Virtual machine (VM) statistics
   c. Component metrics trends

OneView Steps

1. Under the **Servers** submenu, click **Server Hardware**.
2. Select a server.
3. Click **Utilization** on the right pane.
4. Expand **CPU, Temperature**, or **Power** to view metrics.

Note: Only CPU, power, and temperature metrics are available, with the custom report option consisting of any two specific metrics from those three categories.

Quick Access to Power Manager Data

This section outlines the steps we took to validate the availability of a quick overview of power metric–related data.

OpenManage Enterprise Steps

1. Click the **Power Management** tab.
2. Select **Overview View**.
3. Review dashboard sections:
   a. **Top 10 power offenders**
   b. **Top 10 thermal offenders**
   c. **Idle server count**
   d. **Top 10 underutilized racks by power**
   e. **Top 10 underutilized racks by space**
   f. **Space headroom**
   g. **Power headroom**
   h. **Virtual machine min power**
   i. **Virtual machine group min power**
   j. **Virtual Machine max power**
   k. **Virtual machine group max power**

OneView Steps

We didn't find OneView support for an overview of power management via either the interface or documentation.

Energy Consumption and Carbon Emission Data

This section outlines the steps we took to examine carbon emissions and energy consumption through power usage metrics and analytical data.

OpenManage Enterprise Steps

To enable power monitoring, perform the following steps:

1. Navigate to the **Power Management** tab, and then select **Power Manager Devices**.
2. Select the device or devices to be monitored.
3. Click **Add Device(s)** to add the devices.

To configure carbon emission conversion rates for the local grid, perform the following steps:

1. Navigate to the **Power Management** tab, and then select **Settings**.
2. Click the **Edit** button.
3. Scroll to the **Emission Conversion Factor Rate**, and then specify the specific kgCO$_2$e/kWh.
4. Click **Apply**.

To view the carbon emissions based upon actual usage data, perform the following steps:

1. On the main menu, click the **Devices** tab.
2. Click a specific device.
3. On the **Device details** page, select the **Monitoring Metrics** tab.
4. Carbon statistics can be found in the right-hand column of the **Energy Consumption Cost and Carbon Emission** table.

OneView Steps

We didn't find OneView support for carbon emission metrics or data via either the interface or documentation.

Automated Power and Thermal Management

This section outlines the steps we took to examine power and thermal management policies.

OpenManage Enterprise Steps

1. Navigate to **Power Management > Policies**.
2. Click **Create**.
3. From the **Type** dropdown, choose **Static** (for power) or **Temperature-Triggered** (for thermal).
4. Enter policy name.
5. Enter the policy description.
6. Click **Next**.
7. Click the **Select Group** button (or **Select Device**).
8. Specify the group (or device) to which the policy will apply, and then click **OK**.
9. Click **Next**.
10. Configure **Power Cap** or **Temperature Threshold**.
11. Specify the duration of the policy.
12. Click **Next**.
13. Set **Schedule**.
14. Click **Next**.
15. Review, and then click **Finish**.

OneView Steps

At the OneView level, we didn't find support for power and thermal-based policies via either the OneView interface or documentation.

Power Manager Specific Reports

To validate the power manager–specific report availability, complete the following steps.

OpenManage Enterprise Steps

1. Navigate to the **Monitor** tab, and then select **Reports**.
2. Click **Advanced Filters**.
3. From the **Category** dropdown, select **Power Managed Devices**.
4. Note the presence of 19 reports.
5. From the **Category** dropdown, select **Power Managed Groups**.
6. Note the presence of an additional 8 power manager–specific reports.

OneView Steps

At the OneView level, we didn't find support for power management reporting via either the OneView interface or documentation.

Password Rotation

This section outlines the steps we took when validating password rotation claims.

OpenManage Enterprise

1. From the top menu, click **Application Settings**.
2. Select **Console Preferences**.
3. Expand the **iDRAC Password Management** section.
4. Choose the source of password rotation:
    a. To have the local OpenManage Enterprise instance control password rotation, select the **"Internal OME"** radio button, and then specify the following details:
        i. Select the **Enable** checkbox for password rotation.
        ii. Specify a password rotation schedule.
    b. To integrate with an external server for password rotation management, select the **"External – CyberArk integration"** radio button, and then specify the below details about the external server:
        i. Specify a central server host address and port number.
        ii. Specify the **Application ID** as provided by CyberArk for your account.
        iii. Specify the **Safe** value for your CyberArk configuration.
5. From the **Retrieve credentials by** dropdown, select one of **(ip/fqdn/server tag)** as the method by which iDRAC systems will be identified within the CyberArk system, and then click **Apply** to save the changes.

OneView

OneView lacks an external integration for password rotation.

1. From the left-hand menu, click **Settings.**
2. Select **Security.**
3. Click the **Actions** dropdown, and then select **Edit**.
4. Scroll to the **Managed Device Authentication** section, and then click the **Disabled** button.
5. Note the options for days between rotation and time to complete the rotation, but no external server integration.

Verifying AIOps and Compute Ops Management–Based Claims

This section outlines the process we used to validate claims within the AIOps and Compute Ops Management environments. The following steps assume the user has signed into the relevant dashboard as a starting point.

Performance Reports with Customization

This section outlines the steps we took to validate performance report availability and customizability.

AIOps Steps

1. Review section 8.3 (starting at page 16) of the PowerEdge Metrics in AIOps Observability using OpenManage Enterprise paper to confirm the 12 categories of reports available.
2. Review Appendix D (starting at page 211) of Dell AIOps: A Detailed Review for further information on individual metrics
3. Log in to the AIOps interface.
4. Navigate to the **Reports** section.
5. Click **Create/View My Reports**.
6. Existing reports will be available as tabs across the top of the window, and can be viewed, modified, or copied.
7. To create a new report, click **Create Report**.
8. Click the **Add Content** button.
9. Enter a report **Title**.
10. From the format dropdown, select one of **Anomaly Chart, Line Chart**, or **Table**. Of note, per page 11 of the PowerEdge Metrics in AIOps Observability using OpenManage Enterprise paper, not all metrics are available for each format of report.
11. Click **Next**.
12. From the **Product** dropdown, select **PowerEdge Servers**.
13. From the **Category** dropdown, select the metric category in question, such as **Chassis, CPU, Drives**, or **GPU**.
14. Select the specific components of that category to monitor.
15. Click **Next.**
16. Select the specific metrics of the chosen category to report on.
17. Click the **Add Content** button.
18. Report graphs will be displayed on screen.
19. To save the report data, click the ellipsis and select either **Export PDF** or **Export CSV**.

Compute Ops Management Steps

1. Navigate to the **AI Insights** page.
2. From the **Reports** section, select the **View Report** button in the only available card, **Server hardware inventory**.
3. Use the **Aggregate by** menu to customize views by **Server, Generation, Model, Processor, Memory,** or **Management type** for the on-screen display.
4. To download the report, click **Export Report**.

Performance Metrics with Anomaly Detection

This section outlines the steps we took to validate the anomaly detection reports.

AIOps Steps

1. From the left-hand menu, expand the **Monitor** section.
2. Select **Infrastructure**.
3. From the **Device Type** dropdown, select **Servers > All.**
4. Select a device to view performance metrics.
5. Review eight-plus available metric graphs. (A ninth metric is available if the system has a GPU.)
6. Observe historical seasonality and anomaly highlights for each metric.
7. Click the **Forecast** radial button in the top left to show a forecasted usage chart.

Compute Ops Management Steps

1. In the top menu, click the **AI Insights** button.
2. In the **Server Utilization Insights** card, click the **Explore** button.
3. View metrics for **CPU, Memory Bus, I/O Bus,** and **CPU Interconnect**.
4. Click each metric card to show a graph of the relevant statistic; graphs show high, low, and average utilization.

Cybersecurity and Security Risk-Level Alerts

This section outlines the steps taken to verify the risk alert level view and alert resolution.

AIOps Steps

1. From the left-hand menu, expand the **Cybersecurity** option.
2. Click the **Misconfigurations** option to view all system misconfigurations in a single interface.
3. Optionally, expand an alert to see further details about the misconfiguration.
4. Click a server name to open its cybersecurity page.
5. Select the checkbox next to one or more misconfigurations to correct.
6. Click the **Resolve** button.
7. Review the list of issues to resolve in the side pane, and then click the **Resolve** button.

Compute Ops Management Steps

1. In the top menu, click the **Manage** button.
2. Select the **Group** card to view the group overview.
3. Scroll to the bottom of the page, and then click onto the group name of a group with a “Not compliant” value in the **Compliance** column.
4. From the **Settings and Compliance** section, click the **View Details** link.
5. Click the **Details** link next to the **Not Compliant** row of the **iLO Settings** section.
6. In the **Not compliant servers** section, click a server’s name to view the recommended manual resolution action; for example, “Apply iLO settings for Group Name.” Note the lack of a single click-to-resolve button.
7. To apply the recommended fix, navigate to the **Manage > Groups** page.
8. Click the ellipse next to the group name in question.
9. Click **Apply iLO Settings** to update any servers in that group with the requested settings.

GPU Performance Metrics

This section outlines the steps we took to confirm the presence of GPU performance graphs.

AIOps Steps

1. From the left-hand menu, expand the **Monitor** section.
2. Select **Infrastructure**.
3. From the **Device Type** dropdown, select **Servers > All**.
4. Select a device that has one or more GPUs installed to view performance metrics.
5. Select the **Performance** tab.
6. Look for the **GPU Usage** section.
7. **Note:** The **All GPUs** tab will show one line of utilization per GPU; specific GPU tabs will show usage along with historical seasonality and anomaly indicators.

Compute Ops Management Steps

1. In the top menu, click the **AI Insights** button.
2. In the **Server Utilization Insights** card, click the **Explore** button.
3. Note the lack of GPU-based metrics or statistics.

GPU Utilization Insights

This section outlines the steps we used to confirm the availability of historical GPU metrics in the reporting system.

AIOps Steps

1. Navigate to the **Reports** section.
2. Click **Create/View My Reports**.
3. Existing reports will be available as tabs across the top of the window, and can be viewed, modified, or copied.
4. To use the custom report builder to include GPU metrics, click **Create Report**.
5. Click the **Add Content** button.
6. Enter a report **Title**.
7. From the format dropdown, select one of **Anomaly Chart, Line Chart**, or **Table**. Of note, per page 11 of the **PowerEdge Metrics in AIOps Observability using OpenManage Enterprise** paper, not all metrics are available for each format of report.
8. Click **Next**.
9. From the **Product** dropdown, select **PowerEdge Servers**.
10. From the **Category** dropdown, select **GPU**.
11. Select the specific GPU devices to monitor.
12. Click **Next**.
13. Select the specific GPU metrics to report on.
14. Click the **Add Content** button.
15. Report graphs will be displayed on screen and can also be downloaded.

Compute Ops Steps

At the Compute Ops Management level, we didn't find support for GPU metrics and statistics either via the interface or documentation.

Appendix

For this research and testing, we referenced the following materials:

1. The **iDRAC10 user guide**
2. The **iLO 7 user guide**:
   a. Click the **Save PDF** button.
   b. Select **Export All Content**.
3. The **OpenManage Enterprise 4.5 Support Matrix**
4. **OpenManage Mobile Features**
5. The **HPE OneView 10.2 Support Matrix**:
   a. Click the **Save PDF** button.
   b. Select **Export All Content**.
6. The **OneView user guide**:
   a. Click the **Save PDF** button.
   b. Select **Export All Content**.
7. The **AIOps Observability document**
8. The **AIOps Detailed Review**
9. The **HPE Compute Ops Management** user guide:
   a. Click the **Save PDF** button.
   b. Select **Export All Content**.

Legal Notices and Disclaimers

The analysis in this document was done by Prowess Consulting and commissioned by Dell Technologies.
Results have been simulated and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
Prowess Consulting and the Prowess logo are trademarks of Prowess Consulting, LLC.

Other trademarks are the property of their respective owners.