Behind the Report:

Smarter IT Operations with Dell Technologies Server Management Tools

This document describes the methodology used to compare the server management capabilities of iDRAC10 and OME with Supermicro's native baseboard management controller (BMC), IPMI, and with SSM.

Summary

Prowess Consulting evaluated each platform through hands-on testing in the respective graphical user interfaces (GUIs) and through review of vendor documentation to confirm feature behavior and availability. Testing focused on common administrative tasks that administrators perform through supported management consoles, such as security configuration, system setup, monitoring, and maintenance workflows.

Testing Summary

To ensure consistency and real-world relevance, this study evaluated only features accessible through the GUIs. We did not include capabilities available solely through scripting or command-line access because these workflows require custom development and are not representative of typical day-to-day administrative use.

Table 1 | Server management platforms examined

Feature	Dell Technologies Offering	Supermicro Offering
Embedded/remote server management	Integrated Dell™ Remote Access Controller 10 (iDRAC10)	Supermicro® Intelligent Platform Management Interface 2.0 (IPMI)
One-to-many device management console	Dell OpenManage™ Enterprise (OME)	Supermicro Server Manager (SSM)
Cloud-based monitoring	Dell Artificial Intelligence for IT Operations (AIOps)	*No equivalent*

Embedded/Remote Server Management

This section compares the features and behaviors of the one-to-one, baseboard management controller (BMC)-level offerings. The following steps assume that you have freshly logged in to the management platform in question.

Telemetry Streaming

This section outlines the steps taken to validate the presence of telemetry streaming via the GUI.

iDRAC10 validation steps:

1. To access telemetry streaming details, navigate to **Configuration > System Settings > Telemetry Configuration > Telemetry Streaming**.
2. To enable or disable the feature, use the slider next to **Telemetry**, and then click **Apply**.
3. To review available telemetry reports, select the **Metric Report Definition** tab.
4. To review the metrics of a specific report, from the **Telemetry Reports** section, click a specific report, and then review the **Details** pane on the right side.

IPMI validation steps:

1. After a review of the dashboard, in addition to the user guide, we found no GUI-native remote telemetry streaming support, although support is available via Redfish® endpoints.
2. To review the available metrics, navigate to **https://*<IPMI_IP_Address>*/redfish/v1/TelemetryService/MetricReportDefinitions**.

GPU Metrics and Visibility

This section outlines the steps taken to validate the presence of GPU metrics available via the GUI, according to system documentation.

iDRAC10 validation steps:

1. To access the documentation, download the referenced iDRAC user guide.
2. To enable asset tracking, navigate to **Configuration > Asset Tracking**.
3. Click **Add Custom Assets**, select the GPU if it is not already tracked, and then click **Apply**.
4. To view asset tracking reports, navigate to **System > Details > Asset Tracking**.
5. You can find a full list of available metrics in the iDRAC user guide in Table 17 on pages 110 and 111.

IPMI validation steps:

1. You can find GPU statistics in the IPMI user interface by navigating to **Component Info > GPU**.
2. To review available GPU metrics, download the IPMI BMC user guide.
3. Review Figure 2-37 on page 59 for a full list of features.

Import/Export Full Server Configuration Profile

This section outlines the steps taken to validate the server configuration export and import features.

iDRAC10 validation steps:

1. To export a server configuration backup, navigate to **Configuration > Server Configuration Profile > Export**.
    a. From the **Location Type** dropdown menu, select **Local**.
    b. Specify a name in the **File Name** field.
    c. Specify the elements to be backed up:
        i. For a full system backup, select **ALL**.
            1. The resulting file can be manually reviewed for a complete list of settings included in the server backup.
        ii. For a partial system backup, select the desired components, such as just the iDRAC settings.
    d. Specify the file format.
    e. To start the file generation, click **Export**.
    f. Once generated, click **Save Locally** to download the resulting backup.

2. To import a server configuration, navigate to **Configuration > Server Configuration Profile > Import**.
   a. From the **Location Type** dropdown menu, select **Local**.
   b. On the file path line, click **Choose File**, and then select the server export file to be restored.
   c. Select the components to be included in the import from the **Import Components** line of checkboxes.
   d. If non-default values are desired, specify the desired power state after the import, the shutdown method, and the maximum wait time.
   e. To start the import, click **Import**, and then click **OK** to confirm.
   f. Monitor the import progress via the job queue.

IPMI validation steps:

1. To export a BMC-level settings backup, navigate to **Configuration > BMC settings > IPMI Configuration**.
   a. To start the download, click **Download**.
2. To import a server backup, navigate to **Configuration > BMC settings > IPMI Configuration**.
   a. From the **Import BMC Configuration** line, click **Select File,** select the backup file from the resulting file selection windows, and then click **Open**.
   b. Click **Apply** to start the import process.
   c. The BMC resets as part of the import process; attempt reloading the BMC page to confirm when the import has finished.
3. To set BIOS settings that are not part of the automated server backup, open a virtual console and reboot the system.
   a. Press **Delete** during post to enter the system BIOS.
   b. For each section of settings, navigate to the appropriate pane in the BIOS interface, and then use the arrow keys to locate and adjust the individual settings.
      i. **Advanced > CPU Configuration** (14 settings)
      ii. **Advanced > CPU Configuration > Advanced Power Management Configuration** (10 settings)
      iii. **Advanced > Chipset Configuration** (6 settings)
      iv. **Advanced > Chipset Configuration > Memory Configuration** (7 settings)
      v. **Advanced > PCIe/PCI/PnP configuration** (5 settings)
      vi. **Advanced > Trusted Computing** (1 setting)
      vii. **Advanced > ACPI Settings** (2 settings)
      viii. **Advanced > Serial Port Control** (4 settings)
      ix. **Advanced > Network Stack Configuration** (6 settings)
      x. **BMC Configuration** (2 settings)
      xi. **Security** (4 settings)
      xii. **Boot Configuration** (2 settings)
   c. To complete the changes and allow the system to continue booting back up, select **Save and Exit**.

Dynamic USB Port Control

This section outlines the steps taken to validate the ability to dynamically enable or disable the front USB ports.

iDRAC10 validation steps:

1. To enable the dynamic control of the front USB ports, a one-time action, navigate to **Configuration > BIOS Settings > Integrated Devices**.
   a. From the accessible USB ports dropdown, select **All Ports Off (Dynamic)**.
   b. Click **Apply**, and then click **OK** at the confirmation prompt.
   c. To initiate the change, click **Apply**, and then reboot.
2. To enable or disable the USB ports once the feature has been enabled, navigate to **Configuration > System Settings**.
   a. Click the **Hardware Settings > Front Ports** tab.
   b. From the **Front USB port** dropdown, select the desired enabled or disabled option.
   c. To apply the change, click **Apply**, and then click **OK** on the confirmation window.

IPMI validation steps:

1. There is not a BMC-level control for the USB ports via the IPMI BMC.
2. To make the change to the USB ports:
    a. Open the remote console window, and then reboot the system.
    b. During post, press **Delete** to enter the BIOS configuration screen.
    c. Navigate to **Advanced > SuperGuardians Configuration**.
    d. Navigate to **USB Security Policy**, and then select the desired state.
    e. Press **F4** to save the BIOS changes and continue the boot process.

BIOS Live Scanning

This section outlines the steps taken to validate the manual and schedulable BIOS integrity scanning.

iDRAC10 validation steps:

1. Navigate to **Maintenance > Diagnostics > BIOS Live Scanning**.
    a. To start a manual scan, from the **Recurrence** dropdown menu, select **Now**.
        i. Click **Submit**.
        ii. Monitor scan progress via the **Jobs Queue**.
    b. To schedule a recurring scan, from the **Recurrence** dropdown menu, select **Daily**, **Weekly**, **Monthly**, or **Yearly**.
        i. From the **Start Time** dropdown menu, specify the time of day for the scan.
        ii. Click **Submit**.

IPMI validation steps:

1. After a review of the dashboard, in addition to the user guide, no GUI-native live BIOS integrity checking was available.

Automatic Firmware Updates

This section outlines the steps taken to validate the automatic firmware update capabilities.

iDRAC10 validation steps:

1. To enable automatic updates on a specified schedule, navigate to **Maintenance > System Update > Automatic Update**.
    a. Click **Enable Automatic Updates**, and then click **OK** on the confirmation window.
    b. Choose a server reboot behavior from either **Update and Reboot** or **Download but Don't Reboot**.
    c. Select **HTTPS** as the location type.
    d. Select **Use Default Address**.
    e. Specify a time of day for the update to occur.
    f. Specify the schedule as daily, weekly, or monthly.
    g. Click **Schedule Update**.

IPMI validation steps:

1. After a review of the dashboard, in addition to the user guide, no GUI-native automatic scheduled updates were available.
2. To manually source a firmware update file, navigate to **www.supermicro.com/support/resources/bios_ipmi.php**.
    a. Search for the specific motherboard model of the system.
    b. Select the board model in question, and then select **BMC Firmware**.
    c. Next to the update in question, click **Download > Continue as Guest**.
    d. After downloading completes, open the **ZIP** file, select the **BIN** file from the **ZIP** archive for BMC, and then extract that **BIN** file.
    e. In the BMC interface, navigate to **Maintenance > Firmware Management**.
    f. From the **File Format** dropdown, select **BMC**, and then click **Next**.
    g. Click the **Select File** button, and then choose the previously downloaded file.
    h. Click the **Upload** button to upload the file to the server.

Connection View

This section outlines the steps taken to validate the network connection viewing capability.

iDRAC10 validation steps:

1. To enable the **Connection View** feature, navigate to **iDRAC Settings > Connectivity > Common Settings**.
   a. From the **Connection View** dropdown menu, select **Enabled**.
   b. Click **Apply**.
2. To view the network connection view information for a given server, navigate to **System > Overview > Components > Network Devices**.
   a. Click onto the name of the network card to be viewed.
   b. Scroll down to view the **Switch Port Connection ID**.

IPMI validation steps:

1. After a review of the dashboard, in addition to the user guide, no feature showing the network cabling was found.

Full-System BIOS Configuration

This section outlines the steps taken to validate the availability of BIOS settings via the BMC interface.

iDRAC10 validation steps:

1. To access BIOS settings, navigate to **Configuration > BIOS Settings**.
2. Use the tabs at the top of the page to access all BIOS category settings.
3. Modify values per page as desired.
4. Click **Apply** to save the per-page BIOS modifications.
5. To stage the BIOS changes, click **Apply at next reboot**.

IPMI validation steps:

1. After a review of the dashboard, in addition to the user guide, there is no ability to stage BIOS changes without a reboot.
2. To adjust BIOS values, open the remote console window, and then reboot the system.
   a. Press the **Delete** key during post to enter the BIOS settings interface.
   b. Navigate through the interface to access the settings to be changed.
   c. Adjust values as desired.
   d. Press **F4** to save the changes and exit.
   e. Allow the system to finish booting back up.

Two-Factor Authentication via RSA

This section outlines the steps taken to validate the RSA-based multi-factor authentication capability.

iDRAC10 validation steps:

1. To enable RSA-based multi-factor authentication for local users, navigate to **iDRAC Settings > Users**.
   a. Select a user from the list, and then click the **Edit** button.
   b. Click the **Advanced** tab.
   c. From **RSA SecurID state**, select **Enabled**.
   d. Click **Save**, and then click **OK**.

IPMI validation steps:

1. After a review of the dashboard, in addition to the user guide, no support for RSA-based multi-factor authentication for local users was found.

One-to-Many Device Management Console

This section compares the features and behavior of the one-to-many management-interface-level offerings covering OME and SSM. The following steps assume that you have freshly logged in to the management platform in question.

Scope-Based Access Control (SBAC)

This section outlines the steps taken to validate the support for SBAC via the documentation.

OME validation steps.

1. Open the OME user guide.
2. Review the SBAC section found on pages 65 and 66.

SSM validation steps.

1. Navigate to **Application Settings > Users**.
2. Click **Add**, **Edit User**, or **Import Directory Group**.
3. Assign a device manager or custom role to the user or directory group.
4. Assign the scope to all or a select subset of devices.

Credential Management

This section outlines the steps taken to validate support for automatic credential management.

OME validation steps:

1. Navigate to **OME > Application Settings > Console Preferences**.
2. Select **iDRAC Password Management**.
3. Select either **Internal OME** or **External – CyberArk Integration**.
    a. For **Internal OME**, click **Enable**, and then specify the rotation schedule details.
    b. For **External – CyberArk Integration**:
        i. Click **Export** to download a list of iDRAC elements eligible for this feature.
        ii. Click **Upload Certificate** to upload the certificate used to authenticate with the credential provider.
        iii. Specify:
            1. **Central Credential Provider Hostname** and **Port**
            2. **Application ID**
            3. **Safe**
            4. Credential retrieval as **IP Address**, **FQDN**, or **Service Tag**
4. Click **Apply** to save the changes.

SSM validation steps:

1. After a review of the dashboard, in addition to the user guide, no support for automated password rotation was found.

Centralized Identity and Access Management

This section outlines the steps taken to validate the support for OpenID® Connect (OIDC) token-based authentication.

OME validation steps:

1. To add an OIDC provider, navigate to **Application Settings > Users > OIDC**.
    a. Click **Add**.
    b. Specify:
        i. **Name**
        ii. **Discovery URL**
        iii. **Authentication Type**, including:
            1. **Initial access token**
            2. **Username**
            3. **Password**
            4. Optionally an upload certificate for validation
    c. Select the **Enabled** checkbox to activate.
    d. Click **Finish**.

2. To configure PingFederate:
   a. In **OAuth Settings**, under **Scope Management**, add an **Exclusive** or **Default** scope called **dxcua**.
   b. To map the scope that is created, in **OpenID Connect Policy Management > Policy**, select **Include User Info in Token**.
   c. In **Attribute Scope**, add the scope and attribute value as **dxcua**.
   d. In **Contract Fulfillment**, add **dxcua**, and then select the type as **Text**.
   e. Define the user roles for the OME OIDC provider login using one of the following attributes. The role must be a system-defined role.
      i. Administrator: **dxcua : [{"Role": "AD"}]**
      ii. Device manager: **dxcua : [{"Role": "DM"}]**
      iii. Enterprise user: **dxcua : [{"Role": "DM", "Entity":"G1, G2"}]**
      iv. Viewer: **dxcua : [{"Role": "VE"}]**
      v. Custom role: **dxcua : [{"Role": "*Custom role name*"}]**
3. To configure Keycloak, add and map **dxcua** to the **Client ID**. Define the user privileges as follows:
   a. In the **Attributes** section of **Keycloak Users**, define the **Key and Value** for OME login roles using one of the following attributes:
      i. Administrator : **dxcua : [{"Role": "AD"}]**
      ii. Device manager: **dxcua : [{"Role": "DM"}]**
      iii. Viewer: **dxcua : [{"Role": "VE"}]**
      iv. Custom role: **dxcua : [{"Role": "Custom role name"}]**
   b. Once the client is registered in Keycloak, in the **Mappers** section, add a **User Attribute** mapper type with the following values:
      i. **Name: dxcua**
      ii. **Mapper Type: User Attribute**
      iii. **User Attribute: dxcua**
      iv. **Token Claim Name: dxcua**
      v. **Claim JSON Type: String**
      vi. **Add to ID Token: Enable**
      vii. **Add to Access Token: Enable**
      viii. **Add to User Info: Enable**

SSM validation steps:

1. After a review of the dashboard, in addition to the user guide, no support for OIDC was found.

Carbon Emissions Analysis and Capacity Planning

This section outlines the steps taken to validate the support for carbon emission calculations based on real usage data.

OME validation steps:

1. To specify which devices will be monitored for carbon emissions data, navigate to **Power Management > Power Managed Devices**.
   a. Select the devices to be monitored.
   b. View all discovered devices by expanding the various system groups.
   c. Confirm which devices will be monitored via the **Individual Devices** section.
2. To configure the carbon emission conversion factor, navigate to **Power Management** tab, and then select **Settings**.
   a. Click **Edit**.
   b. Scroll down to the **Carbon Emissions Conversion Factor**, and then set the field according to the local power supplier data.
   c. Click **Apply**.
3. To view carbon emissions data based on actual usage, navigate to the **Devices** tab from the main menu.
   a. Select a device from the list.
   b. Click the **Telemetry** tab.
   c. Review the **Energy Consumption and Carbon Emissions** section for data.

SSM validation steps:

1. After a review of the dashboard, in addition to the user guide, no support for usage-based carbon emission calculations was found.

Automated Power and Thermal Management Policies

This section outlines the steps taken to validate the support for automatic actions on power- or thermal-based policies.

OME validation steps:

1. To configure a power usage–based policy, navigate to **Power Management > Policies**.
   a. Under the **Policies** section, click **Create**.
   b. Select **Static** as the policy type.
   c. Provide a **Policy Name** and **Policy Description**.
   d. Select the device or group of devices to which the policy will apply, and then click **Next**.
   e. Provide a value for the **Power Cap**, and then click **Next**.
   f. Specify the schedule during which the policy will apply, and then click **Next**.
   g. Review the summary, and then click **Finish** to save and activate the policy.
2. To configure a thermal-based policy, navigate to **Power Management > Policies**.
   a. Click **Create** to add a new policy.
   b. Select **Temperature-triggered** as the policy type, and then click **Next**.
   c. Provide a policy name and description, and then click **Next**.
   d. Select a **Temperature Threshold** value, and then click **Next**.
   e. Specify the schedule during which the policy will apply, and then click **Next**.
   f. Review the summary, and then click **Finish** to save and activate the policy.

SSM validation steps:

1. To configure a power-based policy, click the **SSM New GUI** link.
   a. Select **Server Group**, and then click on the **Power Management** tab.
   b. Click the **All Power Policies** tab.
   c. Click the **Add** icon to create a new power policy.
   d. Specify values for:
      i. **Name**
      ii. **Description**
      iii. **Domain type**
      iv. **Power Limit type**
      v. **Threshold**
   e. Click **Enable Power Policy**.
   f. Click **Apply**, and then close the confirmation prompt.

Power and Thermal Data

This section outlines the steps taken to validate the available power management data.

OME validation steps:

1. Navigate to the **Power Management** tab, and then select **Overview**.
2. Review the 8 categories with 16 individual metrics.

SSM validation steps:

1. Navigate to the **Power Management** menu, and then to the **Dashboard** view.
2. Review the 4 metric categories with 5 individual metrics.

Power Usage Metrics and Visibility

This section outlines the steps taken to validate the available metrics related to server and power utilization.

OME validation steps:

1. Click the **Devices** tab.
2. Select a device to investigate from the list of devices.
3. Click the **Telemetry** tab.
4. Review the 12 categories and 22 individual metrics available.

SSM validation steps:

1. Navigate to the **Monitoring** menu, and then to the **Host Monitoring** view.
2. Select a specific server to investigate, and then click the **Expand Server View** arrows.
3. Click the **Power Management** tab.
4. Review the 3 metric categories with 3 total utilization metrics.

HTML5-Based Management Interface

This section outlines the steps taken to validate the need for a Java® Runtime Environment (JRE) at the server level.

OME validation steps:

1. Open the OME user guide, pages 25–31.
2. Review the requirements and note that JRE is not one of them.

SSM validation steps:

1. Open the SSM user guide.
2. Review the SSM documentation in section 2.1.
3. Review section 2.1.1 for **Windows Installation**, step 6, where it notes an x64 Java VM with a version between 17 and 18 is needed.
4. Review section 2.1.2 for a **Linux Installation**, step 6, where it notes that JVM versions later than 17.0.0 and earlier than 18.0.0 are supported.

Alert-Based Automated Actions

This section outlines the steps taken to validate the ability to trigger actions automatically based on server alerts.

OME validation steps:

1. To configure alerts, navigate to **Alerts > Alert Policies**:
   a. To add a new policy, click **Create**.
   b. Enter a name and description for the policy, and then click **Next**.
   c. To activate based on a category of alerts, choose one or more; otherwise, click **Next**.
   d. To activate the policy based on message ID, enter a message ID, and then click **Next**.
   e. In the **Target** section, select the specific devices, groups, or all devices to which the policy will apply, and then click **Next**.
   f. Specify the duration when the alert policy will be active, and then click **Next**.
   g. Select an action to be taken, such as powering off the server, and then click **Next.**
   h. Review the settings, and then click **Finish**.

SSM validation steps:

1. No automatic, alert-based server actions were found in a review of the GUI and documentation.
2. To enable administrator notification on an alert, click the **Administration** section of the navigation pane.
   a. Click **Administration > Monitoring Setup > Contacts**.
   b. Click a contact name.
   c. Click the **Edit Host** notification link.
   d. Select notification options, such as email.
   e. Select an existing notifications script or upload a new one.
   f. Specify additional arguments as needed to further format the notifications.
   g. Click **Submit**.
3. To take manual action after an alert is received, navigate to the **Monitoring** tab **> Host Monitoring View > Logical Group** for the server that sent the alert notification.
   a. Click the **SSM New GUI** link.
   b. Select the system associated with the alert, and then click the expand arrows.
   c. Click the **Event View** tab to review the alert and determine the action needed.
   d. Open the **Legacy Console** view.
   e. Click the **Monitoring** tab's **Hosts** view for the group with the alerting server.
   f. From the command view section, select **Redfish > Power [On/Off/Restart]** as needed in response to the alert.
   g. Click **Run** to initiate the action.

Heterogeneous Server Monitoring

This section outlines the steps taken to confirm support for monitoring servers from other manufacturers.

OME validation steps:

1. To begin the server discovery process, navigate to the **Monitor** tab, and then select **Discover**.
2. To start a new discovery job, click **Create**.
   a. Provide a job name.
   b. From the **Device Type** dropdown menu, select **Server**.
   c. Select **Non-Dell Servers**, choose from **HP iLO, Lenovo XClarity**, or **Other**, and then click **OK**.
   d. Specify **IP** and **Supermicro IPMI Credentials**.
   e. Select **Run Now** or **Schedule** for the job.
   f. Click **Finish**.

SSM validation steps:

1. Review the SSM user manual, pages 396–398; note that SMC hardware is a prerequisite.

Power Management Reporting

This section outlines the steps taken to confirm support for customizable reporting relating to power metrics.

OME validation steps:

1. To view existing reports, navigate to **Monitor > Reports**.
   a. Note the 27 built-in reports.
   b. Select a report to view.
   c. Click **Run**.
2. To download the report, click **Download**.
   a. Choose from **HTML**, **CSV, PDF**, or **XLS** document formats.
   b. Click **Finish**.
3. To create a custom report, navigate to **Monitor > Reports**.
   a. Click **Create**.
   b. Enter a name and description for the report.
   c. In the category dropdown, select **Power Management** devices or **Power Management Groups**, as desired.
   d. Select the values to be included with the report from across the available metric categories.
   e. Click **Finish** to create the report.

SSM validation steps:

1. To access available reports, click the **SSM New GUI** link.
   a. Click the **Reports** menu.
   b. Select **Energy Consumption Reports**.
   c. Note the 2 options available for **Host** or **System** energy consumption.

Third-Party Integration Support

This section outlines the steps taken to compare the available third-party extensions for each platform.

OME validation steps:

1. To see supported plugins, review **OpenManage Integrations and Connections | Dell USA**.
   a. Note the support for:
      i. VMware vCenter®
      ii. Microsoft® System Center
      iii. Windows® Admin Center
      iv. ServiceNow®
      v. Ansible®

2. To dive deeper into the capabilities of the VMware plugin, review **OME Integration for VMware vCenter**.
    a. Note support for:
        i. Custom vCenter RBAC with Dell-specific privileges (pages 17 and 18)
        ii. Multi-vCenter support (pages 19 and 24)
        iii. Warranty tracking at the host, cluster, and data center level (page 23)
        iv. Fleet health dashboard (page 23)
        v. Firmware baseline compliance and drift detection (pages 29, 30, 55, and 56)
        vi. Proactive HA provider for hardware components (fan, power, IDSDM, and memory) (pages 57–59)
        vii. vCenter events and alarms configuration for hardware conditions (pages 61 and 62)
        viii. Event logs available directly in vCenter (pages 63 and 86)
        ix. Maintenance mode orchestration during firmware updates (configurable timeout, VM migration, and auto-exit) (page 66)
        x. Direct BMC management actions (UID, intrusion reset, BMC reset, and user account view) via iDRAC link (pages 79 and 80)
        xi. Clickable iDRAC IP/iDRAC launch link from vCenter (page 81)
        xii. Per-host sensor and hardware health monitoring (page 81)
        xiii. Power control (partial, via iDRAC launch) (page 81)
        xiv. Hardware inventory: deep component coverage (FRU, CPU, PSU, memory, NIC, PCI, iDRAC, and storage) (pages 82–85)
        xv. Power monitoring and telemetry (instantaneous, peak, and energy consumption) (page 85)
        xvi. Firmware update: multi-component with cluster-level orchestration and scheduling (pages 91–98)
        xvii. vLCM integration with full firmware catalog provider support (pages 100–102)

SSM validation steps:

1. To see supported plugins, review **Plug-ins | Supermicro Server Management Utilities | Supermicro**.
    a. Note support for:
        i. VMware vCenter
        ii. Nagios®
        iii. Microsoft System Center Operations Manager
2. To dive deeper into the capabilities of the VMware plugin, review **Supermicro vSphere Client Plug-in User's Guide**.
    a. Note support for:
        i. Multi vCenter support (page 3)
        ii. Per-host sensor and health monitoring (page 16)
        iii. Hardware inventory (basic FRU and BMC details, in addition to IPv4/IPv6) (pages 16–18)
        iv. Direct BMC management within the plugin (UID toggle, intrusion reset, BMC reset, and user account view) (pages 18, 19, and 25)
        v. Embedded power control actions, including AC cycle (page 19)
        vi. Maintenance Event Log and Health Event Log in vCenter (assert/deassert event tracking) (pages 21 and 22)
        vii. Firmware update for BIOS and BMC (single host) (page 23)
        viii. vLCM integration for BIOS and BMC firmware only (pages 26–28)

Report Builder with Customization

This section outlines the steps taken to confirm the availability of built-in and custom monitoring reports.

OME validation steps:

1. To view existing reports, navigate to **Monitoring > Reports**.
    a. Take note of the available built-in reports.
2. To make a custom report, click **Create**.
    a. Specify a name and description for the report, and then click **Next**.
    b. Select checkboxes to mix and match specific metrics into a custom report, and then use the right window to adjust the order of the report columns.
    c. Click **Finish**.

SSM validation steps:

1. Click the **SSM New GUI** link.
2. To view available reports, click the **Reports** tab, and then expand out the sub-menus for:
   a. **Energy Consumption Reports**
   b. **Availability Reports**
   c. **State History Reports**
   d. **Inventory Reports**
3. Note the lack of report customization options.

Preconfigured Virtual Appliance Deployment

This section outlines the steps taken to validate the need for JRE at the server level.

OME validation steps:

1. Open the OME user guide, pages 32–42.
2. Note the support for 8 total install methods, both virtual appliance–based and with the programmatic installation option:
   a. VMware vSphere
   b. Microsoft® Hyper-V®
   c. KVM on Red Hat® Enterprise Linux®
   d. KVM VirtInstall
   e. Nutanix® AHV®
   f. Proxmox® VE
   g. Red Hat® OpenShift®
   h. Programmatic install

SSM validation steps:

1. Open the SSM user guide, and then review pages 25–42.
2. Note the support for 3 install methods, both operating system (OS)-based and silent:
   a. Windows
   b. Linux
   c. Silent install

Mobile Integration

This section outlines the steps taken to confirm support for mobile-application support by the one-to-many management platform.

OME validation steps:

1. Review **PowerEdge: Support for Dell OpenManage Mobile**.
   a. Note that OpenManage Mobile allows for management through OME.

SSM validation steps:

1. Review the **SSM Brochure Server Management Utilities brochure's** summary on page 7.
   a. Note the lack of mobile support in the SSM column.

Configuration Template Deployments

This section outlines the steps taken to confirm what features are deployable via templates.

OME validation steps:

1. To deploy based on a template, navigate to **Configuration > Templates**.
   a. Select a template, click **Deploy Template**, and then, at the confirmation prompt, click **Yes**.
   b. From the target window, click **Select**, and then choose one or more servers to apply the template to.
   c. Click **Next** to verify the boot options.
   d. Click **Next** to confirm the iDRAC management IP settings.
   e. Click **Next** to review the target attributes.
      i. Note that iDRAC, BIOS, storage, network, OS host name, and server topology details can be selected.
   f. Click **Next** and confirm if this should be run now or scheduled.
   g. Click **Finish** to start the deploy processes.

SSM validation steps:

1. No full server-based deployment from a single template was supported.
2. To import the BIOS setting, click the **SSM New GUI** link.
   a. Select a group of servers from the left-side menu.
   b. Select one or more servers from the group in the central pane.
   c. From the right side, select **Import BIOS Config**.
   d. Specify the BIOS configuration file to be used.
      i. Note BIOS files are specific to the motherboard model and are not fully general templates.
   e. Click **Run** to apply the settings change.
   f. From the right-side menu, select **Import BMC**.
3. To update the BMC settings, click **Edit BMC Settings** to access:
   a. **Date and Time**
   b. **SSDP**
   c. **IP Access Control**
   d. **Supermicro RAKP**
   e. **LLDP**
4. Alternately, log in to IPMI directly for a single server.
   a. Navigate to **Configuration > BMC Settings > BMC Configuration** tab.
   b. Next to **Import BMC configuration**, click **Select File**, and then click **Open** in the subsequent dialog.
   c. Click **Apply**.

Firmware and Driver Updates

This section outlines the steps taken to confirm support for automatic firmware and driver updates.

OME validation steps:

1. To configure the update source, navigate to **Plugins > Update Management > Repository**.
   a. Click **Create Repository**.
   b. Add a name for the repository.
   c. Confirm use of the default baseline catalog.
   d. Select **Automatically**, set the time of day, and then click **Next**.
   e. Select the devices or groups to be included with the updates.
   f. Review the settings, and then click **Finish**.
2. To check for out-of-date firmware and make updates, click **View Report**.
   a. Select all servers to be brought into compliance.
   b. Click **Make compliant**.
   c. Select to update now or schedule for a later time.
   d. Choose to reboot immediately or stage for next reboot.
   e. Choose to reset iDRAC, if desired.
   f. Choose to clear job queue, if desired.
   g. Click **Update**.

SSM validation steps:

1. SSM was not found to have a single auto-update catalog.
2. To update BMC or BIOS firmware, click the **SSM New GUI** link.
   a. Navigate to the provision menu.
   b. Click the **+** icon to add a new plan.
   c. Enter a name for the plan.
   d. Click the search icon, and then select the hosts to apply the plan to.
   e. Click **Submit**.

3. To update non-BIOS/BMC devices, navigate to **Provision > FW Update**.
    a. From the **Choose Update** section, select one of the following:
        i. CDU
        ii. Broadcom® RAID Adapter
        iii. GPU Package
        iv. Retime
        v. Network AOC
        vi. Motherboard CPLD
        vii. Fan Board CPLD
        viii. Backplane CPLD
        ix. Network AOC CPLD
    b. Click **Next**.
    c. Upload the updated firmware from a local source, and then click **Next**.
    d. Select the target system to be update, and then click **Next**.
    e. Select the schedule, and then click **Next**.
    f. Repeat from step 3 for each remaining device to be updated.

Cloud-Based Monitoring

This section illustrates the cloud-based monitoring features and behavior of the AIOps platform. Because AIOps has no direct equivalent in the Supermicro portfolio, we evaluated its capabilities independently, rather than in all direct feature comparisons. The following steps assume that you have freshly logged in to the AIOps platform in question.

Policy-Based Security Configuration (PBSC)

This section outlines the steps taken to confirm support for policy-based security in the AIOps platform.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (pages 79–85).
    a. **System Risk:** The System Risk page is the multisystem view for cybersecurity. It displays all systems that are enabled for cybersecurity, along with the risk level, the percentage of tests enabled in the evaluation plan, the number of misconfigurations detected by evaluation tests, and the number of security advisories available for each system.
    b. **Misconfigurations:** The Misconfigurations page provides an overall listing of misconfiguration issues detected in the environment. The **Active** tab lists out all active issues and provides the severity, issue name, associated system, and when it was created.
    c. **Misconfiguration Settings:** The Misconfiguration Settings page, accessed through the gear icon on the **Misconfigurations** page, is where users enable, disable, and configure the tests in the evaluation plan.
    d. **Templates:** The Templates tab lists the configured templates and allows users to create templates and view, edit, and delete existing templates. A template contains a list of configured tests that can be assigned to multiple systems of the same product technology.

Cybersecurity Advisories

This section outlines the steps taken to confirm support for security advisories in the AIOps platform.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (page 85).
    a. **Security Advisories:** The Security Advisories page provides a full list of applicable security advisories, along with their impact, a synopsis, their components, the number of impacted systems, and a publish date. Clicking the **View Article** hyperlink opens the advisory details on the Dell support page.

Carbon Footprint Analysis

This section outlines the steps taken to confirm the ability to analyze the carbon footprint of running servers.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (pages 44–46).
    a. **Carbon Footprint:** The Carbon Footprint page provides summary-, system-, and workload-level metrics for carbon emissions and energy usage. Carbon emissions calculations are based on location-specific emission factors provided by the International Energy Agency (IEA) and industry-average power utilization effectiveness (PUE) values. Users with the Admin role can override these default values by clicking the **Settings** button.

Generative AI (GenAI) Assistant

This section outlines the steps taken to confirm the presence of an AI-enabled assistant.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (pages 19–21).
    a. **AIOps Assistant:** Chat with the GenAI-powered AIOps assistant using natural language input to get answers to questions about product support, general product information, and specific information on systems in the user's environment. The AIOps assistant can display results in text, chart, graph, or table format.

Performance Metrics with Anomaly Detection

This section outlines the steps taken to confirm the presence of metrics with anomaly detection.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (pages 40–42 and 154–156).
    a. **PowerEdge system details – Performance:** Using machine learning (ML) and analytics, AIOps identifies performance anomalies. Anomaly charts provide both the value of the metric and the historic seasonality. By plotting the historic seasonality, users can identify any unexpected anomalies or changes in patterns. Anomaly charts show up to 24 hours of data.

Server-Level GPU Utilization

This section outlines the steps taken to confirm the ability to access server-level metrics for GPUs.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (pages 154 and 210–212).
    a. **PowerEdge system details – Performance:** The Performance tab provides 24-hour charts for key performance metrics for chassis and servers, including for GPUs on systems where they are present. A multitude of metrics are available, including anomaly charts for several metrics.

Multiple Performance Reports

This section outlines the steps taken to confirm the ability to update server-level components.

AIOps validation steps:

1. Review **Dell AIOps: A Detailed Review** (pages 63–68).
    a. **System Updates:** The System Updates section allows users to manage updates for several components of Dell PowerEdge™ systems. The System Updates page has up to six tabs: Storage, Networking, HCI, Data Protection, Server, and Collector.
        i. The Storage tab displays a list of all available system code, management software, and drive firmware updates across all supported systems.
        ii. The Networking tab provides a list of recommended switch firmware updates for Connectrix™ switches.
        iii. The HCI tab allows users to initiate multi-cluster updates from AIOps.
        iv. The Data Protection tab lists recommended updates for Dell PowerProtect™ Data Manager instances and PowerProtect DD series appliances.
        v. The Server tab lets users initiate BIOS and firmware updates for their PowerEdge servers and chassis; OME v3.10 or later with CloudIQ plugin v1.2 or later are required.
        vi. The Collector update tab displays a list of AIOps collectors only. Newer versions display when available for each collector, with the update category indicating when the update must be performed.

Referenced Documents

This section describes the locations where the referenced documentation can be found.

IPMI BMC

iDRAC10 user guide

OME user guide

SSM user guide

OME VMware plugin documentation

OME VMM and Configuration Manager documentation

OME Operations Manager documentation

SSM Microsoft System Center Operations Manager plugin documentation

SSM Nagios plugin documentation

SSM VMware plugin documentation

SSM brochure

OpenManage Mobile page

Dell AIOps: A Detailed Review

0626/260003