Hewlett Packard Enterprise

UEFI System Utilities User Guide for HPE Compute Gen11 servers

Part Number: 30-163527A4-001h
Published: November 2025
Edition: 10

UEFI System Utilities User Guide for HPE Compute Gen11 servers

Abstract

This guide details how to access and use the Unified Extensible Firmware Interface (UEFI) that is embedded in the system ROM of all HPE Compute Gen11 servers including the HPE Synergy Compute modules. It details how to access and use both UEFI and Legacy BIOS options provided in BIOS Platform Configuration menus that were formerly known as the ROM-Based Setup Utility (RBSU). All options and available responses are defined. This document is for the person who installs, administers, and troubleshoots servers and storage systems.

Part Number: 30-163527A4-001h
Published: November 2025
Edition: 10

Notices

Revision history

Part number	Publication date	Edition	Summary of changes
30-163527A4-001g	July 2025	8	Added the following topic: • Configuring Uncore Frequency RAPL • Enabling or disabling NUMA • Enabling or disabling Virtual NUMA

Acknowledgments

Table of contents

        - Enabling or disabling Memory PStates
        - Configuring AMD Remap 1TB
        - Setting the maximum memory bus frequency
        - Enabling or disabling Memory Patrol Scrubbing
        - Enabling or disabling node interleaving
        - Configuring Memory Encryption Options
            - Enabling or disabling Transparent Secure Memory Encryption
            - Configuring AMD Secure Memory Encryption
            - Enabling or disabling AMD Secure Nested Paging
        - Configuring the memory mirroring mode
        - Configuring NVDIMM-N Options
            - NVDIMM-N Support
            - NVDIMM-N Sanitize/Erase on Next Reboot Policy
            - NVDIMM-N Interleaving
        - Enabling or disabling Memory Configuration Violation Reporting
        - Enabling or disabling Memory Permanent Fault Detect
        - Configuring the HBM Memory Options
        - Enabling or disabling Total Memory Encryption (TME)
        - Configuring ECC mode
        - Configuring ECC control
        - Enabling or disabling Patrol Scrub
        - Enabling or disabling Demand Scrub
        - Configuring Fine Granularity Refresh (FGR)
    - Changing Virtualization Options
        - Enabling or disabling Virtualization Technology
        - Enabling or disabling Intel VT-d
        - Enabling or disabling Access Control Service
        - Enabling or disabling SR-IOV
        - Setting the Minimum SEV ASID
        - Enabling AMD I/O Virtualization Technology
        - Enabling or disabling AMD DMA Remapping
        - Enabling or Disabling AMD DMAr Support
        - Enabling or Disabling AMD DMA Protection
        - Enabling AMD 5-Level Page
        - Enabling or disabling ARM SMMU PMU
    - Changing Boot Options
        - Setting the boot order policy
        - Setting the filter on nonbootable drives
        - Changing the UEFI Boot Order list
        - Controlling the UEFI boot order
        - Adding a boot option to the UEFI Boot Order list

Getting Started

Subtopics

UEFI System Utilities

The UEFI System Utilities is embedded in the system ROM. Its features enable you to perform a wide range of configuration activities, including:

- Configuring system devices and installed options.
- Enabling and disabling system features.
- Displaying system information.
- Selecting the primary boot controller or partition.
- Configuring memory options.
- Launching other preboot environments.

HPE servers with UEFI can provide:

- Support for boot partitions larger than 2.2 TB. Such configurations could previously only be used for boot drives when using RAID solutions.
- Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security.
- UEFI Graphical User Interface (GUI)
- An Embedded UEFI Shell that provides a preboot environment for running scripts and tools.
- Boot support for option cards that only support a UEFI option ROM.

Subtopics

What is UEFI?

Unified Extensible Firmware Interface (UEFI) defines the interface between the operating system and platform firmware during the boot or start-up process. Compared to BIOS, UEFI supports advanced pre-boot user interfaces. The UEFI network stack enables implementation on a richer network-based OS deployment environment while still supporting traditional PXE deployments. UEFI supports both IPv4 and IPv6 networks. In addition, features such as Secure Boot enable platform vendors to implement an OS-agnostic approach to securing systems in the pre-boot environment.

The ROM-Based Setup Utility (RBSU) functionality is available from the UEFI interface along with additional configuration options.

UEFI System Utilities overview

Subtopics

Launching the System Utilities

Procedure

1. Optional: If you access the server remotely, start an iLO remote console session.
   a. Open a browser and enter `https://<iLO host name or IP address>` to log on to the iLO web interface.
   b. On the login page, enter a directory or local user account name and password, and then click Log In.
   c. Select Remote Console & Media in the iLO navigation tree.

      The Launch tab is displayed.
   d. Verify that your system meets the requirements for using the remote console application you want to use.
   e. Click the launch button for your selected application.

      You can also launch an iLO Remote Console session by selecting:

      - The Integrated Remote Console link on the Information - iLO Overview page.
      - The Console thumbnail in the low left corner of the iLO web interface, and then choosing the application type to launch.
2. Restart or power on the server.

   The server restarts and the POST screen appears.
3. Press F9.

   The System Utilities screen appears.

NOTE

Using System Utilities requires BIOS administrator authorization. If the BIOS administrator requires a password, the server prompts for the password to be entered prior to launching the System Utilities. For information on setting the administrator password, see Server Security options.

Navigating the System Utilities

Procedure

1. Launch the System Utilities and do one of the following.
   - To navigate the screens and modify settings, use your pointing device or press any of the navigational keys. Key functions are shown at the bottom of every System Utilities screen.

TIP

When Setup Browser Selection is set to Auto (the default setting) or GUI, you can use your pointing device to navigate the System Utilities screens. When Setup Browser Selection is set to Text, you must use the navigational keys.

- To access the mobile online help, scan the QR code on the bottom left of the System Utilities screen with your mobile device.

2. To exit the System Utilities screen and reboot the server, press Esc until the main menu is displayed, and then select one of the following options:
   - Exit and resume boot—Exits the system and continues the normal boot process. The system continues through the boot order list and launches the first bootable option in the system.
   - Reboot the System—Exits the system and reboots the system without continuing the normal boot process.

Subtopics

Navigating the System Utilities in GUI mode

Prerequisites

- The System Utilities is accessed through Integrated Remote Console or a physical terminal.
- Setup Browser Selection is set to Auto or GUI.

About this task

System Utilities GUI that allows you to navigate using either your pointing device or navigational keys. In GUI mode, selected menu items turn green.

NOTE

GUI mode is not supported when you access the System Utilities using a serial console.

To set the browser mode to GUI:

Procedure

1. From the System Utilities screen, select Setup Browser Selection.
2. Select Auto or GUI.
3. Save the setting.
4. Reboot the system.

Subtopics

UEFI System Utilities GUI

HPE ProLiant Gen11 and HPE Synergy compute modules support a GUI UEFI System Utilities. Both mouse and keyboard devices are

supported on the UEFI System Utilities GUI.

Regions

The System Utilities GUI has the following regions:

1. Caption Bar—This region shows the UEFI form title and the system buttons. The Form title shows the name of the form that you are currently navigating.
2. Navigation History—This region shows the forms to which you navigated previously. A Navigation History node is added to the navigation history each time you visit a new system utility form.
3. Server Information—This region shows server information and function key information.
4. System Utilities Form—This region shows the menu options of the current form.
5. Activity Bar—This region shows the system wide functions, such as function keys and the system status indicator.

Keyboard support in the GUI

The GUI has support for basic keys to navigate the system utilities form. The Tab key is used to change the focus on the different regions of the form. Supported keys include:

- Up and Down arrows
- Enter
- Function keys
- Esc key

Navigation History region and keyboard support

Navigation History shows system utility forms which user navigated previously. A Navigation History node is added to the Navigation History each time you visit a new form. You can Click a Navigation History node to return to the utility form that you previously visited.

If there are too many Navigation History nodes to fit on the Navigation History bar, the Home node is collapsed. To view a pop-up list of the navigation history node that you visited, you can select the Home node. To return to a previously accessed form, you can Click a Navigation History node from the list.

To move through the Navigation History region, you use the:

- Tab key to change focus in the Navigation History region.
- Enter key to get in to the Navigation History node selection mode and to select a node.
- Arrow keys to move to the node you want to select.
- Esc key to exit the Navigation History node selection mode.

Gen11 features

- Language selection—Located in the Caption Bar.
- Pending Changes—Lists changes that have not been saved.
- Forced Write Settings—Displays options that are forced to change due to changing an option.
- Search—Search for an RBSU option.
- Dependency viewer— Press the question mark button located in the Caption Bar. The information about why the option is greyed out will be showed up in red.

System Utilities key functions

- Up or down arrow—Selects a menu option. When selected, the color of a menu option changes from white to yellow in text browser mode, or to green in GUI mode.
- Enter—Selects an entry. A selected option changes color from white to yellow in text browser mode, or to green in GUI mode. When a submenu is available, the submenu appears.
- Esc—Returns to the previous screen.
- F1—Displays online help about a selection in text mode.

  NOTE

  To display online help in GUI mode, click the ? icon on the upper right corner of the System Utilities main screen.

- F7—Loads default UEFI BIOS configuration settings.

  NOTE

  Pressing F7 only resets the BIOS configuration. It does not reset other entities, such as option cards or iLO.

- F10—Prompts you to save changed settings.
- F12—Prompts you to save changed settings, and then exits the System Utilities.
- Reboot Required (radio button)—Is selected and turns red when changes require that you reboot the server.
- Changes Pending (radio button)—Is selected and turns red when changes are pending that must be saved to take effect.

When is a reboot required?

For certain configuration changes to take effect, a reboot might be required. In such cases, one of the following occurs depending on your Setup Browser Selection that prompts you to do so.

- In GUI mode, the Reboot Required (radio button) is selected and turns red when changes require that you reboot the server.
- In text mode, a prompt appears on the applicable System Utilities screen.

System Utilities menu overview

NOTE

UEFI system configuration options vary by server platform. Therefore, you might not see some of the options that are documented here.

The System Utilities screen is the main screen in the UEFI menu-driven interface. It displays menu options for the following configuration tasks:

- System Configuration—Displays options for viewing and configuring:
  - BIOS/Platform Configuration (RBSU)
  - iLO 6 Configuration Utility
  - Other system-specific devices, such as installed Smart Array devices, PCIe cards, and NICs. For example, Embedded FlexibleLOM Port 1.

NOTE

Throughout the menus, the interface attempts to display the proper marketing name for installed PCI devices. If the interface does not recognize a device, it assigns a generic label to the device, such as a `non-HPE name`. This generic labeling does not affect the functionality or operation of the device. Devices vary based on your system.

- One-Time Boot Menu—Displays options for selecting a boot override option and running a UEFI application from a file system.
- Embedded Applications—Displays options for viewing and configuring:
  - Embedded UEFI Shell
  - Integrated Management Log (IML)
  - Active Health System Log
  - Firmware Update
  - Embedded Diagnostics
  - Intelligent Provisioning
  - Embedded iPXE
- System Information—Displays options for viewing the server name and generation, serial number, product ID, BIOS version and date, power management controller, backup BIOS version and date, system memory, storage devices, and processors.
- System Health—Displays options for viewing the current health status of all devices in the system.
- Exit and resume system boot—Exits the system and continues the normal boot process.
- Reboot the System—Exits the system and reboots it by going through the UEFI Boot Order list and launching the first bootable option in the system. For example, you can launch the UEFI Shell, if enabled and listed as the first bootable option in the list.
- Select Language—Enables you to select a language to use in the user interface. English is the default language.
- Setup Browser Selection—Enables you to select the browser.

Common setup and configuration FAQs

1. **How do I access the UEFI System Utilities?**

   See Launching the System Utilities.

2. **How do I transition from RBSU settings to UEFI settings?**

   The BIOS/Platform Configuration (RBSU) menu replaced the ROM-Based Setup Utility (RBSU). Use this menu to access and use UEFI options. See BIOS/Platform Configuration (RBSU).

3. **How do I update the firmware or system ROM?**

   See Updating firmware or system ROM.

4. **How do I select a boot device?**

   See Launching the System Utilities. To access the One-Time Boot Menu where you can select an option for a one-time boot override, do one of following:

   - Press F11 during server POST.
   - On the System Utilities screen, select One-Time Boot Menu. See One-Time Boot Options.

To modify the boot order for all boots, see Changing UEFI boot order.

5. **How do I enable or disable Intel Hyperthreading?**

   By default, Intel Hyperthreading is enabled. To disable or re-enable this setting, see Enabling or disabling Intel Hyperthreading.

6. **How do I configure the Minimum Processor Idle Power Package State to No Package State?**

   By default, this is set to Package C6 (retention) State, the lowest processor idle power state. To change this setting, see Minimum Processor Idle Power Package C-State.

7. **How do I configure the time zone?**

   See Setting the Date and Time.

8. **How do I save my configuration changes and reboot the system?**

   a. When you are done making changes, if you do not see the prompt `Changes are pending. Do you want to save changes and exit?`, press F10 to display it.

   b. Press Y to save your changes.

      A `Change saved` confirmation prompt appears.

   c. Select a reboot option and press Enter:

      - Exit and resume system boot—Exits the system and continues the normal boot process. The system continues through the boot order list and launches the first bootable option in the system.
      - Reboot the System—Exits the system and reboots the system without continuing

        the normal boot process.

9. **How do I enter the Embedded UEFI Shell?**

   See Launching the Embedded UEFI Shell.

10. **How do I view the health status of all installed options and devices?**

    See Viewing System Health.

11. **How do I use CONREP to replicate UEFI settings?**

    See Configuration Replication Utility (CONREP).

12. **How do I set Jitter Control?**

    See Configuring Advanced Performance Tuning options.

13. **How do I tune performance with Workload Profiles?**

    See Workload Profiles and performance options.

14. **How do I use the RESTful Interface Tool or API to replicate the UEFI settings?**

    See the RESTful Interface Tool documentation on the Hewlett Packard Enterprise website (**https://www.hpe.com/info/redfish**).

15. **How do I change the security settings on my server, such as Secure Boot or TPM?**

    See Server Security Options. Also see HPE Gen10 Servers Intelligent System Tuning at **https://www.hpe.com/support/gen10-intelligent-system-tuning-en**.

16. **What is HPE Intelligent System Tuning and how do I use it?**

    HPE Intelligent System Tuning (IST) includes Jitter Smoothing, Workload Matching, and Core Boosting. See Configuring Advanced Performance Tuning Options and Workload Profiles and performance options.

Updating firmware or system ROM

To update firmware or system ROM, use one of the following methods:

- The Firmware Update option in the System Utilities.
- The `fwupadte` command in the Embedded UEFI Shell.
- Service Pack for ProLiant (SPP)
- HPE online flash components.
- Moonshot Component Pack.

System Utilities main menu options

The System Utilities main menu is your starting point for:

- System Configuration
- One-Time Boot Menu
- Embedded Applications
- System Information
- System Health
- Exit and resume system boot
- Reboot the System
- Select Language
- Setup Browser Selection

Subtopics

System Configuration

Subtopics

System Configuration menu options

- BIOS/Platform Configuration (RBSU)
- iLO 6 Configuration Utility
- Other system-specific devices, such as installed PCIe cards, NICs, and Smart Arrays. For example, Embedded FlexibleLOM Port 1.

BIOS/Platform Configuration (RBSU)

The BIOS/Platform Configuration (RBSU) menu contains many of the nested options for accessing UEFI options, including:

- Workload Profile
- System Options
- Processor Options
- Memory Options
- Virtualization Options
- Boot Options
- Network Options
- Storage Options
- Power and Performance Options
- Embedded UEFI Shell Options
- Server Security Options
- PCI Device Configuration Options
- Advanced Options
- Date and Time
- System Default Options

Using the iLO 6 Configuration Utility

Subtopics

iLO 6 Configuration Utility options

You can access the iLO 6 Configuration Utility from the physical system console, or by using an iLO 6 remote console session. The utility has the following options:

- Network Options
- Advanced Network Options
- User Management
- Setting Options
- Set to factory defaults
- Reset iLO
- About

Network Options

- MAC Address (read-only)—Specifies the MAC address of the selected iLO network interface.
- Network Interface Adapter—Specifies the iLO network interface adapter to use.
  - ON—Uses the iLO Dedicated Network Port.
  - Shared Network Port—Uses the Shared Network Port. This option is only available on supported servers.
  - OFF—Disables all network interfaces to iLO.
- Transceiver Speed Autoselect (iLO Dedicated Network Port only)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network.
  This option is only available when Network Interface Adapter is set to ON.
- Transceiver Speed Manual Setting (iLO Dedicated Network Port only)—Sets the link speed for the iLO network interface.
  This option is only available when Network Interface Adapter is set to ON and Transceiver Speed Autoselect is set to OFF.
- Transceiver Duplex Setting (iLO Dedicated Network Port only)—Sets the link duplex setting for the iLO network interface.
  This option is only available when Network Interface Adapter is set to ON and Transceiver Speed Autoselect is set to OFF.
- VLAN Enable (Shared Network Port only)—Enables the VLAN feature.
  When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN. This option is only available when Network Interface Adapter is set to Shared Network Port.
- VLAN ID (Shared Network Port only)—When a VLAN is enabled, specifies a VLAN tag.
  All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094. This option is only available when Network Interface Adapter is set to Shared Network Port.
- DHCP Enable—Configures iLO to obtain its IP address (and many other settings) from a DHCP server.
- DNS Name—Sets the DNS name of the iLO subsystem.
  This name can only be used if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

- IP Address—Specifies the iLO IP address.
  If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
- Subnet Mask—Specifies the subnet mask of the iLO IP network.
  If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
- Gateway IP Address—Specifies the iLO gateway IP address.
  If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.

Configuring Network Options

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > Network Options.
2. Select any of the Network Options, and then select a setting or enter a value for that option.
3. Save your settings.

Advanced Network Options

- Gateway from DHCP—Specifies whether iLO uses a DHCP server-supplied gateway.
- Gateway #1, Gateway #2, and Gateway #3—If Gateway from DHCP is disabled, specifies up to three iLO gateway IP addresses.
- DHCP Routes—Specifies whether iLO uses the DHCP server-supplied static routes.
- Route 1, Route 2, and Route 3—If DHCP Routes is disabled, specifies the iLO static route destination, mask, and gateway addresses.
- DNS from DHCP—Specifies whether iLO uses the DHCP server-supplied DNS server list.
- DNS Server 1, DNS Server 2, DNS Server 3—If DNS from DHCP is disabled, specifies the primary, secondary, and tertiary DNS servers.
- WINS from DHCP—Specifies whether iLO uses the DHCP server-supplied WINS server list.
- Register with WINS Server—Specifies whether iLO registers its name with a WINS server.
- WINS Server #1 and WINS Server #2—If WINS from DHCP is disabled, specifies the primary and secondary WINS servers.
- Domain Name—The iLO domain name. If DHCP is not used, specifies a domain name.

Configuring Advanced Network Options

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > Advanced Network Options.
2. Select any of the Advanced Network Options, and then select a setting or enter a value for that option.
3. Save your settings.

User Management

- Add User
- Edit/Remove User

Add User

Use this option to add new local iLO user accounts, with the following privileges and information.

iLO 6 user privileges

- Administer User Accounts—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users.
  If you do not have this privilege, you can view your own settings and change your own password.
- Remote Console Access—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
- Virtual Power and Reset—Enables a user to power-cycle or reset the host system.
  These activities interrupt the system availability. A user with this privilege can diagnose the system by using the Generate NMI to System button.
- Virtual Media—Enables a user to use the Virtual Media feature on the host system.
- Configure Settings—Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware. This privilege does not enable local user account administration. After iLO is configured, revoking this privilege from all users prevents reconfiguration using the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the iLO 6 Configuration Utility, or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
- **Host BIOS**—Enables a user to configure the host BIOS settings by using the UEFI System Utilities.
- **Host NIC**—Enables a user to configure the host NIC settings.
- **Host Storage**—Enables a user to configure the host storage settings.
- **Recovery Set**—Enables a user to manage the recovery install set.

  NOTE

  By default, the Recovery Set privilege is assigned to the default Administrator account. To assign this privilege to another account, log into the iLO web interface with an account that already has this privilege. This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

New User Information

- New User Name—Specifies the name that appears in the user list on the User Administration page. It does not have to be the same as the Login Name. The maximum length for a user name is 39 characters. The user name must use printable characters. Assigning descriptive user names can help you to easily identify the owner of each login name.
- Login Name—Specifies the name that must be used when logging in to iLO. It appears in the user list on the User Administration page, on the iLO Overview page, and in iLO logs. The Login Name does not have to be the same as the User Name. The maximum length for a login name is 39 characters. The login name must use printable characters.
- Password and Password Confirm—Sets and confirms the password that is used for logging in to iLO. The maximum length for a password is 39 characters. Enter the password twice for verification.

Adding new user accounts

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > User Management > Add User.
2. Select any of the iLO 6 User Privileges.
3. For each option, select one of the following settings.
   - YES —Enables the privilege for this user.
   - NO—Disables the privilege for this user.
4. Select a New User Information entry.
5. Complete each entry for the new user.
6. Create as many user accounts as needed, and then save your settings.

Edit/Remove User

Use this option to edit iLO user account settings, or to delete user accounts.

Editing or removing user accounts

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > User Management > Edit/Remove User.
2. Select the Action menu for the user account you want to edit or delete.
3. Select one of the following.
   - Delete—Deletes the user account.
   - Edit—Enables you to edit the user login name, password or user permissions.
4. Update as many user accounts as needed, and then save your settings.

Setting Options

Use this menu to view and configure iLO access settings.

- iLO 6 Functionality—Specifies whether iLO functionality is available. When this setting is enabled (default), the iLO network is available and communications with operating system drivers are active. When this setting is disabled, the iLO network and communications with operating system drivers are terminated.
  The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled.

  NOTE

  For ProLiant blade servers, the iLO functionality cannot be disabled on blade servers.

- iLO 6 Configuration Utility —Enables or disables the iLO 6 Configuration Utility.
  If this option is set to Disabled, the iLO 6 Configuration Utility menu item is not available when you access the UEFI System Utilities.

- Require Login for iLO 6 Configuration—Determines whether a user-credential prompt is displayed when a user accesses the iLO 6 functionality.
  If this setting is Enabled, provide user credentials for functions, including updating with SUM and RESTful Interface Tool.
- Show iLO 6 IP Address during POST —Enables the display of the iLO network IP address during host server POST.
- Local Users—Enables or disables local user account access.
- Serial CLI Status—Specifies the login model of the CLI feature through the serial port. Settings are:
  - Enabled-Authentication Required—Enables access to the iLO CLP from a terminal connected to the host serial port. Valid iLO user credentials are required.
  - Enabled-No Authentication Required—Enables access to the iLO CLP from a terminal connected to the host serial port. iLO user credentials are not required.
  - Disabled—Disables access to the iLO CLP from the host serial port.
    Use this option if you are planning to use physical serial devices.
- Serial CLI Speed (bits/second)—Specifies the speed of the serial port for the CLI feature. Settings (in bits per second) are:
  - 9600
  - 19200
  - 57600
  - 115200

  For correct operation, set the serial port configuration to no parity, 8 data bits, and 1 stop bit (N/8/1).

  NOTE

  The 38400 speed is supported in the iLO web interface, but is not currently supported by the iLO 6 Configuration Utility.
- iLO Web Interface—Specifies whether the iLO web interface can be used to communicate with iLO. This setting is enabled by default.

Configuring access settings

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > Setting Options.
2. Update user access Setting Options.
3. Save your settings.

Set to factory defaults

CAUTION

This operation clears all user and license data.

Use this option to reset iLO to the factory default settings. When you do so, you cannot access the iLO 5 Configuration Utility until after the next system reboot. If you are managing iLO remotely, the remote console session is automatically ended.

If the server has a factory installed license key, the license key is retained.

Resetting iLO to the factory default settings

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > Set to factory defaults.

   The iLO 6 Configuration Utility prompts you to select YES or NO.
2. Select YES.
3. When prompted to confirm the reset, press Enter.

   iLO resets to the factory default settings. If you are managing iLO remotely, the remote console session is automatically ended.
4. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The iLO 6 Configuration Utility screen is still open from the previous session.
   b. Press Esc until the main menu is displayed.
   c. Select Exit and Resume Boot in the main menu, and then press Enter.
   d. When prompted to confirm the request, press Enter to exit the screen and resume the boot process.

Reset iLO

If iLO is slow to respond, you can use this option to perform a reset.

Resetting iLO with this method does not make any configuration changes, but it ends all active connections to iLO. When you reset iLO, the iLO 6 Configuration Utility is not available again until the next reboot.

Resetting iLO active connections

About this task

Prerequisite

Configure iLO Settings privilege

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > Reset iLO.

   The iLO 6 Configuration Utility prompts you to select YES or NO.
2. Select YES.
3. When prompted to confirm the reset, press Enter.

   Active iLO connections are reset. If you are managing iLO remotely, the remote console session is automatically ended.
4. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The UEFI System Utilities are still open from the previous session.

b. Press Esc until the main menu is displayed.

c. Select Exit and Resume Boot in the main menu, and press Enter.

d. When prompted to confirm the request, press Enter to exit the utility and resume the normal boot process.

About

Use this menu to view information about the following iLO components.

- Firmware Date—The iLO firmware revision date.
- Firmware Version—The iLO firmware version.
- iLO CPLD Version—The iLO complex programmable logic device version.
- Host CPLD Version—The server complex programmable logic device version.
- Serial Number—The iLO serial number.
- PCI BUS—The PCI bus to which the iLO processer is attached.
- Device—The device number assigned to iLO in the PCI bus.

Viewing information about iLO

Procedure

1. From the System Utilities screen, select System Configuration > iLO 6 Configuration Utility > About.
2. View information about iLO components.

Viewing and configuring embedded device information

Subtopics

Viewing controller information

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Controller Information.
2. In the Controller Information screen, view the information.

Configuring controller settings

Subtopics

- Configuring Embedded Devices

Configuring Embedded Devices

For information on configuring controllers and other embedded devices using the RBSU interface, see the document resources listed in the table below:

For	Refer to
SR Controllers	HPE SR Gen11 Controller User Guide
MR Controllers	HPE MR Gen11 Controller User Guide
Intel VROC	Intel Virtual RAID on CPU for HPE User Guide
NS Boot Device	HPE NS204i Boot Device User Guide
HPE iLO	HPE iLO 6 User Guide

Configure arrays

The topics in this section provide information on arrays based on HPE SR Gen11 controllers. For information on HPE MR Gen11 controllers, see the HPE MR Gen11 Controller User Guide.

Subtopics

- Creating an array using UEFI System Utilities
- Viewing logical drive properties
- Creating a logical drive
- Assigning spare drives
- Deleting a spare drive
- Identifying a device
- Deleting an array
- Editing a logical drive
- Deleting a logical drive

Creating an array using UEFI System Utilities

About this task

When you create an array, you can select drives, specify RAID level, and configure array settings, including strip size and logical drive size.

Procedure

1. From the UEFI System Utilities screen, select **System Configuration > RBSU > Array Configuration > Create Array** .
2. In the Create Array screen, select each drive that you want to include in the array and click Proceed to next Form.

3. In the Set RAID Level screen, select the RAID Level from the drop-down menu and click Proceed to next Form.
4. In the Set Logical Drive Configuration screen, specify the configuration settings or use the default selection.

Setting	Description
Logical Drive Label	Use the default selection for the drive label or enter a new label. The characters in the label can be alphanumeric or spaces.
Strip Size/Full Stripe Size	Strip size is the amount of data that is stored on each physical drive in the array. The full stripe size is the amount of data that the controller can read or write simultaneously on all the drives in the array. For RAID levels that support fault tolerance through parity, the parity information is calculated one full strip size at a time. For hardware RAID, you can specify from 16KiB up to 256KiB, depending on the number of disks and RAID level. The default value is all available space.
Size	Values in decimal; minimum RAID size is 16 MiB.
Unit Size	Logical drive unit size (MiB/GiB/TiB).
Acceleration Method	Logical drive acceleration method (HPE SSD Smart Path, Controller Cache or none).

5. Click Submit Changes.
6. Return to the main menu.
7. Click OK when prompted to save your changes.
8. Reboot the server.

Viewing logical drive properties

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > List Logical Drives > *logical drive* > Logical Drive Details.
2. In the Logical Drive Details screen, view the details.

Creating a logical drive

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > Create Logical Drive.
2. In the Create Logical Drive screen, select the RAID level, and then click Proceed to next Form.
3. In the Set Logical Drive Configuration screen, use the default values for the configuration or specify different values.

Setting	Description
Logical Drive Label	Use the default selection for the drive label or enter a new label. The characters in the label can be alphanumeric or spaces.
Strip Size/Full Stripe Size	Strip size is the amount of data that is stored on each physical drive in the array. The full stripe size is the amount of data that the controller can read or write simultaneously on all the drives in the array. For RAID levels that support fault tolerance through parity, the parity information is calculated one full strip size at a time. You can specify from 16KiB to 256KiB, depending on the number of disks and RAID level. The default value is all available space.
Size	Values in decimal; minimum RAID size is 16 MiB.
Unit Size	Logical drive unit size (MiB/GiB/TiB).
Acceleration Method	Logical drive acceleration method (controller cache or none).

4. Click Submit Changes.

Assigning spare drives

Prerequisites

A spare drive must meet the following criteria.

- It must be an unassigned drive or a spare drive for another array.
- It must be the same type as existing drives in the array (for example, SATA or SAS).
- The drive capacity must be greater than or equal to the smallest drive in the array.

About this task

A spare is a drive that automatically replaces a failed drive in a logical drive.

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > Manage Spare Drives.
2. In the Manage Spare Drives screen, select the spare activation type:
   - Assign Dedicated Spare
   - Assign Auto Replace Spare
3. Select the drive that you want to assign as a spare.

> **NOTE**
>
> Only drives that meet the criteria listed in the prerequisites are displayed.

Deleting a spare drive

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > Manage Spare Drives > Delete Spare Drives.
2. From the Delete Spare Drives screen, select the spare that you want to delete, and click Delete Spare Drives.

Identifying a device

About this task

Use the UEFI System Utilities to identify a drive by turning on its device identification LED.

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > Identify Device.
2. In the Identify Device screen, specify the duration (in seconds) that you want the LED to be on, select the drive configuration type, and click Start.

Results

To turn off the LED, click **Stop**.

Deleting an array

About this task

This procedure deletes:

- All the logical drives on the array.
- All data on the logical drives that are part of the array.

If the deleted array is the only one on the controller, the controller settings are erased, and the default configuration is restored.

To delete an individual logical drive, see "Deleting a logical drive."

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > Delete Array.
2. In the Delete Array screen, click Submit Changes.

Editing a logical drive

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > List Logical Drives > *logical drive* > Edit Logical Drive.
2. In the Edit Logical Drive screen, edit any of the following settings.

Setting	Description
Acceleration method	Acceleration method can increase database performance by writing data to the cache memory instead of directly to the logical drives. Options are: • Controller cache--writes data to the cache memory. • None--disables caching to reserve the cache module for other logical drives on the array.
Logical drive label	This label value appears in the Logical Drive Details screen. The label can contain alphanumeric characters and spaces only.

3. Click Submit Changes.

Deleting a logical drive

About this task

Use this procedure to delete an individual logical drive. To delete all logical drives in an array, see "Deleting an array."

IMPORTANT

If you delete the logical drive, any data on the logical drive is deleted as well. If the logical drive that you are deleting is the only logical drive in the array, the array is also deleted.

For information on deleting a logical drive on arrays based on HPE MR Gen11 Controllers, see **this**.

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Array Configuration > Manage Arrays > *array* > List Logical Drives > *logical drive* > Delete Logical Drive.
2. In the Delete Logical Drive screen, click Submit Changes.

Disk Utilities

Subtopics

Viewing disk device information

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Disk Utilities > *disk* > Device Information.
2. In the Device Information screen, view the information.

Identifying a disk device

Procedure

1. From the System Utilities screen, select System Configuration > *controller* > Disk Utilities > *disk* > Identify Device.
2. In the Identify Device screen, specify the duration (in seconds) that you want the LED to be on, select the drive configuration type, and then click **Start**.

Results

To stop blinking the LED, click **Stop**.

Viewing and configuring NIC and FCoE settings

About this task

Use the System Configuration screens to view information about and configure installed system devices, such as embedded NICs and FCoEs. Devices listed and configuration options available vary by system.

Procedure

1. From the System Utilities screen, select System Configuration.
2. Select a device.

   A System Configuration screen displays information about the embedded device.
3. View, select, or enter settings.
4. Save your settings.

One-Time Boot Menu

Subtopics

One-Time Boot Menu options

Use the One-Time Boot Menu to select a UEFI boot option for a one-time boot override. The option you select does not modify your predefined boot order settings. If you use a USB key or virtual media through the iLO Remote Console, exit and re-enter the System Utilities to refresh this menu so that the devices appear.

Boot options include:

- OS boot manager, such as Windows Boot Manager—Lists the boot manager for your installed OS.
- Generic USB Boot—Provides a placeholder for any USB device that is bootable in UEFI. You can set the boot priority of this option, and retain this priority for use with USB devices you might install in the future. Setting this priority does not affect priorities set for individual USB devices in the UEFI Boot Order list.

NOTE

This option is only available in UEFI Mode. The system attempts to boot all UEFI bootable USB devices in the order you specify in the Generic USB Boot entry, even if installed individual USB devices are configured lower in the boot order.

- Internal SD Card
- Embedded Flexible LOMs
- Embedded UEFI Shell
- Embedded SATA Port
- Run a UEFI Application from a file system —Enables you to select a UEFI application to run from a file system. You can browse all FAT file systems that are available in the system. You can also select an x64 UEFI application (with an .EFI extension) to execute (can be an OS boot loader or any other UEFI application).
- Embedded iPXE

Selecting an option for a one-time boot

Procedure

1. From the System Utilities screen, select One-Time Boot Menu.
2. Select a One-Time Boot Menu option.

Embedded Applications

Subtopics

Launching the Embedded UEFI Shell

Prerequisites

- Embedded UEFI Shell is set to Enabled.

About this task

Use the Embedded UEFI Shell option to launch the Embedded UEFI Shell. The Embedded UEFI Shell is a preboot command-line environment for scripting and running UEFI applications, including UEFI boot loaders. The Shell also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS.

Procedure

1. From the System Utilities screen, select Embedded Applications > Embedded UEFI Shell.

   The Embedded UEFI Shell screen appears.

2. Press any key to acknowledge that you are physically present.

   This step ensures that certain features, such as disabling Secure Boot or managing the Secure Boot certificates using third-party UEFI tools, are not restricted.

3. If an administrator password is set, enter it at the prompt and press Enter.

   The `Shell>` prompt appears.

4. Enter the commands required to complete your task.

5. Enter the `exit` command to exit the Shell.

Viewing or clearing the Integrated Management Log

About this task

Use the Integrated Management Log (IML) option to view or clear the record of historical events that have occurred on the server. Entries in the IML can help you diagnose issues or identify potential issues. The IML time stamps each event with one-minute granularity.

Procedure

1. From the System Utilities screen, select Embedded Applications > Integrated Management Log.

2. Select an option.

   - View IML—Displays the Integrated Management Log records.
   - Clear IML—Clears all entries in the Integrated Management Log.

Downloading an Active Health System Log

About this task

By default, the system downloads an Active Health System Log from the previous seven days if you do not use the Range Start Date and Range End Date fields to specify a different time period. When requested by Hewlett Packard Enterprise Support, you can copy your stored `.ahs` file, and email it to your customer support representative.

Procedure

1. From the System Utilities screen, select Embedded Applications > Active Health System Log.

2. Select Download Active Health System Log.

3. Select or enter the following.

   - Download Entire Log—Unless a support representative advises you to download AHS records for the life of the server, leave this disabled (not selected). The default setting is disabled.
   - Range Start Date—Enter a starting date for log collection.
   - Range End Date—Enter an ending date for log collection.
   - Select File Location—Select this option to open a File Explorer screen and select the FAT16 FAT32 partition on local or virtual writable media on which to download the AHS log.

NOTE

Hewlett Packard Enterprise recommends storing AHS logs on USB or HDD media. Storing logs on SD cards is not supported.

- Optional: Add your customer information, including support case number, and contact information.

4. Select Start Download.

   The UEFI firmware communicates with iLO to download the requested AHS log files and package them into one `.ahs` file.

5. When requested by Hewlett Packard Enterprise Support, copy your stored `.ahs` file, and email it to your customer support representative.

Results

NOTE

You can also download AHS log files by selecting System Utilities > System Health > Download Active Health System Log.

Launching Embedded Diagnostics

About this task

Use the Embedded Diagnostics option to launch the Hardware Diagnostics menu. From there, you can view health summary status, run system tests and component tests, and view test logs.

Procedure

1. From the System Utilities screen, select Embedded Applications > Embedded Diagnostics.

   The Hardware Diagnostics screen appears.

2. Select an option.

   - System Health—Lists a Health Summary (status for BIOS hardware, fans, temperature, battery, memory, network, and storage), Fans (zone, label, status, and speed), Temperature (label, location, status, current reading, and cautions), Power Supplies (power supply summary and smart storage battery), Processors, Memory, NIC Information, Storage, and Firmware Information.
   - System Tests—Lists information and gives you options for checking hardware subsystems to ensure that they are working properly. The Quick Test option performs a 10-minute check of the hardware. The Extensive Test option performs a full check of the hardware and can take two or more hours to complete.
   - Component Tests—Lists information and gives you options for checking Processor, Memory, Hard Drive, Keyboard, Mouse, Network, Optical Drive, System Board, USB Port, and Video tests.
   - Test Logs—Displays test logs, which contain information about test type and results, including failures.
   - IML Log—Displays all IML log files, which include information about the severity, class, initial time, and update time.
   - Language—Selects your language for the Embedded Diagnostics.
   - Exit—Exits the Embedded Diagnostics menu and returns you to the System Utilities screen.

Launching Intelligent Provisioning

About this task

Intelligent Provisioning is an embedded, single-server deployment tool that simplifies server setup, providing a reliable and consistent way to deploy server configurations. The Intelligent Provisioning option lets you select the Intelligent Provisioning host override option for this boot only. It does not modify the normal boot order or boot mode settings. For more information, see the Intelligent Provisioning user guide on the Hewlett Packard Enterprise website (**https://www.hpe.com/info/intelligentprovisioning/docs**).

Procedure

1. From the System Utilities screen, select Embedded Applications > Intelligent Provisioning.
2. To return to the System Utilities menu, reboot the server.

Launching Embedded iPXE

Prerequisites

Embedded iPXE is Enabled.

About this task

Use the Embedded iPXE option to launch the Embedded iPXE. Embedded iPXE provides a full PXE implementation enhanced with additional features.

Procedure

From the System Utilities screen, select Embedded Applications > Embedded iPXE.

The Embedded iPXE launches and it performs the operations specified by Network Options > Embedded iPXE.

System Information and System Health

Subtopics

System Information

Use this option to view:

- Summary—Shows a summary of system settings, including:
  - System Name
  - Serial Number
  - Product ID
  - BIOS Version Power Management Controller FW Version User Defaults
  - System Memory
  - Processor types

- iLO Firmware Version
- Embedded Network Devices

- Processor Information—Shows detailed processor information, including:
  - CPU number, Socket number, and Socket Locator label
  - Whether the CPU socket is Populated with a CPU package
  - A brief CPU Manufacturer Description and a list of Characteristics that the CPU supports
  - The Core Count, the number of enabled cores, and Thread Count (number of logical cores) in the CPU package
  - The Rated Speed and External Clock Speed of the CPU
  - The Voltage of the CPU package
  - A list of Microcode Patches installed by the BIOS
  - L1, L2, and L2 cache size and speed
- Memory Information—Shows detailed memory information, including:
  - Total System Memory
  - Total Memory Slots
  - Operating frequency and voltage
  - The Number of Slots connected to the CPU
  - The number of Installed Modules that are directly connected to the CPU
- Storage Information
- PCI Device Information—Shows detailed information about each PCI device.
- Firmware Information—Shows detailed firmware information.
  Export System Information to file—Opens a screen where you can:
  1. Select file location—Select or specify a new file for the exported information.
  2. Select which type of system information to export:
     - Summary
     - Processor
     - Memory
     - PCI device
     - Firmware
  3. To export the information, save your selections, and then exit the System Utilities.

Viewing System Information

Procedure

1. From the System Utilities screen, select System Information.
2. Select an option to display related information.

Results

NOTE

You can also view firmware information using the RESTful Interface Tool. See the RESTful Interface Tool documentation at **https://www.hpe.com/info/restfulinterface/docs**.

Viewing System Health

About this task

Use the System Health option to check the health status of all devices in the system. This screen shows, for example, the presence of any unsupported devices found during the boot process.

Procedure

1. From the System Utilities screen, select System Health.
2. Select View System Health.

Rebooting the system, selecting a language, and setting the browser mode

Subtopics

Rebooting the system

Subtopics

Exiting and resuming system boot

About this task

Use the Exit and resume system boot option to exit the system and continue the normal boot process. The system continues through the boot order list and launches the first bootable option in the system. For example, you can launch the UEFI Embedded Shell, if it is enabled and selected as first bootable option in the UEFI Boot Order list.

Procedure

1. From the System Utilities screen, select Exit and resume system boot.

   A confirmation message appears.
2. Click OK or press Enter.

Rebooting the system

About this task

Use the Reboot the System option to exit the system and reboot without continuing with the normal boot process.

Procedure

1. From the System Utilities screen, select Reboot the System.

   A confirmation message appears.

2. Click Yes, Reboot, or press Enter.

Selecting a language and browser mode

Subtopics

Selecting a system language

Procedure

1. From the System Utilities screen, select Select Language.
2. Select a language.
   - English
   - Japanese
   - Simplified Chinese
3. Save your setting.

Selecting a browser mode

Procedure

1. From the System Utilities screen, select Setup Browser Selection.
2. Select a setting.
   - GUI—Opens a GUI-based browser when you access the System Utilities using the Integrated Remote Console or a physical terminal.
   - Text—Opens a text-based browser when you access the System Utilities using a serial console.
   - Auto—Depending on how you access the System Utilities, opens either a text-based browser, or a GUI-based browser.
3. Save the setting.

More information

- Navigating the System Utilities in GUI mode

BIOS/Platform Configuration Options

Subtopics

What's new in Gen11?

In Gen11, changes to BIOS options include feature additions, deprecation of certain features and changes to the values of configurable RBSU options. See the subtopics for more information.

Subtopics

RBSU AMD options

To identify the new and deprecated AMD options, and to find the change of configurable AMD option values in RBSU between Gen10 Plus and Gen11, see the following table:

Option Name	Path	Gen10 Plus	Gen11
Removable Flash Media Boot Sequence	System Options > USB Options	• Internal Keys First • External Keys First (Default)	N/A
Processor x2APIC Support	Processor Options	• Auto (default) • Force Enabled • Disabled	• Auto (default) • Force Enabled
Memory Interleave Size	Memory Options	256 (default)/512/1024/2048/4096	N/A

Option Name	Path	Gen10 Plus	Gen11
PCIe Configuration MMIO (MCFG) Base at 3GB	Memory Options	• Auto • Disabled (default)	N/A (No legacy boot in Gen11)

Maximum Memory Bus Frequency	Memory Options	Auto (default)/2933/2667/2400	• **4th Gen EPYC Processor**
			  ○ Auto (default)/3600/4000/4400/4800
			• **5th Gen EPYC Processor**
			  ○ Auto (default)/3600/4000/4400/4800/5200/5600/6000/6400

AMD Secure Nested Paging	Memory Options > Memory Encryption Options	N/A	• Enabled • Disabled (default)
AMD eMCR Boot-Time Reduction	System Options > Boot Time Optimizations	N/A	• Enabled (default) • Disabled

AMD xGMI Link Speed	Power and Performance Options	• Auto (Default)
		• 16 Gbps
		• 18 Gbps
			• **4th Gen EPYC Processor**
			  ○ Auto (Default)
			  ○ 16 Gbps
			  ○ 18 Gbps
			  ○ 25 Gbps
			  ○ 32 Gbps
			• **5th Gen EPYC Processor**
			  ○ Auto (Default)
			  ○ 20 Gbps
			  ○ 25 Gbps
			  ○ 32 Gbps

Maximum SEV ASID	Virtualization Options	• ASIDCount253 • ASIDCount509 (default)	N/A
AMD 5-Level Page	Virtualization Options	N/A	• Enabled • Disabled (default)
AMD Performance Workload Profile	Power and Performance Options	• … • Accelerator Throughput	• Disabled (default) • IOT Gateway • HPC Optimized • OpenStack NFV • OpenStack for RealTime Kernel
Minimum Processor Idle Power Core C-State	Power and Performance Options	• No C-States • C6 (Default)	• No C-States • C1 • C6 (Default)
Preferred I/O Bus	Power and Performance Options > IO Options	• Enabled • Disabled (default)	N/A

Option Name	Path	Gen10 Plus	Gen11
Preferred I/O Bus Number	Power and Performance Options > IO Options	0-255	N/A
NBIOO Bus Base (Hex)	Power and Performance Options > IO Options > NbioLclkDpm Level	0 (default)-255	N/A
NBIOO Bus Limit (Hex)	Power and Performance Options > IO Options > NbioLclkDpm Level	0 (default)-255	N/A
NBIOO LCLK DPM Level	Power and Performance Options > IO Options > NbioLclkDpm Level	• Auto (Default) • Static Low • Static High	N/A
AMD Virtual DRTM Device	Server Security > Advanced Security Options		• Enabled • Disabled (default)
Enhanced Preferred I/O	Power and Performance Options > IO Options	• Enabled • Disabled (default)	N/A
PCIe Hot Plug Error Control	PCIe Device Configuration > Advanced PCIe Configuration	• Hot-Plug Surprise (Default) • eDPC Firmware FIRST • eDPC OS FIRST	• Hot-Plug Surprise (Default) • eDPC Firmware Control • eDPC OS Control **NOTE** • In DL325, DL345, DL365, and DL385 Gen11, support for PCIe Hot-Plug Error Control starts with 2.30 ROM for AMD 5th Generation EPYC processors, and with 2.40 ROM for AMD 4th Generation EPYC processors. • In DL145 Gen11, support for PCIe Hot-Plug Error Control starts with 1.60 ROM for AMD 4th Generation EPYC processors.
Support Dynamic PCIe Rate Change	PCIe Device Configuration > Advanced PCIe Configuration	• Enabled • Disabled (default)	N/A
NVMe PCIe Resource Padding	PCIe Device Configuration > Advanced PCIe Configuration	• Normal (Default) • Medium • High	• Disabled (default) • Enabled
UEFI Variable Access Firmware Control	Server Security > Advanced Security Options	N/A	• Disabled (default) • Enabled

Option Name	Path	Gen10 Plus	Gen11

Infinity Fabric Performance State	Power and Performance Options > Advanced Power Options	• Auto
		• P0
		• P1
		• P2
		• P3
			• 4th Gen EPYC Processor
			  ○ Auto
			  ○ P0
			  ○ P1
			  ○ P2
			  ○ P3
			• 5th Gen EPYC Processor
			  ○ Auto
			  ○ P0
			  ○ P1
			  ○ P2

Extended Memory Test	System Options > Boot Time Optimizations	• Disabled (default) • Enabled	N/A
AMD Periodic Directory Rinse	Memory Options	• Disabled (default) • Enabled	N/A

AMD Periodic Directory Rinse Tuning	Processor Options	N/A	• 4th Gen EPYC Processor
			  ○ Auto (Default)
			  ○ Memory-Sensitive
			  ○ Cache-Bound
			  ○ Neutral
			  ○ Adaptive
			• 5th Gen EPYC Processor
			  ○ Auto (Default)
			  ○ Periodic
			  ○ Blended

ACPI CST C2 Latency	Power and Performance Options	N/A	• 4th Gen EPYC Processor
			  ○ 800 microsecond (Default)
			  ○ 18 microsecond
			• 5th Gen EPYC Processor
			  ○ 100 microsecond (Default)
			  ○ 18 microsecond

AMD DMA Remapping	Virtualization Options	• Enabled
		• Disabled (Default)
			• 4th Gen EPYC Processor
			  ○ Enabled
			  ○ Disabled (Default)
			• 5th Gen EPYC Processor
			  ○ N/A

Option Name	Path	Gen10 Plus	Gen11

AMD DMAr Support	Virtualization Options	N/A	• 4th Gen EPYC Processor
			  ◦ N/A
			• 5th Gen EPYC Processor
			  ◦ Enabled
			  ◦ Disabled (Default)

AMD DMA Protection	Virtualization Options	N/A	• 4th Gen EPYC Processor
			  ◦ N/A
			• 5th Gen EPYC Processor
			  ◦ Enabled
			  ◦ Disabled (Default)

FP512	Processor Options	N/A	• 4th Gen EPYC Processor
			  ◦ N/A
			• 5th Gen EPYC Processor
			  ◦ Enabled (Default)
			  ◦ Disabled

Related topics

- Enabling or disabling AMD Secure Nested Paging
- Enabling AMD 5-Level Page
- Configuring UEFI Variable Access Firmware Control

RBSU Intel® Xeon® Scalable processor options

To identify the new and deprecated Intel options, and to find the change of configurable Intel® Xeon® Scalable processor option values in RBSU between Gen10 Plus and Gen11, see the table below:

Option Name	Path	Gen10 Plus	Gen11
Processor x2APIC Support	Processor Options	• Enabled (default) • Disabled • Force Enabled	• Auto (default) • Force Enabled
Maximum Memory Bus Frequency	Memory Options	• Auto (default) • 1867 • 2133 • 2400 • 2667 • 2933	• Auto (default) • 3200 • 3600 • 4000 • 4400 • 4800
Embedded SATA Configuration	Storage Options > SATA Options	• Ahci (default) • SmartRAIDSwRaid • IntelVrocSata	• Ahci (default) • IntelVrocSata

Option Name	Path	Gen10 Plus	Gen11
Intel(R) VROC Support	Storage Options > NVMe Options > Intel NVMe Option	• None (default) • VmdForIntelNvme • VmdForHpeNvme	• None (default) • Raid1 Only • Premium
Intel(R) Software Guard Extensions (SGX)	Server Security > Intel Security Options	• Enabled • Disabled (default) • Factory Reset	• Enabled • Disabled (default)
SGX Factory Reset	Server Security > Intel Security Options	N/A	• Enabled • Disabled (default)
Minimum Processor Idle Power Package C-State	Power and Performance Options	• C6 NonRetention • No State	• C6 Retention (default) • C6 NonRetention • No State
Intel Performance Monitoring Support	Power and Performance Options	• Enabled • Disabled (default)	N/A
Local/Remote Threshold	Power and Performance Options	• Auto (default) • Low • Medium • High	N/A
Enhanced Processor Performance	Power and Performance Options > Advanced Performance Tuning Options	• Disabled (default) • Enabled	N/A
Enhanced Processor Performance Profile	Power and Performance Options > Advanced Performance Tuning Options	• Conservative • Moderate • Aggressive	• Disabled (default) • Conservative • Moderate • Aggressive
PCI Peer to Peer Serialization	Power and Performance Options > Advanced Performance Tuning Options	• Disabled • Enabled (default)	N/A
NVMe PCIe Resource Padding	PCIe Device Configuration Options > Advanced PCIe Device Settings	• Normal (default) • Medium • High	• Disabled (default) • Enabled
EmbSATA3Enable/Aspm/PCIeOptionROM	PCIe Device Configuration Options > Embedded SATA3 Configuration	N/A	• Auto • Disabled
VMWare Proprietary Page Retire Support	Advanced Options	• Enabled (default) • Disabled	N/A (VMWare proprietary solution dropped.)
UEFI Variable Access Firmware Control	Server Security > Advanced Security Options	N/A	• Disabled (default) • Enabled

Option Name	Path	Gen10 Plus	Gen11
HBM Memory Mode **NOTE** HBM Memory Options are available only on ROM versions 1.32 and later, not on an earlier ROM version.	Memory Options > HBM Memory Options > HBM Memory Mode	N/A	• 2LM • 1LM

Related Topics

- Enabling or disabling SGX Factory Reset
- Configuring UEFI Variable Access Firmware Control
- Configuring the HBM Memory Options

RBSU Intel® Xeon® E processor options

To identify the new and deprecated RBSU Intel® Xeon® E processor options, and to find the change of configurable Intel® Xeon® E option values in RBSU between Gen10 Plus and Gen11, see the table below:

Option Name	Path	Gen10 Plus	Gen11
Processor x2APIC Support	Processor Options	• Enabled (default) • Disabled • Force Enabled	• Auto (default) • Force Enabled
Maximum Memory Bus Frequency	Memory Options	• Auto (default) • 1867 • 2133 • 2400 • 2667 • 2933	• Auto (default) • 2933 • 3200 • 3600 • 4000 • 4400
Row Hammer Mode	Memory Options	N/A	• Auto (default) • pTRR • Disabled
Memory Remap	Memory Options	N/A	• No action (default) • All memory
Total Memory Encryption (TME)	Memory Options > Memory Encryption Options	N/A	• Disabled (default) • Enabled
SR-IOV	Virtualization Options	N/A	• Enabled (default) • Disabled
Intel(R) Software Guard Extensions (SGX)	Server Security > Intel Security Options	• Enabled • Disabled (default) • Software controlled	N/A
Minimum Processor Idle Power Core C-State	Power and Performance Options	• C6 State • C3 State • No C-States	• C6 State • No C-States
Local/Remote Threshold	Power and Performance Options	• Auto (default) • Low • Medium • High	N/A
Enhanced Processor Performance	Power and Performance Options > Advanced Performance Tuning Options	• Disabled (default) • Enabled	N/A
Enhanced Processor Performance Profile	Power and Performance Options > Advanced Performance Tuning Options	N/A	• Disabled (default) • Enabled
Intel DMI Link Frequency	Power and Performance Options	• Auto (default) • Gen1 Speed • Gen2 Speed	• Auto (default) • Gen1 Speed • Gen2 Speed • Gen3 Speed

Related Topics

Configuring Row Hammer mode

RBSU Ampere options

To identify the new Ampere options, see the table below:

Ampere Options	Path	Gen11
ANC mode	Processor Options	• Monolithic (default) • Hemisphere • Quadrant
SLC as L3 cache	Processor Options	• Enable • Disable (default)
Prefetcher	Processor Options	• Enable (default) • Disable
ECC mode	Memory Options	• Auto (default) • SECDED • Symbol
ECC control	Memory Options	• DE enabled • FI enabled • DE and FI enabled (default)
Patrol scrub	Memory Options	• Enable (default) • Disable
Demand scrub	Memory Options	• Enable (default) • Disable
Fine Granularity Refresh (FGR)	Memory Options	• 1x (default) • 2x • 1x with RowHammer • 2x with RowHammer
APEI support	Power Options	• Enable (default) • Disable
CPPC support	Power Options	• Enable (default) • Disable
LPI support	Power Options	• Enable (default) • Disable
ARM SMMU PMU	Virtualization Options	• Enable • Disable (default)
Ampere Max Performance	Power Options	• Enable (default) • Disable

RBSU Common options

Option Name	Path	Gen10 Plus	Gen11
Current TPM Type	Server Security > TPM Options	• No Tpm (default) • Tpm12 • Tpm20	N/A
Current TPM FIPS mode	Server Security > TPM Options	• Not specified (default) • Non FIPs Mode • FIPs Mode	N/A
TpmActivePcrs	Server Security > TPM Options	• Not Specified (default) • sha1 • sha256 • Sha1Sha256	• Not Specified (default) • sha1 • sha256 • Sha384 • Sha1Sha256 • Sha256Sha384
Current TPM 2.0 Software Interface Status	Server Security > TPM Options	• No action (default) • FIFO • Crb	• No action • FIFO (default)
TPM 1.2 Operation	Server Security > TPM Options	• No action (default) • Enable • Disable • Clear	N/A **NOTE** Gen11 is TPM 2.0 only.
TPM Mode Switch Operation	Server Security > TPM Options	• No action (default) • Tpm12 • Tpm20	N/A
TPM 2.0 Software Interface Operation	Server Security > TPM Options	• No action (default) • FIFO • Crb	N/A
TPM FIPS Mode Switch	Server Security > TPM Options > TPM Advanced Options	• No action (default) • Regular mode • FIPs mode	N/A
No-Execute Protection	Server Security > Advanced Security Options	• Enabled (default) • Disabled	N/A
NVM Express Smart RAID SW RAID Support	Storage Options > NVMe Options > NVMe RAID Options	• Enabled • Disabled (default)	N/A **NOTE** SWRAID dropped in Gen11.
PCI Slot X Bifurcation	PCIe Device Configuration > Advanced PCIe Configuration > PCIeBifurcationOptions	• Auto (default) • Bifurcate • Dual Bifurcate	• No Bifurcation (Default) • Bifurcate • Dual Bifurcate

Option Name	Path	Gen10 Plus	Gen11
Maximum PCI Express Speed	PCIe Device Configuration > Advanced PCIe Configuration	• PerPortCtrl (default) • PcieGen1 • PcieGen2 • PcieGen3	• PerPortCtrl (default) • PcieGen1 • PcieGen2 • PcieGen3 • PcieGen4
Time Zone	Date Time		UtcWET **NOTE** Changed from UTCO for Dublin and London.
UEFI Optimized Boot	Boot Options	• Enabled (default) • Disabled	N/A **NOTE** Legacy boot mode is now deprecated.

Workload profiles and performance options

Workload Profiles is one of the HPE Intelligent System Tuning (IST) features and allows you to tune the resources in your HPE ProLiant server by choosing a preconfigured workload profile. The server will automatically configure the BIOS settings to match the selected workload.

System provided workload profiles

The system provides these Workload Profiles:

General Power Efficient Compute

This profile is the default profile for most ProLiant servers and HPE Synergy compute modules.

This profile applies the most common performance settings that benefit most application workloads while also enabling power management settings that have minimal impact to overall performance. The settings that are applied heavily favor a balanced approach between general application performances versus power efficiency.

This profile is recommended for customers that do not typically tune their BIOS for their workload.

General Peak Frequency Compute

This profile is intended for workloads that generally benefit from processors or memory that must achieve the maximum frequency possible, for any individual core, at any time. Power management settings are applied when they ensure that any component frequency upside can be readily achieved. Processing speed is favored over any latencies that might occur. This profile is a general-purpose profile, so optimizations are done generically to increase processor core and memory speed.

This profile benefits workloads that typically benefit from faster compute time.

General Throughput Compute

Use this profile for workloads where you need the total maximum-sustained workload throughput. When the processor runs at the highest individual core speed, it does not necessarily result in an increased throughput. Rather when the processor is able to perform sustained work across all available cores during maximum utilization, it results in an increased throughput. Power management settings are disabled when they are known to have impact on maximum achievable bandwidth.

Best throughput is achieved when the workload is also (Nonuniformed Memory Access) NUMA aware and optimized, so settings that benefit NUMA awareness are applied.

Virtualization - Power Efficient

Use this profile for virtualization environments. The profile ensures that all available virtualization options are enabled. Certain

virtualization technologies can have possible performance impacts to nonvirtualized environments and can be disabled in other profiles. Power management settings can have an impact on performance when running virtualization OS. This profile applies power management settings that are virtualization friendly.

Virtualization - Max Performance

Use this profile for virtualization environments. The profile ensures that all available virtualization options are enabled. Power management settings are disabled in favor of delivering maximum performance.

Low Latency

This profile is for customers who want the least amount of computational latency for their workloads. This profile follows the most common best practices that are documented in the HPE Low Latency Whitepaper. Maximum speed and throughput are often sacrificed to lower overall computational latency. Power management and other management features that might introduce computational latency are also disabled.

The profile benefits customers running Real-Time OS (RTOS) or other transactionallatency-sensitive workloads.

Mission Critical

This profile is for customers who trade off performance for server reliability above the basic server defaults. The profile enables advanced memory reliability, availability, and serviceability (RAS) features that are known to have more than a measurable impact to computational performance. Enabling this profile will have an impact to maximum memory bandwidth and will increase memory latency.

Transactional Application Processing

This profile is for business processing environments, such as online transaction processing (OLTP) applications that require a database back-end. For example, workloads typically comprise a high number of user-based, transactional applications running on a single server with cohosted database component. The profile balances the requirement of managing both peak frequency and throughput.

High Performance Compute (HPC)

This profile is for customers running in a traditional HPC environment. Typically, these environments are clustered environments where each node performs at maximum utilization for extended periods of time to solve large-scale scientific and engineering workloads. The default for our Apollo series servers, power management is typically disabled in favor of sustained available bandwidth and processor compute capacity. This profile is similar to the Low Latency profile except that some latency is accepted to achieve maximum throughput.

Decision Support

This profile is for Enterprise Business Database (Business Intelligence) workloads that are focused on operating data warehouses, such as data mining or online analytical processing (OLAP).

Graphic Processing

This profile is for workloads that are run on server configurations which use Graphics Processing Units (GPUs.) GPUs typically depend on maximum bandwidth between I/O and Memory. Power management features that have impact on the links between I/O and memory are disabled. Peer to Peer traffic is also critical and therefore virtualization is also disabled.

I/O Throughput

This profile is for configurations that depend on maximum throughput between I/O and memory. Processor utilization driven power management features that have performance impact to the links between I/O and memory are disabled.

Custom

This option on the Workload Profiles menu disables Workload Profiles. Use this option if you want to set specific BIOS options for your deployment manually. When you select Custom, all the settings for the previously selected profile are carried forward. You can edit all or some of the options.

Custom is not a profile and settings that you specify are not saved as a template.

Default profiles for servers

Workload Profile options support a variety of power and performance requirements. For most HPE ProLiant Gen10 servers and HPE Synergy compute modules, Workload Profile is set to General Power Efficient Compute by default. This Workload Profile provides common performance and power settings suitable for most application workloads. For ProLiant XL servers in an HPE Apollo system, the Workload Profile is set to High Performance Compute by default.

Selecting a Workload Profile other than the Custom profile affects other setting options. For example, selecting the General Peak Frequency Compute profile automatically sets Power Regulator mode to Static High Performance. This setting cannot be changed and is grayed out.

Subtopics

Workload matching

The default BIOS settings on Hewlett Packard Enterprise servers provide a balance between performance and power efficiency. These settings can be adjusted to match specific application workloads.

HPE Gen10 and later servers offer a UEFI configuration option to help customers tune their BIOS settings by using known workload-based tuning profiles. When matching your workload profile setting to your actual deployed workload, you can realize performance gains versus just using the out-of-box BIOS defaults.

For more information, see the UEFI Workload-based Profiles and Tuning Guide for HPE Servers at **https://www.hpe.com/support/Workload-UG-en-Gen11**.

Workload profiles dependencies overview

Dependencies

There are multiple options that are available for BIOS configuration. Not all profiles set the same options to specific settings. Each profile is designed to obtain specific performance results and sets different options to meet those results. The options that a profile sets are called dependencies. All other options are unaffected by the Workload Profile and are seen as nondependent settings.

Dependencies and switching profiles

When you change a profile, only the dependent settings for that profile are changed. Nondependent settings remain what they were before you changed your profile.

For example:

1. Select the General Power Efficient Compute profile, which has the Energy Performance Bias set to Balanced Performance.
2. Select the General Peak Frequency Compute profile, which has no dependency on Energy Performance Bias. The Energy Performance option is set to Balanced Performance because that setting is carried forward from the General Power Efficient Compute profile.
3. Select the General Throughput Compute profile, which has the Energy Performance Bias set to Maximum Performance.
4. Select the General Peak Frequency Compute profile which has no dependency on Energy Performance Bias. Energy Performance Bias is set to Maximum Performance because that setting is carried forward from the General Throughput Compute profile.

There is no way to revert to a previous profile and dependencies. After you change to a new profile, the new dependencies are applied. The only way to revert to older profiles is to exit without saving your changes. Exiting without saving reverts to where you were when you entered RBSU. After you save a profile, you cannot revert from that profile to any intermediate dependencies.

Dependencies and options matrix

The tables show the Workload Profiles and their dependencies. The Workload Profiles are listed in the order that they are listed on the UI. In the table, "X" means that the option setting has no requirement for the profile and can be edited. Dependencies cannot be edited.

NOTE

Not all the options listed are adjustable on all servers. However, even if you do not have the option of adjusting some of these settings, they default to the values shown here.

Subtopics

Workload profile dependencies for 1st and 2nd Gen AMD EPYC™ processors

NOTE

Options vary based on hardware installed on the server.

Table 1. Workload profiles: General power efficient compute—Low latency

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency	Mission Critical
Power Regulator	OS Control	Static High Performance	Static High Performance	OS Control	Static High Performance	Static High Performance	x
SR-IOV	x	x	x	Enabled	Enabled	Disabled	x
AMD IOMMU	x	x	x	Enabled	Enabled	x	x
AMD Virtualization Technology	x	x	x	Enabled	Enabled	Disabled	x
Minimum Processor Idle Power Core C-state	C6	x	x	C6	No C-states	No C-state	x
AMD Turbo Core	Enabled	Enabled	Enabled	x	Enabled	Disabled	x
L1 Stream HW Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled	Enabled
L2 Stream HW Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled	Enabled
NUMA Group Size Optimization	Flat	Clustered	Clustered	Clustered	Clustered	Clustered	x
Memory Patrol Scrubbing	x	x	x	x	x	Disabled	x
Memory Refresh Rate	x	1x	1x	x	x	1x	2x
x2APIC	x	x	x	x	x	Auto	x

Table 2. Workload profiles: Mission critical—I/O throughput

	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput	Custom	EV Name
Power Regulator	Static High Performance	Static High Performance	x	x	x	x	CQHPER
SR-IOV	x	Disabled	x	Disabled	x	x	CQHSRIOV
AMD IOMMU	x	x	x	x	x	x	CQHSKTPROC
AMD Virtualization Technology	x	Disabled	x	Disabled	x	x	CQHAMD
Minimum Processor Idle Power Core C-state	No C-states	No C-states	x	x	x	x	CQHSKTPOWER
AMD Turbo Core	Enabled	Enabled	x	x	x	x	CQHSKTPOWER
L1 Stream HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	x	CQHSKTPROC
L2 Stream HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	x	CQHSKTPROC
NUMA Group Size Optimization	Clustered	Clustered	Clustered	Clustered	Clustered	x	CQHNUMA
Memory Patrol Scrubbing	x	x	x	x	x	x	CQHMEM
Memory Refresh Rate	x	1x	x	x	x	x	CQHMEM
x2APIC	x	Auto	x	Auto	x	x	CQHSKTPROC

Workload profile dependencies for third Gen AMD EPYC™ processors

IMPORTANT

Options vary based on the hardware installed on the server.

Table 1. Workload profiles: General power efficient compute—Mission critical

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency	Mission Critical
Processor x2APIC Option **NOTE** Processor x2APIC Option is force enabled if more than 256 threads are active in the system.	Auto	x	x	x	x	Auto	x
Memory Refresh Rate	x	x	x	x	x	1x	2x
Memory Patrol Scrubbing	x	x	x	x	x	Disabled	Enabled
NUMA Memory Domains Per Socket	x	x	x	x	x	NPS4	x
AMD I/O Virtualization Technology	x	x	x	Enabled	Enabled	Disabled	x
SR-IOV	x	x	x	Enabled	Enabled	Disabled	x
Power Regulator	OS control	Static High	Static High	OS control	Static High	Static High	x
Minimum Processor Idle Power Core C-state	C6	x	x	C6	x	x	x
Data Fabric C-State Enable	Enabled	Disabled	x	Enabled	Disabled	Disabled	x
AMD Core Performance Boost	Enabled	Enabled	Enabled	x	Enabled	Disabled	x
Collaborative Power Control	x	x	x	x	Disabled	Disabled	x
xGMI Force Link Width **NOTE** This property is not available for DL325 and DL345 Gen11/Gen12 servers with a single processor.	x	x	x	x	x	x16	x
NUMA Group Size Optimization	Flat	Clustered	Clustered	Clustered	Clustered	Clustered	x
L1 Stream HQ Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled	Enabled
L2 Stream HQ Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled	Enabled
Infinity Fabric Power Management	Enabled	x	x	Enabled	Disabled	Disabled	x
Infinity Fabric Performance State	Auto	x	P0	Auto	P0	P0	x

Table 2. Workload profiles: Transaction application processing—I/O throughput

	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput
Processor x2APIC Option **NOTE** Processor x2APIC Option is force enabled if more than 256 threads are active in the system.	x	Auto	x	Auto	x
Memory Refresh Rate	x	x	x	x	x
Memory Patrol Scrubbing	Disabled	x	x	x	x
NUMA Memory Domains Per Socket	x	NPS4	x	NPS4	NPS2
AMD I/O Virtualization Technology	x	Disabled	x	Disabled	x
SR-IOV	Disabled	Disabled	Disabled	Disabled	Disabled
Power Regulator	Static High	Static High	x	x	x
Minimum Processor Idle Power Core C-state	x	x	x	x	x
Data Fabric C-State Enable	x	Disabled	x	Disabled	Disabled
AMD Core Performance Boost	Enabled	Enabled	x	x	x
Collaborative Power Control	x	Disabled	x	x	x
xGMI Force Link Width **NOTE** This property is not available for DL325 and DL345 Gen11/Gen12 servers with a single processor.	x	x16	x	x16	x16
NUMA Group Size Optimization	Clustered	Clustered	Clustered	Clustered	Clustered
L1 Stream HQ Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled
L2 Stream HQ Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled
Infinity Fabric Power Management	x	Disabled	x	Disabled	Disabled
Infinity Fabric Performance State	x	P0	x	P0	P0

Workload profile dependencies for fourth and fifth Gen AMD EPYC™ processors

TIP

'x' in a cell denotes no dependency, no Grey-out.

Table 1. Workload profiles: General power efficient compute—Mission critical

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency	Mission Critical
Processor x2APIC Option **NOTE** Processor x2APIC Option is force enabled if more than 256 threads are active in the system.	x	x	x	x	x	Auto	x
AMD SMT	x	x	x	x	x	x	x
Memory Refresh Rate	x	x	x	x	x	1x	2x
Memory Bus Frequency	x	x	x	x	x	x	x
Memory Patrol Scrubbing	x	x	x	x	x	Disabled	Enabled
NUMA Memory Domains Per Socket	x	x	x	x	x	NPS4	x
Last-Level Cache (LLC) As NUMA Node	x	x	x	x	x	x	x
AMD I/O Virtualization Technology	x	x	x	Enabled	Enabled	Disabled	x
SR-IOV	x	x	x	Enabled	Enabled	Disabled	x
Power Regulator	OS control	Static High	Static High	OS control	Static High	Static High	x
Minimum Processor Idle Power Core C-state	C6	x	x	C6	x	x	x
Data Fabric C-State Enable	Auto	Disabled	x	Enabled	Disabled	Disabled	x
AMD Core Performance Boost	Enabled	Enabled	Enabled	x	Enabled	Disabled	x
xGMI Force Link Width **NOTE** This property is not available for DL325 and DL345 Gen11/Gen12 servers with a single processor.	x	x	x	x	x	x16	x
NUMA Group Size Optimization	Flat	Clustered	Clustered	Clustered	Clustered	Clustered	x
L1 Stream HW Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled	Enabled

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency	Mission Critical
L2 Stream HW Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled	Enabled
Infinity Fabric Power Management	Enabled	x	x	Enabled	Disabled	Disabled	x
Infinity Fabric Performance State	Auto	x	P0	Auto	P0	P0	x
AMD Performance Workload Profile	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Table 2. Workload profiles: Transaction application processing—I/O throughput

	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput
Processor x2APIC Option	x	Auto	x	Auto	x
AMD SMT	x	x	x	x	x
Memory Refresh Rate	x	x	x	x	x
Memory Bus Frequency	x	x	x	x	x
Memory Patrol Scrubbing	Disabled	x	x	x	x
NUMA Memory Domains Per Socket	x	NPS4	x	NPS4	NPS2
Last-Level Cache (LLC) As NUMA Node	x	x	x	x	x
AMD I/O Virtualization Technology	x	Disabled	x	Disabled	x
SR-IOV	Disabled	Disabled	Disabled	Disabled	Disabled
Power Regulator	Static High	Static High	x	x	x
Minimum Processor Idle Power Core C-state	x	x	x	x	x
Data Fabric C-State Enable	x	Disabled	x	Disabled	Disabled
AMD Core Performance Boost	Enabled	Enabled	x	x	x

NOTE

Processor x2APIC Option is force enabled if more than 256 threads are active in the system.

	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput
xGMI Force Link Width	x	x16	x	x16	x16

NOTE

This property is not available for DL325 and DL345 Gen11/Gen12 servers with a single processor.

NUMA Group Size Optimization	Clustered	Clustered	Clustered	Clustered	Clustered
L1 Stream HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled
L2 Stream HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled
Infinity Fabric Power Management	x	Disabled	x	Disabled	Disabled
Infinity Fabric Performance State	x	P0	x	P0	P0
AMD Performance Workload Profile	Disabled	Disabled	Disabled	Disabled	Disabled

Workload profile dependencies for Intel® Xeon® Scalable processors

NOTE

Options vary based on the hardware installed on the server.

Table 1. Workload profiles: General power efficient compute—Low latency

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency
SR-IOV	x	x	x	Enabled	Enabled	Disabled
VT-D	x	x	x	Enabled	Enabled	Disabled
VT-x	x	x	x	Enabled	Enabled	Disabled
Power Regulator	Dynamic Power Savings	Static High Performance	Static High Performance	OS Control	Static High Performance	Static High Performance

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency
Minimum Processor Idle Power Core C-state	C6	x	x	C6	No C-states	No C-states
Minimum Processor Idle Power Package C-state	Package C6 Retention	Package C6 Retention	Package C6 Retention	Package C6 Retention	No C-states	No C-states
Energy Performance Bias	Balanced Performance	x	Max Performance	Balanced Performance	Max Performance	Max Performance
Collaborative Power Control	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
Intel DMI Link Frequency	Auto	Auto	Auto	Auto	Auto	Auto
Intel Turbo Boost Technology	Enabled	Enabled	Enabled	x	Enabled	Disabled
Intel NIC DMA Channels (IOAT)	Enabled	x	x	x	x	x
HW Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled
Adjacent Sector Prefetch	Enabled	Enabled	Enabled	x	x	Enabled
DCU Stream Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled
NUMA Group Size Optimization	Flat	Clustered	Clustered	Clustered	Clustered	Clustered
Memory Patrol Scrubbing	x	x	x	x	x	Disabled
Memory Refresh Rate	x	1x	1x	x	x	1x
UPI Link Power Management	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
*Sub-NUMA Clustering	Disabled	x	Enable SNC4 (4-clusters)	Disable	Enable SNC4 (4-clusters)	x
Energy-Efficient Turbo	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
Uncore Frequency Shifting	Auto	Max	x	Auto	Max	Max
x2APIC	x	x	x	x	x	Auto
Channel Interleaving	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Memory Bus Frequency	x	x	x	x	x	x
Advanced Memory Protection	x	x	x	x	x	Advanced ECC Support
Optimized Power Mode	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency
Intel(R) AVX License Pre-Grant Override	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Intel(R) AVX ICCP Pre-Grant Level	x	x	x	x	x	x
PCI-E ASPM Support (Global)	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

NOTE

*If the plugged processors do not have SNC4 supported and the workload profile is set as "General Throughput Compute" or "Virtualization–Max Performance", the sub-NUMA clustering is modified to “Enable SNC2 (2-clusters)”.

Table 2. Workload profiles: Mission critical—vRAN

	Mission Critical	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput	vRAN
SR-IOV	x	x	Disabled	x	Disabled	x	Enabled
VT-D	x	x	Disabled	x	Disabled	x	Enabled
VT-x	x	x	Disabled	x	Disabled	x	Enabled
Power Regulator	x	Static High Performance	Static High Performance	x	x	x	OS Control
Minimum Processor Idle Power Core C-state	x	No C-states	No C-states	x	x	x	C6
Minimum Processor Idle Power Package C-state	x	No C-states	No C-states	x	x	x	No Package State
Energy Performance Bias	x	Max Performance	Max Performance	x	Max Performance	Max Performance	Max Performance
Collaborative Power Control	x	x	Disabled	x	x	x	Disabled
Intel DMI Link Frequency	Auto	Auto	Auto	Auto	Auto	Auto	Auto
Intel Turbo Boost Technology	x	Enabled	Enabled	x	x	x	Enabled
Intel NIC DMA Channels (IOAT)	x	Enabled	Enabled	x	x	Enabled	Enabled
HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Adjacent Sector Prefetch	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
DCU Stream Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
DCU IP Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

	Mission Critical	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput	vRAN
NUMA Group Size Optimization	x	Clustered	Clustered	Clustered	Clustered	Clustered	Clustered
Memory Patrol Scrubbing	x	x	x	x	x	x	Disabled
Memory Refresh Rate	2x	x	1x	x	x	x	1x
UPI Link Power Management	x	Disabled	Disabled	x	x	x	Disabled
Sub-NUMA Clustering	x	x	x	x	x	x	Disabled
Energy-Efficient Turbo	x	x	Disabled	x	x	x	Disabled
Uncore Frequency Shifting	x	x	Max	x	Max	Max	Custom
x2APIC	x	x	Auto	x	Auto	x	Force Enabled
Channel Interleaving	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Memory Bus Frequency	x	x	x	x	x	x	x
Advanced Memory Protection	ADDDC	x	Advanced ECC Support	x	x	x	ADDDC
Optimized Power Mode	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Intel(R) AVX License Pre-Grant Override	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Intel(R) AVX ICCP Pre-Grant Level	x	x	x	x	x	x	x
PCI-E ASPM Support (Global)	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

IMPORTANT

vRAN workload profile applies only to DL110 servers.

Workload profile dependencies for Intel® Xeon® E processors

NOTE

Options vary based on the hardware installed on the server.

Table 1. Workload profiles: General power efficient compute—Low latency

	General Power Efficient Compute	General Peak Frequency Compute	General Throughput Compute	Virtualization - Power Efficient	Virtualization - Max Performance	Low Latency
SR-IOV	x	x	x	Enabled	Enabled	Disabled
VT-D	x	x	x	Enabled	Enabled	Disabled
Power Regulator	Dynamic Power Savings	Static High Performance	Static High Performance	OS Control	Static High Performance	Static High Performance
Minimum Processor Idle Power Core C-state	C6	x	x	C6	No C-states	No C-states
Enhanced C-states	x	x	x	x	Disabled (hidden)	Disabled (hidden)
Minimum Processor Idle Power Package C-state	Package C6 Retention	Package C6 Retention	Package C6 Retention	Package C6 Retention	No C-states	No C-states
Collaborative Power Control	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
Intel DMI Link Frequency	Auto	Auto	Auto	Auto	Auto	Auto
Intel Turbo Boost Technology	Enabled	Enabled	Enabled	x	Enabled	Disabled
HW Prefetcher	Enabled	Enabled	Enabled	x	x	Enabled
Adjacent Sector Prefetch	Enabled	Enabled	Enabled	x	x	Enabled
Memory Refresh Rate	x	1x	1x	x	x	1x
Energy-Efficient Turbo	Enabled	Disabled	Disabled	Enabled	Disabled	Disabled
x2APIC	x	x	x	x	x	Auto
Memory Bus Frequency	x	x	x	x	x	x
Intel(R) Virtualization Technology (Intel VT)	x	x	x	Enabled	Enabled	Disabled
Intel(R) AVX License Pre-Grant Override	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Intel(R) AVX ICCP Pre-Grant Level	x	x	x	x	x	x
PCI-E ASPM Support (Global)	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Table 2. Workload profiles: Mission critical—I/O throughput

	Mission Critical	Transactional Application Processing	High Performance Compute (HPC)	Decision Support	Graphic Processing	I/O Throughput
SR-IOV	x	x	Disabled	x	Disabled	x
VT-D	x	x	Disabled	x	Disabled	x
Power Regulator	x	Static High Performance	Static High Performance	x	x	x
Minimum Processor Idle Power Core C-state	x	No C-states	No C-states	x	x	x
Enhanced C-states	Disabled	Disabled (Hidden)	Disabled (hidden)	Disabled	Disabled	Disabled
Minimum Processor Idle Power Package C-state	x	No C-states	No C-states	x	x	x
Collaborative Power Control	x	x	Disabled	x	x	x
Intel DMI Link Frequency	Auto	Auto	Auto	Auto	Auto	Auto
Intel Turbo Boost Technology	x	Enabled	Enabled	x	x	x
HW Prefetcher	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Adjacent Sector Prefetch	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Memory Refresh Rate	2x	x	1x	x	x	x
Energy-Efficient Turbo	Disabled	x	Disabled	Disabled	x	x
x2APIC	x	x	Auto	x	Auto	x
Memory Bus Frequency	x	x	x	x	x	x
Intel(R) Virtualization Technology (Intel VT)	x	x	Disabled	x	Disabled	x
Intel(R) AVX License Pre-Grant Override	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Intel(R) AVX ICCP Pre-Grant Level	x	x	x	x	x	x
PCI-E ASPM Support (Global)	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Applying a workload profile

About this task

You apply a workload profile to have the system manage your workload according to predefined settings provided with the system. Dependent options cannot be changed and are grayed out. You can change any nondependent options in a profile.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profile.
2. Select a workload profile.
3. **Optional:**
   Change any nondependent options that you want to change.
4. Save the changes.
5. Reboot to apply your workload profile.

More information

- Workload profiles and performance options

Changing dependent options after applying a profile

Prerequisites

Apply a Workload Profile before you do this task.

About this task

There may be one or more dependent options that you want to change in your Workload Profile. Dependent options cannot be changed for a predefined profile. You can change the dependent options in Custom mode. When you are in Custom mode, your deployment is no longer in profile mode and you can manually adjust option settings. When you enter Custom mode, all the settings from the previously applied profile are shown.

The easiest way to change dependent settings is to modify an applied profile. First apply a Workload Profile that has most of the settings that you want to use then change to Custom mode. Then change only the settings you want to have new values.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Workload Profile.
2. Select the Custom profile option.

   All of the settings from the previously applied Workload Profile are shown. All options are editable.
3. Change the options that you want to have new values.
4. Save and reboot to apply the changes.

Changing System Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options.

Subtopics

Configuring Boot Time Optimizations

Subtopics

Setting Dynamic Power Capping Functionality

About this task

Use the Setting Dynamic Power Capping Functionality option to configure when the system ROM executes power calibration during the boot process.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Boot Time Optimizations > Dynamic Power Capping Functionality.
2. Select a setting.
   - Auto—Power calibration runs the first time the server is booted and is only run again when the hardware configuration settings of the server change.
   - Enabled—Power calibration runs on every system boot.
   - Disabled—Power calibration does not run, and Dynamic Power Capping is not supported.
3. Save your setting.

Enabling or Disabling AMD eMCR Boot-Time Reduction

About this task

Use this option to configure the **AMD eMCR (Enhanced Memory Context Restore) Feature** . Enabling this feature will reduce boot time for most boots by not requiring a full memory training on every boot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Boot Time Optimizations > AMD eMCR Boot-Time Reduction .
2. Select a setting.
   - Enabled: Full memory training is not required on every boot.
   - Disabled: Full memory training will be performed on each boot.
3. Save your setting.

Enabling or disabling Extended Memory Test

About this task

Use the Extended Memory Test option to configure whether the system validates memory during the memory initialization process. When enabled, and uncorrectable memory errors are detected, the memory is mapped out, and the failed DIMMs are logged to the IML.

NOTE

Enabling this option might significantly increase boot time.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Boot Time Optimizations > Extended Memory Test.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Setting the UEFI POST Discovery Mode

About this task

Use the UEFI POST Discovery Mode option to control how the system loads UEFI device drivers.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Boot Time Optimizations > UEFI POST Discovery Mode.
2. Select one of the following:
   - Auto—The system only loads the UEFI device drivers that are required for booting the devices in the UEFI Boot Order list.
   - Force Full Discovery—The system loads the UEFI drivers for all devices, making all boot targets available.

     NOTE

     This setting might significantly increase boot time.
   - Force Fast Discovery—The system starts the fewest number of devices as possible to increase boot time.

     NOTE

     Some devices that do not support Fast Discovery might not work properly.
3. Save your setting.

Enabling or disabling Memory Clear on Warm Reset

About this task

Use the Memory Clear on Warm Reset option to configure when memory is cleared on warm resets. Disabling this option can save boot time by skipping the clearing of memory on warm resets.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Boot Time Optimizations > Memory Clear on Warm Reset.
2. Select a setting.
   - Enabled—Memory is cleared on all reboots.
   - Disabled—Memory is only cleared on a warm reset when requested by the operating system.
3. Save your setting.

Configuring Serial Port Options

Subtopics

Assigning an Embedded Serial Port

About this task

Use the Embedded Serial Port option to assign a logical COM port address and associated default resources to a selected physical serial port.

Prerequisite

For proper screen resolution, set the console resolution in the terminal software to 100x31.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > Embedded Serial Port.
2. Select a setting.
   - COM 1: IRQ4: I/0: 3F8h-3FFh
   - COM 2: IRQ3: I/0: 2F8h-2FFh
   - Disabled
3. Save your setting.

Assigning a Virtual Serial Port

About this task

Use the Virtual Serial Port option to assign a logical COM port address and the associated default resources used by the Virtual Serial Port

(VSP). VSP enables the iLO Management Controller to appear as a physical serial port to support the BIOS Serial Console and the operating system serial console.

Prerequisite

For proper screen resolution, set the console resolution in the terminal software to 100x31.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > Virtual Serial Port.
2. Select a setting.
   - COM 1
   - COM 2
   - Disabled
3. Save your setting.

Mirroring serial console to a USB port

About this task

Enabling this option allows you to mirror a serial console to a USB port. Mirroring requires the HPE Console Cable Kit.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Serial Port Options > USB Console Redirection.
2. Select an option:
   - Enable
   - Disable
3. Save the setting.

Configuring USB Options

Subtopics

Setting USB Control

About this task

Use the USB Options option to configure how USB ports and embedded devices operate at startup.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > USB Options >

USB Control.

2. Select a setting.
   - All USB Ports Enabled—Enables all USB ports and embedded devices.
   - All USB Ports Disabled—Disables all USB ports and embedded devices.
   - External USB Ports Disabled—Disables external USB ports.
   - Internal USB Ports Disabled—Disables internal USB ports.
3. Save your setting.

Enabling or disabling USB Boot Support

About this task

Use the USB Boot Support option to control whether the system can boot from connected USB devices, such as virtual media devices, and the embedded SD card slot, if supported.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > USB Options > USB Boot Support.
2. Select a setting.
   - Enabled—The system can boot from USB devices connected to the server.
   - Disabled—The system cannot boot from USB devices connected to the server.
3. Save your setting.

Configuring the IOS Serial Console and EMS

Subtopics

Enabling or disabling the BIOS Serial Console Port

About this task

Use the BIOS Serial Console Port option to redirect video and keystrokes through the serial port to operating system boot.

NOTE

This option can interfere with nonterminal devices attached to the serial port. In such cases, set this option to disabled.

NOTE

This option is only supported in English language mode when running in the UEFI preboot System Utilities.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > BIOS Serial Console and EMS Options > BIOS Serial Console Port.
2. Select a setting.
   - Auto
   - Physical Serial Port
   - Virtual Serial Port
3. Save your setting.

Selecting the BIOS Serial Console Emulation Mode

About this task

Use the BIOS Serial Console Emulation Mode option to select the emulation mode type. To match the emulation you will use in your serial terminal program, such as HyperTerminal or PuTTY, select this option. The BIOS emulation mode must match the mode selected in your terminal program.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > BIOS Serial Console & EMS > BIOS Serial Console Emulation Mode.
2. Select a setting.
   - VT100
   - ANSI
   - VT100+
   - VT-UTF8
3. Save your setting.

Setting the BIOS Serial Console Baud Rate

About this task

Use the BIOS Serial Console Baud Rate option to This is the transfer rate at which data is transmitted through the serial port.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > BIOS Serial Console & EMS > BIOS Serial Console Baud Rate.
2. Select a setting.

- 9600
- 19200
- 57600
- 115200
- 38400

3. Save your setting.

Configuring EMS Console port settings

About this task

Use the EMS Console port settings option to configure the ACPI serial port setting, which includes the ability to redirect the Windows Server Emergency Management console (EMS) through either the physical or virtual serial port.

EMS configuration options have changed. See your product documentation for details.

NOTE

Not all BAUD rates are supported by an Operating System for Serial Port Redirection (EMS). Consult operating system documentation for supported modes.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > BIOS Serial Console & EMS > EMS Console.
2. Select either a physical or virtual port setting.
3. Save your setting.

Configuring Server Availability

Subtopics

Enabling or disabling ASR

About this task

Prerequisite

The System Management driver is loaded.

Use the ASR Status option to enable or disable Automatic Server Recovery, which automatically reboots the server if the server locks up.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > ASR Status.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

NOTE

The ASR status option is only supported in ProLiant Gen10 servers.

Setting the ASR timeout

About this task

Prerequisite

ASR Status is enabled. Use the ASR Timeout option to set the time to wait before rebooting the server if an operating system crash or server lockup occurs. When the server has not responded in the selected amount of time, the server automatically reboots.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > ASR Timeout.
2. Select a wait time.
   - 5 Minutes
   - 10 Minutes
   - 15 Minutes
   - 20 Minutes
   - 30 Minutes
3. Save your setting.

NOTE

The ASR timeout option is only supported in ProLiant Gen10 servers.

Enabling or disabling Wake-On LAN

About this task

Use the Wake-On LAN option to enable or disable the ability of the server to power on remotely using a WOL-capable NIC.
Prerequisite

A WOL-capable NIC, NIC driver, and operating system.

> **NOTE**
> If you enable this option, remove all power cords before adding or removing any adapters. Some adapters can cause the system to power on when added or removed.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > Wake-On LAN.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Setting the POST F1 prompt delay

About this task

Use the POST F1 Prompt option to configure how the system displays the F1 key in the server POST screen. When enabled and an error occurs, you can press the F1 key to continue with the server power-up sequence.
A series of system tests execute during POST and:

- If failures occur that allow the system to continue operating, the system continues to boot and then posts a message.
- If critical components fail or are missing, the server attempts to boot. If it can boot, it posts a message and, when enabled, an F1 prompt.
- If the system cannot run with the missing or failed components, it halts until those components are replaced.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > POST F1 Prompt.
2. Select a setting.
   - Delayed 20 seconds—If an error occurs, the system pauses for 20 seconds at the F1 prompt, and then continues to boot the OS.
   - Delayed 2 seconds—If an error occurs, the system pauses for two seconds at the F1 prompt, and then continues to boot the OS.
   - Disabled—If an error occurs, the system bypasses the F1 prompt and continues to boot.
3. Save your setting.

Enabling or disabling momentary power button functionality

About this task

Use the Power Button Mode option to enable or disable momentary power button functionality. This mode does not affect the four-second

power button override, or the remote power control functionality.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > Power Button Mode.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Setting the automatic power-on state

About this task

Use the Automatic Power-On option to configure how the server automatically powers on when AC power is applied. By default, the system returns to its previous power state when AC power is restored after an AC power loss.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > Automatic Power-On.
2. Select a setting.
   - Always Power On—The system automatically returns to a power on state, even if it was in the “off” state when power was lost.
   - Always Power Off—The system automatically returns to a power off state.
   - Restore Last Power State—The system automatically returns to its previous power off state.
3. Save your setting.

Setting the power-on delay

About this task

Use the Power-On Delay option to set whether to delay the server from turning on for a specified time. This option enables staggering when the server powers up after a power loss, which can prevent power usage spikes.

NOTE

These events override the Power-On Delay setting and immediately power on the server:

- Pressing the power button using the iLO Virtual Power Button
- Wake-ON LAN events
- RTC (Real-Time Clock) wake-up events

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > Power-On Delay.

2. Select a setting.
   - No Delay
   - Random Delay
   - 15 Second Delay
   - 30 Second Delay
   - 45 Second Delay
   - 60 Second Delay
3. Save your setting.

Setting the POST ASR

About this task

Use the POST ASR option to configure POST Automatic Server Recovery (ASR).

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > POST ASR.
2. Select a setting.
   - Post ASR on
   - Post ASR off
3. Save your setting.

> **NOTE**
>
> The POST ASR option is only supported in ProLiant Gen10 Plus and later servers.

Setting the POST ASR Timer

About this task

Use the POST ASR Timer to set the wait timer before rebooting the server of a server lock up.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > POST ASR Timer.
2. Select a setting.
   - 10 minutes
   - 15 minutes
   - 20 minutes
   - 30 minutes

3. Save your setting.

Enabling or disabling the IPMI Watchdog Timer

About this task

Use the IPMI Watchdog Timer option to enable a Boot Time (POST) IPMI compliant Watchdog Timer (WDT) that is disabled when the user issues an IPMI command to the system. This timer is not automatically disabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timer.
2. Select a setting.
   - Disabled
   - Enabled

   NOTE

   After enabling the IPMI Watchdog Timer, the timer does not stop if the user reboots the system into RBSU or UEFI shell. The WDT still times out after the selected wait time, and the system proceeds with the selected timeout reset action.
3. Save your setting.

Setting the IPMI Watchdog timer timeout

Prerequisites

The IPMI Watchdog Timer is enabled.

About this task

Use IPMI Watchdog Timer Timeout to set the wait timer before performing the desired timeout action on the server, in the event of a server lockup.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timer Timeout.
2. Select a wait time.
   - 10 Minutes
   - 15 Minutes
   - 20 Minutes
   - 30 Minutes
3. Save your setting.

Setting the IPMI Watchdog Timer Action

About this task

Use the IPMI Watchdog Timer Action to configure the timeout action upon expiration of the watchdog timer due to a server lockup.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Availability > IPMI Watchdog Timer Action.
2. Select a setting:
   - Power Cycle
   - Power Down
   - Warm Boot
3. Save your setting.

Viewing and entering server asset information

Subtopics

Entering server information

About this task

Use the Server Information option to enter reference information for the server administrator. For text settings, enter a maximum of 14 characters. By default, all values are blank.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Asset Information > Server Information.
2. Select and complete entries.
   - Server Name—Enter a server name.
   - Server Asset Tag—Enter a server asset number.
   - Asset Tag Protection—Select a setting:
     - Unlocked
     - Locked—Locks asset tag information. The asset tag is not erased if you restore default system settings.
   - Server Primary OS—Enter a description of the primary OS of the server.
   - Server Other Information—Enter additional text describing the server.

3. Save your settings.

Entering administrator information

About this task

Use the Administrator Information option to enter contact information for the server administrator. The number of characters allowed for each entry varies by server model. By default, all values are blank.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Asset Information > Administrator Information.
2. Select and complete entries.
   - Administrator Name—Enter the server administrator's name.
   - Administrator Phone Number—Enter the server administrator's phone number.
   - Administrator E-mail Address—Enter the server administrator's e-mail address.
   - Administrator Other Information—Enter additional text relating to the server administrator.
3. Save your settings.

Entering service contact information

About this task

Use the Service Contact Information option to enter service contact information for the server administrator. The number of characters allowed for each entry varies by server model. By default, all values are blank.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Asset Information > Service Contact Information.
2. Select and complete entries.
   - Service Contact Name—Enter the service contact's name.
   - Service Phone Number—Enter the service contact's phone number.
   - Service Contact E-mail Address—Enter the service contact's e-mail address.
   - Service Contact Other Information—Enter additional text relating to the service contact.
3. Save your settings.

Entering a custom POST message

About this task

Use the Custom POST Message option to display a custom message on the server POST screen.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Server Asset Information > Custom POST Message.
2. Enter a message of up to 62 characters.
3. Save your setting.

Changing Processor Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options.

Subtopics

Enabling or disabling Intel Hyperthreading

About this task

Use the Intel (R) Hyperthreading Options option to disable or enable the logical processor cores on processors supporting Intel Hyperthreading technology. Intel Hyperthreading improves overall performance for applications that benefit from a higher processor core count.

NOTE

Hyperthreading is not supported on all processors. For more information, see the documentation for your processor model.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Intel (R) Hyperthreading Options.

2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling Intel® Speed Select Technology Core Power

About this task

Intel® Speed Select Technology - Core Power allows biasing energy and power budget between cores.

> **IMPORTANT**
> The Speed Select technology option might be hidden in RBSU if your processor does not support it. For more information, see the DCL document of the installed CPU.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Intel® Speed Select Technology - Core Power.
2. Select from one of the settings:
   - Enabled
   - Disabled (default)
3. Save your setting.

Configuring Intel® Speed Select Technology Performance Profile

About this task

> **IMPORTANT**
> The Speed Select technology option might be hidden in RBSU if your processor does not support it. For more information, see the DCL document of the installed CPU.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Intel® Speed Select Technology - Performance Profile.
2. Select from one of the settings:
   - Base
   - Config 1
   - Config 2
3. Save your setting.

Enabling or disabling Intel® Speed Select Technology Base Frequency

About this task

> **IMPORTANT**
> The Speed Select technology option might be hidden in RBSU if your processor does not support it. For more information, see the DCL document of the installed CPU.

s

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Intel® Speed Select Technology - Base Frequency.
2. Select from one of the settings:
   - Enabled
   - Disabled (default)
3. Save your setting.

Setting the number of enabled processor cores

About this task

This option enables limiting the number of enabled processor cores per physical processor. You can set the number of enabled cores to a value supported by the physical processor.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Enabled Cores per Processor.
2. Enter the number of cores to enable.

   If you enter 0, or a value that the processor does not support, all cores are enabled.
3. Save your setting.

Configuring Processor RAPL Wattage value

About this task

Processor RAPL Wattage value is a per processor RAPL value applicable for all populated processors in the system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Processor RAPL Wattage value.
2. Enter or modify the wattage value in milliwatts. Consult your qualified personnel for validating this.
3. Save your setting.

Configuring Processor Physical Addressing

About this task

Processor Physical Addressing limits the processor physical addressing (PAE) to 46-bits. This option may be required to support older Operating Systems that do not support a larger addressing capability.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Processor Physical Addressing.
2. Select from one of the settings:
   - Default
   - Limited [limits the (PAE)]
3. Save your setting.

Configuring AMD Periodic Directory Rinse Tuning

About this task

Controls the PDR settings that impact performance by workload and/or processor.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > AMD Periodic Directory Rinse Tuning.
2. Select a setting.
   - For 4th Gen EPYC processors
     - Auto: It is identical to Memory-Sensitive mode.
     - Memory-Sensitive: It accelerates high bandwidth scenarios.
     - Cache-Bound: It accelerates cache-bound scenarios.
     - Neutral: It is a fallback option for unknown or mixed scenarios.
     - Adaptive: It adjusts based on Memory/Cache Activity.
   - For 5th Gen EPYC processors
     - Auto: It is identical to Blended mode.
     - Periodic: It is Rate-based Directory Rinse.
     - Blended: It is Demand-based Directory Rinses.
3. Save your setting.

Enabling or disabling Intel® TSX Support

About this task

Intel® TSX Support is used to configure the processor Transactional Synchronization Extensions (TSX) support.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Intel® TSX Support.
2. Select from one of the settings:
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling Processor AES-NI Support

About this task

Processor AES-NI Support is used to enable or disable the Advanced Encryption Standard Instruction Set (AES-NI) in the processor.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Processor AES-NI Support.
2. Select from one of the settings:
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling Processor UUID Control

About this task

Processor UUID Control is used to unlock and enable/disable PPIN control.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Processor UUID Control.
2. Select from one of the settings:
   - Lock/Disable
   - Unlock/Enable
3. Save your setting.

Enabling or disabling Processor x2APIC Support

About this task

When enabled, Processor x2APIC Support helps operating systems run more efficiently on high core count configurations and optimizes interrupt distribution in virtualized environments. Enabled mode does not enable x2APIC hardware, but provides the support necessary to the operating system. Unless you are using an older hypervisor or operating system that is not compatible with x2APIC support, leave this option enabled. Some hypervisors and operating systems cannot use X2APIC unless Processor x2APIC Support is set to Force Enabled prior to booting.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Processor x2APIC Support.
2. Select from one of the settings:
   - Auto—Generates the ACPI x2APIC control structures, and adds the option of enabling x2APIC support to the operating system when it loads.
   - Force Enabled—For certain processors, enables x2APIC support to the operating system when it loads.
3. Save your setting.

Enabling AMD Simultaneous Multithreading (SMT)

About this task

Use the AMD SMT Option to enable or disable the AMD SMT functionality.

> **NOTE**
> This option is available on servers with AMD processors.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > AMD SMT Option.
2. Select one of the following:
   - Enabled—Each physical processor core operates as two logical processor cores. Enabling this option can improve overall performance for applications that benefit from a higher processor core count.
   - Disabled—Each physical processor core operates as one logical processor core.
3. Save your setting.

Configuring Performance Determinism Options

About this task

> **NOTE**
> This option is available on servers with AMD processors.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > Performance Determinism.
2. Select one of the following:

   Use this option to configure AMD determinism control.

   - Auto: Uses the processor fused values. AMD may change these based on the processor family.
   - Manual: Allows you to override the fused value allowing the same determinism setting across all processor families.
3. Select one of the following:

   Use this to configure the processor to maximize power or performance, based on your workload requirements.

   - Power Deterministic
   - Performance Deterministic
4. Save your setting.

Selecting AMD Page Table Entry Speculative Lock Scheduling options

About this task

Use this feature to configure the AMD Page Table Entry Speculative Lock Scheduling options.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > AMD Page Table Entry Speculative Lock Scheduling.
2. Select Enabled or Disabled.

   Disabling this forces Page Table Entry locks to only be scheduled nonspeculatively. Disabling this feature will impact performance.

Enabling or disabling UPI3 Link

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > UPI3 Link.
2. Select a setting.
   - Enabled: The PCIe port3 lane 0 is degraded from Gen5 to Gen4.
   - Disabled (default, recommended): Provides maximum PCIe performance from PCIe port3 lane 0.
3. Save your setting.

Configuring ANC mode

About this task

Configure the Ampere Non-Uniform Memory Access Control (ANC) mode to divide the cores, cache, and memory of the processor into multiple Non-Uniform Memory Access (NUMA) domains. Enabling this option can increase performance for workloads that are NUMA aware

and optimized.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options.
2. Select a setting:
   - Monolithic (default)—Systems configured with monolithic mode have a single NUMA partition per socket. All cores have the same access to the available memory channels on the socket.
   - Hemisphere—Systems configured with hemisphere mode have two NUMA partitions per socket. Half of the cores are grouped and half of the memory channels are assigned. The remaining cores are assigned to the other partition with the remaining memory channels.
   - Quadrant—Systems configured with quadrant mode have four NUMA partitions per socket. Each quadrant contains a quarter of the cores and is assigned the physically closest MCU pair.
3. Save your setting.

Enabling or disabling SLC as L3 Cache

About this task

Use SLC as L3 cache to enable or disable using the SLC as L3 Cache and improve system performance in 1P systems. The SLC is not a traditional processor-side L3 or L4 cache. The SLC is a memory-side cache. For 1P systems in monolithic ANC mode, the SLC functions as a traditional 16 MB L3 cache.

NOTE

This is limited to ANC Monolithic mode.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options.
2. Select a setting:
   - Enable
   - Disable (default)
3. Save your setting.

Enabling or disabling Prefetcher

About this task

Use Prefetcher to configure CPU prefetching.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options.
2. Select a setting:
   - Enable (default)
   - Disable

3. Save your setting.

Configuring FP512

About this task

Use FP512 option to configure floating point data path of AVX-512 instruction.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Processor Options > FP512.
2. Select a setting:
   - Enabled: It means that the data path is 512-bit.
   - Disabled: It means that the data path is 256-bit.
3. Save your setting.

Changing Memory Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options.

Subtopics

Configuring Refresh Watermarks

About this task

Use the Refresh Watermarks option to select the memory controller's "Refresh Watermarks" Settings. When Auto is selected, the system automatically sets this feature based on the installed DIMMs and the supported DIMM topology. When Low Watermark (Low WM) is selected, the system can mitigate failures due to row hammer traffic patterns.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Refresh Watermarks.
2. Select a setting.
   - Auto (default)
   - Low WM
3. Save your setting.

Configuring Row Hammer mode

About this task

Use the Row Hammer Mode option to select how the memory controller addresses possible row hammer DRAM vulnerabilities.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Row Hammer Mode.
2. Select a setting.
   - Auto (default)–the system automatically sets mode to RFM (Refresh Management) or pTRR based on the installed DIMMs and the supported DIMM topology.

     RFM securely refreshes all potential victim rows, but could impact performance.
   - pTRR– The Pseudo Target Row Refresh mode refreshes possible victim rows, but with no negative impact on performance or power consumption.
   - Disabled– Row hammer mitigation is not applied.
3. Save your setting.

Configuring memory remapping

About this task

Use the Memory Remap option to remap system memory that might be disabled due to a failure event, such as an uncorrectable memory

error.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Remap.
2. Select a setting.
   - Remap All Memory—Makes all memory in the system available again on the next boot.
   - No Action—Leaves any affected memory unavailable to the system.
3. Save your setting.

Configuring Advanced Memory Protection

About this task

Use the Advanced Memory Protection option to configure additional memory protection with Error Checking and Correcting (ECC). Advanced ECC Support provides the largest memory capacity to the operating system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Advanced Memory Protection.
2. Select a setting.
   - HPE Fast Fault Tolerant (ADDDC)—Enables the system to correct memory errors and continue to operate in cases of multiple DRAM device failures on a DIMM. Provides protection against uncorrectable memory errors beyond what is available with Advanced ECC.

     NOTE

     There must be a minimum of two ranks on each populated channel. Also, only HPE SmartMemory in x4 organization can be used. The x4 organization refers to the data width of the DRAM used to construct the DIMM.
   - Advanced ECC Support—Provides the largest memory capacity to the operating system while protecting the system against all single-bit failures and some multi-bit failures.
   - Mirrored Memory with Advanced ECC Support —Provides the maximum protection against uncorrected memory errors that might otherwise result in a system failure. You must install additional memory to provide mirrored memory to the operating system.
3. Save your settings.

Configuring the Memory Refresh Rate

About this task

The Memory Refresh Rate option controls the refresh rate of the memory controller and might affect the performance and resiliency of the server memory. It is recommended that you leave this setting in the default state unless indicated in other documentation for this server.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Refresh Rate.

2. Select a setting.
   - 1x Refresh
   - 2x Refresh
3. Save your setting.

Configuring DRAM Burst Refresh Mode

About this task

The DRAM Burst Refresh Mode option provides mitigation for the TRRespass and the targeted row refresh exploits.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > DRAM Burst Refresh Mode.
2. Select a setting.
   - Enabled—By default the setting is enabled.
   - Disabled—The setting is disabled for mitigation to the TRRespass.
3. Save your setting.

Enabling or disabling channel interleaving

About this task

Use the Channel Interleaving option to enable or disable a higher level of memory interleaving. Typically, higher levels of memory interleaving result in maximum performance. However, reducing the level of interleaving can result in power savings.
When you are enabling NVDIMM-N Memory Interleaving, you must also enable Channel interleaving.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Channel Interleaving.
2. Select a setting.
   - Enabled—Enables the highest level of interleaving for which the system memory is configured.
   - Disabled—Does not enable memory interleaving.
3. Save your setting.

Enabling or disabling NUMA

About this task

Use this option to enable the NUMA architecture properties for the system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > NUMA.
2. Select from one of the settings:
   - Enabled(Default)
   - Disabled
3. Save your setting.

Enabling or disabling Virtual NUMA

About this task

Use this option to enable the Virtual NUMA architecture properties for the system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Virtual NUMA.
2. Select from one of the settings:
   - Enabled
   - Disabled (Default)
3. Save your setting.

Configuring IMC Interleaving

About this task

Use this option to control the Memory Controller Interleaving option.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Controller Interleaving.
2. Select a setting.
   - Auto—(Recommended) The system automatically enables or disables memory controller interleaving based on the system configuration.
   - Disabled—You can force disable memory controller interleaving. In some instances, selecting Disable showed a performance benefit in all system memory.
3. Save your setting.

Configuring AMD Interleaving

Prerequisites

You can only configure this option if the Workload Profile is set to Custom.

About this task

Use this option to control the Memory Interleaving Mode option. You can modify the level of interleaving for which the memory system is configured. Typically, automatic interleaving results in maximum performance.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > AMD Memory Interleaving.
2. Select one of the following:
   - Channel Interleaving
   - Die Interleaving
   - Socket Interleaving
3. Select a setting:
   - Enable
   - Disable
4. Save your setting.

NOTE

The AMD Memory Interleaving option is only supported in ProLiant Gen10 servers.

Enabling or disabling Memory PStates

About this task

Use the Memory PStates option to enable or disable the memory PStates.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory PStates.
2. Select a setting.
   - Enable
   - Disable
3. Save your setting.

Configuring AMD Remap 1TB

About this task

Enable the AMD remap 1TB option to reclaim 12GB of RAM that is marked reserved when IOMMU is enabled on a system with at least 1TB

of RAM. Enabling this option will cause a large gap in the accessible memory map that may cause problems with some operating systems.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > AMD Remap 1TB.
2. Select one of the following:
   - Enable
   - Disable
3. Save your setting.

Setting the maximum memory bus frequency

About this task

Use the Maximum Memory Bus Frequency option to configure the system to run memory at a lower maximum speed than that supported by the installed processor and DIMM configuration.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Maximum Memory Bus Frequency.
2. Select a setting.
   - Auto—Memory runs at the maximum speed supported by the system configuration.
   - 6400 MHZ
   - 6000 MHZ
   - 5600 MHZ
   - 5200 MHZ
   - 4800 MHZ
   - 4400 MHZ
   - 4000 MHZ
   - 3600 MHZ
   - 3200 MHZ
   - 2933 MHZ

   NOTE

   For the supported memory bus frequency of each processor, see **Maximum Memory Bus Frequency** under What's new in Gen11? section.
3. Save your setting.

Enabling or disabling Memory Patrol Scrubbing

Prerequisites

Workload Profile is set to Custom.

About this task

When enabled, Memory Patrol Scrubbing corrects memory soft errors so that, over the length of the system runtime, the risk of producing multibit and uncorrectable errors is reduced.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Patrol Scrubbing.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling node interleaving

About this task

Use the Node Interleaving option to enable or disable NUMA node interleaving. Typically, you can obtain optimum performance on NUMA nodes by leaving this option disabled. When this option is enabled, memory addresses are interleaved across the memory installed for each processor and some workloads might experience improved performance.

IMPORTANT

This option is only available on HPE ProLiant Gen10 servers, and not on Gen10 Plus servers.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Node Interleaving.
2. Select a setting.
   - Enabled—Memory addresses are interleaved across the memory installed for each processor. All nodes must be of equal memory size. System performance might be impacted.
   - Disabled—Disables node interleaving, providing optimum performance in most environments.
3. Save your setting.

Configuring Memory Encryption Options

See the subtopics for information on configuring Memory encryption options.

Subtopics

Configuring AMD Secure Memory Encryption
Enabling or disabling AMD Secure Nested Paging

Enabling or disabling Transparent Secure Memory Encryption

About this task

Use the Transparent Secure Memory Encryption option to enable or disable Transparent Secure Memory Encryption (TSME).

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Encryption Options > Transparent Secure Memory Encryption.
2. Select a setting.
   - Enable
   - Disable
3. Save your setting.

Configuring AMD Secure Memory Encryption

About this task

Enabling this feature allows you to use the AMD Secure Memory Encryption functionality.

NOTE
This option is available on servers with AMD processors.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Encryption Options > AMD Secure Memory Encryption.
2. Select an option.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling AMD Secure Nested Paging

About this task

Use AMD Secure Nested Paging to enable AMD SEV-SNP. When enabled, SEV-SNP adds strong memory integrity protection to help prevent malicious hypervisor-based attacks like memory replay, memory remapping and more to create an isolated execution environment.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory

Encryption Options > AMD Secure Nested Paging.

2. Select a setting.
   - Enabled
   - Disabled (default)
3. Save your setting.

Configuring the memory mirroring mode

Prerequisites

To activate this feature, enable the Mirrored Memory with Advanced ECC Support option on the Configuring Advanced Memory Protection menu.

About this task

Use the Memory Mirroring option to configure how much of the total available system memory is reserved for mirroring.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Mirroring Mode.
2. Select a setting.
   - Full Mirror—Reserves 50% of the total available memory for mirroring.
   - Partial Mirror (20% above 4GB)—Reserves 20% of the total available memory above 4 GB for mirroring.
   - Partial Mirror (10% above 4GB)—Reserves 10% of the total available memory above 4 GB for mirroring.
   - Partial Mirror (Memory below 4GB)—Depending on the memory configuration, reserves 2 GB or 3 GB of lower memory below 4 GB for mirroring.
   - Partial Mirror (OS Configured)—Enables the operating system to configure partial memory mirroring.
3. Save your setting.

Configuring NVDIMM-N Options

Procedure

1. From the System Utilities screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Memory Options** > **Persistent Memory Options** > **NVDIMM-N Options**.
2. Select **Enabled** or **Disabled** for the following options:
   - NVDIMM-N Support
   - NVDIMM-N Interleaving
   - NVDIMM-N Sanitize/Erase on Next Reboot Policy

IMPORTANT

Sanitizing/Erasing an NVDIMM-N results in the loss of **all** user data saved in the NVDIMM-N. Hewlett Packard Enterprise strongly recommends that you perform a manual backup of all user data in the NVDIMM-Ns before sanitizing/erasing the NVDIMM-Ns.

- Sanitize/Erase all NVDIMM-N in the System
- Sanitize/Erase all NVDIMM-N on Processor —These menu items differ based on your server configuration.
- Sanitize/Erase Processor 1 DIMM 2 —These menu items differ based on your server configuration.

3. Save your changes.

Subtopics

NVDIMM-N Support

This option enables NVDIMM-N support (including backing up the contents of the memory to flash on power down or reset) to be enabled or disabled. If **Disabled** is selected for this option, the NVDIMM-Ns in the system are not presented to the operating system as either persistent storage or system memory.

NVDIMM-N Sanitize/Erase on Next Reboot Policy

This setting is part of the process to sanitize or erase all user data and error status data saved in the selected NVDIMM-Ns. After enabling the NVDIMM-N Sanitize/Erase on Next Reboot Policy, the screen displays various options for sanitizing NVDIMMs. The following selections are available depending on the NVDIMM-Ns installed on the server:

- Sanitize/Erase all NVDIMM-N in the System—Sanitizes all NVDIMM-Ns installed in the server on reboot.
- Sanitize/Erase all NVDIMM-N on Processor X—Sanitizes all NVDIMM-Ns installed in the DIMM slots for processor X on reboot.
- Sanitize/Erase Processor X DIMM Y—Sanitizes the NVDIMM-N installed in DIMM slot Y for processor X on reboot. A selection is available for each Processor X DIMM slot that contains an NVDIMM-N.

Selected NVDIMM-Ns are sanitized on the next reboot of the system. The largest group of NVDIMM-Ns selected is sanitized. For example, if **Sanitize/Erase all NVDIMM-N on Processor 1** is enabled and **Sanitize/Erase Processor 1 DIMM 8** is disabled, all NVDIMM-Ns on processor 1 are sanitized including processor 1 DIMM 8.

The following policies control the action of the system after NVDIMM-Ns are sanitized/erased:

- Power off the system after sanitizing/erasing NVDIMMs
- Boot to the operating system after sanitizing NVDIMMs
- Boot to the System Utilities after sanitizing NVDIMMs

NVDIMM-N Interleaving

This option enables NVDIMM-Ns installed on a particular processor to be interleaved with other NVDIMM-Ns in the memory map. This option does not impact the interleaving of HPE SmartMemory DIMMs. Interleaving is never enabled across NVDIMM-Ns and HPE

SmartMemory DIMMs. NVDIMM-Ns installed on different processors are never interleaved together. If this setting is changed (to **Enabled** or **Disabled**), then all installed NVDIMM-Ns must be sanitized. If all installed NVDIMM-Ns are not sanitized, then an error condition is reported on the next boot and the NVDIMM-Ns are not available for use.

Enabling or disabling Memory Configuration Violation Reporting

About this task

Use Memory Configuration Violation Reporting to configure how the system will message and log memory configuration violations.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Configuration Violation Reporting.
2. Select a setting.
   - Enabled: (Default) In this state, the system reports the memory configurations that are not part of the supported and validated memory guidelines.

     NOTE

     Consult the memory population guidelines for a list of validated and supported configurations.
   - Disabled: In this state, the memory configuration violations are not reported.

     NOTE

     It is recommended that the default configuration (Enabled) be maintained.
3. Save your setting.

Enabling or disabling Memory Permanent Fault Detect

About this task

Memory Permanent Fault Detect controls the Intel Permanent Fault Detect (PFD) functionality. When enabled, the memory controller is able to better detect and correct memory errors which may have a performance impact on the memory subsystem.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Permanent Fault Detect.
2. Select a setting.
   - Enabled (default)
   - Disabled
3. Save your setting.

Configuring the HBM Memory Options

About this task

Sapphire rapids with High Bandwidth Memory (HBM) value provide significant performance improvement for memory bandwidth sensitive workloads (WLs). They have approximately 1 Tera Byte (TB) per second (TB/s) of memory Bandwidth (BW).

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > HBM Memory Options.
2. Select a value for the HBM Memory Mode:
   - 2LM—The system attempts to configure this option to 2LM if the system configuration allows for it.
   - 1LM—The system downgrades to 1LM.
3. Save your setting.

Enabling or disabling Total Memory Encryption (TME)

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options > Memory Encryption Options > Total Memory Encryption (TME).
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Configuring ECC mode

About this task

Use ECC mode to configure how the system handles error correction.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options.
2. Select a setting:
   - Auto (default)—Auto-detect device width and select the recommended mode.
   - SECDED—Single-error correction and double-error detection, recommended for non-x4 DIMMs
   - Symbol—Recommended only for x4 DIMMs
3. Save your setting.

Configuring ECC control

About this task

Use ECC control to configure how the system controls error correction.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options.
2. Select a setting:
   - DE enabled—Defers uncorrectable read errors by sending an OK response. If this bit is clear the system defaults to non-deferred behavior when encountering an unrecoverable error.
   - FI enabled—Enables fault handling interrupt. The fault handling interrupt is raised to give notice that an ECC fault has been recorded.
   - DE and FI enabled (default)
3. Save your setting.

Enabling or disabling Patrol Scrub

About this task

Use Patrol scrub to scrub for a duration of 24 hours.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options.
2. Select a setting:
   - Enable (default)
   - Disable
3. Save your setting.

Enabling or disabling Demand Scrub

About this task

Use Demand scrub to enable or disable the ability to write corrected data back to the memory once a correctable error is detected.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options.
2. Select a setting:
   - Enable (default)
   - Disable
3. Save your setting.

Configuring Fine Granularity Refresh (FGR)

Configuring Fine Granularity Refresh (FGR)

About this task

Configure Fine Granularity Refresh (FGR) mode to address how the memory controller addresses possible row hammer DRAM vulnerabilities.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Memory Options.
2. Select a setting:
   - 1x (default)
   - 2x
   - 1x w/RowHammer mitigation
   - 2x w/RowHammer mitigation
3. Save your setting.

Changing Virtualization Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options.

Subtopics

Enabling or disabling Virtualization Technology

About this task

Use the Intel(R) Virtualization Technology (Intel VT) to control whether a Virtual Machine Manager (VMM) supporting Virtualization Technology can use hardware capabilities provided by UEFI Intel processors.

NOTE

You do not need to disable Virtualization Technology if you are using a VMM or an operating system that does not support AMD-V virtualization.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > Intel(R)

Virtualization Technology (Intel VT).

2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling Intel VT-d

About this task

Use the Intel (R) VT-d option to enable or disable Intel Virtualization Technology for Directed I/O (VT-d) on a Virtual Machine Manager (VMM).

> **NOTE**
> If you are not using a hypervisor or an operating system that supports this feature, it is not necessary to set the Intel (R) VT-d option to disabled. You can leave it enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > Intel (R) VT-d.
2. Select a setting.
   - Enabled—Enables a hypervisor or operating system supporting this option to use hardware capabilities provided by Intel's Virtualization Technology for directed I/O.
   - Disabled—Does not enable a hypervisor or operating system supporting this option to use hardware capabilities provided by Intel's Virtualization Technology for directed I/O.
3. Save your setting.

Enabling or disabling Access Control Service

About this task

Access Control Service is required for virtualization. Hewlett Packard Enterprise recommends enabling this setting for the virtualization use case. For non-virtualization use cases, disabling Access Control Service enables direct peer-to-peer communication between hardware devices.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > Access Control Service.
2. Select a setting.
   - Enable
   - Disable
3. Save your setting.

Enabling or disabling SR-IOV

About this task

The SR-IOV (Single Root I/O Virtualization) interface is an extension to the PCI express (PCIe) specification. It enables the BIOS to allocate more PCI resources to PCIe devices. Enable this option for a PCIe device or operating system that supports SR-IOV. Leave it enabled when using a hypervisor.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > SR-IOV.
2. Select a setting.
   - Enabled—Enables a hypervisor to create virtual instances of a PCIe device, potentially increasing performance.
   - Disabled—Does not enable a hypervisor to create virtual instances of a PCIe device.
3. Save your setting.

Setting the Minimum SEV ASID

About this task

Use the Minimum SEV ASID option to configure the Minimum Address Space Identifier (ASID) that can be used for AMD Secure Encrypted Virtualization (SEV) enabled guests. ASID below this number are only available to SEV enable guest that also enable Encrypted State (SEV-ES).

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > Minimum SEV ASID.
2. Enter a number between 1 to 16.
3. Save your setting.

Enabling AMD I/O Virtualization Technology

About this task

If enabled, a hypervisor or operating system supporting this option can use hardware capabilities provided by AMD VT. You can leave this set to Enabled even if you are not using a hypervisor or an operating system that uses this option.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > AMD I/O Virtualization Technology.
2. Select one of the following:
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling AMD DMA Remapping

About this task

AMD DMA Remapping configures the DMA Remapping setting. DMA Remapping protects from memory corruption and malicious DMA attacks.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > AMD DMA Remapping.
2. Select one of the following:
   - Enabled
   - Disabled
3. Save your setting.

Enabling or Disabling AMD DMAr Support

About this task

Use this option to configure **AMD DMAr Support**. This control enables or disables the DMAR mitigation during POST.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > AMD DMAr Support.
2. Select one of the following:
   - Enabled: Enables the DMAR mitigation during POST.
   - Disabled: Disables the DMAR mitigation during POST.
3. Save your setting.

Enabling or Disabling AMD DMA Protection

About this task

Use this option to configure AMD DMA Protection. This control enables or disables the DMA remap support in IVRS IVinfo Field.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > AMD DMA Protection.
2. Select one of the following:
   - Enabled: Enables the DMA remap support in IVRS IVinfo Field.
   - Disabled: Disables the DMA remap support in IVRS IVinfo Field.

3. Save your setting.

Enabling AMD 5-Level Page

About this task

Enabling AMD 5-Level Page extends the size of virtual addresses from 48 bits to 57 bits, increasing the addressable virtual memory up to 128 PB.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options > AMD 5-Level Page.
2. Select one of the following:
   - Enabled
   - Disabled (default)
3. Save your setting.

Enabling or disabling ARM SMMU PMU

About this task

Use the ARM System Memory Management Unit Performance Monitoring Unit to enable or disable IO virtualization for virtual machines.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Virtualization Options.
2. Select a setting:
   - Enable
   - Disable (default)
3. Save your setting.

Changing Boot Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options.

Subtopics

Deleting boot options from the UEFI Boot Order list

Setting the boot order policy

About this task

Use the Boot Order Policy option to control the system behavior when attempting to boot devices per the UEFI Boot Order list and no bootable device is found.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > Boot Order Policy.
2. Select a setting.
   - Retry Boot Order Indefinitely —The system continuously attempts the boot order until a bootable device is found.
   - Attempt Boot Order Once —The system attempts to execute all items in the boot menu once, and halts the system.
   - Reset After Failed Boot Attempt —The system attempts to execute all items once, and reboots the system.
3. Save your setting.

Setting the filter on nonbootable drives

About this task

Use the Filter Non-bootable Drives option to control the creation of boot options of the system by checking the available file system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > Filter Non-bootable Drives.
2. Select a setting.
   - Auto—When the number of boot options becomes excessive, the system will not create boot options for fixed drives that are not bootable.
   - Enabled—The system will not create boot options for fixed drives that are not bootable.
   - Disabled—The system will create boot options for each fixed drives even if these are not bootable.
3. Save your setting.

Changing the UEFI Boot Order list

About this task

Use the UEFI Boot Order option to change the order in which entries in the UEFI Boot Order list boot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot

Settings > UEFI Boot Order.

2. To navigate within the boot order list, use your pointing device or the arrow keys.
3. Select an entry and change its order in the list:
   - To move an entry higher in the boot list, press the + key, or drag and drop the entry.
   - To move an entry lower in the boot list, press the - key, or drag and drop the entry.
4. Save your changes.

Controlling the UEFI boot order

About this task

Use the UEFI Boot Order Control option to enable or disable individual UEFI boot options. Enabled items are selected (checked). Disabled items remain in their location in the UEFI Boot Order list, but are not attempted during the boot process.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Settings > UEFI Boot Settings > UEFI Boot Order Control.
2. Do the following:
   - To enable an option, select the corresponding check box.
   - To disable an option, select the corresponding check box.
3. Save your changes.

Adding a boot option to the UEFI Boot Order list

About this task

Use Add Boot Option to select an x64 UEFI application with an .EFI extension, such as an OS boot loader or other UEFI application, to add as a new UEFI boot option.

The new boot option is appended to the UEFI Boot Order list. When you select a file, you are prompted to enter the boot option description (which is then displayed in the boot menu), as well as any optional data to be passed to an .EFI application.

Procedure

1. Attach media with a FAT16 or FAT32 partition on it.
2. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Settings > Add Boot Option.
3. Browse for an .EFI application from the list, and then press Enter.
4. If necessary, continue to press Enter to drill-down through the menu options.
5. Enter a boot option description and optional data, and then press Enter.

   The new boot option appears in the UEFI Boot Order list.
6. Select Commit changes and exit.

Deleting boot options from the UEFI Boot Order list

About this task

NOTE

If a deleted option points to a standard boot location, such as a network PXE boot or a removable media device, the system BIOS adds the option on the next reboot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > UEFI Boot Settings > Delete Boot Option.
2. Select one or more options from the list.
3. Select Commit Changes and Exit.

Changing Network Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options.

Subtopics

Network Boot Options
Configuring Pre-Boot Network Settings
iSCSI Boot Configuration
NVMe-oF Boot Configuration
Configuring VLAN Configuration
Changing Embedded iPXE options

Network Boot Options

- Pre-Boot Network Environment Policy
- IPv6 DHCP Unique Identifier
- Network Boot Retry Support
- Network Interface Cards (NICs)
- PCIe Slot Network Boot
- HTTP Support
- iSCSI Software Initiator

Subtopics

Setting the Pre-Boot Network Environment
Setting the IPv6 DHCP Unique Identifier method

Setting the Pre-Boot Network Environment

About this task

Use the Pre-Boot Network Environment option to set a preference for how your network boot targets appear in the UEFI Boot Order list. This option also controls the Pre-Boot network operations from Embedded UEFI Shell.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options > Pre-boot Network Environment.
2. Select a setting.
   - Auto—All network operations initiated in the pre-boot environment occur over IPv4 or IPv6. The order of the existing network boot targets in the UEFI Boot Order list is not modified. New network boot targets are added to the end of the list using the default policy of the system BIOS.
   - IPv4—All network operations initiated in the pre-boot environment only occur over IPv4. Removes all existing IPv6 network boot targets in the UEFI Boot Order list. New IPv6 network boot targets are not added to the list.
   - IPv6—All network operations initiated in the pre-boot environment only occur over IPv6. Removes all existing IPv4 network boot targets in the UEFI Boot Order list. New IPv4 network boot targets are not added to the list.
3. Save your changes.

Setting the IPv6 DHCP Unique Identifier method

About this task

Use the IPv6 DHCP Unique Identifier option to control how the IPv6 DHCP Unique Identifier (DUID is set.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options > IPv6 DHCP Unique Identifier.
2. Select a setting.
   - Auto—Sets the DUID using the Universal Unique Identifier (UUID) of the server or, if the server is not available, the Link-Layer Address Plus Time (DUID-LLT) method.
   - DUID-LLT—Sets the DUID using the Link-Layer Address Plus Time (DUID-LLT) method.
3. Save your changes.

Enabling or disabling Network Boot Retry Support

About this task

Use the Network Boot Retry Support option to enable or disable the network boot retry function. When enabled, the system BIOS attempts to boot the network device up to the number of times set in the Network Boot Retry Count option before attempting to boot the next network device. This setting only takes effect when attempting to boot a network device from the F12 function key and one-time boot options.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options > Network Boot Retry Support.
2. Select a setting.
   - Enabled—Enables network boot retry.
   - Disabled—Disables network boot retry.
3. Save your changes.

Enabling or disabling network boot for a NIC

About this task

Use the Network Interface Cards (NICs) option to enable or disable network boot for an installed NIC. Devices listed vary from system to system and can include, for example:

- Embedded LOM 1 Port 1
- Embedded FlexibleLOM 1 Port 1

NOTE

You might need to configure the NIC firmware to activate the boot option.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options.
2. Select a NIC.
3. Select a setting.
   - Network Boot—Enables network boot.
   - Disabled—Disables network boot.
4. Save your changes.
5. If you selected Network Boot, reboot the server so that the NIC boot option appears in the boot order list.

Enabling or disabling PCIe Slot Network Boot

About this task

Use the PCIe Slot Network Boot option to enable or disable UEFI network boot for NIC cards in PCIe slots.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options > PCIe Slot Network Boot .
2. Select a PCIe slot entry.
3. Select a setting.
   - Enabled—Enables UEFI network boot for NIC cards in PCIe slots.
   - Disabled—Disables UEFI network boot for NIC cards in PCIe slots.
4. Save your changes.

Setting HTTP support

Prerequisites

Use this option to control the UEFI HTTP(s) boot support when in UEFI Mode and using the Embedded UEFI Shell > Discover Shell Auto-Start Script using DHCP setting.

To enable HTTPS boot, either by selecting Auto or HTTPS only, you must enroll the respective TLS certificate of the HTTPS server under Server Security > TLS (HTTPS) Options.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options > HTTP Support.
2. Select a setting.
   - Auto—Automatically adds HTTP(S) boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Enables the system to boot to the HTTP or HTTPS URLs provided by the DHCP server. Any other URLs provided by the DHCP server are ignored.
   - HTTP only—Automatically adds HTTP boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Enables the system to boot to the HTTP URLs provided by the DHCP server, and to ignore any HTTPS or other URLs that are provided.
   - HTTPs only—Automatically adds HTTPS boot options to the UEFI Boot Order list for every network port that is enabled for Network Boot. Enables the system to boot to the HTTPS URLs provided by the DHCP server, and to ignore any HTTP or other URLs that are provided.
   - Disabled
3. Save your changes.

Enabling iSCSI Software Initiator

About this task

Enables or disables the iSCSI Software Initiator. When enabled, the system's iSCSI Software Initiator will be used to access iSCSI targets on any configured NIC ports. When disabled, the system's iSCSI Software Initiator will not attempt to access any configured iSCSI targets.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network

Boot Options > iSCSI Software Initiator .

2. Select a setting.
   - Enabled—Enables the UEFI iSCSI software initiator.
   - Disabled—Disables the UEFI iSCSI software initiator.

   NOTE

   This option only controls whether the iSCSI Software Initiator is Enabled or Disabled. To enable iSCSI boot from the adapter initiator, you must enable iSCSI in the adapter firmware and configure it.

3. Save your changes.

Enabling NVMe-oF Software Initiator

About this task

Enables or disables the NVMe-oF Software Initiator. When enabled, the system's NVMe-oF Software Initiator will be used to access NVMe-oF targets on any configured NIC ports. When disabled, the system's NVMe-oF Software Initiator will not attempt to access any configured NVMe-oF targets.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Network Boot Options > NVMe-oF Software Initiator .
2. Select a setting.
   - Enabled—Enables the UEFI NVMe-oF software initiator.
   - Disabled—Disables the UEFI NVMe-oF software initiator.

   NOTE

   This option only controls whether the NVMe-oF Software Initiator is Enabled or Disabled. To enable NVMe-oF boot from the adapter initiator, you must enable NVMe-oF in the adapter firmware and configure it. This option may not support in some products.

3. Save your changes.

Configuring Pre-Boot Network Settings

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Pre-Boot Network Settings.
2. Select any of the Pre-boot Network Settings options.
3. Select additional settings or enter additional values for that option.
4. Save your changes.

Subtopics

Pre-Boot Network Settings
Prerequisites for Boot from URL

More information

- Pre-Boot Network Settings

Pre-Boot Network Settings

Use this option to configure a preboot network interface and related settings.

> **IMPORTANT**
> If you plan to run `webclient` or `ftp` over the same interface, you do not need to use the Embedded UEFI Shell `ifconfig` command on a network interface. The Pre-Boot Network Settings configured in the System Utilities automatically selects these interface.
> If the interface used by `ftp` and `webclient` are configured by `ifconfig`, that setting is erased. Instead, the System Utilities Pre-Boot Network Settings menu is applied on the interface when the commands are run.

- Pre-Boot Network Interface—Specifies the network interface used for preboot network connections.
  - Auto (default)—The system uses the first available port with a network connection.
  - Select Specific Port—The system uses the selected NIC port.
- DCHPv4—Enables or disables obtaining the preboot network IPv4 configuration from a DHCP server for Network operations from the Embedded UEFI Shell, and Boot from URL.
  - Enabled—Enables DHCPv4 network address configuration. Individual settings are not available.
  - Disabled—Disables DHCPv4 address configuration, requiring you to configure the following static IP address settings manually.
    - IPv4 Address
    - IPv4 Subnet Mask
    - IPv4 Gateway
    - IPv4 Primary DNS
- Preboot Network Proxy—Specifies a preboot network proxy. When set, network operations for the Pre-Boot Network Interface are attempted through the configured proxy. The proxy must be in an HTTP URL format, and can be specified as `http://IPv4_address:port`, `http://[IPv6_address]:port` or `http://FQDN:port`.
- IPv6 Config Policy
  - Automatic—Enables preboot network IPv6 configuration to be automatically obtained for Network operations from the Embedded UEFI Shell. Individual settings are not available.
  - Manual—Enables you to configure static IP address settings individually.
- Boot from URL 1, 2, 3 or 4—Specifies a network URL to a bootable ISO or EFI file. Enter a URL in either HTTP or HTTPS format, using either an IPv4 or IPv6 server address or host name. For example, the URLs can be in any of the following formats: `http://192.168.0.1/file/image.iso`, `http://example.com/file/image.efi`, `https://example.com/file/image.efi`, `http://[1234::1000]/image.iso`. When configured, this URL is listed as a boot option in the UEFI Boot menu. Then you can select this option from the boot menu to download the specified file to the system memory and enable the system to boot from the file.

NOTE

Boot from URL uses the IP address settings configured in Pre-Boot Network Settings page.

Booting from an ISO file can involve only booting a preliminary OS environment image, such as WinPE or a mini Linux, or a complete OS install image if the OS supports the HTTP Boot feature (Old OS versions may not support booting from an ISO file or OS install image). Please check your OS documentation for the HTTP Boot feature support.

Prerequisites for Boot from URL

About this task

Leave the boot mode set to UEFI Mode when using the Boot from URL.

iSCSI Boot Configuration

NOTE

You can also configure iSCSI Boot settings using the RESTful Interface Tool. See the RESTful Interface Tool documentation at **https://www.hpe.com/info/restfulinterface/docs**.

Subtopics

Adding an iSCSI initiator name

About this task

Use the iSCSI Initiator Name option to set a name for the iSCSI initiator using iSCSI Qualified Name (IQN) format. EUI format is not supported. This option replaces the default name set for the initiator.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > iSCSI Boot Configuration > iSCSI Initiator Name.
2. Enter a unique name for the iSCSI initiator using iSCSI Qualified Name (IQN) format. For example: `iqn.2001-04.com.example:uefi-13021088`

   This setting is saved automatically.

Adding an iSCSI Attempt

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > iSCSI Configuration > Add an iSCSI Attempt.

   A message appears stating that this boot attempt will not be in effect until the next server reboot.

2. Press Enter.
3. Select a port on which to attempt an iSCSI connection.
4. Complete the configuration settings:
   - iSCSI Attempt Name—Enter a name.
   - iSCSI Boot Control—Select Enabled or Enabled for MPIO.

     NOTE

     The default setting is Disabled. Use Enabled for MPIO to enable the Multi-Path I/O [MPIO] capability.

   - IP Address Type—Select an address type.
   - Connection Retry Count—Enter a value from 0 to 16. The default is three retries.
   - Connection Timeout—Enter a value in ms from 100 to 20000. The default is 20000 (20 seconds).
   - Initiator DHCP—It is the default setting. If you must configure static IP addresses for the Initiator, clear this option. The target name, IP address, port, and boot LUN must also be configured manually (disable Target DHCP Config) if you configure static addresses for the Initiator.
   - Target DHCP Config—It is the default setting. If you must configure the target settings manually, clear this check box) and enter a target name, IP address, port, and boot LUN.
   - Optional: Authentication Type—Default is NONE. If required, select CHAP, and then complete the CHAP entries.
5. Select Save Changes.
6. Reboot the system.

Deleting iSCSI boot attempts

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > iSCSI Boot Configuration > Delete iSCSI Boot Attempts.
2. Select one or more iSCSI boot attempt entries.
3. Select Commit Changes and Exit.

Viewing and modifying iSCSI boot attempt details

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > iSCSI Boot Configuration > iSCSI Attempts.

2. Select an entry from the list.
3. View or modify the details about the boot attempt.

NVMe-oF Boot Configuration

NOTE

- NVMe-oF Boot Configuration may not support in some products.
- HPE has only validated NVMe-oF storage arrays that are either based on the SPDK framework or implemented using the Linux nvmet-tcp subsystem, as well as HPE-branded storage arrays. Other third-party solutions may exhibit differences in protocol behavior, firmware compatibility, or boot target configuration, which can lead to inconsistent results.
- You can also configure NVMe-oF boot settings using the RESTful Interface Tool. See the RESTful Interface Tool documentation at **https://www.hpe.com/info/restfulinterface/docs**.

Subtopics

Adding a NVMe-oF initiator name

About this task

Use the NVMe-oF Initiator Name option to set a name for the NVMe-oF initiator using NVMe Qualified Name (NQN) format. The EUI format is not supported. This option replaces the default name set for the initiator.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > NVMe-oF Configuration > NVMe-oF Initiator Name.
2. Enter a unique name for the NVMe-oF initiator using the NVMe Qualified Name (NQN) format. For example: `nqn.2001-04.com.example:uefi-13021088`

   This setting is saved automatically.

Adding a NVMe-oF boot attempt

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > NVMe-oF Configuration > Add a NVMe-oF Attempt.

   A message appears stating that this boot attempt will not be in effect until the next server reboot.
2. Press Enter.

3. Select a port on which to attempt an NVMe-oF connection.
4. Complete the configuration settings:
   - NVMe-oF Attempt Name—Enter a name.
   - NVMe-oF Control—Select Enabled or Disabled. This option is used for connecting to the NVMe-oF target during POST.
   - IP Address Type—Select an address type.
   - Connection Retry Count—Enter a value 0–16. The default is three retries.
   - Connection Timeout—Enter a value in ms 100–20000. The default is 20000 (20 seconds).
   - Initiator DHCP—It is the default setting. If you must configure static IP addresses for the Initiator, clear this option. The target name, IP address, and port, must also be configured manually (disable Target DHCP configuration) if you configure static addresses for the Initiator.
   - Target DHCP Config—It is the default setting. If you must configure the target settings manually (clear this check box) and enter a target name, IP address and port.
   - Optional: NID—Default is empty for auto discovery target namespace ID. If required to specific namespace ID, fill the UUID format of NID.
5. Select Save Changes.
6. Reboot the system.

Deleting NVMe-oF boot attempts

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > NVMe-oF Configuration > Delete NVMe-oF Attempts.
2. Select one or more NVMe-oF attempt entries.
3. Select Commit Changes and Exit.

Viewing and modifying NVMe-oF boot attempt details

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > NVMe-oF Configuration > NVMe-oF Attempts.
2. Select an entry from the list.
3. View or modify the details about the boot attempt.

Configuring VLAN Configuration

About this task

Use the VLAN Configuration option to configure global VLAN settings for all enabled network interfaces. The configuration includes interfaces used in PXE boot, iSCSI boot, and HTTP/HTTPS boot, and for all preboot network access from the Embedded UEFI Shell.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > VLAN Configuration.
2. Complete the following.
   a. VLAN Control—Select Enabled to enable VLAN tagging on all enabled network interfaces. This setting is disabled by default.
   b. VLAN ID—When VLAN Control is enabled, enter a VLAN ID between 1 and 4094.
   c. VLAN Priority—When VLAN Control is enabled, enter a priority value of 0 to 7 for VLAN tagged frames.
3. Save your changes.

Changing Embedded iPXE options

About this task

The embedded iPXE is as open source network boot application embedded in system BIOS that you can use to perform network boot. This option also enables the UEFI shell command `ipxe` and an entry in Embedded Application list. Both can be used to launch the Embedded iPXE.

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE.

Subtopics

Enabling or disabling the Embedded iPXE

About this task

Use the Embedded iPXE option to enable or disable the iPXE open source network boot image that is embedded in the system BIOS. Embedded iPXE provides a full PXE implementation enhanced with additional features. When enabled, and Add Embedded iPXE to Boot Order is enabled, the Embedded iPXE is added to the UEFI Boot Order list.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE > Embedded iPXE .
2. Select a setting.
   - Enabled— Enables you to launch the Embedded iPXE from the pre-boot environment and add it to the UEFI Boot Order list.
   - Disabled— The Embedded iPXE is not available in the pre-boot environment and you cannot add it to the UEFI Boot Order list.
3. Save your setting.

Adding the Embedded iPXE to the UEFI Boot Order list

Prerequisites

Boot Mode is set to UEFI Mode.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE > Add Embedded iPXE to Boot Order .
2. Select a setting.
   - Enabled— Adds the Embedded iPXE to the boot order list on the next reboot.
   - Disabled— The Embedded iPXE is not added to the boot order list.
3. Save your setting.

Enabling or disabling automatic execution of the Embedded iPXE startup script

Prerequisites

- Boot Mode is set to UEFI Mode.
- Embedded iPXE is enabled.

About this task

Use the iPXE Script Auto-Start option to enable or disable automatic execution of the Embedded iPXE startup script during Embedded iPXE startup.

- You can use the startup script to automate a sequence of iPXE commands when iPXE is launched.
- You can store the script file on local media, or access it from a network location.
- Name the script file `Startup.ipxe` and place it on the root directory of local media. You can also place the startup script on a network location accessible to the server. The script file name can be arbitrary and the file URL must be specified if a network location is used.
- When auto-start is enabled, and the iPXE Auto-Start Script Location option is set to Auto, the Embedded iPXE looks for the script file in a network location first, followed by any locally attached FAT16, or FAT32-formatted media.
- It is recommended that you have only one `Startup.ipxe` file on one file system

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE > iPXE Script Auto-Start .
2. Select a setting.
   - Enabled— The Embedded iPXE startup script executes during Embedded iPXE startup.
   - Disabled— The Embedded iPXE startup script does not execute during Embedded iPXE startup.
3. Save your setting.

Enabling or disabling Embedded iPXE script verification

Prerequisites

- Boot Mode is set to UEFI Mode.
- Embedded iPXE is enabled.
- iPXE Script Auto-Start is enabled
- Secure Boot is enabled.
- Embedded iPXE scripts are enrolled in the Secure Boot database.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE > iPXE Script Verification .
2. Select a setting.
   - Enabled— Enables iPXE script verification.
   - Disabled— (Default) Does not enable iPXE script verification.
3. Save your setting.

Setting the Embedded iPXE startup script location

Prerequisites

- Embedded iPXE is enabled.
- iPXE Script Auto-Start is enabled

About this task

Use the iPXE Auto-Start Script Location option to select the location of the Embedded iPXE startup script. When iPXE Script Auto-Start is enabled, this setting specifies where the Embedded iPXE looks for the startup script file.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE > iPXE Auto-Start Script Location .
2. Select a setting:
   - Auto: The Embedded iPXE attempts to retrieve the startup script from the network location first, followed by locally attached media.
   - File Systems on Attached Media : The Embedded iPXE looks for the Startup.ipxe script file on a UEFI-accessible local file system, such as a FAT32 partition on a USB disk, an iLO virtual drive, or HDD.
   - Network Location: The Embedded iPXE executes the .ipxe script pointed by the URL specified in this setting.
3. Save your setting.

Setting the network location for the Embedded iPXE auto-start script

Setting the network location for the Embedded iPXE auto-start script

Prerequisites

- Embedded iPXE is enabled.
- Embedded iPXE Auto-Start Script Location is set to Network Location or Auto.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Embedded iPXE > Network Location for iPXE Script-Auto Start .
2. Enter the network location of the `.ipxe` file.

   Valid values are:

   - An HTTP/HTTPS URL for either an IPv4 or IPv6 server address or host name.
   - An FTP URL for either an IPv4 server address or host name.

   Examples:

   - `http://192.168.0.1/file/file.ipxe`
   - `http://example.com/file/file.ipxe`
   - `https://example.com/file/file.ipxe`
   - `http://[1234::1000]/file.ipxe`
3. Save your setting.

Changing Storage Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options.

Subtopics

Enabling SATA Secure Erase

Prerequisites

- The SATA controller on the hard drive is in ACHI mode.
- The hard drive supports the Secure Erase command.

About this task

Use the SATA Secure Erase option to control whether SATA Secure Erase functionality is supported. This function prevents the Secure Freeze Lock command from being sent to SATA hard drives.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > SATA Secure Erase.
2. Select a setting.
   - Enabled—The Security Freeze Lock command is not sent to supported SATA hard drives, enabling Secure Erase to function.
   - Disabled—Disables Secure Erase.
3. Save your setting.

Enabling SATA Sanitize

About this task

Use the SATA Sanitizeoption to control whether sanitize functionality is supported.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > SATA Sanitize.
2. Select a setting.
   - Enabled—The Security Freeze Lock command is not sent to supported SATA hard drives, enabling sanitize to function.
   - Disabled—Disables sanitize.
3. Save your setting.

Enabling embedded chipset SATA controller support

Prerequisites

- The correct operating system drivers for your selected option.
- Boot Mode is set to UEFI Mode.

About this task

Use the Embedded SATA Configuration option to enable embedded chipset SATA (Serial Advanced Technology Attachment) controller support. You can select AHCI or HPE Smart Array SW RAID Support. Make sure that you are using the correct operating system drivers for your selected option.

CAUTION

Dynamic Smart Array is not supported when the boot mode is configured to Legacy BIOS Mode. Enabling Dynamic SmartRAID RAID results in data loss or data corruption on existing SATA drives. Back up all drives before enabling this option.

See your operating system documentation before enabling SATA AHCI support to ensure your base media drivers support this feature.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration.
2. Ensure that you are using the correct ACHI or RAID system drivers for your SATA option.
3. Select a setting.
   - SATA AHCI Support—Enables the embedded chipset SATA controller for AHCI.
   - Intel VROC SATA Support
4. Save your setting.

Setting the embedded storage boot policy

Prerequisites

Boot Mode is set to UEFI Mode.

About this task

Use the Embedded Storage Boot Policy option to select the UEFI BIOS boot targets for embedded storage controllers. By default, all valid boot targets attached to the storage controller are available to the UEFI Boot Order list.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > Embedded Storage Boot Policy.
2. Select a storage controller.
3. Select a setting.
   - Boot All Targets—All valid boot targets attached to the storage controller are available to the UEFI Boot Order list.
   - Boot Limit to 24 Targets—A maximum of 24 boot targets attached to the storage controller are available to the UEFI Boot Order list.
   - Boot No Targets—No boot targets attached to the storage controller are available to the UEFI Boot Order list.
4. Save your setting.

Setting the PCIe storage boot policy

About this task

Prerequisite

Boot Mode is set to UEFI Mode.

Use the PCIe Storage Boot Policy option to select the UEFI BIOS boot targets for storage controllers in PCIe slots.

NOTE

This setting overrides the Fibre Channel/FCoE Scan Policy setting for Fibre Channel controllers in PCIe slots.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > PCIe Storage Boot Policy.
2. Select a storage controller.
3. Select a boot target.
4. Save your setting.

Changing the default Fibre Channel/FCoE scanning policy

About this task

Prerequisite

Boot Mode is set to UEFI Mode.

Use the Fibre Channel/FCoE Scan Policy option to change the default policy for scanning for valid FC/FCoE (or boot from SAN) boot targets. By default, each installed FC/FCoE adapter only scans targets that are preconfigured in the device settings. For Fibre Channel controllers in PCIe slots, this setting is overridden by the PCIe Storage Boot Policy setting.

NOTE

Supported in UEFI mode only.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > Fibre Channel/FCoE Scan Policy.
2. Select a setting.
   - Scan All Targets—Each installed FC/FCoE adapter scans all available targets.
   - Scan Configured Targets Only—Each installed FC/FCoE adapter only scans targets that are preconfigured in the device settings. This setting overrides any individual device settings configured in the device-specific setup.
3. Save your setting.

Enabling or disabling Embedded NVM Express Option ROM

About this task

Use the Embedded NVM Express Option ROM option to control how the NVM Express Option ROM is loaded.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > Embedded NVM Express Option ROM.

2. Select a setting.
   - Enabled—The system loads the NVM Express Option ROM provided by the system BIOS.
   - Disabled—The system loads the NVM Express Option ROM provided by the adapter.
3. Save your setting.

Decommissioning NVM Express drives

About this task

Use the following options to decommission NVM Express drives. The drives you select are securely erased during the next boot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > NVM Express Drive Decommission Option.
2. Select the drives you want to decommission.
3. Save your settings.

Configuring Intel® VMD Configuration Options

Prerequisites

Intel® CPU VMD Support is set to Enabled Individual CPU NVMe Root Ports .

About this task

Use Intel® VMD Configuration Options to enable or disable Intel CPU Volume Management Device Support for NVMe.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > Intel® NVMe > Intel® VMD Configuration Options.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Configuring Intel® VMD Direct Assign

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > Intel® NVMe > Intel® VMD Direct Assign.
2. Select a setting.

- Enable VMD Direct Assign for all VMD
- Disabled

3. Save your setting.

Configuring Intel® CPU VMD Support

About this task

Use the Intel® CPU VMD Support option to enable/disable Intel CPU Volume Management Device Support for NVMe.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > Intel® NVMe > Intel® CPU VMD Support.
2. Select a setting.
   - Enabled Individual CPU NVMe Root Ports
   - Enabled All CPU NVMe Root Ports
   - Disabled
3. Save your setting.

Configuring Intel® PCH VMD Support

About this task

Use the Intel® PCH VMD Support option to enable/disable Intel PCH Volume Management Device Support for NVMe.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > Intel® NVMe > Intel® PCH VMD Support.
2. Select a setting.
   - Enabled all PCH NVMe Root Ports
   - Disabled
3. Save your setting.

Configuring Intel® VROC Support

Prerequisites

- Intel® PCH VMD Support is set to Enabled all PCH NVMe Root Ports.
- Intel® CPU VMD Support is set to Enabled all CPU NVMe Root Ports.

About this task

Use the Intel® VROC Support option to select different types of VROC licenses.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Storage Options > NVM Express Options > Intel® NVMe > Intel® VROC Support.
2. Select a setting.
   - None
   - Raid1 Only
   - Premium
3. Save your setting.

Configuring SED drives for local and remote key management

About this task

The key management mode can be changed between local and remote key management. Encrypted Self-Encrypting Drives (SEDs) remain encrypted, but the encryption keys and the storage of those keys change, based on the key management mode selected.

Procedure

1. From the System Utilities screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Device Encryption Options**.
2. Change the Key Management setting to one of the following:
   - **Local**—Enables local key management. The encryption key is stored locally on the server.

     HPE TPM 2.0 must be installed to view and select this setting.
   - **Remote**—Enables remote key management. The encryption key is stored on a remote key server.

     HPE iLO must be enrolled in and connected to a key manager to view and select this setting.
3. Press the **F12** key to save and exit.
4. Reboot the server.

> **IMPORTANT**
>
> Key Management is not supported on HPE Gen11 servers using Ampere processors.

Changing Power and Performance Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options.

Subtopics

Setting the Power Regulator mode for AMD processors

About this task

Use the Power Regulator settings to help increase server efficiency and manage power consumption.

NOTE

Certain processors only support one power state and operate at their initialized frequency, regardless of the selected power regulator mode.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Power Regulator.

2. Select a setting.
   - Static High Performance Mode Mode—Processors run in the maximum power and performance state, regardless of the OS power management policy. This mode is useful in environments where performance is critical and power consumption is less important.
   - OS Control Mode—Processors run in their maximum power and performance state at all times, unless the OS enables a power management policy.
3. Save your setting.

Setting the Power Regulator mode for Intel/Ampere processors

About this task

Use Power Regulator settings to help increase server efficiency and manage power consumption.

> **NOTE**
> Certain processors only support one power state and operate at their initialized frequency, regardless of the selected power regulator mode.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Power Regulator.
2. Select a setting.
   - Dynamic Power Savings Mode—Automatically varies processor speed and power usage based on processor utilization. This mode uses a ROM-based algorithm to monitor processor activity. It can reduce overall power consumption with little or no impact to performance, and does not require OS support.
   - Static Low Power Mode—Reduces processor speed and power usage. Guarantees a lower maximum power usage for the system. This mode is useful in environments where power availability is constrained and it is critical to lower the maximum power use of the system.
   - Static High Performance Mode—Processors run in the maximum power and performance state, regardless of the OS power management policy. This mode is useful in environments where performance is critical and power consumption is less important.
   - OS Control Mode—Processors run in their maximum power and performance state at all times, unless the OS enables a power management policy.
3. Save your setting.

Setting the minimum processor idle power core C-State

About this task

Use the Minimum Processor Idle Power Core C-State option to select the lowest idle power (C-State) of the processor that the operating system uses. The higher the C-State, the lower the power usage of that idle state.

Prerequisite

Workload Profile is set to Custom.

NOTE

'C6 Without C1E State' allows the processor to operate in the C6 state with the C1E state disabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Core C-State .
2. Select a setting.
   - C6 State (default—lowest)
   - C1E State
   - C6 Without C1E State

     NOTE

     When this value is selected, the Optimized Power Mode (System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options) is forced to 'Disabled' on Gen11 E5 ProLiant and Synergy servers.
   - No C-states
3. Save your setting.

Setting the Minimum Processor Idle Power Package C-State

About this task

Use the Minimum Processor Idle Power Package C-State option to configure the lowest processor idle power state (C-State). The processor automatically transitions into package C-States based on the C-States in which cores on the processor have transitioned. The higher the package C-State, the lower the power usage of that idle package state.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Minimum Processor Idle Power Package C-State .
2. Select a setting.
   - Package C6 (retention) State (default—lowest)
   - Package C6 (non-retention) State
   - No Package State
3. Save your setting.

Configuring Intel(R) Turbo Boost Technology

About this task

Intel(R) Turbo Boost Technology enables the processor to transition to a higher frequency than the processor's rated speed if the processor

has available power and is within temperature specifications.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Intel(R) Turbo Boost Technology.
2. Select a setting.
   - Enabled
   - Disabled

     CAUTION

     Disabling this option reduces power usage, and also reduces system's maximum achievable performance under some workloads.
3. Save your setting.

Enabling or disabling AMD Data Fabric C-State

About this task

Use Data Fabric C-State Enable option to enable or disable the Data Fabric C-States.

NOTE

This option is available on servers with AMD processors.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Data Fabric C-State Enable.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Setting the Energy Performance Preference

About this task

Use Energy Performance Preference to enable or disable the Energy Performance Preference.
In this case, the processor starts off by default at a balanced profile, and changes the profile based on inputs provided over the OOB PECI interface.

Prerequisite

Power Regulator is set to OS Control Mode.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Energy Performance Preference.

2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Configuring AMD Core Performance Boost

About this task

AMD Core Performance Boost controls whether the processor transitions to a higher frequency than the processor's rated speed if the processor has available power and is within temperature specifications.

> **NOTE**
> This option is available on servers with AMD processors.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > AMD Core Performance Boost.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling AMD Fmax Boost Limit Control

About this task

AMD Fmax Boost Limit setting sets the maximum processor boost frequency.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > AMD Fmax Boost Limit Control.
2. Select a setting.
   - Auto—Allows the processor to run at the highest possible boost frequencies.
   - Manual—Allows you to configure a lower maximum boost frequency.
3. Save your setting.

Setting the Energy/Performance Bias

Prerequisites

Workload Profile is set to Custom.

About this task

Use the Energy/Performance Bias option to configure several processor subsystems to optimize the processor's performance and power usage.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Energy/Performance Bias.
2. Select a setting.
   - Maximum Performance—Provides the highest performance and lowest latency. Use this setting for environments that are not sensitive to power consumption.
   - Balanced Performance—Provides optimum power efficiency and is recommended for most environments.
   - Balanced Power—Provides optimum power efficiency based on server utilization.
   - Power Savings Mode—Provides power savings for environments that are power sensitive and can accept reduced performance.
3. Save your setting.

Setting the AMD Infinity Fabric Performance State

About this task

Use the Infinity Fabric Performance State option for customizing the performance state (P-state) of the Infinity Fabric when Infinity Fabric Power Performance is disabled.

NOTE

This option appears only when Infinity Fabric Power Management is disabled.

See the related topic of this chapter for more information.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Infinity Fabric Performance State.
2. Select a setting.
   - Auto
   - P0
   - P1
   - P2
   - P3
3. Save your setting.

More information

- Enabling or disabling Infinity Fabric Power Management

Enabling or disabling collaborative power control

Enabling or disabling collaborative power control

About this task

For operating systems that support the Processor Clocking Control (PCC) interface, enabling Collaborative Power Control configures the operating system to request processor frequency changes, even when the Power Regulator option is set to Dynamic Power Savings Mode on the server. For operating systems that do not support the PCC Interface, or when the Power Regulator mode is not configured for Dynamic Power Savings Mode, this option has no impact on system operation.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Collaborative Power Control.
2. Select a setting.
   - Enabled—The operating system requests processor frequency changes.
   - Disabled—The operating system does not request processor frequency changes.
3. Save your setting.

> **NOTE**
>
> The collaborative power control option is only supported in ProLiant Gen10 servers.

Configuring AMD XGMI Force Link Width

About this task

XGMI Force Link Width setting forces the XGMI link width to a value set by the user.

> **NOTE**
>
> This setting is functional on systems with two CPUs.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > XGMI Force Link Width.
2. Select a setting.
   - Auto— Allows for the system to dynamically change XGMI link width as necessary.
   - x2— Forces the XGMI link width to x2.
   - x8— Forces the XGMI link width to x8.
   - x16— Forces the XGMI link width to x16.
3. Save your setting.

Configuring AMD XGMI Max Link Width

About this task

XGMI Max Link Width setting sets the maximum XGMI link width to a value set by the user.

> **NOTE**
> This setting is functional on systems with two CPUs.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > XGMI Max Link Width.
2. Select a setting.
   - Auto— Allows for the system to dynamically change XGMI Max Link Width as necessary.
   - x2— Caps the XGMI link width to a maximum of x2.
   - x8— Caps the XGMI link width to a maximum of x8.
   - x16— Caps the XGMI link width to a maximum of x16.
3. Save your setting.

Configuring AMD xGMI Link Speed

About this task

Configure **AMD xGMI Link Speed** between two processors. Auto will use a platform-defined setting. Other options will force the speed to user selected value.

> **NOTE**
> This setting is functional on systems with two CPUs.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > AMD xGMI Link Speed.
2. Select a setting.
   - **For 4th Gen EPYC processors**
     - **Auto**— Auto will use the platform-defined setting.
     - **16 Gbps**— Caps the xGMI link speed to 16 Gbps.
     - **18 Gbps**— Caps the xGMI link speed to 18 Gbps.
     - **25 Gbps**— Caps the xGMI link speed to 25 Gbps.
     - **32 Gbps**— Caps the xGMI link speed to 32 Gbps.
   - **For 5th Gen EPYC processors**
     - **Auto**— Auto will use the platform-defined setting.
     - **20 Gbps**— Caps the xGMI link speed to 20 Gbps.
     - **25 Gbps**— Caps the xGMI link speed to 25 Gbps.
     - **32 Gbps**— Caps the xGMI link speed to 32 Gbps.
3. Save your setting.

Configuring AMD ACPI CST C2 Latency

About this task

Use the **ACPI CST C2 Latency** option to configure C2 latency value for the Linux kernel.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > ACPI CST C2 Latency.
2. Select a setting.
   - **For 4th Gen EPYC processors**
     - 800 microsecond: For Linux kernel versions, before 6.0.
     - 18 microsecond: For Linux kernel version, 6.0 or later.
   - **For 5th Gen EPYC processors**
     - 100 microsecond: For Linux kernel versions, before 6.0.
     - 18 microsecond: For Linux kernel version, 6.0 or later.
3. Save your setting.

Setting Intel DMI Link Frequency

About this task

Use the Intel DMI Link Frequency option to force the link speed between the processor and south bridge to run at slower speeds. Doing so can reduce power consumption, but can also impact system performance.

NOTE

You can configure this option on systems with two or more CPUs.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Intel DMI Link Frequency.
2. Select a setting.
   - Auto
   - Gen 1 Speed
   - Gen 2 Speed
   - Gen 3 Speed
3. Save your setting.

Configuring AMD NBIO LCLK DPM Level

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > I/O Options > NBIO LCLK DPM Level.
2. Select a value:
   - Auto
   - Static Low
   - Static High

   > **NOTE**
   >
   > Configuring the NBIO to Static High may improve performance on PCIe devices on the NBIO but will reduce performance in other portions of the processor. This setting should only be used after a review of PCIe device requirements
3. Save your setting.

Setting NUMA Group Size Optimization

About this task

Use the NUMA Group Size Optimization option to configure how the system ROM reports the number of logical processors in a NUMA (Non-Uniform Memory Access) node. The resulting information helps the operating system group processors for application use.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > NUMA Group Size Optimization.
2. Select a setting.
   - Clustered—Optimizes groups along NUMA boundaries, providing better performance.
   - Flat—Enables applications that are not optimized to take advantage of processors spanning multiple groups to utilize more logical processors.
3. Save your setting.

Configuring Uncore Frequency Scaling

About this task

Use the Uncore Frequency Scaling option to control the frequency scaling of the processor's internal buses.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Uncore Frequency Scaling.
2. Select a setting.
   - Auto—Enables the processor to dynamically change frequencies based on workload.
   - Custom—Enables tuning for latency or power consumption by providing two options:

- Maximum Uncore Frequency: Specify a specific maximum value.
- Minimum Uncore Frequency: Specify a specific minimum value.

3. Save your setting.

Configuring Uncore Frequency RAPL

About this task

Use the Uncore Frequency RAPL option to enable the Running Average Power Limit (RAPL) balancer.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Uncore Frequency RAPL.
2. Select a setting.
   - Enabled (Default)
   - Disabled
3. Save your setting.

Disabling Dynamic Loadline (DLL) Switch

About this task

Dynamic Loadline switch controls MSR 0x1FC[Bit33]. Enabling or disabling the switch affects the power and performance by condition. DLL switches between EPB modes depending on the P-state behavior.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Disable Dynamic Loadline Switch.
2. Select a setting.
   - Not Disable DLL Switch
   - Disable DLL Switch
3. Save your setting.

Enabling or disabling Sub-NUMA Clustering

About this task

Sub-NUMA Clustering divides the cores, cache, and memory of the processor into multiple NUMA domains. Enabling this option can increase performance for workloads that are NUMA aware and optimized.

NOTE

Up to 1 GB of system memory might become unavailable when Sub-NUMA Clustering is enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Sub-NUMA Clustering.
2. Select a setting.
   - Disabled
   - SNC2
   - SNC4
3. Save your setting.

Enabling or disabling the Energy Efficient Turbo option

About this task

Use the Energy Efficient Turbo option to control whether the processor uses an energy-efficiency based policy.

Prerequisite

Intel(R) Turbo Boost Technology is enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Energy Efficient Turbo.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Setting the LLC Dead Line Allocation

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > LLC Dead Line Allocation.
2. Select one of the following:
   - Enable—Opportunistically fill dead lines in LLC.
   - Disable—Never fill dead lines in LLC.
3. Save your setting.

Setting the Stale A to S

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Stale A to S.
2. Select one of the following:
   - Auto
   - Enable—Enable Stale A to S directory optimization.
   - Disable—Disable Stale A to S directory optimization.
3. Save your setting.

Disabling Processor Prefetcher Options

About this task

By default, Processor Prefetcher Options are enabled to provide optimal performance for most environments. In some cases, disabling these options can improve performance.

> **IMPORTANT**
> To verify that you can improve performance in your environment, perform application bench marking before you disable a processor prefetcher option.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Processor Prefetcher Options.
2. Select a setting.
   - HW Prefetcher
   - Adjacent Sector Prefetcher
   - DCU Stream Prefetcher
   - DCU IP Prefetcher
   - LLC Prefetch
3. Select Disabled.
4. Save your changes.

Enabling or disabling I/O Options

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > I/O Options.

2. Select an option.
3. Select Enabled or Disabled.
4. Save your changes.

Subtopics

Enabling the ACPI SLIT options

About this task

Enables or disables the Advanced Configuration and Power Interface System Locality Information Table (ACPI SLIT). ACPI SLIT defines the relative access times between processors, memory subsystems, and I/O subsystems. Operating systems that support the SLIT can use this information to improve performance by allocating resources and workloads more efficiently.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > I/O Options.
2. For the option ACPI SLIT, select one of the following:
   - Enabled
   - Disabled
3. Save your changes.

Enabling Intel NIC DMA Channels options

About this task

Enables or disables DMA acceleration on Intel NICs. If your server does not have Intel NICs, leave this setting disabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > I/O Options.
2. For the option Intel NIC DMA Channels, select one of the following:
   - Enabled
   - Disabled
3. Save your changes.

Enabling Memory Proximity Reporting for I/O

About this task

Enables or disables whether the system ROM reports the proximity relationship between I/O devices and system memory to the operating system. Most operating systems can use this information to efficiently assign memory resources for devices, such as network controllers and storage devices.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > I/O Options.
2. For the option Memory Proximity Reporting for I/O, select one of the following:
   - Enabled
   - Disabled

   NOTE

   Certain I/O devices might not be able to take advantage of I/O handling benefits if their OS drivers are not properly optimized to support this feature. For more information, see your operating system and I/O device documentation.
3. Save your changes.

Configuring Intel UPI Options

About this task

Select Intel UPI Options to change settings for ACPI SLIT, Intel NIC DMA, Memory Proximity Reporting for I/O, and I/O Non-posted Prefetching.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Intel UPI Options.
2. Configure the options:
   - Intel UPI Link Enablement -- Configures the UPI topology to use fewer links between processors, when available. Changing from default can reduce UPI bandwidth performance in exchange for less power consumption.
     - Auto
     - Single Link Operation
   - OSB Local/Remote Read -- Use this option to configure Intel Opportunistic Snoop Broadcast(OSB) Local/Remote Read function. This feature will opportunistically enable snoop broadcast across CPU sockets if UPI has extra bandwidth.
     - Disabled- Disables OSB Local/Remote Read settings.
     - Auto- Automatically enables OSB Local/Remote Read settings based on silicon compatibility.

     NOTE

     For systems with 4-processor-sockets (whether all four are populated or not), it is recommended that OSB Local/Remote Read be Disabled, which is the default value for 4-socket HPE ProLiant servers. This will provide optimal performance with most workloads. It is recommended that you only configure this option to Auto if you perform benchmarking with your workload or benchmarks representative of your workload and a performance increase is observed.
   - Intel UPI Link Power Management -- Places the Quick Path Interconnect (UPI) links into a low power state when the links are not

being used. This lowers power usage with minimum effect on performance.

- Enabled (default)
- Disabled

> **IMPORTANT**
>
> You can only configure this option if two or more CPUs are present and the Workload Profile is set to Custom.

- Intel UPI Link Frequency-- Sets the UPI Link Frequency to a lower speed. Running at a lower frequency can reduce power consumption but it can also affect system performance.
  - Auto
  - Min UPI Speed

> **IMPORTANT**
>
> You can only configure this option if two or more CPUs are present and the Workload Profile is set to Custom.

- UPI Prefetcher-- Use this option to disable the processor UPI Prefetch feature. In come cases, disabling this option can improve performance. Typically, enabling this provides better performance.
  - Enabled
  - Disabled

> **TIP**
>
> Only disable this option after performing application benchmarking to verify improved performance in the environment. This option must be enabled when Sub-Numa clustering (SNC) is enabled.

- Direct To UPI (D2K)
  - Auto
  - Enabled
  - Disabled

3. Save your changes.

Configuring DRAM RAPL Options

Subtopics

Enabling or disabling DRAM RAPL Reporting Support

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > DRAM RAPL Options > DRAM RAPL Reporting Support.
2. Select a value:
   - Enabled-- Enables DRAM power reporting.
   - Disabled-- Disables DRAM power reporting.
3. Save your changes.

Configuring DRAM RAPL Limiting Support

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > DRAM RAPL Options > DRAM RAPL Limiting Support.
2. Select a value:
   - Disabled-- Disables DRAM power limiting so that neither System Firmware nor Operating system software is able to limit the DRAM power.
   - OS Control Mode-- Enables DRAM power limiting so that only the Operating system software is able to programme the DRAM power limit.
   - BIOS Control Mode-- Enables DRAM power limiting so that only the system firmware is able to programme the DRAM power limit during POST.

   TIP

   DRAM RAPL values are applied to an entire processor's memory. This value limits the total power from all the memory attached at the processor socket level.
3. Save your changes.

Configuring DRAM RAPL wattage value

About this task

DRAM RAPL wattage value is a per socket DRAM RAPL value applicable for all populated sockets in the system. Modify this value in milliwatts, as instructed by qualified personnel.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > DRAM RAPL Options > DRAM RAPL wattage value.
2. Enter a value in milliwatts in consultation with your personnel.
3. Save your changes.

Enabling or disabling I/O Non-posted Prefecting

About this task

Use the I/O Non-posted Prefecting option to enable or disable Non-posted Prefecting for I/O.
Disabling non-posted prefetching for I/O can significantly improve performance for a small set of configurations that require a balanced mix of read/write I/O traffic. For example, configurations that include InfiniBand or multiple x16 devices that utilize max bandwidth of the PCI-e bus.

NOTE
Disabling this feature has a slight impact on 100% I/O read bandwidth.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > I/O Non-posted Prefecting.
2. Select a setting.
   - Enable
   - Disable
3. Save your setting.

Configuring Advanced Performance Tuning Options

About this task

Use Advanced Performance Tuning to control frequency changes that cause jitters and affect latency. You can manage Jitter Control manually or automatically. You can also specify a frequency to use, regardless of whether the processor frequency changes. For more information about Jitter Control, see HPE Gen11 Servers Intelligent System Tuning.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options.
2. Configure settings.
   - Enhanced Processor Performance Profile: Use this option to enable or disable this feature. When enabled, this option adjusts the processor settings to a more aggressive setting that can results in increased performance, but might results in higher power consumption.
   - Intel(R) AVX P1: This option overrides the default CPU policy for SSE, AVX, and AVX-512 deterministic frequencies. This setting results in lowering the deterministic operational frequency. Disabling Turbo Mode enhances the deterministic behavior, but results in a lower operational frequency. The options are Normal, Level 1, Level 2.
3. Save your changes.

Subtopics

Setting Direct to UPI Options

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options > Direct to UPI.
2. Select an option.
   - Enabled—Provides a performance benefit in multiprocessor configured systems that rely on the UPI bus for remote memory or I/O accesses.
   - Disabled
3. Save your changes.

Configuring IO Direct Cache

About this task

Use the IO Direct Cache option to configure PCI Peer to Peer Serialization.

Some configurations, such as systems populated with multiple GPUs on a processor socket, may see increased performance when this feature is enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options > IO Direct Cache.
2. Select a setting.
   - Auto
   - Disabled—Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores).
   - Enable for Remote InvItoM Hybrid Push
   - InvItoM AllocFlow
   - InvItoM Hybrid AllocFlow
   - Enable for Remote InvItoM and Remote WViLF
3. Save your setting.

Configuring Dead Block Predictor

About this task

Use the Dead Block Predictor option to configure the DBP-F processor performance option. When enabled, this feature can benefit multi-threaded workloads based on improved prediction of cache line evictions.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options

> Advanced Performance Tuning Options > Dead Block Predictor.

2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Configuring Snoop Response Hold-Off

About this task

Snoop Response Hold Off tunes the snoop response time of the I/O subsystem in the rare case that a workload's performance Is hindered by the recommended default setting.

Increasing the value of this setting exponentially increases the amount of time that a snoop request can be held off.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options > Snoop Response Hold Off.
2. Select a value [0-15] in the drop-down.
3. Save your setting.

Intel (R) AVX License Pre-Grant Override

About this task

Use the Intel (R) AVX License Pre-Grant Override option to control AVX ICCP pre_grant level override. When Enabled, this option enables the pre_grant license level selection based on workload with the AVX ICCP Pre_Grant Level option.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options > Intel (R) AVX License Pre-Grant Override .
2. Select a setting:
   - Enabled
   - Disabled
3. Save your settings.

Intel (R) AVX ICCP Pre-Grant Level

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options > Intel (R) AVX ICCP Pre-Grant Level .

2. Select a setting:
   - 128 Heavy
   - 256 Light
   - 256 Heavy
   - 512 Light
   - 512 Heavy
3. Save your settings.

Configuring Snoop Response Hold Off for IOAT Stack

About this task

Snoop Response Hold Off for IOAT Stack tunes the snoop response time of the I/O subsystem in the rare case that a workload's performance Is hindered by the recommended default setting.

Increasing the value of this setting exponentially increases the amount of time that a snoop request can be held off.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Performance Tuning Options > Snoop Response Hold Off for IOAT Stack.
2. Select a value [0-15] in the drop-down.
3. Save your setting.

Performance management

Selected HPE Gen10 and later servers support the following server performance management and tuning features:

- **Workload matching**—Use preconfigured server profiles to maximize application performance.
- **Jitter smoothing**—Use the Processor Jitter Control Mode setting to level and balance frequency fluctuation (jitter) resulting in lower latency.
- Performance monitoring—View performance data collected from supported sensors on servers with Innovation Engine support. You can configure alerts based on the collected data.
- Workload advisor—View selected server workload characteristics. You can view and configure recommended performance tuning settings based on the monitored data.
- **Core boosting**—Enable this feature to produce higher performance across more active processor cores.

  This feature is supported on Gen10 servers only. It is not supported on Gen10 Plus or later servers.

If you reset iLO to the factory default settings, all performance management settings and data are deleted.

When you use the iLO backup and restore feature, the performance management settings are retained. The collected performance data is not backed up or restored.

Subtopics

Performance management feature requirements

Table 1. Performance Feature by HPE Server Generation

HPE Server	Workload matching	Jitter smoothing	Core boosting	Performance monitoring	Workload advisor
HPE Gen10 Servers using Intel Scalable Performance Processors	✓	✓	✓	✓	✓
HPE Gen10 servers using AMD EPYC Processors	✓				
HPE Gen10 Plus Servers using Intel Scalable Performance Processors	✓			✓	✓
HPE Gen10 Plus Servers using AMD EPYC Processors	✓				
HPE Gen11 Servers using Intel Scalable Performance Processors	✓			✓	✓
HPE Gen11 Servers using AMD EPYC Processors	✓				

Table 2. iLO Advanced License Requirement for Performance Features

Requirement	Workload matching	Jitter smoothing	Core boosting	Performance monitoring	Workload advisor
iLO Advanced license		✓	✓	✓	✓

Table 3. HPE Gen10 Server Minimum Firmware Requirements for Performance Features

Firmware	Workload matching	Jitter smoothing	Core boosting	Performance monitoring	Workload advisor
Minimum System ROM	1.00	1.00 for static 1.20 for Dynamic 1.40 for Optimizations	1.20	2.00	2.00
Minimum iLO firmware	N/A	1.15 iLO RESTful API 1.30 iLO Web interface	1.15 iLO RESTful API 1.30 iLO Web interface	1.40 iLO RESTful API 1.40 iLO Web interface	1.40 iLO RESTful API 1.40 iLO Web interface
Minimum HPE Innovation Engine Firmware [1]	N/A	1.2.4	1.2.4	2.0.11	2.0.11

[1] The iLO web interface Performance page is not available on servers without Innovation Engine support. To verify Innovation Engine support, look for the Innovation Engine firmware on the Installed Firmware page.

NOTE

There are no minimum firmware revisions for HPE Gen10 Plus and Gen11 Servers as all supported performance features are supported by the original revision of the firmware which is shipped with those platforms.

Configuring Advanced Power Options

About this task

Use the Advanced Power Options menu to enable advanced power features such as channel interleaving and collaborative power control. You can also set the UPI Link Frequency to a lower speed and set the Processor Idle Power State.

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options.

Subtopics

Configuring Intel HardwarePM Interrupt

About this task

HardwarePM Interrupt is a mechanism within the hardware performance monitoring systems that allows for the triggering of interrupts based on specific performance events or thresholds.

NOTE

This option is only selective when Collaborative Power Control is Enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options > HardwarePM Interrupt.
2. Select a setting:
   - Enabled
   - Disabled (default)
3. Save your setting.

Setting the redundant power supply mode

About this task

Use the Redundant Power Supply Mode option to set how the system handles redundant power supply configurations. All High Efficiency Mode settings provide the most power efficient operation when you are using redundant power supplies by keeping half of the power standby mode at lower power usage levels. Balanced Mode shares the power delivery equally between all installed power supplies.

Prerequisite

Workload Profile is set to Custom.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options

> Advanced Power Options > Redundant Power Supply Mode.

2. Select a setting.
   - Balanced Mode—The system shares the power delivery equally between all installed power supplies.
   - High Efficiency Mode (Auto)—The system selects between the odd or even power supply based on a semirandom distribution within a group of systems.
   - High Efficiency Mode (Odd Supply Standby)—The system places the odd power supply in standby.
   - High Efficiency Mode (Even Supply Standby)—The system places the even power supply in standby.
3. Save your setting.

Configuring Intel Processor PMAX Power Adjustment

About this task

Use the Processor PMAX Power Adjustment option to control the Processor Power Adjustment (PMAX) setting. When configured, this option changes the peak maximum power detection (PMAX) circuit of the processor to begin throttling earlier than the default setting.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options > Processor PMAX Power Adjustment.
2. Enter a value.
3. Save your setting.

Enabling or disabling Infinity Fabric Power Management

About this task

When Infinity Fabric Power Management is enabled, the EPYC processor dynamically varies the clock frequency of the Infinity fabric based on activity levels.
For NUMA optimized workloads, allowing the Infinity fabric to run slower may lead to an increased overall performance due to an increase in the CPU boost. Disabling this feature may be necessary for latency sensitive workloads.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options > Advanced Power Options.
2. For Infinity Fabric Power Management, select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Configuring the Package Power Limit Control Mode

About this task

Package Power Limit Control Mode is a package power limit value per processor that is applicable for all populated processors in the system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power and Performance Options.
2. For Package Power Limit Control Mode , select a setting.
   - Auto—Uses the default processor value.
   - Manual—Allows you to modify the Package Power Limit Value in watts. Do so as instructed by the qualified personnel.
3. Save your setting.

Enabling or disabling APEI Support

About this task

Use APEI support to enable or disable ACPI Platform Error Interface support.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power Options.
2. Select a setting:
   - Enable (default)
   - Disable
3. Save your setting.

Enabling or disabling CPPC Support

About this task

Use CPPC support to enable or disable Collaborative Processor Performance Control The allows the OS to manage the performance of a logical processor on a contiguous and abstract performance scale. There are four CPPC performance states:

- Highest performance
- Nominal performance
- Lowest, Nonlinear performance
- Lowest performance

For Altra Max, the nominal performance and highest performance are identical.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power Options .
2. Select a setting:
   - Enable (default)

- Disable

3. Save your setting.

Enabling or disabling LPI Support

About this task

Use LPI support to enable or disable Lower Power Idle. This allows the OS to selectively turn cores on and off and manage core idle states based on processor workloads.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power Options.
2. Select a setting:
   - Enable (default)
   - Disable
3. Save your setting.

Enabling or disabling Ampere Max Performance

About this task

Use Ampere Max Performance to enable or disable max performance.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Power Options.
2. Select a setting:
   - Enable (default)
   - Disable
3. Save your setting.

Changing Embedded UEFI Shell Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell Options.

Subtopics

Enabling or disabling the Embedded UEFI Shell

About this task

Use the Embedded UEFI Shell option to enable or disable the pre-boot command-line environment for scripting and running UEFI applications, including UEFI boot loaders. The Embedded UEFI Shell also provides CLI-based commands you can use to obtain system information, and to configure and update the system BIOS. When enabled, and Add Embedded UEFI Shell to Boot Order is enabled, the Embedded UEFI Shell is added to the UEFI Boot Order list.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > Embedded UEFI Shell.
2. Select a setting.
   - Enabled—Enables you to launch the Embedded UEFI Shell from the pre-boot environment and add it to the UEFI Boot Order list.
   - Disabled—The Embedded UEFI Shell is not available in the pre-boot environment and you cannot add it to the UEFI Boot Order list.
3. Save your setting.

Adding the Embedded UEFI Shell to the UEFI Boot Order list

About this task

Prerequisite

Boot Mode is set to UEFI Mode.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > Add Embedded UEFI Shell to Boot Order.
2. Select a setting.
   - Enabled—Adds the embedded UEFI Shell to the boot order list on the next reboot.
   - Disabled—The embedded UEFI Shell is not added to the boot order list.
3. Save your setting.

Enabling or disabling automatic execution of the Embedded UEFI Shell startup script

Prerequisites

- Boot Mode is set to UEFI Mode.
- Embedded UEFI Shell is enabled.

About this task

Use the UEFI Shell Script Auto-Start option to enable or disable automatic execution of the Embedded UEFI Shell startup script during Shell startup.

- You can use the startup script to create a RAM disk, download files from the network, collect data, upload results back to network, and then boot to the OS without rebooting the system.
- You can store the script file on local media, or access it from a network location.
- Name the script file `startup.nsh` and place it on local media or a network location accessible to the server.
- When auto-start is enabled, and the Shell Auto-Start Script Location option is set to Auto, the Shell looks for the script file in a network location first, followed by any locally attached FAT16, or FAT32-formatted media.
- It is recommended that you have only one `startup.nsh` file on one file system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > UEFI Shell Script Auto-Start.
2. Select a setting.
   - Enabled—The UEFI Shell startup script executes during Shell startup.
   - Disabled—The UEFI Shell startup script does not execute during Shell startup.
3. Save your setting.

Enabling or disabling Shell script verification

Prerequisites

- Boot Mode is set to UEFI Mode.
- Embedded UEFI Shell is enabled.
- Secure Boot is enabled.
- Shell scripts are enrolled in the Secure Boot database.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > Shell Script Verification.
2. Select a setting.
   - Enabled—Enables Shell script verification.
   - Disabled—(Default) Does not enable Shell script verification.
3. Save your setting.

Setting the Embedded UEFI Shell startup script location

Prerequisites

- Embedded UEFI Shell is enabled.

- UEFI Shell Script Auto-Start is enabled.

About this task

Use the Shell Auto-Start Script Location option to select the location of the Embedded UEFI Shell startup script. When UEFI Shell Script Auto-Start is enabled, this setting specifies where the Shell looks for the `startup.nsh` file.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > Shell Auto-Start Script Location.
2. Select a setting.
   - Auto—The Shell attempts to retrieve the startup script from the network location first, followed by locally attached media.
   - File Systems on Attached Media —The Shell looks for the `startup.nsh` script file on a UEFI-accessible local file system, such as a FAT32 partition on a USB disk or HDD.
   - Network Location—The Shell looks for a `.nsh` script at an HTTP/HTTPS or FTP location accessible to the system.
3. Save your setting.

Enabling or disabling discovery of the Shell auto-start script using DHCP

Prerequisites

- Embedded UEFI Shell is enabled.
- UEFI Shell Script Auto-Start is enabled.
- HTTP Support policy is enabled, and the URL provided by the DHCP server matches the HTTP Support policy setting.
- Shell Auto-Start Script Location is set to Network Location or Auto.
- The DHCP server is configured to provide HTTP/HTTPS or FTP URLs.
- The DHCP server is configured to respond to the `User Class` option set to `UEFIShell`. When using DHCP over IPv4, the User Class option is Option 77, and Option 15 when using DHCP over IPv6.

About this task

Use the Discover Shell Auto-Start using DHCP option to let the Shell discover the startup script URL using DHCP. When enabled, the Shell sends DHCP requests with the DHCP `User Class` option set to the string `UEFIShell`.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > Discover Shell Auto-Start using DHCP.
2. Select a setting.
   - Enabled—The Shell uses DHCP to discover the startup script URL.
   - Disabled—The Shell does not send DHCP requests to discover the startup script URL.
3. Save your setting.

Setting the network location for the Shell auto-start script

Prerequisites

- Embedded UEFI Shell is enabled.
- Shell Auto-Start Script Location is set to Network Location or Auto.
- Discover Shell Auto-Start Script using DHCP is disabled.
- When specifying and HTTPS URL, the TLS certificate of the HTTPS server is configured using Server Security > TLS (HTTPS) Options.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Embedded UEFI Shell > Network Location for Shell Script-Auto Start.
2. Enter the network location of the `.nsh` file. Valid values are:
   - An HTTP/HTTPS URL for either an IPv4 or IPv6 server address or host name.
   - An FTP URL for either an IPv4 or IPv6 server address or host name.

     Examples:

     - `http://192.168.0.1/file/file.nsh`
     - `http://example.com/file/file.nsh`
     - `https://example.com/file/file.nsh`
     - `http://[1234::1000]/file.nsh`
3. Save your setting.

Changing Server Security settings

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security.

Subtopics

Configuring Trusted Platform Module (TPM) options
Configuring Intel Security Options

Server Security options

- Set Power On Password
- Set Admin Password
- Secure Boot Settings
- TLS (HTTPS) Options
- Trusted Platform Module options
- Intel (R) TXT Support
- One-Time Boot Menu (F11 Prompt)
- Backup ROM Image Authentication

Configuring Intel SGX control options

About this task

Use this screen to configure Intel SGX control options.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel Security Options.
2. Configure the following options:
   - Intel(R) Software Guard Extensions (SGX): Enable or disable Software Guard Extensions (SGX).
   - PRMRR Size: Select the size of the PRMRR.
   - Select Owner EPOCH input type: There are three Owner EPOCH modes: no change in Owner EPOCHs, change to new random Owner EPOCHs, and manually enter new Owner EPOCHs. Modifying the Owner EPOCHs will cause all persistent data protected by Intel(R) Software Guard Extensions to be lost.

     CAUTION

     All persistent data protected by Intel(R) Software Guard Extensions Technology will be lost if the Owner EPOCH value is changed.

   - Software Guard Extensions Epoch: Software Guard Extensions 128-bit Epoch hexadecimal value.
   - SGX Launch Control Policy : Software Guard Extensions (SGX) Launch Control Policy. Options are:
     - Intel Locked: Select the Intel Launch Enclave.
     - Unlocked: Enable OS/VMM configuration of Launch Enclave.
     - Locked: Allow owner to configure Launch Enclave.
   - SGX LE Public Key Hash 0: Bytes 0 - 7 of Software Guard Extensions (SGX) Launch Enclave Public Key Hash
   - SGX LE Public Key Hash 1: Byte 8 - 15 of Software Guard Extensions (SGX) Launch Enclave Public Key Hash

- SGX LE Public Key Hash 2: Byte 16 - 23 of Software Guard Extensions (SGX) Launch Enclave Public Key Hash
- SGX LE Public Key Hash 3: Byte 24 - 31 of Software Guard Extensions (SGX) Launch Enclave Public Key Hash

3. Save your options.

Enabling or disabling SGX Factory Reset

Prerequisites

Make sure that:

- You have enabled Total Memory Encryption (TME).
- Your system configuration is not a one-channel memory configuration.

About this task

Enabling SGX Factory Reset performs SGX Factory Reset, and deletes all registration data on reboot. This action forces Initial Platform Establishment flow.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel Security Options > SGX Factory Reset.
2. Select a setting.
   - Enabled
   - Disabled (default)
3. Save your changes.

Setting the power-on password

About this task

Use the Set Power On Password option to set a password for accessing the server during the boot process. When you are powering on the server, a prompt appears where you enter the password to continue. To disable or clear the password, enter the password followed by a / (slash) when prompted to enter the password.

NOTE

In the event of an Automatic Server Recovery (ASR) reboot, the power-on password is bypassed and the server boots normally.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Set Power On Password.
2. Enter your password.

   A password can be:

   - 31 characters maximum
   - Any combination of numbers, letters, and special characters

3. Confirm the password, and then press Enter.

   A message appears confirming that the password is set.

4. Save your changes.
5. Reboot the server.

Allowing login with iLO accounts

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Allow login with iLO accounts.
2. To allow users to login with an iLO account with the CONFIGURE_BIOS privilege, select Allow login with iLO accounts.
3. Save your changes.

Setting an administrator password

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Set Admin Password.
2. Enter the password.

   A password can be:

   - 31 characters maximum
   - Any combination of numbers, letters, and special characters

3. Confirm the password, and then press Enter.

   A message appears confirming that the password is set.

4. Save your changes.
5. Reboot the server.

Secure Boot

Secure Boot is a server security feature that is implemented in the BIOS and does not require special hardware. Secure Boot ensures that each component launched during the boot process is digitally signed and that the signature is validated against a set of trusted certificates embedded in the UEFI BIOS. Secure Boot validates the software identity of the following components in the boot process:

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Preboot UEFI Shell applications
- OS UEFI boot loaders

When Secure Boot is enabled:

- Firmware components and operating systems with boot loaders must have an appropriate digital signature to execute during the boot process.
- Operating systems must support Secure Boot and have an EFI boot loader signed with one of the authorized keys to boot. For more information about supported operating systems, see **https://www.hpe.com/servers/ossupport**.

You can customize the certificates embedded in the UEFI BIOS by adding or removing your own certificates, either from a management console directly attached to the server, or by remotely connecting to the server using the iLO Remote Console.

You can configure Secure Boot:

- Using the System Utilities options described in the following sections.
- Using the iLO RESTful API to clear and restore certificates. For more information, see the Hewlett Packard Enterprise website (**https://www.hpe.com/info/redfish**).
- Using the `secboot` command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Enabling or disabling Secure Boot

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Attempt Secure Boot.
2. Select a setting.
   - Enabled—Enables Secure Boot.
   - Disabled—Disables Secure Boot.
3. Save your changes.
4. Reboot the server.

Configuring server lock settings

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Server Configuration Lock Settings.

   The Server Configuration Lock State status appears on the screen.
2. You can change the following options:
   - Server Configuration Lock Challenge required : Select Enabled or Disabled.
   - Prepare system for Transport: Select Enabled or Disabled.
   - Halt on Server Configuration Lock failure detection : Select Enabled or Disabled.
3. Save the settings.

IMPORTANT

Server Configuration Lock Settings option is not supported on HPE Gen11 servers using Ampere processors.

Subtopics

Setting up Server Configuration Lock

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Server Configuration Lock Settings > Setup Server Configuration Lock .
2. Select the following:
   - Exclude system board.
   - Exclude DIMMs.
   - Exclude CPUs.
   - Exclude PCIe slots.
   - Exclude security configuration.
   - Exclude system fimware revisions.
3. To create a digital fingerprint, click Generate Server Configuration Lock Digital Fingerprint .
4. Save the settings.

IMPORTANT

The option to Setup Server Configuration Lock is not available on HPE Gen11 servers using Ampere processors.

Advanced Secure Boot Options

- PK - Platform Key—Establishes a trust relationship between the platform owner and the platform firmware.
- KEK - Key Exchange Key—Protects the signature database from unauthorized modifications. No changes can be made to the signature database without the private portion of this key.
- DB - Allowed Signatures Database—Maintains a secure boot allowed signature database of signatures that are authorized to run on the platform.
- DBX - Forbidden Signatures Database—Maintains a secure boot blacklist signature database of signatures that are not authorized to run on the platform
- DBT - Timestamp Signatures Database—Maintains signatures of codes in the timestamp signatures database.
- Delete all keys
- Export all keys

- Reset all keys to platform defaults

> **NOTE**
>
> Changing the default security certificates can cause the system to fail booting from some devices. It can also cause the system to fail launching certain system software such as Intelligent Provisioning.

Subtopics

Viewing Advanced Secure Boot Options settings

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select the View entry for the exchange key or signatures database option.
4. Select the entry for the option you want to view.

Example: Viewing HPE UEFI Secure Boot 2016 PK Key details

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > PK - Platform Key > View PK entry > HPE UEFI Secure Boot 2016 PK Key .

Enrolling a Secure Boot certificate key or database signature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select Enroll <*option name*>.
4. Select Enroll <*option name*> using file.

   The File Explorer screen shows attached media devices.
5. Select the attached media device where the certificate file is located, and then press Enter.
6. Continue selecting the menu path for the certificate file. Press Enter after each selection.
7. Optional: Select a Signature Owner GUID.
8. Optional: If you selected Other for the signature owner GUID, enter a Signature GUID.

Use the following format (36 characters): `11111111-2222-3333-4444-1234567890ab`

- For Hewlett Packard Enterprise certificates, enter: `F5A96B31-DBA0-4faa-A42A-7A0C9832768E`
- For Microsoft certificates, enter: `77fa9abd-0359-4d32-bd60-28f4e78f784b`
- For SUSE certificates, enter: `2879c886-57ee-45cc-b126-f92f24f906b9`

9. Select Commit changes and exit.

Example: Enrolling a KEK entry

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > KEK - Key Exchange Key > Enroll KEK entry.
2. Select Enroll KEK using file.
3. Select the location of the certificate file from an attached media device.
4. Optional: Select a Signature Owner GUID.
5. Optional: If you selected Other for the signature owner GUID, enter a Signature GUID.
6. Select Commit changes and exit.

Deleting a Secure Boot certificate key or database signature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Do one of the following:
   - If there is one option available for deletion:
     a. Select the Delete <*option name*> check box.
     b. Click Yes.
   - If there is more than one option available for deletion:
     a. Select Delete <*option name*>.
     b. Select the check box for the option you want to delete.
     c. Click Yes.

Example: Deleting a KEK entry

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > KEK - Key Exchange Key > Delete KEK entry.
2. Select the check box for the entry you want to delete.
3. Click Yes.

Deleting all keys

About this task

The Delete all keys option deletes all keys in the system, including the Platform Key.

> **IMPORTANT**
> After you delete all keys, the system is forced to immediately disable Secure Boot. Secure Boot remains disabled upon system reboot until valid secure boot keys are restored.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > Delete all keys.
2. Press Enter to delete all keys.
3. Confirm the deletion.

Exporting a Secure Boot certificate key or database signature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select Export <*option name*>.
4. Select the entry you want to export.

   A File Explorer screen shows attached media devices.
5. Do one of the following:
   - Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   - To export to a new file, press +, and enter a file name.

Example: Exporting an Allowed Signatures Database signature

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > DB - Allowed Signatures Database > Export Signature > HPE UEFI Secure Boot 2016 DB Key.
2. Select the entry you want to export.

   A File Explorer screen shows attached media devices.
3. Do one of the following:
   - Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   - To export to a new file, press +, and then enter a file name.

Exporting all Secure Boot certificate keys

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > Export all keys.

   A File Explorer screen shows attached media devices.

2. Do one of the following:

   - Select an attached media device where you want to export the files, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   - To export to a new file, press +, and then enter a file name.

Resetting a Secure Boot certificate key or database signature to platform defaults

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options.
2. Select an exchange key or a signatures database option.
3. Select Reset to platform defaults.
4. Click Yes.

Resetting all Secure Boot certificate keys to platform defaults

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Secure Boot Settings > Advanced Secure Boot Options > Reset all keys to platform defaults.
2. Click Yes.

TLS (HTTPS) Options

Subtopics

Viewing TLS certificate details

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > View Certificates.
2. Select a certificate.

Enrolling a TLS certificate

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Enroll Certificate.
2. Select Enroll certificate using File Explorer.

   The File Explorer screen shows attached media devices.
3. Select the attached media device where the certificate file is located, and then press Enter.
4. Continue selecting the menu path for the certificate file. Press Enter after each selection.
5. Select Commit changes and exit.

Deleting a TLS certificate

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Delete Certificate.
2. From the list of certificates, select the certificates you want to delete.
3. Select Commit changes and exit.

Deleting all TLS certificates

About this task

The Delete all Certificates option deletes all certificates in the system.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Delete all Certificates.
2. Press Enter.
3. Confirm the deletion.

Exporting a TLS certificate

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Export Certificate.
2. Select a file format for the exported certificate.

   A File Explorer screen shows attached media devices.
3. Do one of the following:
   - Select an attached media device where you want to export the file, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   - To export to a new file, press +, and then enter a file name.

Exporting all TLS certificates

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Export all Certificates.

   A File Explorer screen shows attached media devices.
2. Do one of the following:
   - Select an attached media device where you want to export the files, and then continue selecting the menu path for the certificate file. Press Enter after each selection.
   - To export to a new file, press +, and then enter a file name.

Resetting all TLS settings to platform defaults

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Reset all settings to platform defaults.
2. Click OK.

Configuring advanced TLS security settings

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > TLS (HTTPS) Options > Advanced Security Settings.
2. Configure options.
   - To configure which cipher suites are allowed for TLS connections:
     a. Select Cipher suites allowed for TLS connections.

b. Select one of the following:

- Individual check boxes for the cipher suites you want to allow.
- Select Platform Default Cipher suites

c. Select Commit changes and exit.

- To configure the certificate validation process for every TLS connection:

a. Select Certificate validation process for every TLS connection.

b. Select a setting:

- PEER (recommended)—The certificate presented by the peer is validated for secure communication.
- NONE—Does not validate the certificate.

- To enable or disable strict host name checking:

a. Select Strict Hostname checking.

b. Select a setting:

- ENABLE—The host name of the connected server is validated with the host name in the certificate supplied by the server.
- DISABLE—The host name of the connected server is not validated with the host name in the certificate supplied by the server.

- To specify which protocol version to use for TLS connections:

a. Select TLS Protocol Version Support.

b. Select a setting:

- AUTO—Negotiates the highest protocol version that is supported by both the TLS server and the client.
- 1.0—Uses TLS protocol version 1.0. (Not supported in Gen10 Plus and later servers)
- 1.1—Uses TLS protocol version 1.1. (Not supported in Gen10 Plus and later servers)
- 1.2—Uses TLS protocol version 1.2.
- 

  NOTE

  ProLiant Gen11 servers support only AUTO and version 1.2.

3. Save your changes.

Changing Advanced Security Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Security Options.

Subtopics

Enabling or disabling platform certificate support

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > Platform Certificate Support.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling login with iLO accounts

About this task

Use the Allow login with iLO accounts option to allow users to login with an iLO account with the `CONFIGURE_BIOS` privilege.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > Allow login with iLO accounts.
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling backup ROM image authentication

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > Backup ROM Image Authentication.
2. Select a setting.
   - Enabled: When enabled, a cryptographic authentication of the backup ROM image occurs on startup.
   - Disabled: When disabled, only the primary ROM image is authenticated on each startup.
3. Save your setting.

Enabling or disabling the one-time boot menu (F11 prompt)

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > One-Time Boot Menu (F11 Prompt).
2. Select a setting.
   - Enabled
   - Disabled: This disables the POST one-time boot F11 prompt. Also, when disabled, the shell `boot` command is not available for use.
3. Save your setting.

Enabling or disabling Intelligent Provisioning (F10 prompt)

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > Intelligent Provisioning (F10 Prompt).
2. Select a setting.
   - Enabled: When enabled, you can use the Intelligent Provisioning functionality.
   - Disabled: When disabled, you are prevented from entering the Intelligent Provisioning environment while pressing F10 during server boot.
3. Save your setting.

Configuring UEFI Variable Access Firmware Control

About this task

Use the UEFI Variable Access Firmware Control option to allow the system BIOS to completely control certain UEFI variables from being written to by other software such as an Operating system.

When Disabled, all UEFI variables are writable. When Enabled, all changes made by software (other than the system BIOS) to critical UEFI variables is blocked.

For instance, for new boot options, the OS attempts to add to the top of Boot Order, but they are actually placed at the bottom of the Boot Order.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Advanced Security Options > UEFI Variable Access Firmware Control.
2. Select a setting.
   - Enabled

     CAUTION

     When enabled, some OS functionality may not work as expected. Errors may occur while installing a new OS.
   - Disabled
3. Save your setting.

Enabling or disabling Microsoft(R) Secured-core Support

About this task

Use Microsoft(R) Secured-core Support option to configure the server for Microsoft(R) Secured-core Support. When enabled, various virtualization and security settings are automatically enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Microsoft(R) Secured-core Support.
2. Select a setting.
   - Enabled

     NOTE

     Enabling this feature on Intel systems enables the following:

     - All processor cores
     - Intel VT
     - Intel VT-d
     - Intel TXT
     - Secure Boot
     - UEFI Optimized Boot
     - Boot Mode is set to UEFI Mode
     - TPM mode is set to TPM 2.0
     - TPM State is set to Present and Enabled

     Enabling this feature on AMD systems enables the following:

     - All processor cores
     - AMD DMA Remapping
     - AMD I/O Virtualization Technology
     - AMD Virtual DRTM Device
     - Transparent Secure Memory Encryption
     - UEFI Optimized Boot
     - Secure Boot
     - Boot Mode is set to UEFI Mode.
     - TPM mode is set to TPM 2.0
     - TPM State is set to Present and Enabled

   - Disabled
3. Save your setting.

Changing Advanced Options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options.

Subtopics

Selecting a ROM image

About this task

On a server with redundant ROMs, use the ROM Selection option to revert the server to a previous BIOS ROM image.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > ROM Selection.
2. Select a setting.
   - Use Current ROM
   - Switch to Backup ROM—Reverts to the image in use before the last flash event.
3. Save your setting.

IMPORTANT

ROM Selection is not supported on HPE Gen11 servers using Ampere processors.

Configuring an embedded video connection

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Embedded Video Connection.
2. Select a setting.
   - Auto—The external video connection to the embedded video controller is automatically disabled to save power when a monitor is not attached. It is enabled automatically when a monitor is attached (including when the server is operating).
   - Always Disabled—The external video connection to the embedded video controller is disabled, and a monitor connected to this port does not display except during system boot.
   - Always Enabled—The external video connection to the embedded video controller is always enabled. This option is only required if a monitor is attached with a monitor detection that does not function, causing Auto mode to not work properly.
3. Save your setting.

Enabling or disabling Consistent Device Naming

About this task

On supported operating systems, use the Consistent Device Naming option to control how NIC ports are named based on their locations in the system.

> **NOTE**
> Existing NIC connections retain their names until reinstalled under the OS environment.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Consistent Device Naming.
2. Select a setting.
   - CDN Support for LOMs and Slots —Names all NIC ports on the system.
   - CDN Support for LOMs Only —Names Embedded NICs and FlexibleLOMs, but no other NIC ports.
   - Disabled—Disables consistent device naming.
3. Save your setting.

Enabling or disabling mixed power supply reporting

About this task

Use the Mixed Power Supply Reporting option to set whether the server logs messages when a mixed supply configuration is present.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Mixed Power Supply Reporting.
2. Select a setting.
   - Enabled
   - Disabled

3. Save your setting.

Changing the POST video support settings

About this task

Use this option to configure the POST Video Support setting. This option is only supported in UEFI Boot Mode and only applies to video output during the POST (preboot) environment.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Video Options.
2. Select a setting:
   - Display All: The system displays POST video to all installed video controllers.
   - Display Embedded Only: The system only displays POST video to the embedded video controller.
3. Save your setting.

Configuring the platform RAS policy

About this task

Platform RAS Policy controls the Platform Resiliency and Serviceability (RAS) policy.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Platform RAS Policy.
2. Select a setting:
   - Firmware First (default)—When in this mode, the BIOS monitors corrected errors and logs an error for the cases where you need to take an action on the corrected errors. The OS does not monitor or log corrected errors.

     NOTE

     This option is the recommended configuration.
   - OS First—In this mode, corrected errors are unmasked to the OS, and OS controls the policy for logging corrected errors. With some operating systems, the OS logs all corrected errors.

     NOTE

     Corrected errors are an expected and natural occurrence and no action is required based on OS logging of corrected errors (unless the BIOS has also logged an event).
3. Save your setting.

Configuring SCI RAS support

About this task

Use SCI RAS Support to select the System Control Interrupt (SCI) signalling mode of operation. This setting can be used to monitor how the system signals the OS for certain error conditions. Certain resiliency features, such as Page Retire, require this setting to be configured properly to allow the OS to react properly to the error event.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > SCI RAS Support.
2. Select a setting:
   - GHES v1 Support
   - GHES v2 Support

   NOTE

   Consult documentation for which operating systems support which mode of SCI operation. The installed OS must support the appropriate GHES signalling mode to ensure proper operation.
3. Save your setting.

Enabling or disabling High Precision Event Timer (HPET) ACPI Support

About this task

Use the High Precision Event Timer (HPET) ACPI Support option to enable or disable the High Precision Event Timer (HPET) table and device object in ACPI.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > High Precision Event Timer (HPET) ACPI Support.
2. Select a setting.
   - Enabled—The HPET is available to an operating system that supports it using the industry standard ACPI name space.
   - Disabled—The HPET is not available to an operating system that supports it using the industry standard ACPI name space.
3. Save your setting.

Changing UEFI Power Supply Requirements

About this task

Use this option to configure the power supply redundancy logic. The server can operate with various workloads and configurations with the required power supplies installed.

IMPORTANT

This option is only available on systems with dual power domain.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options.

2. In Power Supply Requirements, select one of the following:
   - Configured for 1+1 Redundancy: One supply is required and an additional supply is required for a redundant configuration.
   - Configured for 2+2 Redundancy: Two supplies are required and an additional two supplies are required for a redundant configuration.
   - Configured for 3+1 Redundancy: Three supplies are required and an additional power supply is required for a redundant configuration.
   - Configured for 4+0 Redundancy: Four supplies are required with no redundancy.
3. Save your setting.

Setting the thermal configuration

About this task

Use the Thermal Configuration option to select the fan cooling method for the system. Modifying this option is only advised for configurations that differ from typical Hewlett Packard Enterprise-supported configurations that cannot be cooled adequately via Optimal Cooling.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Thermal Configuration.
2. Select a setting.
   - Optimal Cooling—Provides the most efficient solution by configuring fan speeds to the minimum required to provide adequate cooling.
   - Increased Cooling—Operates fans at a higher speed.
   - Maximum Cooling—Provides the maximum cooling available for the system.
   - Enhanced CPU Cooling—Provides additional cooling to the processors, which can improve performance.
3. Save your setting.

Enabling or disabling thermal shutdown

About this task

Use the Thermal Shutdown option to configure the system to shut down when a fan failure occurs in non-redundant fan mode. A shutdown is initiated due to non-redundant fan failures or temperature increases beyond the pre-set threshold. If disabled, the System Management Driver ignores thermal events and the system immediately powers off in data-destructive situations.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Thermal Shutdown.
2. Select a setting.
   - Enabled—The server automatically shuts down when the internal server temperature reaches within five degrees of the critical level.
   - Disabled—The server does not automatically shut down when the internal server temperature reaches within five degrees of the

critical level. Shutdown occurs when the temperature reaches the critical level.

3. Save your setting.

Setting fan installation requirements messaging

About this task

Use the Fan Installation Requirements option to configure how the server reacts when all required fans are not installed. Operating the server without the required fans can result in damage to the hardware components. By default, the server displays messages and log events to the IML when required fans are not installed. The server can still boot and operate.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Fan Installation Requirements.
2. Select a setting.
   - Enable Messaging—The server displays messages and log events to the IML when required fans are not installed. The server can still boot and operate. This setting is the recommended setting.
   - Disable Messaging—The server does not display message and log events when required fans are not installed. All indications that the server is operating without required fans are removed.
3. Save your setting.

Setting the fan failure policy

About this task

Use the Fan Failure Policy option to configure how the server reacts when fans fail, resulting in the server not having required fans in operation.

NOTE

Operating a server without the required fans installed and operating is not recommended and can impact the ability for the system to cool components properly. It can also result in damage to hardware components.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Fan Failure Policy.
2. Select a setting.
   - Shutdown/Halt on Critical Fan Failures—The server cannot boot or operate if it does not have required fans operating due to one or more fan failures. This setting is the recommended setting.
   - Allow Operation with Critical Fan Failures—The server can boot and operate if it does not have required fans operating due to one or more fan failures.
3. Save your setting.

Enabling or disabling higher ambient temperature support

About this task

Use the Extended Ambient Temperature Support option to enable the server to operate at higher ambient temperatures than are normally supported.

> **NOTE**
>
> This option is only supported by specific hardware configurations. See your HPE server documentation before enabling extended ambient temperature support. Improper system operation or damage to hardware components can result from enabling these features in unsupported configurations.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Fan and Thermal Options > Extended Ambient Temperature Support.
2. Select a setting.
   - Disabled
   - Enabled for 40c Ambient (ASHRAE 3)—Enables the server to operate in environments with ambient temperatures up to 40 degrees Celsius.
   - Enabled for 45c Ambient (ASHRAE 4)—Enables the server to operate in environments with ambient temperatures up to 45 degrees Celsius.

     > **NOTE**
     >
     > Not all servers support both 40c Ambient (ASHRAE 3) and 45c Ambient (ASHRAE 4).
3. Save your setting.

Re-entering a serial number

About this task

Use the Serial Number option to re-enter the server serial number after replacing the system board. This value must match the serial number sticker located on the back of the chassis.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options > Serial Number.
2. Enter the serial number, and then press Enter.
3. Save the setting.

Re-entering a product ID

About this task

Use the Product ID option to re-enter the product ID after replacing the system board. This value must match the product ID sticker located on the back of the chassis.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options > Product ID.
2. Enter the product ID, and then press Enter.
3. Save your setting.

Configuring advanced debug options

Prerequisites

Boot Mode is set to UEFI Mode.

Use Advanced Debug Options to control the output level of debug and POST boot progress messages.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Debug Options.
2. Select settings.
   - UEFI Serial Debug Message Level —Sets the level of debug messages output to the serial console.
     - Disabled
     - Errors Only
     - Medium
     - Network
     - Verbose

       NOTE

       This setting can significantly increase boot time.
     - Custom
   - POST Verbose Boot Progress —Enables detailed messaging that might be helpful in determining why a server became unresponsive during the boot process.
     - Disabled
     - Serial Only—Detailed messages are output to the serial console.
     - All—Detailed messages are output to the POST screen and serial console.
   - Advanced Crash Dump Mode -- Configures the system to log additional debug information to the Active Health System (AHS) logs when an unexpected system crash is experienced.
     - Enabled

       IMPORTANT

       This option should only be enabled when directed by qualified service personnel.
     - Disabled
   - PCH Crash Log Feature -- Configures the system to log additional debug information to the Active Health System (AHS) logs when

an unexpected system crash is experienced.

- Enabled

  IMPORTANT

  This option should only be enabled when directed by qualified service personnel.

- Disabled

- CPU Crash Log Feature -- Configures the system to log additional debug information to the Active Health System (AHS) logs when an unexpected system crash is experienced.

  - Enabled

    IMPORTANT

    This option should only be enabled when directed by qualified service personnel.

  - Disabled

3. Save your settings.

Obtaining UEFI serial output log data with the UEFI System Utilities

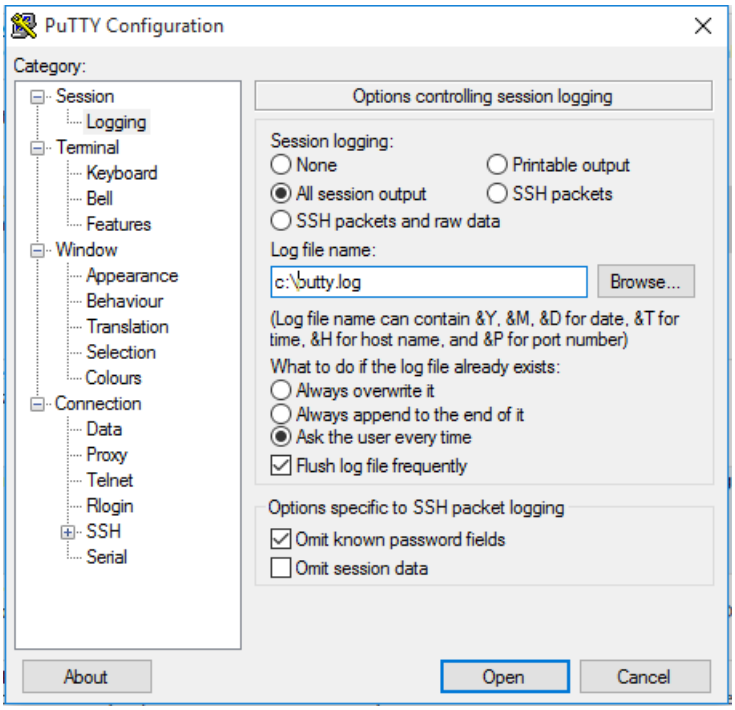
About this task

Use this task to obtain serial output log data if physical access to the server is not available. If you are using a PCIe Expansion Card, you can enable debug collection from the card.

Procedure

1. During POST press F9 to enter System Utilities.
2. From the System Utilities screen, select System Configurations > BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Debug Options.
3. Set the debug level.
   a. Select UEFI Serial Debug Level.
   b. Select Medium Verbosity.
4. If you are using an expansion card, enable debug data collection from the expansion card:
   a. Select POST Verbose Boot Progress.
   b. Select either Serial Only or All.
5. Save and exit System Utilities.
6. Open an iLO Virtual Serial Port (VSP) session.
7. Use a utility, such as PuTTY, to establish the connection and ensure that you enable logging to a file (select **All session output**).

   The following example shows sample PuTTY settings for logging data:



More information

- Launching the System Utilities

Enabling or disabling the One-Time Boot Menu F11 prompt

About this task

Use this option to control whether you can press the F11 key to boot directly to the One-Time Boot Menu during the current boot. This option does not modify the normal boot order settings. When this option is enabled, you can boot directly into the One-Time Boot Menu in the System Utilities by pressing F11 in the POST screen after a server reboot.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > One-Time Boot Menu (F11 Prompt).
2. Select a setting.
   - Enabled
   - Disabled
3. Save your changes.

Enabling or disabling the Intelligent Provisioning F10 prompt

About this task

Use the Intelligent Provisioning (F10 Prompt) option to control whether you can press the F10 key to access Intelligent Provisioning from the POST screen.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intelligent Provisioning (F10 Prompt).
2. Select a setting.
   - Enabled
   - Disabled
3. Save your setting.

Enabling or disabling processor AES-NI support

About this task

Use the Processor AES-NI option to enable or disable the Advanced Encryption Standard Instruction Set in the processor.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Processor AES-NI Support.
2. Select a setting.
   - Enabled—Enables AES-NI support.
   - Disabled—Disables AES-NI support.
3. Save your changes.

Enabling or disabling backup ROM image authentication

About this task

Use the back-up ROM Image Authentication option to enable or disable cryptographic authentication of the backup ROM image on startup.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Backup ROM Image Authentication.
2. Select a setting.
   - Enabled—The backup ROM image is authenticated on startup.
   - Disabled—The backup ROM image is not authenticated on startup. Only the primary image is authenticated.
3. Save your changes.

> **IMPORTANT**
>
> Backup ROM Image Authentication is not supported on HPE Gen11 servers using Ampere processors.

Configuring Trusted Platform Module (TPM) options

About this task

Trusted Platform Modules are computer chips that securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM to store platform measurements to make sure that the platform remains trustworthy. For servers configured with a Trusted Platform Module, TPM enables the firmware and operating system to take measurements of all phases of the boot process.

For information on installing and enabling the TPM module option, see the user documentation for your server model. By default, the Trusted Platform Module is enabled as TPM 2.0 when the server is powered on after installing it.

CAUTION

An OS that is using TPM might lock all data access if you do not follow proper procedures for modifying the server and suspending or disabling TPM in the OS. This includes updating system or option firmware, replacing hardware such as the system board and hard drive, and modifying TPM OS settings. Changing the TPM mode after installing an OS might cause problems, including loss of data.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Trusted Platform Module Options
2. Select an option. On servers configured with an optional TPM, you can set the following:
   - TPM 2.0 Operation: Sets the operation of TPM 2.0 to execute after a reboot. Options are:
     - No Action: There is no TPM configured.
     - Clear: TPM is cleared during reboot, and TPM 2.0 Operation is set to No Action.
   - Current TPM 2.0 Active PCRs: When the PCR banks are switched, the algorithm used to compute the hashed values stored in the PCRs during extend operations is changed. Options are:
     - SHA1 only
     - SHA256 only
     - SHA384 only
     - SHA1 and SHA256
     - SHA256 and SHA384

   In Advanced Trusted Platform Module Options,

   - TPM 2.0 Visibility:Sets whether TPM is hidden form the operating system. Options are:
     - Visible
     - Hidden: Hides TPM from the operating system. Use this setting to remove TPM options from the system without having to remove the actual hardware.
   - TPM UEFI Option ROM Measurement: Enables or disables (skips) measuring UEFI PCI operation ROMs. Options are:
     - Enabled
     - Disabled
   - TPM 2.0 Endorsement Hierarchy: The endorsement hierarchy is the hierarchy of choice when the user has privacy concerns. Options are:
     - Enabled
     - Disabled
   - TPM 2.0 Storage Hierarchy: Storage hierarchy is intended for non-privacy-sensitive operations. Options are:
     - Enabled
     - Disabled

- Omit Boot Device Event: Skips or records measuring PCR Boot Attempt. Options are:
  - Enabled- PCR Boot Attempt Measurements are disabled and measurement in PCR[4] is not recorded.
  - Disabled

3. Save your changes.
4. Reboot the system.

   After the system reboots, you can view the Current TPM Type and Current TPM State settings.
5. Verify that your new Current TPM Type and Current TPM State settings appear at the top of the screen.

Configuring Intel Security Options

This section lists the tasks for Intel specific Security options.

Subtopics

Enabling or disabling Trust Domain Extension (TDX)

Prerequisites

- Processor Physical Addressing is Default.
- Total Memory Encryption (TME) is Enabled.
- Total Memory Encryption Multi-Key (TME-MK) is Enabled.
- Intel(R) Software Guard Extensions (SGX) is Enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel Security Options > Trust Domain Extension (TDX).
2. Select a setting:
   - Enabled
   - Disabled (Default)
3. Save your setting.

Enabling or disabling TDX Secure Arbitration Mode Loader (SEAM Loader)

Prerequisites

Trust Domain Extension (TDX) is Enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel Security Options > TDX Secure Arbitration Mode Loader (SEAM Loader).
2. Select a setting:
   - Enabled
   - Disabled (default)
3. Save your setting.

Configuring TME-MT/TDX key split

Prerequisites

Trust Domain Extension (TDX) is Enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel Security Options > TME-MT/TDX key split.
2. Designate the number of bits for TDX usage by entering a value. The rest are used by TME-MT.
3. Save your setting.

Enabling or disabling TDX excluding CMR below 1MB

Prerequisites

Trust Domain Extension (TDX) is Enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Server Security > Intel Security Options > Disable excluding Mem below 1MB in CMR.
2. Select a setting:
   - Enabled
   - Disabled (Default)
   - Auto
3. Save your setting.

Changing PCIe Device Configuration options

Procedure

From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration.

Subtopics

Selecting advanced PCIe device settings

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration.
2. Select settings.
   - NVMe PCIe Resource Padding —Configures PCIe resources to support PCIe hot-add for NVMe drives.
     - Disabled—Only allocates PCIe resources to devices installed at boot time. PCIe hot-add is not supported on ports where NVMe drives are not present at boot time.
     - Enabled—Allocates additional PCIe resources for each PCIe root port, which may allow a PCIe hot-add event to work without requiring a system reboot to enumerate the device.
   - Maximum PCI Express Speed—When Workload Profile is set to Custom, sets the maximum speed at which the server allows PCI Express devices to operate.
     - Per Port Control
     - PCIe Generation 1.0
3. Save your settings.

Subtopics

Configuring PCIe MCTP options

About this task

Use the PCIe MCTP Options to control the PCIe Management Component Transport Protocol (MCTP) Support for a given slot. This option can be used to disable MCTP support to a given PCIe endpoint that may not properly support this protocol.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe MCTP Options.

2. Select the MCTP Broadcast Support for each PCIe slot.
    - Enabled (recommended for full system functionality)
    - Disabled
3. Save your settings.

Configuring PCIe bifurcation options

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Bifurcation Options.
2. Select the bifurcation option for each PCIe slot.
    - No Bifurcation
    - Bifurcate
    - Dual Bifurcate
3. Save your settings.

Configuring PCIe Data Link feature

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Data Link Feature.
2. The PCIe slots for Data Link Feature Exchange are listed.
3. For each slot, select a setting:
    - Enabled (default)
    - Disabled
4. Save your settings.

Configuring PCIe EOI options

About this task

Use the PCIe EOI Options to control the PCIe EOI (End of Interrupt) message broadcast support for a given slot. This option can be used to disable EOI support to a given PCIe endpoint that may not properly support this protocol.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe EOI Options.
2. Select the EOI Broadcast Support for each PCIe slot.

- Enabled
- Disabled

3. Save your settings.

Setting Maximum PCI Express Speed

About this task

Use the Maximum PCI Express Speed option to lower the maximum PCI Express speed at which the server allows PCI Express devices to operate. The option can also used to address issues with problematic PCI Express devices. Setting this value to Maximum Supported configures the platform to run at the maximum speed supported by the platform or the PCIe device, whichever is lower.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > Maximum PCI Express Speed.
2. Select a setting.
   - Per Port Control
   - PCIe Generation 1.0
   - PCIe Generation 2.0
   - PCIe Generation 3.0
3. Save your setting.

Configuring AMD PCIe Hot-Plug Error Control

About this task

Use the PCIe Hot-Plug Error Control option to select PCIe Hot-Plug support for the AMD platform.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Hot-Plug Error Control.
2. Select a value:
   - Hot-Plug Surprise-- RBSU attempts to protect the platform from experiencing an error on a surprise removal event.

     TIP

     Select this option for older Operating Systems that do not support Enhanced Downstream Port Containment (eDPC).
   - e-DPC Firmware Control-- The platform firmware and OS properly negotiate and log all hot-plug events. [This option is currently not supported by all Operating Systems.]
   - eDPC OS Control-- Hot-plug events are handled by the Operating System with no involvement by the platform. All logging of events in this mode is limited to the OS only.

IMPORTANT

This option must be set properly based on the OS to ensure that hot-plug events and surprise removal events are handled properly by the platform.

Consult OS documentation for additional details.

3. Save your settings.

Configuring Intel PCIe Hot-Plug Error Control

About this task

Use the PCIe Hot-Plug Error Control option to select PCIe (NVMe) Hot-Plug support for the platform.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe Hot-Plug Error Control.
2. Select a value:
   - Hot-Plug Surprise-- RBSU attempts to protect the platform from experiencing an error on a surprise removal event.

     TIP

     Select this option for older Operating Systems that do not support Enhanced Downstream Port Containment (eDPC).
   - e-DPC Firmware Control-- The platform firmware and OS properly negotiate and log all hot-plug events. [This option is currently not supported by all Operating Systems.]
   - eDPC OS Control-- Hot-plug events are handled by the Operating System with no involvement by the platform. All logging of events in this mode is limited to the OS only.

     IMPORTANT

     This option must be set properly based on the OS to ensure that hot-plug events and surprise removal events are handled properly by the platform.

     Consult OS documentation for additional details.
3. Save your settings.

PCIe ASPM Support (Global)

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > Advanced PCIe Configuration > PCIe ASPM Support (Global).
2. Select a setting:
   - Enabled
   - Disabled

3. Save your settings.

Setting GPU Configurations

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > GPU CFG Selection.
2. Select an option.
   - 4:1—Maps 4 PCIe slots to each installed processor.
   - 8:1—Maps all slots to a single processor.
3. Save your settings.

Configuring PCIe Slot to Processor Mapping

About this task

Use the PCIe Slot to Processor Mapping option to change the PCIe to Processor mapping configuration.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration Options > PCIe Slot to Processor Mapping .
2. Select a setting.
   - 4:1—When this option is selected, four PCIe slots are mapped to each installed processor.
   - 8:1—When this option is selected, all slots are mapped to a single processor.
3. Save your setting.

Enabling or disabling PCIe Device Isolation Support

About this task

Use the PCIe Slot to Processor Mapping option to configure PCIe Isolation Support.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration Options > PCIe Device Isolation Support .
2. Select a setting.
   - Enable—When enabled, a PCIe device will be disabled at runtime when an error is detected.
   - Disable—When disabled, a PCIe device will be enabled at runtime when an error is detected.

     Consult Operating System documentation before enabling this option.

3. Save your setting.

Configuring specific PCIe devices

About this task

Use the PCIe Device Configuration options to enable or disable, and select configuration settings for embedded and added-in PCI devices. Disabling devices reallocates the resources (memory, I/O, and ROM space and power) that are normally allocated to the device. By default, all devices are enabled.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration.
2. Select a device from the list.
3. Select settings. Depending on the device, options include:
   - Device Disable
     - Auto—The device is automatically enabled at server boot.
     - Disabled—The device is not automatically enabled.
   - PCIe Link Speed
     - Auto—Sets the link speed to the maximum supported speed of the PCIe link.
     - PCIe Generation 1.0—Sets the link speed to a maximum speed of PCIe Generation 1.0.
     - PCIe Generation 2.0—Sets the link speed to a maximum speed of PCIe Generation 2.0.

     NOTE

     If this feature is not supported, the option is not available.
   - PCIe Power Management (ASPM)
     - Auto
     - Disabled
     - L1 Enabled—The device's link enters a lower power standby state at the expense of a longer exit latency.
   - PCIe Option ROM
     - Enabled—The platform optimally loads PCIe Option ROMs to save boot time.
     - Disabled—The platform disables all PCIe Option ROM optimizations, which might be required for older PCIe devices.
4. Save your settings.

Configuring PCIe Auxiliary Power Options

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > PCIe Device Configuration > PCIe Auxiliary Power Options.

2. For each slot, make a configuration selection:
   - OCP Slot 14 Auxiliary Power —Select Enabled or Disabled.
   - OCP Slot 15 Auxiliary Power —Select Enabled or Disabled.
3. Save your settings.

Setting the Date and Time

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Date and Time.
2. Select a setting, and then complete your entry.
   - Date (mm-dd-yyyy)—Enter the date in a month-day-year (mm-dd-yyyy) format.
   - Time (hh:mm:ss) —Enter the time in a 24-hours format (hh:mm:ss) format.
   - Hour Format —Enter the hour in 12 and 24-hours format.
   - Time Format
     - Coordinated Universal Time (UTC) —Calculates the time stored in the hardware Real Time Clock (RTC) from the associated Time Zone setting.
     - Local Time—Removes the use of the Time Zone setting.
       This option is useful for addressing interaction issues between Windows operating systems set in Legacy BIOS boot mode.
   - Time Zone—Select your current time zone for the system.
   - Daylight Savings Time
     - Enabled—Adjusts the local time displayed by one hour for Daylight Savings Time.
     - Disabled—Does not adjust the local time displayed for Daylight Savings Time.
3. Save your settings.

NOTE

The hour format option is only supported on ProLiant Gen10 Plus and Gen11 servers.

Changing Backup and Restore settings

About this task

Backup files include serial numbers and product ID information. When you restore from a backup, you are prompted whether you want to apply this information to the system or not. If you are using the backup to set up a new system, you can skip restoring the serial number and product ID.

To change device encryption settings, go to System Configuiration > BIOS/Platform Configuration (RBSU) > Server Security > Device Encryption Options > Device Encryption Migration Options.

To change physical NIC interface for backup and restore operation, go to System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > Network Options > Pre-Boot Network Settings > Pre-Boot Network Interface.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options > Backup and Restore Settings.
2. Select one of the following:
   a. Backup
   b. Restore
3. Follow the instructions to navigate to the location of a backup file, or where you want to create a backup file.

   NOTE

   - If you are restoring a backup, the backup file must be a `.json` or `.zip` file.
   - User and password requirement was deprecated since ProLiant Gen10 servers.
   - FTP and HTTP (s) protocols are supported for backup and restore operation.
4. Click Start Operation.

Resetting system defaults

Subtopics

Restoring default system settings

About this task

Use the Restore Default System Settings option to reset all BIOS configuration settings to their default values and immediately and automatically restart the server.
Selecting this option resets all platform settings except:

- Secure Boot BIOS settings
- Date and Time settings
- Primary and redundant ROM Selection (if supported)

  To save a custom default configuration to use during a system restore, use User Default Options. Doing so saves settings you might otherwise lose.
- Other entities, such as option cards or iLO, that must be individually reset.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options > Restore Default System Settings.
2. Select Yes, restore the default settings .
3. Reboot the server.

Restoring default manufacturing settings

About this task

Use the Restore Default Manufacturing Settings option to reset all BIOS configuration settings to their default manufacturing values and delete all UEFI non-volatile variables, such as boot configuration and Secure Boot security keys (if Secure Boot is enabled). Previous changes that you have made might be lost.
The difference between this action and the Restore Default System Settings option is that Restore Default Manufacturing Settings erases all UEFI variables. An OS can write UEFI variables that store such things as entries in the boot order and key database information for Secure Boot. When you Restore Default Manufacturing Settings, this information is cleared, whereas it is retained when you Restore Default System Settings.

To save a custom default configuration to use during a system restore, use User Default Options. Doing so saves settings you might otherwise lose.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options > Restore Default Manufacturing Settings.
2. Select Yes, restore the default settings .
3. Reboot the server.

Changing the default UEFI device priority

Prerequisites

User Default Options are configured and saved.

About this task

Use the Default UEFI Device Priority option to change the UEFI device priority that is used when default system settings are restored. The initial UEFI Boot Order list is created based on the priorities defined in this option. When the default configuration settings are loaded, the settings from the saved Default UEFI Device Priority list are used instead of the system or factory defaults.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options > Default UEFI Device Priority .
2. Select an entry.
3. Use the + key to move the entry higher in the list. Use the - key to move it lower in the list. Use your pointing device or the arrow keys to navigate the list.
4. Save your settings.

Saving or erasing user default options

About this task

Use User Default Options to save or erase a configuration as the custom default configuration. Configure the system as necessary and then enable this option to save the configuration as the default configuration. When the system loads the default settings, the custom default settings are used instead of the manufacturing defaults.

Procedure

1. From the System Utilities screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Default Options > User Default Options.
2. Select an option.
   - Save User Defaults
     - Yes, Save—Saves the current settings as the system default settings.
     - No, Cancel—Does not save the current settings as the system default settings.
   - Erase User Defaults
     - Yes, erase the current settings —Erases (deletes) the current user-defined default settings. Once deleted, you can only restore these settings manually.
     - No, Cancel—Does not erase the current user-defined default settings
3. Save your setting.

Using scripted configuration flows

Subtopics

Scripted configuration flow

Scripted configuration flow

You can use BIOS/Platform Configuration (RBSU) with the RESTful API Tool to create standard server configuration scripts to automate many of the manual steps in the server configuration process.

Subtopics

iLO RESTful API support for UEFI
Configuration Replication Utility (CONREP)
HPE Smart Storage Administrator (HPE SSA)

iLO RESTful API support for UEFI

ProLiant servers and HPE Synergy compute modules include support for configuring UEFI BIOS settings using the RESTful API. The RESTful API Tool is a management interface that server management tools can use to perform server configuration, inventory, and monitoring. A REST client uses HTTPS operations to configure supported server settings, such as iLO 6 and UEFI BIOS settings. For more information about the RESTful API and the RESTful Interface Tool, see the Hewlett Packard Enterprise website (https://www.hpe.com/info/restfulinterface/docs).

Configuration Replication Utility (CONREP)

CONREP is included in the STK and is a utility that operates with the BIOS/Platform Configuration (RBSU) to replicate hardware configuration. This utility is run during State 0, Run Hardware Configuration Utility when performing a scripted server deployment. CONREP reads the state of the system environment variables to determine the configuration and then writes the results to an editable script file. This

file can then be deployed across multiple servers with similar hardware and software components. You can find the STK on the Hewlett Packard Enterprise website (**https://www.hpe.com/info/stk/docs**). For more information, see the Scripting Toolkit User Guide for your operating system environment on the Hewlett Packard Enterprise website (**https://www.hpe.com/info/stk/docs**).

HPE Smart Storage Administrator (HPE SSA)

HPE SSA Scripting is a standalone application that is distributed with the HPE SSA CLI application and is used for configuring arrays on Smart Array devices.

- Scripting Toolkit for Windows User Guide

  https://www.hpe.com/support/STK_Windows_UG_en

- HPE SSA guides

  https://www.hpe.com/info/smartstorage/docs

Troubleshooting

Subtopics

Cannot boot devices

Symptom

You see a message that the option or device you want to boot cannot be found, or it is listed in the system configuration as an unknown device.

Solution 1

Cause

You are attempting to boot to an option that does not have a UEFI Option ROM driver.

Action

1. Verify that your option card has a UEFI option driver (Option ROM) that supports either x64 or EFI Byte Code for boot functionality.

   NOTE

   - UEFI drivers do not display messages on the System Utilities screen or provide function key prompts.
   - If you replace the motherboard, UEFI variables are lost.
   - You must configure PXE servers with a boot image. For x64 EFI machines, you must also configure the DHCP server to support x64 EFI DHCP boot requests. For more information, see the UEFI Information Library: **https://www.hpe.com/info/ProLiantUEFI/docs**

2. Retry the boot procedure.

Solution 2

Cause

You are attempting to boot to an option that is not supported or is not running the latest firmware.

Action

1. Refer to the Quick Specs or Read This First card for your server to make sure that your card is supported before you install it. Although third-party option cards might work, they are not optimized for servers running UEFI System Utilities.
2. Verify that the correct information is listed in the System Health settings for the option.
3. If necessary, use the latest SPP in offline mode to upgrade the firmware to the latest version.

Solution 3

Cause

Your default boot mode settings are different than your user-defined settings.

Action

1. Use User Default Options to save a custom default configuration to use during a system restore.
2. Retry the boot procedure.

Cannot restore system defaults

Symptom

- After moving a drive from one server to another in Windows, you see an error message that certain settings cannot be found.
- After replacing a motherboard, you lose your configuration settings, such as Secure Boot.

Cause

Moving drives and replacing system hardware can disrupt pointers to previously configured settings.

Action

1. Use the Restore Default System Settings option, or the Restore Default Manufacturing Settings option to restore your settings.

2. Retry the procedure.

Cannot download the file in the network boot URL

Symptom

You see an error message when you try to download the file in the URL you specified for a network boot.

Solution 1

Cause

The network URL you specified during static configuration are incorrect.

Action

1. Use the Embedded UEFI Shell `ping` command to check the network connection. See “Ping” in the UEFI Shell user guide.
2. Change your static network connection settings and try to download the file in URL again.

Solution 2

Cause

The DHCP server did not respond.

Action

1. Ensure that there is a DHCP server available and it is operational.
2. Try to download the file in the URL again.

Solution 3

Cause

No cable is connected to the selected NIC port.

Action

1. Ensure that there is a cable connection.
2. Try to download the URL again.

Solution 4

Cause

The file is incorrect or not present on the server, or it cannot be downloaded due to insufficient privileges. Check the file name and that it exists on the server. Make sure that you have admin privileges on the server.

Action

1. Ensure that the file is present, and that you are using the correct file name and have sufficient privileges to download it.
2. Try to download the file in the URL again.

Solution 5

Cause

The HTTP or FTP server is down or did not respond.

Action

1. Ensure that the HTTP or FTP server you specified is available and that it is operational.
2. Try to download the file in the URL again.

Cannot network boot with the downloaded image file

Symptom

Booting from the image specified in the URL fails.

Solution 1

Cause

The image is not signed and Secure Boot is enabled.

Action

1. Ensure that the image is signed and that its Secure Boot settings are correct.
2. Try to download the file in the URL again.

Solution 2

Cause

The downloaded file is corrupt.

Action

1. Select a new file.
2. Repeat the URL configuration, specifying the new file.
3. Try to download the new file in the URL.

Cannot deploy from the UEFI Shell script

Symptom

You attempted to deploy an OS using the UEFI Shell script and you see an error message that the deployment failed.

Cause

Configuration settings are not correct.

Action

1. Verify the following.
   a. The Embedded UEFI Shell interface is added to the UEFI Boot Order list or the One-Time Boot Menu.
   b. When added to the UEFI Boot Order list, the Embedded UEFI Shell interface is the first boot option in the UEFI Boot Order list so that it overrides other boot options to load.
   c. UEFI Shell Script Auto-Start is enabled.
   d. The correct `startup.nsh` script file location in attached media or a network location is specified. If it is in attached media, the `startup.nsh` script must be either inside the `fsX:\` or the `fsX:\efi\boot\` directory.
   e. The `.nsh` script only contains supported commands.
   f. Your system has enough RAM memory to create RAM disks during automated script execution.
   g. Any OS boot loader or diagnostics application launched using the `.nsh script` is supported to run in UEFI the environment.
   h. If the shell script verification is enabled, ensure the script is enrolled in the Secure Boot database and that the script starts with the line #!NSH.
2. Try the deployment again.

Cannot execute Option ROM for one or more devices

Symptom

You cannot execute Option ROM for one or more devices.

Cause

The amount of available Option ROM space has been exceeded.

Action

1. Disable any unnecessary option ROMs (such as PXE).
2. Retry the procedure.

Cannot find a new network or storage device in the Boot Order list

Symptom

You connected a network or storage device, and it does not appear in the Boot Order list.

Cause

Newly-added devices do not appear in the boot order list until you reboot the system.

Action

1. Reboot the system.
2. Verify that your device appears in the Boot Order list.

Intel TXT is not working properly

Intel TXT is not working properly

Cause

One of the prerequisites may not be enabled.

Action

Verify that the prerequisites are enabled:

- VT-d
- TPM

Invalid Server Serial Number and Product ID

Symptom

You see an error message that the Server Serial Number and Product ID are invalid, corrupted, or lost.

Cause

The serial number, product ID, or both, are invalid, corrupted, or lost.

Action

1. Enter the correct values for these fields under BIOS/Platform Configuration (RBSU) > Advanced Options > Advanced Service Options.
2. Verify that the error message does not appear again.

Invalid time or date

Symptom

You see a message stating that the time and date is not set.

Cause

The time or date in the configuration memory is invalid.

Action

1. Use the Date and Time option to change the settings.
2. Verify that the message does not appear again.

Networking devices are not functioning properly

Cause

Only networking devices on the list of supported server options should be used.

Action

Hewlett Packard Enterprise recommends that networking devices be updated to the latest version of firmware before they are used in the

server. Before installing the operating system, use the latest Service Pack for ProLiant in Offline mode to upgrade the firmware to the latest version.

NOTE

If the default boot mode settings are different than the user-configured settings, the system might not boot the OS installation when the defaults are restored. To avoid this issue, use the User Default Options feature in UEFI System Utilities to override the factory default settings.

System unresponsive

Cause

There is a mis-configured or malfunctioning PCIe expansion card.

Action

Enable PCIe debug information collection to identify the problem card.

Single Device Failure

Symptom

Boot failure during POST.

Action

If the server does not boot, refer "POST issues-Boot, no video flowchart" in the **Troubleshooting Guide for HPE ProLiant Gen10and Gen10 Plus servers**

Server will not boot

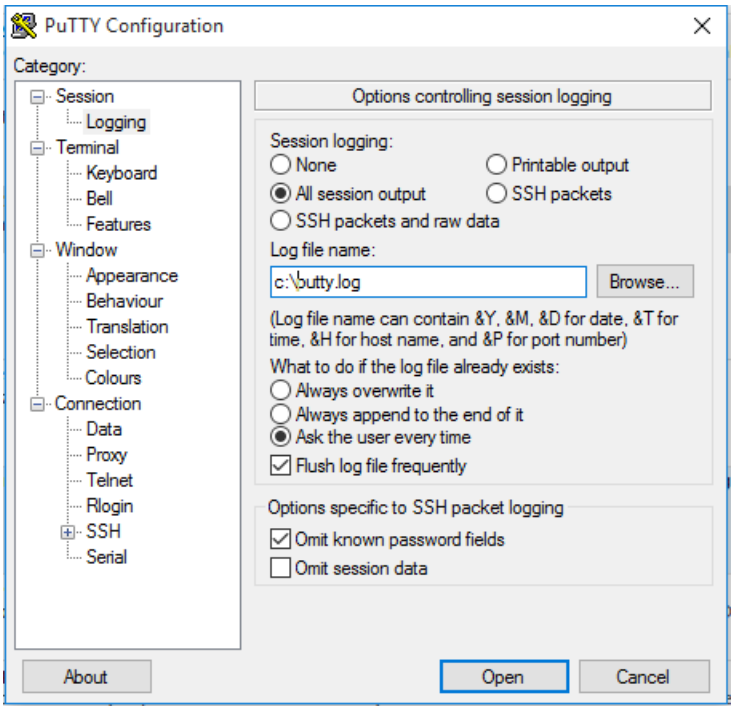
Cause

Enable serial debug with the maintenance switch.

Action

1. Power off the server.
2. Locate the Server Maintenance Switch (12 position switch) and set DIP 4 to the ON position. Refer to the chassis hood label for details on the location of the switch.
3. Attach a NULL mode cable to the server serial port or open an iLO Virtual Serial Port (VSP) session.
4. Use a utility, such as PuTTY, to establish the connection and ensure that you enable logging to a file (select **All session output**).

   The following example shows sample PuTTY settings for logging data:



Smart Array controllers are not functioning properly

Cause

Other Smart Array controllers are not supported and will not function properly.

For more information on supported options, see the server QuickSpecs on the Hewlett Packard Enterprise website (https://www.hpe.com/info/qs).

For more information on the latest firmware and driver versions, see the Hewlett Packard Enterprise website (https://www.hpe.com/support/hpesc).

Action

Hewlett Packard Enterprise recommends that Smart Array controllers be updated to the latest version of firmware before they are used in the server. Before installing the operating system, use the latest Service Pack for ProLiant in Offline mode to upgrade the firmware to the latest version.

VMware not booting in UEFI mode

Cause

UEFI Optimized Boot is not enabled.

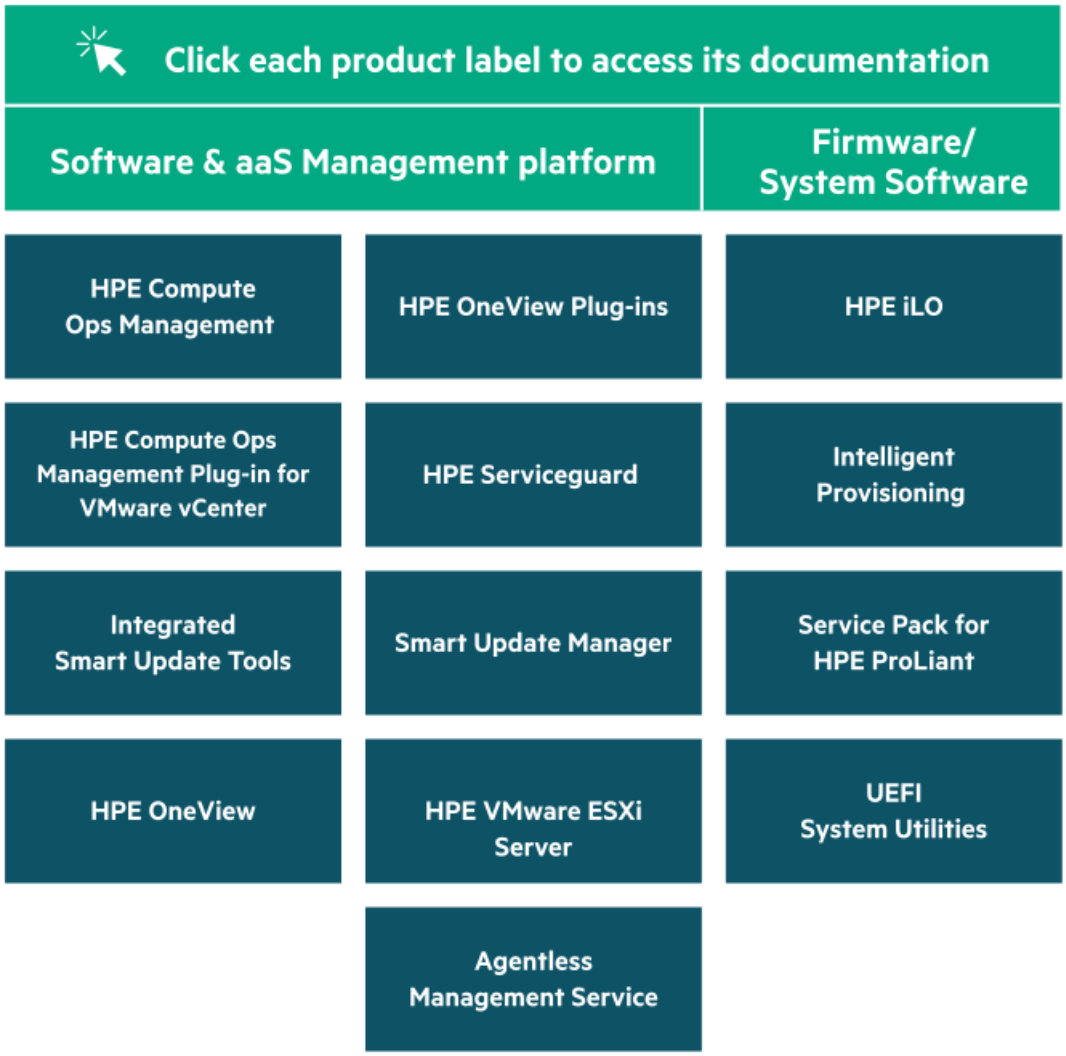
Action

Enable UEFI Optimized Boot.

HPE Compute Software and Firmware Product Documentation Quick Links

This infographic provides quick links for documentation for the listed HPE products. It offers easy access to documentation that helps you to understand, implement, and troubleshoot your products.

Each product-specific section lists the current version, the earlier two major versions, and their revisions.



Navigating the Hewlett Packard Enterprise Support Center

- Navigation and workspace
- Search and product knowledge

Subtopics

UEFI System Utilities Quick links
This page is a comprehensive list of all the documents for UEFI System Utilities. It provides quick links to the recent versions of each document.

UEFI System Utilities Quick links

This page is a comprehensive list of all the documents for UEFI System Utilities. It provides quick links to the recent versions of each document.

Documents	Versions		
UEFI System Utilities User Guide for HPE ProLiant Servers and HPE Synergy	Gen12 with iLO6	Gen12 with iLO7	Gen12 DL384
	Gen11		
	Gen10/Gen10 Plus		
UEFI Workload-Based Profiles and Tuning Guide for HPE Servers	Gen12 with iLO6		Gen12 with iLO7
	Gen11		
	Gen10/Gen10 Plus		
UEFI Deployment Guide	Gen12 with iLO6		Gen12 with iLO7
	Gen11		
	Gen10/Gen10 Plus		
UEFI Shell User Guide for HPE ProLiant Servers and HPE Synergy	Gen12		
	Gen11		
	Gen10/Gen10 Plus		

Websites, support, and other resources

Subtopics

- Websites
- Support and other resources

Websites

General websites

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

UEFI Specification

www.uefi.org/specifications

UEFI Learning Resources

www.uefi.org/learning_center

RESTful API Tool

https://www.hpe.com/info/redfish

Contact Hewlett Packard Enterprise Worldwide

https://www.hpe.com/assistance

Subscription Service/Support Alerts

https://www.hpe.com/support/e-updates

Software Depot

https://www.hpe.com/support/softwaredepot

Customer Self Repair

https://www.hpe.com/support/selfrepair

Insight Remote Support

https://www.hpe.com/info/insightremotesupport/docs

For additional websites, see Support and other resources.

Support and other resources

Subtopics

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

- To download product updates:

  Hewlett Packard Enterprise Support Center

  https://www.hpe.com/support/hpesc

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

  https://www.hpe.com/support/AccessToSupportMaterials

> **IMPORTANT**
> Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Account set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Tech Care Service

https://www.hpe.com/services/techcare

HPE Complete Care

https://www.hpe.com/services/completecare

Warranty information

To view the warranty information for your product, see the warranty check tool.

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. This process captures all document information.