

NML72-GB300 User Manual

Revision History

Refer to the table below for changes made on this version of the NML72-GB300 User Manual.

Date	Version	Updates
9/16/2025	FIRST DRAFT	
10/22/2025	V1.00	

Copyright Notice

The information contained in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF PENGUIN SOLUTIONS, PENGUIN SOLUTIONS MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE.

Penguin Solutions assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. Software described in Penguin Solutions' documents (a) is the property of Penguin Solutions (PENG) Ireland Limited or the third party, (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

Penguin Solutions' documentation describes all supported features of the user interfaces and the application programming interfaces (API) developed by Penguin Solutions. Any undocumented features of these interfaces are intended solely for use by Penguin Solutions personnel and are subject to change without warning.

This document is protected by copyright. All rights are reserved. Penguin Solutions grants you limited permission to download and print a reasonable number of copies of this document (or any portions thereof), without change, for your internal use only, provided you retain all copyright notices and other restrictive legends and/or notices appearing in the copied document.

Intel and the Intel Inside logo are registered trademarks and Xeon is a trademark of Intel Corporation or its subsidiaries in the United States and/or other countries/regions.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other jurisdictions.

All other trademarks and registered trademarks are the property of their respective holders.

Publication Date: August 2026

Penguin Solutions

© 2026 Penguin Solutions (PENG) Ireland Limited. All rights reserved.

Table of Contents

Revision History 1

Copyright Notice 1

About this Document 7

Introduction 7

 System Description 7

 Product Specifications..... 8

 Processor and Memory 8

 Accelerator and Memory 8

 Storage..... 8

 I/O..... 8

 System Monitoring and Management 9

 Power Input and Operating System 9

 Physical Characteristics 9

System Tour..... 10

 Front View 10

 Front Control panel..... 10

 Rear View..... 11

 Server Components 12

 Status LED Indicators 14

 Front panel LED indicators 14

System Architecture..... 16

 System Block Diagram..... 16

 PCIe Topology 16

Safety Considerations..... 18

 Preventing Electrostatic Discharge 18

 Symbols on equipment..... 18

 Warnings and cautions..... 19

 System Battery 20

安全注意事項 21

 防止靜電放電（ESD） 21

 設備符號說明..... 21

 警告與注意事項 21

 電池 22

System Boards 23

 HPM (Main planar) 23

 ConnectX-8 Mezzanine Network Board..... 25

HGX Management Controller (HMC)	26
Power Distribution Board (PDB)	27
Interposer Board	29
Baseboard Management Controller (BMC).....	29
Front IO Board (FIO)	30
FIO Panel Board	30
E1.S Backplane Board	31
OSFP Board	31
M.2 Riser Board	32
1G NIC Board	32
TPM Board	33
PCIe CEM Riser Board	33
CRU Part Assembly Guide	34
E1.S HDD Disassembly	34
E1.S HDD Assembly	36
Cabling.....	38
Compute Tray Signal Cable Connectivity	38
PDB Control Sideband Cable	38
Front IO Cable	38
HMC-BMC MCIO Cable	39
2P Management Custom Cable	39
Ultrapass Cable	40
E1.S MCIO x8 Cable	40
PCIe CEM Riser Cable.....	41
BlueField-3 NCSI Cable	41
MCIO x4 to 1G NIC Cable	42
C-Link Cable.....	42
OSFP Sideband Cable	43
Front IO Panel Cable.....	43
Compute Tray Power Cable Connectivity	44
54V Busbar Cable	44
12V Multi-end Power Cable: Left Tray	44
12V Multi-end Power Cable: Right Tray	45
12V Multi-end Power Cable: Middle Tray	45
MB 12V Standby Cable	46
System utilities	47
Boot Menu	47
Accessing the Boot menu screen	47

BIOS setup	48
Accessing the BIOS setup menu screen	48
Navigating the BIOS setup menu screen	50
Remote Flash BIOS.....	50
BIOS setup menu screen	51
Main menu	51
Advanced menu.....	53
Chipset menu	55
Security menu.....	56
Boot menu	58
Save & Exit menu	59
Server Management menu	60
BMC User Interface	62
Get BMC IP	62
Web GUI.....	65
Log in.....	69
Menu Bar (row)	70
Profile Settings	71
Menu Bar (column).....	72
Overview.....	73
Dashboard	74
Logs	76
Hardware Status.....	84
Operations	98
Settings.....	113
Security and access	134
Resource management	152
BIOS	156
Leak Detection	157
Leak Sensors	157
High risk Leak Points	157
NVIDIA MGX NVL Leak Sensor Installation Location	158
BMC Firmware Secure	163
Secure Boot	163
SPI Monitor.....	163
Redfish Update.....	163
Redfish.....	164
HTTP Methods	164

Status Code165

Available APIs168

Common Gateway Interface173

 Session & Cookies173

Compliance Information.....175

About this Document

This document provides a comprehensive technical overview of the system, including detailed installation and component replacement instructions. It provides specific technical specifications and offers best practices for component installation.

Introduction

System Description

1RU GB300 NVL compute tray with Hybrid-cooled system

- System architecture consists of two NVIDIA GB300 HPMs for compute boards, two ConnectX-8 mezzanine network boards for AI networking (E-W), one BlueField-3 FHHL AIC for cloud networking (N-S), and four E1.S NVMe for GPU data storages
- Supports Rack 48-54V Busbar power solution (~7.3kW per compute tray)
- Featuring NVIDIA GB300 NVL72 rack-scale 5th generation NVLink across 72 NVIDIA Blackwell B300 GPUs and 36 NVIDIA Grace CPUs, optimized for AI and data centers
- Support Maximum Acceleration and Flexibility For LLM, AI/Deep Learning, and HPC Applications

KEY FEATURES

- Compute node consist of 2x GB300 HPMs
- 2x 72-core NVIDIA Grace Arm Neoverse V2 CPUs, up to 960GB memory
- 4x NVIDIA Blackwell B300 GPUs, up to 1152GB memory
- 4x E1.S SSD for data storages
- Support 2x dual OSFP ports NVIDIA ConnectX-8 VPI with 800Gb/s InfiniBand for AI networking
- Support 1x dual QSFP112 NVIDIA BlueField-3 VPI with 400Gb/s InfiniBand and Ethernet for cloud networking
- ORv3 48-54V power busbar compatible in 19" MGX Rack
- Supporting Insyde BMC and GPU Management
- Whole System Server Health Monitoring Supported

Product Specifications

Processor and Memory

Item	Description
CPU	2x NVIDIA Grace Arm Neoverse V2 CPUs
CPU Cores	144-core
CPU Memory	960GB of LPDDR5X memory with ECC
Power (TDP)	600W (300W / CPU)

Accelerator and Memory

Item	Description
GPU	4x NVIDIA Blackwell B300 GPUs
GPU Memory	1152GB HBM3e
CPU-GPU Interconnection	NVLink-C2C, 900GB/s of coherent bandwidth
GPU-GPU Interconnection	5 th generation NVLink of 1.8TB bandwidth / GPU
Power (TDP)	5600W (1400W / GPU)

Storage

Item	Description
Boot Drive	1x 22110 M.2 NVMe SSD
Data storage	4x EDSFF E1.S NVMe SSDs

I/O

Item	Description
I/O Ports	• 1 System Power LED/ Button • 1 System Identify LED/Button • 1 Reset Button • 1 Mini Display Port • 1 USB3.0 Type-A • 1 Micro USB (COM) • 1 BMC Management LAN 1GbE RJ45 • 1 System OS Management LAN 1GbE RJ45 • 1 BlueField-3 Management LAN 1GbE RJ45
Networking	• 4 NVIDIA NVLink Switch ports • 2 Dual OSFP ports support 800GbE / NDR InfiniBand

	1 Dual QSFP ports support 400GbE / NDR InfiniBand and Ethernet
--	--

System Monitoring and Management

Item	Description
System Monitoring	System power status Front ID indicator System fault status NVLink health status
Management	Aspeed AST2600
Security	Microchip CEC1736
GPU-GPU Interconnection	5th generation NVLink of 1.8TB bandwidth / GPU

Power Input and Operating System

Item	Description
Power (TDP)	5600W (1400W / GPU)
Power Supply	ORv3 Power Busbar 48-54V, 1400A
Power per System (TDP)	~136kW
Operating Temperature	40°C

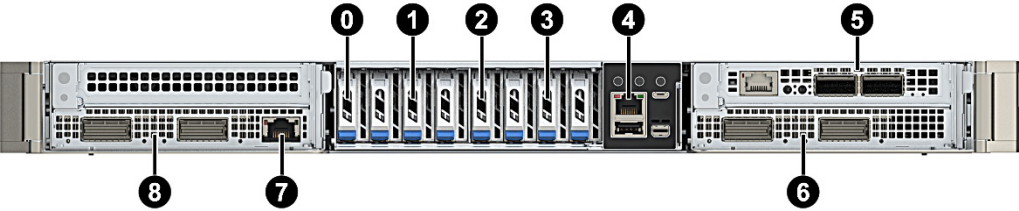
Note: Power supply is not included in this product.

Physical Characteristics

Item	Description
Chassis	1RU Rackmount (Hybrid – Cooling)
System Dimensions	W x D x H: 17.2" (438mm) x 30" (768mm) x 1.7" (43.6mm)

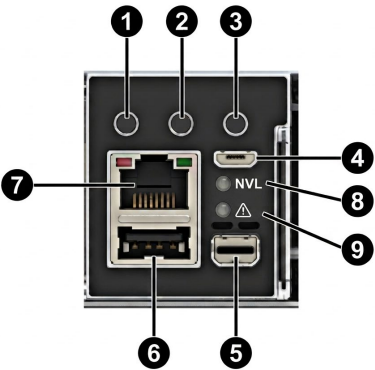
System Tour

Front View



Item	Description	Root port
0-1	PCIe5 x2 E1.S NVMe	ConnectX-8 Mezzanine Network Board 0
2-3	PCIe5 x2 E1.S NVMe	ConnectX-8 Mezzanine Network Board 1
4	Front IO panel	
5	BlueField-3/1 FHHL AIC	CPU1 UPHY3
6	OSFP Board 1	ConnectX-8 Mezzanine Network Board 1
7	1G NIC Board	CPU0 UPHY2 via PCIeSwitch
8	OSFP Board 0	ConnectX-8 Mezzanine Network Board 0

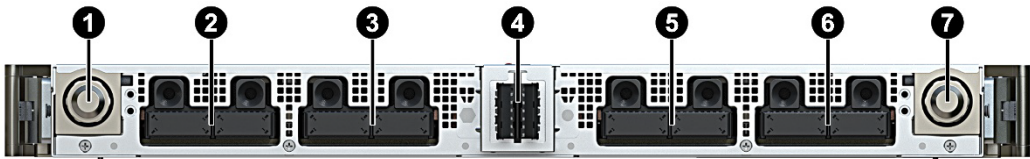
Front Control panel



Item	Description
1	Button with power & status LED
2	Button with unit identification LED
3	System reset button
4	CPU UART0 COM Port (debug)
5	Mini-DisplayPort

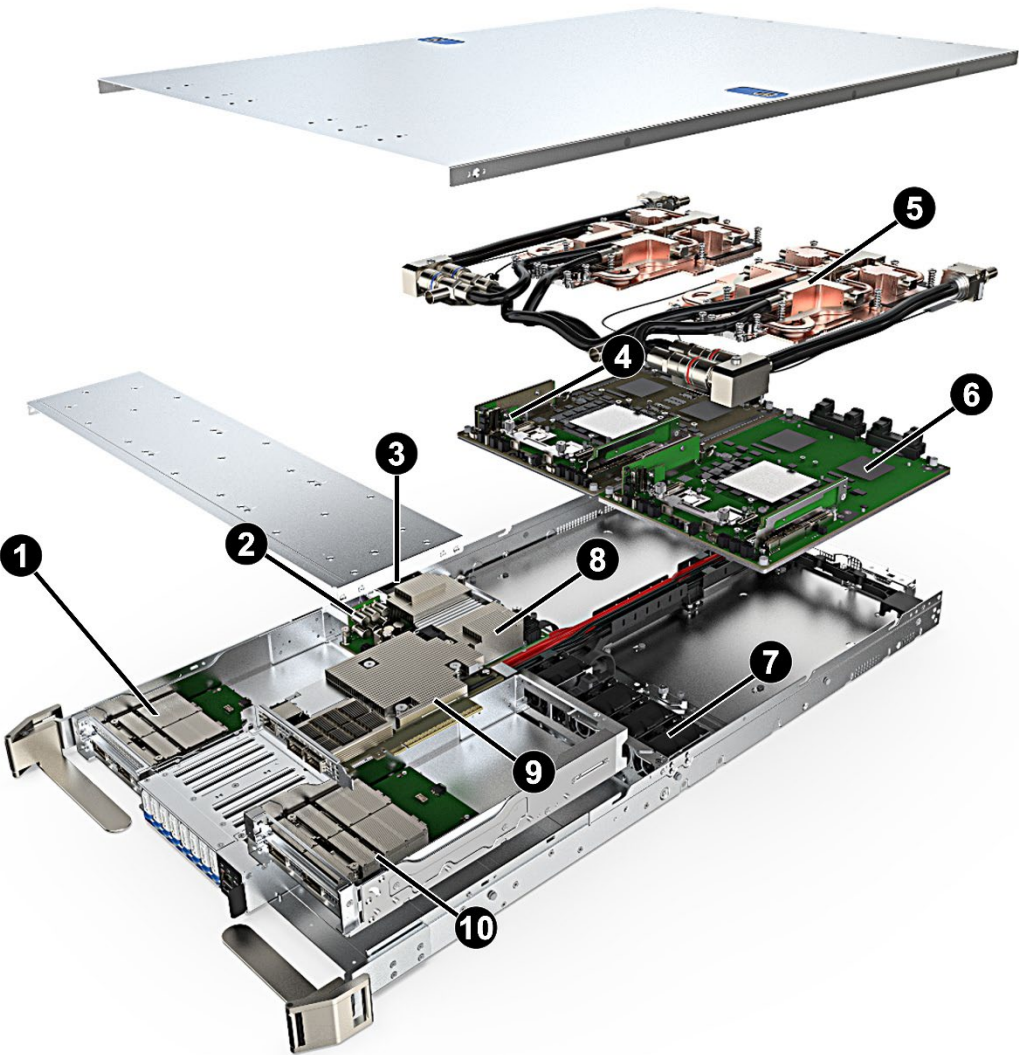
6	USB3.0 type-A connector
7	BMC OOB ethernet (1GbE)
8	NVLink health status LED
9	System fault status LED

Rear View



Item	Description
1	Manifold – Liquid outlet
2	GPU2 NVLink 4x19 connector
3	GPU3 NVLink 4x19 connector
4	ORv3 Busbar Clip – Compute tray power input
5	GPU0 NVLink 4x19 connector
6	GPU1 NVLink 4x19 connector
7	Manifold – Liquid inlet

Server Components



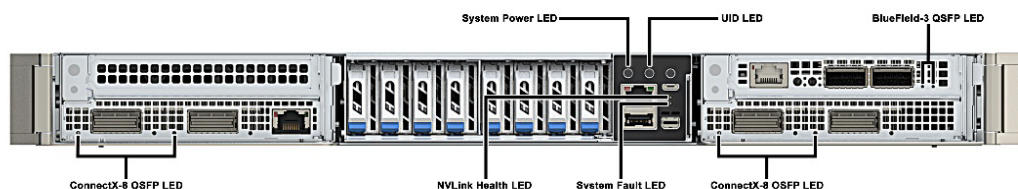
Item	Description
1	OSFP Board 0
2	Interposer Card
3	BMC
4	TPM
5	Cold Plate
6	HMC
7	Fan Module

8	Power Distribution Board
9	BlueField-3/1 FHHL AIC
10	OSFP Board 1

Status LED Indicators

The status LED indicators aid in problem diagnosis by indicating the status of system components and operations of the server.

Front panel LED indicators



E1.S NVMe Drive LED Behavior

LED	Color	State	Description
Status LED	Green	Solid on	Hard drive powered
	Green	Flicker/Activity	Hard drive read/write
	Amber	Solid on	Hard drive fault
	White	Solid on	Hard drive ready to remove

BlueField-3 QSFP LED Behavior

LED	Color	State	Description
Status LED	Green	Solid on	Cable asserted, Ports Link Up
	Amber	Solid on	Cable asserted, Ports Link Down
	None	Off	Cable de-asserted

ConnectX-8 OSFP LED Behavior

LED	Color	State	Description
Status LED	Green	Solid on	Cable asserted, Ports Link Up
	Amber	Solid on	Cable asserted, Ports Link Down
	None	Off	Cable de-asserted

System Power LED Behavior

LED	Color	State	Description
System power status	Green	Solid on	System power on
	Green	Flashing (4 Hz)	System running POST

	Green	Flashing (1 Hz)	Stand by (HMC/BMC booted)
	Green	Off	System off

UID LED Behavior

LED	Color	State	Description
Front ID indicator	Blue	Flashing (1Hz)	Identify server location
	Blue	Off	ID off status/system normal
	Note: ID button should implement toggle functionality. If LED was turned on remotely, pressing the button turns off the ID LED. If the LED was off, pressing the button turns on ID LED.		

System Fault LED Behavior

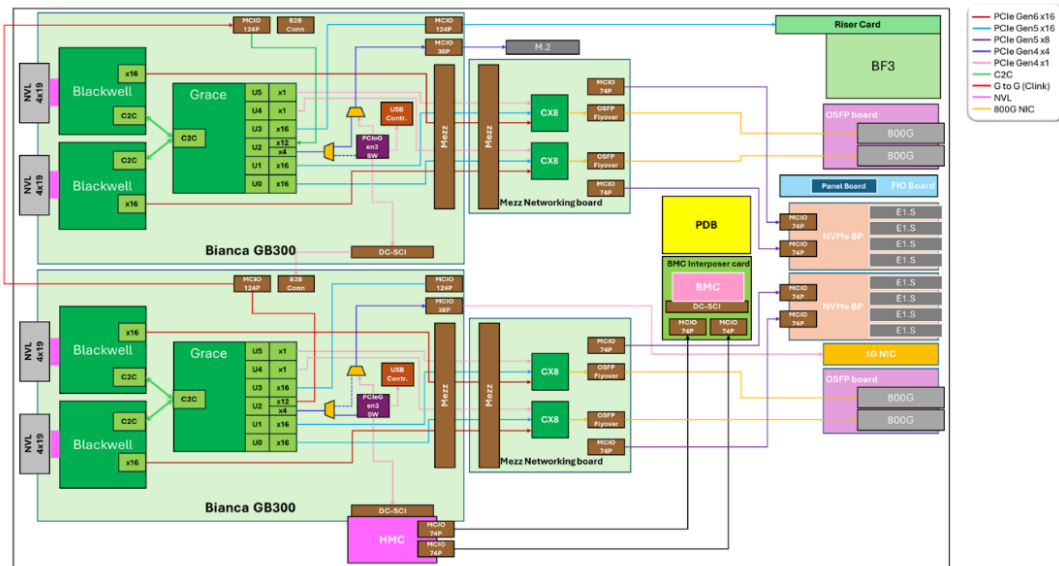
LED	Color	State	Description
System fault status	Amber	Solid on	System faulted (any component)
	Amber	Blinking (4 Hz)	Leak detected
	Amber	Off	System normal

NVLink Health LED Behavior

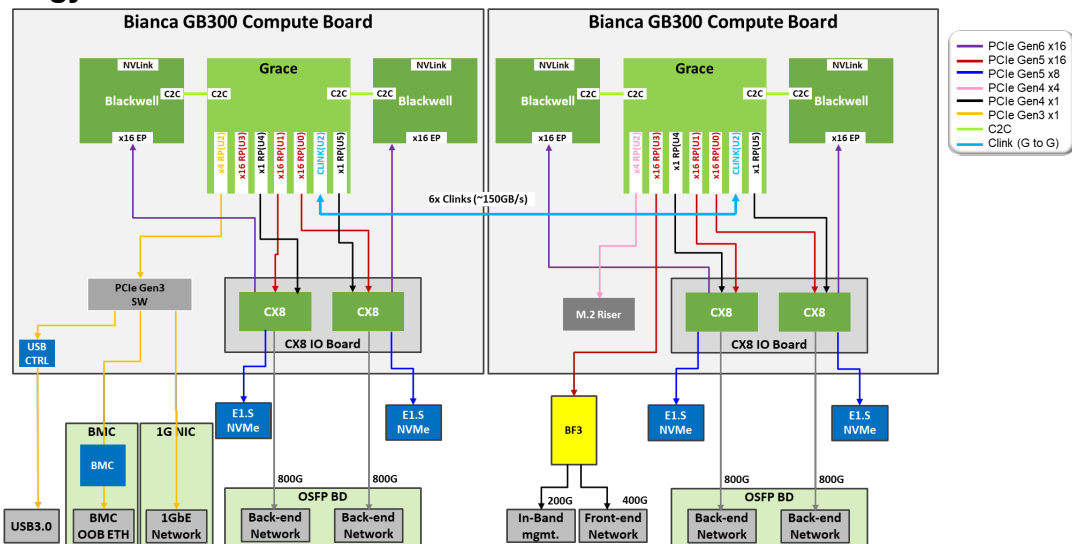
LED	Color	State	Description
NVLink health status	Green	Solid on	Link connected: no traffic
	Green	Blinking (0.5 Hz)	Link connected: active
	Amber	Solid on	Physical link state on any NVLink
	Amber	Blinking (1 Hz)	Beacon (locate) on any NVLink
	Bi-color LED	Off	No link on any NVLink

System Architecture

System Block Diagram



PCIe Topology



PHY	Capability	Interface Connector	End Point
UPHY0	PCIe Gen5 x16	Mirror Mezz connector	ConnectX-8 Mezzanine Network Board
UPHY1	PCIe Gen5 x16	Mirror Mezz connector	ConnectX-8 Mezzanine Network Board
UPHY2	PCIe Gen5 x12	124-pin MCIO connector	C-link interface
	PCIe Gen5 x4	38-pin MCIO connector	M.2 SSD Drive / PCIe Gen3 switch for interface with BMC, USB controller, and 1G NIC
UPHY3	PCIe Gen5 x16	124-pin MCIO connector	BlueField-3 DPU Card
UPHY4	PCIe Gen5 x1	Mirror Mezz connector	ConnectX-8 Mezzanine Network Board
UPHY5	PCIe Gen5 x1	Mirror Mezz connector	ConnectX-8 Mezzanine Network Board

Safety Considerations

Before performing service procedures, review all the safety information. The server should be installed in a restricted area that is accessible only to technicians.

Preventing Electrostatic Discharge

To prevent damaging the system, be aware of the precautions you must follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage mainboards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage:

Avoid hand contact by transporting and storing products in static-safe containers.

Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.

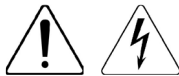
Place parts on a grounded surface before removing them from their containers.

Avoid touching pins, leads, or circuitry.

Always be properly grounded when touching a static-sensitive component or assembly.

Symbols on equipment

The following symbols may be placed on equipment to indicate the presence of potentially hazardous conditions.



This symbol indicates the presence of hazardous energy circuits or electric shock hazards. Refer all servicing to qualified personnel.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure. Refer all maintenance, upgrades, and servicing to qualified personnel.



This symbol indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure.



This symbol indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



29.76 kg
65.61 lb

This symbol indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.



This symbol indicates the presence of a moving fan blade.

WARNING: To reduce the risk of personal injury or damage to the equipment, please keep body parts away from fan blades if access panel is open.

Warnings and cautions

Before installing a server, be sure that you understand the following warnings and cautions.



WARNING: To reduce the risk of electric shock or damage to the equipment:

Do not disable the power cord grounding plug. The grounding plug is an important safety feature.

Connect the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.

Disconnect the power cord from the power supply to disconnect power to the equipment.

Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the rack.



CAUTION: Do not operate the server for long periods with the access panel open or removed. Operating in this manner results in improper airflow and improper cooling that can lead to thermal damage.

System Battery

If the server no longer automatically displays the correct date and time, you might have to replace the battery that provides power to the real-time clock. Under normal use, battery life is 5 to 10 years.



WARNING: To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.



WARNING: The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:

Do not attempt to recharge the battery.

Do not expose the battery to temperatures higher than 70°C (158°F).

Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.

Replace only with the spare designated for this product.

To remove the system battery:

1. Power down the server.
2. Disconnect all peripheral cables from the server.
3. Remove the access panel.
4. Remove the air baffle.
5. Locate the battery on the mainboard.
6. Remove the battery.

To replace the component, reverse the removal procedure.



CAUTION: Risk of fire or explosion if the battery is replaced by an incorrect type. Please follow local regulations for disposal of used batteries.

For more information about battery replacement or proper disposal, contact an authorized reseller or an authorized service provider.

安全注意事項

在執行任何維修程序之前，請先詳閱所有安全資訊。伺服器應安裝於僅限技術人員進入的限制區域內。

防止靜電放電（ESD）

為防止系統受損，請注意在安裝系統或處理零件時必須遵守的防靜電措施。

手指或其他導體釋放的靜電可能會損壞主機板或其他對靜電敏感的元件，此類損壞可能會縮短元件的使用壽命。為防止靜電損害，請遵守以下指示：

- 產品在搬運與儲存時，請放置於**防靜電包裝容器**內，避免直接以手接觸。
- 在抵達**防靜電工作區**前，請勿拆開防靜電包裝。
- 拆封前，請先將零件放置於**接地表面上**。
- 避免觸摸**接腳、導線或電路部分**。
- 當接觸靜電敏感元件或模組時，**請確保已正確接地**。

設備符號說明

以下符號可能標示於設備上，用以提醒使用者注意潛在的危險狀況：



此符號表示設備內含高能電路或觸電危險。

警告：為降低觸電或人身傷害的風險，請勿打開外殼。所有維修作業僅限合格人員執行。



此符號表示區域內含高壓電危險，且無可由使用者或現場人員維修的零件。警告：為避免觸電或人身傷害，請勿因任何理由打開此外殼。



此符號表示存在高溫表面或零件，接觸可能造成燙傷。

警告：為防止燙傷，在接觸前請先讓表面充分冷卻。



29.76 kg
65.61 lb

此符號表示該元件的重量超出單人安全搬運的建議值。

警告：為避免人身傷害或設備損壞，請遵守當地職業安全與衛生相關的手動搬運規範與指導方針。



此符號表示設備內含旋轉中的風扇葉片。

警告：為避免人身傷害或設備損壞，在開啟維修面板時，請勿將身體部位靠近風扇葉片。

警告與注意事項

在安裝伺服器之前，請確實了解以下警告與注意事項。



警告： 為避免觸電或設備損壞：

請勿移除電源線上的接地插腳，該插腳為重要的安全設計。

請將電源線插入隨時可輕易拔除的接地（接地良好）插座。

若需完全切斷設備電源，請拔除電源線與電源供應器的連接。

請勿將電源線放置於行走路徑上或被物品壓迫的位置，特別注意插頭、插座

電源線從機架引出的部分。



注意： 請勿在開啟或移除外殼面板的情況下長時間操作伺服器。如此操作將導致氣流不正確與散熱不足，可能造成系統過熱損壞

電池

當伺服器無法自動顯示正確的日期與時間時，可能需要更換主機板上的電池。在正常使用情況下，電池壽命約為 5 至 10 年。



警告： 為避免因高溫表面導致燙傷，請在接觸硬碟或內部零件前，先讓系統充分冷卻。



警告： 本設備內含鋰錳二氧化物、五氧化二釩或鹼性電池模組。不當處理可能導致火災或燙傷風險。為降低人身傷害風險：

請勿嘗試為電池充電。請勿使電池暴露於超過 70° C (158° F) 的環境中。

請勿拆解、壓碎、刺穿、短路外部接點，或丟棄於火中或水中。

僅使用為本產品指定的相容備用電池替換。

更換系統電池步驟

- A. 關閉伺服器電源。
- B. 拔除所有外接線纜。
- C. 拆下上蓋面板。
- D. 移除導風罩。
- E. 找到主機板上的電池位置。
- F. 取下電池。

若需安裝新電池，請依照相反順序重新安裝。



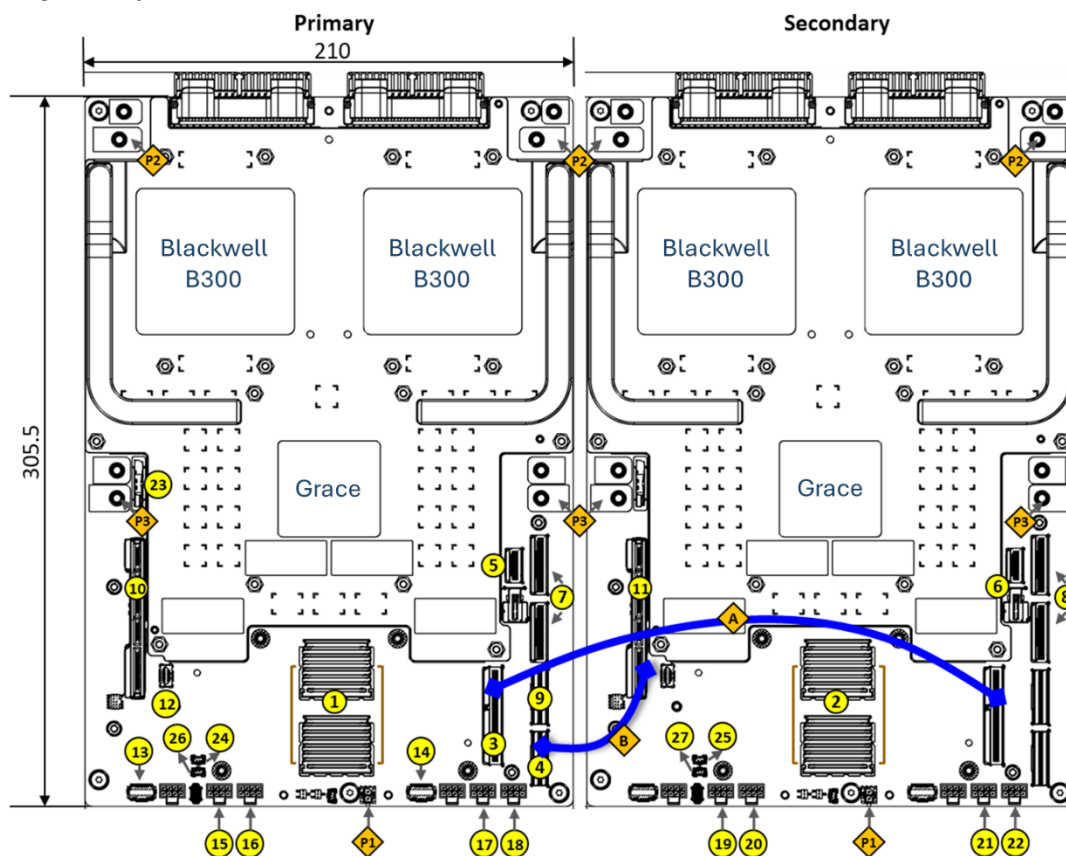
注意： 若使用不正確的電池型號，可能導致火災或爆炸風險。請依照當地法規正確處理廢棄電池。如需更多關於電池更換或正確處理的資訊，請聯繫授權經銷商或授權維修服務提供商。

乾電池回收標誌圖樣：



System Boards

HPM (Main planar)

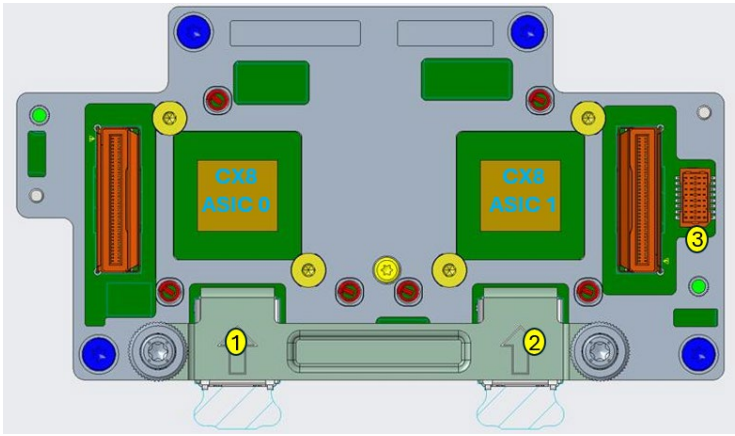


Item	Location	Description
1	J115, J116	(Primary) ConnectX-8 Mezzanine Network Board 0 connector
2	J115, J116	(Secondary) ConnectX-8 Mezzanine Network Board 1 connector
3	J107	MCIOx16 connector for CLINK connection between 2 Grace CPUs
4	J79	(Primary) SlimSAS connector for 2 HPMs management sideband connection
5	J117	(Primary) MCIOx4 connector for 1G NIC board (PCIe3 x1)
6	J117, J23	(Secondary) Multi-Trak + MCIOx4 connector for M.2 riser board (12V, PCIe5 x4)

7	J10, J80	(Primary) 2* MCIOx8 connectors for BlueField-3 FHHL card 0 (PCIe x16)
8	J10, J80	(Secondary) 2* MCIOx8 connectors for BlueField-3 FHHL card 1 (PCIe x16)
9	J82	SlimSAS connector for Front IO board
10	J58	(Primary) DC-SCI connector for HMC module
11	J58	(Secondary) DC-SCI connector for 2 HPMs management sideband connection
12	J55	TPM Board connector
13	J86	NCSI connector for BlueField-3 FHHL card 0
14	JSB2	PDB sideband connector for PDB
15	J46	FAN0 connector
16	J97	FAN1 connector
17	J95	FAN2 connector
18	J38	FAN3 connector
19	J46	FAN4 connector
20	J97	FAN5 connector
21	J95	FAN6 connector
22	J38	FAN7 connector
23	J34	RTC battery socket
24	J18	(Primary) Bianca leak sensor cable header
25	J18	(Secondary) Bianca leak sensor cable header
26	J125	Inlet manifold leak sensor cable header (Y-cable)
27	J125	Outlet manifold leak sensor cable header (Y-cable)
P1	J13	GB300 HPM 12V standby cable connector
P2	MEC39, MEC43	GB300 HPM 12V1 inner busbar
P3	MEC40, MEC44	GB300 HPM 12V2 inner busbar
A	Cable	2 Grace CPUs CLINK connection cable

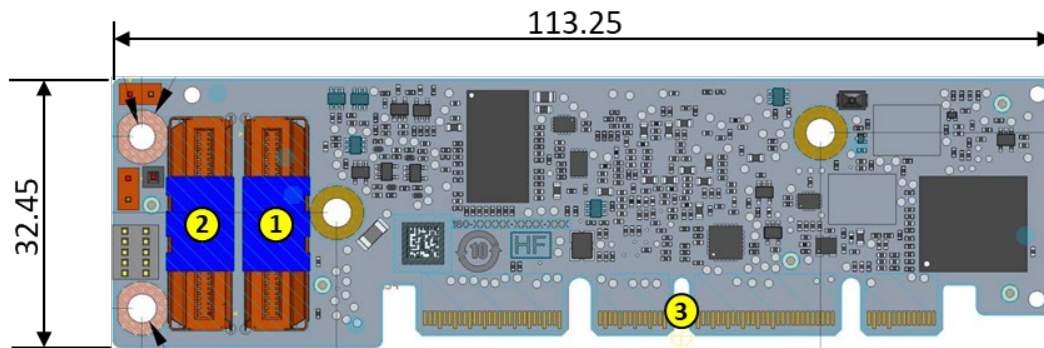
B	Cable	2 HPMS management connection cable
---	-------	------------------------------------

ConnectX-8 Mezzanine Network Board



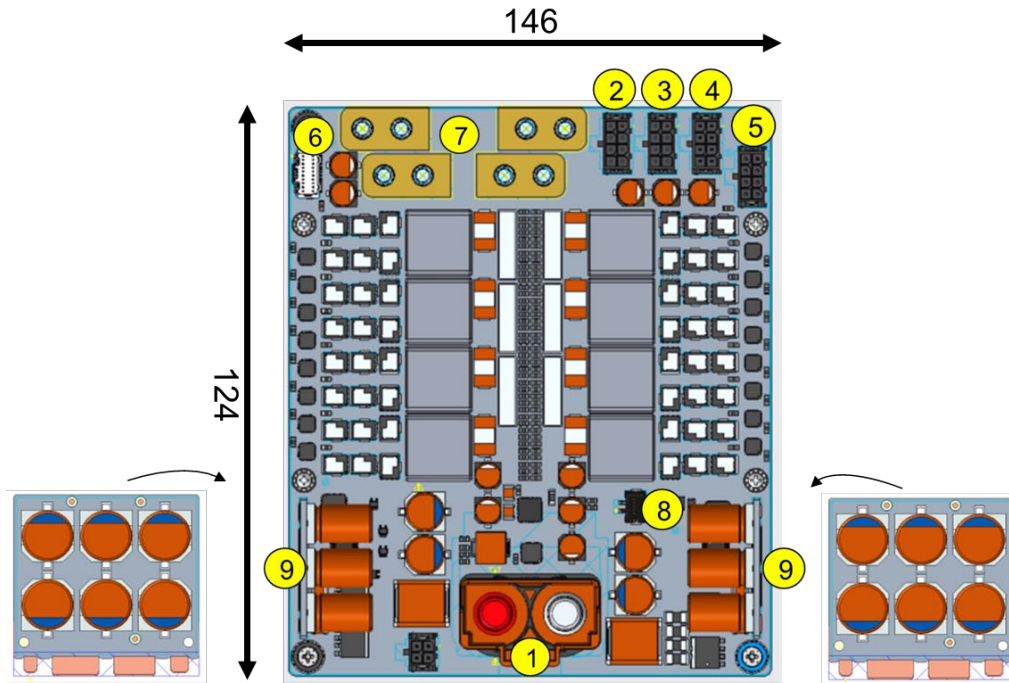
Item	Location	Description
1	-	(CX8 ASIC 0) OverPass to UltraPass cable connector for OSFP board
2	-	(CX8 ASIC 1) OverPass to UltraPass cable connector for OSFP board
3	J2	OSFP board sideband connector

HGX Management Controller (HMC)



Item	Location	Description
1	J21	MCIOx8 connector for interconnection between HMC and BMC (To Interposer board J3)
2	J22	MCIOx8 connector for interconnection between HMC and BMC (To Interposer board J4)
3	-	DC-SCI (4C+) golden finger for plug-in on HPM

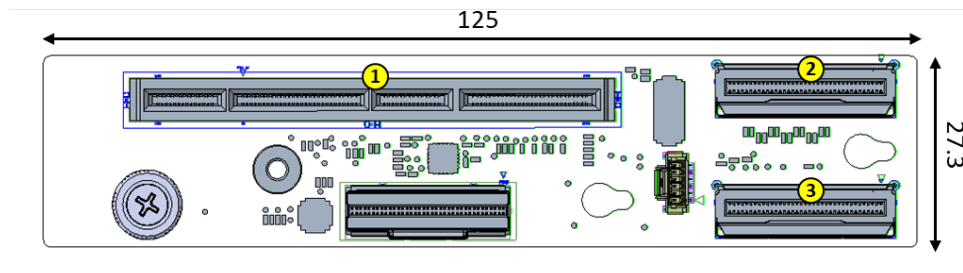
Power Distribution Board (PDB)



Item	Location	Description
1	J59	CoolPowerHD connector for 48-54V rack busbar cable power input
2	J55	Micro-Fit 8P connector for 12V power cable OSFP board(L)
3	J56	Micro-Fit 8P connector for 12V power cable 1G NIC board, E1.S backplane(L), E1.S backplane(R)
4	J57	Micro-Fit 8P connector for 12V power cable PCIe riser(R), OSFP board(R) , and BlueField-3 external(R)
5	J58	Micro-Fit 8P connector for 12V standby power cable Front IO board, Primary HPM, Secondary HPM
6	J50	Wire-to-Board 20P connector for PDB sideband
7	MEC20, MEC21	12V power inner busbar for primary HPM

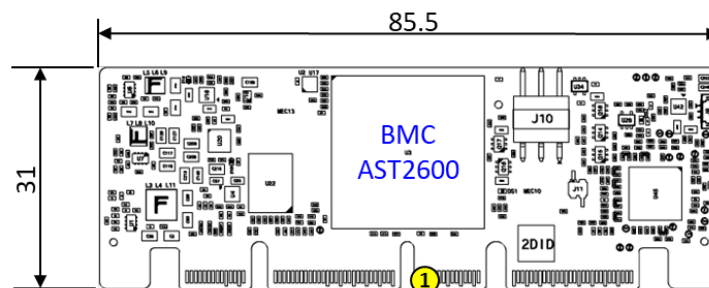
8	MEC22, MEC23	12V power inner busbar for secondary HPM
9	J61	Wire-to-Board 2P connector for 48-54V rack busbar power detection
10	J64, J65	Mounting hole for Cap board

Interposer Board



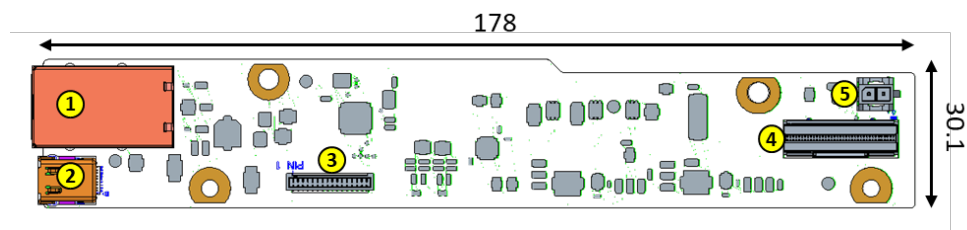
Item	Location	Description
1	J1	DC-SCI (4C+) connector for plug-in BMC board
2	J4	MCIOx8 connector for interconnection between HMC and BMC (To HMC board J22)
3	J3	MCIOx8 connector for interconnection between HMC and BMC (To HMC board J21)

Baseboard Management Controller (BMC)



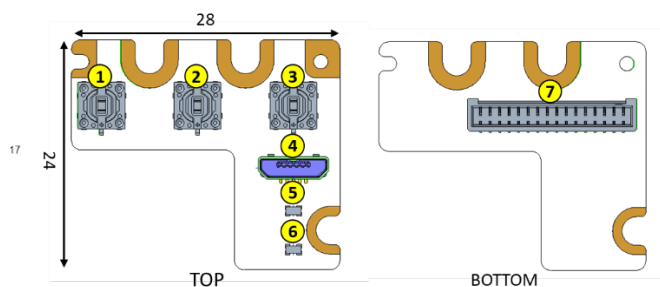
Item	Location	Description
1	CN2	DC-SCI (4C+) golden finger for plug-in on Interposer board

Front IO Board (FIO)



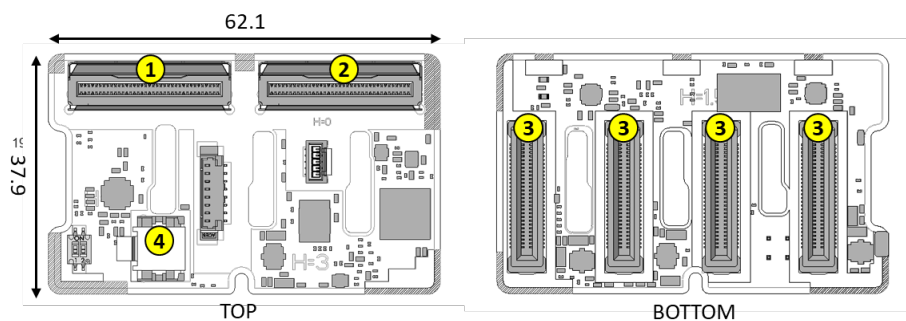
Item	Location	Description
1	J13	1GbE RJ45 connector for BMC OOB ethernet
2	J12	Mini-DP connector
3	J3	Wire-to-Board 16P connector for interconnection between FIO and Panel board
4	J9	SlimSAS connector for FIO cable connection on HPM
5	J1	Micro-Fit 2P connector for 12V standby power cable

FIO Panel Board



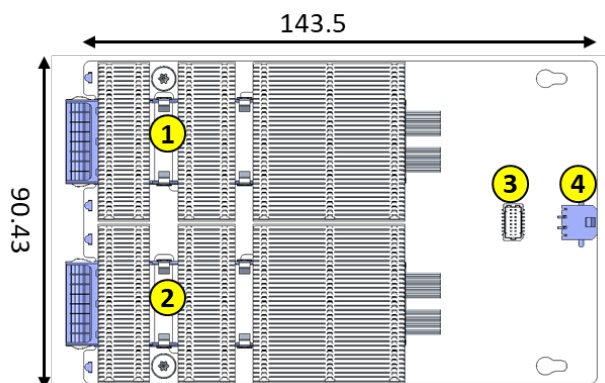
Item	Location	Description
1	SW1	Power button/LED switch
2	SW3	UID button/LED switch
3	SW2	Reset button switch
4	J8	Micro USB connector for CPU UART0 (COM) port
5	LED1	NVLink health status indicator LED
6	LED2	System fault status indicator LED
7	J1	Wire-to-Board 16P connector for interconnection between FIO and Panel board

E1.S Backplane Board



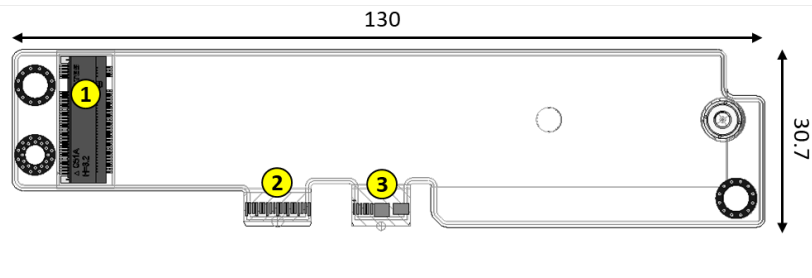
Item	Location	Description
1	J12	MCIOx8 connector for CX8 module connection (PCIe5 x8) (To CX8 module J4)
2	J11	MCIOx8 connector for CX8 module connection (PCIe5 x8) (To CX8 module J3)
3	J1, J2, J3, J4	4* EDSFF E1 connector for E1.S NVMe (PCIe5 x4)
4	J15	Micro-Fit 4P connector for 12V power cable

OSFP Board



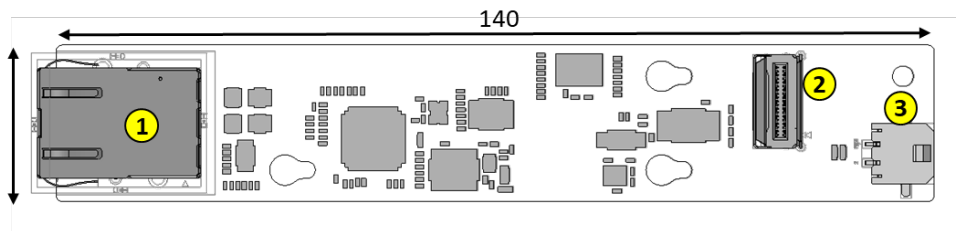
Item	Location	Description
1	J2	UltraPass cable assembly for CX-8 ASIC 0
2	J3	UltraPass cable assembly for CX-8 ASIC 1
3	J1	OSFP board sideband connector
4	JP1	Micro-Fit 2P connector for 12V power cable

M.2 Riser Board



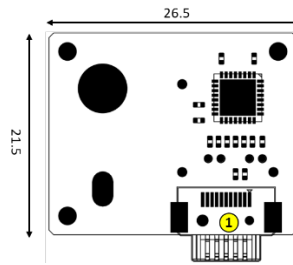
Item	Location	Description
1	J1	NGFF M.2 connector for M.2 NVMe (PCIe5 x4)
2	CN117	MCIOx4 golden finger for plug-in on HPM
3	CN23	Multi-Trak golden finger for 12V power connection

1G NIC Board



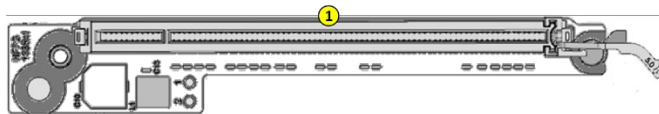
Item	Location	Description
1	J58	1GbE RJ45 connector for system OOB ethernet
2	J1	MCIOx4 connector for 1G NIC board cable connection on HPM (PCIe3 x1)
3	JP1	Micro-Fit 2P connector for 12V power cable

TPM Board



Item	Location	Description
1	J55	TPM board connector for plug-in on HPM

PCIe CEM Riser Board

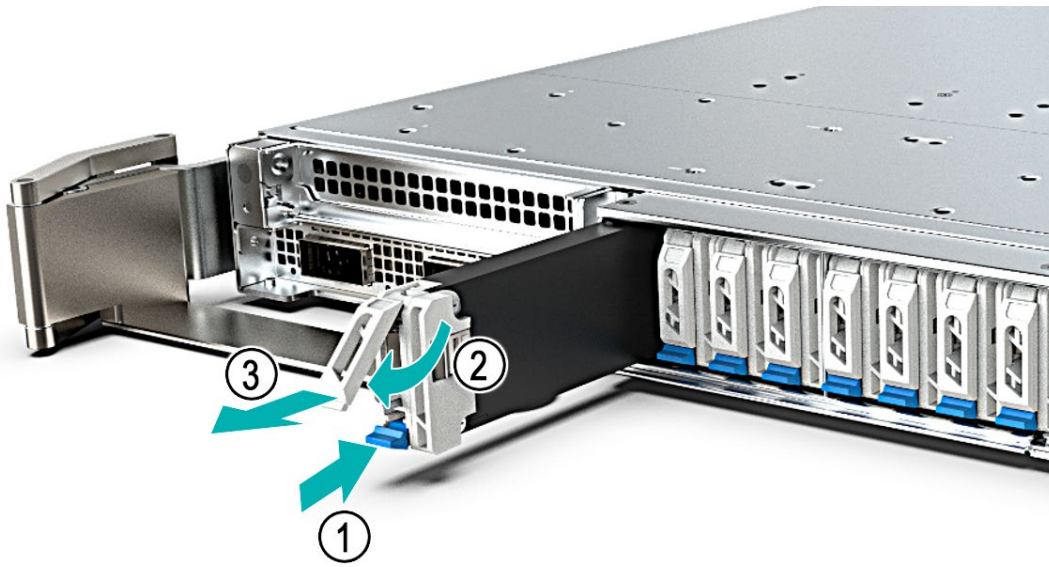


Item	Location	Description
1	J1	PCIe5 x16 connector (cable mount)

CRU Part Assembly Guide

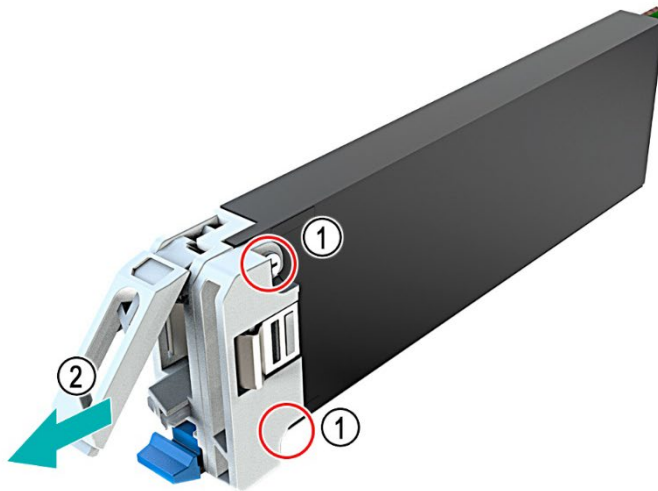
E1.S HDD Disassembly

- A. Remove the E1.s NVMe carrier assembly from the chassis:
1. Push the drive carrier button to disengage the drive carrier bezel.
 2. Pull the drive carrier bezel to detach the carrier assembly from the chassis.
 3. Remove the carrier assembly from the chassis.



B. Remove the E1.s NVMe drive from the carrier:

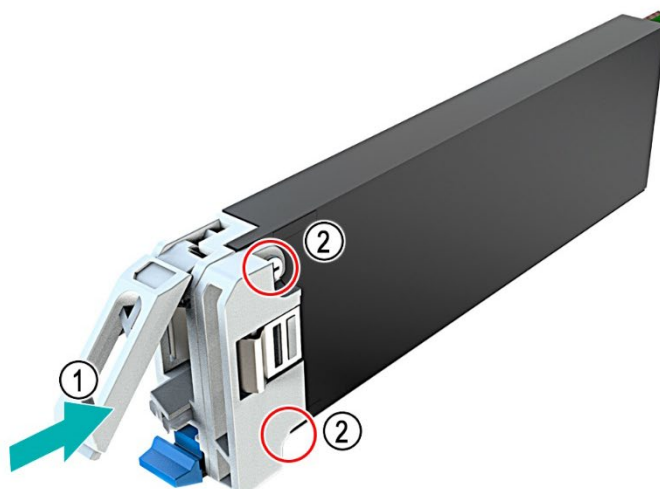
1. Remove the two screws.
2. Remove the E1.s NVMe drive from the carrier.



E1.S HDD Assembly

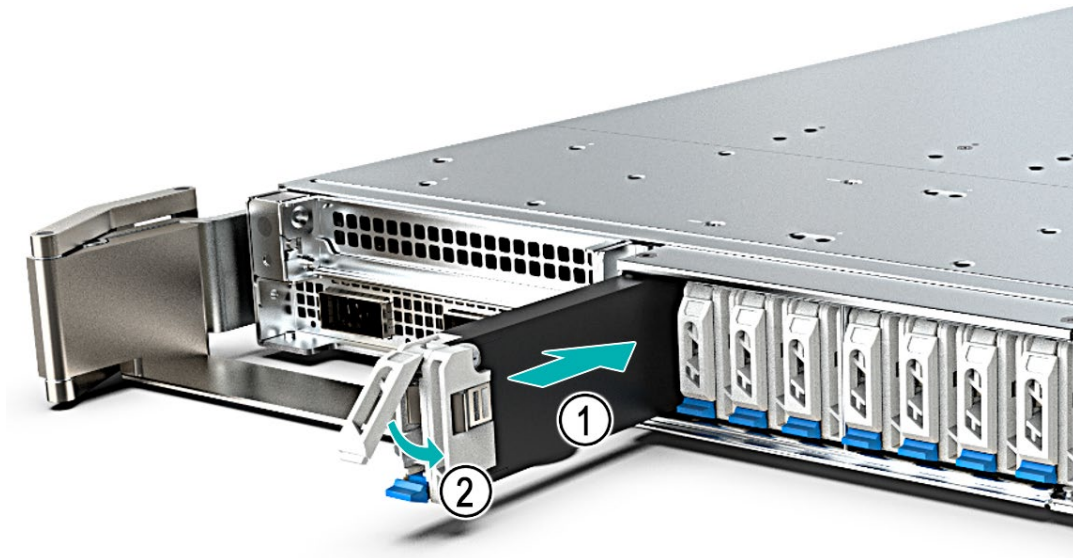
A. Install the E1.s NVMe drive to the carrier:

1. Place the E1.s NVMe drive into the chassis.
2. Use two screws to secure the E1.s NVMe drive to the carrier.



B. Install E1.s NVMe carrier assembly to the chassis:

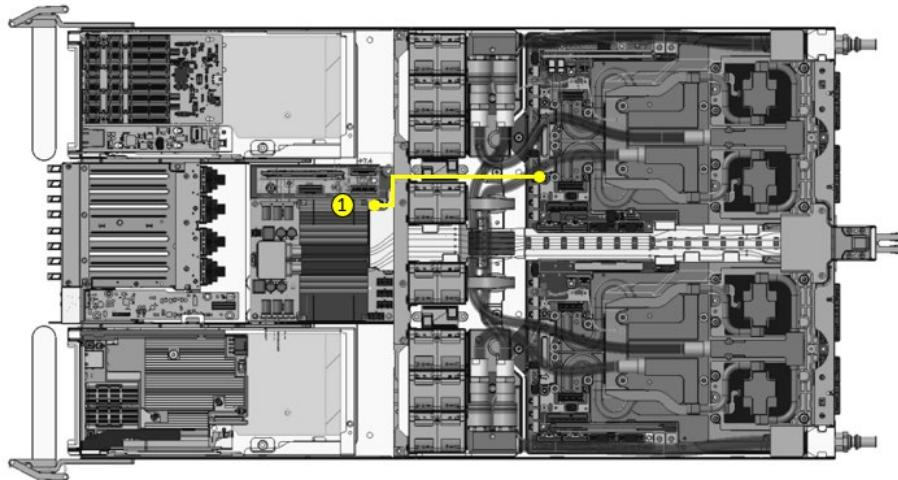
1. Place the E1.s NVMe carrier assembly into the chassis.
2. Push the carrier assembly into the chassis until it latches into place.



Cabling

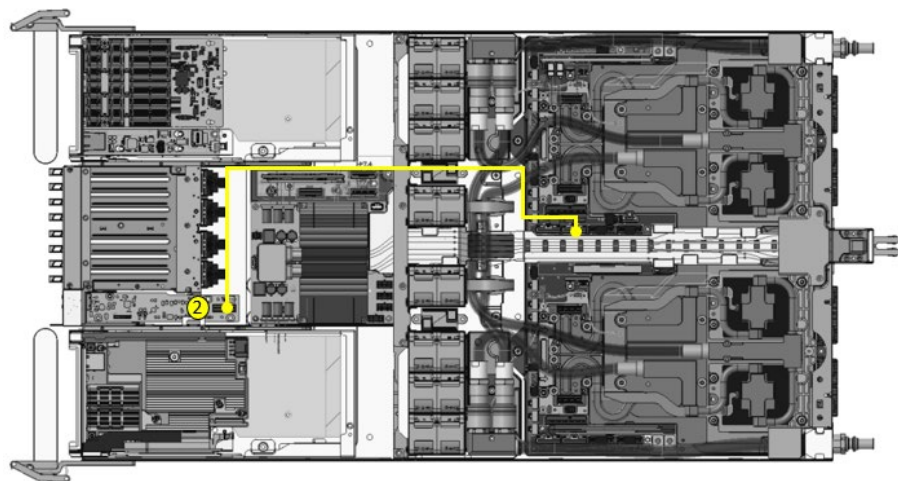
Compute Tray Signal Cable Connectivity

PDB Control Sideband Cable



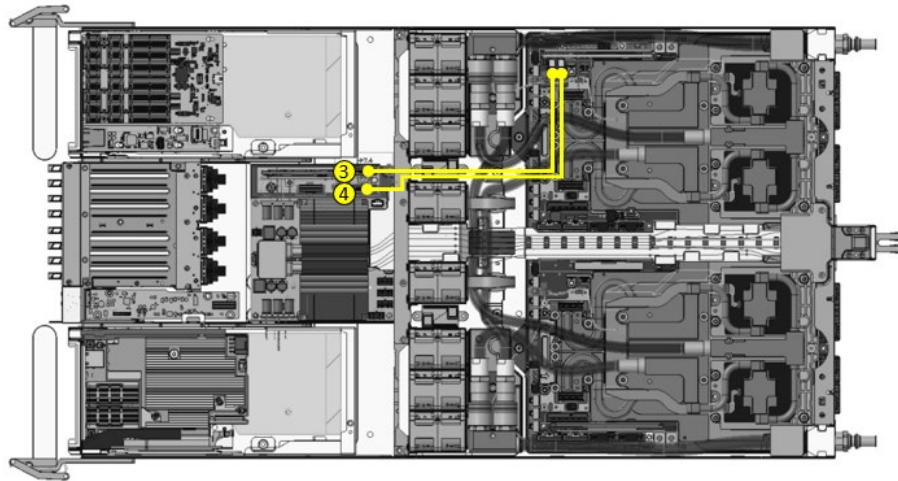
Item	Part No.	Source / Destination
1		HPM1 (JSB2) – PDB (J50)

Front IO Cable



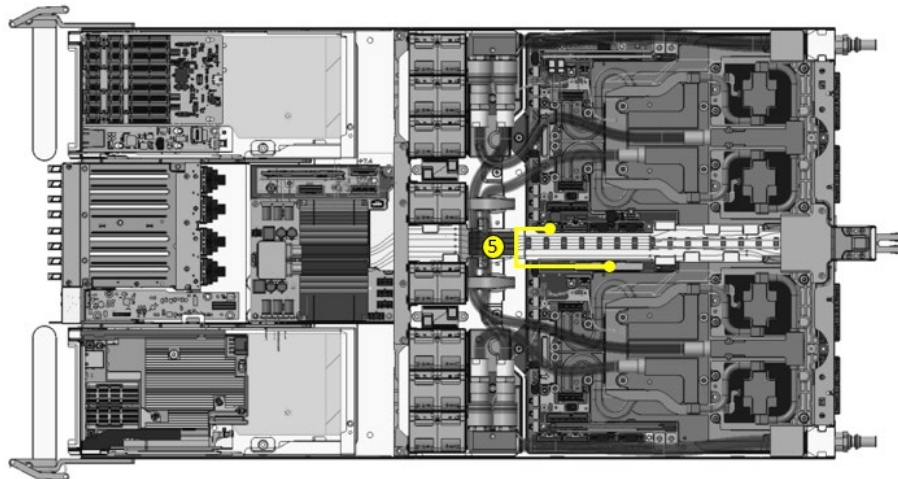
Item	Part No.	Source / Destination
2		HPM1 (J82) – Front IO board (J9)

HMC-BMC MCIO Cable



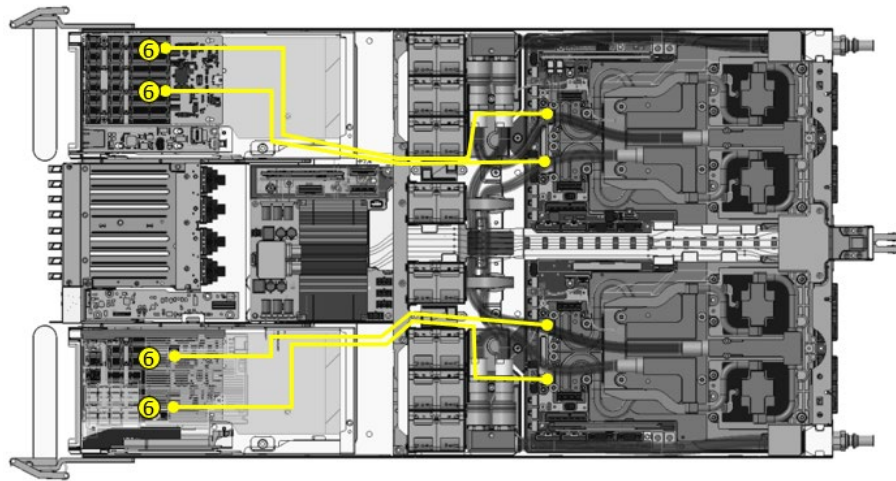
Item	Part No.	Source / Destination
3		HMC (J22) – BMC Interposer board (J4)
4		HMC (J21) – BMC Interposer board (J3)

2P Management Custom Cable



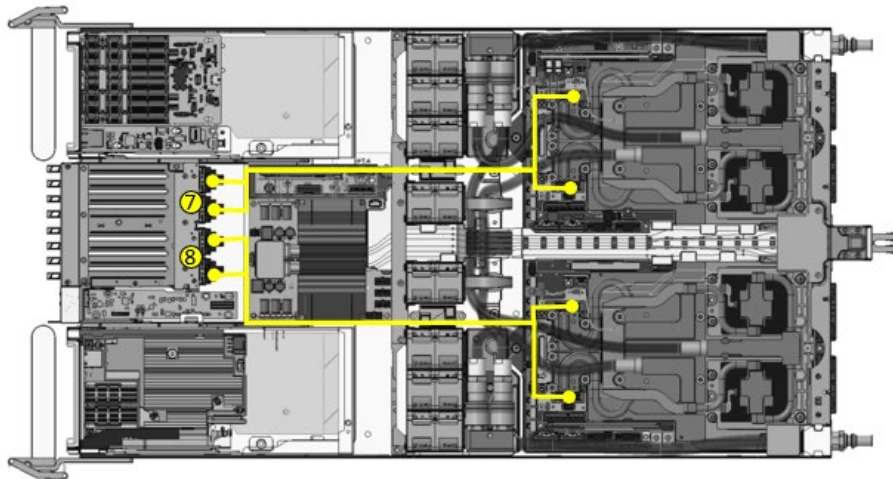
Item	Part No.	Source / Destination
5		HPM1 (J79) – HPM2 (J58)

Ultrapass Cable



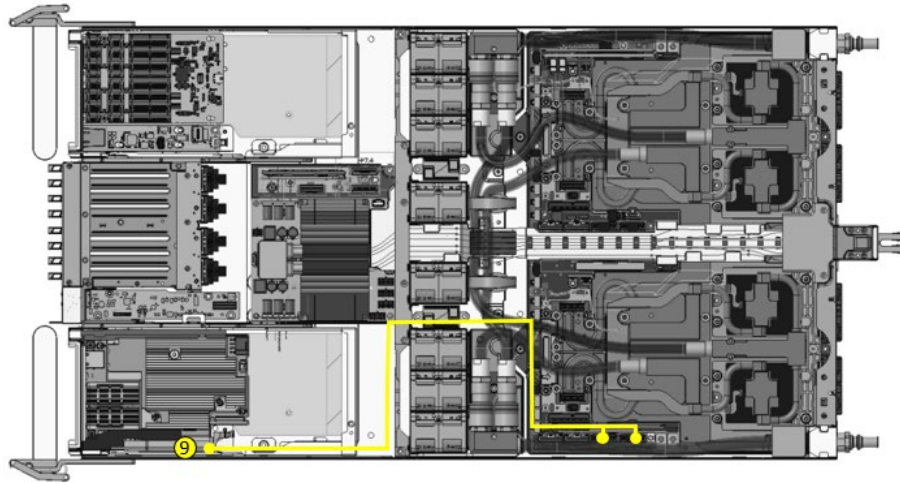
Item	Part No.	Source / Destination
6		ConnectX-8 Mezzanine Network board (Flyover Conn.) – OSFP board cable assembly

E1.S MCIO x8 Cable



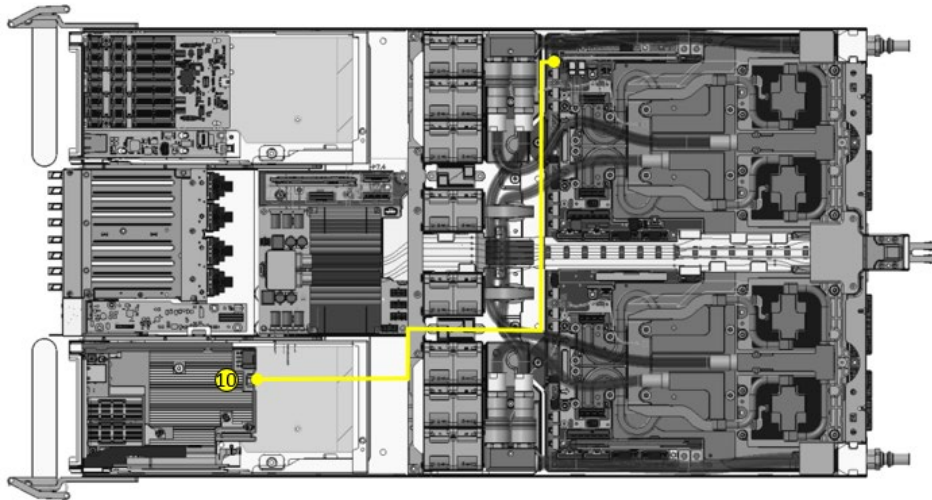
Item	Part No.	Source / Destination
7		CX8 module (J3/J4) – E1.S Backplane (J11/J12) (Left)
8		CX8 module (J3/J4) – E1.S Backplane (J11/J12) (Right)

PCIe CEM Riser Cable



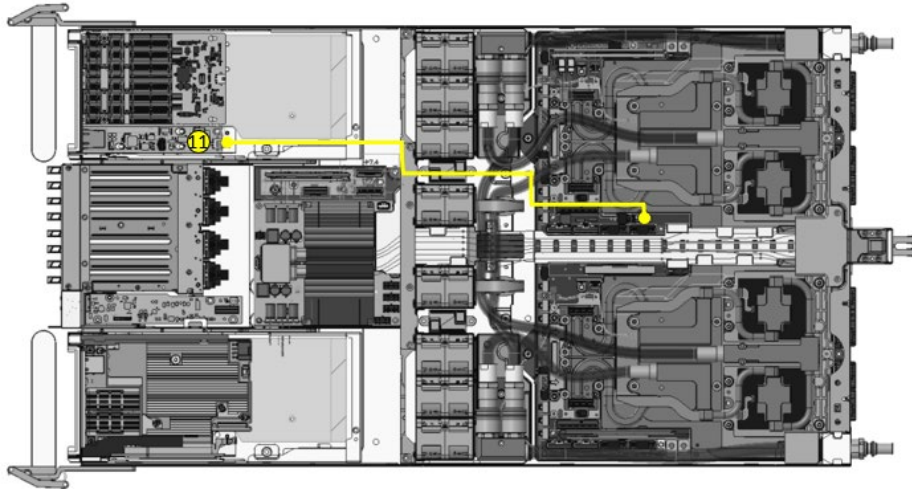
Item	Part No.	Source / Destination
9		HPM1 (J10/J80) – PCIe CEM Riser cable (Right)

BlueField-3 NCSI Cable



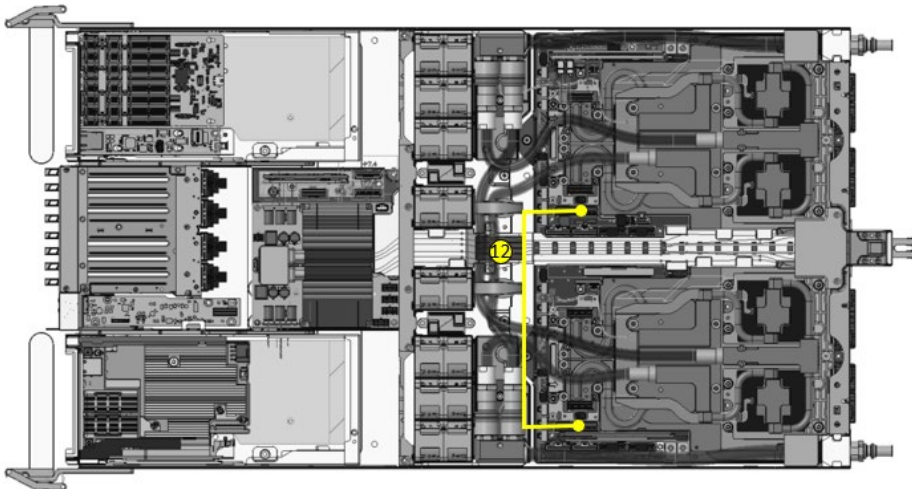
Item	Part No.	Source / Destination
10		HPM1 (J86) – BlueField-3 FHHL AIC NCSI

MCIO x4 to 1G NIC Cable



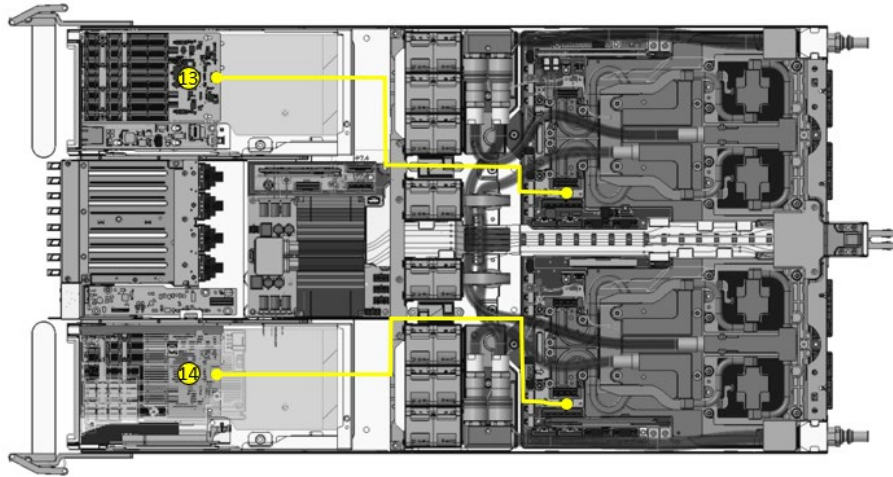
Item	Part No.	Source / Destination
11		HPM1 (J117) – 1G NIC board (J1)

C-Link Cable



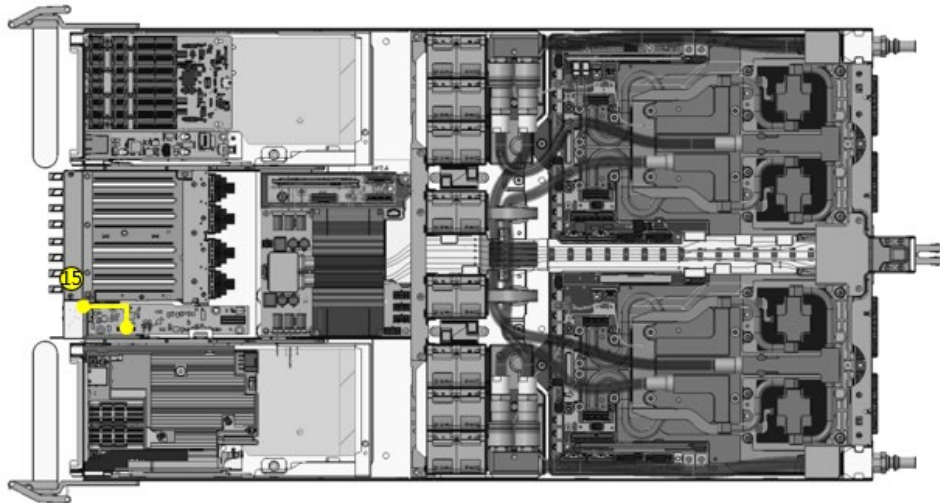
Item	Part No.	Source / Destination
12		HPM1 (J107) – HPM2 (J107)

OSFP Sideband Cable



Item	Part No.	Source / Destination
13		ConnectX-8 Mezzanine Network board – OSFP board (J1) (Left)
14		ConnectX-8 Mezzanine Network board – OSFP board (J1) (Right)

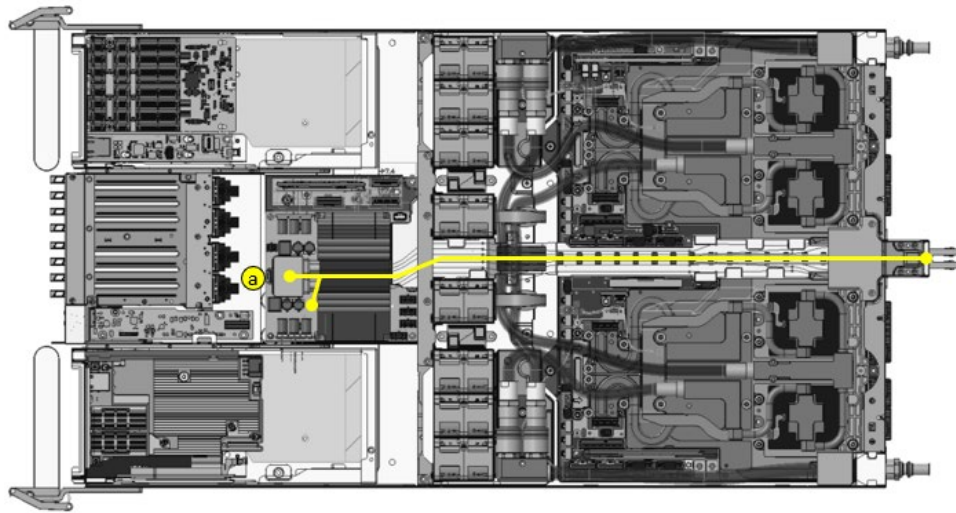
Front IO Panel Cable



Item	Part No.	Source / Destination
15		Front IO board (J3) – FIO Panel board (J1)

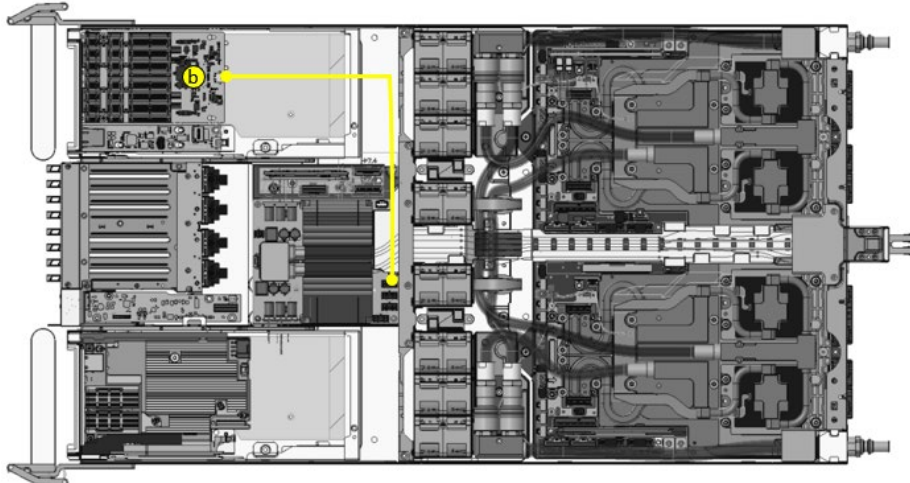
Compute Tray Power Cable Connectivity

54V Busbar Cable



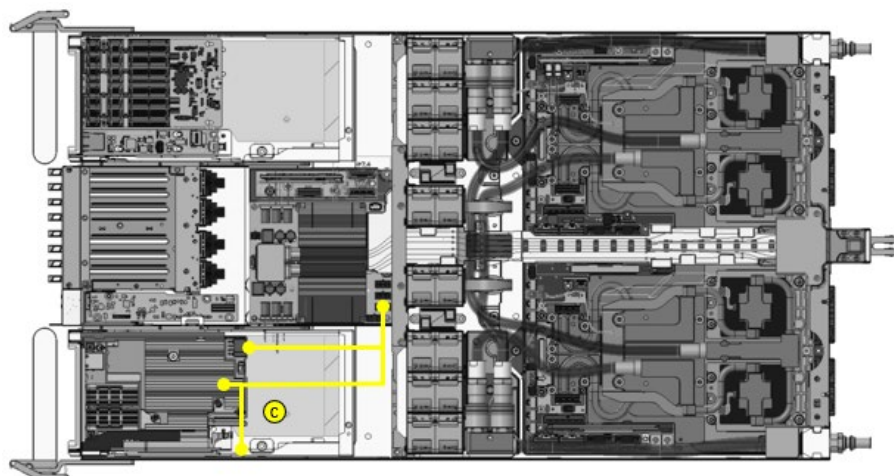
Item	Part No.	Source / Destination
a		Power Busbar Clip – PDB (J59)

12V Multi-end Power Cable: Left Tray



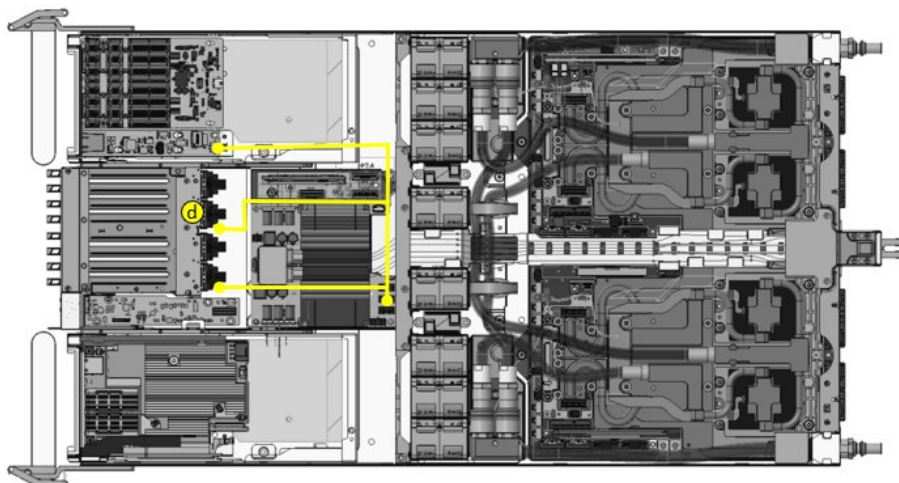
Item	Part No.	Source / Destination
b		PDB (J55) – OSFP board (JP1)

12V Multi-end Power Cable: Right Tray



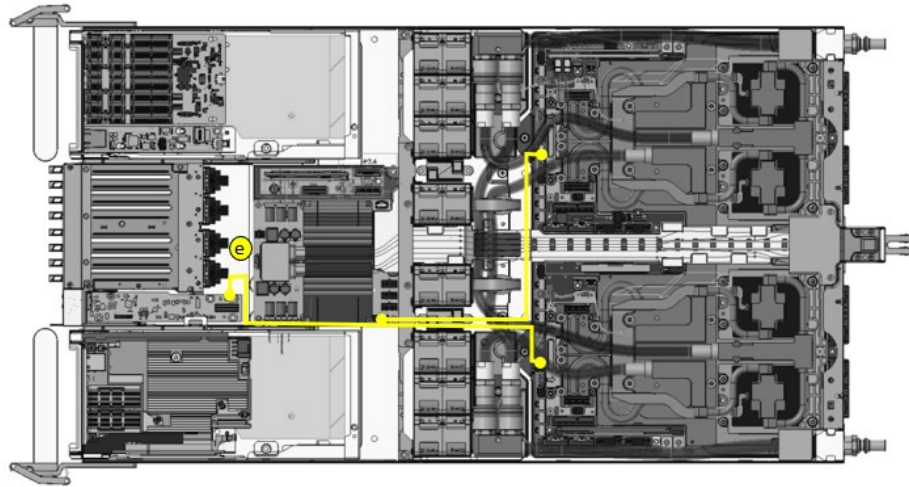
Item	Part No.	Source / Destination
c		PDB (J57) – OSFP board (JP1) – PCIe CEM Riser – BlueField-3 Ext.

12V Multi-end Power Cable: Middle Tray



Item	Part No.	Source / Destination
d		PDB (J56) – 1G NIC board (JP1) – E1.S Backplane (Left) (J15) – E1.S Backplane (Right) (J15)

MB 12V Standby Cable



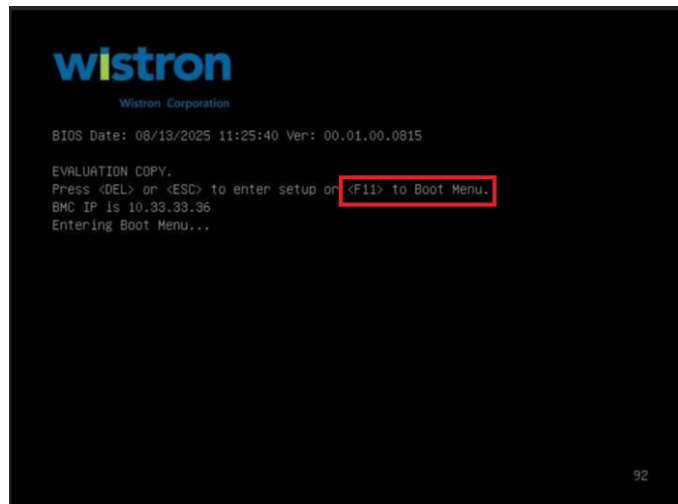
Item	Part No.	Source / Destination
e		PDB (J58) – Front IO board (J1) – HPM1 (J13) – HPM2 (J13)

System utilities

Boot Menu

Accessing the Boot menu screen

1. To access the Boot menu screen, turn on the server. If the server is already turned on, save your data and close all open applications, then restart the server.
2. During POST, press **F11** key to enter Boot menu.



NOTE: The server will take around 3 minutes from turning the power on, booting the system and loading system setup. If you fail to press F11 key before POST is completed, you will need to restart the server.

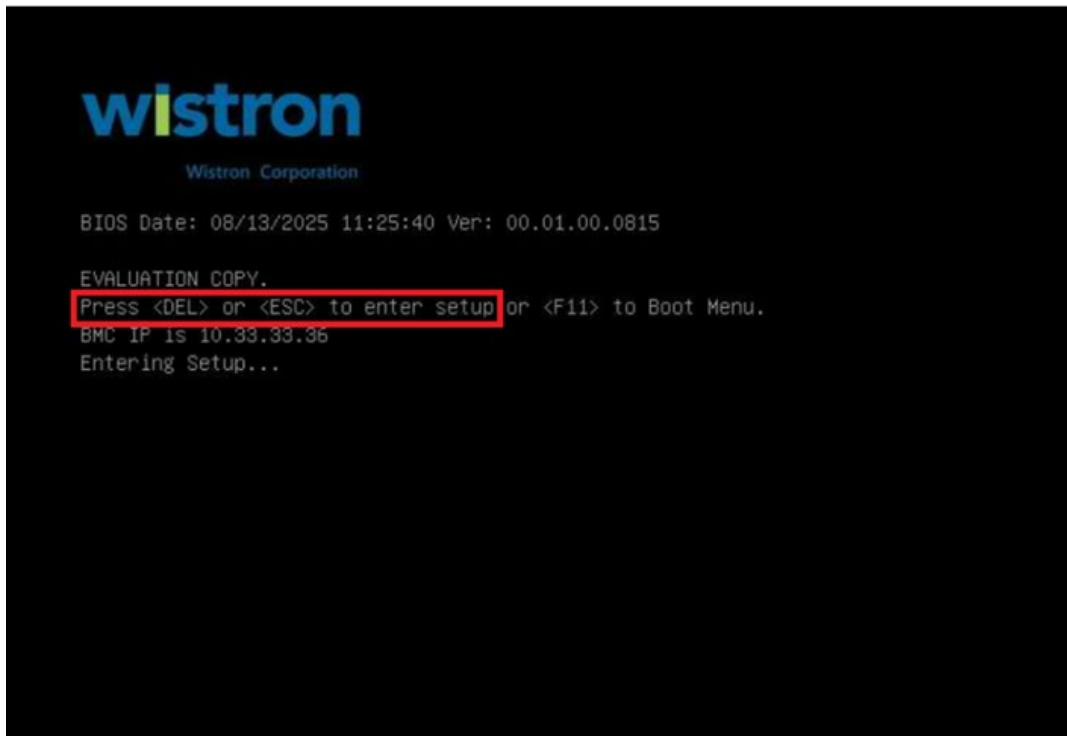


Use the Up/Down arrow keys to move between the menu options, then press **ENTER** to select boot device. Press **ESC** to boot using default device.

BIOS setup

Accessing the BIOS setup menu screen

1. To access the BIOS setup menu screen, turn on the server. If the server is already turned on, save your data and close all open applications, then restart the server.
2. During POST, press **DEL** or **ESC** key to enter BIOS setup menu.



NOTE: The server will take around 3 minutes from turning the power on, booting the system and loading system setup. If you fail to press **DEL** or **ESC** key before POST is completed, you will need to restart the server.



Use the Left/Right arrow keys to move between the menu screens, then press **ENTER** to view that menu tab.

Use the Up/Down arrow keys to move between the menu options, then press **ENTER** to execute that option.

Some options lead to pop-up dialog boxes that prompt you to verify that you wish to execute that option. Other options lead to dialog boxes that prompt you for information.

Some options (marked with a ►) lead to submenus that enable you to change the values for the option.

Use the Up/Down/Left/Right arrow keys to scroll through the items in the submenu.

Navigating the BIOS setup menu screen

Use the keys listed on the bottom right of the Setup screen to work your way through the various BIOS menu and submenu screens. The table below lists these keys and their respective functions.

Key	Function
Left / Right arrow keys	Move the cursor to the menu screen you want. The currently selected screen will be highlighted and the items it contains will be shown.
Up / Down arrow keys	Move the cursor to the item you want. The currently selected field will be highlighted.
Enter	• To open the page for the currently selected menu/submenu • To apply a field value.
+ / - keys	To select a value for the currently selected field (only if it is user-configurable). Press these keys repeatedly to display all possible entries. A parameter that is enclosed in square brackets [] is user-configurable. Black font parameters are not user-configurable for one of the following reasons: • The field value is auto-configured or auto-detected. • The field value is informational only. • The field is password-protected.
F1	To bring up the General Help window. The General Help window describes other setup navigation keys that are not displayed on the legend bar.
F2	Restore the saved User Default settings.
F3	Load optimized default system values.
F4	Save and exit the BIOS setup screen.
Esc	If you press this key: • On one of the primary menu screens, the Exit menu displays. • On a submenu screen, the previous screen displays. • When you are making selections from a pop-up menu, closes the pop-up without selecting.

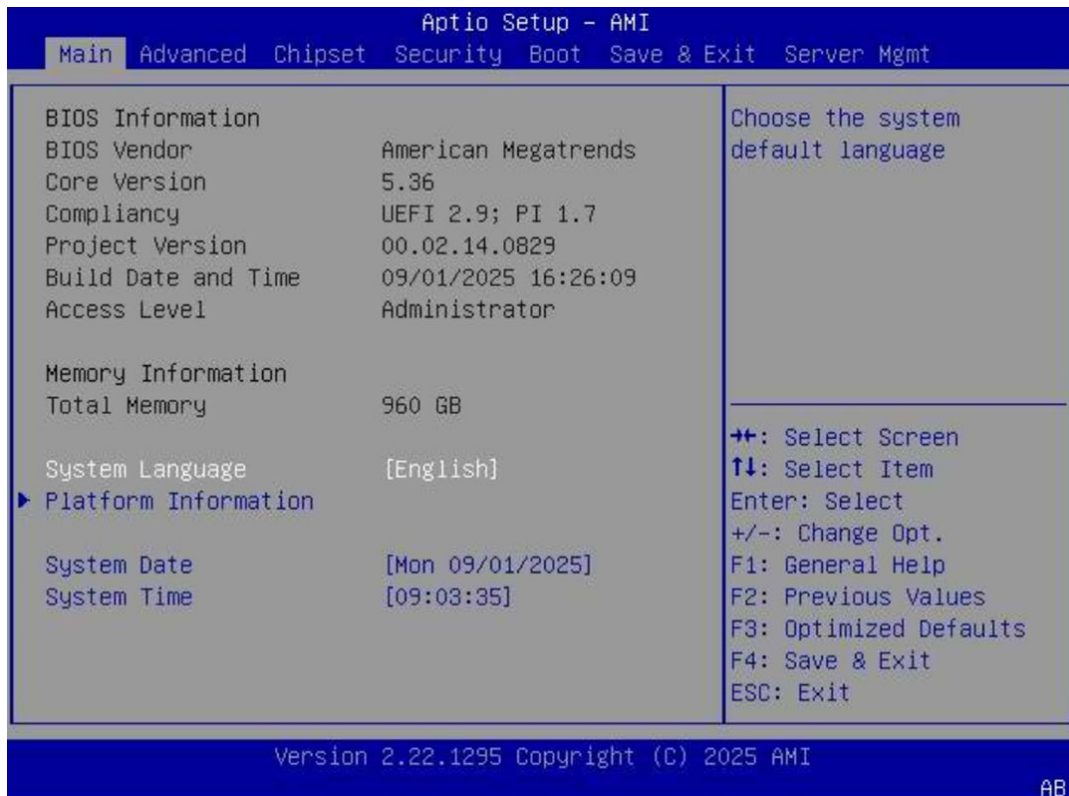
Remote Flash BIOS

To remotely flash BIOS on the NML72-GB300 Server, contact your Penguin Solutions Service Representative for complete step-by-step instructions.

BIOS setup menu screen

NOTE: The screenshots used in this section are for illustration only. The values displayed may not be the same as those on your server. In the descriptive tables following each of the menu screen illustrations, settings in **boldface** are the default and suggested settings.

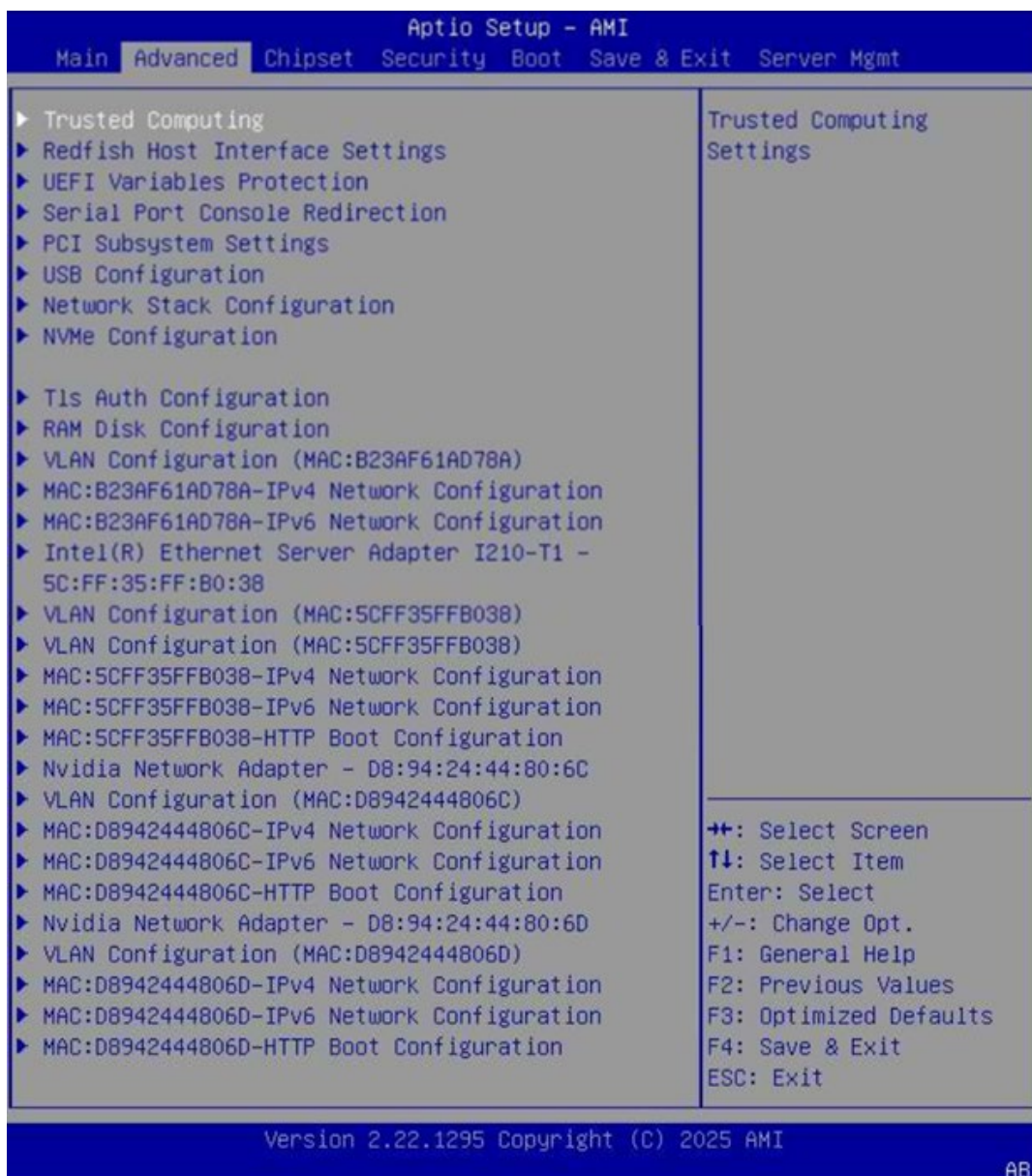
Main menu



Parameter	Description	Value
BIOS Information		
BIOS Vendor	BIOS Vendor	American Megatrends
Core Version	Current system Core version.	5.36
Compliance	BIOS compliance information.	UEFI 2.9; PI 1.7
Project Version	Official project version code of the server.	
BIOS Build Date and Time	Date when the system BIOS was built.	09/01/2025 16:26:09

Access Level	Current access level of the logged-in user.	Administrator
Memory Information		
Total Memory	Size of system memory detected during boot-up.	Total Memory: 960 GB
System Language	Choose the system default language	English
System Date	Set the Date. Use Tab to switch between Data elements. Default Ranges: Year: 1998-9999 Months: 1-12 Days: dependent on month Range of Years may vary	[Mon 09/01/2025]
System Time	Set the Time. Use Tab to Switch between Time elements.	[09:03:35]

Advanced menu



Parameter	Description
Trusted Computing	Trusted Computing Settings
Redfish Host Interface Settings	Redfish Host Interface Parameters
UEFI Variables Protection	NVRAM Runtime Variable Protection Settings

Serial Port Console Redirection	Serial Port Console Redirection
PCI Subsystem Settings	PCI Subsystem Settings
USB Configuration	USB Configuration Parameters
Network Stack Configuration	Network Stack Settings
NVMe Configuration	NVMe Device Options Settings
Tls Auth Configuration	Press <Enter> to select Tls Auth Configuration.
RAM Disk Configuration	Press <Enter> to add/remove RAM disks.
VLAN Configuration	VLAN Configuration
MAC: -IPv4 Network Configuration	Configure network parameters
MAC: -IPv6 Network Configuration	Configure IPv6 network parameters
Intel(R) Ethernet Server Adapter	Configure Gigabit Ethernet device parameters
Nvidia Network Adapter	Configure Device parameters

Chipset menu



Parameter	Description
NVIDIA Configuration	NVIDIA Configuration
CPU Information	CPU Information

Security menu

Aptio Setup - AMI

Main Advanced Chipset **Security** Boot Save & Exit Server Mgmt

Disable Block Sid and Freeze Lock [Disabled]

Password Description

If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.
 If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.
 The password length must be in the following range:
 Minimum length 3
 Maximum length 20

Administrator Password
 User Password

► Secure Boot

TCG Storage Security Configuration:

► SAMSUNG M2TL63T8HFLT-00AW7
 ► SAMSUNG M2TL63T8HFLT-00AW7
 ► SAMSUNG M2TL63T8HFLT-00AW7
 ► SAMSUNG M2TL63T8HFLT-00AW7
 ► SAMSUNG M21L21T9HCLS-00A07

Override to allow SID authentication of TCG Storage device and to skip freeze lock command for SAT3 device. Modified value will be applicable only for next boot.

↔: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

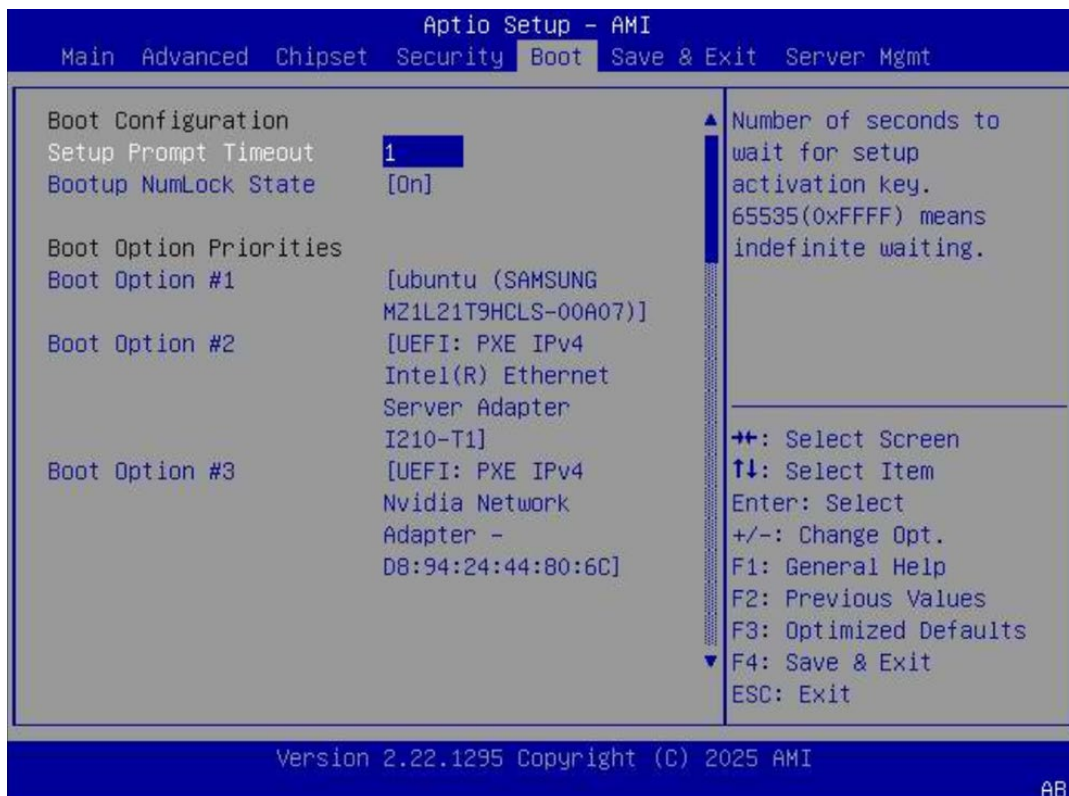
Version 2.22.1295 Copyright (C) 2025 AMI

AB

Parameter	Description	Value
Disable Block Sid and Freeze Lock	Override to allow SID authentication of TCG Storage device and to skip freeze lock command for SAT3 device. Modified value will be applicable only for next boot.	Disabled Enabled
Administrator Password	Set Administrator password.	
User Password	Set User Password.	

Secure Boot	Secure Boot configuration	
TCG Storage Security Configuration	TCG Storage Security Configuration	

Boot menu



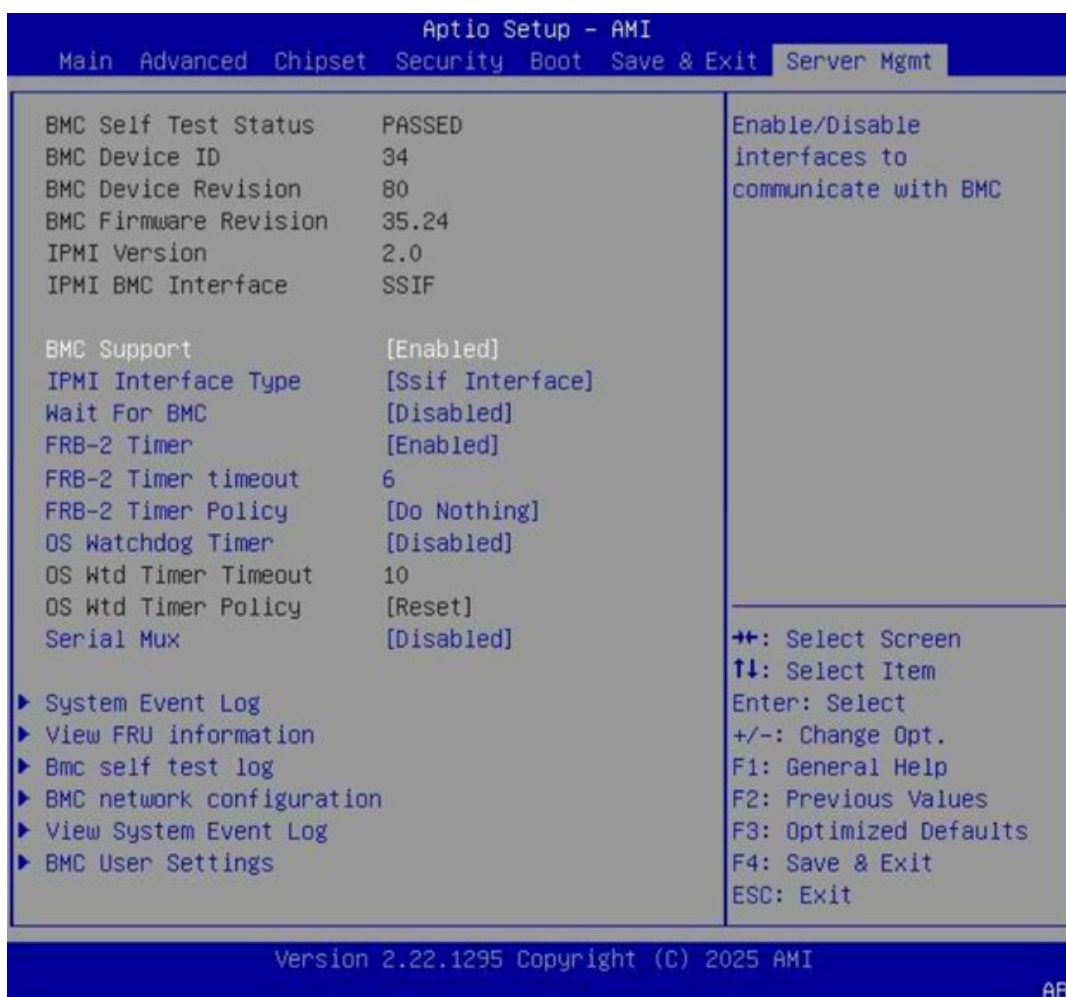
Parameter	Description	Value
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.	1
Bootup NumLock State	Select the keyboard NumLock state	On Off
Boot Option #	Sets the system boot order	
Fast Boot	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.	Disabled Enabled

Save & Exit menu



Parameter	Description
Save Changes and Exit	Exit system setup after saving the changes.
Discard Changes and Exit	Exit system setup without saving any changes.
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes and Reset	Reset system setup without saving any changes.
Save Changes	Save Changes done so far to any of the setup options
Discard Changes	Discard Changes done so far to any of the setup options
Restore Defaults	Restore/Load Default values for all the setup options.
Save as User Defaults	Save the changes done so far as User Defaults.
Restore User Defaults	Restore the User Defaults to all the setup options.

Server Management menu



Parameter	Description	Value
BMC Support	Enable/Disable interfaces to communicate with BMC	Enabled Disabled
IPMI Interface Type	Type of Interface to communicate BMC from HOST	Ssif Interface
Wait For BMC	Wait For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.	Enabled Disabled
FRB-2 Timer	Enable or Disable FRB-2 Timer (POST timer)	Enabled Disabled

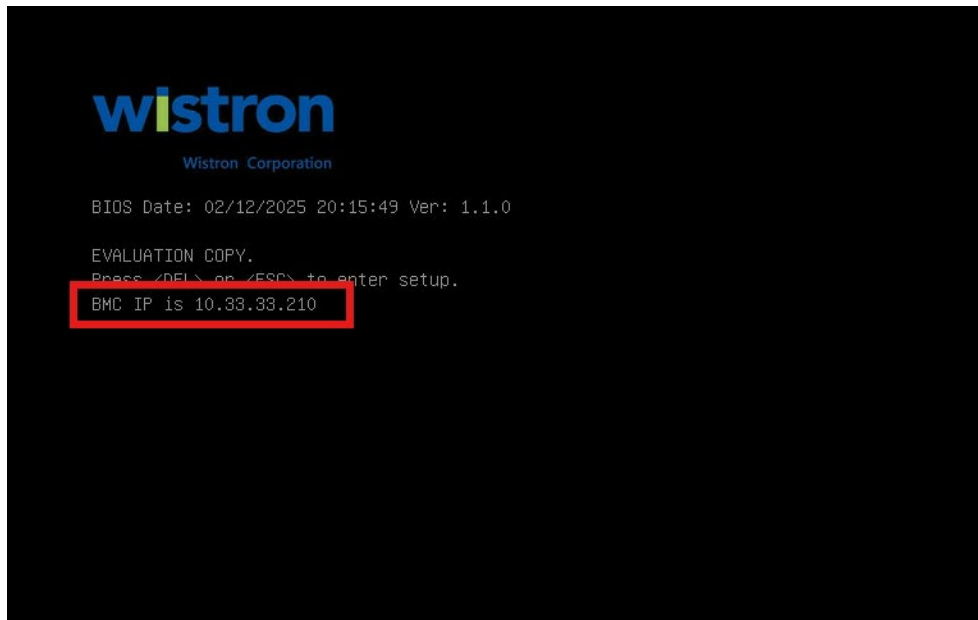
FRB-2 Timer timeout	Enter value Between 1 to 30 min for FRB-2 Timer Expiration	6
FRB-2 Timer Policy	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.	Do Nothing Reset Power Down Power Cycle
OS Watchdog Timer	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.	Enabled Disabled
OS Wtd Timer Timeout	Enter the value Between 1 to 30 min for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.	10
OS Wtd Timer Policy	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.	Do Nothing Reset Power Down Power Cycle
Serial Mux	Press <Enter> to enable or disable Serial Mux configuration.	Enabled Disabled
System Event Log	Press <Enter> to change the SEL event log configuration.	
View FRU information	Press <Enter> to view FRU information.	
Bmc self test log	logs the report returned by BMC self test command	
BMC network configuration	Configure BMC network parameters.	
View System Event Log	Press <Enter> to view the System Event Log Records	
BMC User Settings	Press <Enter> to Add, Delete and Set Privilege level for users.	

BMC User Interface

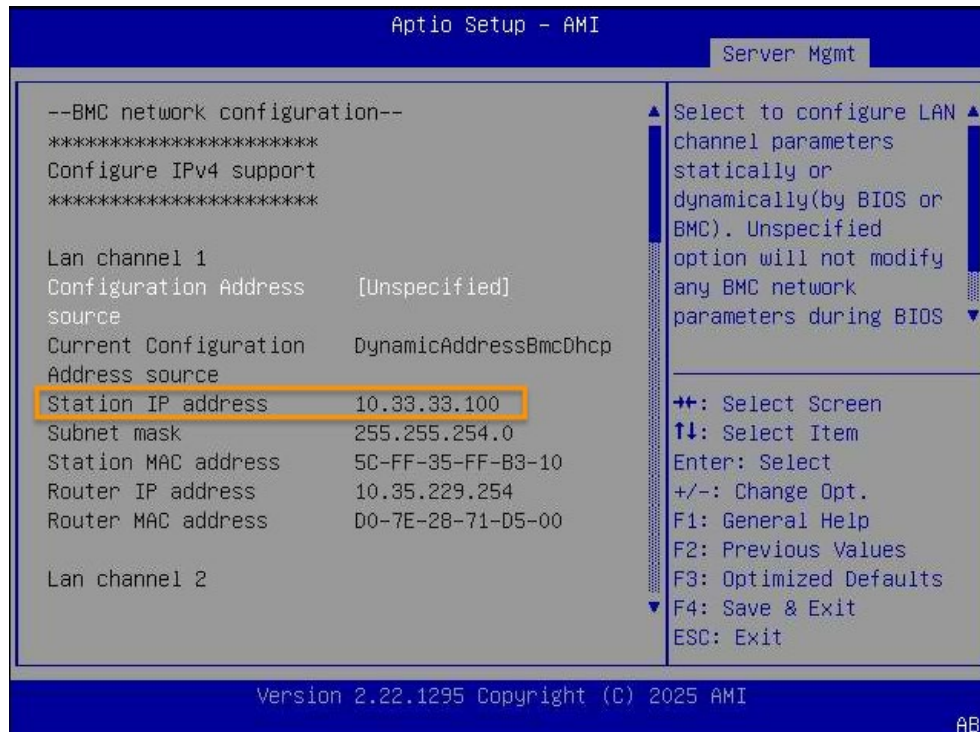
Get BMC IP

This section describes how to get the BMC IP during POST, from the BIOS Setup menu, and from the OS in-band command.

To get BMC IP during POST:



To get BMC IP from BIOS Setup Menu, go to **BIOS Setup Menu > Server Mgmt > BMC network configuration**:



To get the BMC IP using the OS in-band command:

IPMI Command format:

```
ipmitool lan print
```

```
root@PS:~# ipmitool lan print
Set in Progress      : Set Complete
Auth Type Support    :
Auth Type Enable     : Callback :
                    : User      :
                    : Operator  :
                    : Admin    :
                    : OEM       :
IP Address Source    : DHCP Address
IP Address           : 10.35.229.148
Subnet Mask          : 255.255.254.0
MAC Address          : 5c:ff:35:ff:b1:e7
SNMP Community String : public
BMC ARP Control      : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl : 2.0 seconds
Default Gateway IP    : 10.35.229.254
Default Gateway MAC   : d0:7e:28:71:d5:00
Backup Gateway IP     : 0.0.0.0
Backup Gateway MAC    : 00:00:00:00:00:00
802.1q VLAN ID       : Disabled
802.1q VLAN Priority  : 0
RMCP+ Cipher Suites  : 17
Cipher Suite Priv Max : aaaaaaaaaaaaaa
                    : X=Cipher Suite Unused
                    : c=CALLBACK
                    : u=USER
                    : o=OPERATOR
                    : a=ADMIN
                    : O=OEM
```

Web GUI

The web GUI is HTML5 based and added security with SSL (HTTPS).

Function		Description
Overview	BMC time	Show current time and SOL console shortcut link
	System Information	Show the information of Server, Firmware, Network and power
	Status information	Show the total number of critical and warning events and System identify LED
Dashboard	Virtual front panel	Simulate Front Panel LED status
	Date and time	Show current UTC time
	Current user	Show current user information
	Virtual media	Show the status of virtual media
	Screen Preview	TBD
	System Information	Show the information of the BMC system
	Networks	Show the NIC_0 / NIC_1 information
	Temperature	Show the healthy status of the sensors
	Voltage	Show the healthy status of the voltage
	Fan	Show the healthy status of the fan
	System event log	Show the asserted event log
	Power Statistics	Show the wattage of all the subsystem
Logs	Event Logs	Show the event log page. Will display all the event logs that have occurred in this device.
	System event log	System Log page will display all the system events that have occurred in this device that have been already configured.
	POST code	The POST code comparison with current boot and previous boot
	SOL log	
	BIOS log	

	Host video recorder	
	System diagnostics	
Hardware status	System information	
	FRU information	
	CPU information	
	DDR information	
	Inventory and LEDs	
	Sensor readings	
	NIC information (BIOS)	
	NIC information (BMC)	
	NVME/HDD information (BIOS)	
	NVMe information (BMC)	
	System Component	
	SMBIOS	
Operations	Factory reset	
	KVM	
	Firmware	This page shows the version of BMC and component firmware. Provide update firmware function by web.
	Reboot BMC	BMC Reboot function
	SOL console	SOL console redirects the server's serial port output to this window.

	Server power operations	
	Virtual front panel	This page shows the power status of the server.
	Virtual Media	
	Boot config	
Settings	Alerts	
	Alert policies	
	Alert email	
	Date and time	
	Networks	
	VLAN	
	SOL	
	SNMP	
	IKVM and virtual media	
	Dynamic DNS	
	Syslog settings	
	Backup restore	
	Power restore policy	
Security and access	Current users	
	LDAP	
	RADIUS	
	TACACS+	
	Users	
	Policies	
	Certificate management	
	Kerberos authentication	
	Security settings	

	IP access control	
Remote Control	Power	
	Power statistics	
	Power schedule	
BIOS		

Log in

Initial access of BMC prompts you to enter the Username and Password. A sample screenshot of the login screen is given below.

 Please Login Username Password ☐ Remember Username Forgot Password? Log in	Default User Name and Password Username: root Password: OpenBmc Warning: Once you log in to the application, it is recommended not to use the following options. - Refresh button of the browser - Refresh menu of the browser - Back and Forward options of the browser - F5 on the keyboard - Backspace on the keyboard
---	---

Menu Bar (row)

The **Menu Bar** is located at the **top-right corner** of the Web UI and provides quick access to essential functions, status indicators, and user account controls.



Below is an explanation of each icon/button, starting from **left to right**:

Item	Description
Logo	Click the Logo to navigate to the Overview page.
Health	Click this icon to navigate to Logs -> Event logs page. The icon will change based on the severity status of current event logs. Leveling as Critical/ Warning/ OK.
Power	Click this icon to navigate to Operation -> Server power operations page. Status should be On or Off.
Refresh	Click the icon to reload the current page.
User	Clicking this area will show two options: Profile settings: Click to navigate to Profile settings page. Please refer to section 1.3.2 Profile settings. Log out: Click to log out of Web UI.

Profile Settings

Profile settings

Profile information

Username
root

Change password

New password

Password must be between 13 – 20 characters

Confirm new password

Timezone display preference

Select how time is displayed throughout the application

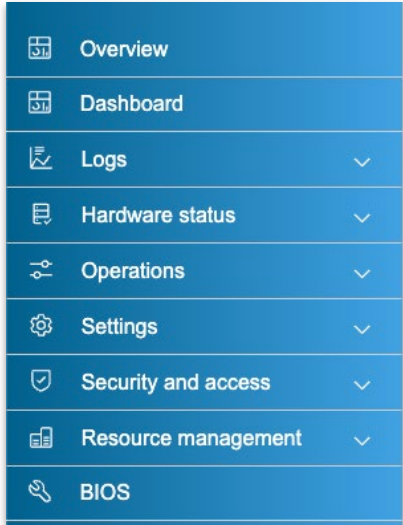
Timezone

- ☒ Default (UTC)
- ☐ Browser offset (台北標準時間 UTC+8)

Save settings

Menu Bar (column)

The menu bar displays the following.

• Overview • Dashboard • Logs • Hardware status • Operations • Settings • Security and access • Resource management • BIOS	
--	--

Overview

The **Overview** provides a quick summary of the system's information, current status, and a shortcut to the SQL console. From this page, users can quickly assess system information, status information, BMC time, monitor activities, and navigate to related management functions. Firmware Information will be displayed with the latest version, date and time details.

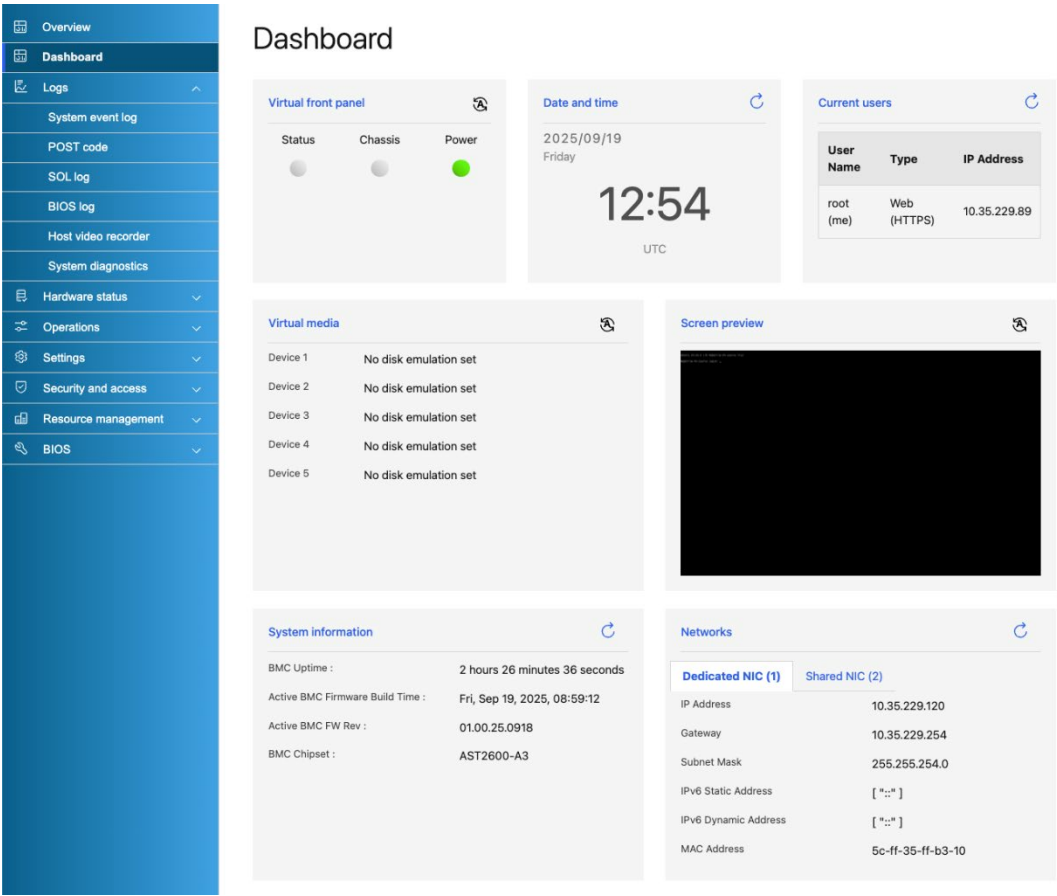
The screenshot shows the 'Overview' page of the Penguin Solutions management interface. On the left is a blue sidebar with navigation links: Overview, Dashboard, Logs (expanded), System event log, POST code, SOL log, BIOS log, Host video recorder, System diagnostics, Hardware status, Operations, Settings, Security and access, Resource management, and BIOS. The main content area is titled 'Overview' and contains several sections: 1. BMC time: 2025-09-19 13:12:39 UTC, with a 'SQL console' button. 2. System information: Four cards for Server information (Model: GB200 NVL, Serial number: R550EU03D005WWSSSSM, MVV), Firmware information (Running: 01.00.25.0918, Backup: ---), Network information (Hostname: nvidia-obmc, Link status: LinkUp, IPv4: ---, DHCPv4: 10.35.229.120), and Power information (Power consumption: CPU0 220.34605212072128 W, CPU1 240.09141158096202 W, Power cap: CPU0 2900 W, CPU1 2900 W). 3. Status information: Two cards. 'Event logs' shows 0 Critical (red X) and 0 Warning (yellow exclamation mark) events, with links for 'Export all' and 'View more'. 'Inventory and LEDs' shows 'System identify LED' is 'Off'.

Item	Description
BMC Time	Displays the current BMC time in UTC
	Provides a shortcut link to open the SOL console
System Information	Server Information: Shows details such as model and serial number of the server.
	Firmware Information: Displays the current version of the BMC and component firmware (running and backup versions).
	Network Information: Provides network details, including hostname, link status, and IP address configuration.
	Power Information: Shows power consumption and power cap settings
Status Information	Event Logs: Displays the number of critical and warning events. Users can export or view detailed logs

	Inventory and LEDs: Shows the state of the system identify LED, which can be toggled on or off to locate the server physically
--	---

Dashboard

The Dashboard provides a centralized view of the system’s current status, active connections, and important operational controls. From this page, users can quickly assess hardware conditions, monitor activities, and navigate to related management functions.



Field Name	Description
Virtual Front Panel	Navigation: <i>Operations → Virtual Front Panel</i> Displays the live status of key front panel indicators: • Status LED – Shows the system’s overall health condition. • Chassis LED – Indicates chassis identification or alert status. • Power LED – Displays whether the system is powered on or off. These LEDs mirror the physical front panel indicators, allowing administrators to verify hardware states remotely without direct physical access.

DateTime	Shows the current system date and time in UTC format. Maintaining accurate time is critical for system logs, scheduled tasks, and event tracking.
Current Users	Navigation: <i>Security and Access</i> → <i>Current Users</i> Lists all users currently connected to the BMC interface, along with their connection details: • User Name – The account currently logged in. • Type – The connection method used: ○ Web (HTTPS) – Standard secure web browser connection. ○ IKVM – Integrated Keyboard, Video, and Mouse session. ○ VM – Virtual Media session. ○ Redfish – Connection via the Redfish API. • IP Address – The source IP address of the connection. This helps administrators monitor access and detect unauthorized sessions in real time.
Virtual Media	Navigation: <i>Operations</i> → <i>Virtual Media</i> Displays the current status of all virtual media devices (e.g., virtual CD/DVD, USB drives). This section shows which devices are mounted, making it easy to confirm or troubleshoot virtual media operations.
Screen Preview	Navigation: <i>Operations</i> → <i>KVM</i> Provides a thumbnail preview of the host system's screen. This feature allows quick visual checks of the host's operating state without launching a full KVM session, saving time when monitoring multiple systems.

Logs

Logs are a critical component of the BMC system, providing detailed information about system operation status, errors, and warnings through various log types. Each log has its specific purpose, helping administrators monitor, troubleshoot, and diagnose the system at different levels. These logs are crucial for maintaining system stability, improving fault diagnosis efficiency, and ensuring hardware health.

Event logs

The event logs capture various changes and critical events related to the server's hardware status, offering detailed insights for monitoring and troubleshooting. These logs assist system administrators in promptly identifying hardware issues, diagnosing failures, and enhancing the server's stability and reliability. They cover a range of events, including hardware status changes, system startups and shutdowns, sensor data, firmware updates, and error warnings, enabling administrators to efficiently track the server's performance and take appropriate actions.

	ID	Severity	Date	Description	Status
▼	1748254949	Warning	2025-05-26 10:22:29 UTC	Service xyz.openbmc_project.ncsidaemon.service has exited unsuccessfully.	Unresolved
▼	1748252992	Warning	2025-05-26 09:49:52 UTC	Service xyz.openbmc_project.ncsidaemon.service has exited unsuccessfully.	Unresolved
▼	1748252870	Warning	2025-05-26 09:47:50 UTC	Service pldmd.service has exited unsuccessfully.	Unresolved
▼	1748252661	Warning	2025-05-26 09:44:21 UTC	Service pldmd.service has exited unsuccessfully.	Unresolved
▼	1748249347	Warning	2025-05-26 08:49:07 UTC	Service xyz.openbmc_project.ncsidaemon.service has exited unsuccessfully.	Unresolved

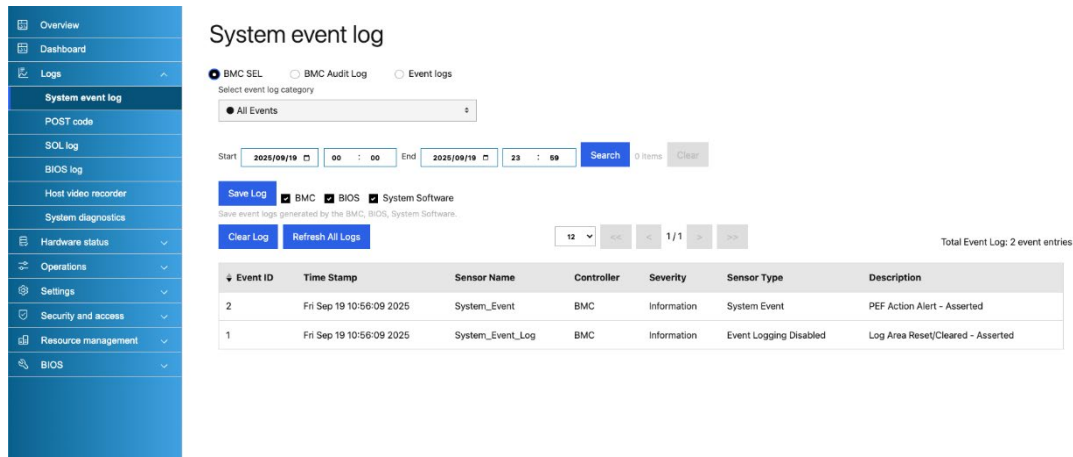
Displays all system-generated events with details such as:

- **ID:** Unique identifier for each log entry.
- **Severity:** Indicates the level of importance (e.g., Critical, Warning, or Informational).
- **Date:** Timestamp in UTC when the event occurred.
- **Description:** Provides detailed information about the event or service failure.
- **Status:** Shows whether the event is **Unresolved** or marked as **Resolved**.
- Provides controls for **filtering**, **searching**, and specifying a date range.

- Logs can be **deleted individually**, **cleared entirely**, or **exported** for analysis.

System Event logs

To go to **System event log** page. Click **Logs -> System event log** from the main menu. This page is used to display System event log (SEL) information.



The BMC system event log helps track and manage various events related to system hardware and administrative actions. It provides detailed logs for both hardware issues and user activities. There are two key types for viewing these logs:

BMC SEL: Displays logs of hardware-related events, such as power failures, temperature alerts, and hardware issues, typically used for diagnosing system problems.

BMC Audit Log: Displays logs of administrative actions on the BMC, including user logins, configuration changes, and system management activities, helping track security and compliance.

Basic operations

Option	Task
Filter by time	Allows users to view event logs that occur within a specific time range, making it easier to analyze and troubleshoot events during that period.
Save Log	Select the event log source (BMC, BIOS, and system software) you want to download and click the download button. It then downloads the logs as a file named SELLOG.zip for further review and analysis.

Clear Log	Deletes all event logs. When clicked, a confirmation dialog will pop up, prompting the user to confirm the action before proceeding.
Refresh All Logs	Reloads the event logs, ensuring that the most up-to-date information is displayed.

POST Code

To go to **POST code** page. Click **Logs -> POST code** from the main menu.

The **POST code** page provides an overview of recent Power-On Self-Test (POST) results, helping users monitor and analyze the host's boot progress. The page displays POST codes for both the previous boot and the current boot. The current boot codes will be moved to the previous boot section when the system is rebooted.

Overview

Dashboard

Logs

System event log

POST code

SQL log

BIOS log

Host video recorder

System diagnostics

Hardware status

Operations

Settings

Security and access

Resource management

BIOS

POST code

Time Style: Offset

Previous Boot

Current Boot

Boot Time

2025-09-19 17:44:08

Time	Code	Description
00:00.000	01000000000001C040	Hardware QSPI FW Flash Init #64
00:00.603	01000000000001C000	Hardware QSPI FW Flash Init
00:00.618	01000000000001C140	FW Boot on BRBCT Load #64
00:00.636	01000000000001C100	FW Boot on BRBCT Load
00:00.651	01000000010001C101	FW Boot on Boot Chain Select #1
00:00.663	01000000010001C141	FW Boot on Boot Chain Select #65
00:00.673	01000000020001C100	FW Boot on BR Exit Done
00:00.693	01000000020001C140	FW Boot on BR Exit Done #64
00:00.704	01000000050001C140	FW Boot on MB1 Start #64
00:00.770	01000000050001C100	FW Boot on MB1 Start
00:00.809	01000000010001C040	Hardware QSPI Data Flash Init #64
00:00.848	01000000010001C000	Hardware QSPI Data Flash Init
00:00.863	01000000020001C042	Hardware QSPI #66
00:00.893	01000000020001C002	Hardware QSPI #2
00:00.915	01000000000002C048	Hardware UPHY Init #72
00:00.942	01000000000002C008	Hardware UPHY Init #8
00:00.956	01000000000002C049	Hardware UPHY Init #73
00:00.995	01000000000002C009	Hardware UPHY Init #9
00:01.029	01000000000002C05A	Hardware UPHY Init #90
00:01.050	01000000000002C01A	Hardware UPHY Init #26
00:01.072	01000000000002C048	Hardware UPHY Init #75
00:01.108	01000000000002C008	Hardware UPHY Init #11
00:01.161	01000000000002C054	Hardware UPHY Init #84
00:01.199	01000000000002C014	Hardware UPHY Init #20
00:01.280	01000000000002C04D	Hardware UPHY Init #77
00:01.307	01000000000002C00D	Hardware UPHY Init #13
00:01.323	01000000000003C040	Hardware NVLINK Init #64

Boot Time

2025-09-19 18:32:42

Time	Code	Description
00:00.000	01000000000001C040	Hardware QSPI FW Flash Init #64
00:00.033	01000000000001C000	Hardware QSPI FW Flash Init
00:00.044	01000000000001C140	FW Boot on BRBCT Load #64
00:00.055	01000000000001C100	FW Boot on BRBCT Load
00:00.074	01000000010001C141	FW Boot on Boot Chain Select #65
00:00.096	01000000010001C101	FW Boot on Boot Chain Select #1
00:00.110	01000000020001C140	FW Boot on BR Exit Done #64
00:00.122	01000000020001C100	FW Boot on BR Exit Done
00:00.236	01000000050001C140	FW Boot on MB1 Start #64
00:00.249	01000000050001C100	FW Boot on MB1 Start
00:00.270	01000000010001C040	Hardware QSPI Data Flash Init #64
00:00.286	01000000010001C000	Hardware QSPI Data Flash Init
00:00.338	01000000020001C042	Hardware QSPI #66
00:00.359	01000000020001C002	Hardware QSPI #2
00:00.496	01000000000002C048	Hardware UPHY Init #72
00:00.508	01000000000002C008	Hardware UPHY Init #8
00:00.611	01000000000002C049	Hardware UPHY Init #73
00:00.623	01000000000002C009	Hardware UPHY Init #9
00:00.711	01000000000002C05A	Hardware UPHY Init #90
00:00.721	01000000000002C01A	Hardware UPHY Init #26
00:00.825	01000000000002C048	Hardware UPHY Init #75
00:00.838	01000000000002C008	Hardware UPHY Init #11
00:00.925	01000000000002C054	Hardware UPHY Init #84
00:00.936	01000000000002C014	Hardware UPHY Init #20
00:00.983	01000000000002C04D	Hardware UPHY Init #77
00:00.997	01000000000002C00D	Hardware UPHY Init #13
00:01.173	01000000000003C040	Hardware NVLINK Init #64

Move the mouse cursor over a record. The web page will automatically highlight other records in the logs with the same code, helping you to identify the specific status (code).

- Shows **Power-On Self-Test (POST) codes** captured during the boot process.
- Helps diagnose hardware initialization errors when the system fails to boot properly.

SOL log

To go to **SOL log** page. Click **Logs -> SOL log** from the main menu. This page provides access to the Serial Over LAN (SOL) log, which captures text-based console output over the network. It is useful for remote troubleshooting, monitoring boot messages, and tracking hardware or system-level events. The SOL log buffer has a maximum capacity of **1,540,000 bytes** (approximately **1503.91 KB** or **1.47 MB**). When the buffer reaches its limit, older log entries are automatically archived. Upon accessing the SOL Log page, the most recent log entries are always retrieved for review.

Overview

Dashboard

Logs

Event logs

System event log

POST code

SOL log

BIOS log

Host video recorder

System diagnostics

Hardware status

Operations

Factory reset

KVM

Firmware

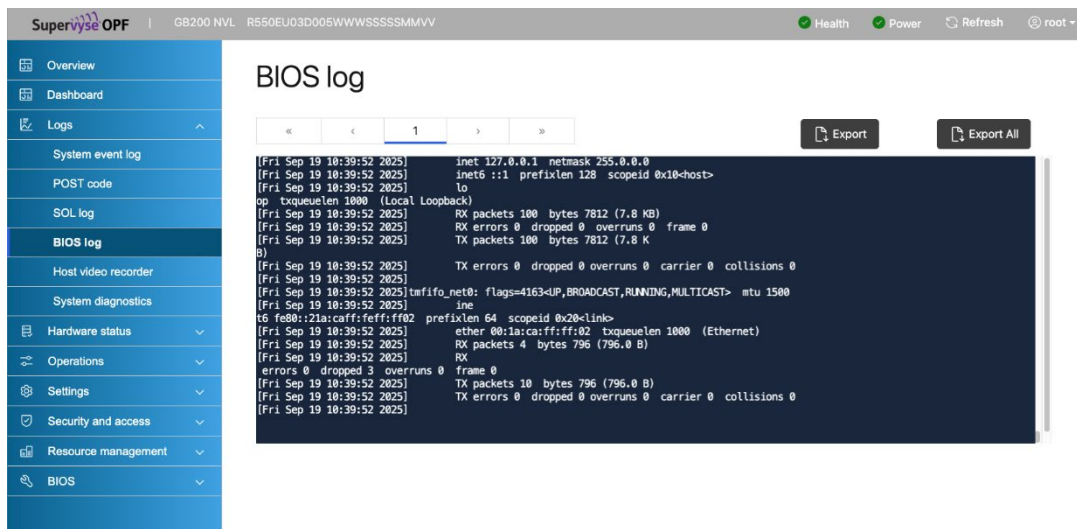
SOL log

Refresh Save SOL Log Clear SOL Log

```
SNMP Community String : public
BMC ARP Control : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl : 2.0 seconds
Default Gateway IP : 10.35.229.254
Default Gateway MAC : d0:7e:28:71:d5:00
Backup Gateway IP : 0.0.0.0
Backup Gateway MAC : 00:00:00:00:00:00
802.1q VLAN ID : Disabled
802.1q VLAN Priority : 0
RMCP+ Cipher Suites : 17
Cipher Suite Priv Max : aaaaaaaaaaaaaa
: X=Cipher Suite Unused
: c=CALLBACK
: u=USER
: o=OPERATOR
: a=ADMIN
: 0=OEM
Bad Password Threshold : 3
Invalid password disable: yes
Attempt Count Reset Int.: 30
User Lockout Interval : 10
root@Skywalker-AMI-PS:~#
```

BIOS log

To go to **BIOS log** page. Click **Logs -> BIOS log** from the main menu. This page allows users to view, navigate, and export system BIOS logs. These logs provide detailed records of system events and errors generated during boot.



- Displays BIOS-related messages recorded during system startup and operation
- Supports troubleshooting firmware-level issues.

Host View Recorder

To go to **Host video recorder** page. Click **Logs -> Host video recorder** from the main menu.

The Host Video Recorder feature allows users to record and manage video of the host's critical events. This feature aids in diagnosing issues and monitoring system health by providing a video record of key moments.

Host video recorder

Dump File List

Dump file not found.

Video Log Setting

☒ Enable Video Log

Video Quality: Normal

Video Trigger

☒ Watchdog Timer Event. ☒ Chassis Power on Event

☒ Chassis Power Off Event. ☒ Chassis Reset.

☒ Host Crash Event.

☒ Date and Time Event

2025 - 01 - 01 00 : 00 : 00

Pre-Event Video Recording

Maximum Dumps: 1 Input Pre-Event maximum dumps of the video.

Duration (Sec): 10 The length of video file recording (in Sec).

Post-Event Video Recording

Maximum Dumps: 1 Input Post-Event maximum dumps of the video.

Duration (Sec): 10 The length of video file recording (in Sec).

☐ Enabled Remote Storage

Save

Record Event Trigger:

Option	Task
Watchdog Timer Event	Triggers video recording when IPMI watchdog commands (such as Hard Reset, Power Down, and Power Cycle) are issued.
Chassis Reset	Triggers video recording when the chassis is reset.
Host Crash Event	Triggers video recording upon detecting a host crash. Notice: CPER for Nvidia

OS SEL Event	Triggers video recording when the operating system encounters a critical error (such as a BSoD (Blue Screen of Death) or Kernel Panic).
--------------	---

System Diagnostics

To go to the **System diagnostics** page. Click **Logs -> System diagnostics** from the main menu. This page offers features designed to assist developers in analyzing and troubleshooting issues. These tools enable efficient debugging and ensure the system operates reliably.

This page includes various platform-specific sections, which may or may not be available depending on the platform.

Overview

Dashboard

Logs ^

System event log

POST code

SOL log

BIOS log

Host video recorder

System diagnostics

Hardware status v

System diagnostics

Generate Diagnostics

Log files should be sent to the system manufacturer for analysis.

Generate Logs

Click the "Generate Logs" button to start generating logs.

Download

Click the "Download" button to download the latest log file.

Latest Log File Generated at: *No log file exists.*

These sections include **Intel Dump Log (ACD)**, **RAS Support List**, and other related features.

Notice: Intel Dump Log (ACD) only supported on Intel platforms.

Notice: RAS Support List only supported on platforms that support RAS offload.

As the user clicks “Generate Logs”, it will gray out until the task completed.

System diagnostics

Generate Diagnostics

Log files should be sent to the system manufacturer for analysis.

Generate Logs

Click the "Generate Logs" button to start generating logs.

Download

Click the "Download" button to download the latest log file.

Latest Log File Generated at: *Generating system debug log - 23%*

Hardware Status

Hardware status refers to the monitoring and display of the current condition of key hardware components within a system. This feature typically provides real-time information on the health and performance of the system's critical hardware, allowing users to quickly assess whether components are functioning properly or if any issues are detected.

The Hardware status page displays all the hardware related information.

A screenshot of this page is given below.



System Information

System Information page displays the system device information. System page shows information like Host Information, BMC Information, Board Information and Product Information of the system device.

System information

Summary

Host Power Status :	Host is currently On
BMC Uptime :	2 Hour(s) 47 Min(s) 37 Second(s)
Active BMC Firmware Build Time :	Thu Nov 14 11:32:43 2024
Active BMC FW Rev :	35.24.46.1240
BMC Chipset :	AST2600-A3
Baseboard Serial Number :	
Chassis Serial Number :	
Product Serial Number :	
Host Interface :	☒ On

Save

Web Session Timeout

30 Min(s) ▼

Save

System Firmware Versions

BIOS Version :	05.61.33.0061
ME Backup Firmware Version :	N/A
ME Operational Firmware Version :	N/A
ME Recovery Firmware Version :	N/A
Microcode Version :	10000680
UEFI Platform Infrastructure Version :	1.70

FRU Information page displays the BMC's FRU device information. FRU page shows information like Basic Information, Chassis Information, Board Information and Product Information of the FRU device.

FRU information

Device

BMC_FRU

Product Information

AssetTag :

FRUFileId : v1.0

Name : BMC Card

PartNumber : R55.0CV04.D007

Serial : R550CV04D007WWSSSSMMVV

Version : 24C044-SB

Extra

Extra 1: BMC_MP.json

Board Information

Manufacturer : Wistron Cooperation

Name : P3809

PartNumber : R55.0CV04.D007

Serial : R550CV04D007WWSSSSMMVV

FRUDeviceID : 0

Language : English

Extra

Extra 1: 01

Extra 2: auto|MAC1:00:00:00:00:00:00

CPU Information (Insyde BIOS joint feature)

To go to CPU information page. Click Hardware -> CPU information from the main menu. This page is used to display CPU information.

This is Insyde BIOS joint feature. You should turn on the host and wait for the BIOS to upload the relevant data.

CPU information

^ CPU_1

Id:	CPU_1
Manufacturer:	NVIDIA
Model:	Grace A02P
PartNumber:	Dfutsrn
Processor Signature:	0x00000012036B0241
ProcessorType:	CPU
SerialNumber:	0x000000017831E140000000009010140
Socket:	G1:1.0
Number of Cores:	72
TotalThreads:	72

^ CPU_0

^ GPU_1

Id:	GPU_1
Manufacturer:	NVIDIA
Model:	NVIDIA GB300
PartNumber:	31C2-893-A1
ProcessorType:	GPU
SerialNumber:	1652525016290

^ GPU_2

^ GPU_3

^ GPU_0

Notice: For more data information, please refer to <https://www.dmtf.org/standards/smbios>

DDR Information

To go to **DDR information** page. Click **Hardware -> DDR information** from the main menu. This page is used to display DDR related information.

DDR information

Q Search	6 items						
Slot Number	Size	Type	Speed	Manufacturer	Asset Tag	Serial Number	Part Number
GPU_0_DRAM_0	285324 MB	HBM	3996 MHz	--	--	--	--
GPU_1_DRAM_0	285324 MB	HBM	3996 MHz	--	--	--	--
GPU_0_DRAM_0	285324 MB	HBM	3996 MHz	--	--	--	--
GPU_1_DRAM_0	285324 MB	HBM	3996 MHz	--	--	--	--
LP5x_0	491520 MB	LPDDR5_SDRAM	6400 MHz	NVIDIA	--	78027483171920388	Dfutsrn
LP5x_0	491520 MB	LPDDR5_SDRAM	6400 MHz	NVIDIA	--	86696660530527776	Dfutsrn

Inventory and LEDs

To go to **Inventory and LEDs** page. Click **Hardware status -> Inventory and LEDs** from the main menu. This page is used to display Inventory and LEDs related information.

This page typically includes two main sections:

- **LEDs:** Shows the LED status of various hardware components. These LEDs indicate different system states, such as power status, drive health, or fault conditions. Users can use the LED indicators to diagnose system issues.
- **Inventory:** Displays all the hardware components in the system, such as motherboards, power supplies, fans, storage devices, and more. Users can view detailed information for each component, including model, status, and health information.

Inventory and LEDs

LED light control

Power status On	System identify LED ☐ Off
--------------------	---

Quick links to hardware components

- ↳ System
- ↳ DIMM slot
- ↳ Processors
- ↳ BMC manager
- ↳ Fans
- ↳ Assemblies
- ↳ Chassis
- ↳ Power supplies

System

	ID	Hardware type	Health	Location number	Identify LED
▼	system	system	✓ OK	--	☐ Off

BMC manager

	ID	Health	Location number	Identify LED
▼	BMC_0	✓ OK	--	--

This page displays inventory information in eight tables, each representing a specific hardware category, providing essential details and status updates for efficient monitoring and management. This page helps

users quickly understand the hardware configuration and current status of the system, making it an essential tool for managing and maintaining a BMC system.

System

The complete server or system configuration, including all essential hardware components.

BMC manager

A Baseboard Management Controller (BMC) that enables remote monitoring and management of the server, even when powered off.

Chassis

The physical enclosure that houses and protects the server's internal components, such as the motherboard and storage devices.

DIMM slot

Slots on the motherboard where Dual Inline Memory Modules (DIMMs) are installed to provide system memory (RAM).

Fans

Cooling components help maintain optimal temperatures by dissipating heat from critical system components.

Power supplies

Units that convert electrical power from the grid into the appropriate voltage for the server, often with redundancy for reliability.

Processors

Central processing units (CPUs) that execute instructions and perform calculations to run the system.

Assemblies

Pre-assembled groups of components, such as motherboards or cooling units, that function as complete units within the system.

Sensor readings

The Sensor Reading page typically shows real-time data from server hardware sensors, which monitor and provide crucial information about the system's health. For instance, it can display parameters such as temperature, fan speed, voltage, and power, enabling system administrators to keep track of the server's hardware performance.

Sensor readings

Use this page to see the sensor readings and their thresholds.

Select a sensor type category

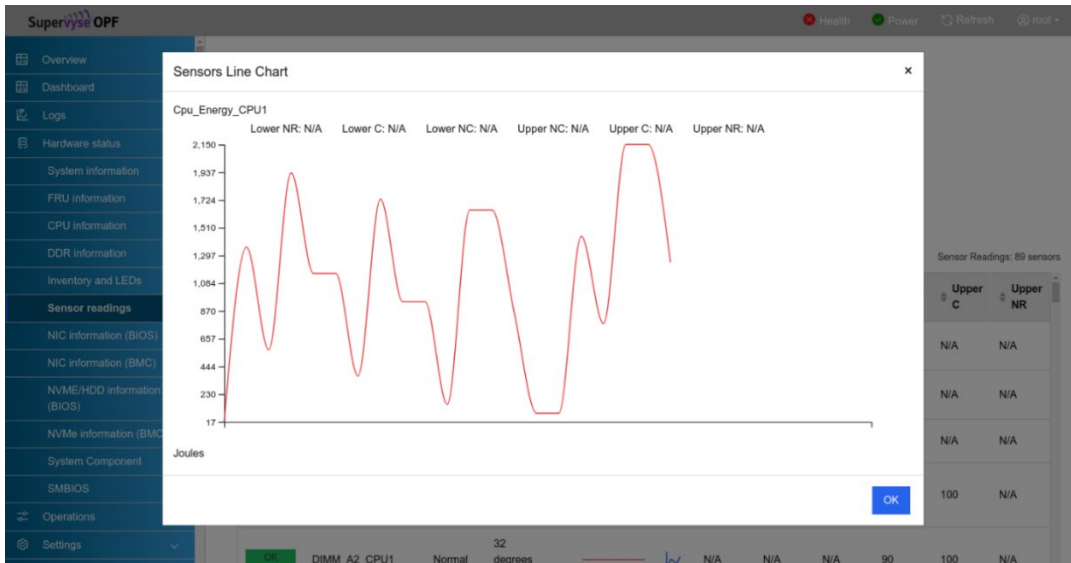
Auto Refresh(sec)

Refresh

Show thresholds

Sensor Readings: 119 sensors

Healthy	Name	Status	Current value	Line chart	View chart
OK	HGX_GPU_1_Temp_0	Normal	22 degrees C		
OK	HGX_GPU_1_Temp_1	Normal	65 degrees C		
OK	HGXGPU2DRA0Powe0	Normal	36.090 Watts		
OK	HGXGPU2DRA0Temp0	Normal	25 degrees C		
OK	HGXGPU2Energy0	Normal	0 Joules		
OK	HGXGPU2Power0	Normal	124.310 Watts		
OK	HGX_GPU_2_Temp_0	Normal	23 degrees C		
OK	HGX_GPU_2_Temp_1	Normal	64 degrees C		



NIC information (BMC)

To go to **NIC information (BMC)** page. Click **Hardware Status -> NIC information (BMC)** from the main menu.

This page is used to display NIC related information from BMC.

NIC information consists of two parts: NIC Entry and Channel Entry.

Each NIC entry will display this NIC's ID, total channels, and device name. By clicking the NIC entry, it will expand detail Manufacturer, Vendor Name, Device Name, Subsystem Name, Subdevice ID, Firmware Name, NC-SI Firmware Version (Hex), and all of its channel entry. The detail manufacturer information and firmware version are from NC-SI Command Get Version ID.

Each channel entry will display this port's ID, link status(up/down) and MAC Address.

Notice: The NIC card must support MCTP to be displayed on this page.

NIC information (BMC)

Total NIC : 1

▼	MT43244 BlueField-3 integrated ConnectX-7 network controller Interface : NCSIOverRBT Total Port Numbers : 2
---	--

NVMe/HDD information (BIOS)

InSyde BIOS joint feature. To go to **NVME/HDD information (BIOS)** page. Click **Hardware Status -> NVME/HDD information (BIOS)** from the main menu. This page is used to display NVME/HDD related information about the server.

Built on OpenBMC

Health Power Refresh root

Overview

Dashboard

Logs

Hardware status

System information

FRU information

CPU information

DDR information

Inventory and LEDs

Sensor readings

NIC information (BIOS)

NIC information (BMC)

NVME/HDD information (BIOS)

NVMe information (BMC)

System component

SMBIOS

Operations

Settings

Security and access

Resource management

BIOS

Storage

NVME/HDD information (BIOS)

Device Count: 10

ST1000DM003-1BD142 Port: 17 MediaType: HDD	Model: ST1000DM003-1BD142 PhysicalLocation: 17 MediaType: HDD RotationSpeedRPM: 7200 SerialNumber: Z1D4DYY3 Firmware Revision: CC46
ST500DM002-1CH162 Port: 18 MediaType: HDD	
Micron_7300_MTFDHB3T8TDF Port: 0 MediaType: NVME	
TOSHIBA DT01ACA100 Port: 20 MediaType: HDD	
TOSHIBA DT01ACA101 Port: 21 MediaType: HDD	
ST1000DM003-1BD142S Port: 24 MediaType: HDD	
Hitachi HDS721010CLA335 Port: 2 MediaType: HDD	
WDC WD5001AALS-00L3B2S Port: 27 MediaType: HDD	
TOSHIBA DT01ACA100S Port: 28 MediaType: HDD	
TOSHIBA DT01ACA101S Port: 29 MediaType: HDD	

NVMe information (BMC)

To go to **NVMe information (BMC)** page. Click **Hardware Status -> NVMe information (BMC)** from the main menu. This page displays status and information that NVMe device information from the host.

Each NVMe entry will display this NVMe's id, NVMe name, state, health, size, protocol and media type. By clicking the NVMe entry, it will expand to display the details of this NVMe device.

Notice: NVMe SSD must support MCTP to obtain SSD information.

Notice: If the value of property shows --, it means it is not supported on this NVMe device.

Notice: The PFA LED display interface depends on whether the device supports this feature. A detailed description of the PFA LED display will be provided in the following content.

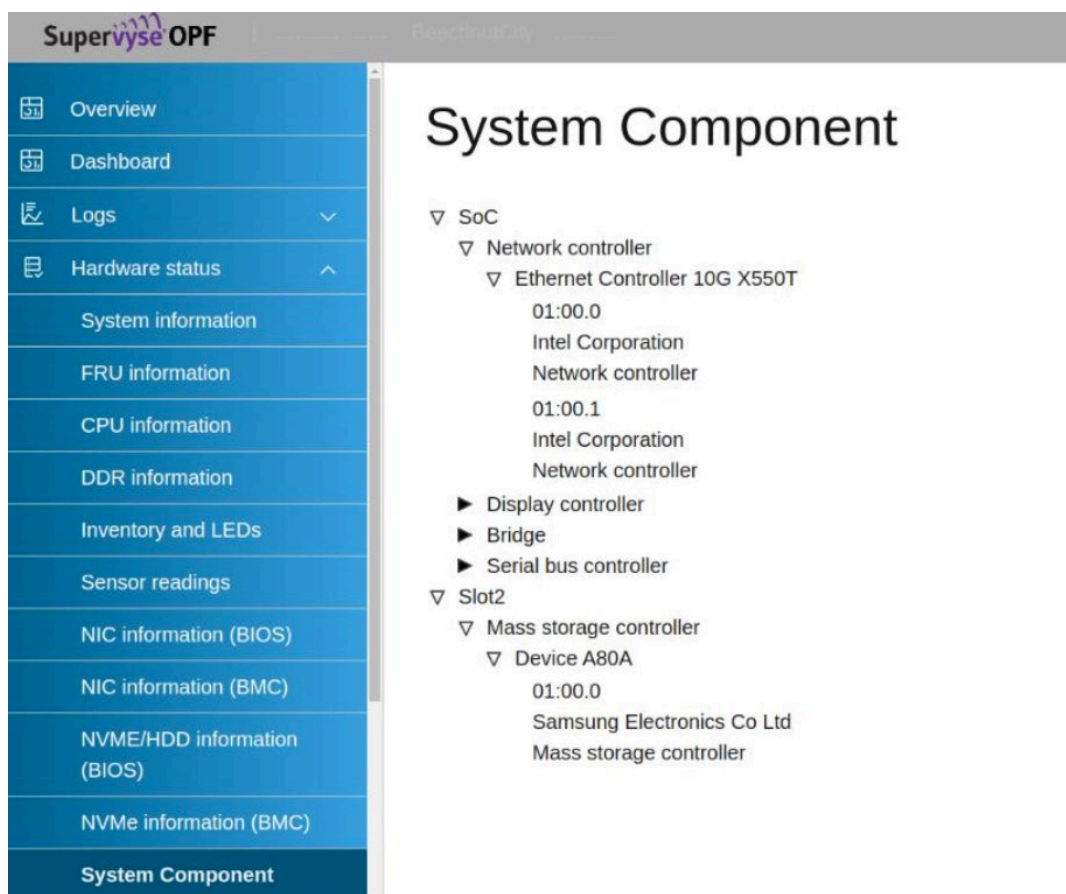
NVMe information (BMC)

Search	2 items						
Id	Name	State	Health	Size	Protocol	Media Type	
^	NVMe1	NVMe1	Enabled	OK	3576.98 GB	NVMe	SSD
Name:		NVMe1		Firmware Version:		LDDJ3U2Q	
PCIe Vendor ID:		0x144D		Powered:		true	
State:		Enabled		Manufacturer:		Samsung	
PCIe Device ID:		0xA900		Functional:		true	
Health:		OK		Model:		PM9D3a	
PCIe Subsystem Vendor ID:		0x144D		Reset Required:		false	
Size:		3576.98 GB		Serial Number		S7UTNG0Y208466	
PCIe Subsystem Device ID:		0xA904		Temperature:		29°C	
Protocol:		NVMe		Part Number		SAMSUNG MZTL63T8HFLT-00AW7	
PCIe Bus Number:		0x07		Overall Health State:		OK	
Media Type:		SSD		Asset Tag:		--	
PCIe Negotiated Link Speed:		--		Percentage Used:		100	
Status Indicator:		OK		PCIe Link Active:		true	
PCIe 0 Link Width:		PCIe x4		Volatile Memory Backup Failed:		--	
Available Spare Threshold:		--		Temperature Threshold:		--	
Reliability Degraded:		--		Media Read Only:		--	

System Component

To go to the **System Component** page. Click **Hardware Status -> System Component** from the main menu. This page provides detailed information about the hardware components of the system, organized hierarchically for easy navigation.

Notice: This page is related to Insyde BIOS Joint Features functionality. The content will only be displayed after the BIOS uploads the relevant data to the BMC via the host interface.



SMBIOS

To go to the **SMBIOS** page. Click **Hardware status -> SMBIOS** from the main menu. This page offers an interface for viewing and configuring SMBIOS settings.

SMBIOS (System Management BIOS) is a standardized interface that allows the operating system to obtain information about hardware components, such as processors, memory, hard drives, motherboards, and more.

SMBIOS provides structured tables that describe detailed hardware information, typically provided by the BIOS, which can be read by the operating system or other management tools. Through this page, you can view and modify the SMBIOS data.

Notice: For more information, please refer to <https://www.dmtf.org/standards/smbios>. This page is related to Insyde BIOS Joint Features functionality. The content will only be displayed after the BIOS uploads the relevant data to the BMC via the host interface.

SMBIOS

Type: 0	
Handle: 0	
DisplayName	[BIOS Information] Type:0 Handle:0
Type	0
Length	26
Handle	0
BIOS_Vendor	American Megatrends International, LLC.
BIOS_Version	01.00.00.0919
BIOS_Segment	0x0000
BIOS_Release_Date	09/17/2025
BIOS_Size	0xFF (see Extended_BIOS_ROM_Size for actual size)
Bios_Characteristics	0x00039A80
BIOS_Characteristics_Extension_Bytes_1	0x01
BIOS_Characteristics_Extension_Bytes_2	0x0D
BIOS_Release	5.36
EC_Release	255.255
Extended_Bios_Size	64 MB

Type: 1

Operations

Operations provide a series of functions for remote management and maintenance of servers, enabling efficient remote server administration.



Factory reset

This page is used to display factory reset options. Click on the Reset button to reset factory settings. Offering various reset options.

Factory reset

Reset options

☐ Reset server settings
Resets firmware settings including: BIOS settings (the specific reset items relate to the BIOS implementation).

☒ Reset BMC settings
This option resets BMC settings, including: all BMC account data, all changed passwords, all policies, LDAP configurations, network addresses, and time of day.
All remote sessions will be ended, and all users and network interfaces will be disabled.
☒ Preserve Configuration

Check All

☒ SDR

☒ SEL

☒ Network

☒ SNMP

☒ SSH

☒ User

☒ Syslog

☒ Web

☒ OEM

Click on the Reset button to reset to Factory defaults settings.

This operation cannot be undone. Click Confirm to continue, or click Cancel to stop now.

Reset

Option	Task
Reset server settings	Reset BIOS settings (the specific reset items relate to the BIOS implementation). Does not affect BMC or network related configurations.
Reset BMC settings	Resets BMC settings.
Reset	Click the button to start the reset process. When clicked, a confirm action dialog will pop up, click Confirm to continue, or click Cancel to abort.

Factory reset options: others will reserve the configurations.

Option	Task
SEL	Preserve system event log.
SSH	SSH RSA key, it will be re-generated if it's not preserved.
OEM	Preserve files under folder /nv/oem and /nv/oemnv in BMC file system.

KVM

The KVM page provides three main features: two types of KVM viewers (HTML5 iKVM Viewer and Java iKVM Viewer) and the Keyboard Macro setting feature. KVM is used to redirect the client's **Keyboard** and **Mouse** inputs to the host system, while the **Video** is exported the host system display to client. These features enable efficient remote system management with flexible access and customizable keyboard macros

KVM

HTML5 iKVM Viewer

Launch

☒ Content Auto Scale

☐ Window Auto Resize

☐ Exclusive Mode

☒ Share Mode

Java iKVM Viewer

NOTE: Please enable the executable bit of the download jar file if double-click cannot launch the iKVM viewer.

Download

Keyboard Macro

You can view and modify keyboard macro on this page. Button Name is optional. Find more supported key detail in user guide.

	Key Sequence	Button Name
1	Ctrl + Alt + Del	Ctrl + Alt + Del
2	Enter	Enter Key
3	PgUp	Page Up Key
4	F1	F1 Key
5	Space	Space Key
6	CapsLk	Caps Lock Key
7		

HTML5 iKVM Viewer

1. Launch - Click on the Launch button to launch the HTML5 iKVM Viewer.
2. Window scale - Select one of the two options: Content Auto Scale or Window Auto Resize.
 - a. Content Auto Scale: If this function is enabled, the host content in the iKVM display area will automatically scale to match the window size, maintaining the aspect ratio and displaying the entire content within the window.

- b. Window Auto Resize: If this function is enabled, the iKVM window will automatically resize to show the full host display. When the window size is reduced, it will focus on a specific area of the host content, and only part of the host screen will be visible.
3. Session mode - Select one of the two options: Exclusive Mode or Share Mode
 - a. Exclusive Mode: If this function is enabled, the iKVM Server will only accept one connection, and others will be rejected.
 - b. Shared Mode: If this function is enabled, the iKVM Server will allow multiple clients to connect simultaneously and share the desktop
4. Download - Click the 'Download' button to download the Java iKVM Viewer jar file. (For more details, please refer to the Supervyse IKVM Java Viewer User Guide.)
5. Save - Click to save the Keyboard Macro settings
6. Key Sequence - Enter the desired key sequence (e.g., Ctrl + Alt + Del) to define the macro
7. Button Name (Optional) - Enter a custom name for the button that triggers the key sequence. Notice: If left blank, it will automatically use the same value as the Key Sequence field.



KVM Features:

Category	Option	Task
Keyboard	Virtual Keyboard	Virtual Keyboard is an on-screen keyboard. Users can use mouse to send keyboard event • Click the button "Keyboard" -> "Virtual Keyboard" to launch the virtual keyboard.
	Keyboard Macro	This feature provides many keyboard-macros as an easy way to send keyboard events. A keyboard macro is a composition of several keys. Such as Ctrl+Alt+Del. The keyboard macro is used to trigger reboot on UEFI shell or un-lock the window on Windows.
Options	Keyboard/ Mouse hotplug	If host has no action when BMC bypass user's keyboard/mouse events to host, user can try to click the "Keyboard Mouse Hotplug" to recovery. This function simulates a USB re-plug action from BMC to the host.

	Preferences	The preferences provide custom settings. C. Click “Preferences” to open “Preferences” window. • Must click “Apply” button to store your setting.
User List	Chat room	Users can do some interaction with others using chatroom. You can also send whisper messages.
	User List	• Click to open user list window. • iKVM users, the yellow head bar is the current privilege owner who can control iKVM, and the grey head is view-only. • The user can click the Privilege Request button to request iKVM control privileges.
Video	Video Recording control	• Start to record video of iKVM. The video format is .webm. • Stop the video recording then save file to local filesystem. • Capture the screen of iKVM then save PNG file to local filesystem. • Setup recording time for timer recording function, default value is 1 minute.
	Video streaming control	• Play the host display • Pause the host display • Refresh the host display • Zoom in/out the host display
IPMI	IPMI Command	Enter the IPMI command to input field and press "Enter" key to send. The maximum length of each command is 500 characters.
Power Control	Host Power Control	Same definitions as WebUI operations.
	Display Power Control	

How to use Java viewer:

1. Login to BMC web.
2. Go to page Operation > KVM.
3. Click the "Launch" button under "Java iKVM Viewer" and download.
4. Double click to launch the iKVMViewer.jar
 - a. You will see a login screen like this. Fill in the required IP, Port, Username, and Password fields
 - b. If Share HTTPS/iKVM/VM Port was configured to On, please fill in the port HTTPS (Web) using to Port.
 - c. If Exclusive Mode is Enabled, only one user can use KVM
5. Press the "Login" button to connect to KVM server.
6. After login, the main window of KVM viewer will display.

iKVM Login v2.15.11 ...

IP: 10.33.33.202 Port: 5900

Share HTTPS/iKVM/VM Port: ☐ On ☒ Off

Encryption: ☐ None ☒ AES-128

Username: root ☐ Remember

Password: ☐ Remember

Exclusive Mode: ☐ Enabled

☐ Save Settings

Firmware

To go to **Firmware** page. Click **Operations -> Firmware** from the main menu.

The firmware page includes a firmware version entry and the update firmware entry.

Firmware

BMC and server

Running image
Version 01.00.25.0918

Component

Running image
CPLD Firmware Version 0x00 0x0b 0x04 0x02 CPLD 2 Firmware Version 0x00 0x0b 0x04 0x02

Update firmware

File source
☒ Workstation
☐ Https Server
☐ SCP Server
Fully Update (BMC Firmware Only)
☐ Disabled
Image file
Add file
Start update

Option	Task
File source select	Chooses to update the image source from either the local system or TFTP.
Fully Update (BMC Firmware Only)	Enables factory reset update function. Note that the factory reset is performed after the firmware update.

	This feature is only applicable to BMC firmware and cannot perform factory updates on other firmware images.
Add File	Uploads the firmware image file from the client-side disks.
Start Update	Starts the update process and for more information. It will show a pop-up to input Password, click "AUTH" for continue, click "Cancel" to do nothing.

Reboot BMC

To go to the **Reboot BMC** page. Click **Operations -> Reboot BMC** from the main menu.

This page provides users with the ability to restart the BMC. This feature is essential for troubleshooting and maintaining system stability when configuration changes or issues arise.

Reboot BMC

Last BMC reboot

2025-09-19 10:26:36 UTC

When you reboot the BMC, your web browser loses contact with the BMC for several minutes. When the BMC is back online, you may need to log in again.

Reboot BMC

SOL console

To go to **SOL (Serial Over Lan)** console page. Click **Operations -> SOL console** from the main menu. This page is used to display the SOL console.

SOL console

SOL console redirects the server's serial port output to this window.

Service: ☒ On

Columns:

Rows:

Status: ☒ Connected

[Open in new tab](#)

```
-rwxr-xr-x 1 root root 10374296 Jul 9 18:07 nvidia-imx-aarch64-580.29.run
-rwxr-xr-x 1 root root 311705636 Jul 9 18:07 NVIDIA-Linux-aarch64-580.29.run
-rwxr-xr-x 1 root root 578322392 Sep 19 16:34 nvssvt-v1.6.1.zip
drwxr-xr-x 7 qt users 4096 Jul 9 17:40 pciutils-3.13.0
-rw-r--r-- 1 root root 672999 Jun 9 2024 pciutils-3.13.0.tar.gz
drwxr-xr-x 5 root root 4096 Jul 9 17:23 Power_cycle
-rwxr-xr-x 1 root root 35472 Jul 9 17:23 PowerIP.sh
-rwxr-xr-x 1 root root 6593 Jul 9 17:23 readme.txt
-rwxrwxrwx 1 root root 12521 Jul 9 17:23 Reboot_stress.sh
-rwxr-xr-x 1 root root 3166 Jul 9 19:02 standard_install.sh
-rwxrwxrwx 1 root root 14635 Jul 9 17:24 system_check.sh
drwxr-xr-x 7 1003 1003 4096 Aug 2 05:06 v1.6.1
root@Naberie-PS-source:~# ifconfig
enp5p9s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.35.229.117 netmask 255.255.254.0 broadcast 10.35.229.255
    inet6 fe80::5eff:35ff:feff:b0f5 prefixlen 64 scopeid 0x20<link>
    ether 5c:ff:35:ff:b0:f5 txqueuelen 1000 (Ethernet)
    RX packets 319482 bytes 262087007 (262.0 MB)
    RX errors 0 dropped 15361 overruns 0 frame 0
    TX packets 99127 bytes 17213717 (17.2 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device memory 0x614041900000-6140419fffff

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 227814 bytes 104863534 (104.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 227814 bytes 104863534 (104.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tmfifo_net0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::21a:caff:feff:ff02 prefixlen 64 scopeid 0x20<link>
    ether 00:1a:ca:ff:ff:02 txqueuelen 1000 (Ethernet)
    RX packets 377 bytes 84202 (84.2 KB)
    RX errors 0 dropped 341 overruns 0 frame 0
    TX packets 17 bytes 1286 (1.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Server power operations

This page allows you to manage and control the server's power state. From this page, you can perform operations such as rebooting, shutting down, or configuring boot settings for the server. This page provides options for both immediate and orderly power operations, allowing for flexible and controlled management of the server's power state.

Server power operations

Current status

Server status

On

Last power operation

2025-09-19 10:32:48 UTC

Boot settings

Boot settings override

None

⌵

☐ Enable one time boot

Save

Operations

Reboot server

- ☒ Orderly – operating system shuts down, then server reboots
- ☐ Immediate – Server reboots without operating system shutting down; may cause data corruption

Reboot

Shutdown server

- ☒ Orderly - operating system shuts down, then server shuts down
- ☐ Immediate - Server shuts down without operating system shutting down; may cause data corruption

Shut down

Virtual front panel

To go to **Virtual front panel** page. Click **Operations -> Virtual front panel** from the main menu. This page provides users with remote control and monitoring capabilities for the server's power status and chassis UID (Unique Identifier). This interface replicates the functionality of a physical front panel, offering a convenient way to manage the server without requiring physical access.

Virtual front panel

This page shows the power status of the server.

Power Control

The following power control operations can be performed.

Host is currently ON

☐ Power On Host

☐ Reset Host

☐ Power Off Host - Immediate

☒ Graceful Shutdown (ACPI Off)

☐ Power Cycle Host

Selecting this option will immediately power off the host, then power it back on after one second.

[Perform Action](#)

Chassis Identify (UID) Control

You can turn on/off/blinking UID Control.

Current UID Status **Off**

Choose An Action

☐ Turn Off

☐ Turn On

☐ Turn Blinking Duration Timeout value range: 1 ~ 254 Seconds, 0: Off , 255: Continuously

[Perform Action](#)

UID Turn Blinking:

- Default Duration: 30 seconds.
- Duration Range: 1 to 254 seconds.
- Special Values:
 - 0: Turns the blinking off.
 - 255: Enables continuous blinking.

Virtual Media

To go to **Virtual Media** page, click **Operations -> Virtual Media** from the main menu. This section demonstrates various methods for using Virtual Media, such as HTTPS, Samba, NFS, and HTML5, to share ISO images or folders from a client to a host.

Virtual Media

Device 1	No disk emulation set.
Device 2	No disk emulation set.
Device 3	No disk emulation set.
Device 4	No disk emulation set.
Device 5	No disk emulation set.

Image Share on Network

Select Device

1 Device 1 ▾

Share Host

2 Samba ▾

3

192.168.0.100

Path To Image

4 /path/to/image.iso

Support .iso, .img or .ima file, and folder "/".

User (Optional)

5 Username

Password (Optional)

6 Password

Remember saving changed data before mount.

7 Save 8 Mount 9 Unmount

HTML5 VM Viewer

Launch Help

A

Java VM Viewer

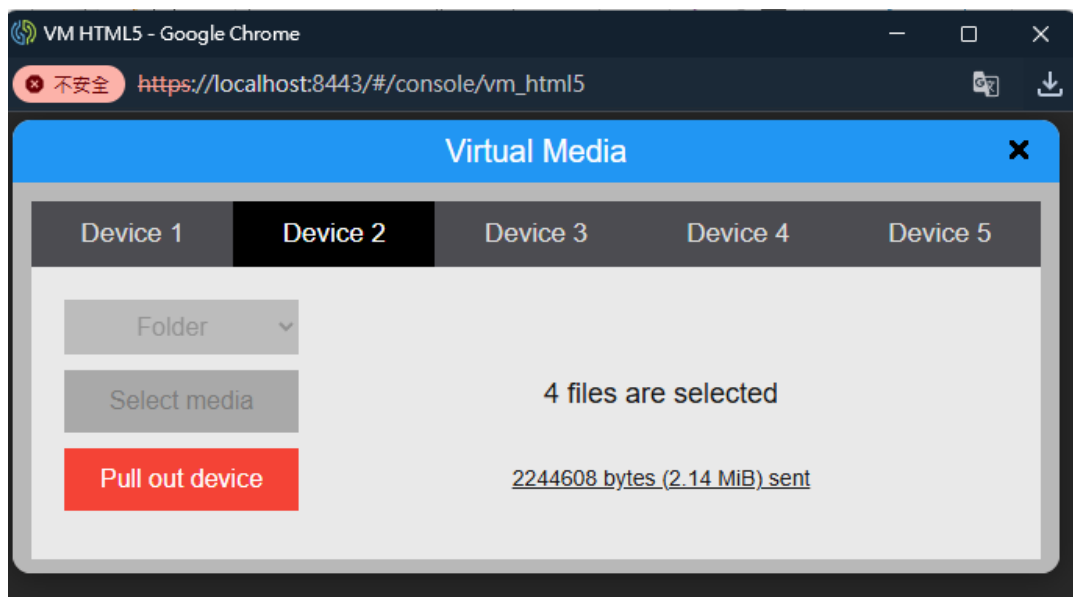
Download

1. Select a device in the dropdown menu.
2. Select [Samba] from the dropdown list.
3. Enter Share Host.
4. Enter Image Path.

5. Enter User.
6. Enter Password.
7. Press Save button and see if "Success" message shows on right top corner.
8. Press the Mount button. If the mounting process is successful, the corresponding device status will display a "Mounted message", and the shared content will also be visible on the host.
9. Press the Unmount button to plug out the image.

VM HTML Viewer

Click **Launch**. The main window of VM over HTML5 will pop up.



Note: Do NOT close the operation window while using Virtual Media over HTML5, as this will terminate all connections.

Media Types:

- ISO -> Mount a local ISO file to the host.
- Folder -> Mount a local folder to the host.
- IMG/IMA -> Mount a IMG or IMA file to the host.

Boot config

BIOS joint feature. This page allows users to configure boot options and order for the system. It is divided into two sections: Boot Option and Boot Order.

Boot config

Boot Option

Boot Source Override

Continuous

Mode

UEFI

Boot Device Selector

None

Save

Boot Order

You can order options and drag between active and inactive options.

Active Options

Inactive Options

Ubuntu

UEFI: PXE IPv4 Intel(R) Ethernet Server Adapter I210-T1

UEFI: PXE IPv4 Nvidia Network Adapter - D8:94:24:44:81:C3

Boot Options:

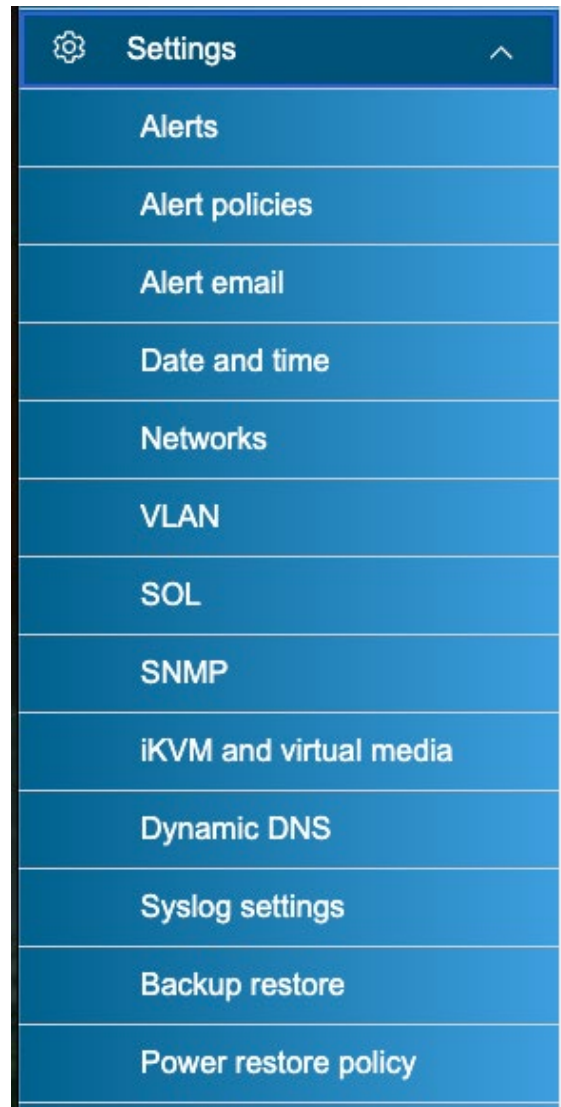
This section provides options to control the boot behavior and source.

Option	Task
Boot Source Override	Temporarily overrides the default boot source. Options value: Disabled: No override; use the system's default boot source. Once: Override the boot source for the next boot only. Continuous: Continuously override the boot source for all subsequent boots until changed.

Mode	Select either Legacy or UEFI depending on your system requirements. Legacy for traditional BIOS-based booting and UEFI for modern firmware-based booting with advanced features.
Save	Save the current configuration settings. A toast notification will display the result of the save operation (success or failure). If the save is successful, a message box will appear reminding you to restart the host to apply the changes. It will also advise verifying that the system boots from the selected boot device and checking the device status if the boot fails.

Settings

The **Settings** section contains various options related to system configuration and management. These settings allow you to adjust alert notifications, network configurations, remote management tools, log recording, and other functionalities according to your needs, thereby improving system management efficiency, enhancing system stability, and simplifying troubleshooting.



Alert

To go to **Alerts** page. Click **Settings -> Alerts** from the main menu. Use this page to configure which system events should trigger alerts and the destination for those alerts. Up to five destinations can be selected for each LAN channel lists the options to select the events that should trigger alerts and where the alerts are to be sent.

Alerts page comprises three key components: PEF (Platform Event Filtering), SNMP Trap, and Alert Destination. These elements work in tandem to monitor system health and deliver alerts when issues arise.

Alerts

PEF

To configure the global PEF configuration, please click [here](#)

▲ No.	PEF Enable	Policy Set	Sensor Type	Sensor Name	Assertion Condition	PEF Actions
1	Yes	1	Temperature	Match All	state:0,2,4,7,9,11	Alert; ✎
2	Yes	1	Voltage	Match All	state:0,2,4,7,9,11	Alert; ✎
3	Yes	1	Current	Match All	state:0,2,4,7,9,11	Alert; ✎
4	Yes	1	Fan	#176	state:0,2,4,7,9,11	Alert; ✎
5	Yes	1	Physical Security	#4	state:4	Alert; ✎
6	Yes	1	Power Supply	#160	state:0 1 2 3 6	Alert; ✎

SNMP Trap

LAN Channel

Dedicated NIC (1) 

SNMP Trap

☒ v1 ☐ v2c ☐ v3

Community String

public

Save

PEF (Platform Event Filtering)

PEF is used to filter and manage system events. It triggers alerts based on specific hardware conditions, such as temperature spikes or power failures. Administrators can set rules to ensure alerts are only triggered by relevant events, allowing for more efficient monitoring.

Global PEF Configuration

The following options allow the user to enable or disable global PEF configuration.

PEF Enable

Enable

Log Event on Filter Action

☒

PEF Actions

☒ Alert

☐ Power Off

☐ Reset

☐ Power Cycle

☐ Graceful Shutdown

☐ Diagnostic Interrupt

Cancel

Save

SNMP Trap

SNMP (Simple Network Management Protocol) Trap is a notification mechanism that sends event information to a management system when critical alerts occur. It helps IT administrators receive real-time notifications of hardware or system issues for prompt action.

SNMP Trap

LAN Channel

Dedicated NIC (1)

SNMP Trap

☒ v1 ☐ v2c ☐ v3

Community String

public

Save

Alert Destination

Alert Destination defines where the alerts are sent, such as email, SNMP management systems. BMC allows multiple destinations to be configured, with up to five per LAN channel, ensuring alerts are directed to the appropriate recipients.

Alert Destination

LAN Channel

Dedicated NIC (1)

Enable Alerting

Alert Destination #1

☒ SNMP

Send SNMP Alerts to IP

IP:default port 1

☐ Email

Send Email to

mail@example.

Alert Destination #2

☒ SNMP

Send SNMP Alerts to IP

IP:default port 1

☐ Email

Send Email to

mail@example.

Alert Destination #3

☒ SNMP

Send SNMP Alerts to IP

IP:default port 1

☐ Email

Send Email to

mail@example.

Alert Destination #4

☒ SNMP

Send SNMP Alerts to IP

IP:default port 1

☐ Email

Send Email to

mail@example.

Alert Destination #5

☒ SNMP

Send SNMP Alerts to IP

IP:default port 1

☐ Email

Send Email to

mail@example.

Save

Send Test Alert

Example: Send an alert via SMTP email server

Prerequisite: "Alert Email" must be configured.

1. Configure one Alert Destination, select "**Email**" and input an alert target mail address.
2. Click the "**Send Test Alert**" button, and an alert email will be received in the target mailbox.



[Alert Policies](#)

To go to **Alert** policies page. Click **Settings -> Alert** policies from the main menu. This page is used to display Alert policies related information.

When an alert is triggered via PEF, the alerting process is managed by an alert policy, which consists of one or more alert destinations. These destinations can include various types and channels, processed sequentially. The use of each destination can be configured based on the success or failure of the previous alert.

The Policies data is stored in the Alert Policy Table, a part of the PEF configuration parameters. The system supports multiple policies, each identified by a unique policy number, which is referenced in the Event Filter Entry to determine which policy to apply when a match occurs.

The Alert String Key is used to associate an alert with predefined conditions, event filters, or alert policies. It allows the system to recognize the nature of the event, what triggered it, and how it should be handled. Typically, the alert string key follows a specific format to ensure it is distinct and easily identifiable, enabling administrators to quickly diagnose and respond to issues.

Alert policies

Policies

Policy Table: 20 entries

⬆ No.	Group Number	Enable	Action	LAN Channel	Destination Selector	Event Specific Alert String	Alert String Key	
1	1	Yes	always send alert to this destination	1	1	No	N/A	✎
2	1	Yes	always send alert to this destination	1	2	No	N/A	✎
3	1	Yes	always send alert to this destination	1	3	No	N/A	✎
4	1	Yes	always send alert to this destination	1	4	No	N/A	✎
5	1	Yes	always send alert to this destination	1	5	No	N/A	✎

Alert String Key

Strings Table: 40 entries

⬆ No.	Strings	
1		✎
2		✎
3		✎

(The Strings Table fixed limit of 40 entries.)

Alert email

To go to **Alert email** page. Click **Settings -> Alert email** from the main menu. This page is used to configure alert email related information.

Alert email

SMTP

SMTP Server Domain/IPv4/IPv6 Address	
Sender Email Address	
SMTP User	
SMTP Password	
SMTP Server Port Number	25
SMTP SSL/TLS Enable	☐ On ☒ Off
STARTTLS Enable	☐ On ☒ Off
Authentication Method	☐ On ☐ Manual ☒ Off
Save Clear	

Example: Using Gmail configuration

Reference Google SMTP configuration

<https://support.google.com/mail/answer/7126229?hl=en&sjid=10907887383758912285-AP#zippy=%2Cstepchange-smtp-other-settings-in-your-email-client>

Date and Time

To go to **Date and time** page. Click **Settings -> Date** and time from the main menu. This page is used to display and modify BMC date and time information.

The Network Time Protocol (NTP) is a server used to synchronize the time of network devices.

Date and time

i To change how date and time are displayed (either UTC or browser offset) throughout the application, visit [Profile Settings](#)

Time Zone

GMT+00:00 | Casablanca, London

NTP

☒ NTP Enable

☐ Use NTP servers (DHCP)

Primary NTP Server

Secondary NTP Server

Date

YYYY-MM-DD

2025-09-19

24-hour time (UTC)

HH:MM

13:34

Save

Sync from RTC

Notice: The date and time cannot be set more than **Jan 19 03:14:07 2038**. After this point, systems relying on a signed 32-bit integer to track time will experience an **integer overflow**, causing the time to be misrepresented as **Dec 13 20:45:52 1901 (UTC)**.

Enable/disable NTP service.

- If NTP is enabled, you have to set the Use NTP servers (DHCP) 、 Primary NTP Server 、 Secondary NTP Server setting fields related to NTP.
- If NTP is disabled, you must manually set the date and time in the Date YYYYMM-DD 、 24-hour time (UTC) HH:MM fields or Sync from RTC.

Networks

To go to **Networks** page. Click **Settings -> Networks** from the main menu. This page allows you to configure the BMC network settings, including LAN channels, IPv4 and IPv6 configurations, as well as DNS server settings.

Networks

Configure IPMI LAN Channel settings for the BMC

LAN Channel

Dedicated NIC (1)

MAC address

5c-ff-35-ff-b3-10

Hostname

nvidia-obmc

Save settings

^ IPv4 Network Settings

Network interface

DHCP Enabled

Gateway

10.35.229.254

IP Address

IP address

Subnet mask

10.35.229.120

255.255.254.0



+ Add static IP

DNS Server

IP address

Search domain

Domain Name Search

VLAN

To go to **VLAN** page. Click **Settings -> VLAN** from the main menu. This page allows you to configure an 802.1Q VLAN private network for a specified LAN channel. This setup is essential for creating isolated virtual networks for better traffic management and security.

Notice: 802.1Q is a standard protocol for implementing VLANs in Ethernet networks.

VLAN

Use this page to configure an 802.1Q VLAN private network on the specified LAN channel.

LAN Channel	Dedicated NI 
Enable VLAN	☐
VLAN ID	0
VLAN Priority	0
Save	

VLAN ID: Enter the VLAN ID (identifier) for the VLAN network. VLAN ID are used to uniquely identify each VLAN on the network. Values are from **1** to **4094**.

VLAN Priority: Set the VLAN Priority to define the traffic class for the VLAN. This value determines the priority level of packets sent through the VLAN.

Valid Range: **0–7**, where **0** is the lowest priority and **7** is the highest priority.

SOL

To go to **SOL** page. Click **Settings -> SOL** from the main menu.

This page allows you to configure the Serial Over LAN (SOL) settings for the BMC. SOL allows you to redirect serial traffic from the baseboard over an IPMI session, enabling communication with the host system during both OS and pre-OS stages. These settings provide the ability to manage and diagnose the host remotely over the network, regardless of the operating system state.

SOL

Serial Over LAN

Enable or disable serial over LAN communications.

LAN Channel	Dedicated NIC (1) ▾
Enable SOL for Baseboard Mgmt	☒ Enabled
Baud Rate	115200 bps ▾
Privilege Level	User ▾

[Save](#)

SOL SSH

Customize the settings of the service used by Serial Over LAN Secure Shell (SOL SSH).

SOL SSH	☒ Enabled
Port	2200
Timeout (sec.)	600

[Save](#)

Serial Over LAN: Configure the Serial Over LAN (SOL) settings for remote management of the host's serial console over the network, specific to the selected channel.

SOL SSH: Customize the settings of the service used by Serial Over LAN Secure Shell (SOL SSH). Changing this setting will immediately terminate all the sessions which are using SOL SSH service.

iKVM and virtual media

To go to **iKVM & virtual media**. Click **Settings -> iKVM & virtual media** from the main menu.

This page allows you to configure iKVM and Virtual Media settings. iKVM (Integrated Keyboard, Video, and Mouse) enables remote control of the host's keyboard, display, and mouse. The Virtual Media feature allows you to remotely mount media (such as ISO files), facilitating OS installation, recovery, or updates. These settings enable flexible host management and support remote maintenance and troubleshooting.

iKVM and virtual media

Virtual Media Settings

☐ Virtual Media Service

Virtual Media over HTML5

☐

Virtual Media over Java

☐

Port

Valid Value: 1 - 65535. Default: 627.

Instance Count

Valid Value: 1 - 5

Session Timeout

Valid Value: 0 - 1440. Unit: minutes.

Save

iKVM Settings

☐ iKVM Service

Session Timeout

Valid Value: 0 - 9999. Unit: minutes.

Enabled HTML5 iKVM Viewer

☐

Enabled KVM Port

☐

KVM Port

Valid Value: 1 - 65535. Default: 5900.

Save

Dynamic DNS

To go to **Dynamic DNS** page. Click **Settings -> Dynamic DNS** from the main menu. This page allows you to configure settings for Dynamic DNS updates. Dynamic DNS is a service that automatically updates changing IP addresses to a DNS server so that users can access the device through a fixed domain name even if the IP address changes.

Supervyse OPF

Health Power Refresh root

Dynamic DNS

Use this page to configure dynamic DNS update settings.

Dynamic DNS ☐

☒ Enable DDNS by nsupdate
☐ Enable DDNS by DHCP Client FQDN

DNS Server IP 192.168.22.1

Domain Name example.com

BMC Hostname bmc-mac000

TSIG ☐ TSIG protocol includes a timestamp, please make sure BMC's time is accurate.

Authentication(Transaction Signature)

TSIG Key Key name: tsig2.

Upload new TSIG Key TSIG .key File Choose File No file chosen

TSIG .private File Choose File No file chosen

Save

Dynamic DNS ☐

☒ Enable DDNS by nsupdate
☐ Enable DDNS by DHCP Client FQDN

DNS Server IP

Domain Name

BMC Hostname nvidia-obmc

TSIG ☐

Authentication(Transaction Signature)

TSIG Key Key name: web.

Upload new TSIG Key TSIG .key File 選擇檔案 未選擇任何檔案

TSIG .private File 選擇檔案 未選擇任何檔案

Save

Option	Task
Dynamic DNS	Enables or disables the DDNS feature. • On: DDNS is active, allowing automatic DNS updates. When enabled, you can choose between: ○ Enable DDNS by nsupdate - Use the nsupdate method to update DNS records dynamically. ○ Enable DDNS by DHCP Client FQDN - Update DNS records using the Fully Qualified Domain Name (FQDN) provided by the DHCP client. • Off: DDNS is inactive.
Enable DDNS by nsupdate	The nsupdate option uses a dynamic DNS update utility to send DNS update packets directly to the DNS server.
Enable DDNS by DHCP Client FQDN	This option allows dynamic DNS updates by utilizing the DHCP Client's Fully Qualified Domain Name (FQDN) , simplifying DNS record management by automating updates through the DHCP server. It allows devices to automatically update their DNS records, ensuring accurate mappings between IP addresses and hostnames. When enabled, the DHCP client sends its full hostname (FQDN) to the DHCP server, which updates the DNS server with the client's IP and FQDN, removing the need for manual DNS record updates.
TSIG Authentication	This setting enables secure communication between the BMC and the DNS server using Transaction Signature (TSIG). Notice: TSIG protocol includes a timestamp, please make sure BMC's time is accurate: Ensure the BMC's system time is accurate, as TSIG uses a timestamp to prevent replay attacks. Incorrect BMC time may cause TSIG authentication to fail. TSIG (transaction signature): is a protocol extension used in DNS to provide secure authentication and integrity for DNS transactions. It achieves this by attaching a cryptographic signature to each DNS message. This signature is computed using a shared secret key and a hashing algorithm, such as HMAC-MD5 or HMAC-SHA256.

Syslog settings

After enabled Syslog option, you can modify the Syslog Level, Kernel Log, Kernel Log Level settings.

Syslog settings

Use this page to collect system debug information about the server.

Basic Setting

Enable Syslog	☐
Syslog Level	4 - Error (default) ▾
Kernel Log	☐
Kernel Log Level	1 - Emergency (default) ▾
Save	

Log to Remote Server

Redirect Syslog to Remote Server	☐
Remote Syslog Server Address	Please input IPv4 address
Protocol	☒ UDP ☐ TCP Syslog service will redirect log message to remote server port UDP:514 or TCP:618.
Remote Facility	1 - user (default) ▾ If remote log is disabled, the facility will be set as the user (default)
Save	

Reset to Default

Click button to reset all syslog settings to default value.

Warning: This action will clean remote server and all filters.

Reset

Restore syslog default settings.

Configuration File

Import File

Choose File

No file chosen

Import

Select a valid DBG configuration file.

Export File

Export

Press the button to export DBG configure file.

The exported configuration file could be opened via text editor.

```
save_syslog.bin
1 # Parameter Descriptions:
2 # =====
3 # syslog_level: Log level [2 - 8]
4 # syslog_facility: Remote facility [1 - 9]
5 # remote_log: Enable/Disable remote log [1: Enable; 0 Disable]
6 # remote_svaddr: Remote logger address [xxx.xxx.xxx.xxx]
7 # remote_transmit: Transmission with UDP, TCP or SSL (only for syslog-ng) [0: UDP; 1: TCP; 2: SSL]
8 # kernel_log: Enable/Disable kernel log [1: Enable; 0 Disable]
9 # func_filter: Filter Type [0: Default; 1: slot; 2: function ]
10 # fBitMask: Bit mask of function filter
11 # strBitMask: Bit mask of string filter
12 # slotBitMask: Bit mask of slot filter
13 # fname/file: Function name for log filter, ex: lookup/test.c. Enabled when func_filter=2.
14 # max_file_count: Max. size of log file (only for syslogd)
15 # max_file_size: max. rotate count of log files (only for syslogd)
16 # console_print: Enable/Disable console print [1: Enable; 0 Disable]
17 # console_device: device name of COM port
18 # console_level: Level of console print for printk
19 # pktdump: Enable/Disable NIC driver raw packet dump function
20 # dump_protocol: IP protocol for raw packet dump
21 # dump_port: port number for raw packet dump
22 # =====
23
24
25 syslog_level=6
26 syslog_facility=1
27 remote_log=1
28 remote_svaddr=192.168.21.8
29 remote_transmit=0
30 kernel_log=1
31 is_log=1
32 func_filter=0
33 fBitMask=0
34 strBitMask=0
35 slotBitMask=0
36 max_file_count=0
37 max_file_size=0
38 console_print=0
39 console_device=
40 console_level=5
41 pktdump=0
42 dump_protocol=0
43 dump_port=0
```

Backup restore

To go to **Backup restore** page. Click **Settings -> Backup restore** from the main menu. This page is used to display Backup restore related information.

BMC offers backup and restore functionality for both the BMC/BIOS configuration file. This feature allows users to back up current configurations, ensuring that system settings can be restored in the event of a failure or for recovery purposes. By securely storing backups, BMC provides a reliable method to maintain system stability and quickly recover from potential issues.

Backup restore

Use this page to backup the current BIOS/BMC configuration and restore it.

Backup BMC settings

Backup the current BMC configuration.

Backup

Restore BMC settings

After upload the BMC config file and Press 'Restore' button to restore BMC settings.

Restore File

Choose File

No file chosen

Upload

Restore

Backup BIOS settings

Backup the current BIOS configuration.

Backup

Restore BIOS settings

Press 'Restore' button to restore BIOS settings.

Restore File

Choose File

No file chosen

Restore

Option	Task
Backup	Click this button to download the current BMC/BIOS configuration to a file. BMC backup file name: backup256.bin ('256' that means sha256 checksum.) BIOS backup file name: bios.cfg Notice: If the BIOS Backup button grays out, it means that the BIOS is not uploading data to the bmc. Please try to reboot host.
Restore (BMC)	Restores the BMC configuration from a previously saved file. When clicked, a confirmation box will appear, prompting the user to confirm the action for BMC restoration. Once confirmed, the BMC will immediately restart, and this action cannot be undone, ensuring the user intentionally restores the previous BMC state.
Restore (BIOS)	For the BIOS configuration restoration, no confirmation box will appear. The BIOS configuration will be immediately restored without additional prompts, and this action is also irreversible, ensuring the user intentionally restores the previous BIOS state.

Power restore policy

To go to **Power restore policy**. Click **Settings -> Power restore policy** from the main menu.

This page allows you to configure the power restore policy settings, which determine how the system behaves when power is restored after a disturbance or outage. You can choose the desired power recovery behavior. The available options enable you to specify whether the system should always power on, remain off, or return to its last known power state when power is re-applied. These settings provide flexibility for managing the system's response to power interruptions.

Power restore policy

Configure power policy to determine how the system starts after a power disturbance.

Power restore policies

- ☐ Always on - The system always powers on when power is applied.
- ☐ Always off - The system always remains powered off when power is applied.
- ☒ Last state - The system returns to its last on or off power state when power is applied.

Save settings

Security and access

Security and access refers to the measures and configurations used to protect systems, networks, and data from unauthorized access, while ensuring that legitimate users can access resources when needed. These settings are crucial for maintaining confidentiality, integrity, and availability of information and services.

	Security and access	
	Current users	
	LDAP	
	RADIUS	
	TACACS+	
	Users	
	Policies	
	Certificate management	
	Kerberos authentication	
	Security settings	
	IP access control	

Current users

To go to **Current Users** page. Click **Security and access -> Current Users** from the main menu. This page is used to display current users.

Current users

Search sessions

2 items

☐	Username	Type	IP address	Kill session
☐	root (me)	Web (HTTPS)	10.35.229.89	Disconnect
☐	root (me)	iKVM	10.35.229.89	Disconnect

20

Items per page

<

1

>

Web Session Timeout

30 Min(s)

▼

Save

LDAP

To go to the **LDAP** page. Click **Security and access -> LDAP** from the main menu. This page provides options to configure server settings for OpenLDAP or Active Directory.

LDAP (Lightweight Directory Access Protocol) is an open protocol used to access and manage directory information services. It is commonly used for authentication and user management in systems like OpenLDAP, Active Directory, and similar directory-based services.

OpenLDAP is an open-source implementation of the LDAP, a protocol used for accessing and managing directory information services over a network.

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. Active Directory uses LDAP as its primary protocol for directory services and supports authentication mechanisms like Kerberos and NTLM. It is widely used for managing enterprise networks and enabling single sign-on (SSO) capabilities.

LDAP

Configure LDAP settings and manage role groups

Settings

LDAP authentication

☐ Enable

Secure LDAP using SSL
A CA certificate and an LDAP certificate are required to enable secure LDAP

☐ Enable

CA Certificate valid until

--

LDAP Certificate valid until

--

[Manage SSL certificates](#)

Service type

☒ OpenLDAP

☐ Active Directory

Server 1

Server URI ⓘ

ldap://

Bind DN

Bind password

Leave empty to keep the previous

Base DN

User ID attribute - optional

Group ID attribute - optional

Save settings

Role groups

ⓘ LDAP authentication must be enabled to modify role groups.

+ Add role group

☐	Group name	Group privilege	Group domain
No items available			

Sample settings

Item	Description	
Service type	OpenLDAP	
Server URI	ldap://192.168.22.156	
Bind DN	cn=admin,dc=bmc,dc=com	
Bind password	admin	
Base DN	ou=insyde,dc=bmc,dc=com	
User ID attribute	cn	
Group ID attribute	gidNumber	
Group Name	Group privilege	Group domain
admin	Administrator	dc=bmc,dc=com
operator	Operator	dc=bmc,dc=com
user	ReadOnly	dc=bmc,dc=com

RADIUS

To go to the **RADIUS** page. Click **Security and access -> RADIUS** from the main menu.

RADIUS (Remote Authentication Dial-In User Service) is a protocol used to manage authentication, authorization, and accounting (AAA) for users who access network services. By configuring RADIUS settings, you can integrate your system with an external RADIUS server for centralized user authentication, ensuring that only authorized users can access the system.

RADIUS

Enable RADIUS	☐
Port	1812
IPv4 Address	192.168.11.90
IPv6 Address	
Secret	... 
Authorizing account	InsydeRadiusAdmin
Authorizing password	... 
Admin Vendor Specific	H=4, I=4
Operator Vendor Specific	H=3, I=3
User Vendor Specific	H=2, I=2
<button>Save settings</button><button>Clear</button>	

TACACS+

To go to **TACACS+** page. Click **Security and access -> TACACS+** from the main menu. This page is used to configure TACACS+ related information.

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol used for network device authentication, authorization, and accounting. It is an enhanced version of the original TACACS (Terminal Access Controller Access-Control System) protocol, developed by Cisco, and is primarily used for centralized management and control of network devices such as routers, switches, wireless access points, and others.

TACACS+

New authentication server.

Enable TACACS+

☐

Port

49

IP Address

Please input IPv4 a

Secret

Please input pass

Save

Users

This page is used to display user information and can modify user settings.

Users

Channel 1

[Account policy settings](#) [Add user](#)

User ID	User Name	Status	Privilege	SOL Payload Access	SNMPv3 Access	IPMI Messaging	Email
1	root	Enabled	Administrator	Enabled	Disabled	Enabled	Edit Delete
8	testnvsvt	Enabled	ReadOnly	Enabled	Disabled	Enabled	Edit Delete

Field Name	Description
Status	Indicates the current state of a user account, enabled or disabled.
Privilege	The level of access or permissions assigned to a user, determining what actions they can perform in the system. • Administrator • Operator • ReadOnly • NoAccess

Account policy settings



Max failed login attempts

Value must be between 0 – 65535

User unlock method

☐ Manual

☒ Automatic after timeout

Timeout duration (seconds)

Cancel

Save

Add user



User ID	2
User Name	
Password	
Confirm Password	
Email	
Network Privilege	Administrator
User Enabled	Enabled
SOL Payload Access	Disabled
Password Expiration Day	0
☐ SNMPv3 Access	
SNMPv3 Access Level	ReadOnly
SNMPv3 Authentication Protocol	HMAC_MD5
SNMPv3 Authentication Passphrase	
SNMPv3 Privacy Protocol	CFB128_AES128
SNMPv3 Privacy Passphrase	

Cancel

Add user

Policies

To go to **Policies** page. Click **Security and access -> Policies** from the main menu. This page is used to configure the ways to access BMC.

Policies

Network services

BMC shell (via SSH)

Allow access to shell sessions via SSH, through port 22 on the BMC.

☒ Enabled

Network IPMI (out-of-band IPMI)

Allow remote management of the platform via IPMI. Tools such as ipmitool require this setting to be enabled.

☒ Enabled

WARNING: It needs some time to let new settings take effect. (Approximately 30 seconds)

Notice: It needs some time to let new settings take effect (Approximately 30 seconds, sometimes 2-3 minutes).

Sometimes when switching, the error "failed" appears, and you can switch again after waiting for about 2-3 minutes.

Certificate management

This page is used to display Certificate management related information.

Certificate management is a security feature within the BMC system, designed to ensure encrypted and secure communication between the server hardware and the BMC. By managing and handling certificates, BMC provides robust authentication and encryption mechanisms to protect the system from unauthorized access and ensure that data is not tampered with during transmission. Certificate management is particularly important in data centers and high-security environments, ensuring the security and integrity of remote management operations.

Certificate management

					+ Generate CSR	+ Add new certificate
Certificate	Issued by	Issued to	Valid from	Valid until		
HTTPS Certificate	Insyde	Insyde	Thu Jan 01 00:00:00 1970	Thu Jan 01 00:00:00 2026	i	🔄 🗑️

Certificate:

Displays the SSL/TLS certificate used for which secure communication.

- HTTPS Certificate
- LDAP Certificate
- CA Certificate
- VM Certificate

Check details of Certificate

The screenshot shows the Supervyse OPF web interface. On the left is a navigation menu with options like Overview, Dashboard, Logs, Hardware status, Operations, Settings, Security and access, Current users, LDAP, RADIUS, TACACS+, Users, Policies, Certificate management (selected), Kerberos authentication, Security settings, IP access control, Resource management, and BIOS. The main content area is titled 'Certificate management'. A modal window titled 'Certificate' is open, displaying the PEM format of an HTTPS Certificate. The certificate text is as follows:

```
-----BEGIN CERTIFICATE-----
MIIErDCCASSgAwIBAgIUAT1gY2a454LEyLZNbJNTU6ANswDQYJKoZIhvcNAQEL
BQAwY0xCZAJBgNVBAYTAUQwCgYDVQQLExFCTUMgU29mdHdhcmUgVGVhbnRl
IFNvZnR3YXJlbnNvbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRl
A1UEAxMGSW5zeWRIMScwZG90b3R5b250YWN0LnR3QGluc3lkZS5j
b20wHhcnZAwMTAxMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
VVMxZzAJBgNVBAYTAUQwCgYDVQQLExFCTUMgU29mdHdhcmUgVGVhbnRl
GjAYBgNVBAsTEUJINyQyOTBzZD02ZyZ5b250YWN0LnR3QGluc3lkZS5j
BglqhkiG9w0BCQEWFWNvbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRl
AQEBBQADggEPADCCAQoCggEBBANPEpcQAYQ8Lq2I71QJRV6v154FoEYf52hvF5EY
+MCwW9lqa4otvL9dxKh9OsLpTm35PchsUMK6Xs4GmTZQs0/9+WpCmIVjxtzuzTs
jMtMdt4ZYWoRyy3qaI25PuiWCK1AC+kleAz39zugKWF98K3F5zTEl6jzQOI/O/G2
Wl0rk+MdeKvNIP8i15Dn8I2IjzOjcit85Utu0RulsLD/fFfLKWYU3T5jmVVMGB7
Nldgs02/ToajbWzXC60lgl0lI0rukebo8cPpPbblP/IVCsIO7ZYRWz2I2ladn
ZXvYX4/60g71n2Lrcv1dab8RyFMZ3EV4bQUiFAH5bEDUCaWEAAOCAQAwgI0w
DAYDVROTBAUwAwEB/AdBgNVHQ4EFgQUJHMH8QXgY85PNeFlu8K5KCMNv1kwgD0G
A1UdhwSbTCBwoAUEHhjbQKXgY85PNeFlu8K5KCMNv1mhgZCkgZawgY0xCZAJBgNV
BAYTAUQwCgYDVQQLExFCTUMgU29mdHdhcmUgVGVhbnRlbnRlbnRlbnRlbnRlbnRl
cnAUMRowGAYDVQQLExFCTUMgU29mdHdhcmUgVGVhbnRlbnRlbnRlbnRlbnRlbnRl
MSQwZG90b3R5b250YWN0LnR3QGluc3lkZS5jZ2CTAE7S1GNNmuEu
CxMi2TZWSTU1OgDbMA0GCSqGSIb3DQEBwUAA4IBAODEYEzVhZKJMP898ZrJfD
0ROh6DczA1OoYCo52KAUawhSP86NklUSv7VzbInsteS4CIFBuDD/15jR8U9m++o
2m+sc6Q+slOEuMoX5hjhPZSTZje4Z7/QdHlt6kZsrzkPzhdkgM38gynHbVZTxP
vY3LGS3o6hrWVQgdqN+Hb7MPPCTAWCgx4+kaWISrX4IXID9NRXEgohmtfEIN48
9sRdtZdfafWoRhc5y7YFH+8D61k6P01Ek+8o5jmyHezUjHZUCAoIXVEW7lidyVV
7DqadleTuowwEP61g6ngcQlw4aCQttf+LpMmBZ0uY/COyfdCdyRBe4BEM9AHn
-----END CERTIFICATE-----
```

At the bottom of the modal, there are 'Copy' and 'Download' buttons.

Kerberos authentication

To go to **Kerberos authentication** page. Click **Security and access** -> **Kerberos authentication** from the main menu. This page is used to configure Kerberos certification related information.

Kerberos is a secure authentication protocol that protects communication between users and services through encryption and a ticketing mechanism. Users only need to login once to securely access multiple services, while preventing replay attacks and ensuring the confidentiality and integrity of data.

Notice: The login privilege depends on configurations of **Role groups of Security and access - LDAP**.

Kerberos authentication

Enable Kerberos Authorization	☐
Kerberos Realm	EXAMPLE.CC
Kerberos KDC Server Domain/IPv4/IPv6	127.0.0.1
Kerberos KDC Server Port	88
Keytab file	Choose File No file chosen
Save settings	Upload

Security settings

To go to **Security settings** page. Click **Security and access -> Security settings** from the main menu. This page is used to configure security settings related information.

In the security settings of the BMC, four components are provided, primarily used to protect the BMC from unauthorized access and attacks.

Security settings

You can view and modify the security settings on this page.

SSL Cipher Policy Control Mode

The SSL Cipher Control Mode allows an administrator to get or set the system SSL cipher mode.

SSL Cipher Mode Advanced ▾

Save

IP Blocking Settings

Configuring the bad password threshold and the login failed attempts interval time of the remote client before that is login blocked out and how long the remote client login blocked out will be expired and the remote client can re-login again.

IP Blocking ☒

Failed Login Attempts (1 - 255) 20

Failed Login Attempts Interval Time (sec) 20

Remote Client Lockout Time (sec) 120

Save Restore

Port Settings

Set the port used for https (default: 443) web sessions. Changing this setting will immediately terminate all current web sessions. Port range is 1 ~ 65535.

HTTPS (Secure) Port 443

Save Restore

Optional Network Services

IPMI over LAN ☒ Enable/Disable the RMCP/RMCP+ service.

Save

SSL Cipher Mode:

When the system starts for the first time, "Advanced" is the default mode.

Available options:

- **Advanced** – wide browser compatibility, like most newer browser versions.
- **Broad Compatibility** – check the compatibility to other protocols before using it, like IMAPS.
- **Widest Compatibility** – compatibility to most legacy browsers, legacy libraries, and other application protocols besides HTTPS, like IMAPS.
- **Legacy** – widest compatibility

SSL Cipher Policy Control Mode

The SSL Cipher Control Mode in BMC systems allows administrators to configure SSL/TLS encryption settings for secure communication between the BMC and remote systems. This feature ensures that all data exchanged is encrypted, preventing eavesdropping, tampering, and unauthorized access. By selecting specific encryption protocols and cipher suites, administrators can enforce strong security standards, protecting sensitive information and maintaining the integrity of communication channels across the network.

IP Blocking Settings

By configuring the bad password threshold, login failed attempts interval time, and login locked out duration, administrators can effectively mitigate brute force attacks while ensuring that legitimate users aren't unfairly locked out. The settings provide a balance between security and usability, preventing unauthorized access while allowing users a chance to re-authenticate after a brief locked out.

Port Settings

BMC system typically provides management functions through multiple network ports. By configuring the port settings, you can control which port number is used, effectively restricting unauthorized access and enhancing system security.

Optional Network Services

This setting configures additional network service that the BMC can use. The service typically has extra features or protocols that enhance the flexibility of management functions, but they may also introduce potential security risks.

IP access control

To go to the **IP access control** page. Click **Security and access -> IP access control** from the main menu.

IP access control is a security feature that allows administrators to manage and restrict access to a system based on IP addresses, MAC addresses, and network ports. This provides more granular control over which devices can connect to the system, adding extra layers to prevent unauthorized access.

IP access control

IPv4

☒ Enable IP Access Control:

Number Of Access Rules: 4

☐	Rule No	Rule Type	Rule	Policy	
☐	1	IP/Mask	192.168.2.0/24	Accept	  
☐	2	IP Range	192.168.3.1 - 192.168.3.255	Accept	  
☐	3	MAC	00-00-00-00-00-00	Drop	  
☐	4	Port	TCP: 1 - 65535	Accept	  

Add

IPv6

☒ Enable IP Access Control:

Number Of Access Rules: 4

☐	Rule No	Rule Type	Rule	Policy	
☐	1	IP/Mask	::192.168.2.0	Accept	  
☐	2	IP Range	::192.168.3.1 - ::192.168.3.255	Accept	  
☐	3	MAC	00-00-00-00-00-00	Drop	  
☐	4	Port	TCP: 1 - 65535	Accept	  

Add

Field Name	Description
Rule No	A unique identifier for each access rule. Rules are processed in ascending order, and the rule number determines the priority.
Rule Type	Specifies the type of rule being created. Possible values include: • IP/Mask: Defines a single IP address or a subnet range using CIDR notation (e.g., 192.168.1.0/24 or 10.0.0.1/32). • IP Range: Defines a range of IP addresses, for example, 192.168.1.1-192.168.1.100. • MAC: Matches devices based on their Media Access Control (MAC) address, for example, 00:1A:2B:3C:4D:5E. • Port: Filters network traffic based on TCP or UDP protocols and specific port numbers or ranges (e.g., TCP:443 for HTTPS or TCP:22 for SSH).
Rule	The specific IP, subnet, MAC address, or port value to which the rule applies. Examples: • For IP/Mask: 192.168.1.0/24 • For IP Range: 192.168.1.1-192.168.1.100 • For MAC: 00:1A:2B:3C:4D:5E • For Port: TCP: 22-80
Policy	Defines the action to take when traffic matches the rule. Possible values include: • Accept: Allow the traffic to pass. • Drop: Silently discard the traffic without notifying the sender (common for blocking).
Number Of Access Rules	Indicates the total number of access rules currently configured or allowed. The system has a maximum limit of 10 rules.

Resource management

The **Resource Management** section focuses primarily on monitoring and managing power, aiming to help administrators optimize the system's energy usage. Through these settings, you can adjust power policies, view power consumption data, set automatic power on/off schedules, and more, thereby balancing performance requirements with energy efficiency needs to enhance system efficiency and reliability. These features are especially important in resource-intensive environments in business operations, helping to reduce energy costs and improve system stability.

Power

To go to **Power** page: Click **Resource management -> Power** from the main menu. This page is used to manage or configure Power related information.

BMC provides a feature that allows administrators to set a power limit for the CPU. This setting is especially important when the server is under heavy load, as it ensures the system consistently stays within the predefined power limit.

Even under high-performance demands, the server will not exceed the set power threshold, effectively preventing excessive power consumption, system overheating, performance degradation, and potential hardware damage.

Power

Set a power cap to keep power consumption at or below the specified value in watts

Current power consumption

CPU0 805.470302033265 Wh

CPU1 882.9599943174791 Wh

Power cap setting (CPU0)

☐ Apply power cap

Power cap value (in watts)

Value must be between 500
and 2900

Save

Power cap setting (CPU1)

☐ Apply power cap

Power cap value (in watts)

Value must be between 500
and 2900

Save

Power cap value (in watts):

This option can only be set when the **Apply power cap** is enabled.

Input the maximum allowable power consumption for the CPU, set in watts. This value helps limit the CPU's energy usage to a predefined threshold, ensuring it doesn't exceed the set power cap for efficiency and safety.

Value must be between xxx and xxx.

xxx: The values will vary depending on the platform.

If this is set to the maximum limit, it means disable power cap.

Power statistics

NVIDIA platform only has Entire Platform and CPU/GPU info. This page displays the current power consumption of the node, providing a detailed breakdown of CPU and GPU power usage, along with the total power consumption for the entire platform.

Power statistics

Current Node Power Consumption

Entire Platform :	6445.162 Watt
CPU 0 :	806.885 Watt
CPU 1 :	884.515 Watt
GPU 0 :	1136.559 Watt
GPU 1 :	1115.508 Watt
GPU 2 :	1236.522 Watt
GPU 3 :	1265.173 Watt

The Entire Platform power consumption is the sum of all CPU and GPU consumptions.

Power schedule

To go to **Power schedule** page. Click **Resource management -> Power schedule** from the main menu. This page allows users to manage automated power control tasks for the server. This feature enables you to schedule actions such as **powering** on or off the host at specified times and dates. Below is a detailed operation for using the power schedule interface and its features.

Supervyse OPF

Health Power Refresh root

Overview

Dashboard

Logs

Hardware status

Operations

Settings

Security and access

Resource management

NM power policy

Power statistics

Power schedule

BIOS

Storage

Power schedule

Delete all Add

Index	Enabled	Start Date	End Date	Trigger Date	Trigger Time	Action	
1	Enabled	2024-11-21	2024-11-23	Daily	03:05	Power Off Host - Immediate	
2	Enabled	2024-11-23	2024-11-23	2024-11-23	00:00	Power On Host	
3	Enabled	2024-11-21	2024-11-21	2024-11-21	23:00	Power Off Host - Immediate	
4	Disabled	2024-11-25	2024-11-25	2024-11-25	00:00	Power Off Host - Immediate	
5	Enabled	2024-11-26	2024-11-30	Monthly, 10	00:00	Reset Host	
6	Enabled	2024-11-21	2024-11-27	Weekly, Sunday	00:00	Graceful Shutdown (ACPI Off)	
7	Enabled	2024-11-21	2024-11-30	Daily	04:00	Power Off Host - Immediate	
8	Disabled	2024-11-21	2024-11-22	Daily	02:00	Reset Host	
9	Enabled	2024-11-21	2024-11-30	Daily	00:00	Power Cycle Host	
10	Enabled	2024-11-23	2024-11-30	Daily	00:00	Power Off Host - Immediate	

Add Schedule

×

Task

10

Enabled

Enabled

Action

Power Off Host - Immediate

Schedule

Time

00

:

00

Date

Specific

2024-12-24

Cancel

Add

BIOS

BIOS (Basic Input/Output System) is firmware located on the computer's motherboard, responsible for initializing hardware during startup and loading the operating system. BIOS is the first program that runs when the computer is powered on, ensuring that hardware and software work together correctly.

These pages allow you to view and configure settings that will be applied to the BIOS during the next boot.

Leak Detection

Leak detection will be performed by leak sensors inside the trays and leak sensors around the rack. The sensors are wired to a Sensor IC (or CPLD in the switch tray), which connects to the BMC (baseboard management controller) over I2C and through the interrupt line. The BMC will be responsible for:

Handling the interrupt by the sensor and reading the liquid amount (or fault condition), if applicable.

If an anomaly is detected:

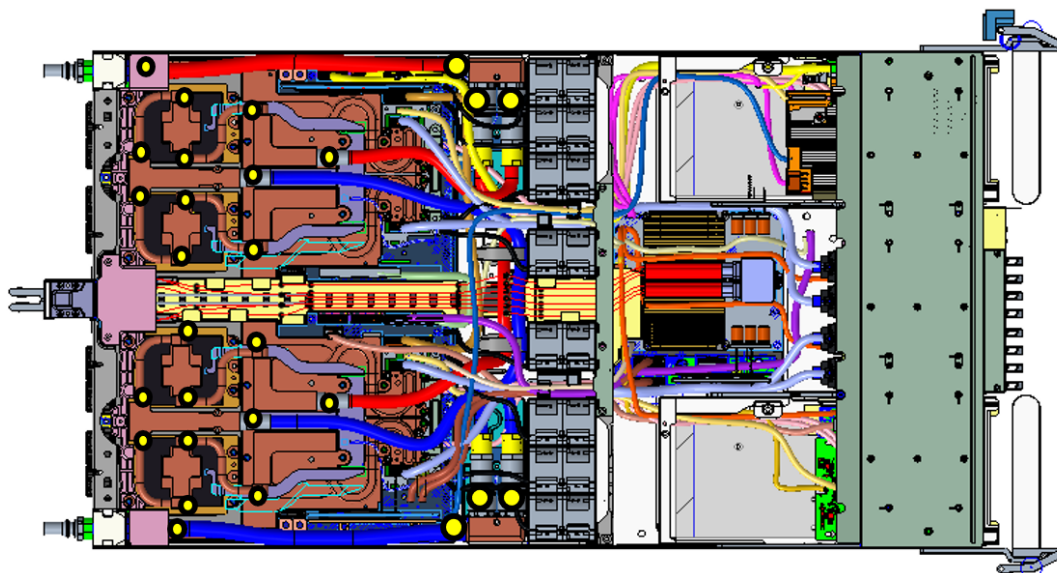
- Send a notification event (Redfish or gNMI, if applicable).
- Blink the amber fault LED in the front panel at 4 Hz.
- Taking emergency action if programmed (e.g. power down the tray)

Leak Sensors

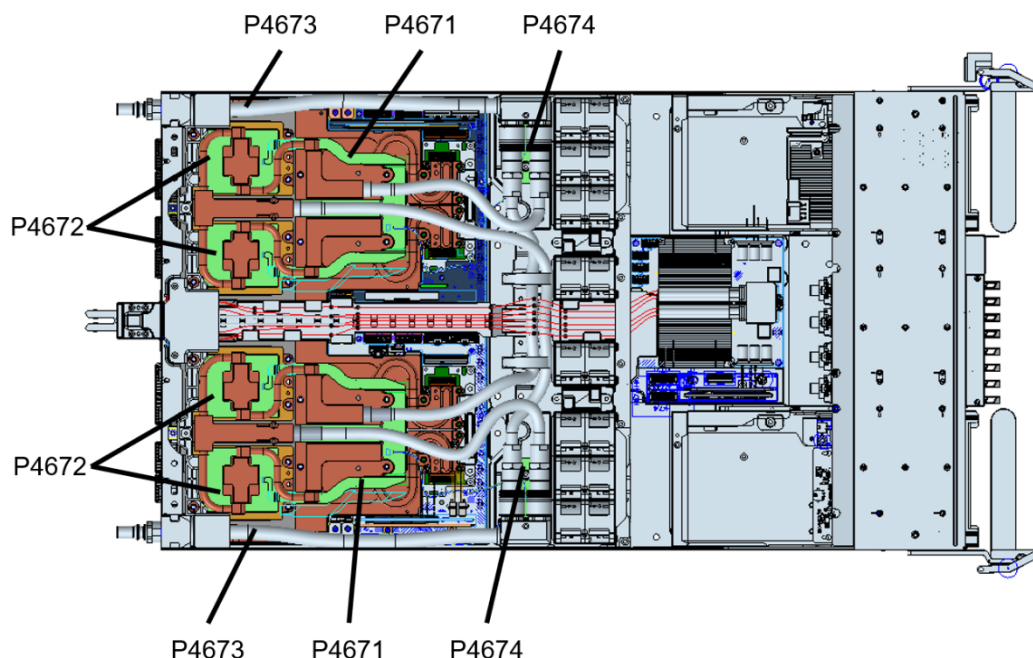
The GB300 NVL 72 trays incorporate custom shaped flex PCB sensors place on the top surface of the cold plates and under or near all O-ring seals, hoses, manifolds, and fluid couplings to be as close as possible to all potential leak locations.

High risk Leak Points

The GB300 NVL 72 tray included 28 locations identified, that would benefit from using leak sensors to reduce this risk.



NVIDIA MGX NVL Leak Sensor Installation Location



The list of leak sensors and their quantity used on the MGX compute tray as follows:

- P4671 – CPU sensor
- P4672 – GPU sensor
- P4673 – Tray QD sensor
- P4674 – Manifold Sensor

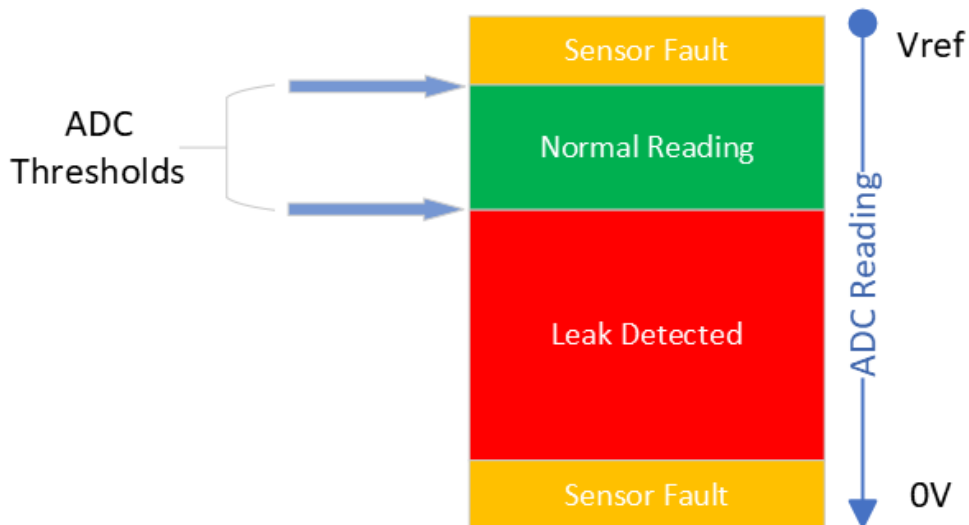
GB300 Leak Sensor Part Details

Chip	Use Case	Primary Board Addr.	Secondary Board Addr.
MAX1363	Primary	0x34h	0x35h
ADS7142	Alternate	0x18h	0x1Eh

As the leak detector sensor encounter liquid, the resistance across the sensor will drop, resulting in lower voltage input to the ADC. The BMC will need to determine if the ADC reading is abnormal or not. ADC output values can indicate the following conditions:

- Sensor resistance above normal range: leak detect sensor may have been disconnected (sensor fault).
- Sensor resistance decreased below normal range: indicates a potential leak

- Sensor resistance at or near zero: sensor may have been shorted, such as cases where it has come into contact with metal (sensor fault)



Check Leakage methods

Leak Self-Test

The leak detection and response can be tested by the FPGA I/O expander, TCA9555. Setting the output of IO1_7 high will pull the sensor input low to simulate a leak, for testing purpose.

Redfish Telemetry

The BMC will support the DMTF Redfish LeakDetection and LeakDetector schemas. The LeakDetection schema will provide information on the LeakDetectors available on the system, and the LeakDetector schema will provide information on the state of the particular LeakDetector.

Example telemetry output:

```
{
  "@odata.id": "/redfish/v1/Chassis/Chassis_0/ThermalSubsystem/LeakDetection/LeakDetectors/Chassis_0_LeakDetector_1_ColdPlate",
  "@odata.type": "#LeakDetector.v1_3_0.LeakDetector",
  "DetectorState": "OK",
  "Id": "Chassis_0_LeakDetector_1_ColdPlate",
  "LeakDetectorType": "Moisture",
  "Name": "Chassis 0 LeakDetector 1 ColdPlate",
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  }
}
```

```

{
  "@odata.id": "/redfish/v1/Chassis/Chassis_0/ThermalSubsystem/LeakDetection/LeakDetectors/Chassis_0_LeakDetector_0_ColdPlate",
  "@odata.type": "#LeakDetector.v1_3_0.LeakDetector",
  "DetectorState": "Critical",
  "Id": "Chassis_0_LeakDetector_0_ColdPlate",
  "LeakDetectorType": "Moisture",
  "Name": "Chassis 0 LeakDetector 0 ColdPlate",
  "Status": {
    "Health": "Critical",
    "State": "Degraded"
  }
}

```

Back-Up Shut Down Timer Configuration

The “Back-Up Shutdown Timer” feature allows the user to configure a timeout value, where upon timer expiration after a leak has been detected, the BMC will shut down the compute tray. The feature shall default to a disabled state, with the configuration accessible through Redfish properties:

/redfish/v1/Chassis/Chassis_0/Oem/Nvidia/Policies/LeakDetectionPolicy

```

"@odata.id": "/redfish/v1/Chassis/Chassis_0/Oem/Nvidia/Policies/LeakDetectionPolicy",
"@odata.type": "#NvidiaPolicy.v1_0_0.NvidiaPolicy",
"Id": "LeakDetectionPolicy",
"Name": "Policy for Leak Detection",
"PolicyConditionLogic": "AnyOf",
"PolicyConditions": [
  {
    "Property": "/redfish/v1/Chassis/Chassis_0/ThermalSubsystem/LeakDetection/LeakDetectors/Chassis_0_LeakDetector_0_ColdPlate/#DetectorState",
    "PropertyStringValue": "Critical"
  },
  {
    "Property": "/redfish/v1/Chassis/Chassis_0/ThermalSubsystem/LeakDetection/LeakDetectors/Chassis_0_LeakDetector_0_Manifold/#DetectorState",
    "PropertyStringValue": "Critical"
  },
  {
    "Property": "/redfish/v1/Chassis/Chassis_0/ThermalSubsystem/LeakDetection/LeakDetectors/Chassis_0_LeakDetector_1_ColdPlate/#DetectorState",
    "PropertyStringValue": "Critical"
  },
  {
    "Property": "/redfish/v1/Chassis/Chassis_0/ThermalSubsystem/LeakDetection/LeakDetectors/Chassis_0_LeakDetector_1_Manifold/#DetectorState",
    "PropertyStringValue": "Critical"
  }
],
"PolicyEnabled": false,
"PolicyReactions": [
  {
    "CommonReaction": "HardPowerOff",
    "ReactionDelaySeconds": 0.0
  }
],
"Status": {
  "Health": "OK",
  "State": "Enabled"
}

```

The user can PATCH the following properties to update Policy settings related to shutdown.

- PolicyEnabled
 - “true” - Shutdown enabled on leak detection
 - “false” - Shutdown disabled on leak detection
- PolicyReactions: ReactionDelaySeconds
 - Sets the delay in seconds after a leak is detected before BMC executes a system shutdown

The BMC shall persist such settings through resets and power cycles. Please note the final property naming and URI path may change as design is updated and feedback received.

BMC Firmware Secure

External Root of Trust (ERoT) hardware is part of the BMC module, which is intended for production. ERoT hardware provides a secure flash and boot mechanism to validate the BMC firmware is sourced from reliable organization.

(ERoT is currently not supported on BMC module card)

Secure Boot

- Meets NIST 800-193 PFR Guidelines
- **Detection and Recovery are currently not supported**
- Authenticates SPI Flash image before loading
- Support AES-256/384/512 Encrypted SPI Flash images

SPI Monitor

- Allows 50 MHz operation of SPI Flash (TBD)
- Real Time load module verification and execution path matching during Host boot
- Prevents unauthorized Read/Write/Erase during Host runtime

Redfish Update

- Support on-line redfish update with Insyde BMC

```
curl -k -u root:OpenBmc -H "Content-Type: application/octet-stream" -X POST -T <TARBALL>  
https://<BMC\_IP>/redfish/v1/UpdateService/update
```

Redfish

Redfish is a management standard which uses data model representation inside of a hypermedia RESTful interface. It is based on REST, that's how Redfish is easier to use and implement than many other solutions. Since its model oriented, it is capable of expressing the relationships between components in modern systems as well as the semantics of the services and components within them. It is also easily extensible. By using a hypermedia approach to REST, Redfish can express a large variety of systems from multiple vendors. Utilizing JSON (JavaScript Object Notation) data format which is in plain text, allows many types of parameters to be available such that it enables scalability, human readability, and flexibility for most programming environments by easily interpreting payload.

HTTP Methods

The following HTTP methods are used to implement different actions, as described below:

HTTP Method	Description
POST	The POST method is used to create a new resource. The POST request is submitted to the resource collection in which the new resource is to belong. Submitting a POST request to a resource representing a collection is equivalent to submitting the same request to the Members property of that resource. The POST method is used to initiate operations on the object (such as Actions). Services shall support the POST method for sending actions. The POST operation may not be idempotent.
GET	The GET method is used to retrieve a representation of a resource. That representation can either be a single resource or a collection.
PATCH	The PATCH method is the preferred method used to perform updates on pre-existing resources. Changes to the resource are sent in the request body. Properties not specified in the request body are not directly changed by the PATCH request. The response is either empty or a representation of the resource after the update was done. The implementation may reject the update operation on certain fields based on its own policies and, if so, shall not apply any of the update requested.
DELETE	The DELETE method is used to remove a resource. Services shall support the DELETE method for resources that can be deleted.

PUT	The PUT method is used to completely replace a resource. Properties omitted from the request body are reset to their default value.
-----	---

Status Code

HTTP defines status codes that can be returned in response messages.

Status Code	Status Name	Description
200	OK	The request was successfully completed and includes a representation in its body.
201	Created	A request that created a new resource completed successfully. The Location header shall be set to the canonical URI for the newly created resource. A representation of the newly created resource may be included in the response body.
202	Accepted	The request has been accepted for processing, but the processing has not been completed. The Location header shall be set to the URI of a Task resource that can later be queried to determine the status of the operation. A representation of the Task resource may be included in the response body.
204	No Content	The request succeeded, but no content is being returned in the body of the response.
301	Moved Permanently	The requested resource resides under a different URI
302	Found	The requested resource resides temporarily under a different URI.
304	Not Modified	The service has performed a conditional GET request where access is allowed, but the resource content has not changed. Conditional requests are initiated using the headers If-Modified-Since and/or If-None-Match (see HTTP 1.1, sections 14.25 and 14.26) to save network bandwidth if there is no change.
401	Unauthorized	The authentication credentials included with this request are missing or invalid.

403	Forbidden	The server recognized the credentials in the request, but those credentials do not possess authorization to perform this request.
404	Not Found	The request specified a URI of a resource that does not exist.
405	Method Not Allowed	The HTTP verb specified in the request (e.g., DELETE, GET, HEAD, POST, PUT, PATCH) is not supported for this request URI. The response shall include an Allow header which provides a list of methods that are supported by the resource identified by the Request-URI.
406	Not Acceptable	The Accept header was specified in the request and the resource identified by this request is not capable of generating a representation corresponding to one of the media types in the Accept header.
409	Conflict	A creation or update request could not be completed, because it would cause a conflict in the current state of the resources supported by the platform (for example, an attempt to set multiple attributes that work in a linked manner using incompatible values).
410	Gone	The requested resource is no longer available at the server and no forwarding address is known. This condition is expected to be considered permanent. Clients with link editing capabilities SHOULD delete references to the Request-URI after user approval. If the server does not know, or has no facility to determine, whether or not the condition is permanent, the status code 404 (Not Found) SHOULD be used instead. This response is cacheable unless indicated otherwise.
411	Length Required	The request did not specify the length of its content using the Content-Length header (perhaps Transfer-Encoding: chunked was used instead). The addressed resource requires the Content-Length header.
412	Precondition Failed	Precondition (such as OData-Version, If Match or If Not Modified headers) check failed.

415	Unsupported Media Type	The request specifies a Content-Type for the body that is not supported.
500	Internal Server Error	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	Not Implemented	The server does not (currently) support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting the method for any resource.
503	Service Unavailable	The server is currently unable to handle the request due to temporary overloading or maintenance of the server.

Available APIs

Username: root Password: OpenBmc

Resource	Resource URI	Redfish Schema
ServiceRoot	/redfish/v1/	ServiceRoot.v1_17_0.ServiceRoot
ComputerSystemCollection	/redfish/v1/Systems	ComputerSystemCollection.ComputerSystemCollection
ComputerSystem	/redfish/v1/Systems/<SystemID>	ComputerSystem.v1_23_1.ComputerSystem
BootOptionCollection	/redfish/v1/Systems/<SystemID>/BootOptions	BootOptionCollection.BootOptionCollection
BootOption	/redfish/v1/Systems/<SystemID>/BootOptions/<BootOptionId>	BootOption.v1_0_6.BootOption
MemoryCollection	/redfish/v1/Systems/<SystemID>/Memory	MemoryCollection.MemoryCollection
Memory	/redfish/v1/Systems/<SystemID>/Memory/<MemoryID>	Memory.v1_20_0.Memory
ProcessorCollection	/redfish/v1/Systems/<SystemID>/Processors	ProcessorCollection.ProcessorCollection
Processor	/redfish/v1/Systems/<SystemID>/Processors/<ProcessorId>	Processor.v1_20_0.Processor
EthernetInterfaceCollection	/redfish/v1/Managers/<ManagerId>/EthernetInterfaces	EthernetInterfaceCollection.EthernetInterfaceCollection
EthernetInterface	/redfish/v1/Managers/<ManagerId>/EthernetInterfaces/<InterfaceId>	EthernetInterface.v1_12_3.EthernetInterface
Bios	/redfish/v1/Systems/<SystemID>/Bios /redfish/v1/Systems/<SystemID>/Bios/Settings	Bios.v1_2_3.Bios Bios.v1_2_3.Bios
LogServiceCollection	/redfish/v1/Systems/<SystemID>/LogServices	LogServiceCollection.LogServiceCollection
LogService	/redfish/v1/Systems/<SystemID>/LogServices/<LogType>	LogService.v1_7_0.LogService
LogEntryCollection	/redfish/v1/Systems/<SystemID>/LogServices/<LogType>/Entries	LogEntryCollection.LogEntryCollection
LogEntry	/redfish/v1/Systems/<SystemID>/LogServices/<LogType>/Entries/<EntryId>	LogEntry.v1_17_0.LogEntry
Chassis		
ChassisCollection	/redfish/v1/Chassis	ChassisCollection.ChassisCollection

Chassis	/redfish/v1/Chassis/<ChassisID>	Chassis.v1_26_0.Chassis
Power	/redfish/v1/Chassis/Self/Power	Power.v1_5_4.Power (TBD, Intel/AMD)
Thermal	/redfish/v1/Chassis/Self/Thermal	Thermal.v1_5_3.Thermal (TBD, Intel/AMD)
PowerSubsystem	/redfish/v1/Chassis/<ChassisID>/PowerSubsystem	PowerSubsystem.v1_1_3.PowerSubsystem
PowerSupplyCollection	/redfish/v1/Chassis/<ChassisID>/PowerSubsystem/PowerSupplies	PowerSupplyCollection.PowerSupplyCollection
PowerSupply	/redfish/v1/Chassis/<ChassisID>/PowerSubsystem/PowerSupplies/<PowerSupplyId>	PowerSupply.v1_4_0.PowerSupply
ThermalSubSystem	/redfish/v1/Chassis/<ChassisID>/ThermalSubsystem	ThermalSubsystem.v1_3_3.ThermalSubsystem
ThermalMetrics	/redfish/v1/Chassis/<ChassisID>/ThermalSubsystem/ThermalMetrics	ThermalMetrics.v1_3_2.ThermalMetrics
FanCollection	/redfish/v1/Chassis/<ChassisID>/ThermalSubsystem/Fans	FanCollection.FanCollection
Fan	/redfish/v1/Chassis/<ChassisID>/ThermalSubsystem/Fans/<FanId>	Fan.v1_5_2.Fan
Managers		
ManagerCollection	/redfish/v1/Managers	ManagerCollection.ManagerCollection
Manager	/redfish/v1/Managers/<ManagerID>	Manager.v1_20_0.Manager
ManagerNetworkProtocol	/redfish/v1/Managers/<ManagerID>/NetworkProtocol	ManagerNetworkProtocol.v1_10_1.ManagerNetworkProtocol
SerialInterfaceCollection	/redfish/v1/Managers/<ManagerID>/SerialInterfaces	SerialInterfaceCollection.SerialInterfaceCollection
SerialInterface	/redfish/v1/Managers/<ManagerID>/SerialInterfaces/<SerialInterfaceId>	SerialInterface.v1_2_1.SerialInterface
General		
AccountService	/redfish/v1/AccountService	AccountService.v1_17_0.AccountService
Manager Account Collection	/redfish/v1/AccountService/Accounts	ManagerAccountCollection.ManagerAccountCollection
Manager Account	/redfish/v1/AccountService/Accounts/<AccountId>	ManagerAccount.v1_13_0.ManagerAccount
Role Collection	/redfish/v1/AccountService/Roles	RoleCollection.RoleCollection
Role	/redfish/v1/AccountService/Roles/<RoleId>	Role.v1_3_3.Role

EventService	/redfish/v1/EventService	EventService.v1_10_3.EventService
Event Destination Collection	/redfish/v1/EventService/Subscriptions	EventDestinationCollection.EventDestinationCollection
EventDestination	/redfish/v1/EventService/Subscriptions/<Subscriptions_ID>	EventDestination.v1_13_0.EventDestination (TBD)
TaskService	/redfish/v1/TaskService	TaskService.v1_2_1.TaskService
TaskCollection	/redfish/v1/TaskService/Tasks	TaskCollection.TaskCollection
Task	/redfish/v1/TaskService/Tasks/{{Task_instance}}	Task.v1_7_4.Task
JSON Schema file collection	/redfish/v1/JsonSchemas	JsonSchemaFileCollection.JsonSchemaFileCollection
JSON Schema file	/redfish/v1/JsonSchemas/<json_schema_name>	JsonSchemaFile.v1_1_5.JsonSchemaFile
Session Service	/redfish/v1/SessionService	SessionService.v1_2_0.SessionService
Session Collection	/redfish/v1/SessionService/Sessions	SessionCollection.SessionCollection
Session	/redfish/v1/SessionService/Sessions/<SessionId>	Session.v1_8_0.Session
MessageRegistryFileCollection	/redfish/v1/Registries	MessageRegistryFileCollection.MessageRegistryFileCollection
MessageRegistryFile	/redfish/v1/Registries/Base TaskEvent ResourceEvent OpenBMC	MessageRegistryFile.v1_1_5.MessageRegistryFile
Storage Collection	/redfish/v1/Systems/<SystemID>/Storage	StorageCollection.StorageCollection
Storage	/redfish/v1/Systems/<SystemID>/Storage/<StorageId>	Storage.v1_18_0.Storage
UpdateService	/redfish/v1/UpdateService	UpdateService.v1_15_0.UpdateService
SecureBoot	/redfish/v1/Systems/<SystemID>/SecureBoot	SecureBoot.v1_1_2.SecureBoot
DrivesCollection	/redfish/v1/Systems/<SystemID>/Storage/<StorageId>/Drives	DriveCollection.DriveCollection
Drive for NVME	/redfish/v1/Systems/<SystemID>/Storage/SystemDisk1/Drives/<DriveId>	Drive.v1_21_0.Drive
Drive for SATA	/redfish/v1/Systems/<SystemID>/Storage/SystemDisk1/Drives/<DriveId>	Drive.v1_21_0.Drive
Drive for RAID	/redfish/v1/Systems/<SystemID>/Storage/SystemDisk1/Drives/<DriveId>	Drive.v1_21_0.Drive

SensorCollection	/redfish/v1/Chassis/<ChassisID>/Sensors	SensorCollection.SensorCollection
Sensor	/redfish/v1/Chassis/<ChassisID>/Sensors/<SensorId>	Sensor.v1_10_1.Sensor
SecureBootDatabasesCollection	/redfish/v1/Systems/system/SecureBoot/SecureBootDatabases	SecureBootDatabaseCollection.SecureBootDatabaseCollection
SecureBootDatabase	/redfish/v1/Systems/system/SecureBoot/SecureBootDatabases/<SecureBootDatabaseID>	SecureBootDatabase.v1_0_3.SecureBootDatabase
Certificate		
CertificateService	/redfish/v1/CertificateService	CertificateService.v1_0_6.CertificateService
CertificateLocations	/redfish/v1/CertificateService/CertificateLocations	CertificateLocations.v1_0_4.CertificateLocations
CertificateCollection	/redfish/v1/Managers/<ManagerID>/NetworkProtocol/HTTPS/Certificates /redfish/v1/AccountService/LDAP/Certificates /redfish/v1/Managers/<ManagerID>/Truststore/Certificates /redfish/v1/Managers/<ManagerID>/VirtualMedia/Oem/Insyde/Certificates /redfish/v1/Systems/<SystemID>/Boot/Certificates /redfish/v1/Chassis/<ERoTChassisID>/Certificates	CertificateCollection.CertificateCollection
Certificate	Reference above.	Certificate.v1_9_0.Certificate
FirmwareInventory		
SoftwareInventoryCollection	/redfish/v1/UpdateService/FirmwareInventory	SoftwareInventoryCollection.SoftwareInventoryCollection
SoftwareInventory	/redfish/v1/UpdateService/FirmwareInventory/<SoftwareInventoryId>	SoftwareInventory.v1_10_2.SoftwareInventory
HostInterfaceCollection	/redfish/v1/Managers/<ManagerID>/HostInterfaces	HostInterfaceCollection.HostInterfaceCollection
HostInterface	/redfish/v1/Managers/<ManagerID>/HostInterfaces/<HostInterfaceId>	HostInterface.v1_3_3.HostInterface
Telemetry		
TelemetryService	/redfish/v1/TelemetryService	TelemetryService.v1_3_4.TelemetryService
MetricDefinitionCollection	/redfish/v1/TelemetryService/MetricDefinitions	MetricDefinitionCollection.MetricDefinitionCollection
MetricDefinition	/redfish/v1/TelemetryService/MetricDefinitions/<MetricDefinitionID>	MetricDefinition.v1_3_4.MetricDefinition

MetricReportDefinitionCollection	/redfish/v1/TelemetryService/MetricReportDefinitions	MetricReportDefinitionCollection.MetricReportDefinitionCollection
MetricReportDefinitions	/redfish/v1/TelemetryService/MetricReportDefinitions/<MetricReportDefinitionId>	MetricReportDefinition.v1_4_1.MetricReportDefinition
MetricReportCollection	/redfish/v1/TelemetryService/MetricReports	MetricReportCollection.MetricReportCollection
MetricReport	/redfish/v1/TelemetryService/MetricReports/<MetricReportId>	MetricReport.v1_4_2.MetricReport
TriggersCollection	/redfish/v1/TelemetryService/Triggers	TriggersCollection.TriggersCollection
Triggers	/redfish/v1/TelemetryService/Triggers/<TriggersID>	Triggers.v1_4_0.Triggers

Common Gateway Interface

The Common Gateway Interface (CGI) is a standard method that defines how web servers interact with external programs to generate dynamic content. Essentially, it acts as an interface between a web server (like Apache) and an executable program (often called a CGI program or script), enabling the server to pass user requests and data to the program and receive dynamic content back, typically in the form of HTML

Beyond Redfish API operations, our BMC still maintain multiple CGI interfaces for debug and deep operation usage.

Session & Cookies

To ensure CGI functions properly, a cookie mechanism is required to maintain the on-going session. Below is example command for start session and obtain cookie.

bmc=192.168.100.1

user=root

pass=openBmc

```
cookie=$(mktemp /tmp/cookie-XXXXXXX)

##Login

curl -s -k -c "$cookie" -X POST -H 'Content-Type: application/json' -d
'{"data":["$user","$pass"]}' https://\$bmc/login

## Get CSRF

csrf=$(cat $cookie | sed -nre 's/\.XSRF-TOKEN\s(.*)$/\1/p')

## Request Simple GET

curl -k -c "$cookie" -b "$cookie" -X GET -H 'QUERY: DATETIME'
https://\$bmc/cgi/config\_datetime.cgi

##Logout

curl -k -c "$cookie" -b "$cookie" -X POST -H "X-XSRF-TOKEN: $csrf"
https://\$bmc/logout
```

For POST, PUT, and DELETE requests, an additional CSRF token check is required.

Please make sure to include the CSRF token in the request header using the key X-XSRF-TOKEN.

In addition, please ensure that the request method and corresponding data are properly specified.

Here's an example of how to add it:

```
curl -k -c "$cookie" -b "$cookie" -X POST -H "X-XSRF-TOKEN: $csrf" -H
'QUERY: DATETIME2' -H 'Content-Type: application/json' -d
'{"ntp":{"primaryNTPServer":"time.google.com",
"secondaryNTPServer":"ntp.ubuntu.com"}}'
https://\${bmc}/cgi/config\_datetime.cgi
```

Note: Do not forget to log out to drop session.

```
jasmine@TPEA90158309:~$ curl -k -c "$cookie" -b "$cookie" -X GET -H "QUERY: CHASSIS_STATUS" https://${bmc}/cgi/chassis.cgi
{
  "powerStatus": "off"
}
jasmine@TPEA90158309:~$ curl -k -c "$cookie" -b "$cookie" -X GET -H "QUERY: LED_STATUS" https://${bmc}/cgi/chassis.cgi
{
  "powerLED": {
    "color": 0,
    "state": 0
  },
  "statusLED": {
    "color": 0,
    "state": 0
  },
  "chassisLED": {
    "color": 0,
    "state": 0
  }
}
jasmine@TPEA90158309:~$
```

Compliance Information

限用物質含有情況標示聲明書

設備名稱: 伺服器 Equipment name :		型號 (型式) : GS-31B00 Type designation (Type):				
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機箱/擋板 Chassis/Enclosure	—	○	○	○	○	○
金屬機械部件(支架) Metallic Mech parts,(Bracket)	○	○	○	○	○	○
電路板組件 PCBA	—	○	○	○	○	○
機構零件 Metallic Accessories	○	○	○	○	○	○
散熱片 Heatsink	○	○	○	○	○	○
連接線 Cable	—	○	○	○	○	○
配件 Accessories	○	○	○	○	○	○
備考1. “超出0.1 wt %”及“超出0.01 wt %”係指限用物質之百分比含量超出百分比含量基準值。 Note 1 : “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition. 備考2. “○”係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2 : “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence. 備考3. “—”係指該項限用物質為排除項目。 Note 3 : The “—” indicates that the restricted substance corresponds to the exemption.						

FCC, Class A - USA

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

ICES-003 Class A Notice - Avis NMB-003, Class A - Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CISPR 32 / EN 55032, Class A - International, European Union

Warning: Operation of this equipment in a residential environment could cause radio interference.

VCCI, Class A – Japan

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI – A