Contents

1 Introduction to the NVIDIA DGX H100 System 3
  1.1 Hardware Overview ........................................ 3
    1.1.1 DGX H100 Component Descriptions .................. 3
    1.1.2 Mechanical Specifications ........................... 4
    1.1.3 Power Specifications ................................ 5
      1.1.3.1 Support for PSU Redundancy and Continuous Operation 5
    1.1.4 DGX H100 Locking Power Cord Specification ....... 5
    1.1.5 Using the Locking Power Cords ....................... 6
    1.1.6 Environmental Specifications ....................... 7
    1.1.7 Front Panel Connections and Controls ............... 7
      1.1.7.1 With a Bezel .................................. 7
      1.1.7.2 With the Bezel Removed ........................ 8
    1.1.8 Rear Panel Modules ................................ 9
    1.1.9 Motherboard Connections and Controls .............. 10
    1.1.10 Motherboard Tray Components ...................... 10
    1.1.11 GPU Tray Components .............................. 11
  1.2 Network Connections, Cables, and Adaptors .......... 12
    1.2.1 Network Ports ...................................... 12
    1.2.2 Compute and Storage Networking .................... 14
    1.2.3 Network Modules ................................... 14
    1.2.4 BMC Port LEDs ..................................... 15
    1.2.5 Supported Network Cables and Adaptors ............ 15
  1.3 DGX H100 System Topology .............................. 16
  1.4 DGX OS Software ........................................ 16
  1.5 Customer Support ........................................ 17

2 Connecting to the DGX H100 19
  2.1 Connecting to the Console ............................... 19
    2.1.1 Direct Connection .................................. 19
    2.1.2 Remote Connection through the BMC ................ 21
  2.2 SSH Connection to the OS ................................ 23

3 First Boot Setup ............................................ 25
  3.1 System Setup ............................................ 25
  3.2 Post Setup Tasks ....................................... 27
    3.2.1 Obtaining Software Updates ......................... 27
    3.2.2 Enabling the SRP Daemon ........................... 27

4 Quickstart and Basic Operation .......................... 29
  4.1 Installation and Configuration .......................... 29
  4.2 Registration ............................................. 29
  4.3 Obtaining an NGC Account ............................... 30
  4.4 Turning DGX H100 On and Off ............................ 30
4.4.1 Startup Considerations .............................................. 30
4.4.2 Shutdown Considerations ........................................... 30
4.5 Verifying Functionality - Quick Health Check ..................... 30
4.6 Running the Pre-flight Test ............................................. 31
4.7 Running NGC Containers with GPU Support ....................... 32
  4.7.1 Using Native GPU Support ........................................ 32
  4.7.2 Using the NVIDIA Container Runtime for Docker .......... 33
4.8 Managing CPU Mitigations .............................................. 34
  4.8.1 Determining the CPU Mitigation State of the DGX System 34
  4.8.2 Disabling CPU Mitigations ...................................... 35
  4.8.3 Re-enabling CPU Mitigations .................................. 35

5 SBIOS Settings ............................................................. 37
  5.1 Accessing the SBIOS Setup ......................................... 37
  5.2 Configuring the Boot Order ......................................... 38
  5.3 Configuring the Local Terminal ..................................... 40
    5.3.1 Linux ................................................................. 40
    5.3.2 Windows and MacOS ............................................ 40
  5.4 Power on or Reboot the System .................................... 40

6 Using the Baseboard Management Controller (BMC) .................. 41
  6.1 Connecting to the BMC ............................................... 41
  6.2 Overview of BMC Controls .......................................... 42
  6.3 Changing the BMC Login Credentials ............................... 45
    6.3.1 User Name and Password Requirements .................... 45
    6.3.2 Procedure ......................................................... 45
  6.4 Using the Remote Console .......................................... 46
  6.5 Setting Up Active Directory, LDAP, or E-Directory ............. 46
  6.6 Configuring Platform Event Filters ................................. 47
  6.7 Uploading or Generating SSL Certificates .......................... 47
    6.7.1 Viewing the SSL Certificate ................................ 48
    6.7.2 Generating the SSL Certificate ............................... 49
    6.7.3 Uploading the SSL Certificate ................................ 50
    6.7.4 Updating the SBIOS Certificate ............................... 50

7 Security ................................................................. 55
  7.1 User Security Measures ............................................. 55
    7.1.1 Securing the BMC Port ........................................ 55
  7.2 System Security Measures .......................................... 55
    7.2.1 Secure Flash of DGX H100 Firmware .......................... 56
    7.2.2 Encryption ....................................................... 56
    7.2.3 NVIDIA System Manager Security ............................. 56
  7.3 Secure Data Deletion ............................................... 56
    7.3.1 Prerequisites ..................................................... 56
    7.3.2 Procedure ....................................................... 57

8 Redfish APIs Support ................................................... 59
  8.1 Supported Redfish Features ....................................... 59
  8.2 Connectivity Between the Host and BMC ............................ 60
  8.3 Redfish Examples ..................................................... 60
    8.3.1 BMC Manager .................................................... 60
    8.3.2 Firmware Update ................................................. 61
    8.3.3 BIOS Settings .................................................... 63
    8.3.4 Telemetry .......................................................... 64
    8.3.5 Chassis .............................................................. 65
### 8.3.6 SEL Logs

- Page 65

### 8.3.7 Virtual Image

- Page 65

### 8.3.8 Collect BMC Debug Data

- Page 66

### 8.3.9 Clear BIOS and Reset to Factory Defaults

- Page 66

### 9 Safety

- Page 67

#### 9.1 Safety Information

- Page 67

#### 9.2 Safety Warnings and Cautions

- Page 67

#### 9.3 Intended Application Uses

- Page 68

#### 9.4 Site Selection

- Page 68

#### 9.5 Equipment Handling Practices

- Page 69

##### 9.6 Electrical Precautions

- Page 69

###### 9.6.1 Power and Electrical Warnings

- Page 69

###### 9.6.2 Power Cord Warnings

- Page 70

#### 9.7 System Access Warnings

- Page 70

#### 9.8 Rack Mount Warnings

- Page 71

#### 9.9 Electrostatic Discharge

- Page 72

#### 9.10 Other Hazards

- Page 72

##### 9.10.1 CALIFORNIA DEPARTMENT OF TOXIC SUBSTANCES CONTROL

- Page 72

##### 9.10.2 NICKEL

- Page 72

##### 9.10.3 Battery Replacement

- Page 72

##### 9.10.4 Cooling and Airflow

- Page 73

### 10 Compliance

- Page 75

#### 10.1 United States

- Page 75

#### 10.2 United States/Canada

- Page 75

#### 10.3 Canada

- Page 76

#### 10.4 CE

- Page 76

#### 10.5 Australia and New Zealand

- Page 77

#### 10.6 Brazil

- Page 77

#### 10.7 Japan

- Page 77

#### 10.8 South Korea

- Page 79

#### 10.9 China

- Page 80

#### 10.10 Taiwan

- Page 82

#### 10.11 Russia/Kazakhstan/Belarus

- Page 83

#### 10.12 Israel

- Page 84

#### 10.13 India

- Page 84

#### 10.14 South Africa

- Page 85

#### 10.15 Great Britain (England, Wales, and Scotland)

- Page 85

### 11 Third-Party License Notices

- Page 87

#### 11.1 Micron msecli

- Page 87

#### 11.2 Mellanox (OFED)

- Page 88

### 12 Notices

- Page 89

#### 12.1 Notice

- Page 89

#### 12.2 Trademarks

- Page 90

#### 12.3 Copyright

- Page 90
The *NVIDIA DGX H100 System User Guide* is also available as a PDF.
Chapter 1. Introduction to the NVIDIA DGX H100 System

The NVIDIA DGX H100 System is the universal system purpose-built for all AI infrastructure and workloads, from analytics to training to inference. The system is built on eight NVIDIA H100 Tensor Core GPUs.

1.1. Hardware Overview

1.1.1. DGX H100 Component Descriptions

The NVIDIA DGX H100 640GB system includes the following components.
Table 1: Component Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPU</td>
<td>8 x NVIDIA H100 GPUs that provide 640 GB total GPU memory</td>
</tr>
<tr>
<td>CPU</td>
<td>2 x Intel Xeon 8480C PCIe Gen5 CPU with 56 cores each 2.0/2.9/3.8 GHz (base/all core turbo/Max turbo)</td>
</tr>
<tr>
<td>NVSwitch</td>
<td>4 x 4th generation NVLink that provide 900 GB/s GPU-to-GPU bandwidth</td>
</tr>
<tr>
<td>Storage (OS)</td>
<td>2 x 1.92 TB NVMe M.2 SSD (ea) in RAID 1 array</td>
</tr>
<tr>
<td>Storage (Data Cache)</td>
<td>8 x 3.84 TB NVMe U.2 SED (ea) in RAID 0 array</td>
</tr>
<tr>
<td>Network (Cluster) card</td>
<td>4 x OSFP ports for 8 NVIDIA ConnectX-7 Single Port InfiniBand cars that each provide the following speeds: InfiniBand (default): Up to 400Gbps Ethernet: 400GbE, 200GbE, 100GbE, 50GbE, 40GbE, 25GbE, and 10GbE</td>
</tr>
<tr>
<td>Network (Storage) card</td>
<td>2 x NVIDIA ConnectX-7 Dual Port Ethernet cards that each provide the following speeds: Ethernet (default): 400GbE, 200GbE, 100GbE, 50GbE, 40GbE, 25GbE, and 10GbE InfiniBand: Up to 400Gbps</td>
</tr>
<tr>
<td>System Memory (DIMM)</td>
<td>2 TB per 32 DIMMs</td>
</tr>
</tbody>
</table>
| BMC (out-of-band system management) | 1 GbE RJ45 interface  
Supports Redfish, IPMI, SNMP, KVM, and Web user interface |
| In-band system management | Dual port 100GbE in slot 3 and 10 GbE RJ45 interface |
| Power Supply         | 6 x 3.3 kW                                                                 |

1.1.2. Mechanical Specifications

Table 2: Mechanical Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>8U Rackmount</td>
</tr>
<tr>
<td>Height</td>
<td>14” (356 mm)</td>
</tr>
<tr>
<td>Width</td>
<td>19” (482.3 mm) max</td>
</tr>
<tr>
<td>Depth</td>
<td>35.3” (897.1 mm) max</td>
</tr>
<tr>
<td>System Weight</td>
<td>287.6 lbs (130.45 kg) max</td>
</tr>
</tbody>
</table>
1.1.3. Power Specifications

The DGX H100 system contains six power supplies with balanced distribution of the power load.

Table 3: Table 3. Power Specifications

<table>
<thead>
<tr>
<th>Input</th>
<th>Specification for Each Power Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>200-240 volts AC</td>
<td>10.2 kW max.</td>
</tr>
<tr>
<td></td>
<td>3300 W @ 200-240 V, 16 A, 50-60 Hz</td>
</tr>
</tbody>
</table>

1.1.3.1 Support for PSU Redundancy and Continuous Operation

The system includes six power supply units (PSU) configured for 4+2 redundancy. Refer to the following additional considerations:

▶ If a PSU fails, troubleshoot the cause and replace the failed PSU immediately.
▶ If faulty PSUs must be replaced, the system should be idle or shut down the system and install operational PSUs.
▶ If three PSUs lose power as a result of a data center issue or power distribution unit failure, the system continues to function, but at a reduced performance level.
▶ If only three PSUs have power, shut down the system before replacing an operational PSU.
▶ The system only boots if at least three PSUs are operational. If fewer than three PSUs are operational, only the BMC is available.
▶ Do not operate the system with PSUs depopulated.

1.1.4. DGX H100 Locking Power Cord Specification

The DGX H100 is shipped with a set of six (6) locking power cords which have been qualified for use with the DGX H100 to ensure regulatory compliance.

**Warning:** To avoid electric shock or fire, only use the NVIDIA-provided power cords to connect power to the DGX H100. For more details, refer to *Electrical Precautions*.

**Important:** Do not use the provided cables with any other product or for any other purpose.
1.1.5. Using the Locking Power Cords

This section provides information about how to use the locking power cords.

**Locking and Unlocking the PDU Side**

Power Distribution Unit side
- To INSERT, push the cable into the PDU socket.
- To REMOVE, press the clips together and pull the cord out of the socket.

**Locking/Unlocking the PSU Side (Cords with Twist-Lock Mechanism)**

Power Supply (System) side - Twist locking
- To INSERT or REMOVE make sure the cable is UNLOCKED and push/ pull into/out of the socket.

To UNLOCK the power cord, twist the gray locking ring to the unlocked position (indicator will show an unlocked padlock).

To LOCK the power cord, twist the gray locking ring to the locked position (indicator should show a locked padlock).
1.1.6. Environmental Specifications

Here are the environmental specifications for your DGX H100 system.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>5° C to 30° C (41° F to 86° F)</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>20% to 80% non-condensing</td>
</tr>
<tr>
<td>Airflow</td>
<td>1105 CFM Front-to-Back @ 80% fan PWM</td>
</tr>
<tr>
<td>Heat Output</td>
<td>38,557 BTU/hr</td>
</tr>
</tbody>
</table>

1.1.7. Front Panel Connections and Controls

This section provides information about the front panel, connections, and controls of the DGX H100 system.

1.1.7.1 With a Bezel

Here is an image of the DGX H100 system with a bezel.
<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Button</td>
<td>Press to turn the DGX H100 system On or Off.</td>
</tr>
<tr>
<td></td>
<td>- Green flashing (1 Hz): Standby (BMC booted)</td>
</tr>
<tr>
<td></td>
<td>- Green flashing (4 Hz): POST in progress</td>
</tr>
<tr>
<td></td>
<td>- Green solid On: Power On</td>
</tr>
<tr>
<td>ID Button</td>
<td>Press to have the blue LED turn On or blink (configurable through the BMC)</td>
</tr>
<tr>
<td></td>
<td>as an identifier during servicing.</td>
</tr>
<tr>
<td></td>
<td>Also causes an LED on the back of the unit to flash as an identifier during</td>
</tr>
<tr>
<td></td>
<td>servicing.</td>
</tr>
<tr>
<td>Fault LED</td>
<td>Amber On: System or component faulted</td>
</tr>
</tbody>
</table>

**1.1.7.2 With the Bezel Removed**

Here is an image of the DGX H100 system without a bezel.

---

**Important:** Refer to the section *First Boot Setup* for instructions on how to properly turn the system.
1.1.8. Rear Panel Modules

Here is an image that shows the real panel modules on DGX H100.
1.1.9. Motherboard Connections and Controls

Here is an image that shows the motherboard connections and controls in a DGX H100 system.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Button</td>
<td>Press to turn the system On or Off.</td>
</tr>
<tr>
<td>ID LED Button</td>
<td>Blinks when ID button is pressed from the front of the unit as an aid in identifying the unit needing servicing.</td>
</tr>
<tr>
<td>BMC Reset button</td>
<td>Press to manually reset the BMC.</td>
</tr>
</tbody>
</table>

See *Network Connections, Cables, and Adaptors* for details on the network connections.

1.1.10. Motherboard Tray Components

Here is an image that shows the motherboard tray components in DGX H100.
1.1.11. GPU Tray Components

Here is an image of the GPU tray components in a DGX H100 system.
1.2. Network Connections, Cables, and Adaptors

This section provides information about network connections, cables, and adaptors.

1.2.1. Network Ports

Here is an image that shows the network ports on a DGX H100 system.
<table>
<thead>
<tr>
<th>Port</th>
<th>PCI Bus</th>
<th>Default</th>
<th>Optional</th>
<th>RDMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSFP1P1</td>
<td>dc:00.0</td>
<td>ibp220s0</td>
<td>enp220s0np0</td>
<td>mlx5_11</td>
</tr>
<tr>
<td>OSFP1P2</td>
<td>9a:00.0</td>
<td>ibp154s0</td>
<td>enp154s0np0</td>
<td>mlx5_6</td>
</tr>
<tr>
<td>OSFP2P1</td>
<td>ce:00.0</td>
<td>ibp206s0</td>
<td>enp206s0np0</td>
<td>mlx5_10</td>
</tr>
<tr>
<td>OSFP2P2</td>
<td>c0:00.0</td>
<td>ibp192s0</td>
<td>enp192s0np0</td>
<td>mlx5_9</td>
</tr>
<tr>
<td>OSFP3P1</td>
<td>4f:00.0</td>
<td>ibp79s0</td>
<td>enp79s0np0</td>
<td>mlx5_4</td>
</tr>
<tr>
<td>OSFP3P2</td>
<td>40:00.0</td>
<td>ibp64s0</td>
<td>enp64s0np0</td>
<td>mlx5_3</td>
</tr>
<tr>
<td>OSFP4P1</td>
<td>5e:00.0</td>
<td>ibp94s0</td>
<td>enp94s0np0</td>
<td>mlx5_5</td>
</tr>
<tr>
<td>OSFP4P2</td>
<td>18:00.0</td>
<td>ibp24s0</td>
<td>enp24s0np0</td>
<td>mlx5_0</td>
</tr>
<tr>
<td>Slot1 P1</td>
<td>aa:00.0</td>
<td>ibp170s0f0</td>
<td>enp170s0f0np0</td>
<td>mlx5_7</td>
</tr>
<tr>
<td>Slot1 P2</td>
<td>aa:00.1</td>
<td>enp170s0f1np1</td>
<td>ibp170s0f1np1</td>
<td>mlx5_8</td>
</tr>
<tr>
<td>Slot2 P1</td>
<td>29:00.0</td>
<td>ibp41s0f0</td>
<td>enp41s0f0np0</td>
<td>mlx5_1</td>
</tr>
<tr>
<td>Slot2 P2</td>
<td>29:00.1</td>
<td>enp41s0f1np1</td>
<td>ibp41s0f1np1</td>
<td>mlx5_2</td>
</tr>
<tr>
<td>Slot3 P1</td>
<td>82:00.0</td>
<td>ens6f0</td>
<td>N/A</td>
<td>irdma0</td>
</tr>
<tr>
<td>Slot3 P2</td>
<td>82:00.1</td>
<td>ens6f1</td>
<td>N/A</td>
<td>irdma1</td>
</tr>
<tr>
<td>On-board</td>
<td>0b:00.0</td>
<td>eno3</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
1.2.2. Compute and Storage Networking

1.2.3. Network Modules

- New form factor for aggregate PCIe network devices
- Consolidates four ConnectX-7 networking cards into a single device
- Two networking modules are installed on interposer board
- Interposer board connects to CPUs on one end and to GPU tray on the other
- DensiLink cables are used to go directly from ConnectX-7 networking cards to OSFP connectors at the back of the system

Each DensiLink cable has two ports, one from each ConnectX-7 card

Table 6: Table 6. Network Modules

<table>
<thead>
<tr>
<th>Port</th>
<th>ConnectX Device</th>
<th>Network Module/CPU</th>
<th>GPU</th>
<th>Default</th>
<th>RDMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSFP1P1</td>
<td>CX0</td>
<td>1</td>
<td>7</td>
<td>ibp220s0</td>
<td>mlx5_11</td>
</tr>
<tr>
<td>OSFP1P2</td>
<td>CX1</td>
<td>1</td>
<td>4</td>
<td>ibp154s0</td>
<td>mlx5_6</td>
</tr>
<tr>
<td>OSFP2P1</td>
<td>CX2</td>
<td>1</td>
<td>6</td>
<td>ibp206s0</td>
<td>mlx5_10</td>
</tr>
<tr>
<td>OSFP2P2</td>
<td>CX3</td>
<td>1</td>
<td>5</td>
<td>ibp192s0</td>
<td>mlx5_9</td>
</tr>
<tr>
<td>OSFP3P1</td>
<td>CX2</td>
<td>0</td>
<td>2</td>
<td>ibp79s0</td>
<td>mlx5_4</td>
</tr>
<tr>
<td>OSFP3P2</td>
<td>CX3</td>
<td>0</td>
<td>1</td>
<td>ibp64s0</td>
<td>mlx5_3</td>
</tr>
<tr>
<td>OSFP4P1</td>
<td>CX0</td>
<td>0</td>
<td>3</td>
<td>ibp94s0</td>
<td>mlx5_5</td>
</tr>
<tr>
<td>OSFP4P2</td>
<td>CX1</td>
<td>0</td>
<td>0</td>
<td>ibp24s0</td>
<td>mlx5_0</td>
</tr>
</tbody>
</table>
1.2.4. BMC Port LEDs

The BCM RJ-45 port has two LEDs.

The LED on the left indicates the speed. Solid green indicates the speed is 100M. Solid amber indicates the speed is 1G.

The LED on the right is green and flashes to indicate activity.

1.2.5. Supported Network Cables and Adaptors

The DGX H100 system is not shipped with network cables or adaptors. You will need to purchase supported cables or adaptors for your network.

The ConnectX-7 firmware determines which cables and adaptors are supported. For a list of cables and adaptors compatible with the NVIDIA ConnectX cards installed in the DGX H100 system,

1. Visit the NVIDIA Adapter Firmware Release page.

2. From the left navigation menu, select the ConnectX model and corresponding firmware included in the DGX H100.

3. Select Firmware Compatible Products.
1.3. DGX H100 System Topology

Here is an image of the DGX H100 system topology.

1.4. DGX OS Software

The DGX H100 system comes pre-installed with a DGX software stack incorporating the following components:

- An Ubuntu server distribution with supporting packages.
- The following system management and monitoring software:
  - NVIDIA System Management (NVSM)
    Provides active health monitoring and system alerts for NVIDIA DGX nodes in a data center. It also provides simple commands for checking the health of the DGX H100 system from the command line.
  - Data Center GPU Management (DCGM)
    This software enables node-wide administration of GPUs and can be used for cluster and data-center level management.
- DGX H100 system support packages.
- The NVIDIA GPU driver
- Docker Engine
- NVIDIA Container Toolkit
1.5. Customer Support

Contact NVIDIA Enterprise Support for assistance in reporting, troubleshooting, or diagnosing problems with your DGX H100 system. Also contact NVIDIA Enterprise Support for assistance in moving the DGX H100 system.

- For contracted Enterprise Support questions, you can send an email to enterprisesupport@nvidia.com.
- For additional details about how to obtain support, go to NVIDIA Enterprise Support.

Our support team can help collect appropriate information about your issue and involve internal resources as needed.
Chapter 2. Connecting to the DGX H100

2.1. Connecting to the Console

Connect to the DGX H100 console using either a direct connection or a remote connection through the BMC.

**Important:** Connect directly to the DGX H100 console if the DGX H100 system is connected to a 172.17.xx.xx subnet.

DGX OS Server software installs Docker Engine which uses the 172.17.xx.xx subnet by default for Docker containers. If the DGX H100 system is on the same subnet, you will not be able to establish a network connection to the DGX H100 system.

Refer to Configuring Docker IP Addresses in the *NVIDIA DGX OS 6 User Guide* for instructions on how to change the default Docker network settings.

2.1.1. Direct Connection

At the front or the back of the system, you can connect a display to the VGA connector and a keyboard to any of the USB ports.

The system provides video to one of the two VGA ports at a time. Simultaneous video output is not supported. If you connect two both VGA ports, the VGA port on the rear has precedence.

**Note:** The display resolution must be 1440x900 or lower.
2.1.2. Remote Connection through the BMC

Here is some information about how you can remotely connect to DGX H100 through the BMC. NVIDIA recommends that customers follow best security practices for BMC management (IPMI port). These include, but are not limited to, such measures as:

- Restricting the DGX H100 IPMI port to an isolated, dedicated management network.
- Using a separate, firewalled subnet.
- Configuring a separate VLAN for BMC traffic if a dedicated network is not available.

This method requires that you have the BMC login credentials. These credentials depend on the following conditions:
Before the First Boot Setup

**Caution:** You perform the First Boot Setup to change the default credentials before connecting the BMC to an unsecured network.

▶ The default credentials are:
  ▶ Username: admin
  ▶ Password: admin

**Caution:** When you create a BMC admin user, we strongly recommend that you change the default password for this user - DO NOT use the default password.

After the First Boot Setup

During the first-boot procedure, you were prompted to configure an administrator username and password and a password for the BMC. The BMC username is the same as the administrator username:

▶ Username: <administrator-username>
▶ Password: <bmc-password>

1. Make sure you have connected the BMC port on the DGX H100 system to your LAN.
2. Open a browser within your LAN and go to \https:∕∕<bmc-ip-address>\/
   Make sure popups are allowed for the BMC address.
3. Log in.
4. From the navigation menu, click Remote Control.
   The Remote Control page enables you to open a virtual Keyboard/Video/Mouse (KVM) on the DGX H100 system, as if you were using a physical monitor and keyboard connected to the front of the system.
5. Click Launch KVM.
   The DGX H100 console appears in your browser.
2.2. SSH Connection to the OS

After the system has been configured, you can also establish an SSH connection to the DGX H100 OS through the network port. Refer to *Network Ports* to identify the port to use.
Chapter 3. First Boot Setup

This section provides information about the set up process after you first boot the DGX H100 system. While NVIDIA partner network personnel or NVIDIA field service engineers will install the DGX H100 system at the site and perform the first boot setup, the first boot setup instructions are provided here for reference and to support any reimaging of the server.

3.1. System Setup

These instructions describe the setup process that occurs the first time the DGX H100 system is powered on after delivery or after the server is re-imaged.

Be prepared to accept all End User License Agreements (EULAs) and to set up your username and password. To preview the EULA, visit https://www.nvidia.com/en-us/data-center/dgx-systems/support/ and click the DGX EULA link.

1. Connect to the DGX H100 console as explained in Connecting to the Console.
2. Power on the DGX H100 system in one of the following ways:
   - Using the physical power button.
3. Refer to First Boot Process for DGX Servers in the NVIDIA DGX OS 6 User Guide for information about the following topics:
   ▶ Optionally encrypt the root file system.
Use the first boot wizard to set the language, locale, country, and so on.
Create an administrative user account for the system, BMC, and Grub boot loader.
Configure the primary network interface.

3.2. Post Setup Tasks

This section explains recommended tasks to perform after the initial system first-boot setup.

**Note:** RAID 1 rebuild can temporarily affect system performance.

When the system is booted after restoring the image and running the first-boot setup, software RAID begins the process of rebuilding the RAID 1 array, which creates a mirror of (or resynchronizing) the drive containing the software. System performance can be affected during the RAID 1 rebuild process. The process can take an hour to complete.

During this time, running the `nvsm show health` command reports a warning that the RAID volume is re-syncing.

You can monitor status of the RAID 1 rebuild process by running the `sudo nvsm show volumes` command, and then view the output under `/systems/localhost/storage/volumes/md0/rebuild`.

3.2.1. Obtaining Software Updates

To ensure that you are running the latest version of DGX OS, you might need to update the software. Updating the software ensures that your DGX H100 system contains important updates, including security updates. The Ubuntu Security Notice site, [https://usn.ubuntu.com/](https://usn.ubuntu.com/), lists known common vulnerabilities and exposures (CVEs), including those that can be resolved by updating the DGX OS software.

Refer to Upgrading in the *NVIDIA DGX OS 6 User Guide* for information about updating the operating system.

3.2.2. Enabling the SRP Daemon

The NVIDIA networking drivers provide the SRP daemon software. The daemon is disabled by default. Enabling the daemon is required if you want to use RDMA over Infiniband. You can enable the daemon by running the following commands:

```bash
sudo systemctl enable srp_daemon.service
sudo systemctl enable srptools.service
```
Chapter 4. Quickstart and Basic Operation

This chapter provides basic requirements and instructions for using the DGX H100 system, including how to perform a preliminary health check and how to prepare for running containers. Go to the DGX documentation for additional product documentation.

4.1. Installation and Configuration

Before you install DGX H100, ensure you have given all relevant site information to your Installation Partner.

**Important:** Your DGX H100 System must be installed by NVIDIA partner network personnel or NVIDIA field service engineers. If not performed accordingly, your hardware warranty will be voided.

4.2. Registration

To obtain support for your DGX H100, follow the instructions for registration in the Entitlement Certification email that was sent as part of the purchase.

Registration allows you to access the NVIDIA Enterprise Support Portal, obtain technical support, get software updates, and set up an NGC for DGX systems account. If you did not receive the information, open a case with the NVIDIA Enterprise Support Team at [https://www.nvidia.com/en-us/support/enterprise/](https://www.nvidia.com/en-us/support/enterprise/).

To obtain support for your DGX H100 system, follow the instructions for registration in the Entitlement Certification email that was sent as part of the purchase.

Registration allows you to access the NVIDIA Enterprise Support Portal, obtain technical support, get software updates, and set up an NGC for DGX systems account. If you did not receive the information, open a case with the NVIDIA Enterprise Support Team at [https://www.nvidia.com/en-us/support/enterprise/](https://www.nvidia.com/en-us/support/enterprise/).

Refer to Customer Support for contact information.
4.3. Obtaining an NGC Account

NVIDIA NGC provides access to GPU-optimized software for deep learning, machine learning, and high-performance computing (HPC). An NGC account grants you access to these tools and gives you the ability to set up a private registry to manage your customized software.

If you are the organization administrator for your DGX system purchase, work with NVIDIA Enterprise Support to set up an NGC enterprise account. Refer to the NGC Private Registry User Guide for more information about getting an NGC enterprise account.

4.4. Turning DGX H100 On and Off

DGX H100 is a complex system, integrating a large number of cutting-edge components with specific startup and shutdown sequences. Observe the following startup and shutdown instructions.

4.4.1. Startup Considerations

To keep your DGX H100 running smoothly, allow up to a minute of idle time after reaching the login prompt. This ensures that all components can complete their initialization.

4.4.2. Shutdown Considerations

When shutting down DGX H100, always initiate the shutdown from the operating system, momentary press of the power button, or by using Graceful Shutdown from the BMC, and wait until the system enters a powered-off state before performing any maintenance.

**Warning:** Risk of Danger - Removing power cables or using Power Distribution Units (PDUs) to shut off the system while the Operating System is running may cause damage to sensitive components in the DGX H100 server.

4.5. Verifying Functionality - Quick Health Check

NVIDIA provides customers a diagnostics and management tool called NVIDIA System Management, or NVSM. The `nvsm` command can be used to determine the system’s health, identify component issues and alerts, or run a stress test to make sure all components are in working order while under load. The use of Docker is key to getting the most performance out of the system since NVIDIA has optimized containers for all the major frameworks and workloads used on DGX systems.

The following are the steps for performing a health check on the DGX H100 System, and verifying the Docker and NVIDIA driver installation.

1. Establish an SSH connection to the DGX H100 System.
2. Run a basic system check.
   
   ```bash
   sudo nvsm show health
   ```

3. Verify that the output summary shows that all checks are Healthy and that the overall system status is Healthy.

4. Verify that Docker is installed by viewing the installed Docker version.
   
   ```bash
   sudo docker --version
   ```

   On success, the command returns the version as `Docker version xx.yy.zz`, where the actual version may differ depending on the specific release of the DGX OS Server software.

5. Verify connection to the NVIDIA repository and that the NVIDIA Driver is installed.
   
   ```bash
   sudo docker run --gpus all --rm nvcr.io/nvidia/cuda:12.1.1-base-ubuntu22.04
   ```

   The preceding command pulls the `nvidia/cuda` container image layer by layer, then runs the `nvidia-smi` command.

   When complete, the output shows the NVIDIA Driver version and a description of each installed GPU.

   For more information, refer to *Containers For Deep Learning Frameworks User Guide*.

4.6. Running the Pre-flight Test

Instructions for running the DGX stress test.

NVIDIA recommends running the pre-flight stress test before putting a system into a production environment or after servicing. You can specify running the test on the GPUs, CPU, memory, and storage, and also specify the duration of the tests.

To run the tests, use NVSM.

**Syntax**

```bash
sudo nvsm stress-test [--usage] [--force] [--no-prompt] [<test>...] [DURATION]
```

For help on running the test, issue the following.

```bash
sudo nvsm stress-test --usage
```
**Recommended Command**

The following command runs the test on all supported components (GPU, CPU, memory, and storage), and takes approximately 20 minutes.

```
sudo nvsm stress-test --force
```

### 4.7. Running NGC Containers with GPU Support

To obtain the best performance when running NGC containers on DGX H100 systems, the following methods of providing GPU support for Docker containers are available:

- **Native GPU support (included in Docker 20.10.18 and later)**

  The method implemented in your system depends on the DGX OS version installed.

<table>
<thead>
<tr>
<th>DGX OS Releases</th>
<th>Method Included</th>
</tr>
</thead>
</table>
| 6.0             | ▶ Native GPU support  
|                 | ▶ NVIDIA Container Runtime for Docker (deprecated - availability to be removed in a future DGX OS release) |

Each method is invoked by using specific Docker commands, described as follows.

#### 4.7.1. Using Native GPU Support

Use `docker run --gpus` to run GPU-enabled containers.

- **Example using all GPUs**
  ```
sudo docker run --gpus all ...
  ```

- **Example using two GPUs**
  ```
sudo docker run --gpus 2 ...
  ```

- **Examples using specific GPUs**
  ```
sudo docker run --gpus '"device=1,2"' ...
sudo docker run --gpus '"device=UUID-ABCDEF,1"' ...
  ```
4.7.2. Using the NVIDIA Container Runtime for Docker

If you need to use nvidia-docker2, install it using `sudo apt install nvidia-docker2`, then run:

```
sudo systemctl restart docker
```

The DGX OS also includes the NVIDIA Container Runtime for Docker (nvidia-docker2) which lets you run GPU-accelerated containers in one of the following ways:

▶ Use docker run and specify runtime=nvidia.

```
docker run --runtime=nvidia ...
```

▶ Use nvidia-docker run.

```
nvidia-docker run ...
```

The nvidia-docker2 package provides backward compatibility with the previous nvidia-docker package, so you can run GPU-accelerated containers using this command and the new runtime will be used.

▶ Use docker run with nvidia as the default runtime.

You can set nvidia as the default runtime, for example, by adding the following line to the `/etc/docker/daemon.json` configuration file as the first entry.

```
"default-runtime": "nvidia",
```

Here is an example of how the added line appears in the JSON file. Do not remove any pre-existing content when making this change.

```
{
  "default-runtime": "nvidia",
  "runtimes": {
    "nvidia": {
      "path": "/usr/bin/nvidia-container-runtime",
      "args": []
    }
  }
}
```

You can then use docker run to run GPU-accelerated containers.

```
docker run ...
```

**Caution:** If you build Docker images while nvidia is set as the default runtime, make sure the build scripts executed by the Dockerfile specify the GPU architectures that the container will need. Failure to do so might result in the container being optimized only for the GPU architecture on which it was built. Instructions for specifying the GPU architecture depend on the application and are beyond the scope of this document. Consult the specific application build process.

For more information, refer to the *NVIDIA DGX OS 6 User Guide*.
4.8. Managing CPU Mitigations

DGX OS Server includes security updates to mitigate CPU speculative side-channel vulnerabilities. These mitigations can decrease the performance of deep learning and machine learning workloads.

If your installation of DGX systems incorporates other measures to mitigate these vulnerabilities, such as measures at the cluster level, you can disable the CPU mitigations for individual DGX nodes and thereby increase performance. This capability is available starting with DGX OS Server release 4.4.0.

4.8.1. Determining the CPU Mitigation State of the DGX System

If you do not know whether CPU mitigations are enabled or disabled, issue the following.

```
cat /sys/devices/system/cpu/vulnerabilities/*
```

CPU mitigations are enabled if the output consists of multiple lines prefixed with *Mitigation:.*

**Example**

```
KVM: Mitigation: Split huge pages
Mitigation: PTE Inversion; VMX: conditional cache flushes, SMT vulnerable
Mitigation: Clear CPU buffers; SMT vulnerable
Mitigation: PTI
Mitigation: Speculative Store Bypass disabled via prctl and seccomp
Mitigation: usercopy/swapgs barriers and _user pointer sanitization
Mitigation: Full generic retpoline, IBPB: conditional, IBRS_FW, STIBP: conditional,
            __RSB filling
Mitigation: Clear CPU buffers; SMT vulnerable
```

CPU mitigations are disabled if the output consists of multiple lines prefixed with *Vulnerable*.

**Example**

```
KVM: Vulnerable
Mitigation: PTE Inversion; VMX: vulnerable
Vulnerable; SMT vulnerable
Vulnerable
Vulnerable
Vulnerable
Vulnerable: __user pointer sanitization and usercopy barriers only; no swapgs barriers
Vulnerable, IBPB: disabled, STIBP: disabled
Vulnerable
```
4.8.2. Disabling CPU Mitigations

**Caution:** Performing the following instructions will disable the CPU mitigations provided by the DGX OS Server software.

1. Install the `nv-mitigations-off` package.
   ```
   sudo apt install nv-mitigations-off -y
   ```
2. Reboot the system.
3. Verify CPU mitigations are disabled.
   ```
   cat /sys/devices/system/cpu/vulnerabilities/*
   ```
   The output should include several `Vulnerable` lines. See *Determining the CPU Mitigation State of the DGX System* for example output.

4.8.3. Re-enabling CPU Mitigations

1. Remove the `nv-mitigations-off` package.
   ```
   sudo apt purge nv-mitigations-off
   ```
2. Reboot the system.
3. Verify CPU mitigations are enabled.
   ```
   cat /sys/devices/system/cpu/vulnerabilities/*
   ```
   The output should include several `Mitigations` lines. See *Determining the CPU Mitigation State of the DGX System* for example output.
Chapter 5. SBIOS Settings

The NVIDIA DGX H100 system comes with a system BIOS with optimized settings for the DGX system. There might be situations where the settings need to be changed, such as changes in the boot order, changes to enable PXE booting, or changes in the BMC network settings. Instructions for these use cases are provided in this section.

**Important:** Do not change settings in the SBIOS other than those described in this or other DGX H100 user documents. Contact NVIDIA Enterprise Services **before** making other changes.

### 5.1. Accessing the SBIOS Setup

Here is information about how you can access the SBIOS setup.

1. Access the DGX H100 console, either from a locally connected keyboard and mouse or through the BMC remote console.
2. Reboot the DGX H100.
3. When presented with the SBIOS version screen, press the Del or F2 key to enter the BIOS Setup Utility.
Here are some occasions where it might be necessary to reconfigure settings in the SBIOS:

▶ Configuring a BMC Static IP Address Using the System BIOS
▶ Enabling the TPM and Preventing the BIOS from Sending Block SID Requests
▶ Clearing the TPM

5.2. Configuring the Boot Order

The following instructions describe how to set the boot order at boot time. You can also set the boot order from the SBIOS setup > Boot screen.

1. Access the DGX H100 console, either from a locally connected keyboard and mouse or through the BMC remote console.
2. Reboot the DGX H100.
3. Press the F11 key at the NVIDIA splash screen.
4. Select the boot device.

The following figure shows virtual media selected.
5.3. Configuring the Local Terminal

There are two ways to access the BIOS setup screen:

▶ A direct-attached keyboard and monitor
▶ Serial-over-LAN (SOL) using IPMI tools

To use the SOL connection, you might need to configure your terminal application.

5.3.1. Linux

1. Set the locale and language for your terminal:
   ```bash
   sudo localectl set-locale LANG=en_US.UTF-8
   ```

2. Set the locale for the current session:
   ```bash
   export LANG=en_UTF-8
   ```

3. Type `xterm` to launch the terminal with the set locale.

5.3.2. Windows and MacOS

▶ Configure your terminal application for `en_US.UTF-8` support.

5.4. Power on or Reboot the System

1. Reboot the system using one of the following methods:
   ▶ Connect to the BMC web interface and click `power on/reboot`.
   ▶ From an operating system command line, run `sudo reboot`.

2. Connect to the DGX H100 SOL console:
   ```bash
   ipmitool -I lanplus -H <ip-address> -U admin -P dgxluna.admin sol activate
   ```

3. Press the Del or F2 key when the system is booting.
   The system confirms your choice and shows the BIOS configuration screen.
Chapter 6. Using the Baseboard Management Controller (BMC)

The NVIDIA DGX H100 system comes with a baseboard management controller (BMC) for monitoring and controlling various hardware devices on the system. It monitors system sensors and other parameters.

6.1. Connecting to the BMC

Here are the steps to connect to the BMC on a DGX H100 system.

Before you begin, ensure that you connected the BMC network interface controller port on the DGX system to your LAN.

1. Open a browser within your LAN and enter the IP address of the BMC in the location.

   The BMC is supported on the following browsers:
   - Internet Explorer 11 and later
   - Firefox 29.0 (64-bit) and later
   - Google Chrome 7.0.3396.87 (64-bit) and later

2. Log in.

   The BMC dashboard opens.
6.2. Overview of BMC Controls

The left-side navigation menu bar on the BMC main page contains the primary controls.
6.2. Overview of BMC Controls
Table 1: BMC Main Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Links</td>
<td>Provides quick access to several tasks.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Displays the overall information about the status of the device.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Provides status and readings for system sensors, such as SSD, PSUs, voltages, CPU temperatures, DIMM temperatures, and fan speeds.</td>
</tr>
<tr>
<td>System Inventory</td>
<td>Displays inventory information of system modules.</td>
</tr>
<tr>
<td>FRU Information</td>
<td>System, Processor, Memory Controller, Base-Board, Power, Thermal, PCIE Device, PCIE Function, and Storage.</td>
</tr>
<tr>
<td>GPU Information</td>
<td>Provides basic information on all the GPUs in the systems, including GUID, VBIOS version, InfoROM version, and number of retired pages for each GPU.</td>
</tr>
<tr>
<td>Logs and Reports</td>
<td>View, and if applicable, download and erase, the IPMI event log, and System, Audit, Video, and POST Code logs.</td>
</tr>
<tr>
<td>Settings</td>
<td>Configure the following settings: Captured BSOD, External User Services, KVM Mouse Setting, Log Settings, Media Redirection Settings, Network Settings, PAM Order Settings, Platform Event Filter, Services, SMTP Settings, SSL Settings, System Firewall, User Management, and Video Recording</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Opens the KVM Launch page to remotely access the DGX H100 console.</td>
</tr>
<tr>
<td>Power Control</td>
<td>Perform the following power actions: Power On, Power Off, Power Cycle, Hard Reset, and ACP/Shutdown</td>
</tr>
<tr>
<td>Chassis ID LED Control</td>
<td>“Virtual LED” is a button to toggle the UID LED on/off:</td>
</tr>
<tr>
<td></td>
<td>– Off</td>
</tr>
<tr>
<td></td>
<td>– Solid on</td>
</tr>
<tr>
<td></td>
<td>– Blinking on (select from five (5) to 255 second blink interval).</td>
</tr>
<tr>
<td></td>
<td>This is activated by the “Chassis Identify LED” option above the “Quick Links” drop down.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Perform the following maintenance tasks:</td>
</tr>
<tr>
<td></td>
<td>Backup Configuration, Firmware Image Location, Firmware Update, Preserve Configuration, Restore Configuration, Restore Factory Defaults, and System Administrator</td>
</tr>
<tr>
<td>Sign out</td>
<td>Sign out of the BMC web UI.</td>
</tr>
</tbody>
</table>
6.3. Changing the BMC Login Credentials

6.3.1. User Name and Password Requirements

Refer to the following requirements for the user name:

▶ a string of 1 to 16 alphanumeric characters
▶ must start with an alphabetical character
▶ case-sensitive
▶ special characters - (hyphen), _ (underscore), and @ (at sign) are allowed

Refer to the following requirements for the password:

▶ a string up to 20 characters
▶ case-sensitive
▶ special characters that must be preceded by a \ (backslash) character: ! "&'();<>`|~\n▶ special characters that do not require any special consideration: #$%*+,.-/:=?@[\]^_\}

6.3.2. Procedure

To change your credentials or add or remove users, perform the following steps:

1. Select Settings from the left-side navigation menu.
2. Select the User Management card.
3. Click the help icon (?) for information about configuring users and creating a password.
4. Log out and then log in with the new credentials.
6.4. Using the Remote Console

To use the remote console, perform the following steps:

1. Click Remote Control from the left-side navigation menu.
2. Click Launch KVM to start the remote KVM and access the DGX system console.

6.5. Setting Up Active Directory, LDAP, or E-Directory

To set up Active Directory, LDAP, or E-Directory, perform the following steps:

1. From the side navigation menu, click Settings > External User Services.
2. Click Active Directory Settings or LDAP/E-Directory Settings and follow the instructions.
6.6. Configuring Platform Event Filters

From the side navigation menu, click **Settings** and then click **Platform Event Filters**.

The Event Filters page shows all configured event filters and available slots. You can modify or add new event filter entry on this page.

- To view available configured and unconfigured slots, click **All** in the upper-left corner of the page.
- To view available configured slots, click **Configured** in the upper-left corner of the page.
- To view available unconfigured slots, click **UnConfigured** in the upper-left corner of the page.
- To delete an event filter from the list, click the **x** icon.

6.7. Uploading or Generating SSL Certificates

You can set up a new certificate by generating a (self-signed) SSL or by uploading an SSL (for example, to use a Trusted CA-signed certificate).

From the side navigation menu, click **Settings > SSL Settings**.
Refer to the following sections for more information.

6.7.1. Viewing the SSL Certificate

To view the SSL certificate, on the SSL Setting page, click **View SSL Certificate**.

The View SSL Certificate page displays the following basic information about the uploaded SSL certificate:

- Certificate Version, Serial Number, Algorithm, and Public Key
- Issuer information
- Valid Date range
- Issued to information
### 6.7.2. Generating the SSL Certificate

Here is some information about generating an SSL certificate.

1. From the SSL Setting page, click **Generate SSL Certificate**.

2. Enter the information as described in the following table.

<table>
<thead>
<tr>
<th>Items</th>
<th>Description and Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>The common name for which the certificate is to be generated.</td>
</tr>
<tr>
<td></td>
<td>▶ Maximum length of 64 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>▶ Special characters ‘#’ and ‘$’ are not allowed.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>The name of the organization for which the certificate is generated.</td>
</tr>
<tr>
<td></td>
<td>▶ Maximum length of 64 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>▶ Special characters ‘#’ and ‘$’ are not allowed.</td>
</tr>
<tr>
<td>Organization Unit (OU)</td>
<td>Overall organization section unit name for which the certificate is generated.</td>
</tr>
<tr>
<td></td>
<td>▶ Maximum length of 64 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>▶ Special characters ‘#’ and ‘$’ are not allowed.</td>
</tr>
<tr>
<td>City or Locality (L)</td>
<td>City or Locality of the organization (mandatory)</td>
</tr>
<tr>
<td></td>
<td>▶ Maximum length of 64 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>▶ Special characters ‘#’ and ‘$’ are not allowed.</td>
</tr>
<tr>
<td>State or Province (ST)</td>
<td>State or Province of the organization (mandatory)</td>
</tr>
<tr>
<td></td>
<td>▶ Maximum length of 64 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>▶ Special characters ‘#’ and ‘$’ are not allowed.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Country code of the organization.</td>
</tr>
<tr>
<td></td>
<td>▶ Only two characters are allowed.</td>
</tr>
<tr>
<td></td>
<td>▶ Special characters are not allowed.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Email address of the organization (mandatory)</td>
</tr>
<tr>
<td>Valid for</td>
<td>Enter a range from 1 to 3650 (days)</td>
</tr>
<tr>
<td>Key Length</td>
<td>Enter 4096.</td>
</tr>
</tbody>
</table>

3. To generate the new certificate, click **Save**.
6.7.3. Uploading the SSL Certificate

In BMC, you can upload your SSL certificate. Make sure the certificate and key meet the following requirements:

▶ SSL certificates and keys must both use the .pem file extension.
▶ Private keys must not be encrypted.
▶ SSL certificates and keys must each be less than 3584 bits in size.
▶ SSL certificates must be current (not expired).

1. On the SSL Setting page, click **Upload SSL Certificate**.

2. Click the **New Certificate** folder icon, browse to locate the appropriate file, and select it.
3. Click the **New Private Key** folder icon, browse and locate the appropriate file, and select it.
4. Click **Save**.

6.7.4. Updating the SBIOS Certificate

The CA Certificate for the trusted CA that was used to sign the SSL certificate must be uploaded to allow the SBIOS to authenticate the certificate.

1. Obtain the CA certificate from the signing authority that was used to sign the SSL certificate.
2. Copy the CA certificate onto a USB thumb drive or to /boot/efi on the operating system.
3. Access a console from a locally connected keyboard and mouse or through the BMC remote console.
4. Reboot the server.
5. To enter BIOS setup menu, when prompted, press DEL.

**Note:** you may need to be logged in with admin privileges.

6. In the BIOS setup menu on the **Advanced** tab, select **Tls Auth Config**.
7. Select **Server CA Configuration**.

8. Select **Enroll Cert**.
9. Select **Enroll Cert Using File**.

10. Select the device where you stored the certificate.

11. Navigate the file structure and select the certificate.
6.7. Uploading or Generating SSL Certificates
Chapter 7. Security

This section provides information about security measures in the DGX H100 system.

7.1. User Security Measures

The NVIDIA DGX H100 system is a specialized server designed to be deployed in a data center. It must be configured to protect the hardware from unauthorized access and unapproved use. The DGX H100 system is designed with a dedicated BMC Management Port and multiple Ethernet network ports.

When you install the DGX H100 system in the data center, follow best practices as established by your organization to protect against unauthorized access.

7.1.1. Securing the BMC Port

NVIDIA recommends that you connect the BMC port in the DGX H100 system to a dedicated management network with firewall protection.

If remote access to the BMC is required, such as for a system hosted at a co-location provider, it should be accessed through a secure method that provides isolation from the internet, such as through a VPN server.

7.2. System Security Measures

This section provides information about the security measures that have been incorporated in an NVIDIA DGX H100 system.
7.2.1. Secure Flash of DGX H100 Firmware

Secure Flash is implemented for the DGX H100 to prevent unsigned and unverified firmware images from being flashed onto the system.

7.2.2. Encryption

Here is some information about encrypting the DGX H100 firmware.

The firmware encryption algorithm is AES-CBC.
- The firmware encryption key strength is 128 bits or higher.
- Each firmware class uses a unique encryption key.
- Firmware decryption is performed either by the same agent that performs signature check or a more trusted agent in the same COT.

7.2.3. NVIDIA System Manager Security

For information about security in NVIDIA System Management, refer to NVSM documentation page.

7.3. Secure Data Deletion

This section explains how to securely delete data from the DGX H100 system SSDs to permanently destroy all the data that was stored there.

This process performs a more secure SSD data deletion than merely deleting files or reformatting the SSDs.

7.3.1. Prerequisites

You need to prepare a bootable installation medium that contains the current DGX OS Server ISO image.

Refer to Reimaging in the NVIDIA DGX OS 6 User Guide for information on the following topics:
- Obtaining the DGX OS ISO Image
- Booting the DGX OS ISO Image
### 7.3.2. Procedure

Here are the instructions to securely delete data from the DGX H100 system SSDs.

1. Boot the system from the ISO image, either remotely or from a bootable USB key.
2. At the GRUB menu, select:
   - (For DGX OS 6): **Rescue a broken system** and configure the locale and network information.
3. When prompted to select a root file system, select **Do not use a root file system** and then select **Execute a shell in the installer environment**.
4. Log in.
5. Run the following command to identify the devices available in the system:

   ```bash
   nvme list
   ```

   If the `nvme-cli` package is not installed, then install the CLI as follows and then run `nvme list`.

   ```bash
   dpkg -i /usr/lib/live/mount/rootfs/filesystem.squashfs/curtin/repo/<nvme-cli-package.deb>
   ```

6. Perform a secure erase:

   ```bash
   nvme format -s1 <device-path>
   ```

   where `<device-path>` is the specific storage node as listed in the previous step. For example, `/dev/nvme0n1`.
Chapter 8. Redfish APIs Support

The DGX System firmware supports Redfish APIs. Redfish is DMTF’s standard set of APIs for managing and monitoring a platform. By default, Redfish support is enabled in the DGX H100 BMC and the BIOS. By using the Redfish interface, administrator-privileged users can browse physical resources at the chassis and system level through the REST API interface. Redfish provides information that is categorized under a specific resource endpoint and Redfish clients can use the endpoints by using the following HTTP methods:

- GET
- POST
- PATCH
- PUT
- DELETE

Not all endpoints support all these operations. Refer to the Redfish JSON Schema for more information about the operations. The Redfish server follows the DSP0266 1.7.0 Specification and Redfish Schema 2019.1 documentation. Redfish URIs are accessed by using basic authentication and implementation, so that IPMI users with required privilege can access the Redfish URIs.

8.1. Supported Redfish Features

Here is some information about the Redfish features that are supported in DGX H100.

The following features are supported:

- Manage user accounts, privileges, and roles
- Manager Sessions
- BMC configuration
- BIOS configuration
- BIOS boot order management
- Get PCIe device and functions inventory
- Get storage Inventory
- Get system component information and health (PSU, FAN, CPU, DIMM, and so on)
- Get sensor information (Thermal/Power/Cooling)
- BMC configuration change/BMC reset
8.2. Connectivity Between the Host and BMC

You can configure internal network connectivity between the host and the BMC rather than using external network connectivity and routing traffic outside the host.

To configure internal network connectivity, you must configure an interface on the 169.254.0.0/255.255.0.0 network. The interface can then send and receive Redfish API traffic between the host and the BMC. The BMC is preconfigured to use the 169.254.0.17 IP address.

Run an `ifconfig` command like the following example to configure connectivity:

```
sudo ifconfig enx9638a3b292ec 169.254.0.18 netmask 255.255.0.0
```

Replace the network interface name and IP address in the preceding example according to your needs.

After you configure the network interface, you can use commands such as `curl` and `nvfwupd` with the 169.254.0.17 IP address to connect to the BMC and use the Redfish API.

The following example command shows the firmware versions:

```
nvfwupd -t ip=169.254.0.17 username=<bmc-user> password=<password> show_version
```

8.3. Redfish Examples

8.3.1. BMC Manager

Accounts

The following curl command changes the password for the admin user.

```
curl -k -u <bmc-user>:<password> --request PATCH 'https://<bmc-ip-address>/redfish/v1/AccountService/Accounts/1' --header 'If-Match: *' --header 'Content-Type: application/json' --data-raw '{"Enabled" : true,
"Password" : "DGXuser12345678!", "UserName" : "admin", "RoleId" :
"Administrator", "Locked" : false}'
```

Reset BMC

The following curl command forces a reset of the DGX H100 BMC.
8.3.2. Firmware Update

Firmware inventory

curl -k -u <bmc-user>:<password> --request GET --location 'https://<bmc-ip-address>/redfish/v1/UpdateService/FirmwareInventory'

Example Output

```json
{
    "@odata.context": "/redfish/v1/$metadata#SoftwareInventoryCollection",
    "@odata.etag": "\"1683226281\"",
    "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory",
    "@odata.type": "#SoftwareInventoryCollection",
    "Description": "Collection of Firmware Inventory resources available to the UpdateService",
    "Members": [
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/CPLDMB_0"
        },
        {
            "@odata.id": "/redfish/v1/UpdateService/FirmwareInventory/CPLDMID_0"
        },
        // ...
    ],
    "Members@odata.count": 66,
    "Name": "Firmware Inventory Collection",
    "Oem": {
        "Ami": {
            "FirmwareInventory": [
                {
                    "DataSourceUri": "/redfish/v1/UpdateService/FirmwareInventory/CPLDMB_0",
                    "Name": "CPLDMB_0",
                    "Version": "0.2.1.6"
                }
            ]
        }
    }
}
```

(continues on next page)
Update GPU tray components

To update the GPU tray components in your DGX H100 system, you need to specify HGX_0 as the target regardless of the GPU tray component that you want to update.

```bash
echo "{"Targets":[{"/redfish/v1/UpdateService/FirmwareInventory/HGX_0"}]}" > parameters.json
```

curl -k -u <bmc-user>:<password> -H 'Expect:' --location --request POST https://<bmc-ip-address>/redfish/v1/UpdateService/upload -F 'UpdateParameters=@parameters.json;type=application/json' -F 'UpdateFile=@<fw_bundle>'

Make sure to specify the nvfw_DGX-HGX-H100x8_0002_xxxxxx.x.x_prod-signed.fwpkg firmware file.

Update motherboard tray components

To update the motherboard tray components, you need to specify the component name as a target in a JSON file. The following example updates the host BMC:

```bash
echo "{"Targets":[{"/redfish/v1/UpdateService/FirmwareInventory/HostBMC_0"}]}"> parameters.json
curl -k -u <bmc-user>:<password> -H 'Expect:' --location --request POST https://<bmc-ip-address>/redfish/v1/UpdateService/upload -F 'UpdateParameters=@parameters.json;type=application/json' -F 'UpdateFile=@<fw_bundle>'
```

The following targets are available:

- **HostBMC_0** — This is the DGX H100 BMC.
- **HostBIOS_0** — This is the DGX H100 BIOS.
- **EROT_BMC_0** — This is the external root of trust for the host BMC.
- **EROT_BIOS_0** — This is the external root of trust for the host BIOS.
- **CPLDMID_0** — This is the midplane CPLD.
- **CPLDMB_0** — This is the CPU tray CPLD.
- **PSU_0** to **PSU_5** — These are the PSUs.
- **PCIeSwitch_0** and **PCIeSwitch_1** — These are the Gen5 PCIe switches on the CPU tray.
- **PCIeRetimer_0** and **PCIeRetimer_1** — These are the PCIe retimers on the CPU tray.
To update a target, change the path \redfish\v1\UpdateService\FirmwareInventory\HostBMC_0 in the preceding example. For example, for CPU tray CPLD, specify \redfish\v1\UpdateService\FirmwareInventory\CPLDMB_0.

Make sure to specify the nvfw_DGX-HGX-H100x8_0002_xxxxx.x.x_prod-signed.fwpkg firmware file.

▶ Forced Update

The DGX H100 system components firmware is only updated if the incoming firmware version is newer than the existing version. To override this behavior and flash the component anyway, specify the ForceUpdate field and set it to true.

```
curl -k -u <bmc-user>:<password> --request PATCH 'https:∕∕<bmc-ip-address>∕redfish∕v1∕UpdateService' --header 'If-Match: *' --header 'Content-Type: application/json' --data-raw '{"HttpPushUriOptions" : { "ForceUpdate": true}}'
```

On success, the command returns a 204 HTTP status code. If you attempt to set the flag to the currently set value, the command returns a 400 HTTP status code.

To get the value of the ForceUpdate parameter:

```
curl -k -u <bmc-user>:<password> --request GET 'https:∕∕<bmc-ip-address>∕redfish∕v1∕UpdateService'
```

8.3.3. BIOS Settings

▶ Supported BIOS attributes

1. Get a list of all the attributes your particular BIOS supports:

```
curl -k -u <bmc-user>:<password> --location --request GET 'https://<bmc-ip-address>∕redfish∕v1∕Registries'
```

One of the Registries in the list is your BIOS attribute registry. The format is BiosAttributeRegistry<version><version>. For example, for BIOS 0.1.6, the registry is BiosAttributeRegistry106.1.0.6.

2. Get the URI of the BIOS registry:

```
curl -k -u <bmc-user>:<password> --location --request GET 'https://<bmc-ip-address>∕redfish∕v1∕Registries∕BiosAttributeRegistry016.0.1.6∕'
```

The response includes the location of the JSON file that describes all the BIOS attributes. Under Location, the Uri is specified. For example, Uri":"∕redfish∕v1∕Registries∕BiosAttributeRegistry106.1.0.6.

3. Get the JSON file with the registry of all your BIOS attributes:

```
curl -k -u <bmc-user>:<password> --location --request GET 'https://<bmc-ip-address>∕redfish∕v1∕Registries∕BiosAttributeRegistry106.en-US.1.0.6.json' --output BiosAttributeRegistry106.en-US.1.0.6.json
```

Each attribute name has a default value, display name, help text, a read-only indicator, and an indicator of whether a reset is required to take effect.

To get the current value of all your attributes from the BIOS:
curl -k -u <bmc-user>:<password> --location --request GET 'https://<bmc-ip-address>/redfish/v1/Systems/DGX/Bios/SD'

Match the attribute name with the value in the registry for a description.

To change an attribute, PATCH the SD URI and specify the attribute name with the new value. Also, you can change more than one attribute at one time. For example, the following PATCH request specifies how the system responds when the SEL log is full:

```
curl -k -u <bmc-user>:<password> --location --request PATCH 'https://<bmc-ip-address>/redfish/v1/Systems/DGX/Bios/SD' -H 'Content-Type: application/json' -H 'If-Match: *' --data-raw '{"Attributes": {"IPMI002":"IPMI002DoNothing", "IPMI201": "IPMI201Donotloganymore"}}'
```

The following example changes the boot order to boot from PXE:

```
```

The following example changes the boot order back to boot from M.2:

```
curl -k -u <bmc-user>:<password> --location --request PATCH 'https://<bmc-ip-address>/redfish/v1/Systems/DGX/Bios/SD' -H 'Content-Type: application/json' -H 'If-Match: *' --data-raw '{"Attributes": {"FBO201": "FBO201NVMEubuntuSAMSUNGMZ1L21T9HCLS00A07"}}'
```

### 8.3.4. Telemetry

- **GPU tray sensors**
  ```
curl -k -u <bmc-user>:<password> --location --request GET 'https://<bmc-ip-address>/redfish/v1/TelemetryService/MetricReportDefinitions/HGX_PlatformEnvironmentMetrics_0'
  ```

- **DGX platform sensors**
  ```
curl -k -u <bmc-user>:<password> --location --request GET 'https://<bmc-ip-address>/redfish/v1/Chassis/DGX/Sensors'
  ```

The endpoint returns 75 members at a time. To page through the results, use the URI in the Members@odata.nextLink field. For example, `/redfish/v1/Chassis/DGX/Sensors?$skip=75`. 

---

Chapter 8. Redfish APIs Support
8.3.5. Chassis

- **Chassis Restart (IPMI chassis power cycle)**
  ```bash
curl -k -u <bmc-user>:<password> --request POST --location 'https:∕∕<bmc-ip-address>∕redfish∕v1∕Systems∕DGX∕Actions∕ComputerSystem.Reset' --header 'Content-Type: application/json' --data '{"ResetType": "ForceRestart"'}
  ```

- **Chassis Start (IPMI chassis power on)**
  ```bash
curl -k -u <bmc-user>:<password> --request POST --location 'https:∕∕<bmc-ip-address>∕redfish∕v1∕Systems∕DGX∕Actions∕ComputerSystem.Reset' --header 'Content-Type: application/json' --data '{"ResetType": "On"'}
  ```

- **Chassis Off (IPMI chassis power off)**
  ```bash
curl -k -u <bmc-user>:<password> --request POST --location 'https:∕∕<bmc-ip-address>∕redfish∕v1∕Systems∕DGX∕Actions∕ComputerSystem.Reset' --header 'Content-Type: application/json' --data '{"ResetType": "ForceOff"'}
  ```

- **Chassis Off Gracefully (IPMI chassis soft)**
  ```bash
curl -k -u <bmc-user>:<password> --request POST --location 'https:∕∕<bmc-ip-address>∕redfish∕v1∕Systems∕DGX∕Actions∕ComputerSystem.Reset' --header 'Content-Type: application/json' --data '{"ResetType": "GracefulShutdown"'}
  ```

8.3.6. SEL Logs

To view all the SEL entries using redfish:

```bash
curl -k -u <bmc-user>:<password> --location --request GET 'https:∕∕<bmc-ip-address>∕redfish∕v1∕Managers∕BMC∕LogServices∕SEL∕Entries'
```

The endpoint returns 75 members at a time. To page through the results, use the URI in the Members@odata.nextLink field. For example, `https://<bmc-ip-address>/redfish/v1/Managers/BMC/LogServices/SEL/Entries?$skip=75`.

8.3.7. Virtual Image

1. Make sure Virtual Media is enabled:
   ```bash
curl -k -u <bmc-user>:<password> --request POST --location 'https:∕∕<bmc-ip-address>∕redfish/v1/Managers/BMC/Actions/AMIVirtualMedia.EnableRMedia' --data-raw '{"RMediaState": "Enable"'}
   ```

2. Mount the media:
   ```bash
   ```
8.3.8. Collect BMC Debug Data

1. Create a request for BMC to start collecting debug data:

```bash
  "DiagnosticDataType": "OEM"
}'
```

**Example Output**

```json
{
  "@odata.context": "/redfish/v1/$metadata#Task.Task",
  "@odata.id": "/redfish/v1/TaskService/Tasks/1",
  "@odata.type": ">#Task.v1_4_2.Task",
  "Description": "Task for Manager CollectDiagnosticData",
  "Id": "1",
  "Name": "Manager CollectDiagnosticData",
  "TaskState": "New"
}
```

2. Monitor the task returned until it completes. Change task number as appropriate:

```bash
curl -k -u <bmc-user>:<password> --request GET 'https://<bmc-ip-address>/redfish/v1/TaskService/Tasks/1'
```

3. After the task stats reports Complete, download the attachments:

```bash
curl -k -u <bmc-user>:<password> --request GET 'https://<bmc-ip-address>/redfish/v1/Managers/BMC/LogServices/DiagnosticLog/Entries/All/Attachment' --output debugBMC.tgz
```

8.3.9. Clear BIOS and Reset to Factory Defaults

To clear the BIOS and reset the system to factory defaults:

```bash
echo "{"Targets":[{"/redfish/v1/UpdateService/FirmwareInventory/HostBIOS_0"}]}" > parameters.json
curl -k -u <bmc-user>:<password> -H 'Expect:' --location --request POST https://<bmc-ip-address>/redfish/v1/UpdateService/Actions/Oem/NvidiaUpdateService.ClearNVRAM -F 'UpdateParameters=@parameters.json;type=application/json'
```
Chapter 9. Safety

This section provides information about how to safely use the DGX H100 system.

9.1. Safety Information

To reduce the risk of bodily injury, electrical shock, fire, and equipment damage, read this document and observe all warnings and precautions in this guide before installing or maintaining your server product.

In the event of a conflict between the information in this document and information provided with the product or on the website for a particular product, the product documentation takes precedence.

Your server should be integrated and serviced only by technically qualified persons.

You must adhere to the guidelines in this guide and the assembly instructions in your server manuals to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products or components will void the UL Listing and other regulatory approvals of the product and may result in noncompliance with product regulations in the region(s) in which the product is sold.

9.2. Safety Warnings and Cautions

To avoid personal injury or property damage, before you begin installing the product, read, observe, and adhere to all of the following safety instructions and information.

The following safety symbols may be used throughout the documentation and may be marked on the product and the product packaging.

- **CAUTION**: Indicates the presence of a hazard that may cause minor personal injury or property damage if the CAUTION is ignored.

- **WARNING**: Indicates the presence of a hazard that may result in serious personal injury if the WARNING is ignored.

Indicates potential hazard if indicated information is ignored.

---

![Safety Symbol]

Indicates shock hazards that result in serious injury or death if safety instructions are not followed.
9.3. Intended Application Uses

This product was evaluated as Information Technology Equipment (ITE), which may be installed in offices, schools, computer rooms, and similar commercial type locations.

The suitability of this product for other product categories and environments (such as medical, industrial, residential, alarm systems, and test equipment), other than an ITE application, may require further evaluation.

9.4. Site Selection

Choose a site that is:

► Clean, dry, and free of airborne particles (other than normal room dust).
► Well-ventilated and away from sources of heat including direct sunlight and radiators.
► Away from sources of vibration or physical shock.
In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.

- Provided with a properly grounded wall outlet.
- Provided with sufficient space to access the power supply cord(s), because they serve as the product’s main power disconnect.

9.5. Equipment Handling Practices

To reduce the risk of personal injury or equipment damage, do the following:

- Conform to local occupational health and safety requirements when moving and lifting equipment.
- Use mechanical assistance or other suitable assistance when moving and lifting equipment.

9.6. Electrical Precautions

9.6.1. Power and Electrical Warnings

**Caution:** The power button, indicated by the stand-by power marking, DOES NOT completely turn off the system AC power; standby power is active whenever the system is plugged in. To remove power from system, you must unplug the AC power cord from the wall outlet. Make sure all AC power cords are unplugged before you open the chassis, or add or remove any non hot-plug components.

Do not attempt to modify or use an AC power cord if it is not the exact type required. A separate AC cord is required for each system power supply.

Some power supplies in servers use Neutral Pole Fusing. To avoid risk of shock use caution when working with power supplies that use Neutral Pole Fusing.

The power supply in this product contains no user-serviceable parts. Do not open the power supply. Hazardous voltage, current and energy levels are present inside the power supply. Return to manufacturer for servicing.

When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing it from the server.

To avoid risk of electric shock, turn off the server and disconnect the power cords, telecommunications systems, networks, and modems attached to the server before opening it.
9.6.2. Power Cord Warnings

**Caution:** To avoid electrical shock or fire, check the power cord(s) that will be used with the product as follows:

- Do not attempt to modify or use the AC power cord(s) if they are not the exact type required to fit into the grounded electrical outlets.
- The power cord(s) must meet the following criteria:
  - The power cord must have an electrical rating that is greater than that of the electrical current rating marked on the product.
  - The power cord must have safety ground pin or contact that is suitable for the electrical outlet.
  - The power supply cord(s) is/are the main disconnect device to AC power. The socket outlet(s) must be near the equipment and readily accessible for disconnection.
  - The power supply cord(s) must be plugged into socket-outlet(s) that is/are provided with a suitable earth ground.

9.7. System Access Warnings

To avoid personal injury or property damage, the following safety instructions apply whenever accessing the inside of the product:

- Turn off all peripheral devices connected to this product.
- Turn off the system by pressing the power button to off.
- Disconnect the AC power by unplugging all AC power cords from the system or wall outlet.
- Disconnect all cables and telecommunication lines that are connected to the system.
- Retain all screws or other fasteners when removing access cover(s). Upon completion of accessing inside the product, refasten access cover with original screws or fasteners.
- Do not access the inside of the power supply. There are no serviceable parts in the power supply.
- Return to manufacturer for servicing.
- Power down the server and disconnect all power cords before adding or replacing any non hot-plug component.
- When replacing a hot-plug power supply, unplug the power cord to the power supply being replaced before removing the power supply from the server.

**Caution:** If the server has been running, any installed processor(s) and heat sink(s) may be hot. Unless you are adding or removing a hot-plug component, allow the system to cool before opening the covers. To avoid the possibility of coming into contact with hot component(s) during a hot-plug installation, be careful when removing or installing the hot-plug component(s).
Caution: To avoid injury do not contact moving fan blades. Your system is supplied with a guard over the fan, do not operate the system without the fan guard in place.

9.8. Rack Mount Warnings

The following installation guidelines are required by UL to maintain safety compliance when installing your system into a rack.

The equipment rack must be anchored to an unmovable support to prevent it from tipping when a server or piece of equipment is extended from it. The equipment rack must be installed according to the rack manufacturer’s instructions.

Install equipment in the rack from the bottom up with the heaviest equipment at the bottom of the rack.

Extend only one piece of equipment from the rack at a time.

You are responsible for installing a main power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server(s).

To avoid risk of potential electric shock, a proper safety ground must be implemented for the rack and each piece of equipment installed in it.

Elevated Operating Ambient- If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading- Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading- Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing- Reliable earthing of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (for example, the use of power strips).
9.9. Electrostatic Discharge

**Caution:** ESD can damage drives, boards, and other parts. We recommend that you perform all procedures at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground (any unpainted metal surface) on your server when handling parts.

Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

9.10. Other Hazards

9.10.1. CALIFORNIA DEPARTMENT OF TOXIC SUBSTANCES CONTROL

Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/perchlorate.

Perchlorate Material: Lithium battery (CR2032) contains perchlorate. Please follow instructions for disposal.

9.10.2. NICKEL

NVIDIA Bezel. The bezel’s decorative metal foam contains some nickel. The metal foam is not intended for direct and prolonged skin contact. Please use the handles to remove, attach or carry the bezel. While nickel exposure is unlikely to be a problem, you should be aware of the possibility in case you are susceptible to nickel-related reactions.

9.10.3. Battery Replacement

**Caution:** There is the danger of explosion if the battery is incorrectly replaced. When replacing the battery, use only the battery recommended by the equipment manufacturer.

Dispose of batteries according to local ordinances and regulations. Do not attempt to recharge a battery.
Do not attempt to disassemble, puncture, or otherwise damage a battery.

9.10.4. Cooling and Airflow

**Caution:** Carefully route cables as directed to minimize airflow blockage and cooling problems. For proper cooling and airflow, operate the system only with the chassis covers installed.

Operating the system without the covers in place can damage system parts. To install the covers:

- Check first to make sure you have not left loose tools or parts inside the system.
- Check that cables, add-in cards, and other components are properly installed.
- Attach the covers to the chassis according to the product instructions.

The equipment is intended for installation only in a Server Room/Computer Room where both these conditions apply:

- Access can only be gained by SERVICE PERSONS or by USERS who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken.
- Access is through the use of a TOOL or lock and key, or other means of security, and is controlled by the authority responsible for the location.
Chapter 10. Compliance

The NVIDIA DGX H100 Server is compliant with the regulations listed in this section.

10.1. United States

Federal Communications Commission (FCC) FCC Marking (Class A)

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 any interference that may cause undesired operation of the device.

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.

California Department of Toxic Substances Control: Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/perchlorate.

10.2. United States/Canada

TÜV Rheinland of North America is accredited as a Nationally Recognized Testing Laboratory (NRTL), by OSHA (The Occupational Safety and Health Administration) in the United States, and as a Product Certification Body by SCC (Standards Council of Canada) in Canada. Refer to https://www.tuv.com/usa/en/ctuvus-certification.html

cTUVus Mark

![cTUVus Mark](image-url)
10.3. Canada

Innovation, Science and Economic Development Canada (ISED) CAN ICES-3(A)/NMB-3(A)

The Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la class A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

10.4. CE

European Conformity; Conformité Européenne (CE)

This is a Class A product. In a domestic environment this product may cause radio frequency interference in which case the user may be required to take adequate measures.

This device bears the CE mark in accordance with Directive 2014/53/EU. This device complies with the following Directives:

► Low Voltage Directive for electrical safety.
► RoHS Directive for hazardous substances.
► Energy-related Products Directive (ErP).

The full text of EU declaration of conformity is available at the following URL: http://www.nvidia.com/support

A copy of the Declaration of Conformity to the essential requirements may be obtained directly from NVIDIA GmbH (Bavaria Towers – Blue Tower, Einsteinstrasse 172, D-81677 Munich, Germany).
10.5. Australia and New Zealand

Australian Communications and Media Authority

This product meets the applicable EMC requirements for Class A, I.T.E equipment.

10.6. Brazil

INMETRO

10.7. Japan

Voluntary Control Council for Interference (VCCI)
This is a Class A product.

In a domestic environment this product may cause radio interference, in which case the user may be required to take corrective actions. VCCI-A.

A Japanese regulatory requirement, defined by specification JISC 0950, 2008, mandates that manufacturers provide Material Content Declarations for certain categories of electronic products offered for sale after July 1, 2006. A "Material Content Declaration" is a listing of specific materials contained in a product.}

To view the JISC 0950 material declaration for this product, visit [this link](#).

### Japan RoHS Material Content Declaration

<table>
<thead>
<tr>
<th>機種名</th>
<th>特定化学物質記載</th>
<th>重金属</th>
<th>Cd</th>
<th>Cr(VI)</th>
<th>Hg</th>
<th>Pb</th>
<th>PBBs</th>
<th>PBDEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>主な分類</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>電源</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ジャンパー</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>システムメモリ</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ハードディスクドライブ</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>機械部品（フット、ヒートシンク、ベゼル、…）</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ケーブル/ケーブル</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>はんだ付け材料</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>フラックス、クリームはんだ、フラスム、その他の消耗品</td>
<td>除外項目</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

注：
1. 「R」は、特定化学物質の含有率が日本工業規格JIS C 0950:2008に記載されている含有基準値より低いたことを示します。
2. 「除外項目」は、特定化学物質が有するマークの除外項目に該当するため、特定化学物質について、日本工業規格JIS C 0950:2008に基づく有無の表示が不要であることを示します。
3. 「0.01wt%」または「0.01wt%」は、特定化学物質の含有率が日本工業規格JIS C 0950:2008に記載されている含有基準値を満たしていないことを示します。
10.8. South Korea

Korean Agency for Technology and Standards (KATS)

Class A Equipment (Industrial Broadcasting & Communication Equipment). This equipment Industrial (Class A) electromagnetic wave suitability equipment and seller or user should take notice of it, and this equipment is to be used in the places except for home.
China Compulsory Certificate

No certification is needed for China. The NVIDIA DGX H100 is a server with power consumption greater than 1.3 kW.
### China RoHS Material Content Declaration

<table>
<thead>
<tr>
<th>部件名称</th>
<th>材质</th>
<th>汞</th>
<th>铅</th>
<th>镉</th>
<th>六价铬</th>
<th>多溴联苯</th>
<th>多溴联苯醚</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCA</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Processor</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Motherboard</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Power supply</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>System memory</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hard drive</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mechanical parts (fan, heat sink, bezel, etc.)</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cables/Connectors</td>
<td>X</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
10.10. Taiwan

Bureau of Standards, Metrology & Inspection (BSMI)

Warning:
This is a high-power equipment, which should be used in a safe environment to avoid the risk of human injury. In case of any danger, users should take appropriate measures to prevent accidents.

Responsible Party:

Hong Kong Hui Tong Electronics Co., Ltd. Taiwan Branch

统一编号：80022300

Taoyuan Nanhua District Jihua Road No. 8.
Taiwan RoHS Material Content Declaration

This device complies with the technical regulations of the Customs Union (CU TR)

ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ ТАМОЖЕННОГО СОЮЗА О безопасности низковольтного оборудования (ТР ТС 004/2011)

ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ ТАМОЖЕННОГО СОЮЗА Электромагнитная совместимость технических средств (ТР ТС 020/2011)

Технический регламент Евразийского экономического союза "Об ограничении применения опасных веществ в изделиях электротехники и радиоэлектроники" (ТР ЕАЭС 037/2016)

Federal Agency of communication (FAC)

This device complies with the rules set forth by Federal Agency of Communications and the Ministry of Communications and Mass Media.

Federal Security Service notification has been filed.

10.11. Russia/Kazakhstan/Belarus
10.12. Israel

SII

Authenticity may be verified by visiting the Bureau of Indian Standards website at http://www.bis.gov.in.

10.13. India

Bureau of India Standards (BIS)

Authenticity may be verified by visiting the Bureau of Indian Standards website at http://www.bis.gov.in.
India RoHS Compliance Statement

This product, as well as its related consumables and spares, complies with the reduction in hazardous substances provisions of the “India E-waste (Management and Handling) Rule 2016”. It does not contain lead, mercury, hexavalent chromium, polybrominated biphenyls or polybrominated diphenyl ethers in concentrations exceeding 0.1 weight % and 0.01 weight % for cadmium, except for where allowed pursuant to the exemptions set in Schedule 2 of the Rule.

10.14. South Africa

South African Bureau of Standards (SABS)

This device complies with the following SABS Standards:

National Regulator of Compulsory Specification (NRCS)

This device complies with following standard under VC 8055:
SANS IEC 60950-1

10.15. Great Britain (England, Wales, and Scotland)

UK Conformity Assessed

This device complies with the following Regulations:
▶ SI 2016/1091: Electromagnetic Compatibility (EMC)
▶ SI 2016/1101: The Low Voltage Electrical Equipment (Safety)
▶ SI 2012/3032: The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (As Amended)

A copy of the Declaration of Conformity to the essential requirements may be obtained directly from NVIDIA Ltd. (100 Brook Drive, 3rd Floor Green Park, Reading RG2 6UJ, United Kingdom)
Chapter 11. Third-Party License Notices

This NVIDIA product contains third party software that is being made available to you under their respective open source software licenses. Some of those licenses also require specific legal information to be included in the product. This section provides such information.

11.1. Micron msecli

The msecli utility is provided under the following terms:

Micron Technology, Inc. Software License Agreement PLEASE READ THIS LICENSE AGREEMENT ("AGREEMENT") FROM MICRON TECHNOLOGY, INC. ("MTI") CAREFULLY: BY INSTALLING, COPYING OR OTHERWISE USING THIS SOFTWARE AND ANY RELATED PRINTED MATERIALS ("SOFTWARE"), YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS OF THIS AGREEMENT, DO NOT INSTALL THE SOFTWARE. LICENSE: MTI hereby grants to you the following rights: You may use and make one (1) backup copy the Software subject to the terms of this Agreement. You must maintain all copyright notices on all copies of the Software. You agree not to modify, adapt, decompile, reverse engineer, disassemble, or otherwise translate the Software. MTI may make changes to the Software at any time without notice to you. In addition MTI is under no obligation whatsoever to update, maintain, or provide new versions or other support for the Software. OWNERSHIP OF MATERIALS: You acknowledge and agree that the Software is proprietary property of MTI (and/or its licensors) and is protected by United States copyright law and international treaty provisions. Except as expressly provided herein, MTI does not grant any express or implied right to you under any patents, copyrights, trademarks, or trade secret information. You further acknowledge and agree that all right, title, and interest in and to the Software, including associated proprietary rights, are and shall remain with MTI (and/or its licensors). This Agreement does not convey to you an interest in or to the Software, but only a limited right to use and copy the Software in accordance with the terms of this Agreement. The Software is licensed to you and not sold.

DISCLAIMER OF WARRANTY:

THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MTI EXPRESSLY DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, NONINFRINGEMENT OF THIRD PARTY RIGHTS, AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. MTI DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. FURTHERMORE, MTI DOES NOT MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU. IN NO EVENT SHALL MTI, ITS AFFILIATED COMPANIES OR THEIR SUPPLIERS BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR SPECIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF
INFORMATION) ARISING OUT OF YOUR USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF MTI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Because some jurisdictions prohibit the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

TERMINATION OF THIS LICENSE: MTI may terminate this license at any time if you are in breach of any of the terms of this Agreement. Upon termination, you will immediately destroy all copies the Software.

GENERAL: This Agreement constitutes the entire agreement between MTI and you regarding the subject matter hereof and supersedes all previous oral or written communications between the parties. This Agreement shall be governed by the laws of the State of Idaho without regard to its conflict of laws rules.

CONTACT: If you have any questions about the terms of this Agreement, please contact MTI’s legal department at (208) 368-4500. By proceeding with the installation of the Software, you agree to the terms of this Agreement. You must agree to the terms in order to install and use the Software.

11.2. Mellanox (OFED)

MLNX_OFED <http://www.mellanox.com/> is provided under the following terms:

Copyright (c) 2006 Mellanox Technologies. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Chapter 12. Notices

12.1. Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer’s own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or
services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

12.2. Trademarks

NVIDIA, the NVIDIA logo, DGX, DGX-1, DGX-2, DGX A100, DGX H100, DGX Station, and DGX Station A100 are trademarks and/or registered trademarks of NVIDIA Corporation in the United States and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

12.3. Copyright

© [2023] NVIDIA Corporation & Affiliates. All rights reserved.

Copyright

©2022-2023, NVIDIA