Connecting to BMC Interfaces

Table of contents

BMC Management Interface

The BMC has a separate Ethernet interface which provides network connection for management traffic to the BMC. The NVIDIA® BlueField® networking platform's bracket (DPU or SuperNIC) has an RJ45 port labeled "MGMT" which is the management interface port. The management port is configured with auto-negotiation capabilities by default (100MbE to 1GbE).

The BMC interface `eth0` is the management interface, so any information displayed by `ifconfig eth0` pertains to the management interface. The MAC address to be used for `eth0` is pre-programmed in the BMC FRU EEPROM and can be found on the BlueField's board label. By default, the IP address used for `eth0` is acquired via DHCP but can be configured differently.

BMC Password Policy

The BMC password must comply with the following policy parameters:

- Using ASCII and Unicode characters is permitted
- Minimum length: 12
- Maximum length: 20
- Maximum number of consecutive character pairs: 4

Info

Two characters are consecutive if `|hex(char_1)-hex(char_2)|=1`.

Examples of passwords with 5 consecutive character pairs (invalid): `DcBa123456AbCd!`; `ab1XbcYcdZdeGef!`; `Testing_123abcgh!`.

The following is a valid example password:

- `HelloNvidia3D!`

> **Note**
>
> A user account is locked for 10 minutes after 10 consecutive failed attempts.

Changing Default Password

When initially logging into the system, it is mandatory to update the default BMC password, `0penBmc`. The BlueField BMC offers two methods/interfaces for changing the password:

- SSH/serial:

  To change the password, connect to the BMC via SSH/serial and log in using the root user and the default password. Upon logging in, you are prompted with the following:

  ```
  dpu-bmc login: root
  Password: <Type default password>
  You are obliged to immediately change your password
  (mandatory for administrators).
  Changing the root password.
  Current password: <Retype the default password>
  New password: <Type the new password according to the above
  rules>
  Retype the new password: <Retype the new password>
  ```

- Redfish:

  The Redfish user management interface may be used to configure the new password. The following Redfish command can be employed to alter the default password:

```
curl -k -u root:0penBmc -H "Content-Type: application/json" -X PATCH
https://<bmc_ip>/redfish/v1/AccountService/Accounts/root -d
'{"Password" : "<password>"}'
```

Account Service

The Redfish root user can inquire about and modify the applied account policies, which encompass settings such as the number of consecutive login attempts permitted and the time period for which the system will remain locked.

The following Redfish command provides the current settings:

```
curl -k -u root:'<password>' -H 'Content-Type: application/json' -X GET
https://10.237.53.58/redfish/v1/AccountService
```

Example output:

```
{
  "@odata.id": "/redfish/v1/AccountService",
  "@odata.type": "#AccountService.v1_10_0.AccountService",
  "AccountLockoutDuration": 600,
  "AccountLockoutThreshold": 4,
  "Accounts": {
    "@odata.id": "/redfish/v1/AccountService/Accounts"
  },
  "ActiveDirectory": {
    "Authentication": {
      "AuthenticationType": "UsernameAndPassword",
      "Password": null,
      "Username": ""
    },
    "LDAPService": {
      "SearchSettings": {
        "BaseDistinguishedNames": [
          ""
        ],
        "GroupsAttribute": "",
        "UsernameAttribute": ""
      }
    },
    "RemoteRoleMapping": [],
    "ServiceAddresses": [
      ""
    ],
    "ServiceEnabled": false
  },
  "Description": "Account Service",
  "Id": "AccountService",
  "LDAP": {
    "Authentication": {
      "AuthenticationType": "UsernameAndPassword",
      "Password": null,
      "Username": ""
    },
    "Certificates": {
      "@odata.id": "/redfish/v1/AccountService/LDAP/Certificates"
    },
    "LDAPService": {
      "SearchSettings": {
        "BaseDistinguishedNames": [
          ""
        ],
        "GroupsAttribute": "",
        "UsernameAttribute": ""
      }
    },
    "RemoteRoleMapping": [],
    "ServiceAddresses": [
      ""
    ],
    "ServiceEnabled": false
  },
  "MaxPasswordLength": 20,
  "MinPasswordLength": 13,
  "Name": "Account Service",
  "Oem": {
    "OpenBMC": {
      "@odata.id": "/redfish/v1/AccountService#/Oem/OpenBMC",
      "@odata.type": "#OemAccountService.v1_0_0.AccountService",
      "AuthMethods": {
        "BasicAuth": true,
        "Cookie": true,
        "SessionToken": true,
        "TLS": true,
        "XToken": true
      }
    }
  },
  "Roles": {
    "@odata.id": "/redfish/v1/AccountService/Roles"
  },
  "ServiceEnabled": true
}
```

By default, if a user attempts to log into the system with an incorrect password four times in a row, their account is locked for 600 seconds. Afterwards, the user is allowed another opportunity to log in with the correct credentials. If the user fails to log in again, the account is immediately locked for an additional 600 seconds. If the user logs in successfully, the counter of consecutive login failures is reset.

The `patch` command may be used to modify the default policy settings. The following example illustrates how to alter the number of allowed consecutive login attempts into the system.

```
curl -k -u root:'<password>' -H 'Content-Type: application/json'
-X PATCH https://<IP>/redfish/v1/AccountService -d
'{"AccountLockoutThreshold" : 10}'
```

Info

For a comprehensive understanding of the schema, please refer to the DMTF definition of the AccountService.v1_10_0.AccountService schema.

If an account becomes inaccessible, users may check the system's status using the Redfish interface using the following GET operation:

```
curl -k -u root:'<password>' -H 'Content-Type: application/json' -X GET
https://<IP>/redfish/v1/AccountService
```

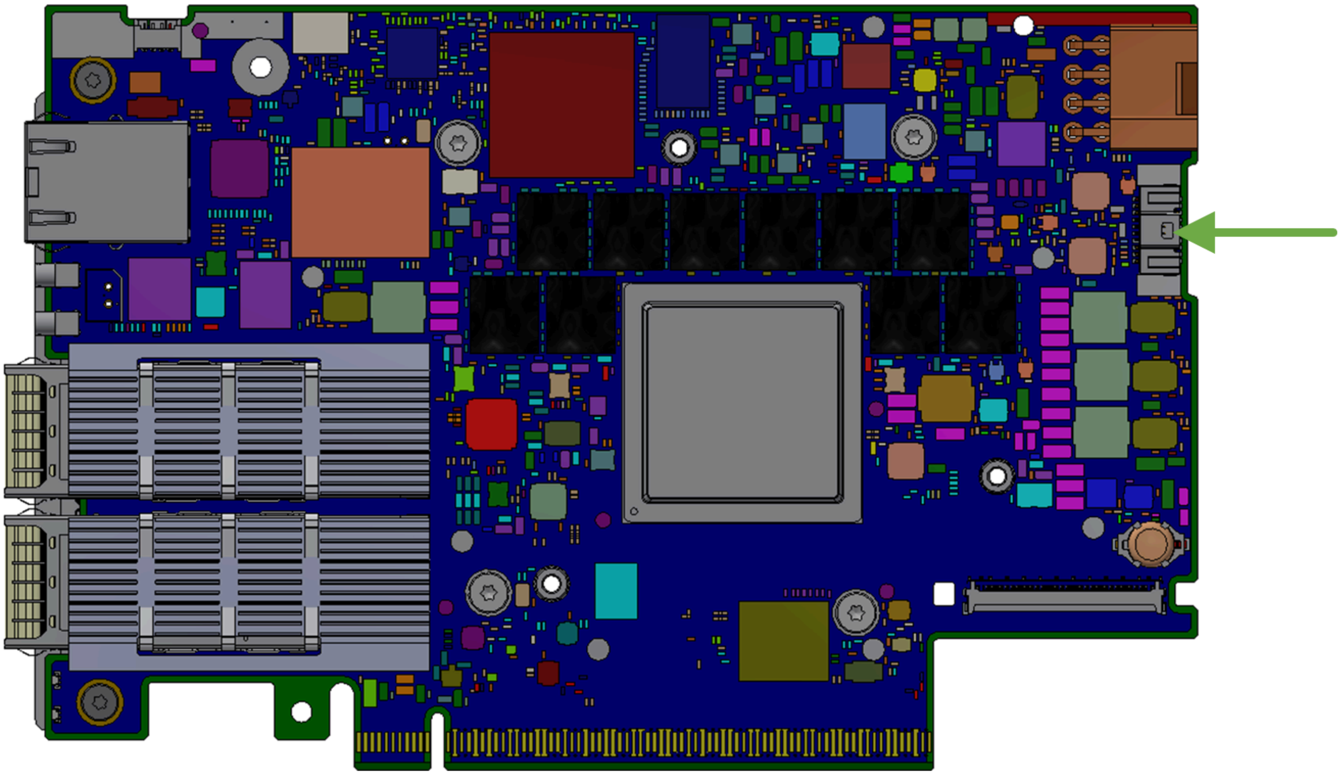
Example output:

```
{
   "error" :  {
      "@Message.ExtendedInfo" :  [
         {
            "@odata.type" :  "#Message.v1_1_1.Message",
            "Message" :  "While accessing the resource at '/redfish/v1/AccountService', the service
received an authorization error 'Account temporarily locked out for 600 seconds due to multiple
authentication failures'.",
                "MessageArgs" :  [
                    "/redfish/v1/AccountService" ,
                    "Account temporarily locked out for 600 seconds due to multiple authentication failures"
                ] ,
                "MessageId" :  "Base.1.15.0.ResourceAtUriUnauthorized" ,
                "MessageSeverity" :  "Critical" ,
                "Resolution" :  "Ensure that the appropriate access is provided for the service in order for it to access the URI."
            }
        ] ,
        "code" :  "Base.1.15.0.ResourceAtUriUnauthorized" ,
        "message" :  "While accessing the resource at '/redfish/v1/AccountService', the service received an authorization error 'Account temporarily locked out for 600 seconds due to multiple authentication failures'."
    }
}
```

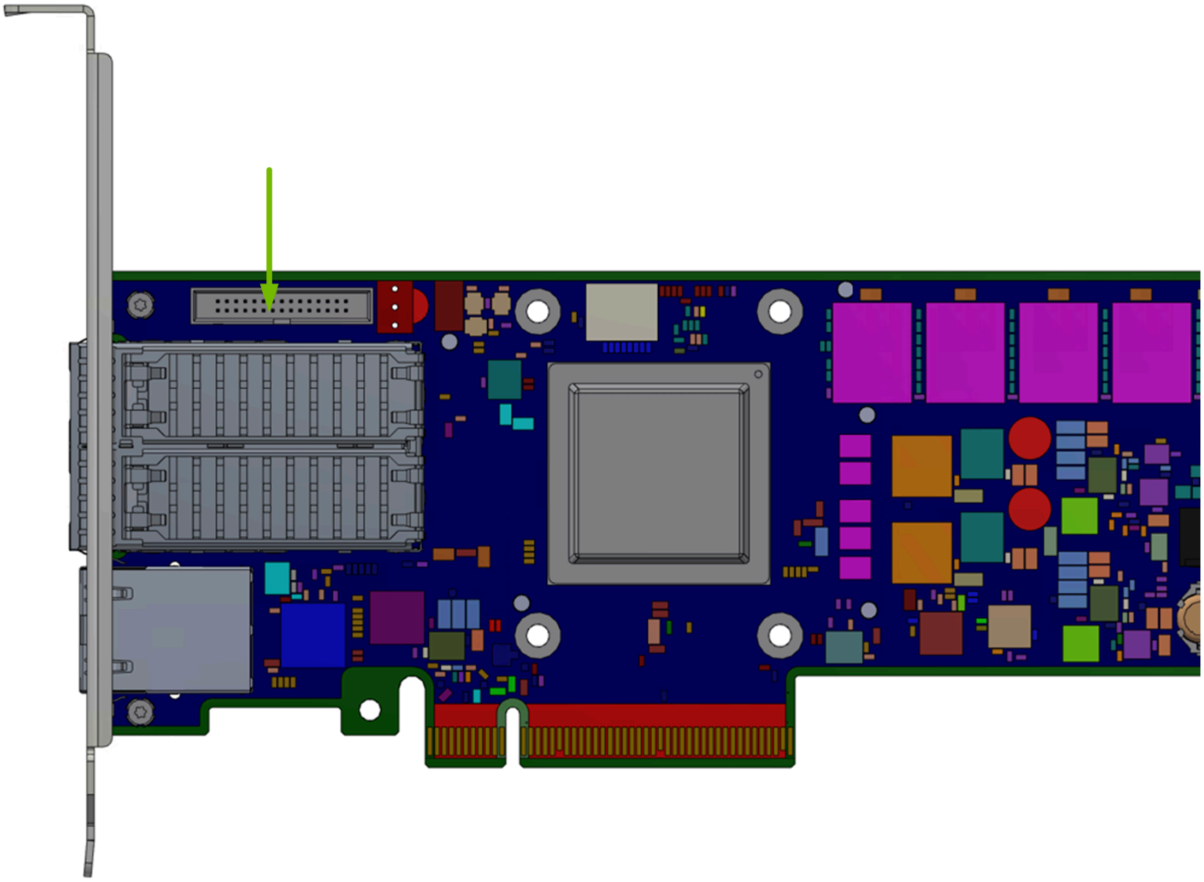
BMC Console Interface

The BMC UART1 console is available on the IO panel. The BMC is connected to a 20-pin connector for BlueField-3 or 30-pin connector for BlueField-2 which allows the Linux console to be monitored.

BlueField-3 BMC Connector



BlueField-2 BMC Connector



Network Configuration

⚠ **Warning**

Do not manually modify the network configuration file `/etc/systemd/network/00-bmc-eth0.network`.

There are two ways of configuring the network interfaces:

- Dynamic (DHCP)
- Static

See section "Network Protocol Support" for more details.

BMC USB Port

This section describes the use cases for the BMC USB port. Note that only BMC Linux has access to the USB port and its feature set. There is no access to BMC USB port while running u-boot.

ⓘ **Note**

Due to a hardware bug in AST2500, the USB interface is only able to work at USB 1.0 speeds.

ⓘ **Note**

Storage device support on this port has only been validated with USB flash drives.

Providing Removable Storage via USB Stick

Once a USB stick is plugged in to the BMC's USB port, issue the command `lsusb` and/or check the dmesg log to see if the USB stick has been detected. The successful insertion of a USB stick will create a device under `/dev` called `sda` (or `sdb`), and a mountable partition `/dev/sda1`. To mount the USB stick as a filesystem, just issue the command "`mount /dev/sda1 /mnt`" to mount it at `/mnt`. The command "`umount /mnt`" unmounts the device.

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

Trademarks