SN10-8R system administration guide (3 PDU)

Version 1.12

Chapter 1. SambaNova support and documentation

SambaNova customers with valid support contracts can contact SambaNova Support and can access product knowledge base (KB) articles and product documentation.

- Find SambaNova KB articles at https://support.sambanova.ai.
- Find SambaNova documentation at https://docs.sambanova.ai.

1.1. How to contact SambaNova support

In the event of hardware or software issues, contact SambaNova Support through the SambaNova Support portal (https://sambanova.ai/support). The portal gives access to many KB articles for resolving problems.

- To get help resolving an issue, go to the SambaNova Support portal (https://support.sambanova.ai) and open a support case.
- To open a support case, see the KB article #1017, “SambaNova Systems Support Best Practices”

1.2. About this document

Overview: This document provides details for how to perform administrative tasks within the SambaNova DataScale SN10-8R (hereafter called DataScale SN10-8R), for example, how to access, monitor, upgrade, and debug the system.

Audience: System administrators and support personnel.

Chapter 2. Overview of SambaNova DataScale SN10-8R hardware

The DataScale SN10-8R is self-contained in a standard 42 rack unit (RU) datacenter rack. System population begins at the bottom of the rack with system 1 and increments up the rack to system 2. Network switches and other equipment are installed at the top of the rack.

A DataScale SN10-8 system consists of the following:

- Four DataScale SN10-2 reconfigurable data units (RDU) modules, also called XRDUs.
- An x86 server DataScale SN10-H host module running either Red Hat® Enterprise Linux® or Ubuntu® Linux

Each of the four DataScale SN10-2 RDU modules contains two RDUs, for a total of eight RDUs per DataScale SN10-8 system. The RDUs are managed by the SambaNova SambaFlow™ software stack running on the DataScale SN10-H host module. The DataScale SN10-2 RDU modules and the DataScale SN10-H host module are 2RU chassis.

Switch equipment at the top of the rack provides a data network and an access network. Figure 1 and Table 1 identify the main components in the DataScale SN10-8R.

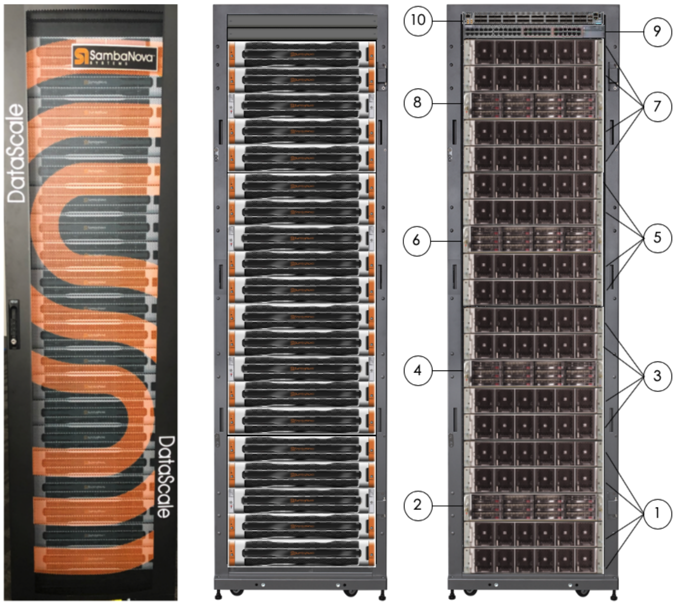


Figure 1. DataScale SN10-8R components (front view)

Table 1. DataScale SN10-8 rack components

No.	Component
1	System 1 SN10-8 (four SN10-2 RDU modules)
2	System 1 SN10-8 (one SN10-H host module)
3	System 2 SN10-8 (four SN10-2 RDU modules)
4	System 2 SN10-8 (one SN10-H host module)
5	System 3 SN10-8 (four SN10-2 RDU modules)
6	System 3 SN10-8 (one SN10-H host module)
7	System 4 SN10-8 (four SN10-2 RDU modules)
8	System 4 SN10-8 (one SN10-H host module)
9	Juniper® QFX5200-32c Eth (default) Mellanox® SB7800 IB (optional) high-bandwidth data switch
10	Juniper® EX4300 access switch

SambaNova delivers the DataScale SN10-8R internal components preconfigured and cabled in the 42RU rack. This section identifies what is cabled internally.

> **NOTE**
>
> You are *not* expected to interact with the internal cabling of the DataScale SN10-8R. You have to interact only with cables for the network and power components. You connect those cables to provide power and network connectivity to the DataScale SN10-8R. See the *DataScale SN10-8R Hardware Installation* documentation, which you can find in the SambaNova documentation portal (https://docs.sambanova.ai).

Figure 2 and Table 2 identify the locations of the main components in the DataScale SN10-8R.

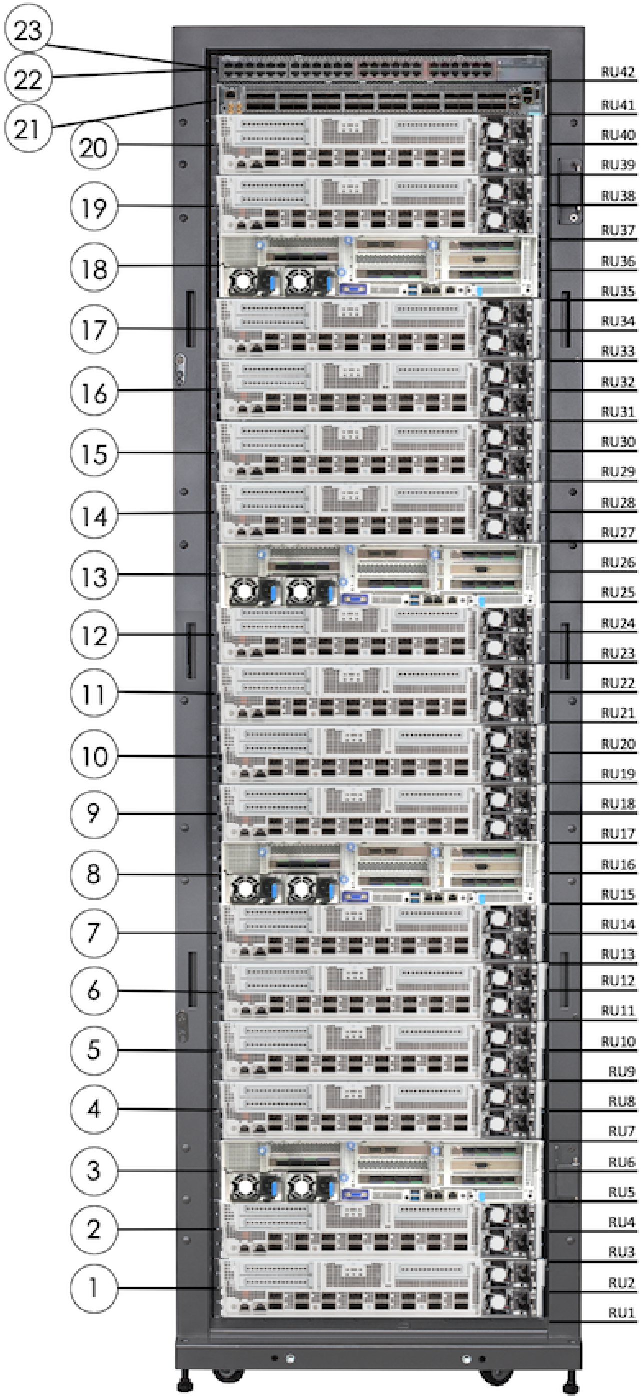


Figure 2. DataScale SN10-8R (rear view)

Table 2. DataScale SN10-8R component identification

No.	Component Description
1	SN10-2-1 (system 1)
2	SN10-2-2 (system 1)
3	SN10-H-1 (system 1)
4	SN10-2-3 (system 1)
5	SN10-2-4 (system 1)
6	SN10-2-5 (system 2)
7	SN10-2-6 (system 2)
8	SN10-H-2 (system 2)
9	SN10-2-7 (system 2)
10	SN10-2-8 (system 2)
11	SN10-2-9 (system 3)
12	SN10-2-10 (system 3)
13	SN10-H-3 (system 3)
14	SN10-2-11 (system 3)
15	SN10-2-12 (system 3)
16	SN10-2-13 (system 4)
17	SN10-2-14 (system 4)
18	SN10-H-4 (system 4)
19	SN10-2-15 (system 4)
20	SN10-2-16 (system 4)
21	Juniper® QFX5200-32c Eth (default) Mellanox® SB7800 IB (optional) high-bandwidth data switch
22	Juniper EX4300 access switch
23	Lantronix® serial console server (behind Juniper EX4300)
0RU power distribution units (PDUs), not shown, are on the right side of the rack when you face the rack rear.	

Chapter 3. SambaNova SambaFlow software stack

The software stack contains several pieces including:

- Front-end APIs

- Compilers
- SambaFlow Runtime (which executes the models)

The entire software stack is called the SambaFlow software stack. The SambaFlow software is installed and executed on the SN10-H host modules.

The SambaFlow documentation (*SambaFlow SDK* and *SambaFlow Runtime*) describe the software stack, model development, and deployment. See https://docs.sambanova.ai.

3.1. DataScale SN10-8R operating systems

In addition to the SambaFlow software stack, the DataScale SN10-8R includes two preinstalled operating system (OS) flavors that run on the DataScale SN10-H host module on each system:

- An image for Red Hat Enterprise Linux (RHEL)
- An image for Ubuntu Linux Server

NOTE Both images are preinstalled on each of the SN10-H host modules within the DataScale SN10 rack.

For specific versions of the supported OS flavors on the SN10-H host module, see the "Supported versions of the SN10-H operating systems" section of this document.

SambaNova provides updates to the OS images, as well as updates for the software components, through a repository that is described in the "Connecting to the SambaNova repository" section under "*Administrative tasks for the SN10-H host module*."

3.2. Identifying the SambaFlow software version

he command you run to identify the version of the SambaFlow software packages that are installed on the DataScale SN10-H host modules depends on the OS that is running on the module.

Identify the software version on RHEL:

```
$ rpm -qa | grep samba[nf]
sambanova-deps-libfabric-1.8.1-1.el7.x86_64
sambanova-deps-openssl-1.1.1-3.el7.x86_64
sambaflow-1.0.0-2003130359.el7.x86_64
sambanova-tools-python3-3.7.6-0.el7.x86_64
sambanova-deps-grpc-protobuf-1.0.0-2002191211.el7.x86_64
sambanova-deps-mpich-3.3.1-0.el7.x86_64
sambanova-arcprism-1.0.0-2003130359.el7.x86_64
sambanova-runtime-1.0.0-2003130359.el7.x86_64
sambanova-deps-pytorch-1.3.1-3.el7.x86_64
```

Identify the software version on Ubuntu Linux:

```
$ dpkg -l | grep samba[nf]
sambanova-arcprism 1.0.1-2006030747 amd64 SambaFlow model compiler
sambanova-deps-mpich 3.3.1-2 amd64 auto-generated package by debmake
sambanova-deps-pytorch 1.5.0-2 amd64 auto-generated package by debmake
sambanova-deps-torchvision 0.6.0-2 all SambaNova 3rd party dependencies…
sambanova-model-analyzer 1.0.1-2006030747 amd64 SambaNova Model Analyzer
sambanova-runtime 1.0.1-2006030747 amd64 SambaNova Runtime
sambanova-runtime-diag 1.0.1-2006030747 amd64 SambaNova Runtime Diagnostics
sambanova-tools-llvm-8 8.0.0-4 amd64 auto-generated package by debmake
sambanova-tools-pip3 20.1.1-1 all SambaNova tools: pip3
sambanova-tools-python3 3.7.6-1 amd64 auto-generated package by debmake
```

Chapter 4. IP address assignments

The tables in this section show the DataScale SN10-8R IP address assignments for the access network and the data network, as described in the *DataScale SN10-8R Hardware Installation* document, which you can find in the SambaNova documentation portal (https://docs.sambanova.ai). The subnets and host IP addresses were provided by your company via the Pre-Delivery Site Survey document prior to the delivery and installation of the DataScale SN10-8R.

4.1. IP address assignments for the access network

Table 3 shows the access network IP address assignments for components such as the BMC, the switch equipment, and the PDUs in the DataScale SN10-8R. The example IP addresses shown in the **Example (10.0.1.0/26)** column assume a customer provided a 10.0.1.0/26 subnet.

See *Default username and passwords for components* for details. Reserved addresses and the broadcast IP address don’t have default usernames and passwords.

Table 3. Access network IP address assignments

Base IP address	Example IP address (10.0.1.0/26)	Component	System #
x.x.x.0 Broadcast IP address for network	10.0.1.0	-	-
x.x.x.1 Customer router virtual IP (VIP) address	10.0.1.1	-	-
x.x.x.2 Customer router #1	10.0.1.2	-	-
x.x.x.3 Customer router #2	10.0.1.3	-	-
x.x.x.4	10.0.1.4	-	-
x.x.x.5	10.0.1.5	Serial console server	-
x.x.x.6	10.0.1.6	Access switch	-

Base IP address	Example IP address (10.0.1.0/26)	Component	System #
x.x.x.7	10.0.1.7	Data switch	-
x.x.x.8	10.0.1.8	PDU 1	-
x.x.x.9	10.0.1.9	PDU 2	-
x.x.x.10	10.0.1.10	PDU 3	-
x.x.x.20	10.0.1.20	SN10-H-1 OS	System 1
x.x.x.21	10.0.1.21	SN10-H-1 BMC	System 1
x.x.x.22	10.0.1.22	SN10-2-1 BMC	System 1
x.x.x.23	10.0.1.23	SN10-2-2 BMC	System 1
x.x.x.24	10.0.1.24	SN10-2-3 BMC	System 1
x.x.x.25	10.0.1.25	SN10-2-4 BMC	System 1
x.x.x.30	10.0.1.30	SN10-H-2 OS	System 2
x.x.x.31	10.0.1.31	SN10-H-2 BMC	System 2
x.x.x.32	10.0.1.32	SN10-2-5 BMC	System 2
x.x.x.33	10.0.1.33	SN10-2-6 BMC	System 2
x.x.x.34	10.0.1.34	SN10-2-7 BMC	System 2
x.x.x.35	10.0.1.35	SN10-2-8 BMC	System 2
x.x.x.40	10.0.1.40	SN10-H-3 OS	System 1
x.x.x.41	10.0.1.41	SN10-H-3 BMC	System 1
x.x.x.42	10.0.1.42	SN10-2-9 BMC	System 1
x.x.x.43	10.0.1.43	SN10-2-10 BMC	System 1
x.x.x.44	10.0.1.44	SN10-2-11 BMC	System 1
x.x.x.45	10.0.1.45	SN10-2-12 BMC	System 1
x.x.x.50	10.0.1.50	SN10-H-4 OS	System 2
x.x.x.51	10.0.1.51	SN10-H-4 BMC	System 2
x.x.x.52	10.0.1.52	SN10-2-13 BMC	System 2
x.x.x.53	10.0.1.53	SN10-2-14 BMC	System 2
x.x.x.54	10.0.1.54	SN10-2-15 BMC	System 2
x.x.x.55	10.0.1.55	SN10-2-16 BMC	System 2
x.x.x.63 Broadcast IP address for network	10.0.1.63	-	

4.2. IP address assignments for the data network

Table 4 shows the high-bandwidth data network IP address assignments for the compute components in the DataScale SN10-8R. The example IP addresses shown in the **Example (10.0.1.64/27)** column assume a customer who povided a 10.0.1.64/27 subnet.

Table 4. Data network IP address assignments

Base IP address	Example IP address (10.0.1.64/27)	Component	System #	Note
x.x.x.0	10.0.1.64	-	-	Broadcast IP address for network
x.x.x.1	10.0.1.65	-	-	Customer router VIP
x.x.x.2	10.0.1.66	-	-	Customer router #1
x.x.x.3	10.0.1.67	-	-	Customer router #2
x.x.x.4	10.0.1.68	SN10-H-1 PCIe CX5	System 1	-
x.x.x.5	10.0.1.69	SN10-2-1 PCIe CX5	System 1	-
x.x.x.6	10.0.1.70	SN10-2-2 PCIe CX5	System 1	-
x.x.x.7	10.0.1.71	SN10-2-3 PCIe CX5	System 1	-
x.x.x.8	10.0.1.72	SN10-2-4 PCIe CX5	System 1	-
x.x.x.9	10.0.1.73	SN10-H-2 PCIe CX5	System 2	-
x.x.x.10	10.0.1.74	SN10-2-5 PCIe CX5	System 2	-
x.x.x.11	10.0.1.75	SN10-2-6 PCIe CX5	System 2	-
x.x.x.12	10.0.1.76	SN10-2-7 PCIe CX5	System 2	-
x.x.x.13	10.0.1.77	SN10-2-8 PCIe CX5	System 2	-
x.x.x.14	10.0.1.78	SN10-H-3 PCIe CX5	System 3	-
x.x.x.15	10.0.1.79	SN10-2-1 PCIe CX5	System 3	-
x.x.x.16	10.0.1.80	SN10-2-2 PCIe CX5	System 3	-
x.x.x.17	10.0.1.81	SN10-2-3 PCIe CX5	System 3	-
x.x.x.18	10.0.1.82	SN10-2-4 PCIe CX5	System 3	-

Base IP address	Example IP address (10.0.1.64/27)	Component	System #	Note
x.x.x.19	10.0.1.83	SN10-H-4 PCIe CX5	System 4	-
x.x.x.20	10.0.1.84	SN10-2-5 PCIe CX5	System 4	-
x.x.x.21	10.0.1.85	SN10-2-6 PCIe CX5	System 4	-
x.x.x.22	10.0.1.86	SN10-2-7 PCIe CX5	System 4	-
x.x.x.23	10.0.1.87	SN10-2-8 PCIe CX5	System 4	-
x.x.x.31	10.0.1.95	-	-	Broadcast IP address for network

Chapter 5. Default username and passwords for components

Table 5 shows several components in the DataScale SN10-8R that are assigned default passwords for users who have administrative/root credentials. SambaNova highly recommends changing these passwords.

NOTE Do not use a slash character in a password for an XRDU. Both forward slash (/) and backward slash (\) can cause problems.

Table 5. Default usernames and passwords

Component	Username	Default password
Lantronix serial console server	`sysadmin`	`Changeme`
Juniper QFX5200 high-bandwidth Ethernet data switch	`root`	`Changeme`
Mellanox SB7800 IB high-bandwidth data switch	`admin`	`Changeme`
Juniper EX4300 access switch	`root`	`Changeme`
DataScale SN10-2 BMC	`root`	`1Changeme`
DataScale SN10-H BMC	`admin`	`Changeme` **NOTE**: Password must not exceed 14 characters.
DataScale SN10-H OS	`root`	`Changeme`
DataScale SN10-H OS	`snuser1`	`Changeme`

Component	Username	Default password
Vertiv^{TM} PDU	`admin`	`Changeme`

IMPORTANT The operating system on SN10-H by default is configured with user `snuser1` which has superuser privileges (i.e. can run `sudo` commands). This user is used to run example applications during the post-install test of the system. For security reasons it is highly recommended that you delete this user after the test is completed. You can then create your own users or configure the system to use a company-wide LDAP server.

NOTE For information on PDU password recovery, see KB article 1054.

Chapter 6. Managing power for the DataScale SN10-8R

For proper operation of the DataScale SN10-8R and to prevent issues, be sure you power on and power off the system appropriately, as described below.

6.1. Warnings and general notes

The following notices apply to the DataScale SN10-8R.

WARNING Some components within the rack work at high voltage. To prevent personal injury and voiding of the warranty, do **not** attempt to service components except where noted.

WARNING To prevent the DataScale SN10-8R from failing and to prevent damage to its components, keep the front and rear rack doors closed during standard operation.

WARNING To prevent DataScale SN10-8R components from overheating, keep the front and rear of the rack clear of obstructions to allow proper airflow.

WARNING Before starting the DataScale SN10-8R, read the SambaNova *DataScale SN10-8R Release Notes* (at https://docs.sambanova.ai) to ensure you understand any known issues or limitations that might apply to the system. If you do not read the release notes, you might incorrectly configure the system components or software, which might necessitate a factory reset.

WARNING Do not power off or reboot the DataScale SN10-8R components during a firmware update. Doing so might damage the DataScale SN10-8R components, and damaged components might not be recoverable. Perform a shutdown or reboot only **after** a firmware update has been completed.

NOTE When the PDUs are physically connected to the datacenter’s power receptacles and

> power is applied to the rack, all DataScale SN10-8R components begin to power on. These components' fans initially run at full speed but eventually ramp down once the BMCs finish their boot sequence. Power is not immediately applied to the rack components because the breakers on the PDUs are turned off. You must manually turn on these breakers to begin feeding power to the DataScale SN10-8R components.

6.2. Powering on the DataScale SN10-8R

IMPORTANT Power on the DataScale SN10-2 RDU modules before powering on the DataScale SN10-H host modules, as described in the following steps.

6.2.1. Task 1: Turn on the six circuit breakers for each PDU

Power is automatically applied to the DataScale SN10-8R components once the PDUs are plugged into the datacenter power and you close the circuit breakers. Figure 3 illustrates what a PDU circuit breaker group looks like (breaker switch 6 circled). Each PDU has a bank of three circuit breakers grouped together, and there are two groups on a PDU.

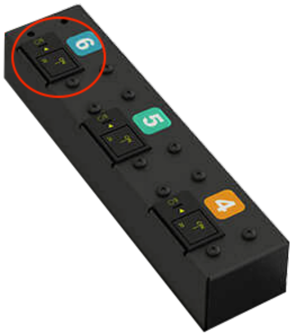


Figure 3. Circuit breakers on PDU

The DataScale SN10-H host modules and DataScale SN10-2 RDU modules boot into standby mode and wait to be manually powered on. The networking equipment in the rack does not go into standby mode; instead, it completely boots once power is established.

If power is provided to the networking components, but they are not powering on, see the product-specific documentation for how to power on the network device:

- Lantronix SLC8000 serial console server: https://cdn.lantronix.com/wp-content/uploads/pdf/SLC8000_UG.pdf
- Juniper EX4300 access switch (for the access network): https://www.juniper.net/documentation/product/en_US/ex4300
- Juniper QFX5200 Ethernet high-bandwidth data switch (for the data network): https://www.juniper.net/documentation/product/en_US/qfx5200
- Mellanox SB7800 IB high-bandwidth data switch (for the data network): https://docs.mellanox.com/category/mlnxos

6.2.2. Task 2: Power on the DataScale SN10-2 modules

Boot the DataScale SN10-2 RDU modules in the system using one of the following methods:

Option 1: Use SSH to connect to the SN10-2 BMC

1. From a system that has access to the DataScale SN10-8R access network:

    a. Open a terminal session

    b. Use the `ssh` command to securely connect to the first DataScale SN10-2 RDU module in each system. See the "*IP address assignments*" section of this document to get the IP address to connect to.

    Here’s an example for system 1 given IP address subnet 10.0.1.0/26 for the access network:

    ```
    $ ssh root@10.0.1.13
    root@10.0.1.5’s password: <Enter root password>
    root@xrdu:~#
    ```

    The first DataScale SN10-2 RDU module in each system is as follows:

    - System 1: SN10-2-1
    - System 2: SN10-2-5
    - System 3: SN10-2-9
    - System 4: SN10-2-13

2. Run the following `xrduutil` command to power on the system:

    ```
    root@xrdu:~# xrduutil -U root -P <root_password> poweron
    ```

3. To ensure that the DataScale SN10-2 RDU modules are up before you boot the DataScale SN10-H host module, run the following command to check the status of each of the DataScale SN10-2 RDU modules.

    ```
    root@xrdu:~# xrduutil -U root -P <root_password> powerstate
    Power is on for XRDU_0
    Power is on for XRDU_1
    Power is on for XRDU_2
    Power is on for XRDU_3
    ```

Option 2: Send a REST API call to the SN10-2 BMC

1. Generate a token (recommended).

    If you use the REST API, SambaNova recommends that you use token-based authentication so that plain-text passwords are not sent over the network for REST API commands. See Generating a secure API login token for details.

2. Run the REST API power-on command for each DataScale SN10-2 RDU module. Run this command for each DataScale SN10-2 RDU module in each of the nodes, in no particular order.

   Format:

   ```
   $ curl -b cjar -k -H "X-Auth-Token: $token" -X PUT -d
   '\{"data":"xyz.openbmc_project.State.Chassis.Transition.On"}' https://<SN10-
   2_BMC_IP>/xyz/openbmc_project/state/chassis0/attr/RequestedPowerTransition
   ```

   Example:

   ```
   $ curl -b cjar -k -H "X-Auth-Token: $token" -X PUT -d
   '\{"data":"xyz.openbmc_project.State.Chassis.Transition.On"}'
   https://10.0.1.21/xyz/openbmc_project/state/chassis0/attr/RequestedPowerTransi
   tion
   ```

3. To ensure the DataScale SN10-2 RDU modules are up before you boot the SN10-H, run the following command against each of the DataScale SN10-2 RDU modules:

   Format:

   ```
   $ curl -b cjar -k -H "X-Auth-Token: $token" https://<SN10-
   2_BMC_IP>/xyz/openbmc_project/state/chassis0
   ```

   Example:

   ```
   $ curl -b cjar -k -H "X-Auth-Token: $token"
   https://10.10.0.21/xyz/openbmc_project/state/chassis0
   ```

   Example output after an SN10-2 RDU module is powered on:

   ```
   {
   "data": {
   "CurrentPowerState": "xyz.openbmc_project.State.Chassis.PowerState.On",
   "LastStateChangeTime": 1591197275103,
   "POHCounter": 75,
   "RequestedPowerTransition": "xyz.openbmc_project.State.Chassis.Transition.On"
   },
   "message": "200 OK",
   "status": "ok"
   ```

```
}
```

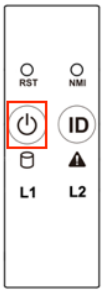
6.2.3. Task 3: Power the DataScale SN10-H host module

Boot the DataScale SN10-H host module using one of the following methods.

IMPORTANT	To ensure the DataScale SN10-H host module populates the system device tree properly, power on the host module only after the DataScale SN10-2 RDU modules are powered on fully.

Option 1: Mechanical power on

Power on the SN10-H host module by pressing the power button located on the front panel of the SN10-H. This panel is located on the front left side of the server.



Option 2: Power on via IPMI

Run the following command from a system that has `ipmitool` installed and has access to the SN10-H host module's BMC via the access network.

```
$ ipmitool -I lanplus -H <SN10-H_BMC_IP_Address> -U root -P <root password> power
on
```

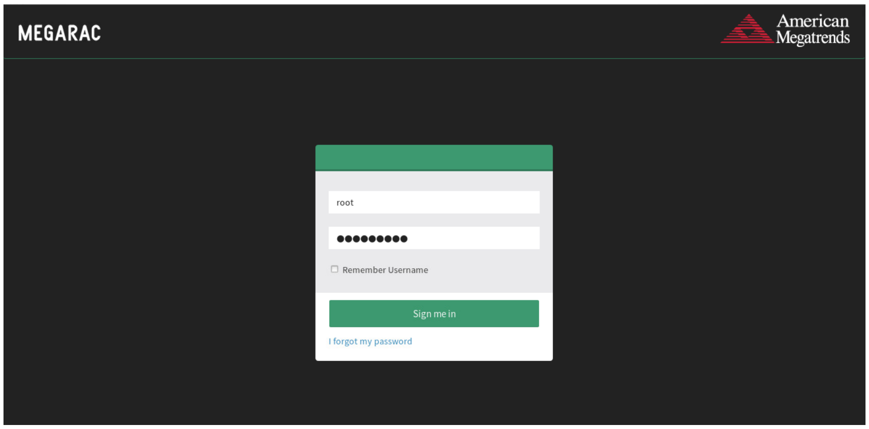
Option 3: Power on via WebUI

To power on via Web UI your system must meet the following requirements:

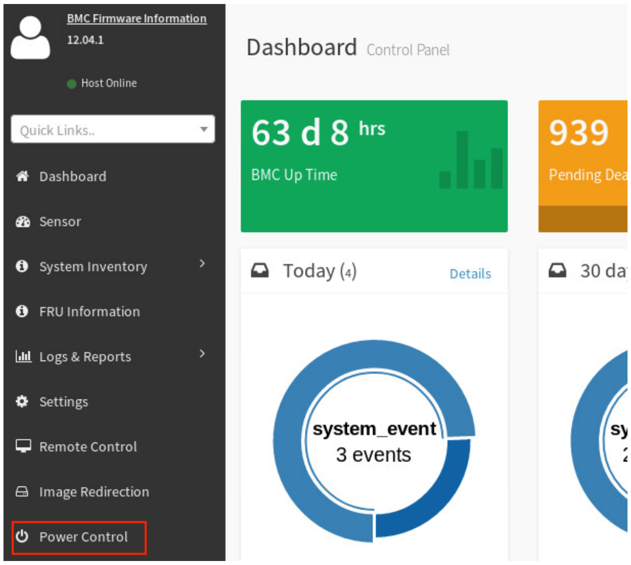
- Access to the DataScale SN10-H host module's BMC via the access network
- One of the following supported web browsers:
  - Chrome (latest version)
  - Firefox (latest version)

Follow these steps:

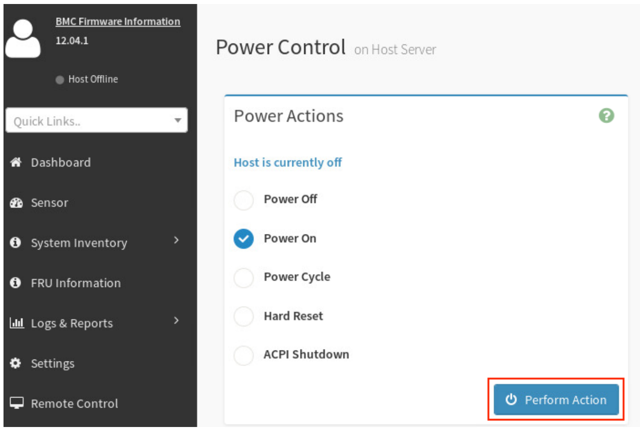
1. In the browser's address bar, enter the IP address of the SN10-H host module's BMC.
2. Log in to the management console by entering the user credentials.
3. Click **Sign me in**.



4. From the BMC dashboard, select **Power Control**.



5. Select the **Power On** checkbox, and then click **Perform Action**.



6. Perform this boot sequence for all nodes in the DataScale SN10-8R. The order in which you bring up the nodes does not matter.

6.3. Gracefully shutting down the DataScale SN10-8R

In order to shut down the DataScale SN10-8R, but not completely power off the entire rack, perform the following steps for each of the nodes in the DataScale SN10-8R rack.

6.3.1. Shut down the SN10-H host module in each system

Shut down the SN10-H host module in each system by using one of the following methods:

Option 1: Shut down from the OS

Log in to the node via `ssh` as `snuser1` and run the `shutdown` command.

```
$ ssh snuser1@<SN10-H_OS_IP_Address>
snuser1@SN10-H1’s password: <password>
$ sudo shutdown
```

This command does not shut down the system immediately but waits about a minute for users to save their work.

Option 2: Power off via IPMI

Run the following command from a system that has the following:

- Access to the SN10-H host module’s BMC via the access network
- The `ipmitool` installed

```
$ ipmitool -I lanplus -H <SN10-H_BMC_IP_Address> -U root -P <root password>
power off
```

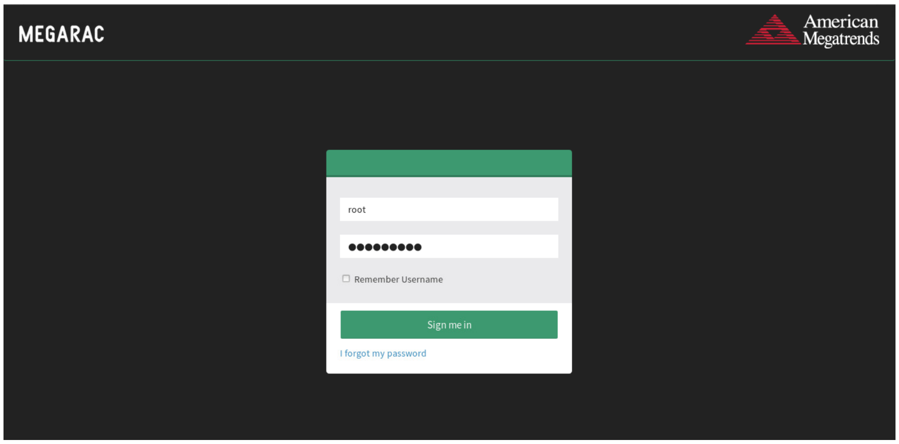
Option 3: Power off via Web UI

To power on via Web UI, your system must meet the following requirements:

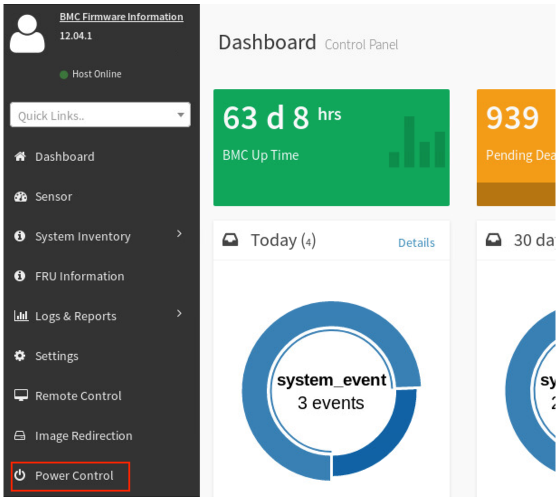
- Access to the DataScale SN10-H host module’s BMC via the access network
- One of the following supported web browsers:
  - Chrome (latest version)
  - Firefox (latest version)

Follow these steps:

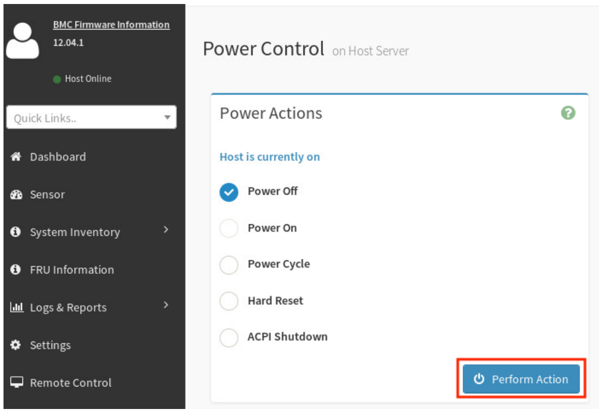
1. In the browser’s address bar, enter the IP address of the SN10-H host module’s BMC.
2. Log in to the management console by entering the user credentials.
3. Click **Sign me in**.



4. Select **Power Control** from the BMC dashboard.



5. Select the **Power Off** checkbox in the Power Actions screen and click **Perform Action**.



6.3.2. Shut down the DataScale SN10-2 RDU modules

Shut down the DataScale SN10-2 RDU modules in the node using one of the following methods:

Option 1: Use SSH to connect to the DataScale SN10-2 BMC

1. From a system that has access to the DataScale SN10-8R access network, open a terminal session and use `ssh` to connect to the first DataScale SN10-2 in each node.

   Example for system 1 given IP address subnet 10.0.1.0/26 for the access network:

   ```
   $ ssh root@10.0.1.13
   root@10.0.1.5’s password: <Enter root password>
   root@xrdu:~#
   ```

   See the "*IP address assignments*" section in this document to get the IP address.

   The first DataScale SN10-2 in each of the nodes is as follows:

   - System 1: SN10-2-1 (SN10-H-1-XRDU0)
   - System 2: SN10-2-5 (SN10-H-2-XRDU0)
   - System 1: SN10-2-9 (SN10-H-3-XRDU0)
   - System 2: SN10-2-13 (SN10-H-4-XRDU0)

2. Run the `xrduutil poweroff` command:

   ```
   root@xrdu:~# xrduutil -U root -P <root_password> poweroff
   ```

Option 2: Send a REST API call to the DataScale SN10-2 BMC

1. Generate a token (recommended).

   If you use the REST API, SambaNova recommends that you use token-based authentication so that plain-text passwords are not sent over the network for REST API commands. See Generating a secure API login token for details.

2. Run the REST API power-off command for each of the DataScale SN10-2 RDU modules in each of the systems.

   Format:

   ```
   $ curl -b cjar -k -H "X-Auth-Token: $token" -X PUT -d
   '\{"data":"xyz.openbmc_project.State.Chassis.Transition.Off"}' https://<SN10-
   2_BMC_IP>/xyz/openbmc_project/state/chassis0/attr/RequestedPowerTransition
   ```

   Example:

   ```
   $ curl -b cjar -k -H "X-Auth-Token: $token" -X PUT -d
   '\{"data":"xyz.openbmc_project.State.Chassis.Transition.Off"}'
   https://10.0.1.21/xyz/openbmc_project/state/chassis0/attr/RequestedPowerTransi
   tion
   ```

Run this command for each of the DataScale SN10-2 RDU modules in each of the systems.

3. Shut down the Mellanox SB7800 IB high-bandwidth data switch, the Lantronix SLC8000 serial console server, and the Juniper EX4300 access switch.

   When you power down the entire DataScale SN10-8R, shut down the Juniper EX4300 access switch last, because this switch controls the final access to the system via the network.

   See the following product-specific documentation for information on how to shut down each of these network devices:

   - Lantronix SLC8000 serial console server:
     https://cdn.lantronix.com/wp-content/uploads/pdf/SLC8000_UG.pdf
   - Juniper EX4300 access switch:
     https://www.juniper.net/documentation/product/en_US/ex4300
   - Juniper QFX5200 Ethernet high-bandwidth data switch (for the data network):
     https://www.juniper.net/documentation/product/en_US/qfx5200
   - Mellanox SB7800 IB high-bandwidth data switch:
     https://docs.mellanox.com/category/mlnxos

   NOTE After shutting down the Lantronix serial console server, the only method for powering this network device back on is to physically disconnect power to the device and then reconnect the power.

Chapter 7. Administrative tasks for the SN10-H host module

Administrative tasks differ depending on which supported OS you are running on each of the SN10-H host modules.

7.1. Supported versions of the SN10-H operating systems

The SN10-H host module supports the following OS versions:

- Red Hat Enterprise Linux 8.2
- Ubuntu Server 18.04.4 Long-Term Support (LTS)

7.2. Red Hat Enterprise Linux administration

7.2.1. General notes and warnings

WARNING Some third-party software and OS packages may prevent the SambaFlow software stack from functioning properly. In this case, SambaNova Support may require all non-certified third-party software or non-certified packages, including the package version, to be removed to get the DataScale SN10-H host module to a satisfactory state and to continue working on any support issues.

WARNING

DataScale SN10-H host modules are configured with a default login password for users `root` and `snuser1`. SambaNova highly recommends that you change these passwords immediately upon logging in to a DataScale SN10-H host module.

WARNING

SambaNova strongly recommends that you do not perform a major upgrade or a kernel update to the DataScale SN10-H host module OS without referring to the supported OS, kernel, and package versions noted within this document and the software release notes, because there are some strict packages dependencies the SambaNova software relies on. In general, SambaNova recommends that you do not perform any major updates unless you are directed to do so by SambaNova.

NOTE

Before performing package updates, see the SambaFlow software release notes to ensure there are no package dependencies that could break the SambaFlow software if the packages are not at the correct level.

7.2.2. Operating system licensing

SambaNova provides the needed package repositories for Red Hat Enterprise Linux running on the DataScale SN10-8R. A partnership with Red Hat allows SambaNova to distribute a customized repository for the DataScale SN10-8R. Adding other repositories might cause issues with the operation of the SambaFlow software because there are some package and kernel version dependencies.

If the SambaNova software stack has problems running, SambaNova Support might request that you remove any packages that were not included from the SambaNova Red Hat Enterprise Linux repository or that you downgrade certain packages to a version that was certified.

7.2.3. Logging in

To access the DataScale SN10-H host module:

1. Use `ssh` as user `snuser1` to log in to the DataScale SN10-H host module from a system that can access the DataScale SN10-8R access network
2. When you are prompted, enter the default password for `snuser1`. You can find default passwords in the "*Default username and passwords for components*" section of this document.

```
$ ssh snuser1@<SN10-H_OS_IP_Address>
snuser1@<SN10-H_OS_IP_Address>’s password: <Default Password>
```

NOTE

It is highly recommended that you change the default password for `root` and `snuser1`. To change the `snuser1` password from the default password to a more secure password, run the following command and enter the new password information when you are prompted:

```
$ passwd
Changing password for snuser1.
(current) UNIX password: <Current_Default_Password>
Enter new UNIX password: <New_Secure_Password>
Retype new UNIX password: <New_Secure_Password>
passwd: password updated successfully
```

7.2.4. Connecting to the SambaNova repository

DataScale SN10-H host module connectivity to the SambaNova repository is set up as part of the DataScale SN10-8R installation and relies on the site survey that your company completed before that step. As part of the initial installation, SambaNova provides a `sambanova.repo` file that contains the appropriate credentials and paths to your specific repository.

If you need to check the setup for the SambaNova OS repository, see KB article #1058.

7.2.5. Modifying the repository configuration file

WARNING

Do not modify the `sambanova.repo` repository file. Doing so may break SambaFlow software package dependencies, which might cause unrecoverable package dependency issues and could result in the need to rebuild the SN10-H host module. If you need any packages that are not provided by SambaNova, open a support case with SambaNova Support.

7.2.6. Updating the DataScale SN10-H host module OS

SambaNova patch releases handle major upgrades to the DataScale SN10-H host module OS (for example, going from RHEL 8.2 to RHEL 8.5 or later). SambaNova provides a release notes file that contains any special notes and information about the commands you need to run to perform the upgrade.

7.2.7. Updating the SambaFlow software

To update the SambaFlow software packages, log in to the DataScale SN10-H host module(s) where the software packages need to be updated.

To view what packages are installed on the DataScale SN10-H host module, run the following command:

```
$ rpm -qa | grep samba[nf]
```

To view which SambaFlow packages have an update you can apply, run the following command:

```
$ dnf check-update | grep samba[nf]
```

To update the SambaFlow packages, examine the list provided in the output produced by the `check-update` command, and then run the following command to update a package and any of its package dependencies:

```
$ sudo dnf update <package_name>
```

For example, if the output produced by the `check-update` command shows an update is available for the `sambanova-runtime` package, run the following command:

```
$ sudo dnf update sambanova-runtime
```

Repeat this step for each SambaFlow package that needs to be updated.

7.3. Ubuntu Linux Server administration

7.3.1. General notes and warnings

WARNING

Some third-party software and OS packages may prevent the SambaFlow software stack from functioning properly. In this case, SambaNova Support may require all non-certified third-party software or non-certified packages, including the package version, be removed to get the DataScale SN10-H host module to a satisfactory state and to continue to work on any support issues.

WARNING

DataScale SN10-H host modules are configured with a default login password for users `root` and `snuser1`. SambaNova recommends that you change these passwords immediately upon logging in to a DataScale SN10-H host module.

WARNING

SambaNova strongly recommends that you do not perform a major upgrade or a kernel update to the DataScale SN10-H host module OS without referring to the supported OS, kernel, or package versions noted within this document and the software release notes, because there are some strict dependencies that the SambaFlow software relies on. In general, SambaNova recommends that you do not perform any major updates unless you are directed to do so by SambaNova.

NOTE

Before performing package updates, see the SambaFlow software release notes to ensure there are no package dependencies that could break the SambaFlow software if the packages are not at the correct level.

7.3.2. Operating system licensing

SambaNova provides the package repositories for Ubuntu running on the DataScale SN10-8R. A partnership with Ubuntu allows SambaNova to distribute a customized repository for the DataScale SN10-8R. Adding other repositories might cause issues with the operation of the SambaFlow software because there are some package and kernel version dependencies.

If the SambaFlow software stack has problems running, SambaNova Support may request that you remove any packages that were not installed from the SambaNova Ubuntu repository or that you downgrade certain packages to a version that was certified.

7.3.3. Logging in

To access the DataScale SN10-H host module for the first time, from a system that can access the DataScale SN10-8R access network, use `ssh` as user `snuser1` to log in to the DataScale SN10-H host module.

When you are prompted, enter the default password for `snuser1`. You can find default passwords in the "*Default username and passwords for components*" section of this document.

```
$ ssh snuser1@<SN10-H_OS_IP_Address>
snuser1@<SN10-H_OS_IP_Address>’s password: <Default Password>
```

NOTE

SambaNova highly recommends that you change the default password for `root` and `snuser1`. To change the `snuser1` password from the default password to a more secure password, run the following command and enter the new password information when you are prompted:

```
$ passwd
Changing password for snuser1.
(current) UNIX password: <Current_Default_Password>
Enter new UNIX password: <New_Secure_Password>
Retype new UNIX password: <New_Secure_Password>
passwd: password updated successfully
```

7.3.4. Connecting to the SambaNova repository

DataScale SN10-H host module connectivity to the SambaNova repository is set up as part of the DataScale SN10-8R installation and relies on the site survey that was completed prior to that step. As part of the initial installation, a `sources.list` file under the `/etc/apt/` directory is provided, and the appropriate credentials for accessing your specific repository are configured in the `/etc/apt/auth.conf` file. If you need to check the setup for the SambaNova OS repository, see KB article #1057.

7.3.5. Modifying the repository configuration files

WARNING

Do not modify the `sources.list` repository file. Doing so may break SambaFlow software package dependencies, which might cause unrecoverable package dependency issues and could result in the need to rebuild the SN10-H host module. If you need any packages that are not provided by SambaNova, open a support case with SambaNova Support.

7.3.6. Updating the DataScale SN10-H host module OS

SambaNova patch releases handle major upgrades to the DataScale SN10-H host module OS (for example, going from 18.4 LTS to 20.04 LTS or kernel updates). A readme file contains any special notes and information about the commands to execute to perform the upgrade.

7.3.7. Updating the SambaFlow software

To update the SambaFlow software packages, log in to the DataScale SN10-H host module(s) where the software packages need to be updated.

To view what packages are installed on the DataScale SN10-H host module, run the following command:

```
$ dpkg -l | grep samba[nf]
```

To view which SambaNova packages have an update you can apply, run the following command:

```
$ apt list --upgradable | grep samba[nf]
```

To update all the packages that need to be updated, run the following command, which updates the packages and any package dependencies:

```
$ sudo apt install --only-upgrade samba[nf]
```

To update a specific package, replace `samba[nf]` with the name of a specific package. For example, to update `sambanova-runtime`, run the following command:

```
$ sudo apt install --only-upgrade sambanova-runtime
```

Chapter 8. Network device administration

For general configuration and maintenance of the network devices in the DataScale SN10-8R (data switch, access switch, and serial console server), see the administration documentation for the specific product:

- Lantronix SLC8000 serial console server:
  https://cdn.lantronix.com/wp-content/uploads/pdf/SLC8000_UG.pdf
- Juniper EX4300 access switch:
  https://www.juniper.net/documentation/product/en_US/ex4300
- Juniper QFX5200 Ethernet high-bandwidth data switch (for the data network):
  https://www.juniper.net/documentation/product/en_US/qfx5200

- Mellanox SB7800 IB high-bandwidth data switch: https://docs.mellanox.com/category/mlnxos

There should be minimal need to configure the serial console server and the Juniper access switch. The Mellanox IB high-bandwidth data switch is delivered with a minimal configuration of the ports and routing. Based on your site-specific requirements, you can configure this switch beyond its initial configuration. For port connection details, see the *DataScale SN10-8R Hardware Installation* document in the SambaNova documentation portal (https://docs.sambanova.ai).

NOTE

At first login, SambaNova highly recommends that you change the default passwords. Use the following commands to initiate a password change on specified devices, and follow the prompts to create a new, secure password:

Juniper EX4300 access switch and QFX5200 data switch:

```
$ ssh root@<Juniper_switch_IP_address>
root@:RE:0% cli
root> configure
root# set system root-authentication plain-text-password
```

Mellanox SB7800 IB high-bandwidth data switch:

```
$ ssh admin@<Mellanox_switch_IP_address>
> enable
# configure terminal
(config) # username admin password
```

Lantronix SLC8000 serial console server:

```
$ ssh sysadmin@<Lantronix_switch_IP_address>
> set localusers password sysadmin
```

SambaNova provides a quarterly patch release for these network devices, although there may not be any new updates for these devices in a give patch. You can download these patches from the SambaNova `ext-infra-patch` repository. See KB article #1062 "Listing and downloading available SN10-8R firmware" for details on acquiring the patch releases. Patch release notes explain any steps that differ from the standard steps described in the specific product administration documentation.

For details on saving the networking configurations, see the "*Backing up and restoring components*" section in this document, which lists the relevant KB articles.

NOTE

The Mellanox SB7800 IB high-bandwidth data switch has TCP port 1234 open because the Mellanox Unified Fabric Manager (UFM) software uses this port to communicate to UFM agents running on Mellanox switches. If you do not use UFM software in your datacenter and you would like to close this port, see KB article #1045 for details on how to filter this port on the Mellanox SB7800 IB high-bandwidth data switch.

Chapter 9. Administrative tasks for the baseboard management controller (BMC)

9.1. General notes and warnings

WARNING

Do not power off or reboot the DataScale SN10-8R components during firmware updates. Interrupting a firmware update may damage the DataScale SN10-8R components, and the damaged component might not be recoverable. Perform a shutdown or reboot only after a firmware update has been completed successfully.

NOTE

With the exception of updating the BMCs, collecting diagnostic material, or changing the log in credentials, most settings on the BMCs should remain static and should not need modification. Unless you are otherwise instructed, do not make configuration changes to the BMCs.

9.2. DataScale SN10-H host module administration

Administrative tasks for the DataScale SN10-H host module mainly involve the following:

- Updating the DataScale SN10-H host module BMC firmware
- Updating the DataScale SN10-H host module BIOS
- Recovering the DataScale SN10-H BMC
- Viewing diagnostic information and logs to debug a system in the event of a system component failure

WARNING

Do not remove the admin user account or change this account’s password. This account is needed for password recovery of the DataScale SN10-H host module’s BMC.

NOTE

If you start the update firmware process and you decide to cancel the process, you need to reset BMC. To do that, close the web browser that was logged in to the BMC WebUI, and then log in to the BMC WebUI again before attempting any administrative operations for the BMC.

Before you update the firmware, back up the existing configuration of the DataScale SN10-H host module. In some cases, having a backup helps with recovering the BMC.

To back up the existing configuration, your system must meet the following requirements:

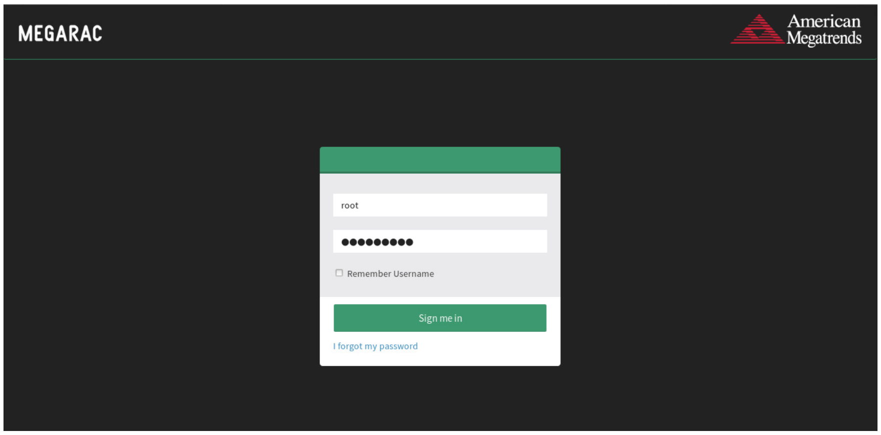
- Access to the DataScale SN10-H host module’s BMC via the access network.
- One of the following supported web browsers:

- Chrome (latest version)
- Firefox (latest version)

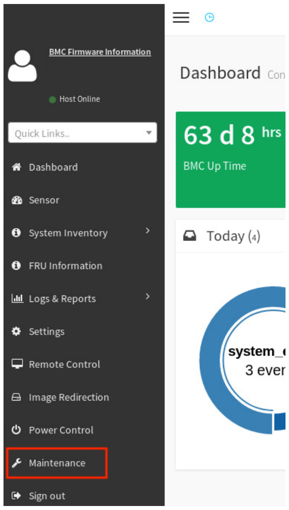
Preparing for update of the host module BMC firmware

Follow these steps:

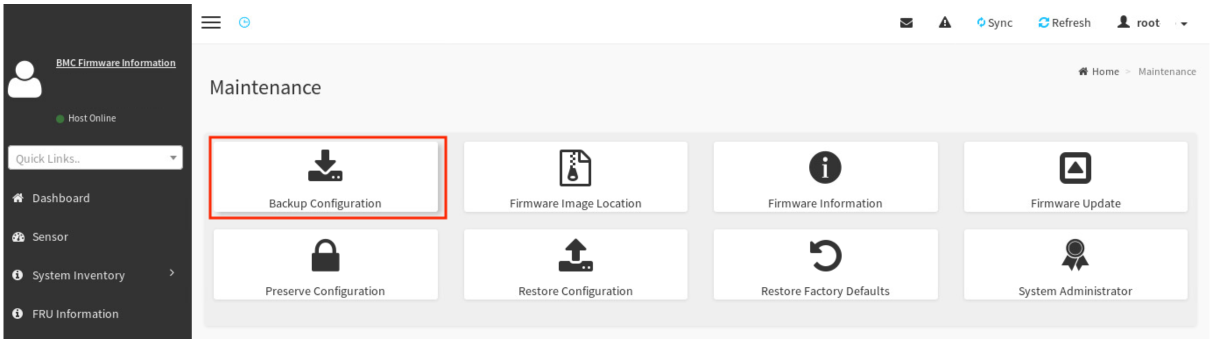
1. In the browser's address bar, enter the IP address of the DataScale SN10-H host module's BMC, and log in to the management console with your user credentials.
2. Click **Sign me in**.



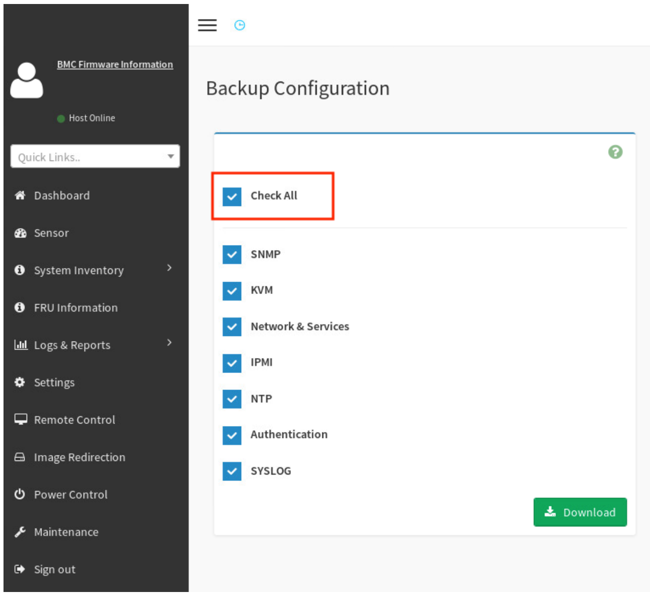
3. From the dashboard, select **Maintenance.**



4. In the Maintenance screen, select **Backup Configuration**.



5. In the Backup Configuration screen, select **Check All** to back up all the BMC configuration details.



Backup Configuration

☑ Check All

☑ SNMP

☑ KVM

☑ Network & Services

☑ IPMI

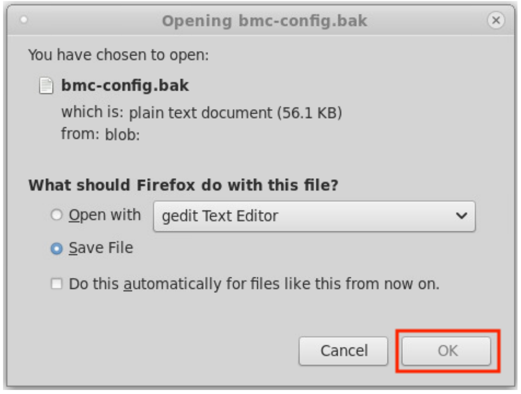
☑ NTP

☑ Authentication

☑ SYSLOG

6. Click **Download** to save this configuration to the local system that is the BMC through the Web UI.

7. Click **OK** to download the `bmc-config.bak` backup configuration file that you can use later if a restore is needed.



Opening bmc-config.bak

You have chosen to open:

bmc-config.bak

which is: plain text document (56.1 KB)
from: blob:

What should Firefox do with this file?

○ Open with gedit Text Editor

● Save File

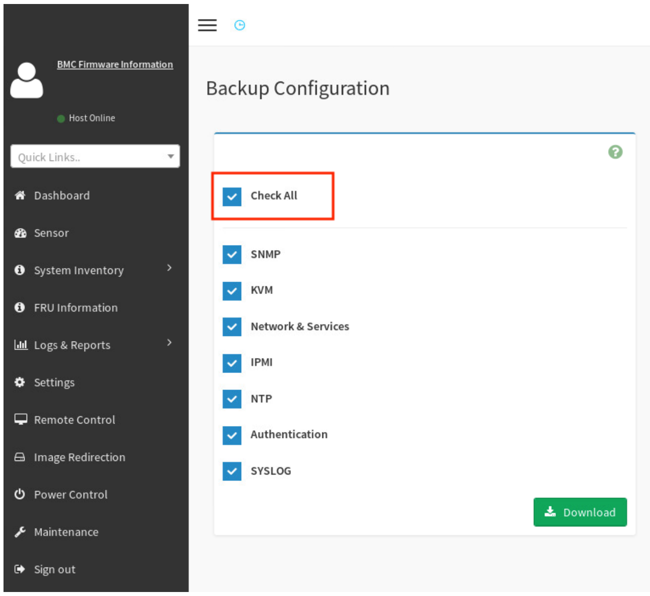
□ Do this automatically for files like this from now on.

Updating the DataScale SN10-2 BMC host module BMC firmware

When you have backed up the BMC configuration, you can update the SN10-H host module's BMC firmware while preserving the configuration.

To preserve the existing configuration, follow these steps:

1. Download the DataScale SN10-H host module’s BMC patch update from the SambaNova Support portal to the local system that is accessing the BMC Web UI.
2. Unzip the SambaNova patch update to a directory on the local system.
3. From the Backup Configuration screen, select **Maintenance** from the left pane.

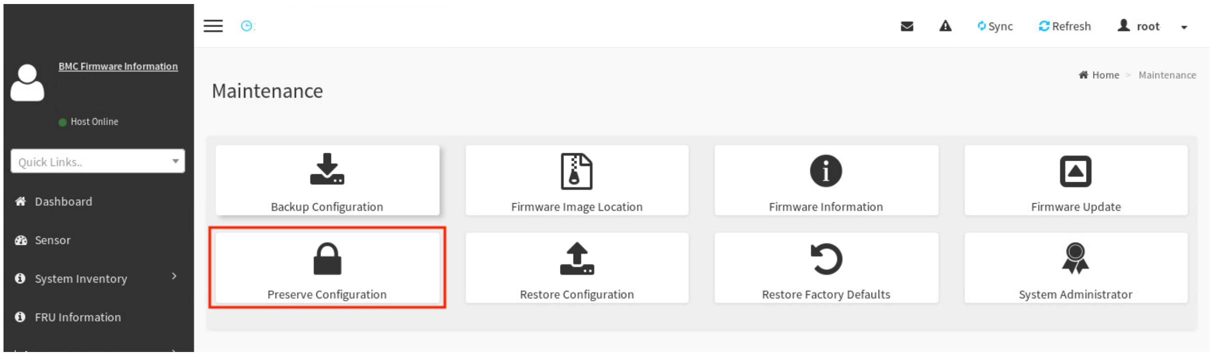


Backup Configuration

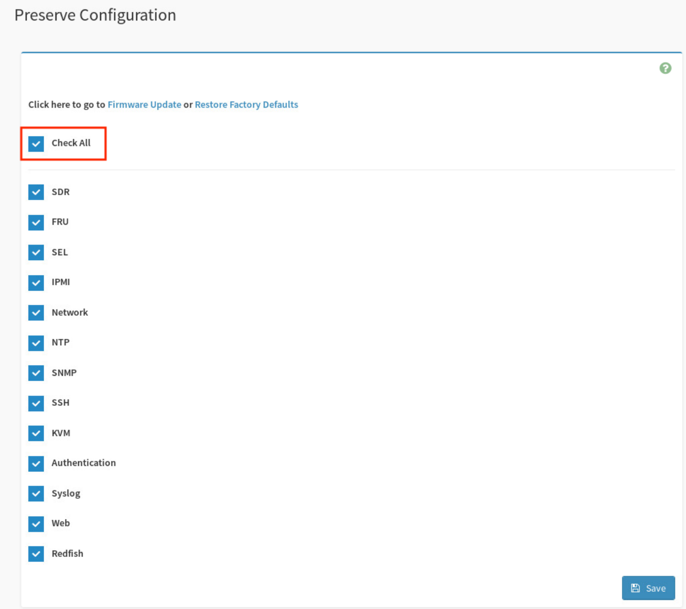
☑ Check All

☑ SNMP
☑ KVM
☑ Network & Services
☑ IPMI
☑ NTP
☑ Authentication
☑ SYSLOG

4. From the Maintenance screen, select **Preserve Configuration**.



5. Select **Check All** at the top of the list to preserve the configuration of everything.



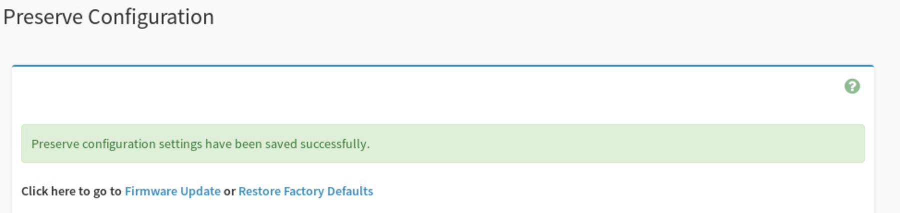
Preserve Configuration

Click here to go to Firmware Update or Restore Factory Defaults

☑ Check All

☑ SDR
☑ FRU
☑ SEL
☑ IPMI
☑ Network
☑ NTP
☑ SNMP
☑ SSH
☑ KVM
☑ Authentication
☑ Syslog
☑ Web
☑ Redfish

6. The following message appears if the configuration preservation was successful.



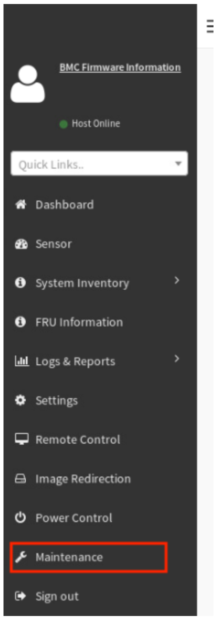
Preserve Configuration

Preserve configuration settings have been saved successfully.

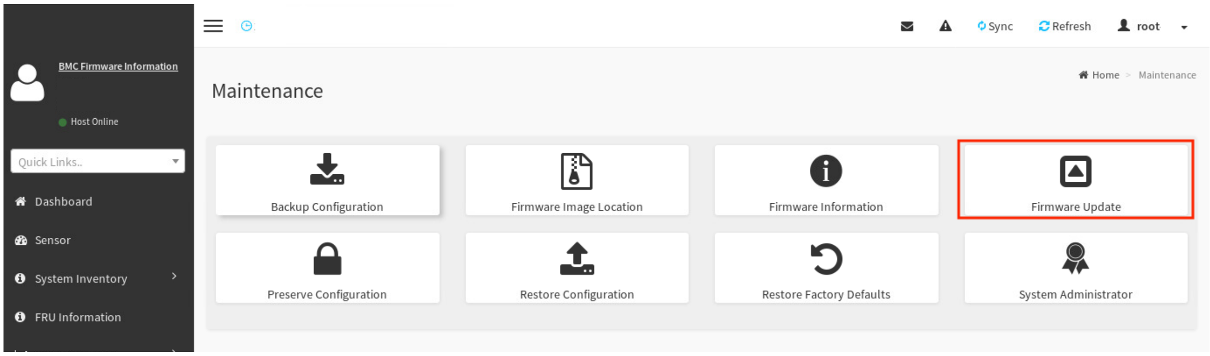
Click here to go to Firmware Update or Restore Factory Defaults

After configuration preservation is successful, follow these steps to update the firmware:

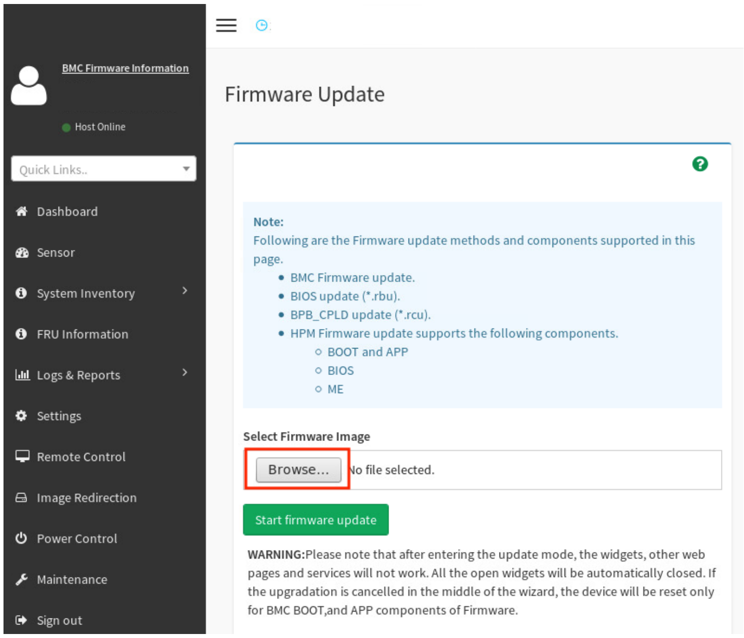
1. In the left pane, click **Maintenance**.



2. In the Maintenance screen, select **Firmware Update**.



3. In the Firmware Update screen, click **Browse**.



Note:
Following are the Firmware update methods and components supported in this page.

- BMC Firmware update.
- BIOS update (*.rbu).
- BPB_CPLD update (*.rcu).
- HPM Firmware update supports the following components.
    - BOOT and APP
    - BIOS
    - ME

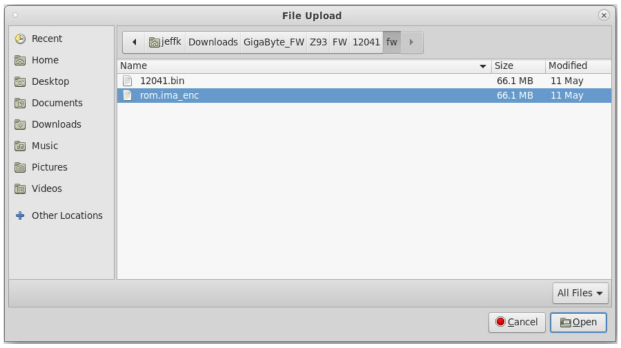
Select Firmware Image

Browse... No file selected.

Start firmware update

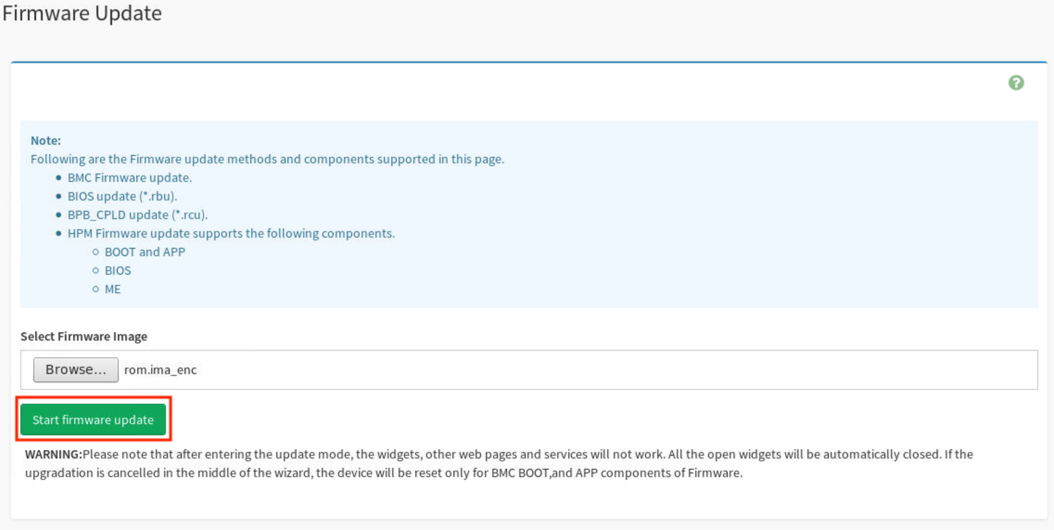
WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

4. Navigate to the `.bin` file that you downloaded and unzipped erlier. This file is in the `/SN10-8R/<version>/HostBMC_FW/` directory of the unzipped patch bundle. Select the `rom.ima_enc` file and click **Open**.



Name	Size	Modified
12041.bin	66.1 MB	11 May
rom.ima_enc	66.1 MB	11 May

5. Back in the Firmware Update screen, click **Start firmware update**.



Firmware Update

Note:
Following are the Firmware update methods and components supported in this page.

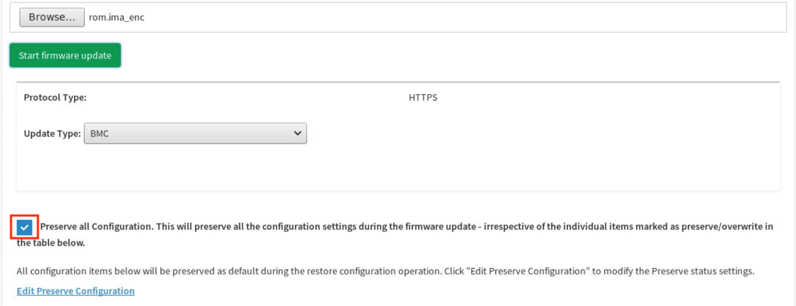
- BMC Firmware update.
- BIOS update (*.rbu).
- BPB_CPLD update (*.rcu).
- HPM Firmware update supports the following components.
  - BOOT and APP
  - BIOS
  - ME

Select Firmware Image

Browse... rom.ima_enc

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

6. The screen is expanded below the button that you just clicked. Select the **Preserve all Configuration** checkbox to use the preserved configuration you saved earlier.



Browse... rom.ima_enc

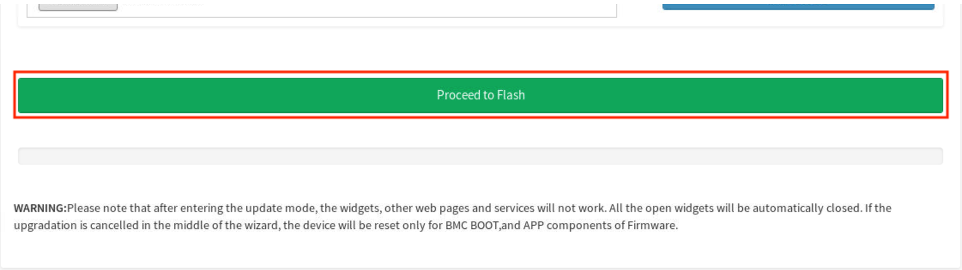
Protocol Type: HTTPS

Update Type: BMC

☑ **Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.**

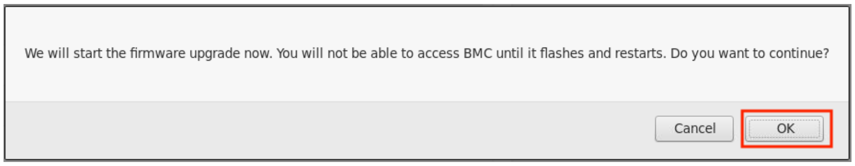
All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

7. Scroll to the bottom of the screen and click **Proceed to Flash**.



WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

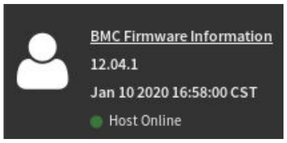
8. Click **OK** in the BMC update confirmation screen.



We will start the firmware upgrade now. You will not be able to access BMC until it flashes and restarts. Do you want to continue?

After the BMC update process has started, the BMC is not reachable for 5 to 10 minutes while the update is being applied. The DataScale SN10-H host module OS continues to run normally during the BMC update.

After 10 minutes, log in to the BMC Web UI and confirm that the update was successful by checking the information in the upper left side of the dashboard. The BMC firmware version is identified as <XX.XX.X>.



BMC Firmware Information

12.04.1

Jan 10 2020 16:58:00 CST

● Host Online

9.2.1. Updating the DataScale SN10-H host module BIOS

WARNING After you enter update mode, the widgets and other web pages and services will not work. All the open widgets are automatically closed. If you cancel the upgrade in the middle of the process, the SN10-H host module are reset only for the BMC BOOT and APP components of the firmware. Therefore, ensure the update process is not interrupted.

NOTE The SN10-H host module BIOS update requires a reboot of the system to apply the updated BIOS. Plan accordingly.

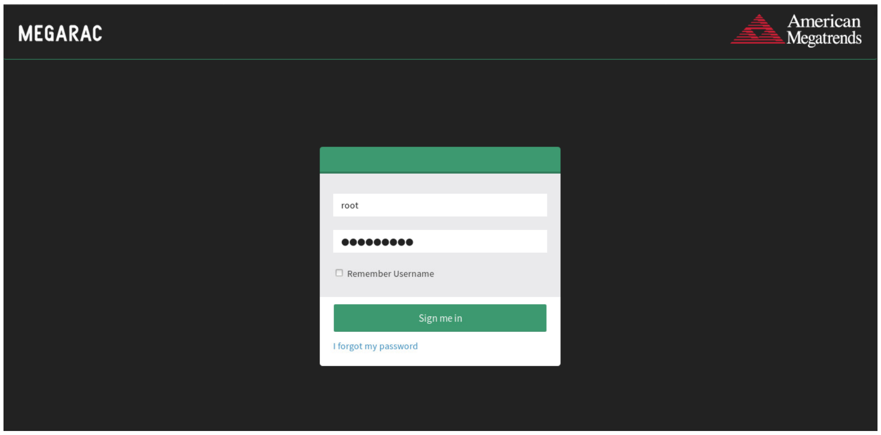
To update the SN10-H host module BIOS, your system must meet the following requirements:

- Access to the DataScale SN10-H host module's BMC via the access network
- One of the following supported web browsers:
  - Chrome (latest version)
  - Firefox (latest version)

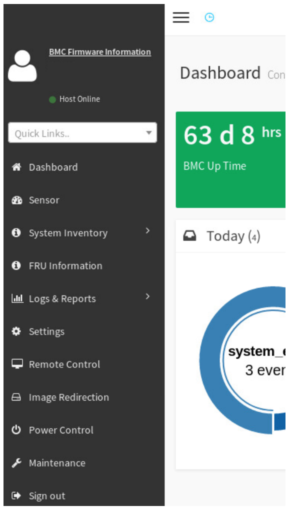
You will first perform the BIOS update, and then update the OS. Follow these steps:

Performing the SN10-H BIOS update

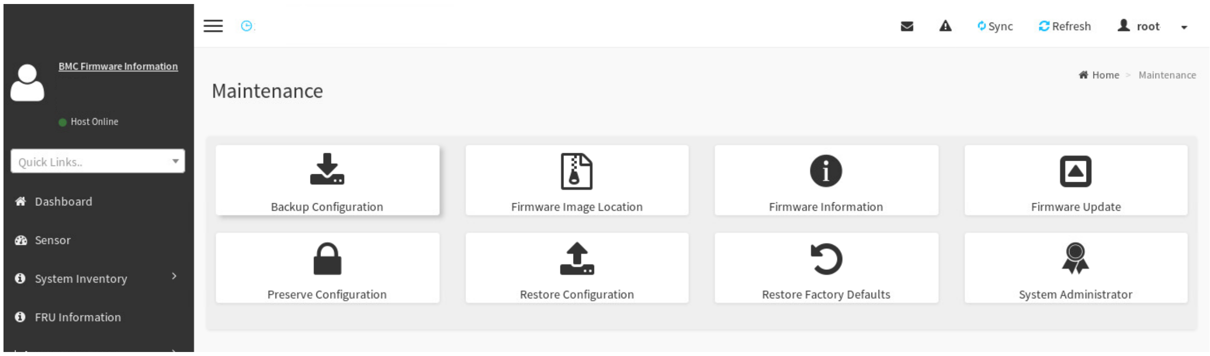
1. In the browser's address bar, enter the IP address of the DataScale SN10-H host module's BMC, and log in to the management console with your user credentials.
2. Click **Sign me in**.



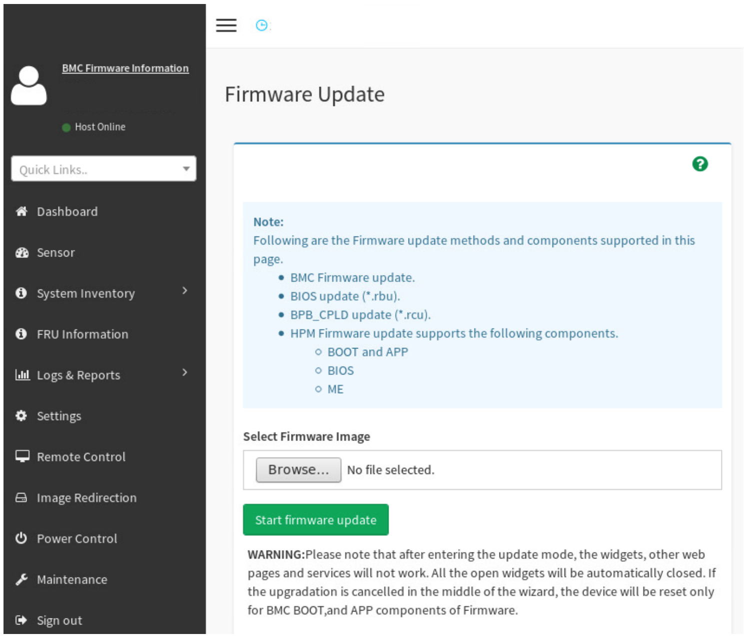
3. In the dashboard, select **Maintenance**.



4. In the Maintenance screen, select **Firmware Update**.



5. In the Firmware Update screen, click **Browse**.



Note:
Following are the Firmware update methods and components supported in this page.

- BMC Firmware update.
- BIOS update (*.rbu).
- BPB_CPLD update (*.rcu).
- HPM Firmware update supports the following components.
  - BOOT and APP
  - BIOS
  - ME

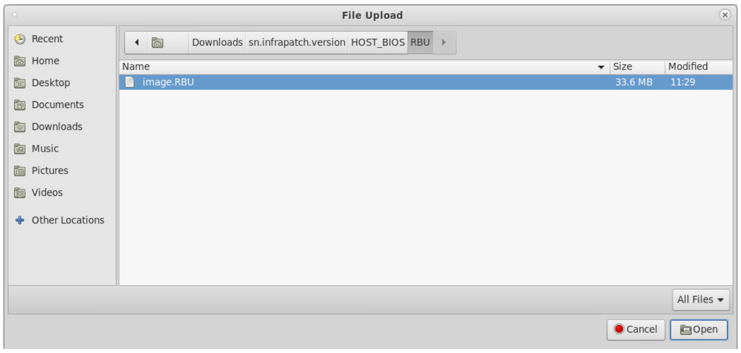
Select Firmware Image

Browse... No file selected.

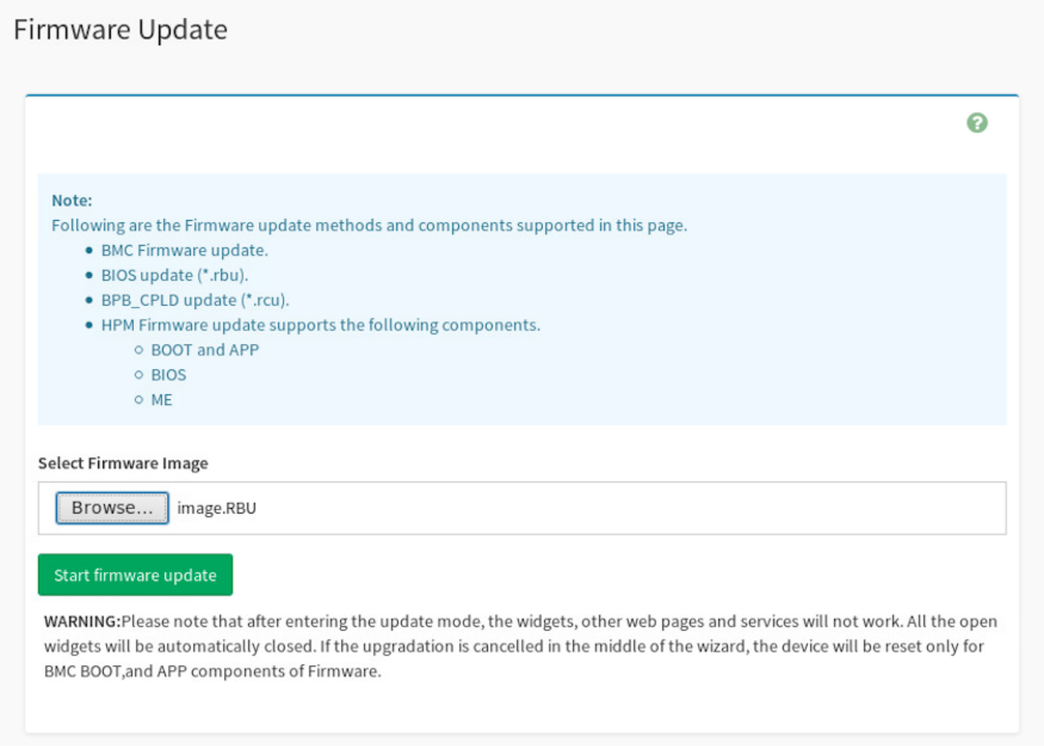
Start firmware update

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

6. Navigate to the `image.RBU` file that you downloaded and uncompressed earlier, select the file, and click **Open**. The file is located in the `/Host_BIOS/RBU/` directory of the uncompressed infrastructure patch bundle.



7. Back in the Firmware Update screen, click **Start firmware update**.



Firmware Update

Note:
Following are the Firmware update methods and components supported in this page.

- BMC Firmware update.
- BIOS update (*.rbu).
- BPB_CPLD update (*.rcu).
- HPM Firmware update supports the following components.
  - BOOT and APP
  - BIOS
  - ME

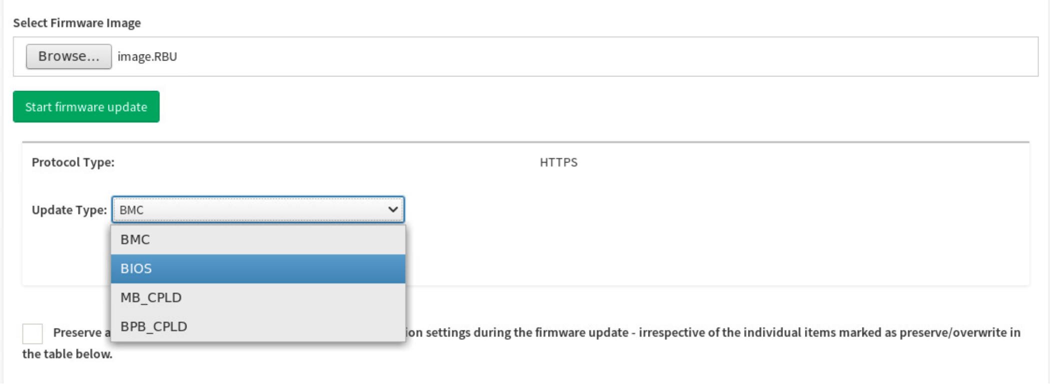
Select Firmware Image

Browse... image.RBU

Start firmware update

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

8. The screen is expanded below the button you clicked. From the **Update Type** drop-down, select **BIOS**.



Select Firmware Image

Browse... image.RBU

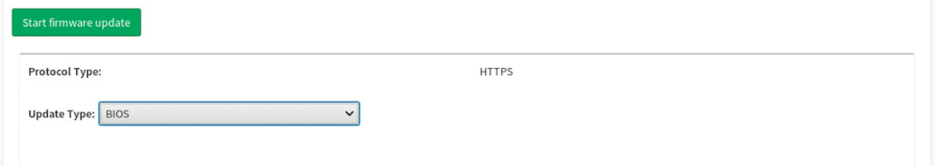
Start firmware update

Protocol Type: HTTPS

Update Type: BMC

□ **Preserve a** **ion settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.**

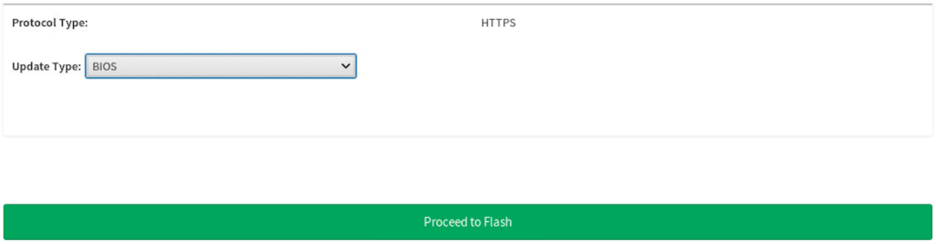
The **Update Type** drop-down shows that **BIOS** is selected.



Protocol Type: HTTPS

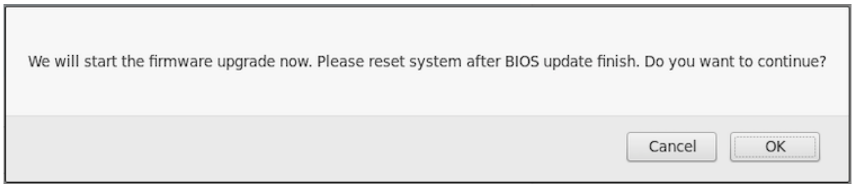
Update Type: BIOS

9. Click **Proceed to Flash**.


Protocol Type: HTTPS

Update Type: BIOS

10. Click **OK** in the firmware upgrade confirmation screen.


We will start the firmware upgrade now. Please reset system after BIOS update finish. Do you want to continue?

This initiates uploading the BIOS firmware update to the DataSale SN10-H host module, but it does not automatically apply the firmware update.

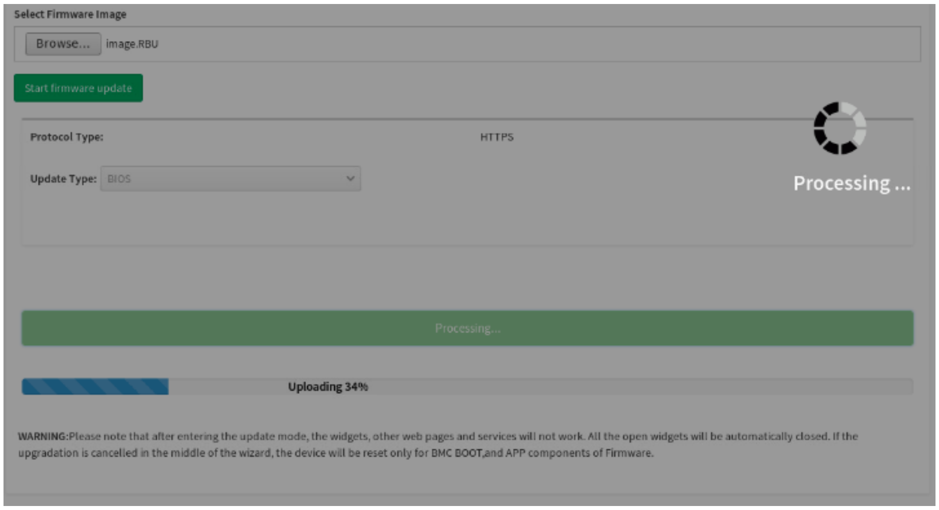

Select Firmware Image

image.RBU

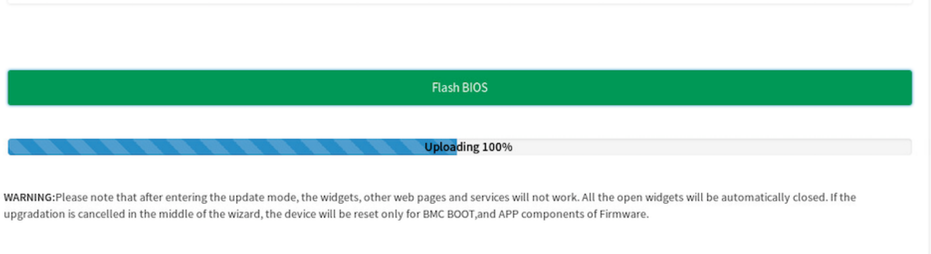
Protocol Type: HTTPS

Update Type: BIOS

Uploading 34%

WARNING:Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

11. When the screen shows **Uploading 100%**, click the **Flash BIOS** button.


Uploading 100%

WARNING:Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

This initiates the BIOS update process.

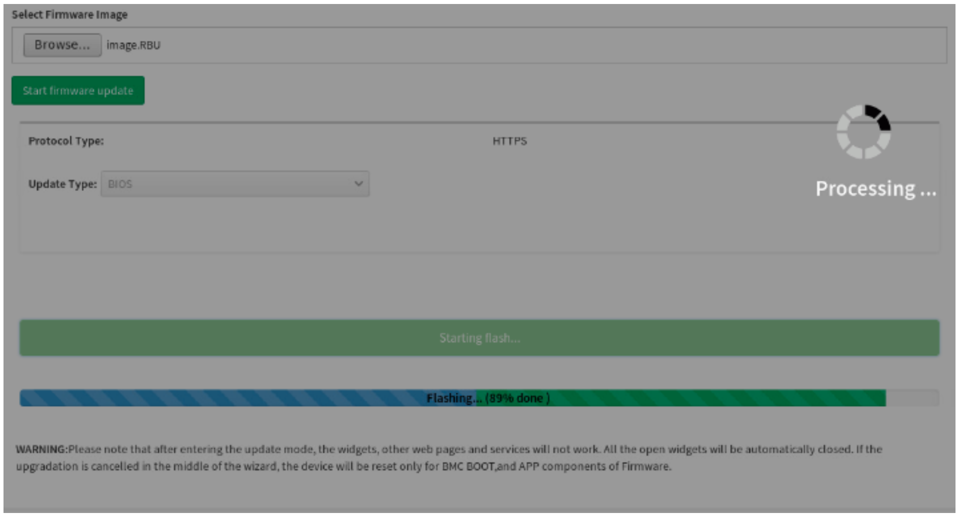


image.RBU

Protocol Type: HTTPS

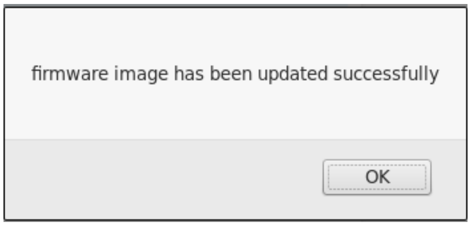
Update Type: BIOS

Starting flash...

Flashing... (89% done)

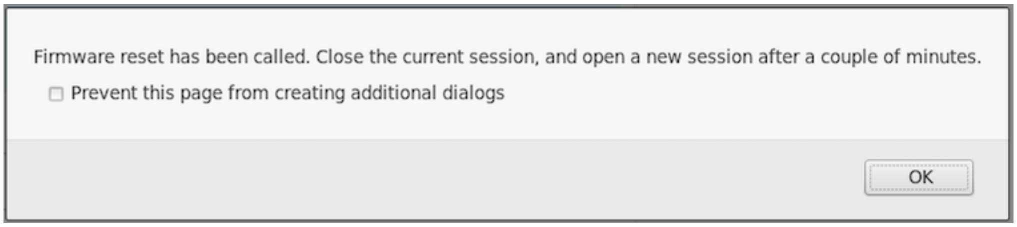
WARNING:Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

12. When the flash process is complete, a **firmware image has been updated successfully** message appears. Click **OK** to continue.



firmware image has been updated successfully

13. Another message appears stating that the firmware reset has been called. Click **OK** to log out of the SN10-H BMC Web UI.



Firmware reset has been called. Close the current session, and open a new session after a couple of minutes.

☐ Prevent this page from creating additional dialogs

Resetting the SN10-H OS

As a final step, you reset the SN10-H OS to complete the BIOS update.

1. After you are logged out of the SN10-H BMC, log in to the SN10-H OS.

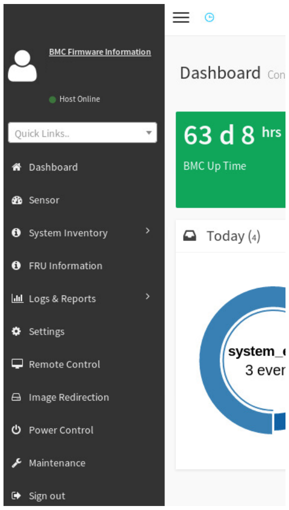
```
$ ssh snuser1@<SN10-H_OS_IP_Address>
snuser1@<SN10-H_OS_IP_Address>'s password: <snuser1 Password>
```

2. Reset the SN10-H OS to complete the BIOS update.

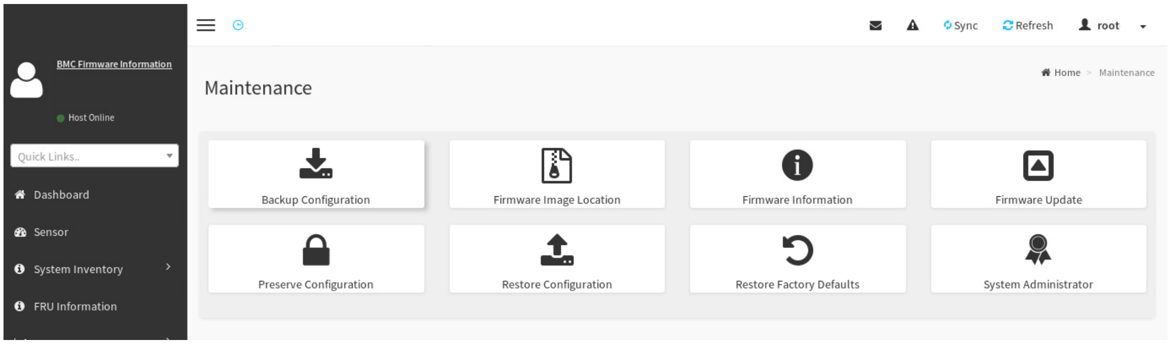
```
$ sudo shutdown -r now
[sudo] password for snuser1: <snuser1 Password>
```

3. After the SN10-H host module is back online, log in to the SN10-H BMC and confirm that the BIOS update has been applied. To do this:

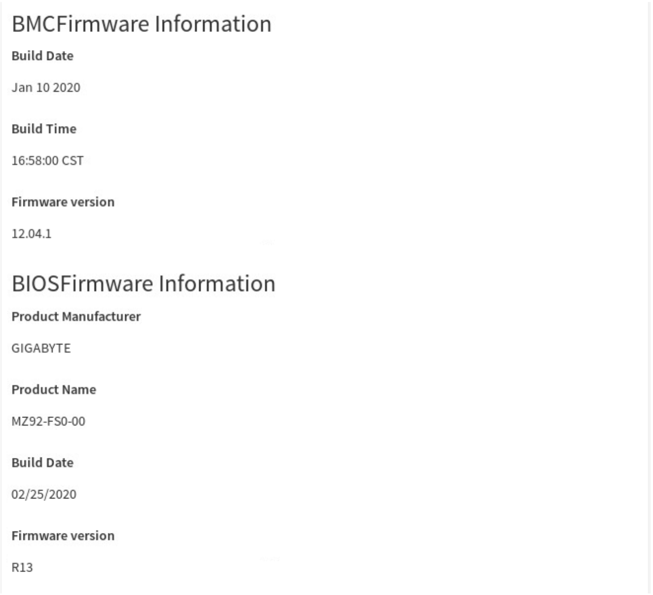
   a. Select **Maintenance** from the left pane of the dashboard.



   b. From the Maintenance screen, select **Firmware Information**.



   c. On the **BMCFirmware Information** screen, check the firmware version under **BIOSFirmware Information**.



BMCFirmware Information

Build Date

Jan 10 2020

Build Time

16:58:00 CST

Firmware version

12.04.1

BIOSFirmware Information

Product Manufacturer

GIGABYTE

Product Name

MZ92-FS0-00

Build Date

02/25/2020

Firmware version

R13

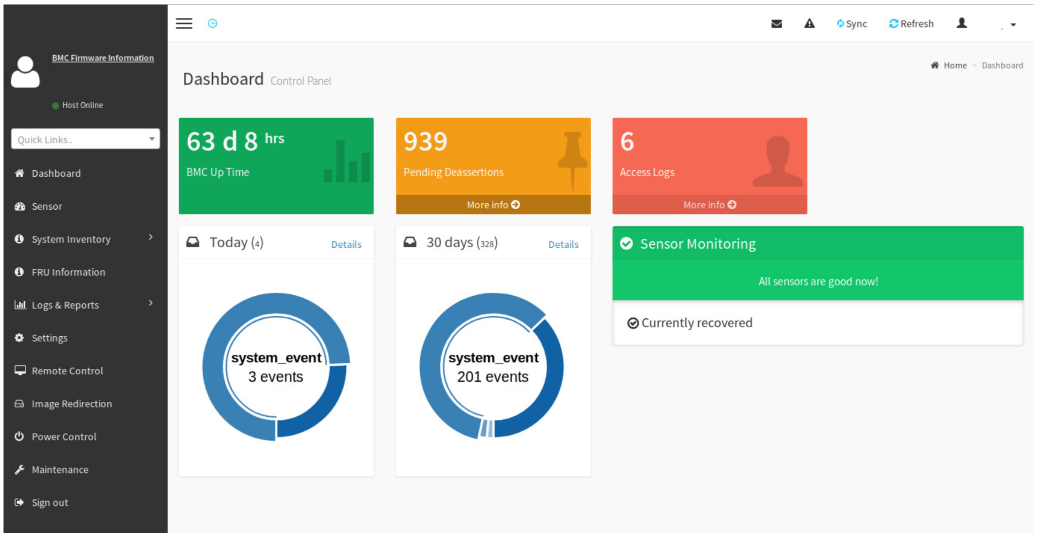
9.2.2. Recovering the DataScale SN10-H BMC

If the DataScale SN10-H host module’s BMC is no longer responding or no longer accessible, or the DataScale SN10-H host module’s BMC password has been lost or forgotten, see the "*Backing up and restoring components*" section in this document.

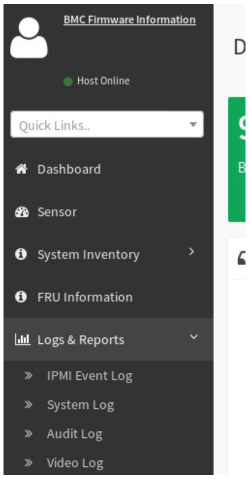
9.2.3. Viewing SN10-H BMC diagnostic information and logs

You can quickly identify a system’s status and view diagnostic information and logs for the DataScale SN10-H BMC from the Web UI.

1. Log in to the BMC’s Web UI and view the BMC dashboard.
2. Click the **More info** link in each box for details on logs and pending events/deassertions.



3. Click **Logs & Reports** in the left pane and select a sub-item to find more logs and reports.



See KB article #1039, “Diagnostic Data Collection Tool(samba_diag),” in the SambaNova Support portal (https://support.sambanova.ai) for details on:

- Diagnosing a DataScale SN10-H host module’s BMC specifically.
- Diagnosing the DataScale SN10-H host module.
- Collecting the required diagnostic and log material.

9.3. DataScale SN10-2 RDU module administration tasks

Administrative tasks for the DataScale SN10-2 RDU module’s BMC include the following:

- Updating the DataScale SN10-2 BMC and RDU controller (RDU-C) firmware
- Changing the root password
- Generating a secure API login token for authentication
- Configuring the DataScale SN10-2 BMC network
- Configuring the DataScale SN10-2 BMC hostname
- Viewing diagnostic information and logs to debug the system in the event of a system component failure

NOTE There is a built-in secure account on the DataScale SN10-2 BMC called `snservice`. It is used for password recovery of root if the password is forgotten. For more details on this account, see KB article #1049.

9.3.1. Updating the DataScale SN10-2 BMC and RDU controller (RDU-C) firmware

Updating the BMC and RDU-C firmware consistes of several tasks:

- Preparing for update
- Updating the DataScale SN10-2 BMC primary partition
- Updating the DataScale SN10-2 BMC secondary/recovery partition

- Updating the DataScale SN10-2 RDU-C primary partition
- Updating the DataScale SN30-2 RDU-C secondary/recovery partition

Preparing for update

Before you can start the update, you have to prepare, as follows:

1. Shut down the DataScale SN10-H host module in the system to ensure that no graphs or any other load are running. See the Gracefully shutting down the DataScale SN10-8R procedure.
2. Shut down the DataScale SN10-2 RDU module. See the Gracefully shutting down the DataScale SN10-8R procedure.
3. Log in to the DataScale SN10-2 BMC and reboot the BMC to clear the BMC registers, as follows:

   ```
   $ ssh root@<SN10-2_BMC_IP_Address>
   Password: <Enter root password>

   root@xrdu:~# reboot
   ```

   The reboot process takes about 3-5 minutes to complete. Meanwhile, you can go to the next step to download the DataScale SN10-2 firmware update.

4. Download the DataScale SN10-2 firmware update file `sn-xrdu-sys-fw-v<version_number>.tar.gz` from the SambaNova `ext-xrdu-fw` repository, under the `/latest` subdirectory, to a system that has access to the network that the DataScale SN10-2 BMC is on. See KB Article #1063 Listing and Downloading Available SN10-8R Firmware.
5. Uncompress the `sn-xrdu-sys-fw-v<version_number>.tar.gz` file.
6. Copy the `.mtd` and `.mtd.md5` firmware files from the `rdu-128` directory to each of the DataScale SN10-2 BMCs that are to be updated. Place these files under the `/dev/shm/` directory on the SN10-2.

   ```
   $ scp /<uncompressed directory>/rdu-128/obmc-rdu-<version>* root@<SN10-
   2_BMC_IP_Address>:/dev/shm/
   Password: <Enter root password>
   ```

   Confirm that the `.mtd` and `.mtd.md5` files have been completely transferred to the BMC’s `/dev/shm/` directory.

   NOTE Ensure that the files copied over are from the `rdu-128` directory and not the `rdu-64` directory.

Updating the DataScale SN10-2 BMC primary partition

1. After the files are in the BMC’s `dev/shm` partition, log in to the DataScale SN10-2 BMC.

   ```
   $ ssh root@<SN10-2_BMC_IP_Address>
   ```

```
Password: <Enter root password>

root@xrdu:~# cd /dev/shm/
```

2. Confirm that the following files are located in this directory:

    - obmc-rdu-<version>.mtd
    - obmc-rdu-<version>.mtd.md5

```
root@xrdu:/dev/shm# ls obmc*
obmc-rdu-<version>.mtd  obmc-rdu-<version>.mtd.md5
```

3. Run the update on the `obmc-rdu-<version>.mtd` firmware file.

```
root@xrdu:~# obmcupdate -p primary -t bmc -f /dev/shm/obmc-rdu-<version>.mtd
```

   Do not run any other commands or disconnect the power supply at this time.

4. Confirm that the Erasing, Writing, and Verifying stages complete to 100%.
5. When all stages are completed, reboot the BMC with the new firmware.

```
root@xrdu:~# reboot -f
```

6. After about 3 to 5 minutes, log back into the DataScale SN10-2 BMC.

```
$ ssh root@<SN10-2_BMC_IP_Address>
Password: <Enter root password>
```

NOTE The update re-images the DataScale SN10-2 BMC and so the .ssh identification will likely have changed, and may be prompted to remove the old host entry in the `.ssh/known_hosts` file on the client that was used to ssh into the system before.

7. Run the `obmcupdate -i` command to confirm that the update has been successful and the DataScale SN10-2 BMC firmware patch has been applied:

```
root@xrdu:~# obmcupdate -i
***** RDU-C *****
RDU-C Release Version: <current version>
RDU-C BuildDate: #.## ####   DesignVer: ##   BoardID: ##
***** BMC *****
BMC Release Version: <updated version>
BMC BUILD ID: <updated BMC buildid>
BMC Flash: Primary
BMC Flash Size: 128MB
```

8. If there are any issues running the update, re-attempt step 9 once more. If the update process continues to fail, contact SambaNova support.

Updating the DataScale SN10-2 BMC secondary/recovery partition

The re-imaging of the BMC will have removed the `obmc-rdu-<version>.mtd` and `obmc-rdu-<version>.mtd.md5` files from `/dev/shm/`. You have to copy them back, as follows:

1. Exit out of the SN10-2 BMC.
2. Log back in to the client system where the BMC firmware files were uncompressed, and copy the `obmc-rdu-<version>.mtd` and `obmc-rdu-<version>.mtd.md5` firmware files back to the DataScale SN10-2 BMCs `/dev/shm/` directory.

```
$ scp /<uncompressed directory>/rdu-128/obmc-rdu-<version>* root@<SN10-
2_BMC_IP_Address>:/dev/shm/
Password: <Enter SN10-2 BMC root password>
```

3. Confirm these two files have been completely transferred to the BMC’s /dev/shm/ directory.

NOTE Ensure that the files copied over are from the rdu-128 directory and not the rdu-64 directory.

4. Log back in to the DataScale SN10-2 BMC that was just updated:

```
$ ssh root@<SN10-2_BMC_IP_Address>
Password: <Enter root password>
```

5. Go to the `/dev/shm/` directory on the DataScale SN10-2 BMC.

```
root@xrdu:~# cd /dev/shm/
```

6. Confirm that the following two files are located in this directory:
   - obmc-rdu-<version>.mtd
   - obmc-rdu-<version>.mtd.md5

```
root@xrdu:/dev/shm# ls obmc*
obmc-rdu-<version>.mtd  obmc-rdu-<version>.mtd.md5
```

7. Run the update on the BMC recovery partition using the `obmc-rdu-<version>.mtd` firmware file.

```
root@xrdu:~# obmcupdate -p recovery -t bmc -f /dev/shm/obmc-rdu-<version>.mtd
```

Do not run any other commands at this time or disconnect the power supply.

8. Confirm that the Erasing, Writing, and Verifying stages complete to 100%.
9. If there are any issues running the update, attempt run the `obmcupdate` command again. If the update process continues to fail, contact SambaNova support.

Once completed, move onto updating the DataScale SN10-2 RDU Controller (RDU-C) primary partition.

Updating the DataScale SN10-2 RDU-C primary partition

When secondary partition update has been completed, move on to updating the DataScale SN10-2 RDU Controller (RDU-C) primary partition.

1. Exit out of the SN10-2 BMC and log back in to the client system where the BMC and RDU-C firmware files were uncompressed.
2. Copy the `rduc-<version>-primary.spi`, `rduc-<version>-primary.spi.md5`, `rduc-<version>-recovery.spi`, and `rduc-<version>-recovery.spi.md5` firmware files to the DataScale SN10-2 BMCs `/dev/shm/` directory.

   ```
   $ scp /<uncompressed directory>/rduc/rduc-<version>-* root@<SN10-
   2_BMC_IP_Address>:/dev/shm/
   Password: <Enter SN10-2 BMC root password>
   ```

3. Log onto the DataScale SN10-2 BMC where the update files were transferred to.

   ```
   $ ssh root@<SN10-2_BMC_IP_Address>
   Password: <Enter root password>
   ```

4. Go to the /dev/shm/ directory on the DataScale SN10-2 BMC.

   ```
   root@xrdu:~# cd /dev/shm/
   ```

5. Confirm that the following files are located in this directory:
   - `rduc-<version>-primary.spi`
   - `rduc-<version>-primary.spi.md5`
   - `rduc-<version>-recovery.spi`
   - `rduc-<version>-recovery.spi.md5`

   ```
   root@xrdu:/dev/shm# ls rduc*
   ```

```
rduc-<version>-primary.spi  rduc-<version>-primary.spi.md5  rduc-<version>-
recovery.spi
rduc-<version>-recovery.spi.md5
```

6. Run the update using the `primary.spi` firmware file to update the DataScale SN10-2 RDU-C primary partition.

   ```
   root@xrdu:/dev/shm# obmcupdate -p primary -t rduc -f /dev/shm/rduc-<version>-
   primary.spi
   ```

   Do not run any other commands at this time or disconnect the power supply.

7. Confirm that the update of the RDU-C has taken affect by running the `"obmcupdate -i"` command.

   ```
   root@xrdu:~# obmcupdate -i
   ***** RDU-C *****
   RDU-C Release Version: <updated version>
   RDU-C BuildDate: #.## ####   DesignVer: ##   BoardID: ##
   ***** BMC *****
   BMC Release Version: <updated version>
   BMC BUILD ID: <updated build id>
   BMC Flash: Primary
   BMC Flash Size: 128MB
   ```

   The RDU-C Release Version should appear as the updated version.

Updating the DataScale SN10-2 RDU-C secondary/recovery partition

1. To update the DataScale SN10-2 RDU-C recovery partition, run the update using the `rduc-<version>-recovery.spi` firmware file:

   ```
   root@xrdu:/dev/shm# obmcupdate -p recovery -t rduc -f /dev/shm/rduc-
   <recovery>-recovery.spi
   ```

If any issues occur during the update of the DataScale SN10-2 BMC or RDU-C, contact SambaNova support

After the DataScale SN10-2 BMC and RDU-C have successfully been updated, it is safe to power on the DataScale SN10-2 and SN10-H modules. Powering on the DataScale SN10-8R discusses how to first safely power on the DataScale SN10-2 and then power on the DataScale SN10-H.

9.3.2. Changing the root password

NOTE SambaNova highly recommends that you change the default password for root to a more secure password.

NOTE Passwords cannot be based on dictionary words for the DataScale SN10-2 BMC. Using a dictionary-based word results in a ‘BAD PASSWORD’ message, and the password will not be changed. Also, passwords should not include the "#" character because that affects DataScale SN10-2 BMC tools.

To change the default password for root on the DataScale SN10-2 BMC, follow these steps:

1. Log in to the DataScale SN10-2 BMC where you transferred the update files:

```
$ ssh root@<SN10-2_BMC_IP_Address>
Password: <Enter root password>
```

2. Run the `passwd` command and enter a new password:

```
root@xrdu:~# passwd
New password: <New Password>
Retype new password: <New Password>
passwd: password updated successfully
```

9.3.3. Generating a secure API login token

To support REST API calls that don’t use plain-text passwords, you can generate a secure token for the DataScale SN10-2 BMC root user.

1. Log in to the client system from which you want to run the REST API calls. The system must have network access to the DataScale SN10-2 BMC.
2. Run the following command to generate the token:

```
$ export token=`curl -k -H "Content-Type: application/json" -X POST
https://<SN10-2_BMC_IP_Address>/login -d '\{"username" : "root", "password" :
"<Password>"}' | grep token | awk '\{print $2;}' | tr -d '"'`
```

3. Confirm that a token has been generated for your session:

```
$ echo $token
1h0Dk9xjtjsOtBkMhgIN
```

4. Test the token to validate operation from the client system. To do that, run the following cURL

command replacing <SN10-2_BMC_IP_Address> with the correct DataScale SN10-2 BMC IP address.

```
$ curl -k -H "X-Auth-Token: $token" https://<SN10-
2_BMC_IP_Address>/xyz/openbmc_project/
{
"data": [
"/xyz/openbmc_project/Ipmi",
"/xyz/openbmc_project/certs",
...
"/xyz/openbmc_project/user"
],
"message": "200 OK",
"status": "ok"
}
```

If you execute the cURL command correctly and similar output is generated, the token works correctly and you can use it with other API calls, for example, to power on and power off the DataScale SN10-2 RDU module.

9.3.4. Configuring the DataScale SN10-2 BMC network

WARNING

When you change the IP address of the DataScale SN10-2 BMC, there are potential dependencies with tools that rely on known IP addresses that were set during the DataScale SN10-8R installation. Update the IP_ADDRESS_SP# entries in the /platform/network.json files for the updated DataScale SN10-2 BMC as well as in the other DataScale SM10-2 BMCs directly connected to the updated DataScale SN10-2 BMC in the node.

NOTE

After changing the IP address and resetting the network service in the steps below, currently connected ssh sessions will be terminated or left in a hung state, because the network IP connection has changed. Log in to the DataScale SN10-2 BMC using the new IP address.

DataScale SN10-2 BMC networking is configured as part of the DataScale SN10-8R delivery. It’s not usually necessary to modify the network configuration upon delivery, although there might be situations where the network has to be reconfigured later.

You can change the network settings by running the network-settings command.

```
root@xrdu:~# network-settings [-h] -i [IPADDRESS] -n [NETMASK] -g [GATEWAY] -d
[DNS] [{static,DHCP}]
```

Table 6 describes the command options.

Table 6. Command options

Option	Function
`{static,DHCP}`	Specify the network mode.
`-h` `--help`	Show the help message and exit.

`-i [IPADDRESS]`
`--ipAddress [IPADDRESS]`
	IP address for static connection.
	Example: `"10.10.0.0"`. Use `""` for DHCP.

`-n [NETMASK]`
`--netMask [NETMASK]`
	Netmask number for static network mode (between 0 to 32). Use any number for DHCP.

`-g [GATEWAY]`
`--gateWay [GATEWAY]`
	Gateway for static connection.
	Example: `"10.10.0.0"`. Use `""` for DHCP.

`-d [DNS]`
`--dns [DNS]`
	DNS for static connection.
	Example: `"10.10.0.0"`. Use `""` for DHCP.

1. Set the IP address configuration using the `network-settings` command.

   Example 1

   Set a static IP address of 10.10.0.15 on a /24 subnet with gateway address 10.10.0.1 and a DNS server on 10.0.0.13:

   ```
   root@xrdu:~# network-settings -i "10.10.0.15" -n 24 -g "10.10.0.1" -d
   "10.0.0.13" static
   Modifiying network settings ...
   Toggling network settings ...
   ```

   Example 2

   Set the network mode to DHCP:

   ```
   root@xrdu:~# network-settings -i "" -n 0 -g "" -d "" DHCP
   Modifiying network settings ...
   Toggling network settings ...
   ```

2. After you successfully run the command, restart the network service to ensure that the configuration is set and running:

   ```
   root@xrdu:~# systemctl restart systemd-networkd.service
   ```

3. At this point, the current `ssh` session should have been terminated or be in a hung state. Open a new terminal and log in to the DataScale SN10-2 BMC:

   ```
   $ ssh root@<SN10-2_New_BMC_IP_Address>
   ```

```
Password: <Enter root password>
```

4. To confirm the IP address configuration, run the `ip address` command. In the command output, the assigned IP address appears as the second `inet` value under `eth0`.

```
root@xrdu:~# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
inet 169.254.192.89/16 brd 169.254.255.255 scope link eth0
valid_lft forever preferred_lft forever
inet 10.10.0.15 brd 10.10.0.255 scope global dynamic eth0
valid_lft 40746sec preferred_lft 40746sec
inet6...
```

9.3.5. Configuring the DataScale SN10-2 hostname

1. To configure or modify the DataScale SN10-2 hostname, log in to the DataScale SN10-2 BMC:

```
$ ssh root@<SN10-2_BMC_IP_Address>
Password: <Enter root password>
```

2. Run the following command to configure or modify the DataScale SN10-2 hostname:

```
root@xrdu:~# hostnamectl set-hostname <hostname>
```

3. To see the new hostname, log out and log back in to the DataScale SN10-2 BMC.

Chapter 10. Monitoring the DataScale SN10-8R

The DataScale SN10-8R provides standard methods to monitor and triage the system through Simple Network Management Protocol (SNMP), along with log files that are generated by each of the DataScale SN10-8R components.

10.1. Viewing diagnostic information and logs

You can use the `xrdutool` tool and logs to diagnose a DataScale SN10-2 issue, as well to collect information for SambaNova Support to triage an issue.

The first step is to check the overall status of the DataScale SN10-2 RDU module as well as the hosted RDUs and memory. The `xrdutool` is useful to get the status of the DataScale SN10-2 node the tool is being run on. Follow these steps to run the tool and review the output on the power and fault status of the DataScale SN10-2 board:

1. Log in to the DataScale SN10-2 RDU module's BMC that is having problems:

```
$ ssh root@<BMC_IP_Address>
Password: <Enter root password>
```

2. Execute the `xrdutool` utility:

```
root@xrdu:~# xrdutool status
```

3. The output of `xrdutool status` provides a quick view into the state of the DataScale SN10-2 RDU module along with two RDUs and the RDU controller. This output identifies whether any faults have been detected, and it shows the power state of the DataScale SN10-2 RDU module and of the RDU.

```
Power is on
2020-08-10 23:29:49,732 DEBUG RDU-C BuildDate: 7.14 1056   DesignVer: 28
BoardID: 28
2020-08-10 23:29:49,738 DEBUG
--------------------------------------------------------
RDU-C BuildDate: 7.14 1056   DesignVer: 28   BoardID: 28
RDU-C Release Version: 1.5.5
XRDU_0: STATUS
------------------------------------------------------------------------------
------------------------------
SYSTEM :  chm1    chm0    stby    ps      pex0    pex1    sys     p3v3
mss_op_state   mss_log_level
           1       1       1       1       1       1       1       1
4               1
------------------------------------------------------------------------------
------------------------------
RDU_0 <RDU_ID> ON and no current faults detected
------------------------------------------------------------------------------
------------------------------
ENABLES:  vddo    pvpp            pvdd    pvddq           pvtt
pavddh  pavdd   vddc
```

```
           1       1               1       1               1               1
1       1
PWRGOOD:  vddo    pvpp0   pvpp1   pvdd    pvddq0  pvddq1  pvtt0   pvtt1
pavddh  pavdd   vddc0   vddc1
           1       1       1       1       1       1       1       1       1
1       1       1
EVENTS :  vddo    pvpp0   pvpp1   pvdd    pvddq0  pvddq1  pvtt0   pvtt1
pavddh  pavdd   vddc0   vddc1
           0       0       0       0       0       0       0       0       0
0       0       0
 -VRHOT:  pvddc0  pvddc1  pvddc0  pvddq1          -FAULT: pvddc0  pvddc1
pvddq0  pvddq1  vr_alert
           0       0       0       0                       0       0       0
0       0
 -THERM:  thub0   thub1   therm
           0       0       0
------------------------------------------------------------------------------
------------------------------
RDU_1 <RDU_ID> ON and no current faults detected
------------------------------------------------------------------------------
------------------------------
ENABLES:  vddo    pvpp            pvdd    pvddq           pvtt
pavddh  pavdd   vddc
           1       1               1       1               1               1
1       1
PWRGOOD:  vddo    pvpp0   pvpp1   pvdd    pvddq0  pvddq1  pvtt0   pvtt1
pavddh  pavdd   vddc0   vddc1
           1       1       1       1       1       1       1       1       1
1       1       1
EVENTS :  vddo    pvpp0   pvpp1   pvdd    pvddq0  pvddq1  pvtt0   pvtt1
pavddh  pavdd   vddc0   vddc1
           0       0       0       0       0       0       0       0       0
0       0       0
 -VRHOT:  pvddc0  pvddc1  pvddc0  pvddq1          -FAULT: pvddc0  pvddc1
pvddq0  pvddq1  vr_alert
           0       0       0       0                       0       0       0
0       1
 -THERM:  thub0   thub1   therm
           0       0       0
------------------------------------------------------------------------------
------------------------------
CLEAR EVENTS :: cleared event status register on RDU_0
CLEAR EVENTS :: cleared event status register on RDU_1
```

For details on diagnosing a DataScale SN10-2 RDU module’s BMC and collecting the required diagnostic and log material, see KB article #1024, “DataScale SN10-2 Diagnostic Collection,” in the

SambaNova Support portal (https://support.sambanova.ai).

10.2. Setting up SNMP alerts

To configure SNMP alerts for third-party components in the DataScale SN10-8R, see the vendor-specific documentation:

- Lantronix SLC8000 serial console server:
  https://cdn.lantronix.com/wp-content/uploads/pdf/SLC8000_UG.pdf
- Juniper EX4300 access switch:
  https://www.juniper.net/documentation/product/en_US/ex4300
- Juniper QFX5200 Ethernet high-bandwidth data switch:
  https://www.juniper.net/documentation/product/en_US/qfx5200
- Mellanox SB7800 IB high-bandwidth data switch:
  https://docs.mellanox.com/category/mlnxos
- Vertiv UU30010L (switched PDU):
  https://www.vertiv.com/globalassets/products/critical-power/power-distribution/vertiv-geist-power-distribution-upgradeable-installeruser-guide.pdf
- GIGABYTE® R282-Z93 (DataScale SN10-H BMC):
  https://download.gigabyte.com/FileList/Manual/server_manual_mgt_console_user_guide_ami_v1.x.pdf
- Red Hat Enterprise Linux (DataScale SN10-H OS option):
  https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/
- Ubuntu Linux Server (DataScale SN10-H OS option):
  https://help.ubuntu.com/18.04/serverguide/index.html

10.3. Viewing system logs

There are several log files you can use to identify and resolve issues with the system or an application:

- BMC logs
- OS logs
- Software application logs
- SambaNova compiler logs

10.3.1. BMC logs

See the "*Administrative tasks for the baseboard management controller (BMC)*" section of this document.

10.3.2. OS logs

SambaNova does not alter the logs or log directories for Red Hat Enterprise Linux or Ubuntu. The majority of logs reside under the `/var/log/` directory, along with others log tools such as `journalctl`.

10.3.3. Software application logs

The following SambaNova-related log files are also located in the `/var/log/sambaflow/runtime/` directory:

`sn.log`	Logs related to SambaNova graph operations. Events received by the graph process and graph-specific events (including errors) that do not get logged to `snd.log`.
`snd.log`	SambaNova daemon (SND) system logs. Provides a summary of RDUs resources and hardware error events.

Additional log events such as kernel logs (from the RDU driver module) go to `dmesg(1)`.

NOTE You can use different log verbosity settings to get more logging details for the SambaFlow Runtime and other SambaFlow components. See "Changing Runtime Log Levels" in the *SambaNova Runtime Guide*.

10.3.4. SambaNova compiler logs

Additional logs for the compilers are available in a user-specified directory that was specified at the time the models were compiled. These logs are fairly low level and might be requested by SambaNova Support to troubleshoot issues. For details see "Collecting diagnostic materials for SambaNova Support".

10.4. SambaNova daemon (SND)

The SambaNova daemon (SND) is an important service running on the DataScale SN10-H host module that manages several critical pieces of the SambaNova operation. The SND is responsible for the following:

- Loading and unloading the RDU drivers
- Initializing RDU system resources
- Managing hardware faults for the RDU system
- Enabling the debugging of the RDU system’s hardware resources

The SND is required to run graphs and models because:

- The SND handles the RDU drivers and the initialization of RDU resources.
- The SND is aware of issues with RDU resources and can avoid problematic resources.

The SND starts automatically:

- At boot time of the DataScale SN10-H OS and starts the discovery and initialization of the RDUs. This is why it is important to power on the DataScale SN10-2 RDU modules first, before powering on the SN10-H host module.
- When the SambaFlow package is installed. In this case, the SND waits a few minutes after the installation for the RDU system discovery and initialization processes to complete.

NOTE All logs from the SND are written to `/var/log/sambaflow/runtime/snd.log`.

The SND service also automatically starts when the SambaFlow package is installed, but it waits a few minutes after the installation for the RDU system discovery and initialization processes to be completed.

10.4.1. Check SND status

To check the status of the SND, run the `systemctl status snd` command. Below is sample output showing what the command might return:

```
$ sudo systemctl status snd
snd.service - SN Devices Service
Loaded: loaded (/usr/lib/systemd/system/snd.service; enabled; vendor preset:
enabled)
Active: active (running) since Wed 2020-05-27 15:40:01 PDT; 17h ago
Process: 3166 ExecStart=/usr/sbin/snd.sh start (code=exited, status=0/SUCCESS)
Main PID: 3203 (setup.sh)
Tasks: 8 (limit: 39321)
CGroup: /system.slice/snd.service
|-3203 /bin/bash ./sbin/setup.sh -s
 -5592 /opt/sambaflow/bin/snd
May 27 15:40:01 labhost snd.sh[3166]: DevCtl2[0x0]
May 27 15:40:01 labhost snd.sh[3166]: DevSta2[0x0]
May 27 15:40:01 labhost snd.sh[3166]: LnkCap2[0x180001e]
May 27 15:40:01 labhost snd.sh[3166]: LnkCtl2[0x4]
May 27 15:40:01 labhost snd.sh[3166]: LnkSta2[ 0x11f]
May 27 15:40:01 labhost snd.sh[3166]: Capabilities 0x11[0xd0]
May 27 15:40:01 labhost snd.sh[3166]: Capabilities 0x01[0xf8]
May 27 15:40:01 labhost snd.sh[3166]: PCI Bus scan completed
May 27 15:40:01 labhost snd.sh[3166]: Enter 'q' to stop the SND server:
May 27 15:40:01 labhost systemd[1]: Started SN Devices Service.
```

10.4.2. Start, stop, and restart SND

You can start, stop, and restart the SND with the following commands:

To start the SND:

```
$ sudo systemctl start snd
```

To stop the SND:

```
$ sudo systemctl stop snd
```

To restart the SND:

```
$ sudo systemctl restart snd
```

10.4.3. Using SND for debugging

The SND CLI provides physical visibility into the entire DataScale SN10-8 system. This allows complete access to the RDU system for debugging, triage, and validation efforts.

The SND also responds to error events that occur on the RDU and on the entire DataScale SN10-2 RDU module.

All logs from the SND are written to `/var/log/sambaflow/runtime/snd.log`. This log provides a summary of the RDU resources available to the system and includes any hardware error events that occur. The information is useful for diagnosing and resolving hardware issues.

Chapter 11. Debugging the DataScale SN10-8R and collecting diagnostic materials

11.1. Debugging issues within the DataScale SN10-8R

Troubleshooting might require that you debug issues with the following DataScale SN10 rack components:

- Compilation of models
- Running of models
- Third-party components

11.1.1. Debugging model compilation

For problems that occur while compiling models, run the following command and examine the logs that are generated in the user-specified output directory:

```
$ python <model_script.py> compile --output-folder=<output_directory>
```

NOTE You can use different log verbosity settings to get more logging details for the SambaFlow Runtime and other SambaFlow components. See "Changing Runtime Log Levels" in the *SambaNova Runtime Guide*.

11.1.2. Debugging running models

For problems that occur while running models, see the following resources for details:

- The `/var/log/sambaflow/runtime/` log files

  These logs provide an initial glance into an issue that is occurring while running a model. If a problem occurs and is reproducible, enable more logging verbosity for SambaFlow Runtime. See the "Changing Runtime Log Levels" section of the *SambaNova Runtime Guide* for details.

- The SambaNova Fault Management (SNFM) tool

  SNFM is a tool that provides a framework to monitor, log, and clear various faults associated with a DataScale SN10-2 RDU module and provide corrective actions to recover from these faults. This capability is built into the SambaNova daemon (SND) and installed as part of SambaFlow. See the "SambaNova Fault Management (SNFM) User" section in the *SambaNova Runtime Guide* for more details.

11.1.3. Third-party components

For operational issues with the third-party components in the DataScale SN10 rack, see the following vendor-specific product documentation. For issues that require additional support or for questions related to troubleshooting, open a support case through SambaNova Support.

IMPORTANT Do not open a case directly with the product vendor.

- Lantronix SLC8000 serial console server:
  https://cdn.lantronix.com/wp-content/uploads/pdf/SLC8000_UG.pdf
- Juniper EX4300 access switch:
  https://www.juniper.net/documentation/product/en_US/ex4300
- Juniper QFX5200 Ethernet high-bandwidth data switch:
  https://www.juniper.net/documentation/product/en_US/qfx5200
- Mellanox SB7800 IB high-bandwidth data switch:
  https://docs.mellanox.com/category/mlnxos
- Vertiv UU30010L (switched PDU):
  https://www.vertiv.com/globalassets/products/critical-power/power-distribution/vertiv-geist-power-distribution-upgradeable-installeruser-guide.pdf
- GIGABYTE R282-Z93 (DataScale SN10-H BMC):
  https://www.gigabyte.com/us/Rack-Server/R282-Z93-rev-100/support#support-manual
- Red Hat Enterprise Linux 8.1 (DataScale SN10-H OS option):
  https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/
- Ubuntu Server 18.04 LTS (DataScale SN10-H OS option):

https://help.ubuntu.com/community/TroubleShootingGuide

11.2. Collecting diagnostic materials for SambaNova Support

When you open a support case, provide details on the issue that has occurred and initial diagnostic materials. For collecting diagnostic materials, see the following KB articles in the SambaNova Support portal:

- DataScale SN10-2 Diagnostic Collection: KB article #1024
- DataScale SN10-H BMC Diagnostic Collection: KB article #1039
- DataScale SN10-H (Red Hat Enterprise Linux) Diagnostic Collection: KB article #1039
- DataScale SN10-H (Ubuntu) Diagnostic Collection: KB article #1039
- Ethernet Data Switch Diagnostic Collection: KB Article #1053
- InfiniBand Data Switch Diagnostic Collection: KB article #1034
- Access Switch Diagnostic Collection: KB article #1053
- Serial Console Server Diagnostic Collection: KB article #1121
- PDU Diagnostic Collection: KB article #1120

Chapter 12. Backing up and restoring components

For backing up and restoring components of the DataScale SN10-8R, continue to use your site-specific guidelines and tools for backing up and restoring systems.

If you change the standard configuration of the networking equipment that is shipped to you, you need to save the configuration changes you make to the devices. Details are covered in the KB articles listed below. You can find KB articles in the SambaNova Support portal at https://support.sambanova.ai.

For the process to recover the Mellanox data switch, see the following KB articles:

- Mellanox Data Switch Password Recovery: KB article #1031
- Mellanox Data Switch Configuration Factory Reset Recovery: KB article #1033
- Mellanox Data Switch Saving Running Configuration (CLI): KB article #1027
- Mellanox Data Switch Saving Running Configuration (WebUI): KB article #1028

For the process to recover the Juniper access switch and data switch, see the following KB articles:

- Juniper Switch Password Recovery: KB article #1056
- Juniper Switch Factory Reset Recovery: KB article #1056
- Juniper Switch Saving Running Configuration: KB article #1056

For the process to recover the Lantronix serial console server, including recovering the sysadmin password, see the following KB articles:

- Lantronix Serial Console Server Password Recovery: KB article #1059
- Lantronix Serial Console Server Factory Reset Recovery: KB article #1059
- Lantronix Serial Console Server Saving Running Configuration: KB article #1059

If the DataScale SN10-H OS needs to be recovered, and the SN10-H host boot partitions are not damaged, contact SambaNova Support. Recovering the SN10-H OS to factory baseline may be possible and a faster recovery option compared to using the recovery ISOs. For the processes to recover the DataScale SN10-H host module, see the following KB articles:

- DataScale SN10-H OS Recovery Using the Recovery ISO – Ubuntu: KB article #1051
- DataScale SN10-H OS Recovery Using the Recovery ISO – Red Hat: KB article #1099
- DataScale SN10-H BMC Password Recovery: KB article #1021
- DataScale SN10-H BMC Non-Corruption Recovery: KB article #1038

For the process to recover the DataScale SN10-2 RDU module, see the following KB article:

- SambaNova DataScale SN10-2 BMC Password Recovery: KB article #1049

For the process to upload configuration files used as part of the recovery process for some of these components, see the following KB articles:

- Uploading Configuration Files for Recovery: KB article #1055
- Listing and Downloading Configuration Files for Recovery: KB article #1044

For questions concerning any of these recovery KB articles or for anything that is not covered here, open a support case through the SambaNova Support portal (https://support.sambanova.ai).

Chapter 13. SambaNova Support

In the event of hardware or software issues, contact SambaNova Support through the SambaNova Support portal (https://support.sambanova.ai), as directed in the “Contacting SambaNova Support” section of this document.

There are also several KB articles that may help you resolve simpler problems.

13.1. Opening a support case

To open a support case, see KB article #1017, “SambaNova Systems Support Best Practices,” which provides the proper procedure for creating a support case.

13.2. Contacting SambaNova Support

To contact SambaNova Support to get help resolving an issue, go to the SambaNova Support portal (https://support.sambanova.ai) and open a support case.

Chapter 14. Disclaimers

All product names, trademarks, and registered trademarks are the property of their respective owners.