R&S®SpycerNode SC
Storage Solution
User Manual

2902.5569.02
Version 02

ROHDE&SCHWARZ
Make ideas real

Hanomaghof 1, 30449 Hanover, Germany
Phone: +49-511-67807-0
Fax: +49-511-67807200
Email: support.media@rohde-schwarz.com
Internet: https://www.rohde-schwarz.com

Throughout this manual, products from Rohde & Schwarz are indicated without the ® symbol, e.g. R&S®SpycerNode SC is indicated as SpycerNode SC.

Contents

General

This chapter includes the following sections:

About this Documentation

This documentation describes how to use the hardware of SpycerNode SC, a storage system by Rohde & Schwarz. It contains installation, operation and maintenance instructions as well as safety instructions which must be followed by the client company and the system operator. For this reason, the manual should always be accessible in the immediate vicinity of the system.

Required Reading

The client company and operator of the system are advised to read this manual, and to follow the instructions.

Each person who is responsible for installation, operation, maintenance or setting of the system must read and understand this manual.

Target Groups

To use this manual you should know how to handle computer equipment. Furthermore, to connect the R&S system to a network you should have experience as a network administrator and know how to set up the required network connections on the installation site both in hard- and software.

When performing maintenance tasks on the hardware of the R&S system, you must be qualified to work on, repair and test electrical equipment.

The target groups are differentiated as follows:

- Client company
- Setup personnel & administrators
- Operators

Client Company

The term "client company" applies to persons who use a product for commercial or economic purposes or authorize a third party for the use or application of a product, and during operation have the legal responsibility to users of their product or other thirds.

Setup Personnel & Administrators

Setup personnel and administrators have corresponding technical skills to perform installation, setup, maintenance, troubleshooting and decommissioning. Administrators are also responsible for the setup within a network, integration into existing technical infrastructure and the ongoing communication with the front-end clients over the network.

Operators

Operators are responsible for the day-to-day operation of the system, troubleshooting and basic maintenance work. Also, operators must be trained by the client company to prevent hazards from electrical or mechanical components and to avoid property damage.

Additional Documentation

The complete documentation can be downloaded from **https://gloris.rohde-schwarz.com** after registering/logging in to access restricted information. There you may find updated manuals as well as further information on your product.

Chapters Overview

The chapters contain the following information:

Chapter "General" on page 5	Begins with a short introduction to SpycerNode SC, followed by a note regarding the audience this manual is written for, and information on additional documentation.
Chapter "Safety" on page 11	Provides all required safety instructions and important notes you must adhere to protect your equipment and avoid personal injury.
Chapter "Product Description" on page 17	This chapter gives a front and rear overview of the system detailing all items, connectors and interfaces. Additionally, it contains some further information, for example, about the digital video in- and outputs.
Chapter "Installation" on page 29	Describes the necessary steps to install the hardware of the system and perform the initial software setup.
Chapter "Operation" on page 63	Explains how to operate the system via the R&S®Device Manager - a monitoring and setup tool for all Rohde & Schwarz devices connected within the same network.
Chapter "Maintenance" on page 75	Details maintenance work, for example, in case of a disk, an or power supply unit failure.
Chapter "Appendix" on page 97	Provides technical details and general information about the hardware of the system.

Appropriate Use

The R&S system may only be used according to its intended function. Any other use or extension of this function is considered inappropriate. Inappropriate use may lead to situations resulting in personal injury or property damage.

General

SpycerNode SC has been built according to the applying safety regulations.

NOTICE

Inappropriate use

If the R&S system is not used in compliance with the safety instructions, the warranty and all resulting liability claims will be void.

Carefully read the following safety instructions before attempting any installation and/or performing any work on the system hardware

To correctly use the R&S system heed the following:

- To minimize the possibility of a faulty operation of the device you must have access at all times to all manuals and guides at the operation site. Before installing and/or using the R&S system it is strongly recommended to read the manuals and follow the instructions.
- The hardware of the R&S system works with voltages that can be hazardous to your health. Never work on the system or access its interior with the power cable(s) being plugged in. Make sure the power supply is disconnected from the components you intend to work on.
- Computer hardware contains components that are sensitive to electrostatic discharge. If you touch them without precautionary measures, they can be destroyed. Use a wrist strap connected to ground when accessing electronic parts and take care of grounding the system. Avoid touching the internal components of the R&S system whenever possible.
- Computer hardware contains components that are sensitive to changing voltages. Connecting or disconnecting the R&S system to or from peripheral hardware while any of them is switched on may damage the hardware. Switch off all peripheral hardware before connecting or disconnecting anything.
- Use, store and transport the R&S system only in compliance with the technical data laid out in chapter "Appendix" on page 97.
- If fluids or solid objects get inside the casing, the R&S system must be disconnected from the power supply immediately. Before using the system again, it has to be checked by authorized service personnel.
- Only use a damp tissue without any cleaning agents to clean the casing.
- The R&S system must not be misused, abused, physically damaged, neglected, exposed to fire, water or excessive changes in the climate or temperature, or operated outside maximum rating.

- Do not perform any changes or extensions to the R&S system whatsoever.

Environmental Conditions

For error-free working and a long service life SpycerNode SC needs some basic environmental conditions:

- Do not expose the R&S system to sources of heat, such as direct sunlight or a radiator.
- Do not cover or obstruct the ventilation holes of the system.
- When installing the R&S system in a rack, take care that warmed up air is conducted to the rear of the rack and properly vented away.
- Avoid areas with high humidity or dust. Best operating conditions are given in an air-conditioned site.
- Do not expose the R&S system to strong electric or magnetic fields.
- Avoid areas where the R&S system will be subject to vibrations or shocks.

Observe also the environmental data provided in "Appendix" > "Environmental Conditions" (page 100).

Appropriate Use

Safety

The product documentation helps you use SpycerNode SC safely and efficiently. Provide access to this product documentation and pass it on to the subsequent users. Use SpycerNode SC only in its designated purpose as described in the product documentation. Observe the performance limits and operating conditions stated in the specification (data sheet).

Safety information is part of the product documentation. It warns you about the potential dangers and gives instructions how to prevent personal injury or damage caused by dangerous situations. In this chapter you will find information on basic safety issues grouped according to subjects. Throughout the documentation, safety instructions will be provided to specific topics that require your attention during setup or operation.

Always read the safety instructions carefully. Make sure to fully comply with them. Do not take risks and do not underestimate the potential danger of small details.

This chapter is divided into the following sections concerning different safety topics:

General

Please observe the following important safety notes:

- If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.
- This equipment is to be installed for operation in an environment with ambient temperature below 35°C, see also "Environmental Conditions" (page 100).
- All plug-in modules and blank plates are part of the fire enclosure and must only be removed when a replacement can be immediately added. The system must not be run without all modules or blanks in place.
- Unplug the system before you move it or if you think it has become damaged in any way.
- In order to comply with applicable safety, emission and thermal requirements no covers should be removed, and all bays must be populated with plug-in modules or blanks.
- Do not remove cooling fans, PSUs or I/O Modules unless you have a replacement model of the correct type ready for insertion.
- The system is to be operated only when mounted and mechanically secured into a 19-inch rack.
- The storage drives are to be installed only after having mounted the system into the rack. Also, the storage drives must be removed prior to dismounting the system from the rack.
- It is recommended that you wear a suitable anti-static wrist or ankle strap and observe all conventional ESD precautions when handling plug-in modules and components. Avoid contact with backplane components and module connectors, etc.

Electrical

WARNING

Electric Shock

Opening or removing the system cover while the system is powered on may expose you to a risk of electric shock.

Maintenance inside the system should only be performed by personnel qualified for handling and testing electrical equipment. Exercise utmost care when performing any kind of work inside the system while it is on.

Please observe also the following:

- The enclosure must only be operated from a power supply input voltage range of 200-240 VAC. The power supply units, as well as the cooling fans are hot-swappable.
- The plug on the power supply cord is used as the main disconnect device. Ensure that the socket outlets are located near the equipment and are easily accessible.
- When powered by multiple AC sources, disconnect all supply power for complete isolation.
- A safe electrical earth connection must be provided to the power supply cords. Check the grounding of the casing before applying power.
- Provide a suitable power source with electrical overload protection to meet the requirements laid down in the technical specification.
- A faulty PSU must be replaced with a fully operational module within 24 hours.
- The power ratings are: voltage: 200 to 240 VAC; frequency: 50 to 60 Hz.

Network

Before connecting the product to a local area network (LAN), consider the following:

- Install the latest firmware to reduce security risks.
- For Internet or remote access, use secured connections if applicable, such as HTTPS, SFTP, FTPS instead of HTTP, FTP.
- Ensure that the network settings comply with the security policies of your company. Contact your local system administrator or IT department before connecting your product to your company LAN.
- When connected to the LAN, the product may potentially be accessed from the Internet, which may be a security risk. For example, attackers might misuse or damage the product.

Lithium Cells or Batteries

The product contains lithium polymer or lithium ion cells or batteries. The use of the word battery in the following always means all types. Only the battery contents are potentially hazardous. As long as a battery is undamaged and the seals remain intact, there is no danger.

Impact, shock or heat can cause damage such as dents, punctures and other deformations. A damaged battery poses a risk of personal injury. Handle a damaged or leaking battery with extreme care. Immediately ventilate the area since the battery releases harmful gases. If you come into contact with the battery fluid, immediately remove all contaminated clothing. Irritation can occur if the battery fluid comes in contact with your skin or eyes. Immediately and thoroughly rinse your skin or eyes with water and seek medical aid.

For safe handling, follow these rules:

- Do not short-circuit the battery.
- Do not mechanically damage the battery. Do not open or disassemble the battery.
- Do not expose the battery to high temperatures such as open flames, hot surfaces and sunlight.
- Only use the battery with the designated product.
- Only use the appropriate charger to charge the batteries. If the batteries are improperly charged, there is a risk of explosion.
- Store the battery at room temperature (approximately 20°C | 68°F) enclosed in the original packaging.
- Dispose of batteries separately from normal household waste as specified by the local waste disposal agency.

⚠ WARNING

Safety Regulations

If you disregard these safety regulations, you risk serious personal injury or even death due to explosion, fire or hazardous chemical substances.

When replacing a defective battery, only use the same battery type. When returning batteries to Rohde & Schwarz subsidiaries, choose a carrier qualified to transport dangerous goods and follow the carrier's transport stipulations in line with IATA-DGR, IMDG-Code, ADR or RID. If you need assistance, contact the carrier or customer service.

Transportation

CAUTION

Risk of Injury

Lifting the system by yourself may result in serious injury and property damage.

Do not attempt to lift the system by yourself, always get others to assist you.

Please observe the following general important notes:

- When lifting or moving the casing, only use the transportation handles provided in the delivery box, and the front handles to lift the system.
- Important: The casing must be mounted in a rack.
- An unpopulated casing can weigh up to 48kg (106lbs). Use appropriate lifting methods.
- A fully populated casing weighs 95kg/210lbs (60 x HDDs) or 72kg/159lbs (60 x SSDs). Do not attempt to lift the casing when populated with drives. Mount the system into a rack prior to installing the drives.
- When closing any drawers, do so firmly, ensuring the latches are engaged.

Product Description

The R&S®SpycerNode SC is a storage server for media and entertainment applications. With its ideal size as a building block, it is easy to lift, install and deploy. It provides features such as advanced PCI4.0 technology, activity and status indicators for all key components, alarms and lockable carriers. With the compact design, and advanced file system functionality the R&S®SpycerNode SC is ready to fulfill a wide range of applications while offering you the stability, scalability, and performance you need to keep up with your customers' requirements.

This chapter is divided into the following sections:

Models

SpycerNode SC configurations may differ in terms of storage capacity and additional connection options.

Basic Unit Configuration

Each SpycerNode SC system consists of the following components:

- 16-core/32-thread CPU
- 128GB RAM
- PCIe4 slot architecture
- 2 x 10GBECu on board
- 1 x 1GbE IPMI I/F
- CentOS operating system

A SpycerNode SC basic unit has 60 media drive bays organized in two LUNs (30 drives per LUN).

Storage Capacity Options

The following drive bundle options are available:

Name	Bundle content	Usable size estimate in TB
SBO-B130	HDD bundle 4TB (30 drives)	99
SBO-B131	HDD bundle 8TB (30 drives)	198
SBO-B132	HDD bundle 16TB (30 drives)	396
SBO-B140	SSD bundle 1.92TB (30 drives)	47
SBO-B141	SSD bundle 3.84TB (30 drives)	95
SBO-B142	SSD bundle 7.68TB (30 drives)	190

Additional HBA Options

The following HBA options (backbone and networking) are also available:

- 100GbE Dual Port Ethernet Card
- 200GbE Dual Port Ethernet Card

Certified Clients for SpycerNode SC

There are different ways to connect clients to SpycerNode SC.

SpycerNode SC exposes the storage via the NSD (Network Shared Disk) protocol to the ethernet network. A NSD client is any server or workstation that has the native Spectrum Scale protocol installed and is designated to operate as a client. Physically reading or writing user data to the SAN disks is done on behalf of the NSD clients that trigger the disk operations

The following operating systems are supported for native Spectrum Scale 5 clients:

- Windows 10
- RHEL/CentOS 7.7 (or later)
- SLES12 SP1 (or later)
- Ubuntu 16.04 and 18.04.1

Besides the native clients the following file sharing protocols are supported:

Protocol	Version	Operating System
Samba	SMBv2, SMBv3	Linux/Windows/OSX
NFS	NFSv4	Linux/OSX
FTP	-	Linux/Windows/OSX

Performance values may differ for individual client configuration.

The Front of the System

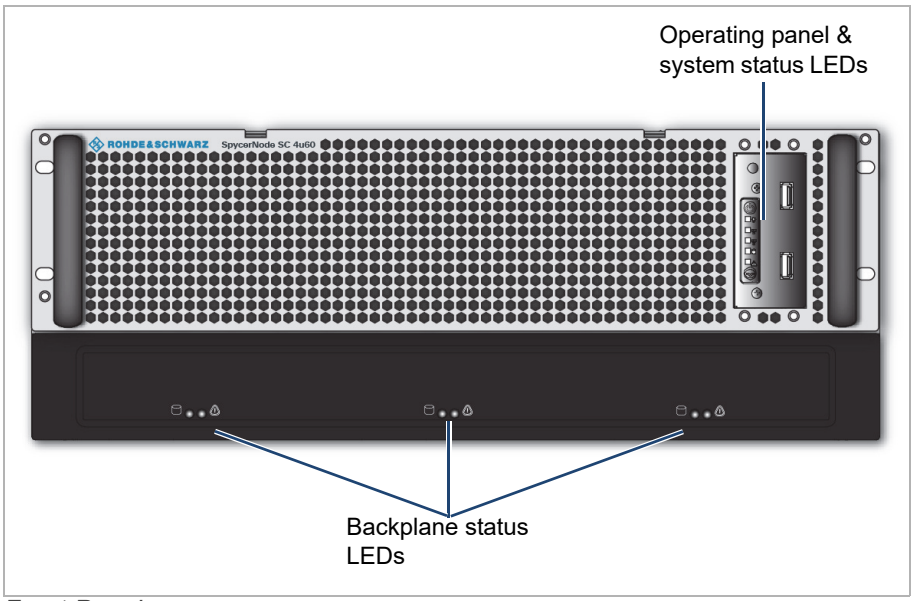
This section gives an overview of the front of the system.

The following topics are covered:

- Front Panel (page 20)
- Operating Panel (page 21)

Front Panel

The front of the system is equipped with a front cover for mechanical protection and sufficient air circulation.



Front Panel

Operating panel & system status LEDs	See "Operating Panel" (page 21).
Backplane status LEDs	See "Backplane Status LEDs" (page 21).

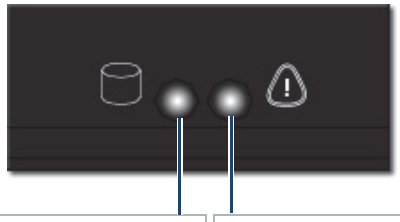
Operating Panel

	ID System Indicator
	Power On/Off
	System Power LED
	LAN 1 LED
	LAN 2 LED
	System HDD Activity LED
	Service ID LED On/Off
	System Reset

Operating Panel & Status LEDs

Backplane Status LEDs

There are three drive backplanes hosting the storage drives (with 20 drive trays each). The status of each backplane is displayed on the lower front panel of the system.



LED11:
Blue (ON) - Drive OK

OFF - Drive not connected or power is off.

LED12:
Red (ON) - Drive failure

OFF - Normal operation

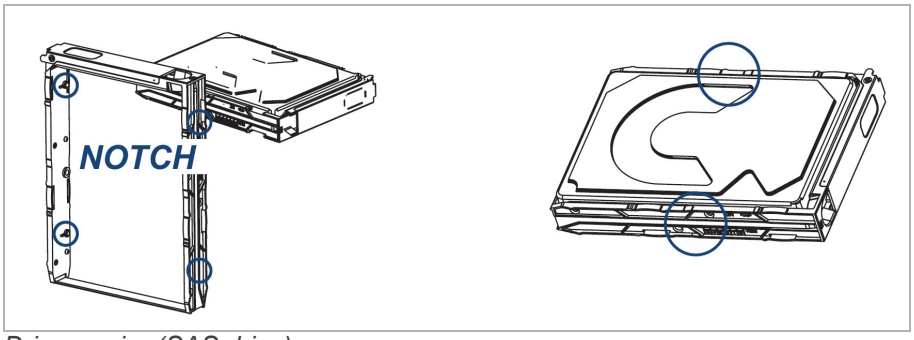
Backplane Status LEDs

Drives

Drives in SpycerNode SC are protected by RAID 6. RAID 6 uses two parity stripes to distribute data across the set of drives. It allows for two disk failures within the RAID set before any data is lost. All drives provide error detection and correction capabilities. These are reported to the application in line with the SCSI specifications.

Carriers

Drive carriers are used to hold the storage disks. A drive carrier houses a single 3.5 SAS drive or, with an adapter, a 2.5 inch SAS SSD.

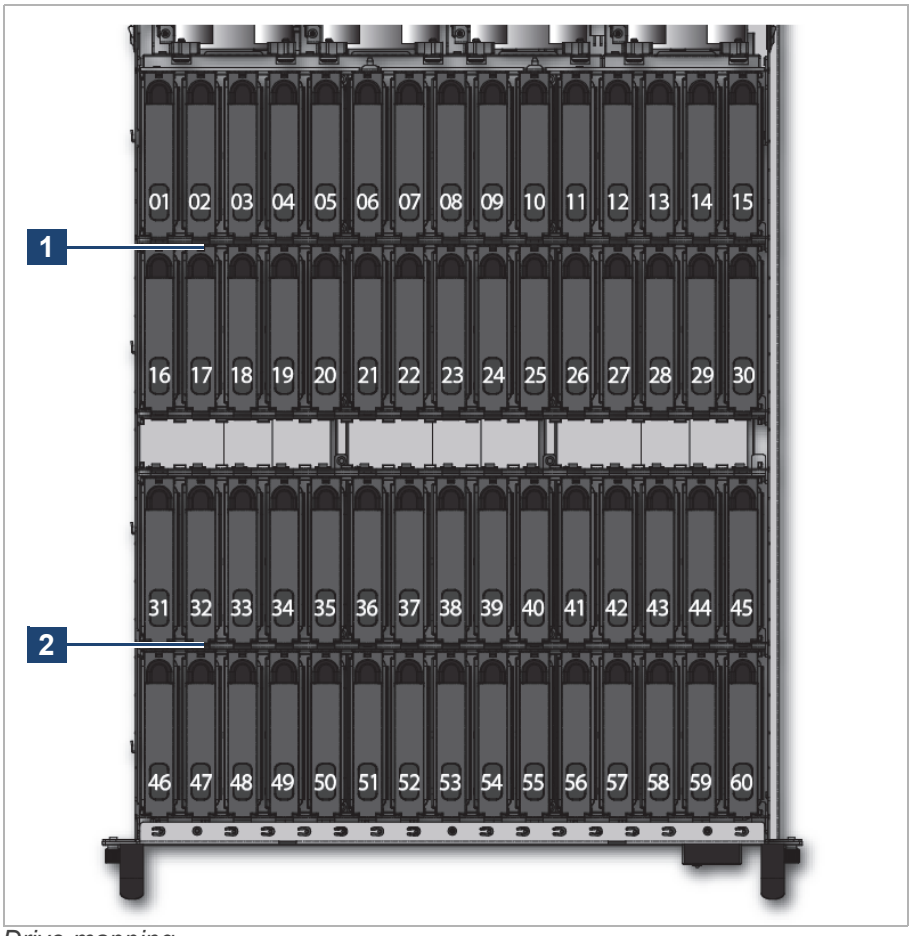


Drive carrier (SAS drive)

Disks Layout

At shipment, the hard disks are delivered separately and therefore have to be installed before putting the system into operation, see also "Installing the Drives" (page 36).

The drives are divided into two drives sets (01 - 30 and 31 - 60) for a total of 60 drives. A system with half capacity will have only the first set populated. The layout of the drive sets is as follows:



Drive mapping

Status LED

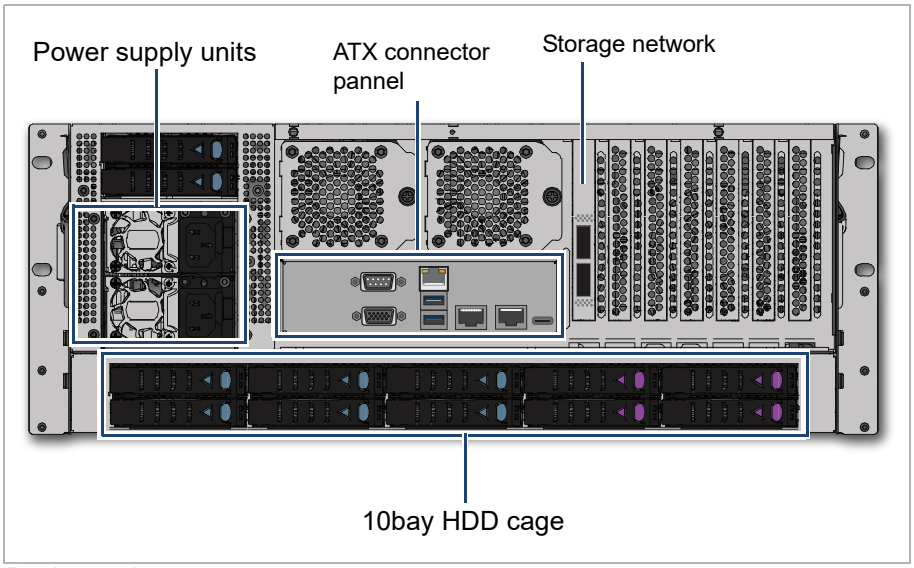
The drive carriers have a status LED to indicate the current state of the drive.

HB and EB drive carrier LEDs

Blue (ON)	Disk connected
Blue (blinking)	Disk activity
Red (blinking)	Rebuild status for RAID
Red	Disk failure

The Rear of the System

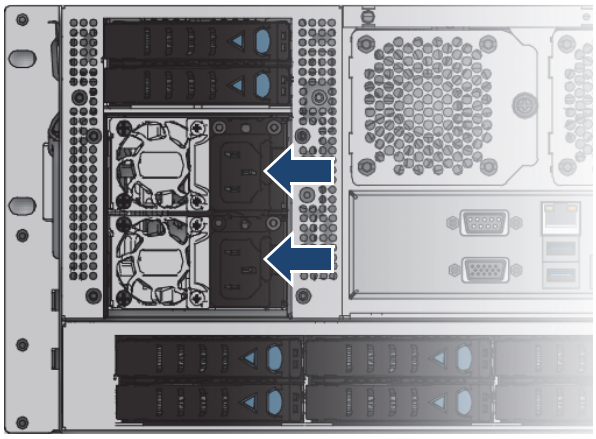
The rear of the chassis provides access to the I/O modules, the power supply units, and the system drives.



Back panel

Power supply units	Dual redundant power supply units, see also "Power Supply Units" (page 25)
ATX connector panel	Provides the standard connectors of the computer system, see also "ATX Panel" (page 26)
Storage network connection	Provides (optional) connection to external storage devices with either a 100GbE or a 200GbE Dual Port Ethernet Card.
10bay HDD cage	Hosts the system disks for the operating system and meta-data, see also "System Disks" (page 27).

Power Supply Units



Power connectors	Power is provided by two 1600 W PSU's These require an input of 200 to 240 VAC at 50 to 60 Hz. The IEC C14 AC connector requires a C13 AC jack.

Dual PSUs provide redundant power for the system: if one PSU fails, the other will keep the system running while you replace the faulty module. The PSUs are hot-swappable.

NOTICE

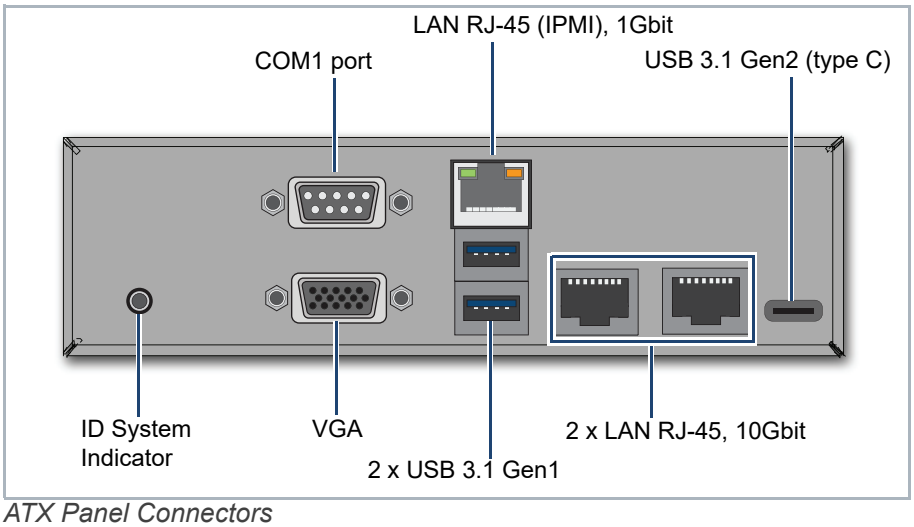
System Damage

Replacement of a PSU can be performed while the system is running, but the procedure must be completed immediately after the removal of the defective PSU, otherwise a continued operation of the system cannot be guaranteed.

Change a failed power supply unit immediately. Ensure you have a replacement PSU before you remove the defective unit.

For information on how to exchange a PSU see "Replacing a Power Supply Unit" (page 78).

ATX Panel

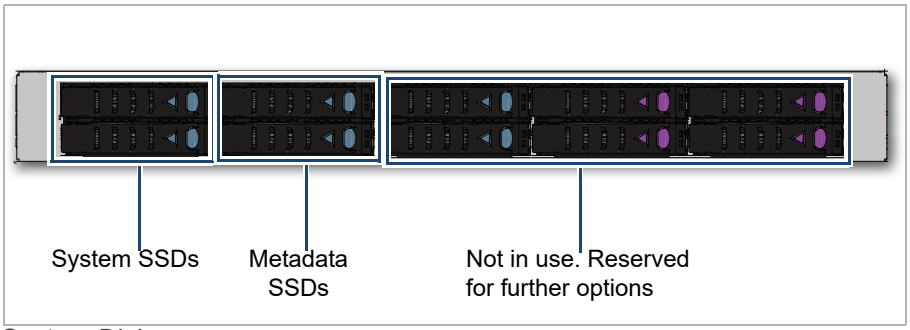


ATX Panel Connectors

The ATX connector panel on the rear of the R&S system holds the connectors of the computer system. It provides the following connections:

COM1 Port	RS232 connector for the connection of serial interface devices.
LAN RJ-45 (IPMI)	1 Gb Ethernet connection port to connect the system to a network.
USB 3.1 Gen2 (type C)	A type-C USB to connect external devices to the system.
ID System Indicator	Press to trigger the green ID LED located on the front of the system. Useful e.g. to locate the system within a rack among many other systems.
VGA	DB-15 connector (female) to connect a monitor to the system.
USB 3.1 Gen1	USB connectors to connect external devices to the system.
2 x LAN RJ-45	2 x 10 Gb Ethernet connection ports to connect the system to a network. By default, the left network port is set to **DHCP** (Dynamic Host Configuration Protocol), whereas the left one is pre-configured to a static 10.0.0.4 IP address.

System Disks



System Disks

The system disk array at the rear of the system contains SSDs for the operating system and metadata. To prevent data loss in case a disk fails, they are RAID1 protected.

The system SSDs are connected to the system with the help of disk carriers which make the removal of a disk easy, for example, in the event of a failure.

NOTICE

Disk failure in the same RAID array

If the second disk fails in the meantime, the data will be unrecoverable.

Replace a broken disk immediately to prevent data loss.

The Rear of the System

Installation

This chapter is divided into the following sections:

Unpacking the System

Perform the following steps:

1. Open the SpycerNode SC delivery box and unpack first only the accessories.

NOTICE

Warranty Claims

To make warranty claims you have to keep the original packing and use it in case of a return transportation.

2. Check your delivery and compare it with the delivery note. In case of missing items, please contact your local vendor or R&S immediately.

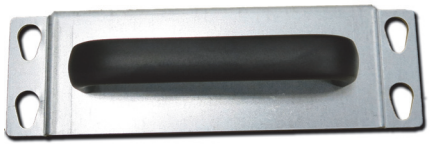
NOTICE

Environmental Conditions

For error-free working and a long service life SpycerNode SC needs some basic environmental conditions:

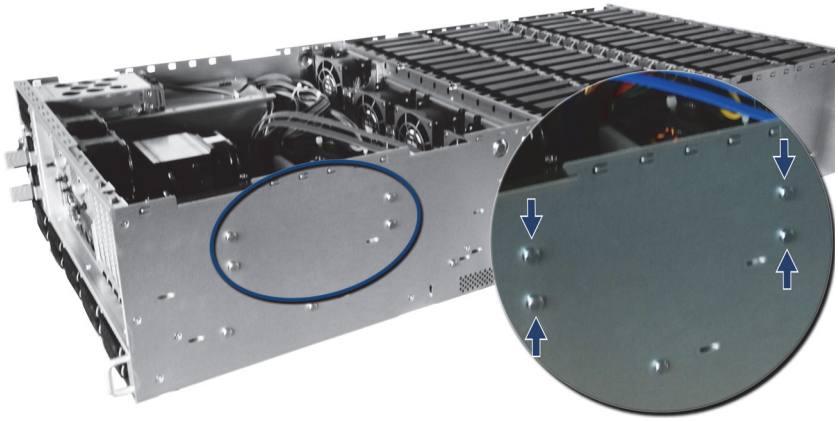
- Do not expose the SpycerNode SC to sources of heat, such as direct sunlight or a radiator.
- Do not cover or obstruct the ventilation holes of the system. When installing the system in a rack, take care that warmed up air is conducted to the rear of the rack and properly vented away.
- Avoid areas with high humidity or dust. Best operating conditions are given in an air-conditioned site.
- Do not expose the SpycerNode SC to strong electric or magnetic fields.
- Avoid areas where the SpycerNode SC will be subject to vibrations or shocks.

3. Locate the two transportation handles inside the delivery box.



x 2

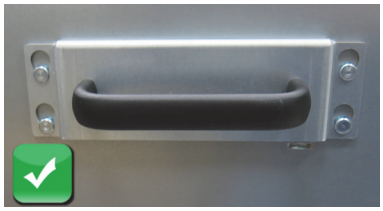
4. There are four transportation hooks at each side of the casing. Attach the two transportation handles to the transportation hooks.

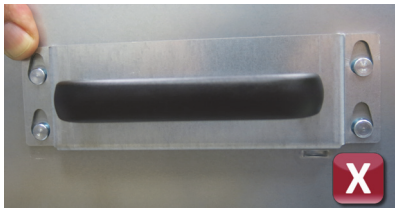


CAUTION

Risk of Injury

Make sure the openings on the handles completely embrace the hooks. Also, the openings must be attached at the narrow end, and NOT at the wide end.





5. Place the system on a flat surface to prepare it for mounting into the rack.

CAUTION

Risk of Injury

Lifting the system by yourself may result in serious injury and property damage

Do not attempt to lift the system by yourself, always get others to assist you.

Mounting the System into a Rack

Rack System Precautions

The following safety requirements must be considered when the unit is mounted in a rack.

- The rack construction must be capable of supporting the total weight of the installed enclosure(s) and the design should incorporate stabilizing features suitable to prevent the rack from tipping or being pushed over during installation or in normal use.
- The system must be operated with low pressure rear exhaust installation [back pressure created by rack doors and obstacles not to exceed 5 pascals (0.5mm water gauge)].
- The rack design should take into consideration the maximum operating ambient temperature for the unit, which is 35°C.
- The rack should have a safe electrical distribution system. It must provide over-current protection for the unit and must not be overloaded by the total number of units installed in the rack. When addressing these concerns consideration should be given to the electrical power consumption rating shown on the nameplate.
- The electrical distribution system must provide a reliable earth for each unit in the rack.
- The design of the electrical distribution system must take into consideration the total earth leakage current from all the power supplies in all the units. The rack may require labeling with “HIGH LEAKAGE CURRENT. Earth connection essential before connecting supply”.
- The rack when configured with the units must meet the safety requirements of UL 60950-1 and IEC 60950-1.

⚠ WARNING

Rack Toppling Over

Racks may toppling over due to a massive overweight in the upper part.

Do not slide more than one enclosure out of the rack at a time. When loading a rack with enclosures, fill from the bottom up; empty from the top down. Close all enclosures before loading.

⚠ CAUTION

Risk of injury

An unpopulated enclosure can weigh up to 48kg (106lbs) and more.

Do not attempt to lift the system by yourself, always get others to assist you. Never attempt to lift the enclosure when populated with drives.

NOTICE

Electronic discharge

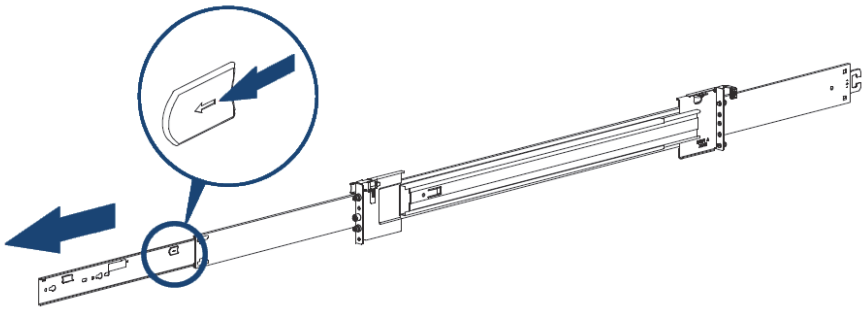
Computer hardware contains components that are sensitive to electrostatic discharge. If you touch them without precautionary measures, they can be destroyed.

Ensure that you have fitted and checked a suitable anti-static wrist or ankle strap and observe all conventional ESD precautions when handling modules and components. Avoid contact with backplane component and module connectors, etc.

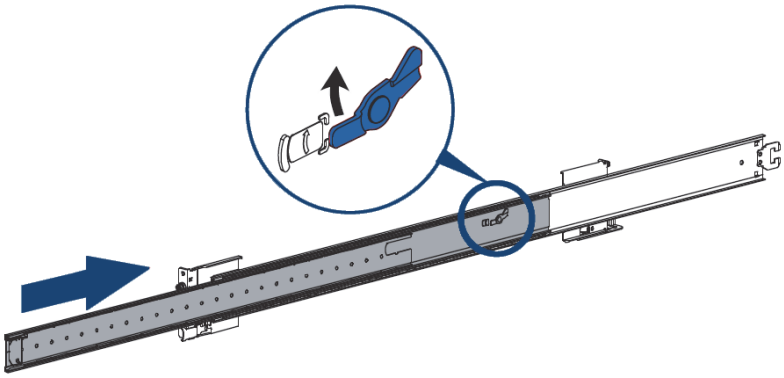
Mounting the System

Perform the following steps:

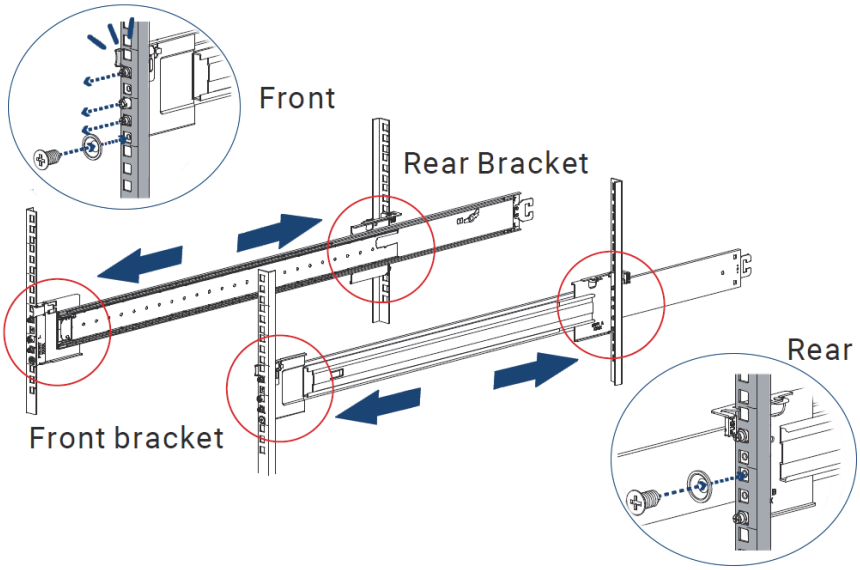
1. Make sure the system is unpacked and placed on a flat surface, see "Unpacking the System" (page 30).
2. Pull the tab forwards and take out the inner rail.



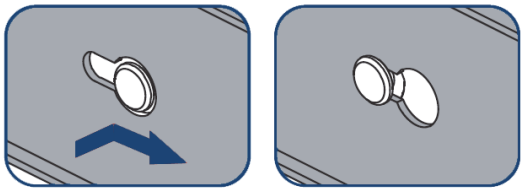
3. Release the latch and slide back the middle rail.

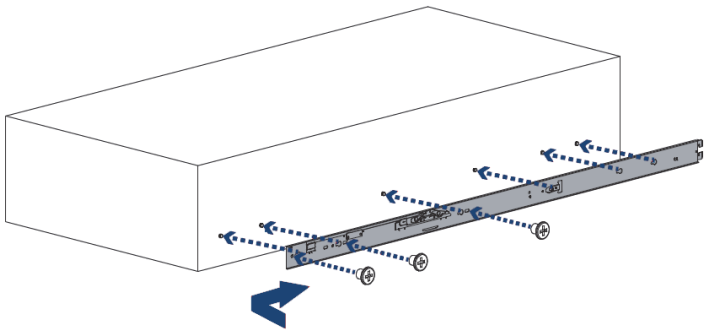


4. Align the front bracket of the outer rail with the mounting hole. Attach the rail to the rack frame and secure it with the screws from both the front and the rear.

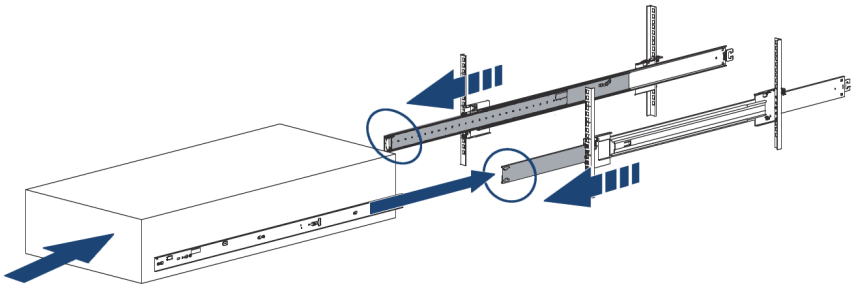


5. Attach the outer rails to both sides of the casing using the hooks. Secure the rails with the screws provided.

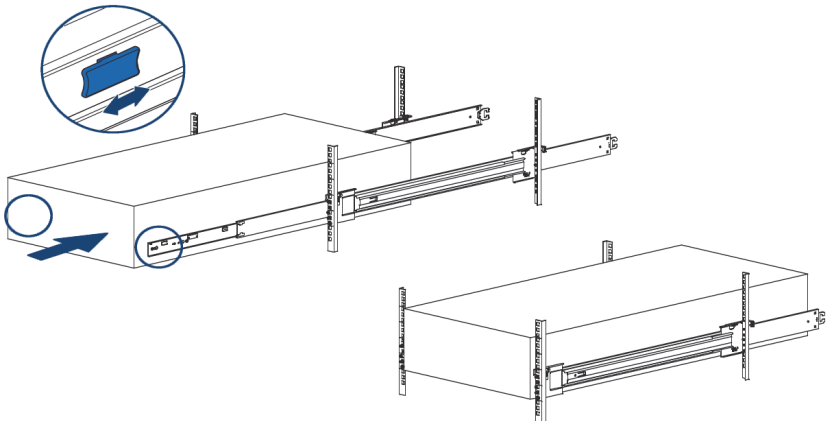




6. Pull the middle rails on the frame to fully extended position. Align the inner slides with the outer slides.



7. Slide the case into the frame. When hitting a stop, push the blue release stop on the inner rails.



SpycerNode SC is now mounted into the rack.

Installing the Drives

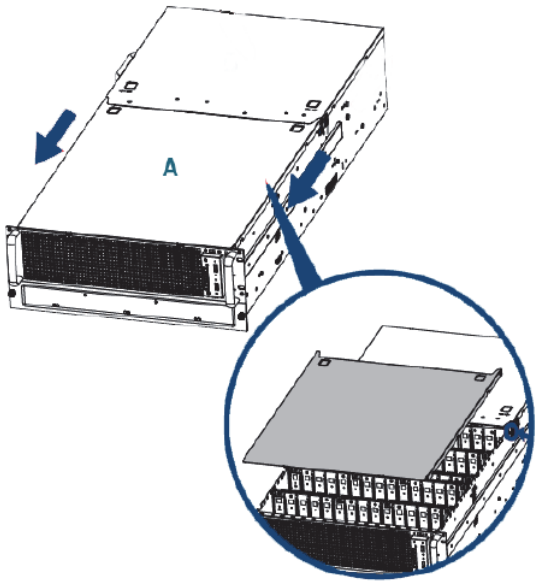
Perform the following steps:

NOTICE

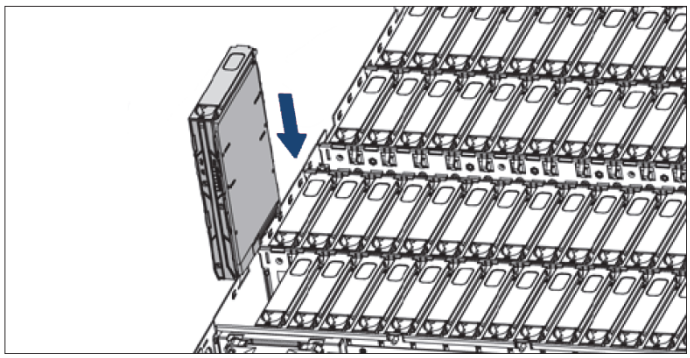
Risk of Damage

Install the drives only after the system has been mounted into the rack!

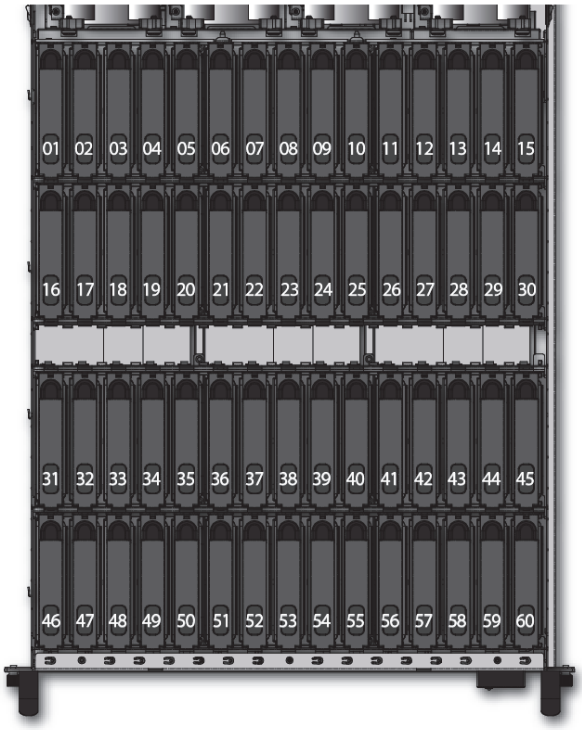
1. Simultaneously push the lock buttons on both sides of the casing and remove the top cover on the front side.



2. Insert the disk drives into the associated slots.



3. The drives are divided into two drives sets (01 - 30 and 31 - 60) for a total of 60 drives. The layout of the drive sets is as follows:



A system with half capacity will have only the first set populated.

Connecting the Power Source

NOTICE

Loss of Data/Corrupt Data

In the event of a power failure the device will be abruptly switched off. This can result in corrupt data, loss of data and equipment damage.

Connect the system to an uninterruptible power supply redundantly on two phases.

NOTICE

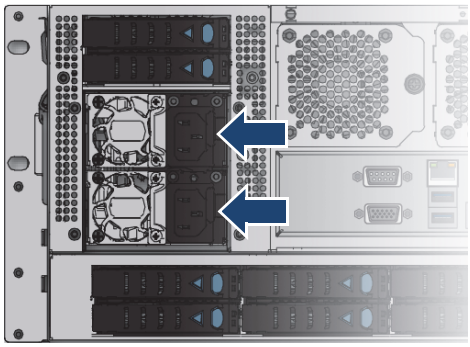
Electrical Shock

If any part of the device is damaged and the exterior of the system is still under power.

The casing must be grounded before applying power.

Perform the following steps:

1. Connect both power cords to the power supplies inlets.

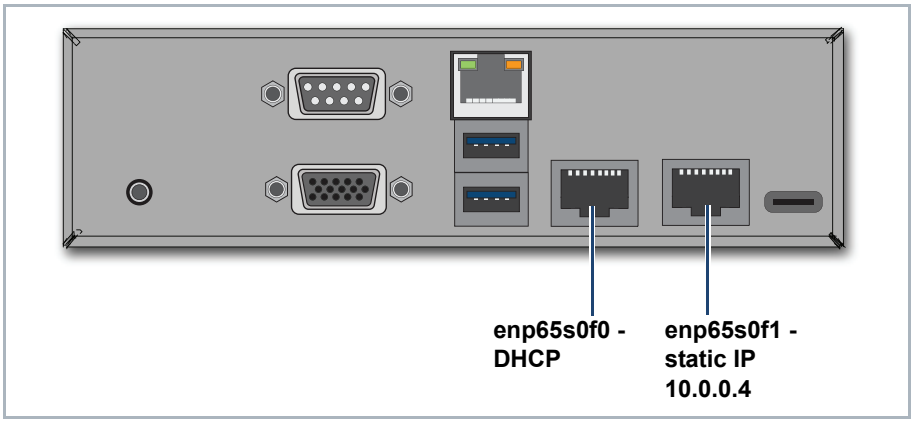


2. Turn on the system

Initial Setup

For initial setup the device must be integrated into a network to establish access to the R&S®Device Manager. The Device Manager is the tool that allows you to configure and monitor all R&S devices connected within a local network.

The network connection can be done via either of the two 10Gbit network ports (also compatible to 1Gbit and 100Gbit connection ports) at the rear of system. However, depending on which one you choose, different settings must be applied, since the first one is set to DHCP (Dynamic Host Configuration Protocol) and the second one to static IP (10.0.0.4).



The following topics are covered:

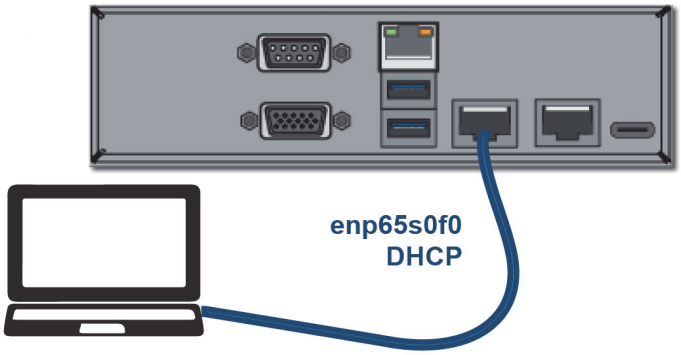
- Using Dynamic Host Configuration Protocol (DHCP) (page 39)
- Using Static IP (page 44)

Using Dynamic Host Configuration Protocol (DHCP)

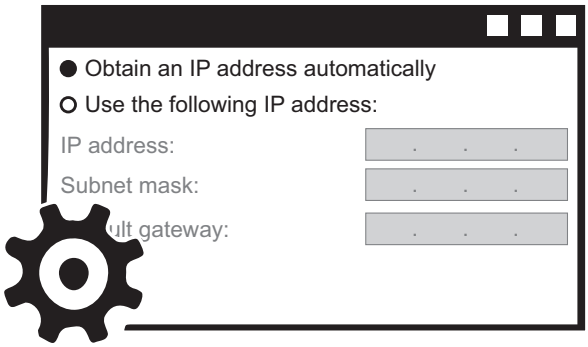
With a zeroconf capable PC/MAC it is possible to automatically detect network services. You can also use a zeroconf browser to view all zeroconf capable devices in your network. If your PC is not zeroconf capable use tools such as Bonjour.exe for the automatic detection of network services or connect your system using a static IP address ("Using Static IP" (page 44)).

Perform the following steps:

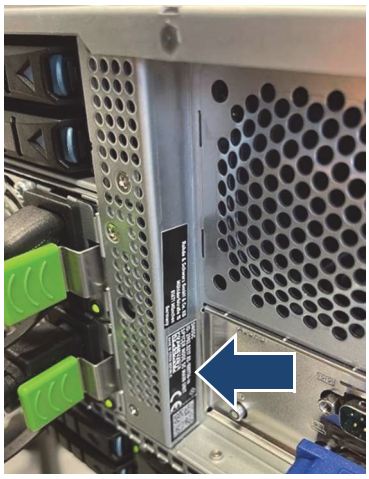
1. Connect port **ENP65S0F0** to a PC/Mac.



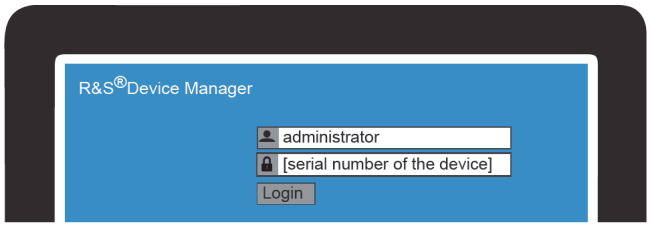
2. Select **Obtain an IP address automatically** on the PC/Mac.



3. Enter the host name of the system in the Chrome web browser to open the R&S®Device Manager on your local system:
   `http://snosc-[serial number].local`
   The host name itself consists of the keyword snosc, followed by a dash, the serial number of the system, and the extension „.local“. The label with serial number is located at the rear panel.

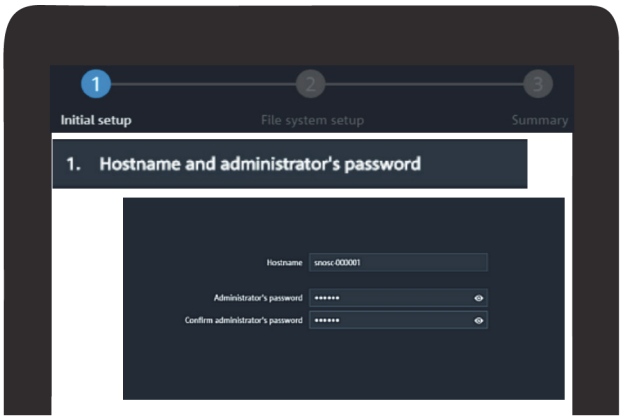


4. The first time you log in, enter the following credentials:
   USERNAME: **administrator**
   PASSWORD: **[serial number of the device]**

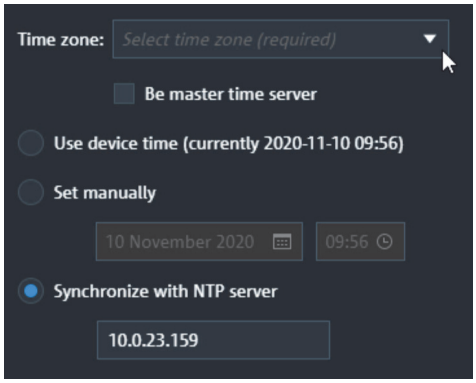


   ▸ The Easy Setup Wizard of the Device manager initiates automatically right after the first login.

5. Define hostname and password for the system:



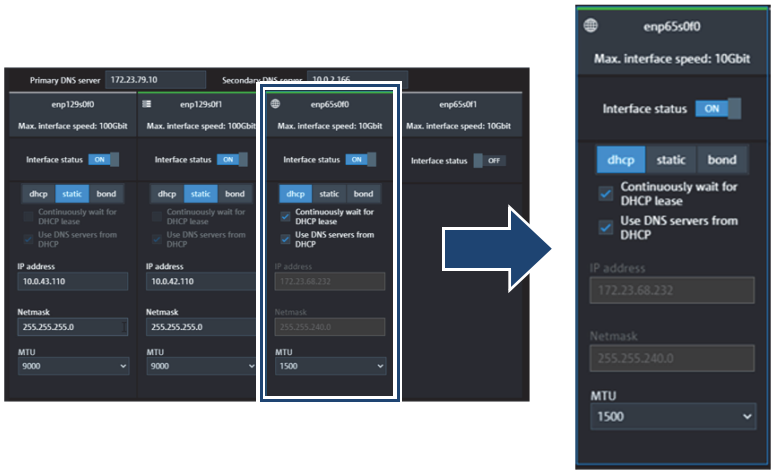
6. Specify date and time settings for the system.



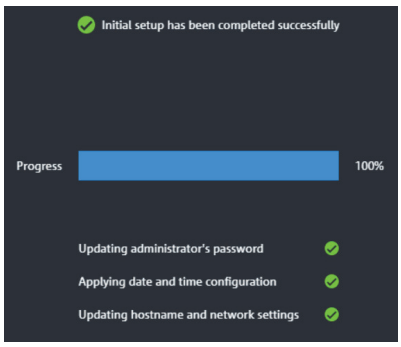
Time zone	Select your time zone from various predefined selection options.
Be master time server	Set the checkbox if you want to designate this particular system as the main NTP server within your local network.
Use device time	Read the current date and time of the device and set it as default.

Set manually	Manual entry of the date and time settings.
Synchronize with NTP server	Synchronize the date and time settings with a central NTP server from your local network.

7. Click the third network port section (from left to right - enp65s0f0) and make sure the **INTERFACE STATUS** is set to **ON** and **DHCP** mode is enabled. The **IP ADDRESS** and **NETMASK** are set automatically.



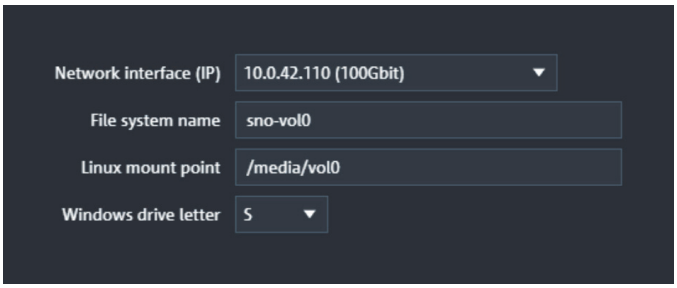
▸ With this step, the first part of the setup is completed:



8. In the next installation phase, the file system configuration is carried out. First, the metadata drives and the installed storage capacity are displayed.

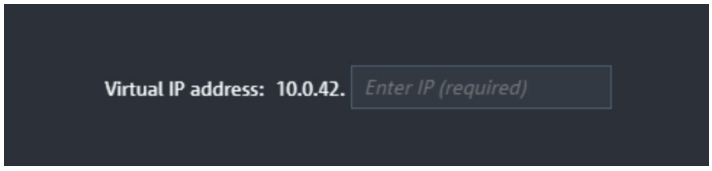
Zone 1	Shows the number of metadata drives, the drive type, the capacity and RAID level.
Zone 2 / Zone 3	Shows the installed storage drives type, their capacity and the level of RAID protection. Each zone represents a single drive set which consists always of 30 drives. A system with half the capacity will have only one zone populated.

9. In the next step you select the interface for you storage network connection.

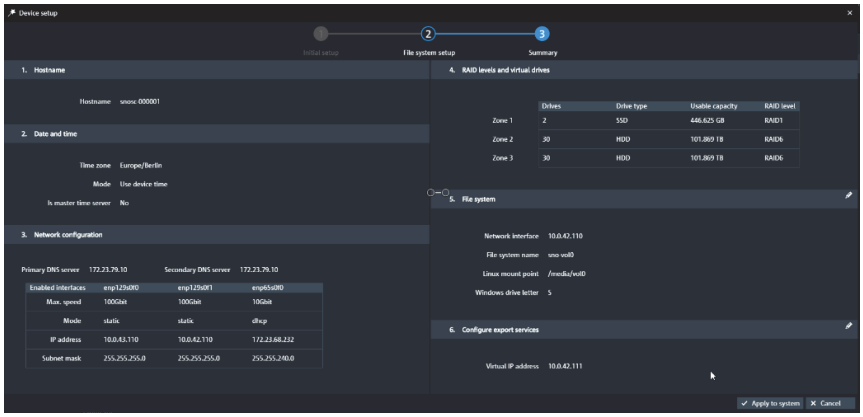


Network interface (IP)	Select the network interface for your file system. The connection is usually established via the 100Gbit (optionally 200Gbit) interfaces.
File system name	Provide a name for your file system.
Linux mount point	Define the mount path for this file system at your connected Linux native clients.
Windows drive letter	Define the drive letter designation for the your file system at your connected Windows native clients.

10. Define a virtual IP address for the export services (e.g. via Samba). It is already preset to the same subnet domain, thus you have to provide only the last three digits.



11. A summary is presented in the last step with the option to make changes to the file system and virtual IP configuration settings.

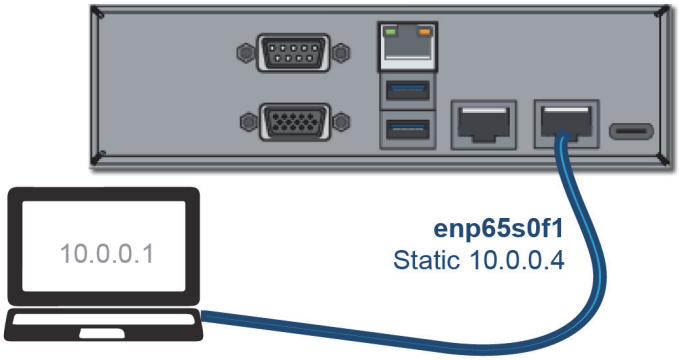


The SpycerNode SC hardware is now properly installed and ready for first use.

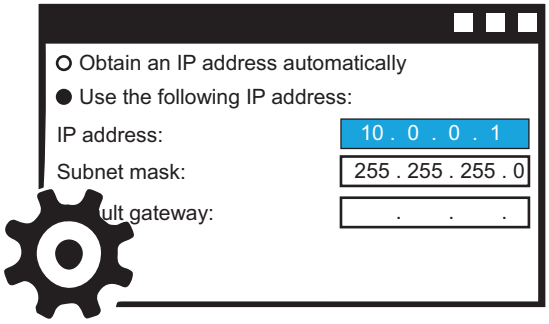
Using Static IP

Perform the following steps:

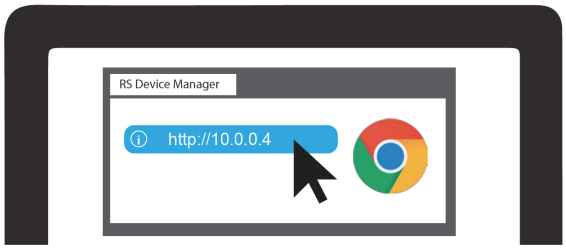
1. Connect port **ENP65S0F1** to a PC/Mac.



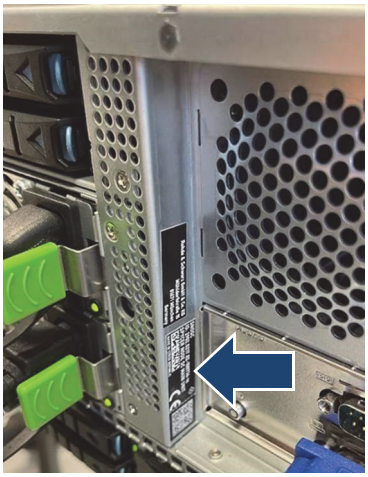
2. Change the IP for the connected network interface in the network settings of your PC/Mac to „10.0.0.1“.



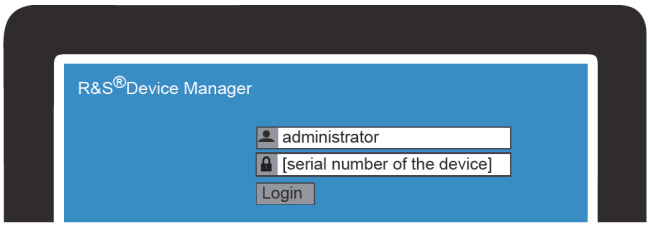
3. Enter the static IP in the Chrome web browser to open the R&S®Device Manager on your local system. (i.e. http://10.0.0.4).



4. Locate the serial number of the device which is to be found at the rear of system.

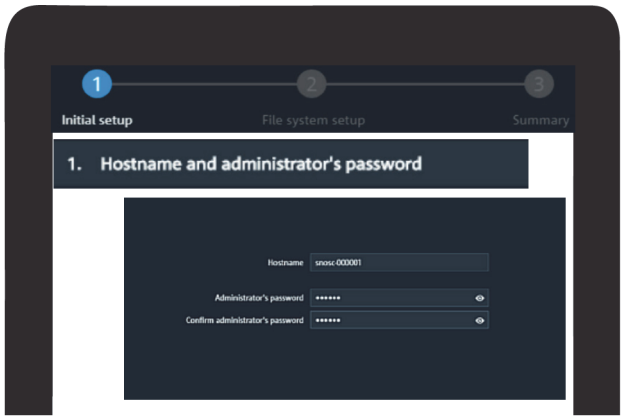


5. The first time you log in, enter the following credentials:
   USERNAME: **administrator**
   PASSWORD: **[serial number of the device]**

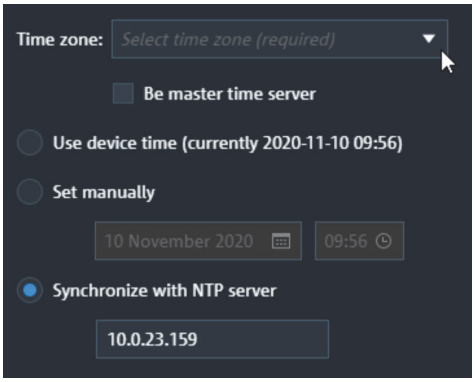


   ▸ The Easy Setup Wizard of the Device manager initiates automatically right after the first login.

6. Define hostname and password for the system:



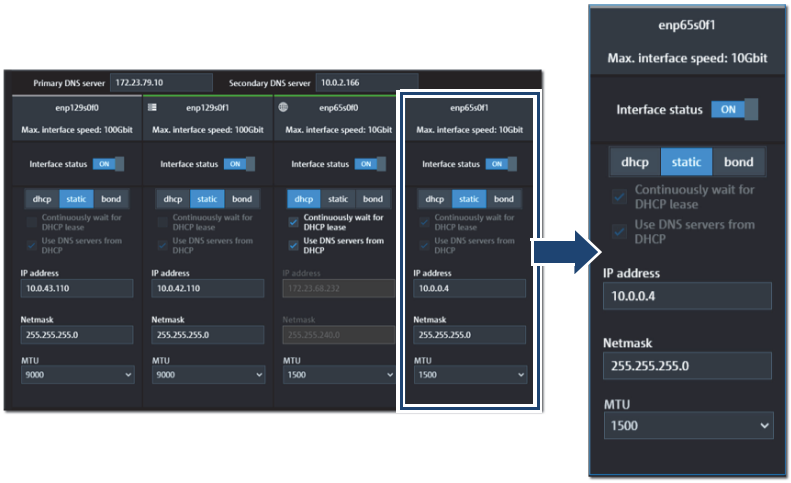
7. Specify date and time settings for the system.



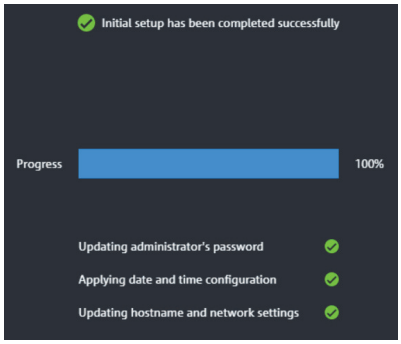
Time zone	Select your time zone from various predefined selection options.
Be master time server	Set the checkbox if you want to designate this particular system as the main NTP server within your local network.
Use device time	Read the current date and time of the device and set it as default.

Set manually	Manual entry of the date and time settings.
Synchronize with NTP server	Synchronize the date and time settings with a central NTP server from you local network.

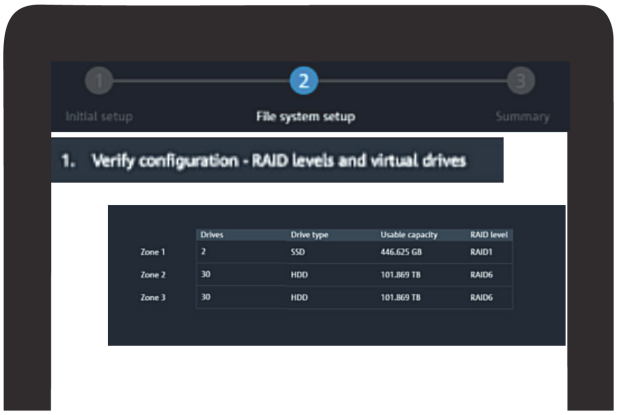
8. The network settings are displayed in the outermost network port section on the right (enp65s0f1). The **IP ADDRESS** is set to **`10.0.0.4`** and the **NETMASK** to **`255.255.255.0`**. If you wish to use another static IP address you can enter it here into the IP address field.



▸ With this step, the first part of the setup is completed:

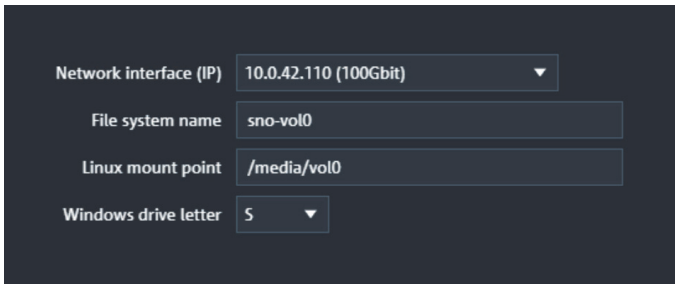


9. In the next installation phase, the file system configuration is carried out. First, the metadata drives and the installed storage capacity are displayed.



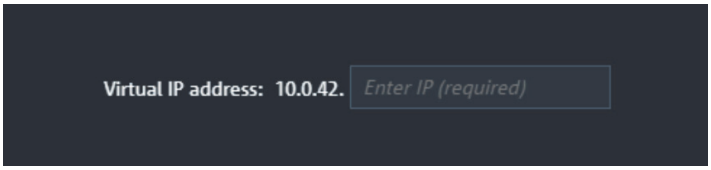
Zone 1	Shows the number of metadata drives, the drive type, the capacity and RAID level.
Zone 2 / Zone 3	Shows the installed storage drives type, their capacity and the level of RAID protection. Each zone represents a single drive set which consists always of 30 drives. A system with half the capacity will have only one zone populated.

10. In the next step you select the interface for your storage network connection.

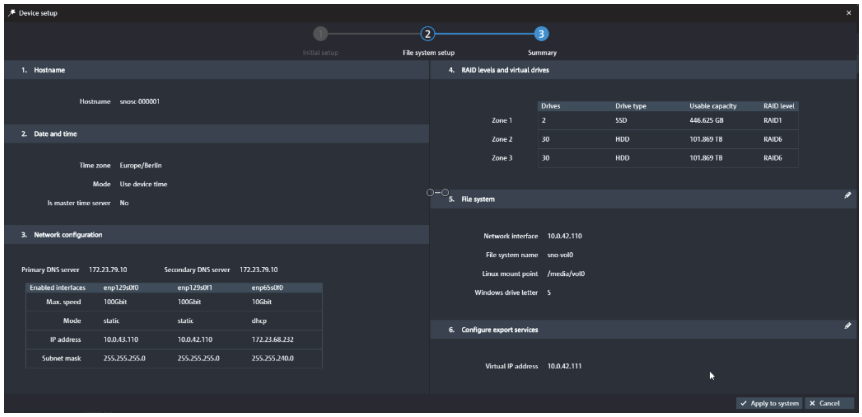


Network interface (IP)	Select the network interface for your file system. The connection is usually established via the 100Gbit (optionally 200Gbit) interfaces.
File system name	Provide a name for your file system.
Linux mount point	Define the mount path for this file system at your connected Linux native clients.
Windows drive letter	Define the drive letter designation for the your file system at your connected Windows native clients.

11. Define a virtual IP address for the export services (e.g. via Samba). It is already preset to the same subnet domain, thus you have to provide only the last three digits.



12. A summary is presented in the last step with the option to make changes to the file system and virtual IP configuration settings.



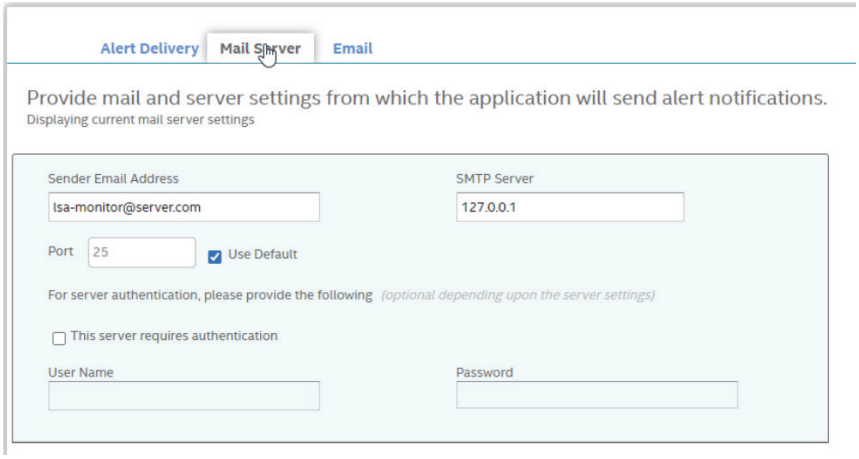
The SpycerNode SC hardware is now properly installed and ready for first use.

Setting Up Mail Notifications in Broadcom UI

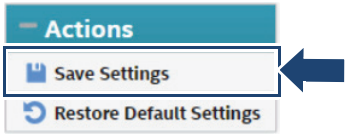
Based on your configuration, the email notifications are delivered to your inbox. In the email notification, besides the event's description, the email also contains system information and the controller's image details. Using this additional information, you can determine the system and the controller on which the fatal error occurred.

Perform the following steps:

1. Select **Settings** in the Server dashboard.
   - The **ALERT SETTINGS** window appears with the default alert delivery methods for each severity level.
2. Click the **Mail Server** tab.
   - The Mail Server tab appears and displays the current mail server settings.



3. Enter a sender's email address in the **SENDER EMAIL ADDRESS** field, or edit the existing sender email address.
4. Enter your SMTP server name/IP address in the **SMTP SERVER** field, or edit the existing details.
5. Clear the **USE DEFAULT** check box to enter the desired port number in the **PORT** field.
6. (Optional) On your SMTP server, if the Auth Login feature is enabled and if you want to enable this feature on the LSI Storage Authority software, select the **THIS SERVER REQUIRES AUTHENTICATION** check box and specify the authentication details in the **USER NAME** and **PASSWORD** fields.
7. Click **Save settings** to confirm.



Mail notifications have been set up.

Installing the Spectrum Scale Client

This section describes the spectrum scale client installation on your system.

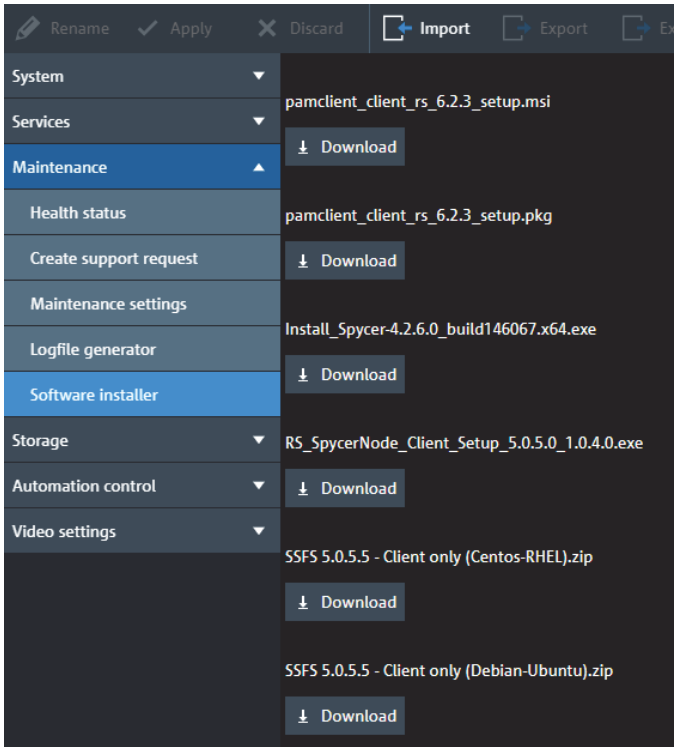
The following topics are covered:

Installing under Linux

Preparations

Perform the following steps:

1. In the R&S®Device Manager navigate to **Maintenance > Software installer**, and download the corresponding SSFS installer package.



2. Install the packages:

```
yum -y install gpfs.base gpfs.docs gpfs.ext
gpfs.gpl gpfs.gskit gpfs.msg.en_US gpfs.gui
gpfs.gss.pmsensors gpfs.gnr gpfs.license.ds
```

3. Install the following package:

```
yum -y install gpfs.gplbin-3.10.0-514.el7.x86_64-
5.0.1-0.x86_64
```

The kernel version in the package must be equal to the kernel version of your system (e.g. 3.10.0-514). The version can be queried with **`uname -a`**. If the system has a different kernel version the **`gpfs.gplbin`** package must be generated with **`mmbuildgpl --build-package.`**

Repositories

The embedding of the necessary repositories is important for a successful installation.

The package include the following files:

```
[DIR] ganesha_debs/ 2019-02-05 17:27 -
[DIR] ganesha_rpms/ 2019-02-05 17:27 -
[DIR] gpfs_debs/ 2018-10-25 07:19 -
[DIR] gpfs_rpms/ 2018-10-25 07:18 -
[DIR] gui/ 2018-10-25 07:14 -
[DIR] installer/ 2018-10-25 07:19 -
[DIR] license/ 2019-02-05 17:27 -
[ ] manifest 2018-10-25 07:20 35K
[DIR] object_debs/ 2019-02-05 17:27 -
[DIR] object_rpms/ 2019-02-05 17:27 -
[DIR] smb_debs/ 2019-02-05 17:27 -
[DIR] smb_rpms/ 2019-02-05 17:27 -
[DIR] tools/ 2019-02-05 17:27 -
[DIR] zimon_debs/ 2019-02-05 17:27 -
[DIR] zimon_rpms/ 2019-02-05 17:27 -
```

Embed all directories with **`.rpms`** as local or central repository.

Example: Creating a Repository

For every repository one **.repo** file must be created. The following example shows the creation of a local repository (.rpms).

Perform the following steps:

1. Change directory:

```
/etc/yum.repos.d/
```

2. Create file:

```
touch ganesha_rpms.repo
```

3. Open the .repo file with an editor.
4. Enter the description of the configuration into the file:

```
[ganesha_rpms]
name=ganesha_rpms
baseurl=file:///<path to repository>
enabled=1
gpgcheck=0
```

Installing under Windows

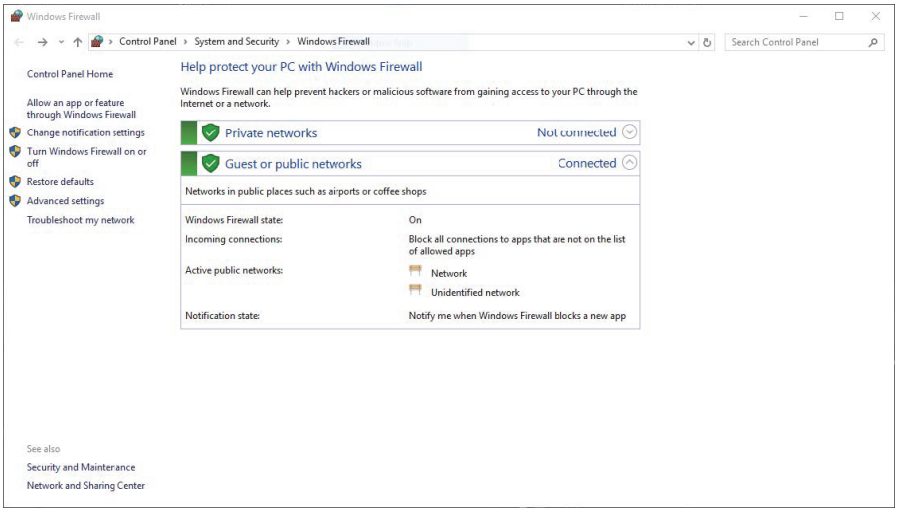
Preparations

Perform the following steps:

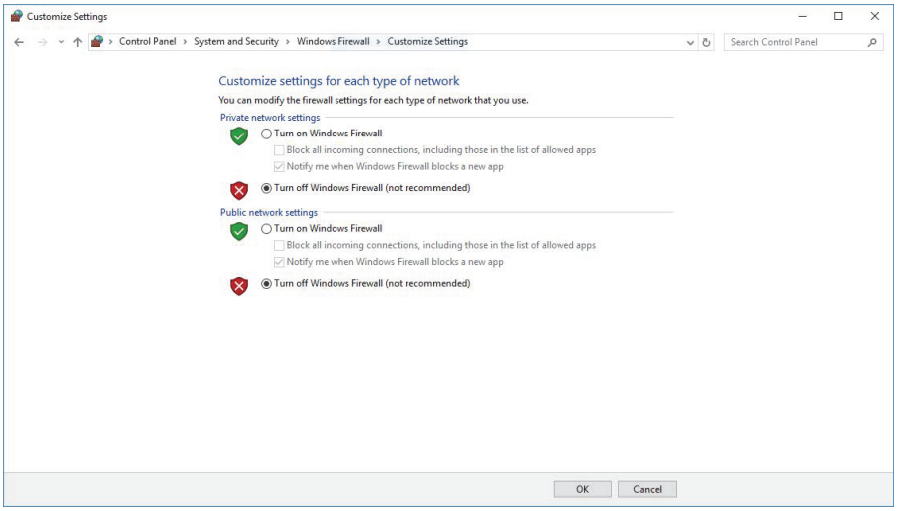
If you are unfamiliar with these settings, contact your system administrator.

Note that creating a new user, requires a current account with administrator rights.

1. Open the Windows Control Panel to disable the Windows firewall.



2. Select "Turn Windows Firewall on or off".
3. Select "Turn off Windows Firewall" in "Private network settings" and in "Public network settings".



4. Confirm your changes with "OK".
5. Disable SECURE BOOT in the mainboard BIOS.
6. Unzip the file **`GPFS_Client.zip`** to **`C:\`**

Installing the Mellanox Network Card

Perform the following steps:

1. Install the network card according to the Mellanox installation manual.
2. Change the directory to:

```
C:\GPFS_Client\Network\Mellanox\MCX556AECAT-DRV
```

3. In administration mode execute:

```
MLNX_WinOF2-2_0_50000_All_x64
```

4. Follow the instructions on screen.
5. Select "Complete Installation".

If a firmware update is necessary it is done automatically through the installation routine.

6. Change the directory to:

```
C:\GPFS_Client\Network\Mellanox\MCX556AECAT_FW_Tools
```

7. In administration mode execute:

```
WinMFT_x64_4_10_0_104
```

8. Follow the onscreen instruction of the installation routine.
9. Open a Windows command shell (cmd) in administrator mode.
10. Change the corresponding directory:

```
cd c:\programfiles\mellanox\winmft
```

11. Change the port type to **`Ethernet`** by using the following command:
    ➔ For a dual Mellanox network card:

```
mlxconfig -d /dev/mst/mt4119_pciconf0 set
LINK_TYPE_P1=2 LINK_TYPE_P2=2
```

    ➔ For a single port Mellanox network card:

```
mlxconfig -d /dev/mst/mt4119_pciconf0 set
LINK_TYPE_P1=2
```

12. Type in **y** to apply the Ethernet mode.

```
Device #1:
----------

Device type:    ConnectX5
PCI device:     /dev/mst/mt4119_pciconf0

Configurations:          Current New
...
         LINK_TYPE_P1    IB(1)   ETH(2)
         LINK_TYPE_P2    IB(1)   ETH(2)
...
Apply new Configuration? ? (y/n) [n] : y
Applying... Done!

-I- Please reboot machine to load new configurations.
```

Now you can proceed with the network settings.

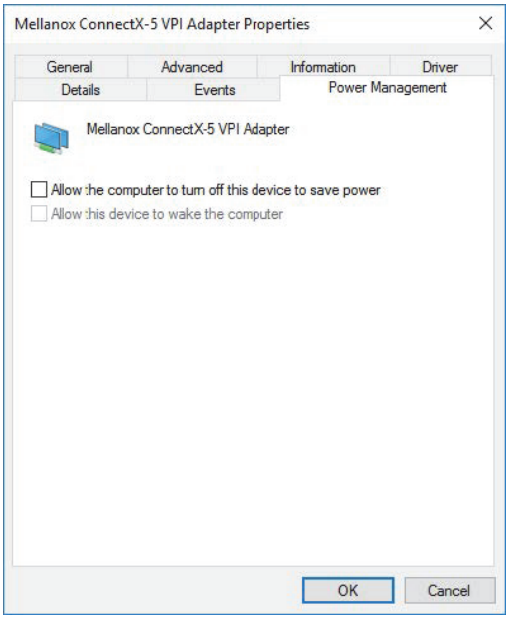
Mellanox Network Card Configuration

If you are unfamiliar with these settings, contact your system administrator.

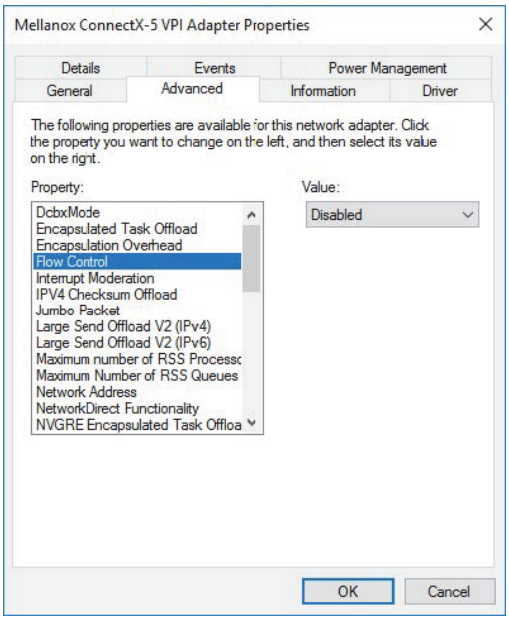
Perform the following steps:

1. Open the "Mellanox ConnectX-5 VPI Adapter Properties".
2. Disable "IPv6" in the Ethernet properties.
3. Set a static IPv4 network address that is in the address area of your GPFS cluster.

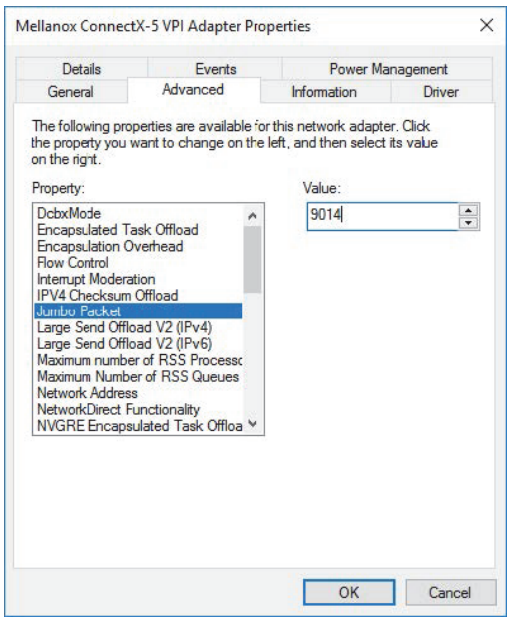
4. Disable "Power Management".



5. Disable "Flow Control".



6. Set the "Jumbo Packet" to **9014**.

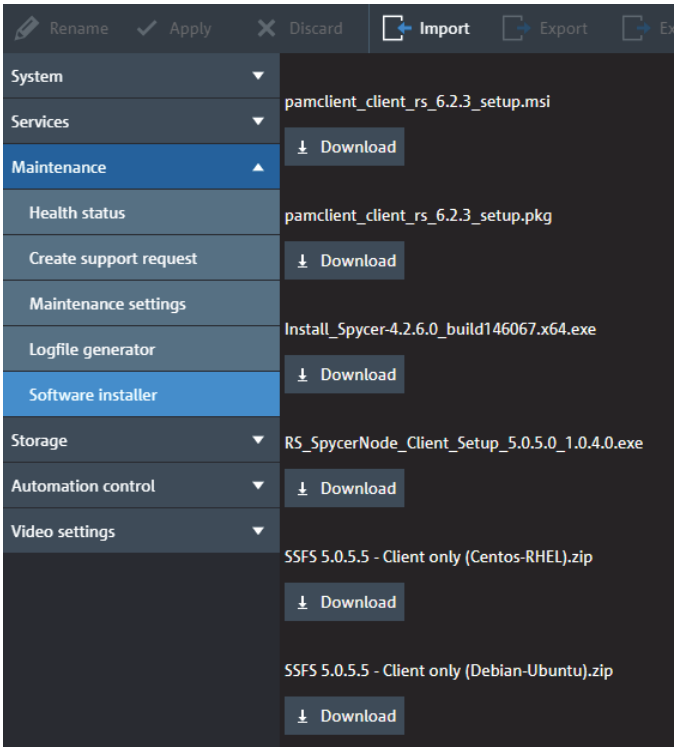


The configuration of the network card is complete.

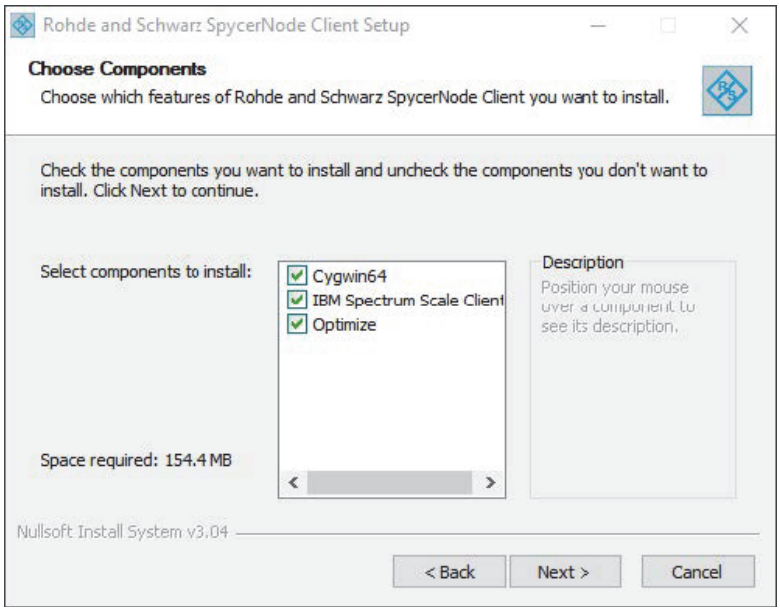
Installing Spectrum Scale

Perform the following steps:

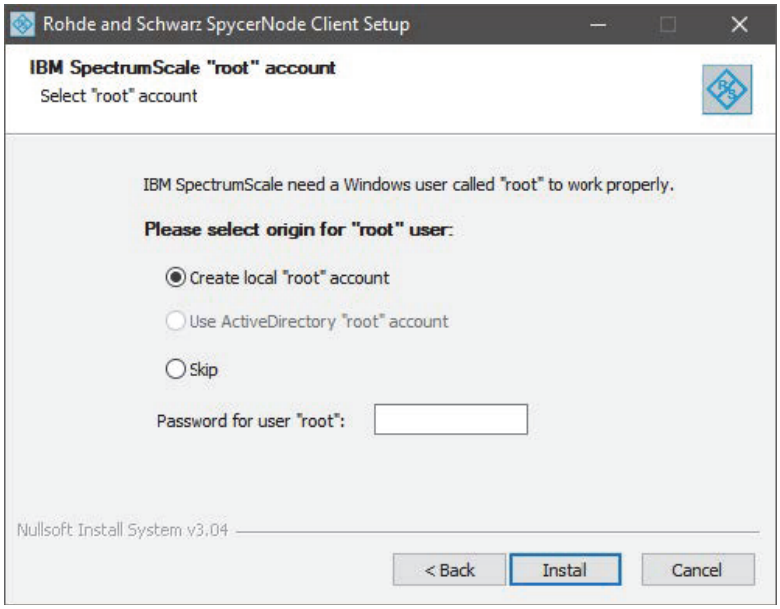
1. In the R&S®Device Manager navigate to **Maintenance > Software installer**, and download the corresponding SSFS installer package.



2. Execute the client installer on your client device and accept th license agreement.
3. Select all components to install.



4. Create a local "root" account with password if this hasn't been done.



5. Confirm with "Install".

The Spectrum Scale Client installation has been successfully completed.

Adding a Native Spectrum Scale Client

Perform the following steps:

1. Start Spectrum Scale on the client.
2. Copy the public SSH keys from all system controllers to the client:

```
#> ssh-copy-id -o StrictHostKeyChecking=no <client
hostname>
```

3. Login to a SpycerNode controller that is already part of the existing cluster to add the client system to the cluster.

```
#> mmaddnode -N <client hostname> #> mmchlicense
client --accept -N <client hostname>
```

4. Change client specific Spectrum Scale settings.
5. Set the pagepool size.

```
#> mmchconfig pagepool=16G -N <client hostname> -i
```

The recommended pagepool size for is 16 GB. The minimum size for the pagepool is 2 GB.

6. (Optional if required) Change the drive letter of the file system (Windows clients).
   ➔ Unmount the file system from all nodes first.

```
#> mmumount -a
```

   ➔ Change the drive letter (add ":" to the letter, e.g. "S:").

```
#> mmchfs sno-vol0 -t <drive letter>
```

   ➔ Re-mount the file system on all nodes.

```
#> mmmount -a
```

Done.

Removing a Native Spectrum Scale Client

Perform the following steps:

1. Login to a R&S storage system that is part of the cluster.
2. Shutdown Spectrum Scale on the client node.

```
#> mmshutdown -N <client hostname>
```

3. Remove the client from the cluster.

```
#> mmdelnode -N <client hostname>
```

Done.

Operation

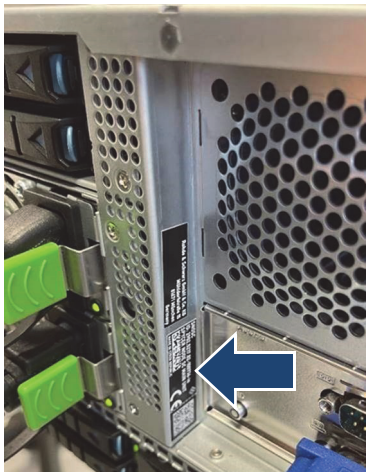
This chapter includes the following section:

Using the R&S®Device Manger

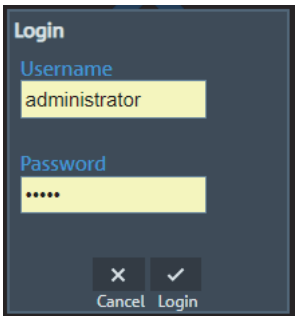
For installation and system monitoring purpose use the R&S®Device Manager, the convenient solution also developed by Rohde & Schwarz.

Perform the following steps:

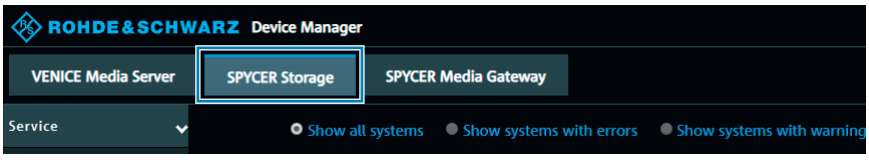
1. Enter the host name of the system in the Chrome web browser to open the R&S®Device Manager on your local system:
   `http://snosc-[serial number]`
   The host name itself consists of the keyword snosc, followed by a dash, and the serial number of the system. The label with serial number is located at the rear panel.



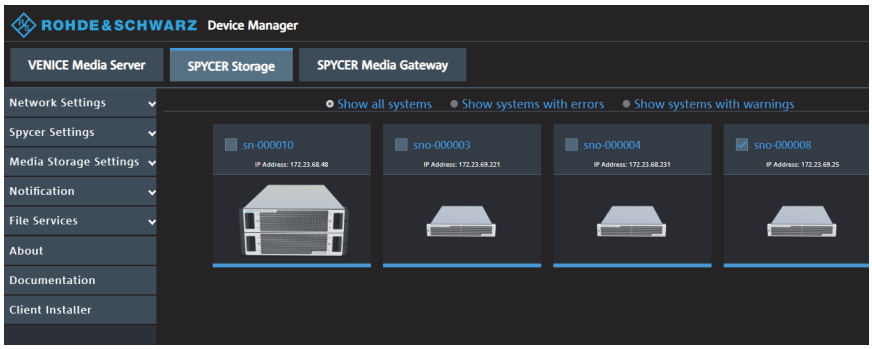
2. Select **Login** to get access to all configuration options.
   ▶ The **LOGIN** window opens.
3. Enter username and password as defined in the Easy Setup Wizard, see "Initial Setup" (page 39).



4. Select the **SPYCER STORAGE** tab.



5. Select the corresponding system (host name) to get access to the menu options.



After login the complete menu becomes visible.

System Monitoring

The R&S®Device Manager allows you to monitor and query the state of the SpycerNode SC and single parts of the hardware. You will be able to define critical values and configure an e-mail notification as well. Remote management (IPMI) is also possible via the R&S®Device Manager.

There are various methods to monitor the system:

- Monitoring through SNMP (page 66)
- Monitoring through the Device Manager (page 68)
- Monitoring the Drives via Broadcom UI (page 69)

Monitoring through SNMP

The Simple Network Management Protocol (SNMP) is a standard internet protocol for device management in IP networks. SNMP allows you to e.g. monitor and query the state of several SpycerNode SC devices in a network or single parts of the hardware.

SpycerNode SC provides a **`RS-FBMS-IPMI-V1-MIB`** and a **`RS-FBMS-RAID-V1-MIB`** file that give you the opportunity to query the state of the system or parts of it, using SNMP.

Explanation of the OIDs

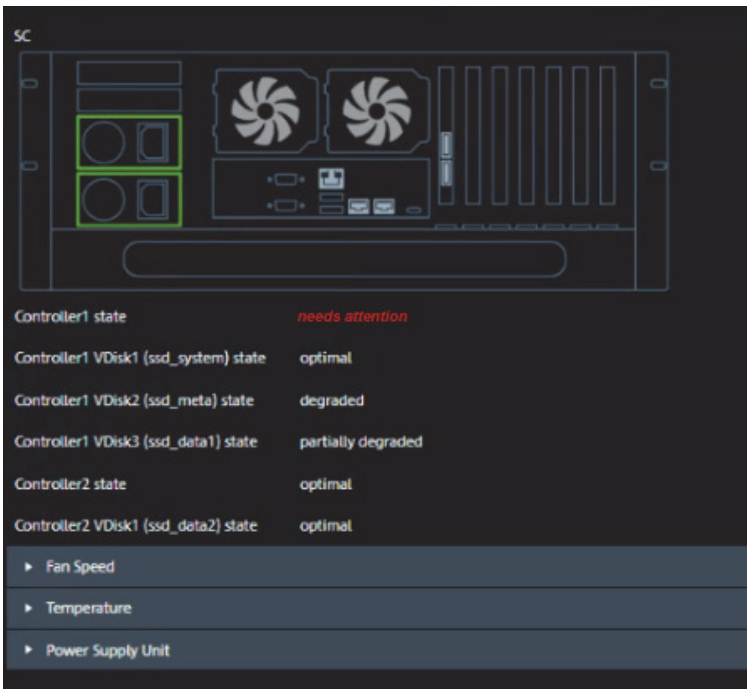
When using a monitoring software, you will have to enter all OIDs once to be able to monitor the hardware‘s state continuously.

File	OIDs	Object	Value
RS-FBMS-IPMI-V1-MIB	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10000.1.1.0	Fan1 name	Fan description
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10000.1.2.0	Fan1 speed	RPM (rounds per minute)
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10000.1.3.0	Fan1 state	ok, warning, failure, unknown
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10000.2.1.0	Fan2 name	Fan description
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10000.2.2.0	Fan2 speed	RPM (rounds per minute)
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10000.2.3.0	Fan2 state	ok, warning, failure, unknown
	[…]	[…]	
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10001.1.1.0	Temperature 1 name	temperature description
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10001.1.2.0	Temperature 1 value	temperature in °C
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10001.1.3.0	Temperature 1 state	ok, warning, failure, unknown
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10001.2.1.0	Temperature 2 name	temperature description
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10001.2.2.0	Temperature 2 value	temperature in °C
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10001.2.3.0	Temperature 2 state	ok, warning, failure, unknown
	[…]	[…]	
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10002.1.0	PSU 1 state	ok, warning, failure, unknown
	.1.3.6.1.4.1.2566.127.1.4.1.8.1.2.10002.2.0	PSU 2state	

File	OIDs	Object	Value
RS-FBMS-RAID-V1-MIB	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.1.0	RAID controller 1 state	ok, warning, failure, unknown
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.2.1.0	RAID controller 2 state	
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.6.0	RAID controller 1 BBU state	ok, warning, failure, unknown
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.2.6.0	RAID controller 2BBU state	
	[…]	[…]	
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.9.1.2.0	Virtual disk 1 name	Name of virtual disk 1, e.g. “123456_system”
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.9.1.4.0	Virtual disk 1 state	optimal/degraded/offline
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.9.2.2.0	Virtual disk 2 name	Name of virtual disk 2, e.g. “123456_meta”
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.9.2.4.0	Virtual disk 2 state	optimal/degraded/offline
	[…]	[…]	
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.8.1.4.0	Physical disk 1 state	online/offline/ unconfigured-Good/rebuild
	.1.3.6.1.4.1.2566.127.1.4.1.8.2.2.10000.1.8.2.4.0	Physical disk 2 state	

Monitoring through the Device Manager

The Health Status panel monitors critical system components in realtime and displays the gathered information. The panel can be accessed by selecting the corresponding system and navigating to **Maintenance > Health status**.



Health Status Panel

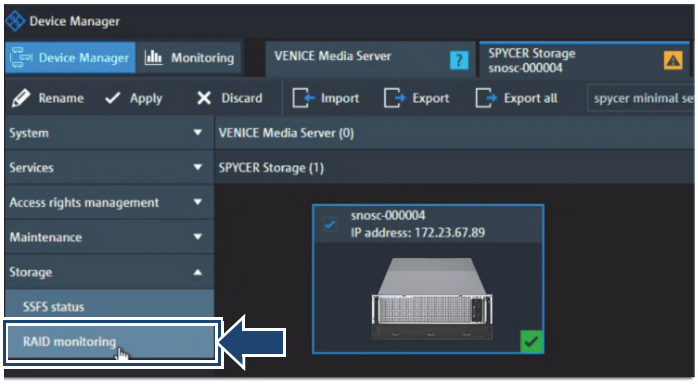
Each component category is separated in a dropdown menu and can be extended to view the details on any single component. Each dropdown bar signals the status of the contained components - OK (green), Warning (yellow), Error (red).

Monitoring the Drives via Broadcom UI

Perform the following steps:

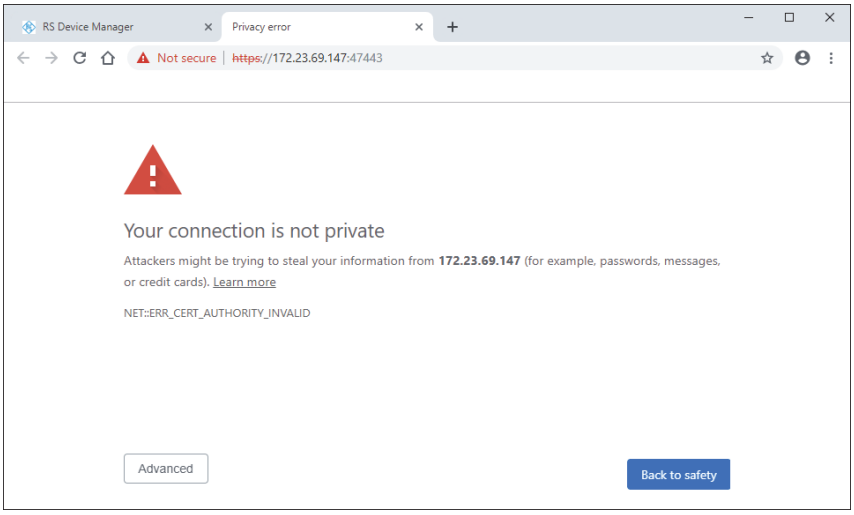
1. Open the R&S®Device Manager on your local system as described in "Using the R&S®Device Manger" on page 64.
2. Navigate to the storage section and make sure your system is selected.

3. Select **Storage > RAID monitoring** in the settings menu.

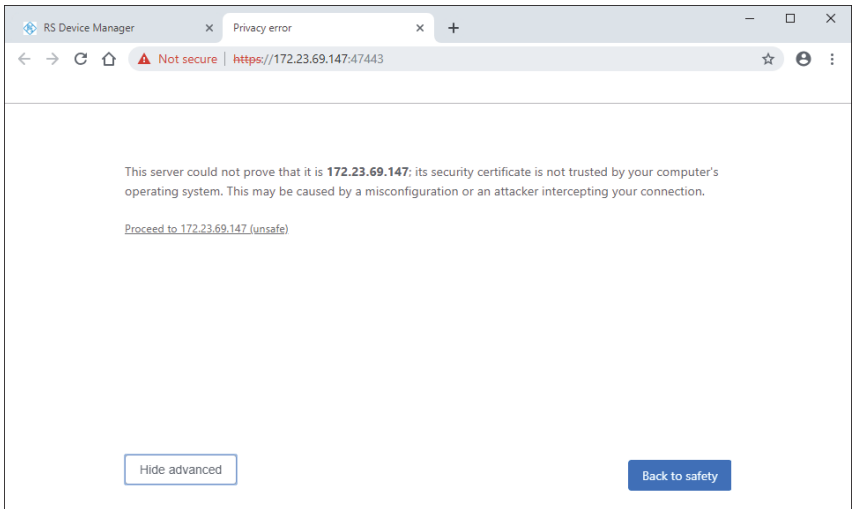


▸ A new tab opens.

4. If you open this tab for the first time you will get a Privacy error in the browser. Select „Advanced“ to continue.

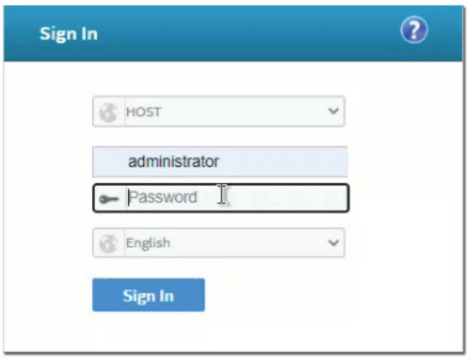


5. Select „Proceed to xxx.xx.xx.xxx (unsafe) to continue.

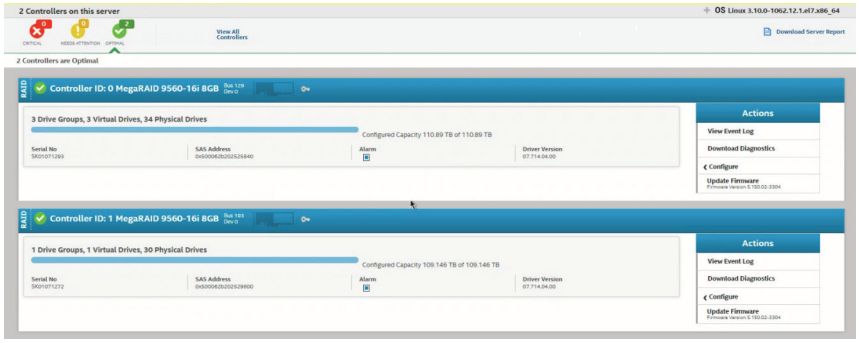


▸ The monitoring interface is now accessible.

6. Enter the username and password as defined in "Initial Setup" (page 39) and confirm with the **Sign In** button.

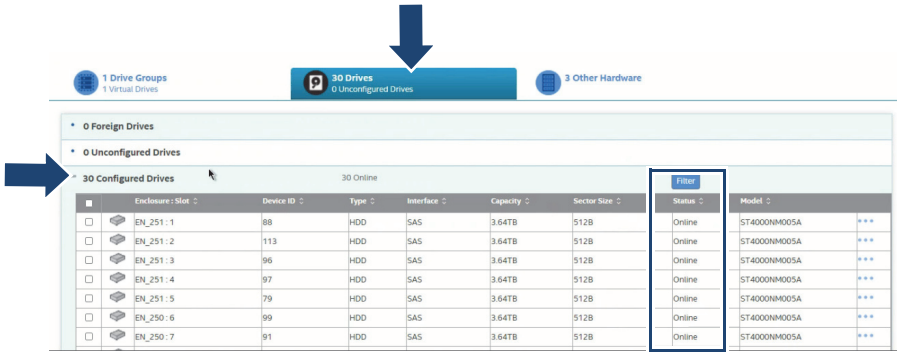


▶ The Web UI Application for the installed controllers opens. It allows you to monitor and manage the storage drives in use through the controllers.



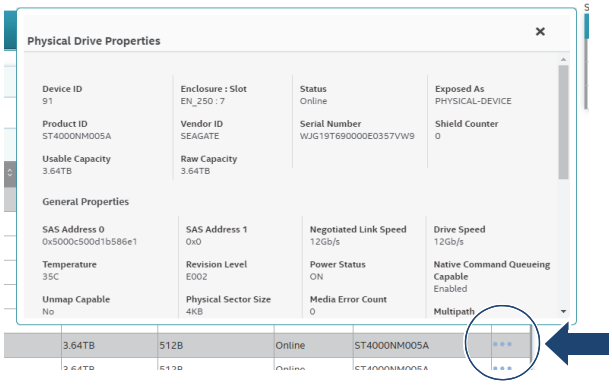
A SpycerNode SC with two populated LUNs will display two controllers. One of them will also be responsible for the system and metadata drives.

7. Choose a controller to check its status. Select the **Drives** tab and expand the **Configured drives** menu.



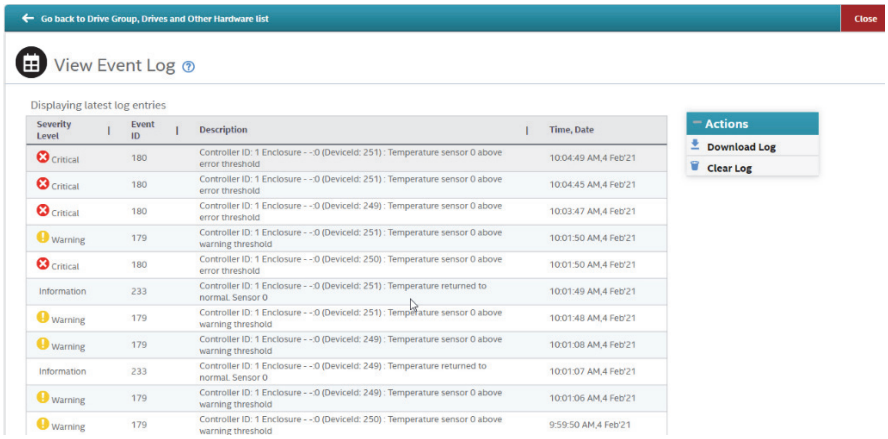
▶ The status of the drives is displayed under the **STATUS** column.

8. To get more information, select one of the drives and click the Physical Drive Properties button (three blue dots).



9. To locate a particular drive, select the drive you want to identify in the Controller dashboard, and navigate to **Element(s) actions > Start locating**.
   - The LED status indicator on the corresponding physical drive will start blinking.

10. To get access to all severity events, in the Controller dashboard navigate to the **ACTIONS** panel and click **View Event Log** to view the event log.



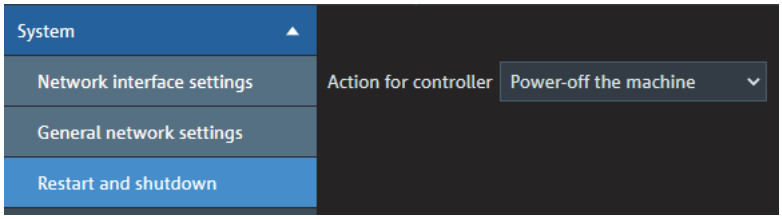
   - Each message that appears in this log has a severity level to indicate the importance of the event (severity), an event ID, a brief description, and a date and timestamps (when it occurred). The event logs are sorted by date and time in chronological order.

Done.

Shutting down the System

Perform the following steps:

1. Open the R&S®Device Manager on your local system as described in "Using the R&S®Device Manger" on page 64.
2. Select **Restart and Shutdown** in the SYSTEM menu.



3. Select the respective method and apply your setting.

The system is shut down.

Shutting down the System

Maintenance

This chapter is divided into the following sections:

Safety Instructions

NOTICE

Electronic discharge

Computer hardware contains components that are sensitive to electrostatic discharge. If you touch them without precautionary measures, they can be destroyed.

It is recommended that you fit and check a suitable antistatic wrist or ankle strap and observe all conventional ESD precautions when handling plug-in modules and components. Avoid contact with midplane components and module connectors.

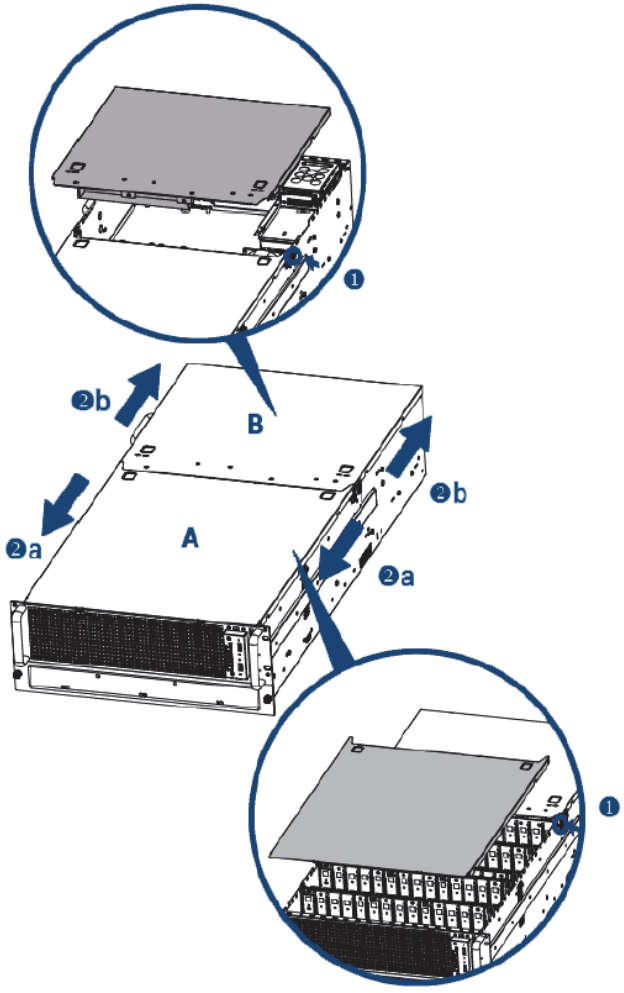
Always have available a replacement or blank module before removing the old module. When you replace a module, you must never leave an empty bay in the rear of the enclosure.

Removing the Top Cover

This section guides you through the process of opening the casing. This is required e.g. in case you have to replace a defective storage drive or a cooling fan.

Perform the following steps:

1. Simultaneously press the cover release buttons on both sides of the casing.
2. Push and slide the top covers in the direction shown. Push in the direction of 2a to open cover A; push in the direction of 2b to open cover B.
3. Lift the covers to remove them and set them aside.



4. Reverse the steps above to mount the top cover back in place.

The top cover is now removed.

Replacing a Power Supply Unit

The redundant power supply provides the system with power. It is a reliable and enduring part of the system because it consists of several independent power supply units: Even if one fails the others will still offer enough power to keep the system working.

NOTICE

System Damage

The system can be operated with one power supply unit out of order. However, if another one fails, a continued operation of the system cannot be guaranteed.

Exchange a failed power supply unit immediately.

Each power supply unit in the R&S system is hot-swappable, so you can safely replace it with the system running.

⚠ CAUTION

Danger of Injury

Do not reach inside the system when removing a power supply unit or when the unit is out of the system.

NOTICE

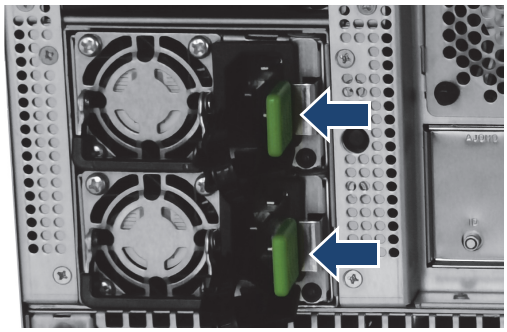
System Damage

Third-party spare parts might damage your system.

Only use original manufacturer spare parts.

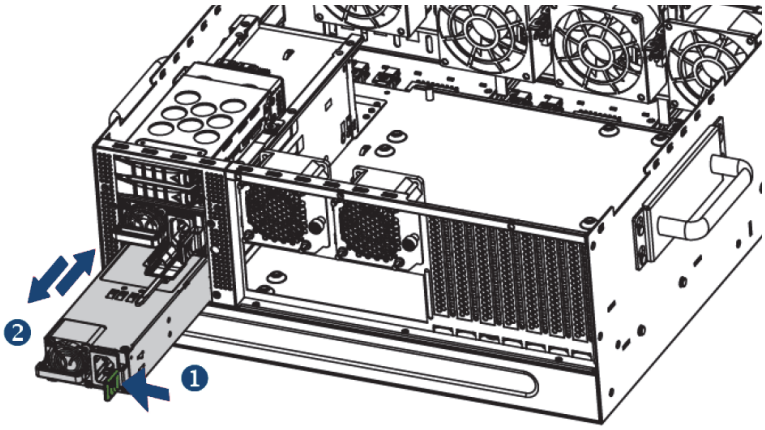
Perform the following steps:

1. Press the ejector to release the power supply unit.



2. Pull the handle to remove the module out of the casing.

3. Insert the new power supply module into the casing. Ensure that the module is properly hooked within the cage.

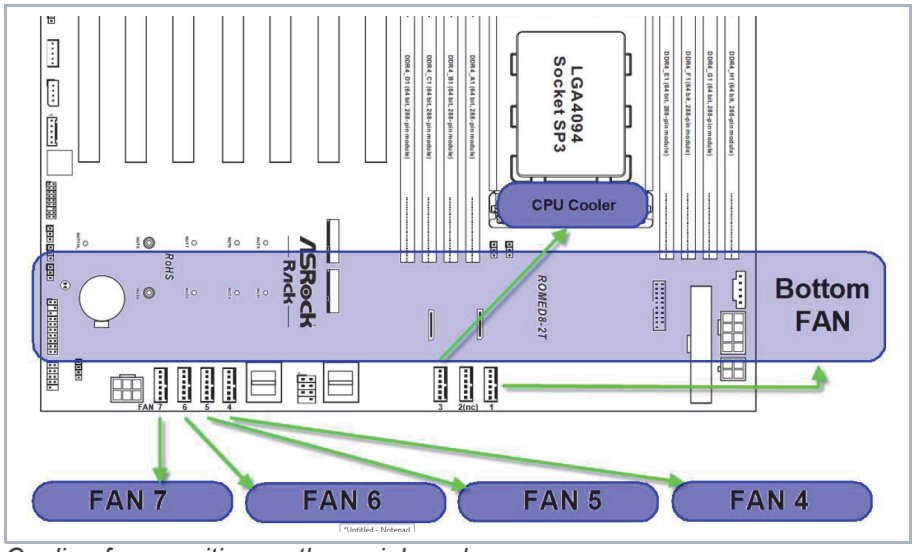


Fan Maintenance

To cool the many storage disks installed in the system as well as the other electronic parts, the system is equipped with several fans that can be easily exchanged in case of a failure.This section describes how to monitor the internal fans and how to exchange them in case of failure.

Monitoring the Fans

The state of the internal fans is monitored by and displayed in the Device Manager. To get access to the fan monitoring navigate to **Maintenance > Health status** and expand the **Fan speed** drop-down section. The following table and illustration will help you determine the physical location of each fan displayed in the Health Panel.



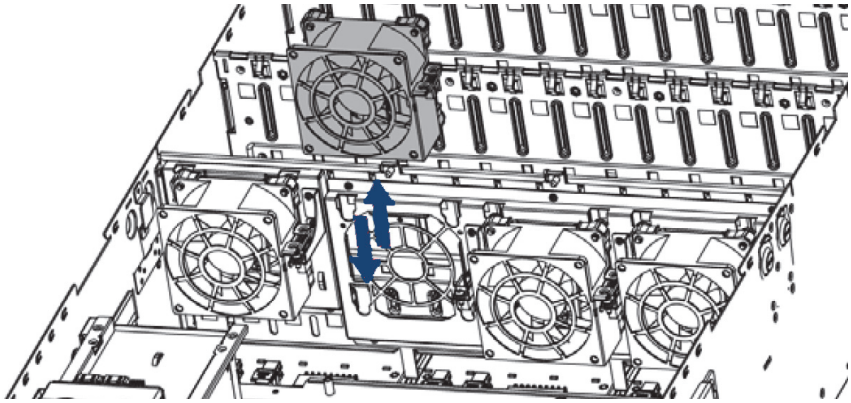
Cooling fans position on the mainboard

Physical connector on main-board	Physical location of the fan	Naming in the Health Status panel (Device Manager)	Label on the connection cable
1	5 bottom fans	FAN1	bottom
2	not connected	not displayed	not available
3	CPU Cooler	FAN3	no label
4	FAN4	FAN4	FAN1
5	FAN5	FAN5	FAN2
6	FAN6	FAN6	FAN3
7	FAN7	FAN7	FAN4

Replacing a Fan

Perform the following steps:

1. Open the casing of the system as described in "Removing and Mounting the Top Cover" (page 77).
2. Unplug the cables and connectors of the fan to the motherboard.
3. Pull the fan from the node. Make sure to carefully dislodge the rubber connectors from the attached bracket.



4. Insert the replacement fan into the node. Make sure to align the rubber connectors to the appropriate slot in the bracket.

Done.

Replacing a Drive

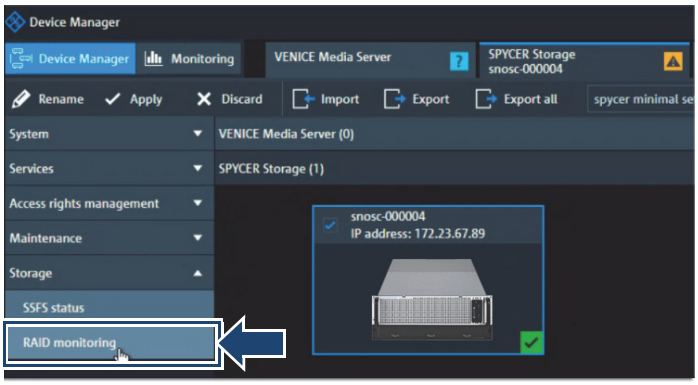
The following topics are covered:

- Identifying a Defective Drive (page 82)
- Removing a Defective Drive (page 85)
- Installing a New Drive (page 86)

Identifying a Defective Drive

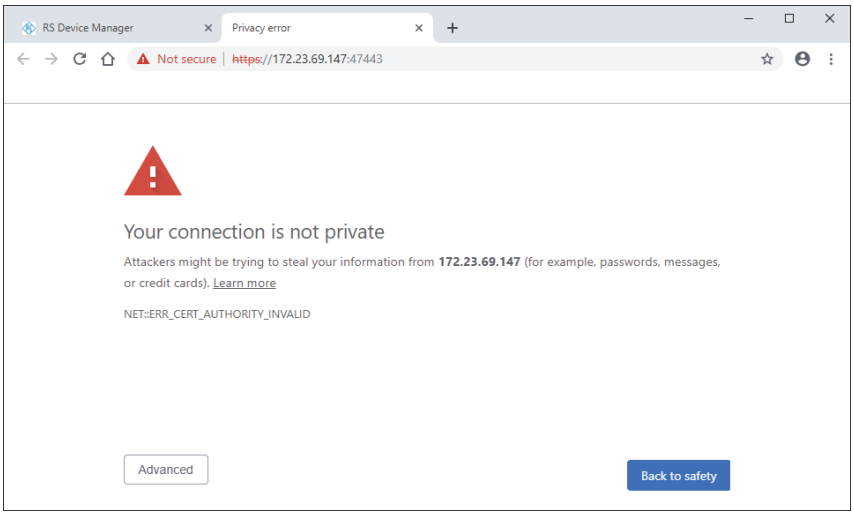
Perform the following steps:

1. Open the R&S®Device Manager on your local system as described in "Using the R&S®Device Manger" on page 64. Navigate to the storage section and make sure your system is selected.
2. Select **Storage > RAID monitoring** in the settings menu.

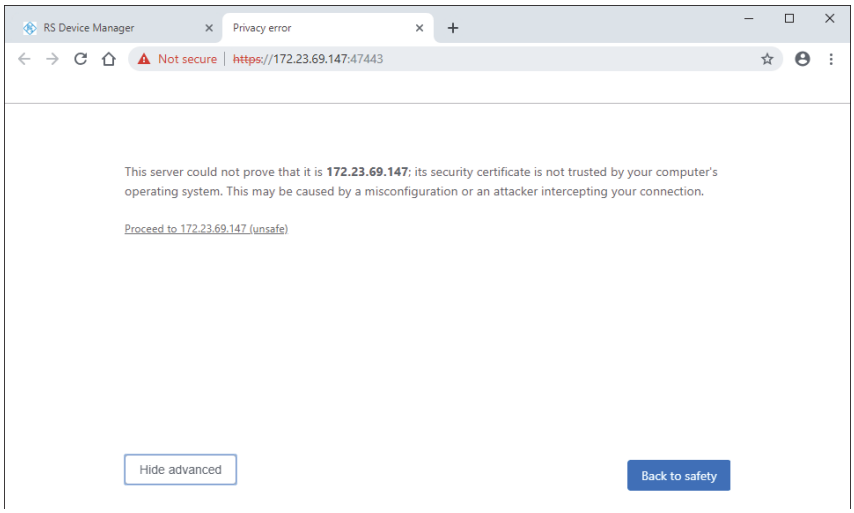


▶ A new tab opens.

3. If you open this tab for the first time you will get a Privacy error in the browser. Select „Advanced“ to continue.

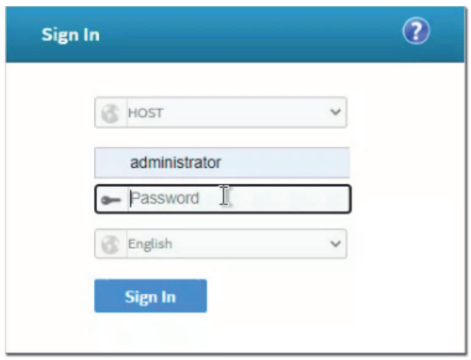


4. Select „Proceed to xxx.xx.xx.xxx (unsafe) to continue.

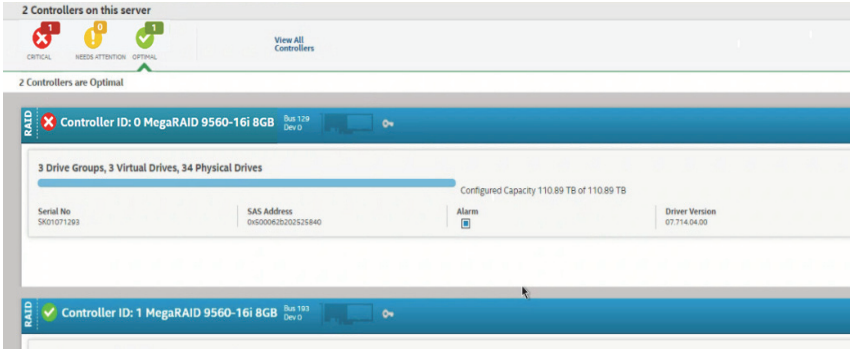


- The monitoring interface is now accessible.

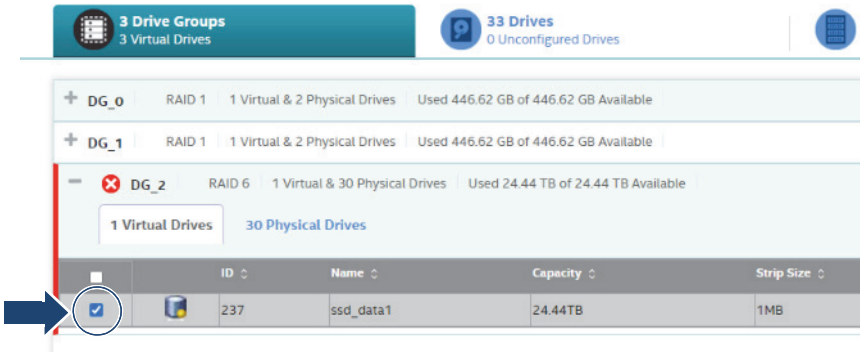
5. Enter the username and password as defined in "Initial Setup" (page 39) and confirm with the **Sign In** button.



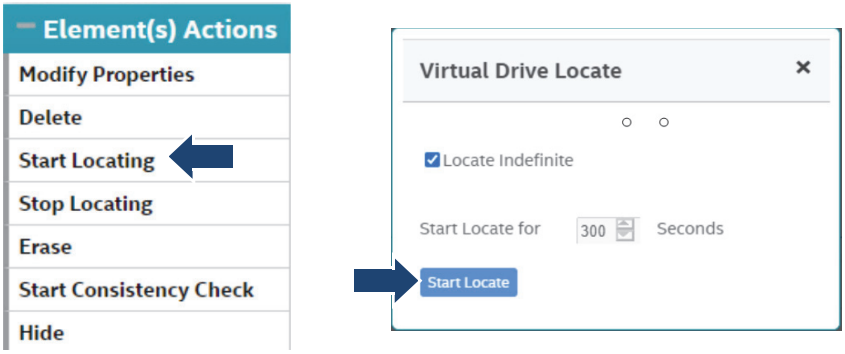
- The Web UI Application for the installed controllers opens. It allows you to monitor and manage the storage drives in use through the controllers.
- If there is a disk failure or malfunction, the pertaining controller will indicate an error.



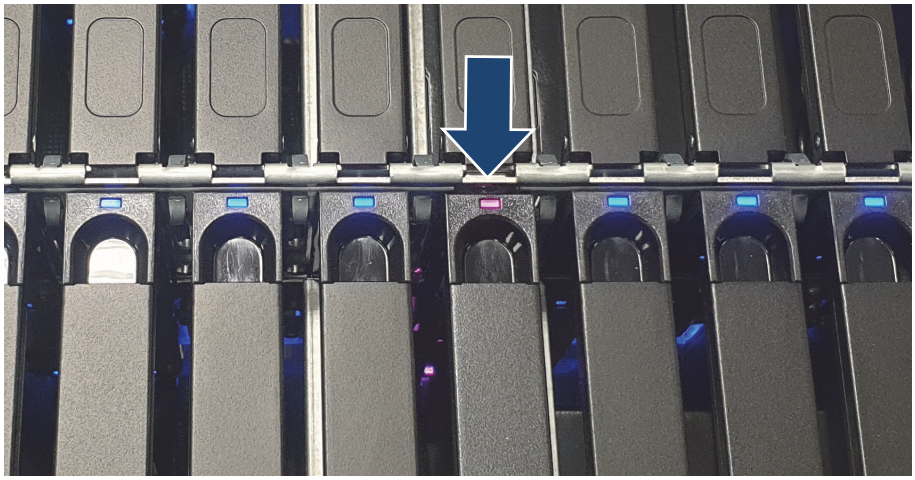
6. Open the controller displaying the error and navigate to the Drive Groups tab. Expand the RAID pack menu with the red error symbol and select the checkbox of the corresponding virtual drive:



7. In the **Element(s) Actions** menu on the right side select **Start locating**. Subsequently, you have the option to customize the locating procedure before confirmation.



▸ The LED indicators of all drives are blinking now blue. LED indicators of drives with malfunctions will be red, or will not be lit at all (in case of total failure).



The defective disk has been identified.

Removing a Defective Drive

NOTICE

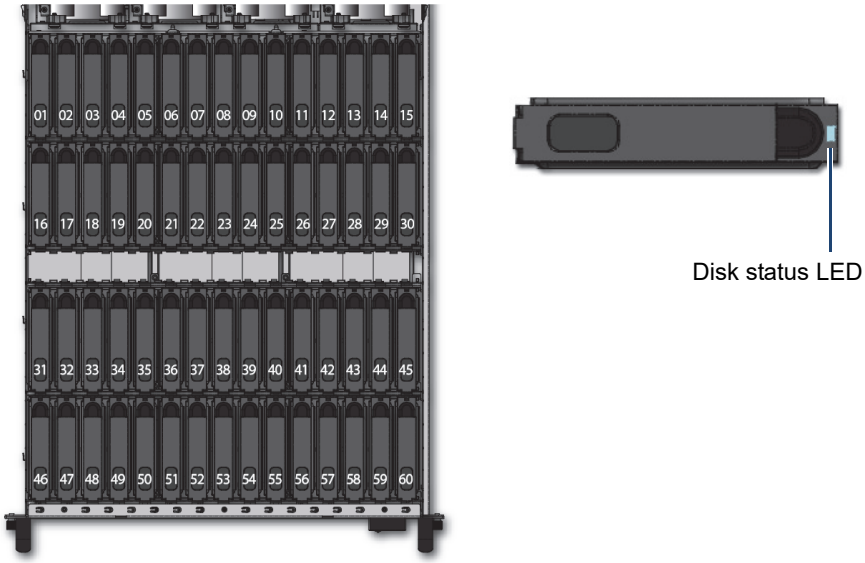
Electronic Discharge

Observe all conventional ESD precautions when handling modules and components.

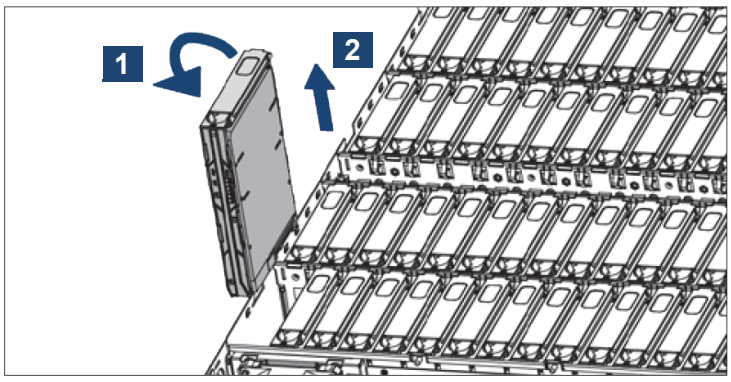
Avoid contact with midplane components and module connectors.

Perform the following steps:

1. Identify the defective drive as described in "Identifying a Defective Drive" (page 82). The status LED of a defective disk drive will be lit in red or not at all (total failure).



2. Push the drive carrier latch upwards to unlock and pull the drive carrier out of the casing.



The disk drive carrier is successfully removed.

Installing a New Drive

NOTICE

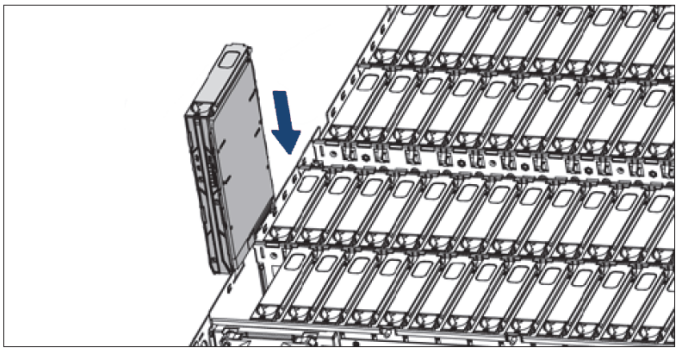
Data Loss

Before you start this operation, be sure that an available unconfigured replacement drive is available.

The replacement drive must have at least as much capacity as the drive you are replacing. Also, failed drives must be always replaced with approved drives. Contact your storage vendor for details.

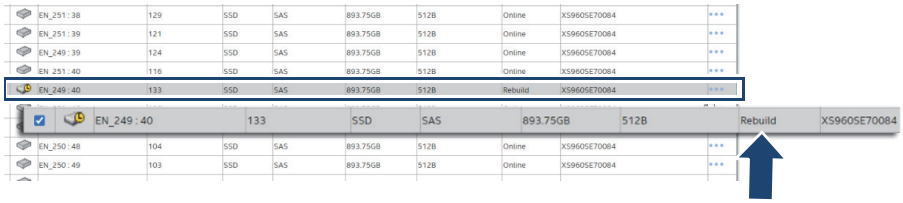
Perform the following steps:

1. Lower the drive carrier into the slot.
2. Push the drive carrier downwards and hold it down while sliding the drive carrier plate in the direction.

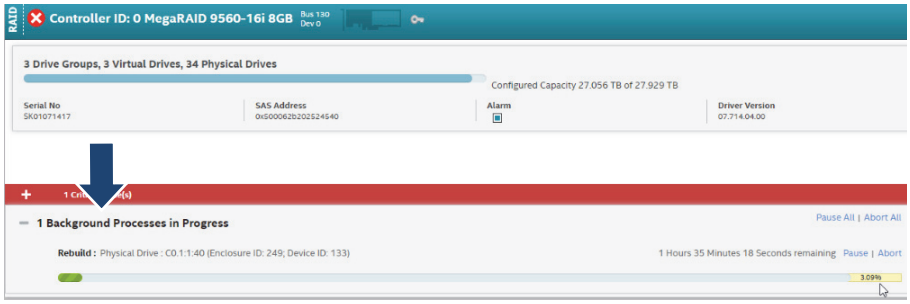


3. Push the drive carrier latch inwards to lock the drive in place.

4. In the Web UI application, open the Drives tab and check the **STATUS** column. New drives will have the status **REBUILD**.



5. To monitor the rebuild process, navigate back to the **Controller** tab and expand the **Background Process in Progress** menu:



The Rebuild procedure may take several hours depending on the data size to be restored. The time to rebuild several drives will add up, as the system rebuilds only a single drive at a time.

The new drive is successfully installed.

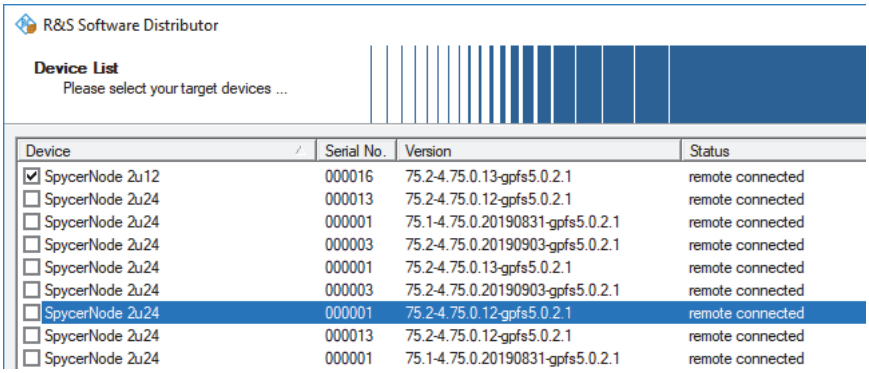
System Update

Perform the following steps:

1. Download the last version of the installation package (zip-file) from: **https://gloris.rohde-schwarz.com** on your host PC.

The installation of the packages can only be done on a Windows platform. The respective machine have to be in the same network as SpycerNode SC.

2. Open the file manager (Windows Explorer).
3. Switch to the directory that contains the installation file.
4. Unzip the installation package.
5. Execute the installation file with a double-click of the mouse.
   - The installation routine starts and will guide you through the installation process.
6. Select the systems you want to update.
   Identify the system with the serial number on the controller label or type plate.



Note, that only one controller can be updated on one SpycerNode SC system. Various controller can be updated only on different systems.

7. Follow the instructions given on the screen.
   - During the installation procedure all necessary files and libraries will be installed on the computer system. The installation will be finished as soon as a message reports this.
8. Restart the server by pressing the power switch.

After the cold start the system update will be complete and it can be started at any time.

System Disk Recovery

This section describes the procedures on how to recover the system image.

The following topics are covered:

Preparing a Bootable USB Drive

This instructions guide you through the process of preparing a bootable USB drive to be able to create a backup image of your system. The same drive will be then used to recover the system disk.

Downloading the R&S Backup Software

Perform the following steps:

1. If not already registered in GLORIS, the Rohde & Schwarz Service and Support portal, please do so to get access to the download area:
   `https://gloris.rohde-schwarz.com/rs.com~extnet~app~registration~web/form/register`

After an initial registration, your new profile will be checked and verified by Rohde & Schwarz. As this is not an automated process, it may take a while before you can proceed.

2. Login with your credentials to the GLORIS system:
   `https://idp1.aaa.rohde-schwarz.com/logon/LogonPoint/tmindex.html`
3. Upon successful login, navigate to
   Support & Services > My Products > Broadcast &Media
4. Depending on the number of product groups you have access to, you will find a different amount of products on the page. Select the **Media storage** tab and click the SpycerNode SC icon.

5. Set the filter to **Firm-/Software** and search for **R&S RESCUE BUNDLE (SYSTEM RECOVERY)**.

6. Download the archive file and store it on a Windows system for further use.

Proceed with next step.

Creating the Installation Media

In this instruction sequence we will use the software bundle downloaded in the previous step to prepare a bootable flash drive.

This procedure is only possible on a Windows operating system.

Perform the following steps:

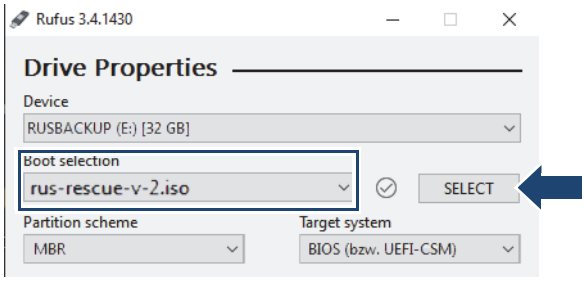
1. Prepare an empty USB drive. The device should have the following specifications:

Size	32 GB or more
Type	USB 3

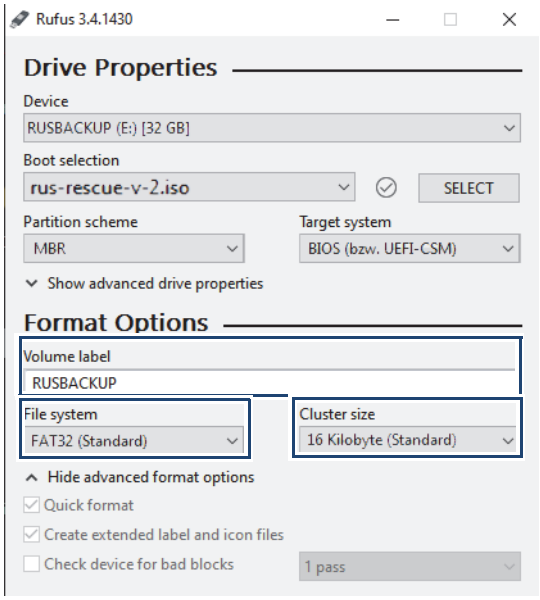
2. Unzip the archive on your Windows system. It contains two main programs:

Rufus-3.4.exe	Rufus is a third-party utility that helps format and create bootable USB flash drives, such as USB keys, or memory sticks.
rus-rescue-v-2.4.iso	R&S imaging and cloning tool used to create backups and restore system images.

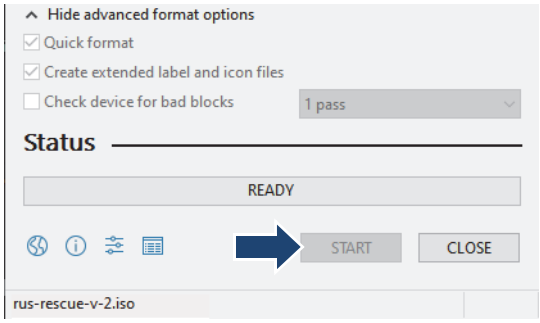
3. Connect the USB drive to the system.
4. Execute the **Rufus-3.4.exe** software (version 3.4.1430 or higher).
5. Click the **SELECT** button to navigate to the ISO file.



6. Enter RUSBACKUP as volume label, select FAT32 as file system, and 16 kB for the cluster size.



7. Initiate the process with the **START** button.



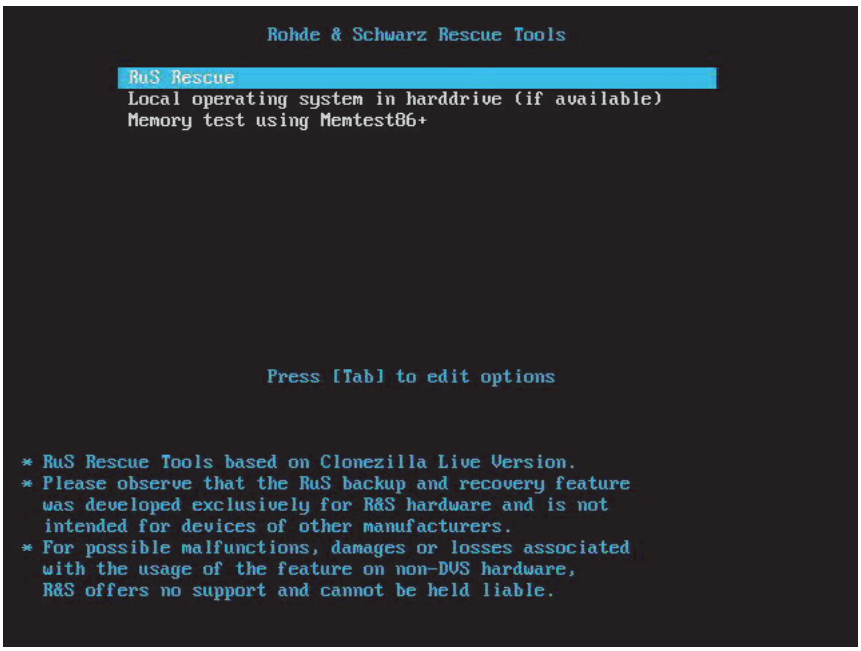
USB flash drive is now ready for use.

Creating a Backup Image

The following describes the steps to make a backup image of the current system disk and save it to the USB flash drive.

Perform the following steps:

1. If appropriate, disconnect all externally connected storage devices from the system.
2. Connect the bootable USB flash drive created in "Preparing a Bootable USB Drive" (page 89).
3. Turn on the SpycerNode SC. At the indicated moment during start-up you have to press **[F11]** to enter the boot menu.
   - The boot menu is displayed on the screen.
4. Select the USB flash drive as the boot device.



5. Press **[Enter]**.
   - The system will boot from the USB flash drive.
   - You will see a window on the screen where you can select the R&S Rescue environment for loading.

To complete the loading of the R&S Rescue environment some user entries are required. For this follow the instructions given on the screen.

The loading of the environment and the process itself will both try to initialize hardware that may not be present on your system. Any error messages displayed during loading/initialization, e.g. **`Failed`** or **`Warning`**, can be disregarded. The backup/recovery process should work nonetheless.

6. Select RuS Rescue and press **[Enter]**.

If you do not perform any action, RuS Rescue will be loaded automatically after 30 seconds.

- Once the loading has finished, you will see the RuS Rescue script with its options on the screen. Your display should look similar to the following:

```
--- RuS Rescue ---

1 - Backup on internal USB device
2 - Restore from internal USB device
3 - Backup on self selected external device
4 - Restore from self selected external device
5 - Reboot the system
6 - Poweroff the system

0 - Exit

Enter selection:
```

7. To create a backup image of your system disk and save it to the USB flash drive, press **[1]** and then **[Enter]**.
   - A list of possible source devices will be detailed on the screen. The system disk normally is the 'ATA' disk with, for example, 'sda', 'sdb' or 'sdc' as its device name (e.g.: **`1:0:0:0 disk ATA <device info> /dev/sda`**).

Ex factory the SpycerNode SC will be delivered with 'sda' as the default system disk. If other configurations have been made later or on customer request, this may be different.

NOTICE

Data Loss

Selecting the wrong source device may lead to an unwanted configuration and malfunctions when the system is operating.

Continue with the following steps only if you are able to identify the correct source device.

8. Enter the name of the system disk: Type in e.g. **`sda`** (or in other cases **`sdb`**, **`sdc`**, etc.) and press **[Enter]**.
   - The system will ask you to enter the image name for the backup image to be saved to the USB flash drive. By entering the name of an already existing backup image you can overwrite it.
9. Type in the name of the image you want to save to the USB flash drive for a later recovery. To confirm your entry press **[Enter]**.
   - The system will ask you to confirm your selection and whether you want to continue:

To abort the process at this point enter **n** for ‘no’ and press **[Enter]**. You will be redirected to the RuS Rescue script.

After starting the process its termination is no longer possible.

10. To start the backup process type in **y** for ‘yes’ and press **[Enter]**.
    - The program starts the backup process. Its progress will be indicated on the screen.

The backup process may take some time.

If during the process the screen turns black, press **[Space]** to get it back again.

When the system has finished the backup process, you will be notified about this. Then after pressing **[Enter]**, you will be redirected to the R&S Rescue script once more where you can choose, for example, ‘reboot’ or ‘poweroff’ to restart or turn off the system.

Restoring the System

The following describes the steps to make a recovery of the system disk.

NOTICE

Total Loss of Data

Selecting the wrong device for restoring the system partition will lead to a total loss of data.

Do not execute any commands if you are not sure about the correct target device.

Perform the following steps:

1. If appropriate, disconnect all externally connected storage devices from the system.
2. Connect the bootable USB flash drive created in "Preparing a Bootable USB Drive" (page 89).
3. Turn on the SpycerNode SC. At the indicated moment during start-up you have to press **[F11]** to enter the boot menu.
   - The boot menu is displayed on the screen.
4. Select the USB flash drive as the boot device.
5. Press **[Enter]**.
   - The system will boot from the USB flash drive. You will see a window on the screen where you can select the R&S Rescue environment for loading.

To complete the loading of the R&S Rescue environment some user entries are required. For this, follow the instructions given on the screen.

The loading of the environment and the process itself will both try to initialize hardware that may not be present on your system. Any error messages displayed during loading/initialization, e.g. **`Failed`** or **`Warning`**, can be disregarded. The backup/recovery process should work nonetheless.

6. Select RuS Rescue and press **[Enter]**.

If you do not perform any action, RuS Rescue will be loaded automatically after 30 seconds.

- Once the loading has finished, you will see the R&S Rescue script with its options on the screen. Your display should look similar to the following:

```
--- RuS Rescue ---

1 - Backup on internal USB device
2 - Restore from internal USB device
3 - Backup on self selected external device
4 - Restore from self selected external device
5 - Reboot the system
6 - Poweroff the system

0 - Exit

Enter selection:
```

7. To restore your system disk from the USB flash drive, press **[2]** and then **[Enter]**.
   - A list of possible target devices will be detailed on the screen. The system disk normally is the 'ATA' disk with, for example, 'sda', 'sdb' or 'sdc' as its device name:
     (e.g.: `1:0:0:0 disk ATA <device info> /dev/sda`).

Ex factory the SpycerNode SC will be delivered with 'sda' as the default system disk. If other configurations have been made later or on customer request, this may be different.

NOTICE

Data Loss

A recovery will overwrite all your data.

Continue with the following steps only when you are able to identify the correct target device.

8. Enter the name of the system disk: Type in e.g. **sda** (or in other cases **sdb**, **sdc**, etc.) and press **[Enter]**.
   - A further list of possible source images will be detailed on the screen. If there is only the R&S recovery image on the USB flash drive, this one will be listed. If there are several images, all images will be displayed.
9. Select the image you want to use for the recovery. Normally, it provides the serial number of the SpycerNode SC in its name. To confirm your choice press **[Enter]**.
   - The system will ask you to confirm your selection and whether you want to continue.

To abort the process at this point enter **n** for 'no' and press **[Enter]** on your keyboard. You will be redirected to the RuS Rescue script.

After starting the process its termination is no longer possible.

10. To start the recovery process type in **y** for 'yes' and press **[Enter]**.
    - The program starts the recovery process. Its progress will be indicated on the screen.

The recovery process may take some time.

If during the process the screen turns black, press **[Space]** to get it back again.

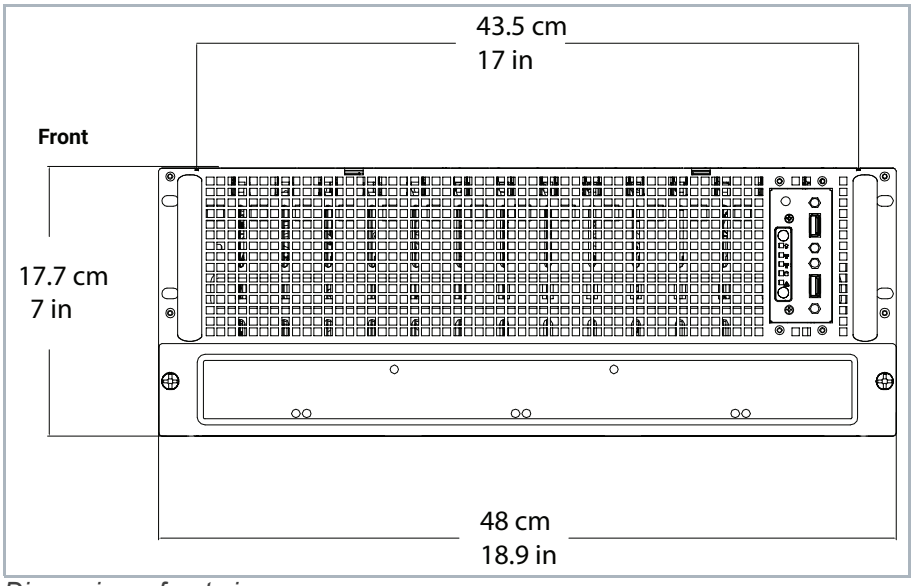
When the system has finished the recovery process, you will be notified. Then after pressing **[Enter]**, you will be redirected to the RuS Rescue script once more where you can choose, for example, 'reboot' or 'poweroff' to restart or turn off the system. The next time the system is started, it will load the restored operating system.

Appendix

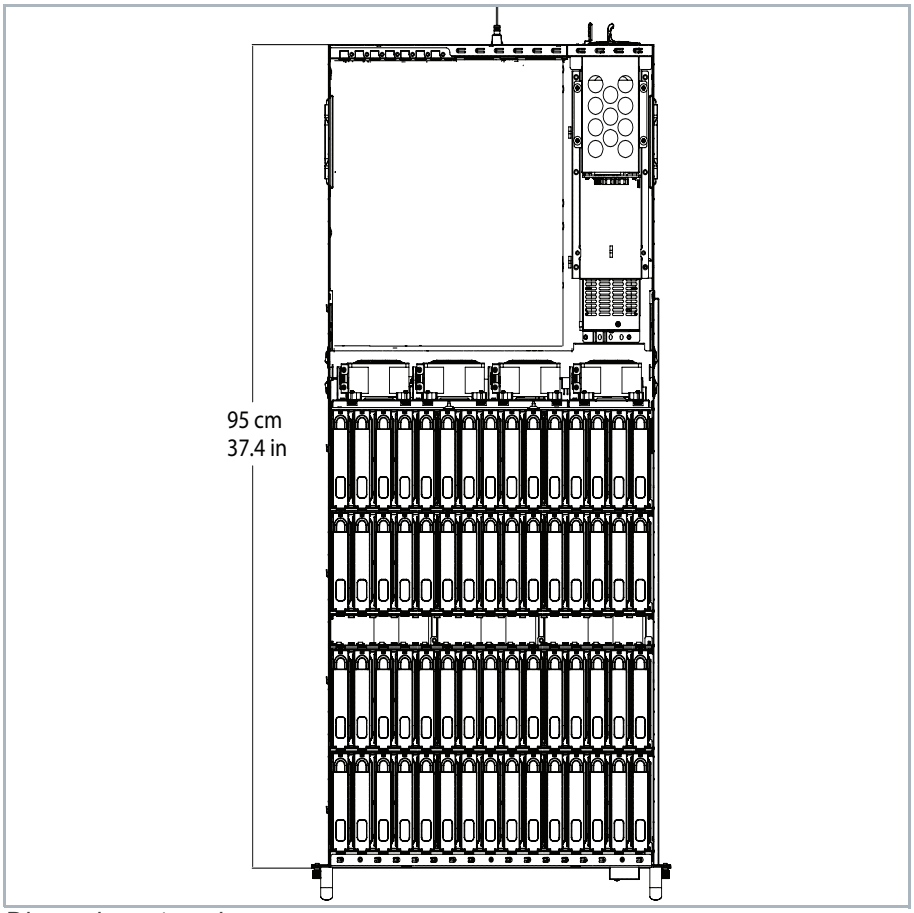
This chapter includes the following sections:

Dimensions

The following figures show the dimensions of the system:



Dimensions, front view



Dimensions, top view

Technical Data

This section lists important technical data.

Power Rating

Rated voltage	200 V to 240 V AC
Rated frequency	50/60Hz
Power consumption	max. 1600W
	1480W (average with HDD drives)
	1370W (average with SSD drives)
Cooling capacity	7510 BTU/h

System Configuration

Casing	4U rack mount
Total number of drives	30 or 60 data drives per casing
CPU	AMD EPYC processor (second generation)
RAM	DDR4 RDIMM
System drives	Redundant SSDs for operating system and metadata
PCI	PCIe 4.0 technology

Connection Ports

10 Gbit Ethernet	2 x RJ-45
Dedicated IPMI (1 Gbit)	RJ-45
USB 3.2 Gen1	2 ports
USB 3.2 Gen1	1 port, Type C
Serial port	1 x COM
Video port	VGA, D-Sub

Environmental Conditions

Temperature	+5 °C to +35 °C
	+5 °C to +30 °C (above 2133 m)
Relative humidity	10% to 80%
Altitude	0 to 3000 m (operating)
	-100 to 12192 m (non operating)
Mechanical resistance	Vibration: • Frequency range: 5 Hz to 55 Hz • Displacement: 0.3 mm (pk-pk) (1. 8g at 55 Hz) • Frequency range: 55 Hz to 510 Hz • Acceleration: 0.5 g constant

Weight

Case without storage	48 kg / 106 lbs
With HDD storage	max. 95 kg / 210 lbs
With SSD storage	max. 72 kg / 159 lbs

Data Sheet

R&S®SpycerNode 4u60 SC STORAGE SERVER

Specifications

Description

The R&S®SpycerNode 4u60 SC is a storage server for media and entertainment applications. With its ideal size as a building block, it is easy to lift, install and deploy. The storage server provides advanced PCI Express (PCIe) 4.0 technology, activity and status indicators for all key components and alarms. With the compact design, advanced file system functionality and support for enterprise level NL-SAS and dual-ported SSD drives, the R&S®SpycerNode 4u60 SC is ready to fulfill a wide range of applications.

Specifications

System configuration		• 4 HU rack mount • 30 or 60 data drives per chassis • AMD EPYC processor (second generation) • DDR4 RDIMM • redundant SSDs for operating system • redundant SSDs for meta data • enterprise class drive technology • PCIe 4.0 technology
Controller connectivity		
10 Gigabit Ethernet		2 × RJ-45
Dedicated IPMI		1 × RJ-45
USB 3.2 Gen1		2 ports
USB 3.2 Gen2		1 port, type C
Serial port		1 × COM
Video port		1 × VGA, D-Sub
Environmental conditions		
Temperature	operating temperature range	+5 °C to +35 °C
	above 2133 m	+5 °C to +30 °C
Relative humidity	operating	10 % to 80 % relative humidity
Altitude	operating	0 m to 3000 m
	nonoperating	–100 m to 12192 m
Mechanical resistance		
Vibration	operating	frequency range: 5 Hz to 55 Hz, displacement: 0.3 mm (pk-pk) (1.8 g at 55 Hz), frequency range: 55 Hz to 150 Hz, acceleration: 0.5 g constant
Power rating		
Rated voltage		200 V to 240 V AC
Rated frequency		50/60 Hz
Power consumption		max. 1600 W
	average, with HDD	1480 W
	average, with SSD	1370 W
Cooling capacity		7510 BTU/h

Data Sheet | Version 01.00

ROHDE&SCHWARZ
Make ideas real

Product conformity		
Electrical safety		in line with EN 62368-1
Electromagnetic compatibility (EMC)	USA and Canada	FCC 47 CFR part 15, subpart B
	Europe	in line with EN 55032:2015, EN 55035:2018, EN 61000-3-2, EN 61000-3-3
Conformity marks	North America	FCC
	Europe	CE
	Australia/New Zealand	RCM (formerly C-tick)
Dimensions and weight		
Dimensions	W × H × D	435 mm × 177 mm × 950 mm (17 in × 7 in × 37.4 in)
Weight		48 kg
	including HDD	max. 95 kg
	including SSD	max. 72 kg
Rack mounting		universal rack mount kit

Ordering information

Designation	Type	Order No.
R&S®SpycerNode 4u60 SC main unit	R&S®SNOSC	2902.5217.02
R&S®SpycerNode SC HDD bundle 120 Tbyte (30 data drives)	R&S®SNO-B130	2902.5330.02
R&S®SpycerNode SC HDD bundle 240 Tbyte (30 data drives)	R&S®SNO-B131	2902.5346.02
R&S®SpycerNode SC HDD bundle 480 Tbyte (30 data drives)	R&S®SNO-B132	2902.5352.02
R&S®SpycerNode SC SSD bundle 57 Tbyte (30 data drives)	R&S®SNO-B140	2902.5500.02
R&S®SpycerNode SC SSD bundle 115 Tbyte (30 data drives)	R&S®SNO-B141	2902.5517.02
R&S®SpycerNode SC SSD bundle 230 Tbyte (30 data drives)	R&S®SNO-B142	2902.5523.02
100 Gigabit Ethernet dual port HBA QSFP	R&S®CLP6-B25	2904.1160.00
R&S®SpycerNode SC block level client license bundle (10 licenses)	R&S®SNO-K120	2902.5269.00
Spare parts		
Power supply unit		2902.5817.00
SSD for meta data and operating system		2902.5898.00
Backplane fan module		2902.5781.00
HDD (SATA), 4 Tbyte		2902.5369.00
HDD (SATA), 6 Tbyte		2902.5375.00
HDD (SATA), 8 Tbyte		2902.5381.00
SSD, 2 Tbyte		2902.5530.00
SSD, 4 Tbyte		2902.5546.00
SSD, 8 Tbyte		2902.5552.00
Service level agreements		
R&S®SpycerNode SC warranty upgrade to advanced	R&S®SWASNSC	2902.5700.38
R&S®SpycerNode SC SLA advanced 1 year	R&S®SA1SNSC	2902.5700.08

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

Rohde & Schwarz training
www.training.rohde-schwarz.com
Rohde & Schwarz customer support
www.rohde-schwarz.com/support

Certified Quality Management
ISO 9001

PD 3609.0166.22 | Version 01.00 | December 2020 (jr)
R&S®Spycernode 4u60 SC Storage Server
Data without tolerance limits is not binding | Subject to change

ROHDE&SCHWARZ

CE Declaration of Conformity

CE

This is to certify that:

Equipment type	Stock No.	Designation
Spycernode SC	2902.5217.02	SPYCER NODE SC MAIN UNIT

complies with the provisions of the Directive of the Council of the European Union on the approximation of the laws of the Member States

- relating to electrical equipment for use within defined voltage limits (2014/35/EU) [LVD]
- relating to electromagnetic compatibility (2014/30/EU) [EMCD]
- relating to restriction of the use of hazardous substances in electrical and electronic equipment (2011/65/EU) [RoHS]

Conformity is proven by compliance with the following standards:

EN 62368-1:2014 +AC:2015
EN 55032:2015 + A11:2020
EN 55035:2018-04
EN 61000-3-2:2019
EN 61000-3-3:2013 + A1:2019
EN 50581: 2012 (ROHS)

For the assessment of electromagnetic compatibility, the limits of radio interference for Class A equipment as well as the immunity to interference for operation in industry have been used as a basis.

Template: CE_BESCH_B_3573703805.dotx 3573.7038.05. / Äl 04.00

ROHDE & SCHWARZ GmbH & Co. KG
Mühldorfstr. 15, D-81671 Munich

Munich, 2021-02-25

i. V. Kemmet

Corporate Quality Management CF-QP1 / Kemmet

QM CI

3679.9927.02 01.00 CE EN

Page 1 / 1

CE Declaration of Conformity

Index

T

U

W