

NetWitness Platform[®] Platform

Version

Series 6 Hardware Setup Guide

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

October, 2024

Contents

About this Document	4
S6 R640 Hardware Description	5
Package Contents	6
Customer Supplied Materials	6
Front View of the Series 6 Hardware (Except Hybrid)	7
Rear View of the Series 6 Hardware (Except Hybrid)	9
Series 6 Hardware Specifications	10
Install a Deep-Rack Adapter for R640 Hardware	13
S6 R740xd Hybrid Hardware Description	16
Package Contents	16
Customer Supplied Materials	17
Front View of the Series 6 Hybrid Hardware	18
Rear View of the Series 6 Hybrid Hardware	20
Series 6 R740xd Hybrid Hardware Specifications	21
Install a Deep-Rack Adapter for an R740xd Hybrid	22
Connect to the Series 6 Hardware Console	25
10.6.5.2 and Later 10.6.x.x Versions Installation Tasks	27
Configure Network Parameters	27
Specify the Network Clock Source	28
Best Practices	28
Set Time on the Security Analytics Server Host using the NwConsole Utility	29
Finish Host Setup in NetWitness Platform	29
Log On to NetWitness Platform	30
Open the Online Help	30
11.1.0.2 and Later Installation Tasks	31
NIC Bonding	32
Example for Bonding em3 or em4 (10G fiber interfaces)	35
Revision History	39

About this Document

This document provides instructions for setting up NetWitness® Platform Series 6 (S6) physical hosts and connecting them to your network.

This document applies to both Series 6 and Series 6E hardware. Series 6E hardware uses self-encrypting drives (SEDs).

The hardware setup instructions in this document are for hardware only; they do not apply to a specific release of NetWitness Platform software. After completing the hardware setup, continue setup and configuration of the NetWitness Platform Series 6 physical hosts as described in the NetWitness® Platform online documentation at RSA Link (<https://community.rsa.com/docs/DOC-40370>).

This document is not a replacement for the original manufacturer's documentation; it contains information specifically for the NetWitness Platform Series 6 hardware.

Note: When viewing a printed guide, be aware that a newer version of the guide may be available online at RSA Link in RSA NetWitness Platform under Hardware Setup Guides: <https://community.rsa.com/community/products/netwitness/hardware-setup-guides>

S6 R640 Hardware Description

All but one of the NetWitness® Platform Series 6 (S6) physical hosts are based on the Dell PowerEdge R640 chassis. The exception is the Hybrid host, which is based on the Dell PowerEdge R740xd chassis. The Series 6 hosts are shipped with NetWitness Platform software installed.

In NetWitness Platform 11.3 and later, the R640 can also support Hybrid host software, but additional external storage is required. For more information on Hybrids, see [S6 R740xd Hybrid Hardware Description](#).

This section describes the Series 6 hosts that are based on the Dell PowerEdge R640 chassis:

- Network Decoder and Log Decoder
- Concentrator, Broker, and Archiver
- NetWitness Server
- Malware Analysis
- Event Stream Analysis (ESA)
- User and Entity Behavior Analytics (UEBA)

Except for the Analytics hardware used for ESA and UEBA, all Dell PowerEdge R640-based hosts have the same components and physical specifications. The Analytics hardware has additional hard drives, memory, and a different CPU. [Series 6 Hardware Specifications](#) provides details.

The initial setup of a Series 6 host in your network involves these steps:

1. Review site requirements and safety information in the *Deployment Guide* for your NetWitness Platform software version. To locate this document, go to the NetWitness® Platform online documentation at RSA Link (<https://community.rsa.com/docs/DOC-40370>) and for your software version, click the **Documentation** link. The Deployment Guide is located in the **Administration** section.
2. Mount or place the host hardware securely in accordance with your site requirements.
3. Connect the RSA physical host (appliance) to your network. See [Connect to the Series 6 Hardware Console](#).
4. Finish the host setup in one of the following sections, depending on your NetWitness Platform version:
 - [10.6.5.2 and Later 10.6.x.x Versions Installation Tasks](#)
 - [11.1.0.2 and Later Installation Tasks](#)

Caution: To avoid damaging NetWitness servers, hosts, and JBODs, remove them from the rack and dismantle the rack before transporting them to another location. Follow the recommendations of the server manufacturer and rack manufacturer for packaging, transport, and installation. RSA does not support re-shipping of racked servers. The customer assumes all risk and liability for transporting NetWitness servers and hosts mounted in a rack.

Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install and configure the RSA physical host.

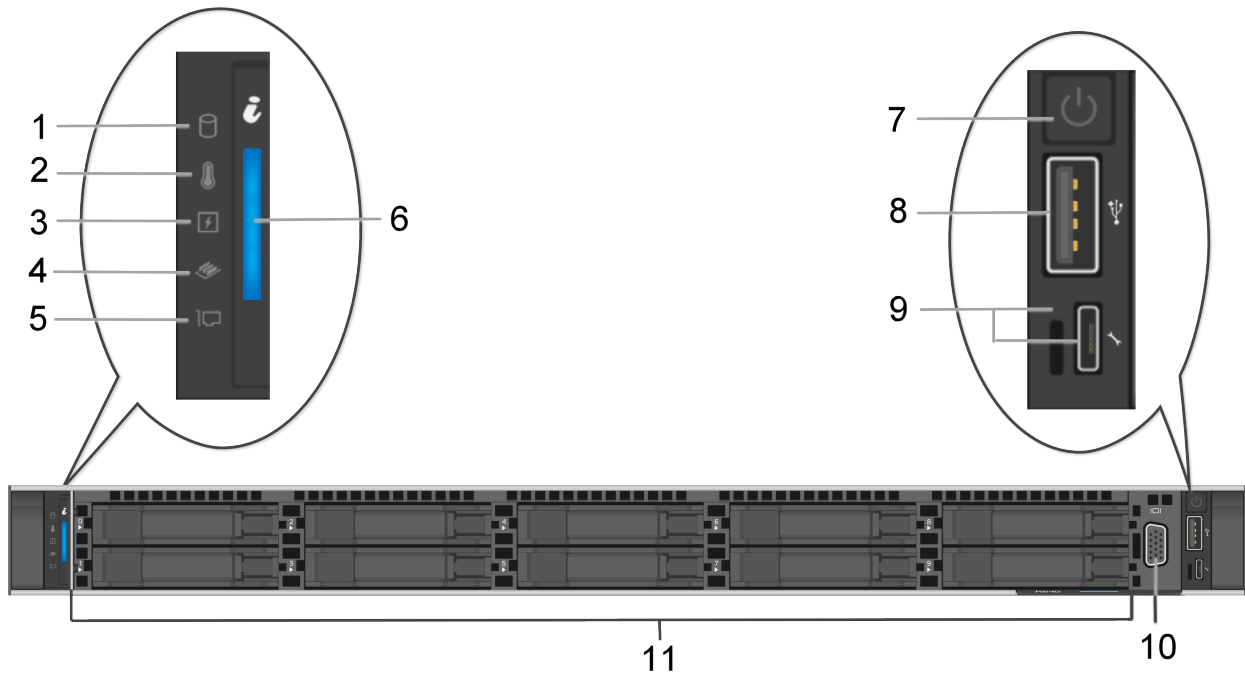
- NetWitness® Platform Series 6 physical host (Decoder, Concentrator, Broker, Archiver, NetWitness Server, Malware Analysis, or ESA)
- Static Ready Rails 1U (1 set)
- Left Rail Adapter for EMC deep rack (1)
- RSA Bezel (1) - Keys are taped to the bezel.
- Power Cord (2)
- Short Range (SR) SFP Optical Transceivers (2)
- Safety Environment and Regulatory Information booklet (1)
- RSA Documentation Folder (1)
- RSA EULA (1)

Customer Supplied Materials

To complete the setup procedure, you will need:

- One Ethernet connection (application)
- One Ethernet connection (iDRAC)
- Cables to connect a monitor or KVM adapter to the VGA port and a keyboard or KVM adapter to the USB port
- Fiber cables if using SR SFP fiber connections
- Standard tools

Front View of the Series 6 Hardware (Except Hybrid)



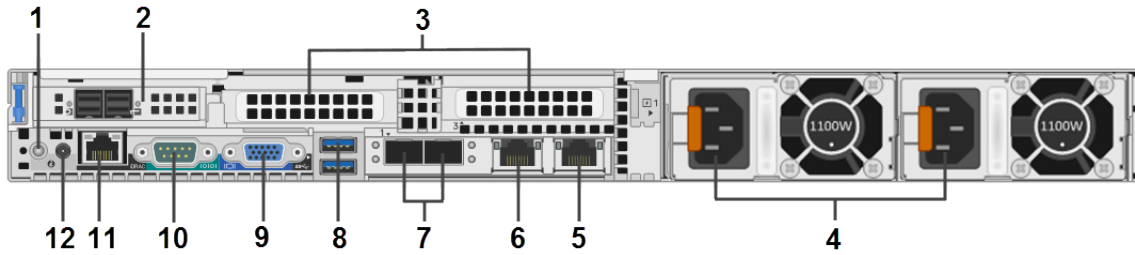
Item numbers 1-5 are status LED indicators, which indicate the status of the system. The status LED indicators are always off and only turn on to a solid amber if any error occurs.

Key	Description
1	Drive indicator. This turns solid amber if there is a drive error.
2	Temperature indicator. This turns solid amber if the system experiences a thermal error, such as the ambient temperature is out of range or there is a fan failure.
3	Electrical indicator. This turns solid amber if the system experiences an electrical error, such as voltage out of range, a failed power supply unit (PSU), or a failed voltage regulator.
4	Memory indicator. This turns solid amber if a memory error occurs.
5	PCIe indicator. This turns solid amber if a PCIe card experiences an error.

Key	Description
6	<p>System health and system ID indicators:</p> <ul style="list-style-type: none"> • Solid blue: Indicates that the system is turned on, the system is healthy, and system ID mode is not active. Press the system health and system ID button to switch to system ID mode. • Blinking blue: Indicates that the system ID mode is active. Press the system health and system ID button to switch to system health mode. • Solid amber: Indicates that the system is in fail-safe mode. • Blinking amber: Indicates that the system is experiencing a fault. Check the System Event Log or the LCD panel, if available on the bezel, for the specific error message.
7	Power button
8	USB port
9	iDRAC Direct LED indicator and iDRAC Direct port. The indicator lights up to indicate that the iDRAC Direct port is actively connected to a device. The iDRAC Direct port is micro USB 2.0-compliant. This port enables you to access the iDRAC Direct features. For more information, see the <i>iDRAC User's Guide</i> at Dell.com .
10	VGA Port. Enables you to connect a display device to the system.
11	Ten 2.5-inch hard drive bays (field replaceable). The specifications below identify the number and types of hard drives installed on the hosts.

For more information, refer to the Dell documentation, the *Dell EMC PowerEdge R640 Installation and Service Manual*, and the *Dell Event and Error Messages Reference Guide*.

Rear View of the Series 6 Hardware (Except Hybrid)



Key	Description
1	System identification connector
2	PERC H840 RAID controller. It is in PCIe slot 1. The PERC H840 is the the RAID controller for the storage expansion JBOD. It requires a cable with a Mini-SAS port to connect to the JBOD.
3	PCIe expansion slots 2 and 3. The Decoder may use a PCIe slot for an optional Intel i350 Quad RJ-45 port network interface card. These slots can also be used for an Emulex HBA card to connect to a SAN and for an Intel 520 based dual port 10G NIC Fiber card.
4	Hot Swappable Power Supply 1 and 2 (field replaceable)
5	Secondary Network 1000BASE-T port: em2
6	Primary Network 1000BASE-T management port: em1
7	Fiber ports em3 and em4 (This is where the Short Range (SR) SFP Optical Transceivers that were included with the shipment need to be installed.)
8	USB Ports (Keyboard, mouse, USB thumb drive, and so on)
9	VGA Video Port (monitor)
10	RS232 Serial Port (serial connection to laptop via DB9 or serial server)
11	iDRAC port. The default IP is 192.168.0.120 and the default authentication is root/themaster01
12	System identification button

Note: The PERC H840 RAID controller requires a cable with a Mini-SAS port to connect to the JBOD. The cables are included with the storage.

Series 6 Hardware Specifications

Item	Core	ESA/Analytics	Hybrid
Host Type	NW Server, Log Decoder, Network Decoder (Packets), Concentrator, Broker, Archiver, Malware Analysis	ESA UEBA	Log Decoder Hybrid, Network Decoder Hybrid (Packets), Endpoint Log Hybrid
Model	Dell PowerEdge R640	Dell PowerEdge R640	Dell PowerEdge R740
Processor			
Type	Intel Xeon Gold 6134	Intel Xeon Gold 6126	Intel Xeon Gold 6132
Processor Speed	3.2Ghz	2.6Ghz	2.6Ghz
Cache	24.75M 1 Cache	19.25M Cache	19M Cache
# of Processors	2	2	2
# of Cores	8 Cores per Processor	12 Cores per Processor	14 Cores per Processor
# of Threads	16 Threads per Processor	24 Threads per Processor	28 Threads per Processor
Series 6 Hard Drives Field replaceable Hot swappable	2 X 1TB NL-SAS 7.2K 2 X 2TB NL-SAS 7.2K <u>Total - 4 Drives</u> Slots 0-1: 1TB Slots 2-3: 2TB	2 X 1TB NL-SAS 7.2K 4 X 2.4TB SAS 10K <u>Total - 6 Drives</u> Slots 0-1: 1TB Slots 2-5: 2.4TB	4 X 2TB NL-SAS 7.2K 8 X 8TB NL-SAS 7.2K 2 x 1.6TB SSD <u>Total - 14 Drives</u> Slots 0-3 (Front): 2TB Slots 4-11 (Front): 8TB Slots 12-13 (Rear): 1.6TB SSD
Series 6E Self-Encrypting Drives (SEDs) FIPS140 Certified Field replaceable Hot swappable	2 X 1.2TB SAS 10K SED 2 X 2.4TB SAS 10K SED <u>Total - 4 Drives</u> Slots 0-1: 1.2TB Slots 2-3: 2.4TB	2 X 1.2TB SAS 10K SED 4 X 2.4TB SAS 10K SED <u>Total - 6 Drives</u> Slots 0-1: 1.2TB Slots 2-5: 2.4TB	2 X 2.4TB SAS 10K SED 10 X 8TB NL-SAS 7.2K SED 2 x 1.92TB SSD SED <u>Total - 14 Drives</u> Slots 0-1 (Front): 2.4TB Slots 2-11 (Front): 8TB Slots 12-13 (Rear): 1.92TB SSD

Item	Core	ESA/Analytics	Hybrid
Memory	128GB 4 * 32GB RDIMM 2666MT/s Dual Rank	256GB 8 * 32GB RDIMM 2133MT/s	128GB 4 * 32GB RDIMM 2666MT/s Dual Rank
Storage Controllers	External PERC H840, Internal PERC H740P		
Network Interface Card	Intel X710 DP 10Gb DA/SFP+, + 1350 DP 1Gb Ethernet, Network Daughter Card		
Power			
PSU	Dual, Hot-plug, Redundant Power Supply (1+1), 1100 W AC		
BTU/hr	4100 BTU/hr (Maximum)		
Voltage	100-240 V AC, auto-ranging		
Current	12 A - 6.5 A		
Form Factor	1U, full depth		2U, full depth
Weight (approximate)	21.9 kg (48.28 lbs)		33.1 kg (72.91 lb)
Dimensions (approximate)	With bezel: 482.0 mm (18.97 in) [w] x 808.51 mm (31.83 in) [d] x 42.8 mm (1.68 in) [h] Without bezel: 482.0 mm (18.97 in) [w] x 794.67 mm (31.29 in) [d] x 42.8 mm (1.68 in) [h]		With bezel: 482.0 mm (18.98 in) [w] x 751.34 mm (29.58 in) [d] x 86.8 mm (3.42 in) [h] Without bezel: 482.0 mm (18.98 in) [w] x 737.50 mm (29.04 in) [d] x 86.8 mm (3.42 in) [h]
Shipping Dimensions	Server boxed for shipping (includes rail kit) Height: 30.48 cm (12 inch) Width: 104.14 cm (41 inch) Depth: 64.14 cm (25.25 inch) Weight: 25.85 kg (57 lb)		Server boxed for shipping (includes rail kit) Height: 32.39 cm (12.75 inch) Width: 95.25 cm (37.50 inch) Depth: 66.04 cm (26.00 inch) Weight: 35 kg (81.86 lb)
Throughput / EPS	Network: 2-10 Gbps Logs: 30K EPS	N/A	Network: 1 Gbps Logs: 20K EPS

Item	Core	ESA/Analytics	Hybrid
Supported SFPs & Add-On Cards	<u>Add-On Cards</u> 1G QP Intel Copper Adapter 10G DP Intel Copper Adapter 10G DP Intel Optical Adapter External PERC H840 16G DP Emulex HBA <u>SFPs</u> 1G SFP Intel Copper 10G SFP Short Range Intel Optical (standard) 10G SFP Long Range Intel Optical		

Install a Deep-Rack Adapter for R640 Hardware

Note: This procedure is only applicable if you are installing the RSA S6 R640 physical host in the EMC Titan D Ultra Rack.

When installing the RSA S6 R640 physical host into the EMC Titan D Ultra Rack, a 1U deep-rack adapter is required. Follow this procedure to install a new bracket on the server rails.

Caution: Pay attention to rail markings. They are marked left and right. Be sure to place them on the correct side.

1. Locate the alternate rail bracket in the accessory box in the R640 host carton.



2. Remove the left side rail from the rail carton.



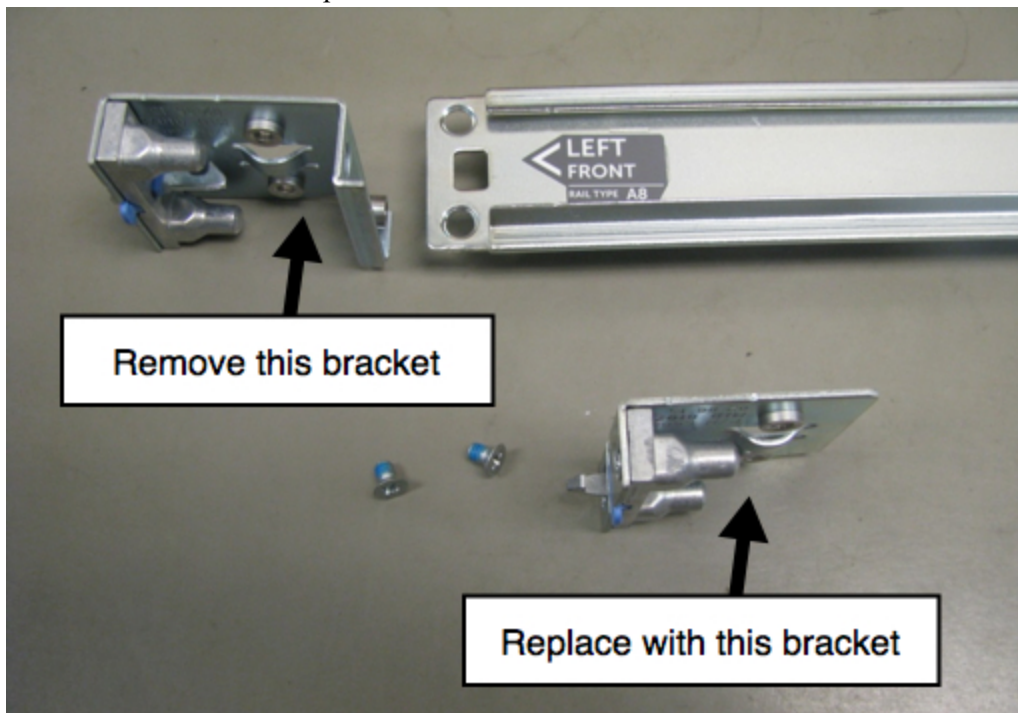
Each rail is marked.



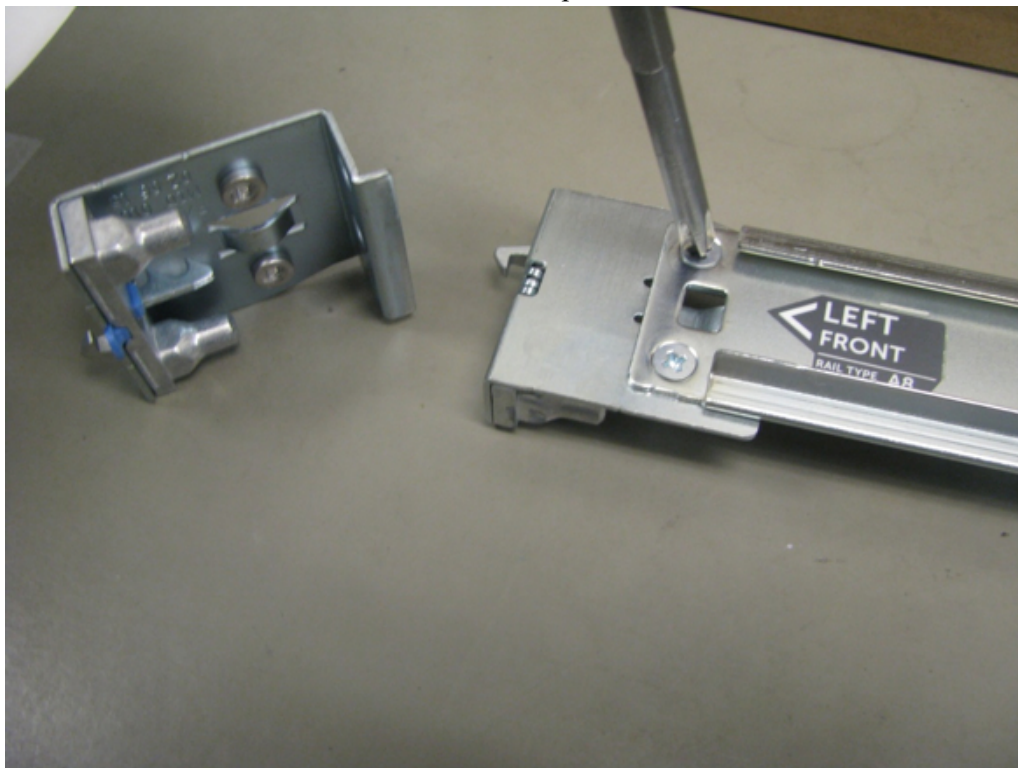
3. Use a Phillips screwdriver to remove the two mounting screws.



4. Remove the bracket and replace it with the new bracket.



5. Re-use the screws to fasten the new bracket in place.



The rail is now ready for the R640 host installation.

S6 R740xd Hybrid Hardware Description

The NetWitness® Platform Series 6 Hybrid physical host is based on the Dell PowerEdge R740xd chassis. The Series 6 Hybrid host is shipped with NetWitness Platform Hybrid host software installed. Hybrid host software includes Concentrator and Decoder (log or packet, not both).

This section describes the Series 6 Hybrid hosts that are based on Dell PowerEdge R740xd chassis:

- Network Decoder Hybrid (Packets)
- Log Decoder Hybrid
- Endpoint Log Hybrid (Includes Endpoint Server and Log Collector service)

The initial setup of a Series 6 host in your network involves these steps:

1. Review site requirements and safety information in the *Deployment Guide* for your NetWitness Platform software version. To locate this document, go to the NetWitness® Platform online documentation at RSA Link (<https://community.rsa.com/docs/DOC-40370>) and for your software version, click the **Documentation** link. The Deployment Guide is located in the **Administration** section.
2. Mount or place the host hardware securely in accordance with your site requirements.
3. Connect the RSA physical host (appliance) to your network. See [Connect to the Series 6 Hardware Console](#).
4. Finish the host setup in one of the following sections, depending on your NetWitness Platform version:
 - [10.6.5.2 and Later 10.6.x.x Versions Installation Tasks](#)
 - [11.1.0.2 and Later Installation Tasks](#)

Caution: To avoid damaging NetWitness servers, hosts, and JBODs, remove them from the rack and dismantle the rack before transporting them to another location. Follow the recommendations of the server manufacturer and rack manufacturer for packaging, transport, and installation.

RSA does not support re-shipping of racked servers. The customer assumes all risk and liability for transporting NetWitness servers and hosts mounted in a rack.

Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install and configure your RSA Hybrid physical host.

- NetWitness® Platform Series 6 Hybrid physical host
- Static Ready Rails 2U (1 set)
- Left Rail 2U Adapter for EMC deep rack (1)
- 2U RSA Bezel (1) - Keys are taped to the bezel

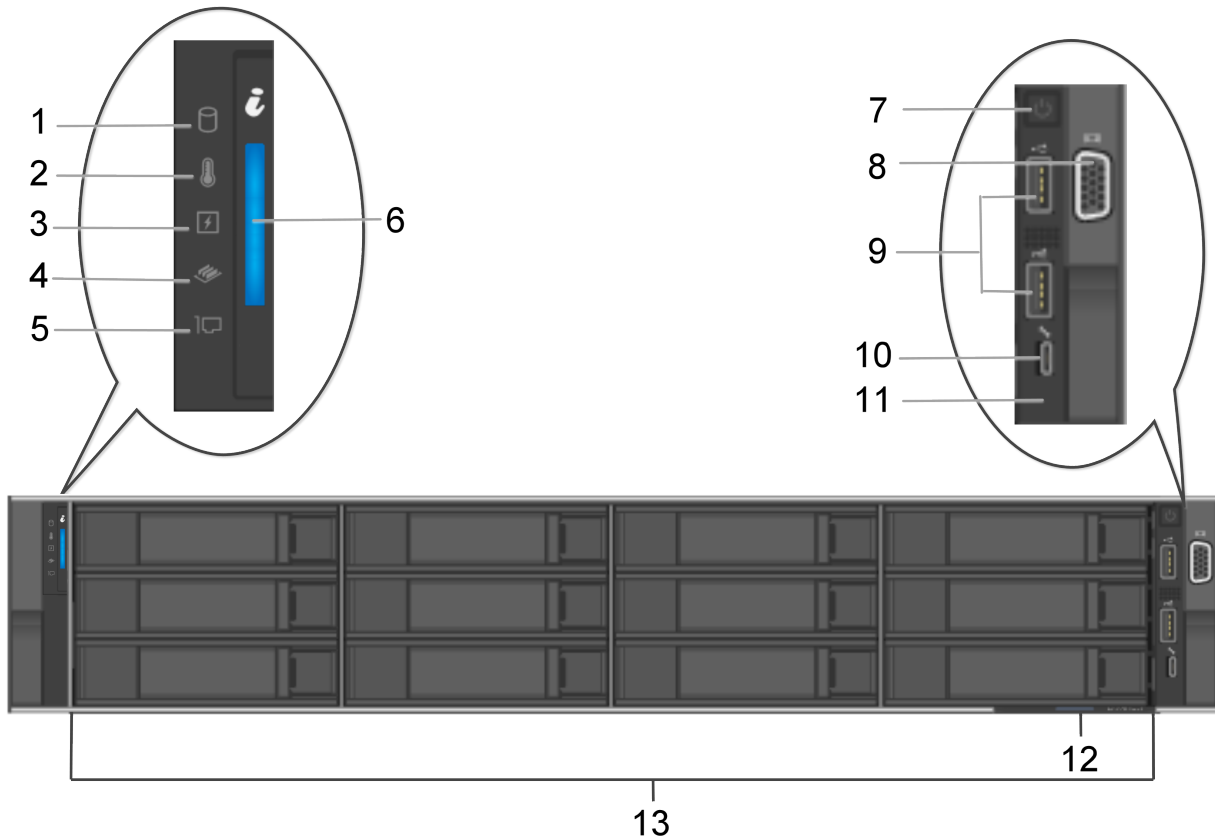
- Power Cord (2)
- Short Range (SR) SFP Optical Transceivers (2)
- Safety Environment and Regulatory Information booklet (1)
- RSA Documentation Folder (1)
- RSA EULA (1)

Customer Supplied Materials

To complete the setup procedure, you will need:

- One Ethernet connection (application)
- One Ethernet connection (iDRAC)
- Cables to connect a monitor or KVM adapter to the VGA port and a keyboard or KVM adapter to the USB port
- Fiber cables if using SR SFP fiber connections
- Standard tools

Front View of the Series 6 Hybrid Hardware



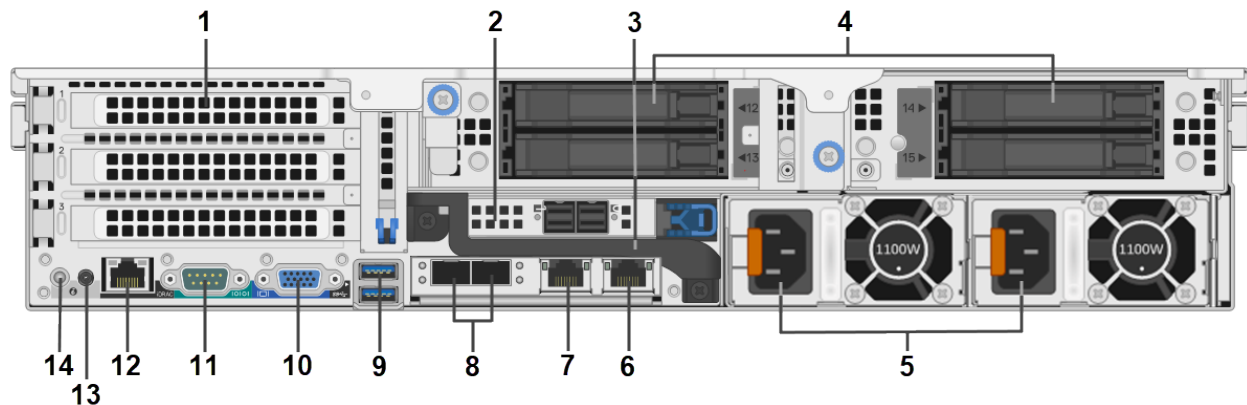
Item numbers 1-5 are status LED indicators, which indicate the status of the system. The status LED indicators are always off and only turn on to a solid amber if any error occurs.

Key	Description
1	Drive indicator. This turns solid amber if there is a drive error.
2	Temperature indicator. This turns sold amber if the system experiences a thermal error, such as the ambient temperature is out of range or there is a fan failure.
3	Electrical indicator. This turns solid amber if the system experiences an electrical error, such as voltage out of range, a failed power supply unit (PSU), or a failed voltage regulator.
4	Memory indicator. This turns solid amber if a memory error occurs.
5	PCIe indicator. This turns solid amber if a PCIe card experiences an error.

Key	Description
6	<p>System health and system ID indicators:</p> <ul style="list-style-type: none"> • Solid blue: Indicates that the system is turned on, the system is healthy, and system ID mode is not active. Press the system health and system ID button to switch to system ID mode. • Blinking blue: Indicates that the system ID mode is active. Press the system health and system ID button to switch to system health mode. • Solid amber: Indicates that the system is in fail-safe mode. • Blinking amber: Indicates that the system is experiencing a fault. Check the System Event Log or the LCD panel, if available on the bezel, for the specific error message.
7	Power button
8	VGA Port. Enables you to connect a display device to the system.
9	2 USB ports. The USB ports are 4-pin, 2.0-compliant.
10	iDRAC Direct port. The iDRAC Direct port is micro USB 2.0-compliant. This port enables you to access the iDRAC Direct features. For more information, see the <i>iDRAC User's Guide</i> at Dell.com .
11	iDRAC Direct LED indicator. The indicator lights up to indicate that the iDRAC Direct port is actively connected to a device.
12	Information tag location
13	12 3.5-inch hard drives (HDDs) (field replaceable). The NetWitness Platform Hybrid host has a total of 14 disks. There are 12 HDDs on the front and 2 solid state disks (SSDs) on the back. See the host specifications below for additional details.

For more information, refer to the Dell documentation, the *Dell EMC PowerEdge R740xd Installation and Service Manual*, and the *Dell Event and Error Messages Reference Guide*.

Rear View of the Series 6 Hybrid Hardware



Key	Description
1	Full-height PCIe expansion card slots (3). The Decoder may use a PCIe slot for an optional Intel i350 Quad RJ-45 port network interface card. These slots can also be used for an Emulex HBA card to connect to a SAN and for an Intel 520 based dual port 10G NIC Fiber card.
2	PERC H840 RAID controller. It is shown in the half-height PCIe expansion card slot. The PERC H840 is the RAID controller for the storage expansion JBOD. It requires a cable with a Mini-SAS port to connect to the JBOD. The PERC H840 card is installed inverted (upside down) in slot 4, which means that port 0 is on the right and port 1 is on the left on the R740xd Hybrid. You must attach cables to the R740xd with the connector's blue tab on the bottom.
3	Rear handle
4	Four 2.5-inch hard drive bays (field replaceable). The specifications below identify the number and types of hard drives installed on the hybrid host.
5	Hot swappable power supply 1 and 2 (field replaceable)
6	Secondary Network 1000BASE-T Port: em2
7	Primary Network 1000BASE-T Management Port: em1
8	Fiber Ports: em3 and em4 (This is where the Short Range (SR) SFP Optical Transceivers that were included with the shipment need to be installed.)
9	The USB ports are 9-pin and 3.0 compliant (Keyboard, mouse, USB thumb drive, and so on)
10	VGA video port (monitor)
11	RS232 Serial port (serial connection to laptop via DB9 or serial server)
12	iDRAC9 dedicated port. The default IP is 192.168.0.120 and the default authentication is root/themaster01
13	System identification connector

Key	Description
14	System identification button

Note: The PERC H840 RAID controller requires a cable with a Mini-SAS port to connect to the JBOD. The cables are included with the storage.

Series 6 R740xd Hybrid Hardware Specifications

See [Series 6 Hardware Specifications](#).

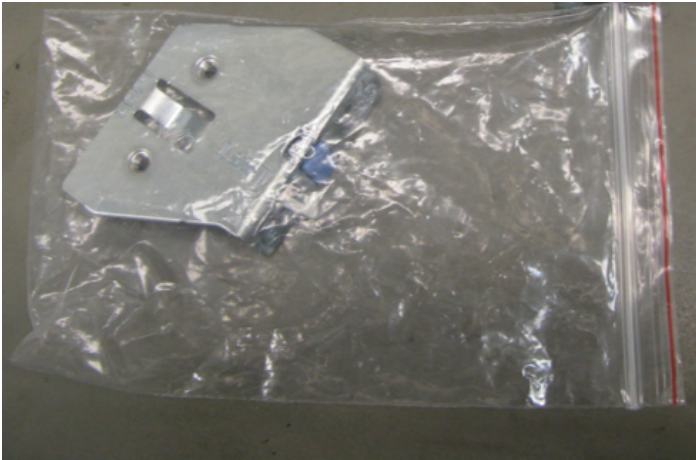
Install a Deep-Rack Adapter for an R740xd Hybrid

Note: This procedure is only applicable if you are installing the RSA S6 R740xd Hybrid physical host in the EMC Titan D Ultra Rack.

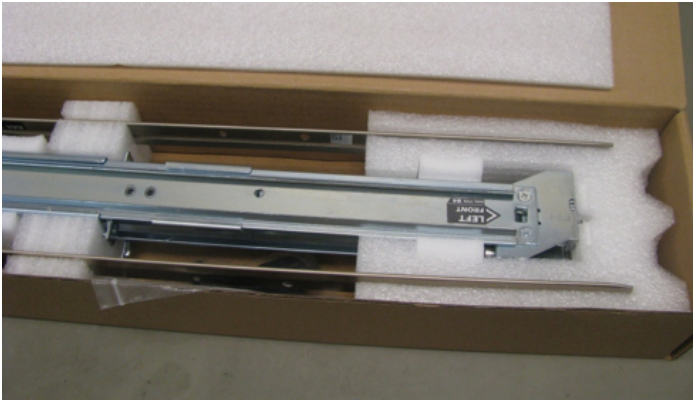
When installing the RSA S6 R740xd Hybrid physical host into the EMC Titan D Ultra Rack, a 2U deep-rack adapter is required. Follow this procedure to install a new bracket on the server rails.

Caution: Pay attention to rail markings. They are marked left and right. Be sure to place them on the correct side.

1. Locate the alternate rail bracket in the accessory box in the R740xd Hybrid host carton.



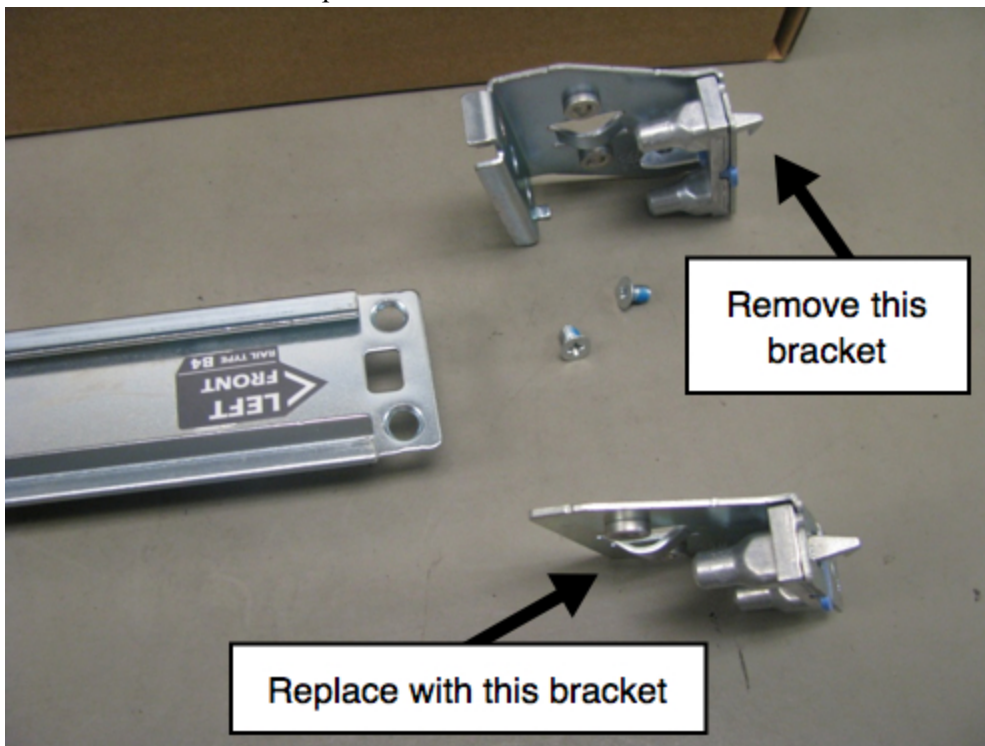
2. Remove the left side rail from the rail carton. Each rail is marked.



3. Use a Phillips screwdriver to remove the two mounting screws.



4. Remove the bracket and replace it with the new bracket.



5. Re-use the screws to fasten the new bracket in place.

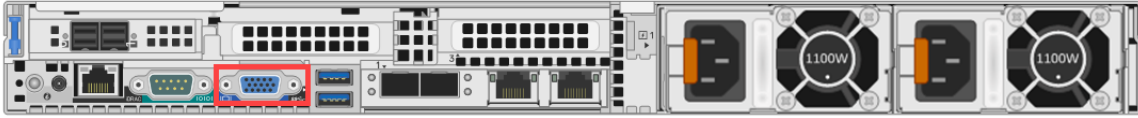


The rail is now ready for the R740xd Hybrid host installation.

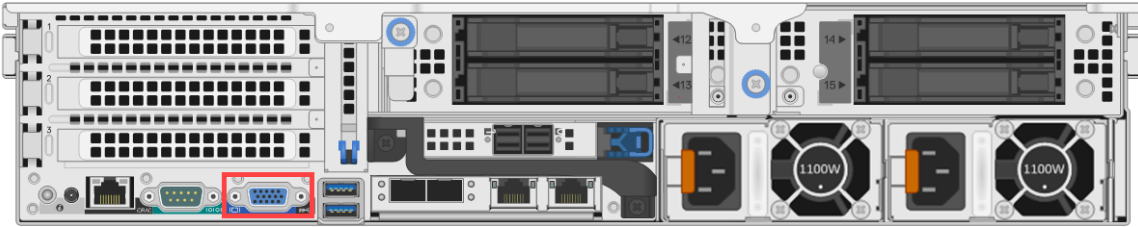
Connect to the Series 6 Hardware Console

Before installing software on your Series 6 hardware, you need to add a keyboard and monitor to it, connect it to your network, and power it on.

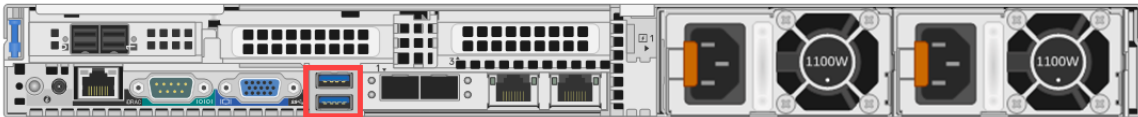
1. Connect a monitor or KVM adapter to the VGA Port on the back of the host.



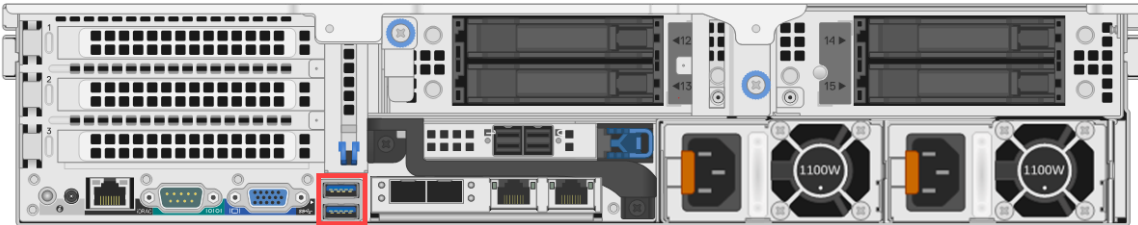
The following figure shows the VGA Port location for the Hybrid host.



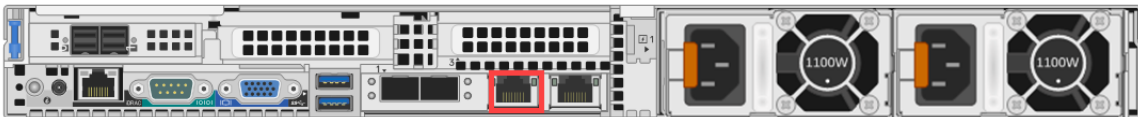
2. Connect a keyboard or KVM adapter to one of the USB ports on the back of the host.



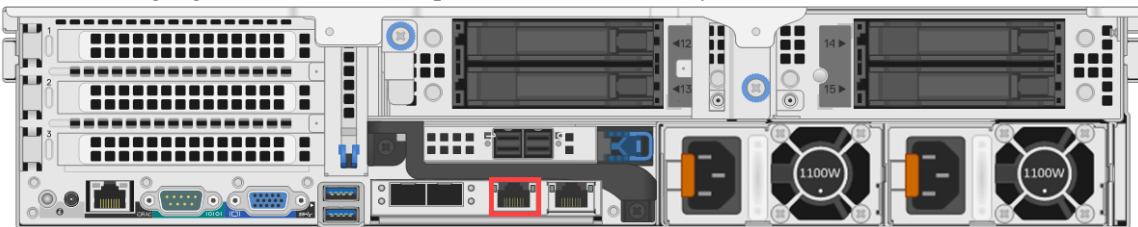
The following figure shows the USB port location for the Hybrid host.



3. Connect an Ethernet cable from the network to the em1 port on the back of the host.



The following figure shows the em1 port location for the Hybrid host.



4. Connect a power cord to each of the two power supplies on the rear of the host. Connect the power cords to a power source. To provide a more robust setup, connect each power supply to a different circuit.

Caution: 5V standby power is active whenever the system is plugged in. To remove power from the system, you must unplug both AC power cords from the power source.

5. Power on the host and continue to one of the following sections, depending on your NetWitness Platform version:
 - [10.6.5.2 and Later 10.6.x.x Versions Installation Tasks](#)
 - [11.1.0.2 and Later Installation Tasks](#)

10.6.5.2 and Later 10.6.x.x Versions Installation Tasks

If you are on NetWitness Platform version 10.6.5.2 or later 10.6.x.x versions, follow the steps below to configure the network parameters on the RSA physical host and finish the setup in NetWitness Platform. If you are on version 11.x, see [11.1.0.2 and Later Installation Tasks](#).

Note: NetWitness® Platform Series 6 physical hosts require version 10.6.5.2 or later.

Configure Network Parameters

1. At the login prompt, enter the default credentials to gain access to the operating system:

```
NWAPPLIANCE<xxxxxxx> login: root  
Password: netwitness
```

Note: If you do not receive the prompts for configuring network parameters, you can run `#netconfig.sh` from the command line to prompt you to enter the configuration options.

2. Enter the following information when prompted:
 - a. System IP Address (or **d** for DHCP)
 - b. System Netmask
 - c. Default Gateway
 - d. Primary DNS Server IP Address
 - e. Secondary DNS Server IP (or press **Enter** for none)
 - f. Local Domain Name (or press **Enter** for none)
 - g. Unqualified Hostname

After you complete the initial configuration, you should see a prompt that allows you to save the configuration as shown in the following figure.

```

you entered the following network parameters
IP Address: 192.168.1.20
Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
Primary DNS: 192.168.1.2
Secondary DNS: 192.168.1.3
Local Domain: SampleDomain.com
Host Name: SA-Server
-----
enter y to confirm and save
enter q to quit without saving
enter d for don't save or ask me this
enter 1 to re-enter IP address
enter 2 to re-enter netmask
enter 3 to re-enter default gateway
enter 4 to re-enter primary DNS
enter 5 to re-enter secondary DNS
enter 6 to re-enter local domain
enter 7 to re-enter host name
enter a to re-enter all network data
-----
? █

```

3. Verify the entered information and enter `y` to save the configuration. This sets the network information and restarts the network services.
4. If your RSA physical host is not a Security Analytics Server host, **wait approximately 15 seconds for a prompt** and then enter the Security Analytics Server host IP Address at the prompt.
5. Verify network connectivity by pinging your DNS Server.
6. Continue to the *Specify the Network Clock Source* section.

Specify the Network Clock Source

Caution: Do not enable the RSA physical host (appliance) before getting the network clock working. This ensures that the certificates sign correctly for enablement and that the hosts and services are in synch.

Configuring time synchronization between services and hosts is required. It is highly recommended to use an NTP time source for synchronization. Not only is time crucial for underlying communications between services, but not having hosts in synch can result in mismatched times shown during analysis of data. If the NTP server is not configured or reachable at this time, the network clock source configuration will fail, but can be done from the RSA NetWitness Platform interface later.

Best Practices

RSA recommends the following best practices:

For better data integrity, configure the Security Analytics Server host as the clock source for all other hosts. All RSA physical hosts, including Event Stream Analysis (ESA), get their time from the Security Analytics Server host. Only the Security Analytics Server host is configured to an external NTP time source.

For the NetWitness Server host, use the NwConsole utility to connect to the NTP time source.

If the other RSA physical hosts have NetWitness Platform 10.5.1 or later, the time is automatically set on all RSA physical hosts attached to the NetWitness Server hosts. If the other RSA physical hosts do not have NetWitness Platform 10.5.1 or later, set the time to point to the Security Analytics Server host manually.

Set Time on the Security Analytics Server Host using the NwConsole Utility

To set the network clock source on the NetWitness Platform using the NwConsole utility:

1. At the root prompt `[root@NwAppliance~]#` enter the following command:
`NwConsole`
NwConsole starts up and the startup message with a version and date displayed:
`RSA NetWitness Platform Console`
2. In NwConsole, enter the following command:
`login localhost:50006 <username> <password>`
The system administrator account username for NetWitness Platform is **admin** and the default password is **netwitness**.
You are logged onto the RSA physical host and the following message is displayed:
`Successfully logged in as session <session #>`
3. At the localhost prompt `[localhost:50006] />` do one of the following:
 - a. If you want to use your network clock source, enter the following command:
`appliance setNTP source=<NTP_server_hostname or IP_address>`
For example: `appliance setNTP source=0.pool.ntp.org`
 - b. If you want to use the RSA physical host clock as a clock source, type:
`appliance setNTP source=local`
4. When you see an output of `Success` from the command, type `exit` to log out and exit the NwConsole program.

Note: If you specified an NTP clock source of local, the RSA physical host clock serves as the clock source and the time is configured using Set Host Built-In Clock as described in NetWitness Platform online documentation.

Finish Host Setup in NetWitness Platform

To finish configuration of a Series 6 host, you need to log on to NetWitness Platform and use the configuration options available in the NetWitness Platform Administration module. Each type of host has a slight variation in configuration steps. This section provides basic information and links to online help documents to guide you through the process.

Log On to NetWitness Platform

RSA NetWitness Platform is a web-based application that you launch in a browser window. Compatible browsers include any browser that supports WebSockets, LocalStorage, and the HTML5 History API: Google Chrome, Apple Safari, Mozilla Firefox, and Internet Explorer 10 and above.

1. Type the following in your web browser:
`https://<hostname or IP address>/login`
Where <hostname or IP address> is the hostname or IP address of your Security Analytics Server host.
The NetWitness Platform login screen is displayed.
2. Type your username and password, and then click **Login**.
The system administrator account username for NetWitness Platform is **admin** and the default password is **netwitness**.

Open the Online Help

Instructions for configuring individual RSA physical hosts are provided based on the software version installed on the host.

For NetWitness Platform 10.6.5.2 or later 10.6.x.x versions, read these documents: *Configuration Guides* and the *Licensing Guide*. A good starting point to understand the general configuration process and begin configuration is the *Hosts and Services Getting Started Guide*. To locate these documents, go to the NetWitness® Platform online documentation at RSA Link (<https://community.rsa.com/docs/DOC-40370>) and for your software version, click the **Documentation** link. The configuration guides are in the **Configuration** section and the Licensing Guide is in the **Administration** section.

11.1.0.2 and Later Installation Tasks

If you are on NetWitness® Platform version 11.1.0.2 or later, go to the *Physical Host Installation Guide* and follow the steps for installing and configuring your RSA physical host. To locate this document, go to the NetWitness® Platform online documentation at RSA Link (<https://community.rsa.com/docs/DOC-40370>) and for your software version, click the **Documentation** link. This guide is located in the **Installation & Upgrade Guides** section.

Note: NetWitness® Platform Series 6 hosts, except those on Analytics hardware, require version 11.1.0.2 or later. Series 6 Analytics hardware (ESA and UEBA) requires version 11.2 or later.

NIC Bonding

The following procedure outlines a NIC Bonding fault tolerance configuration. If one of the underlying physical NICs is broken or its cable is unplugged, the NW host will detect the fault condition and automatically failover traffic to the slave NIC in the bond, which eliminates a single point of failure for the network interfaces.

The following is an example for bonding em1 or em2 (1G copper interfaces) for use as management interface “eth0”.

Warning: Do not run `nwsetup-tui` before configuring NIC bonding.

1. Log into host through Integrated Dell Remote Access Controller (iDRAC) or console connection.

2. List the interfaces using the following command:

```
ifconfig -a
```

Check the network and make sure that em1, em2 are set to ONBOOT=no

3. Verify the following interface types are 1G copper. Supported link modes should return 1000baseT

```
ethtool <Interface name>
```

Make sure that the link modes are correct.

For example, `ethtool em1`

```
[root@NWAPPLIANCE30202 network-scripts]# ethtool em1 | grep -i -A2 'Supported link modes'
Supported link modes:    10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
```

4. Enable the bonding using the following command:

```
modprobe --first-time bonding
```

5. Verify if the bonding is enabled using the following command:

```
modinfo bonding
```

```
[root@NWAPPLIANCE30202 network-scripts]# modinfo bonding
filename:                /lib/modules/3.10.0-1160.11.1.el7.x86_64/kernel/drivers/net/bonding/bonding.ko.xz
author:                  Thomas Davis, tadavis@lbl.gov and many others
description:             Ethernet Channel Bonding Driver, v3.7.1
version:                 3.7.1
license:                 GPL
alias:                   rtnl-link-bond
retpoline:               Y
rhelversion:             7.9
srcversion:              3B2F8F8533AEAE2EB01F706
depends:                  :
intree:                  Y
vermagic:                3.10.0-1160.11.1.el7.x86_64 SMP mod_unload modversions
signer:                  CentOS Linux kernel signing key
sig_key:                 CE:19:A5:22:D5:5C:85:59:DF:08:5B:03:96:45:91:52:2B:41:E9:03
sig_hashalgo:            sha256
```

6. Create bonding definition file.

- a. Navigate to script directory using the following command:

```
cd /etc/sysconfig/network-scripts/
```

- b. Create `ifcfg-eth0` using the following command:

```
vi ifcfg-eth0
```

Add the following attributes in the file:

```
DEVICE=eth0
```

```
TYPE=Bond
```

```
NAME=eth0
```

```
BONDING_MASTER=yes
BOOTPROTO=none
IPADDR=<ip address of the host>
```

IMPORTANT: This IP address MUST be assigned during nwsetup-tui network configuration.

```
NETMASK=255.255.255.x
GATEWAY=192.x.x.x
BONDING_OPTS="mode=1 miimon=100"
```

c. Save the `ifcfg-eth0` file

7. Open the interface definition file for `em1` using the following command:

```
vi ifcfg-em1
```

Make a note of UUID.

a. Remove the attributes except the UUID and append the following attributes:

```
TYPE="Ethernet"
BOOTPROTO=none

NAME=em1

UUID=xxxxxxxx-yyy-zzzz-aaaa-bbbbbbbbbbbbbb

DEVICE=em1

ONBOOT=yes

MASTER=eth0

SLAVE=yes
```

b. Save the `ifcfg-em1` file.

8. Open the interface definition file for `em2` using the following command:

```
vi ifcfg-em2
```

Make a note of UUID.

a. Remove the files except the UUID and append the following attributes:

```
TYPE=Ethernet

BOOTPROTO=none

NAME=em2

UUID=xxxxxxxx-yyy-zzzz-aaaa-bbbbbbbbbbbbbb

DEVICE=em2

ONBOOT=yes

MASTER=eth0

SLAVE=yes
```

b. Save the `ifcfg-em2` file

9. Open the interface definition file for `em3` using the following command:

```
vi ifcfg-em3
```

a. Make sure the following attributes in the file are as below:

```
ONBOOT=no
```

b. Save the `ifcfg-em3` file.

10. Open the interface definition file for em4 using the following command:

```
vi /etc/sysconfig/network-scripts/ifcfg-em4
```

- a. Make sure the following attributes in the file are as below:

```
ONBOOT=no
```

- b. Save the file.

11. Restart the network service using the following command:

```
systemctl restart network
```

12. Verify that em1, em2 and bond interface is active using the following command:

```
systemctl restart network
```

13. Check the status of bond interface (ifcfg-eth0) using the following command:

```
cat /proc/net/bonding/eth0
```

Make sure that em1, em2 are listed and Bonding Mode is 'fault-tolerance (active-backup)' and Speed is 1000 Mbps.

```
[root@NWAPPLIANCE5847 ~]# cat /proc/net/bonding/eth0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)
```

```
Bonding Mode: fault-tolerance (active-backup)
```

```
Primary Slave: None
```

```
Currently Active Slave: em2
```

```
MII Status: up
```

```
MII Polling Interval (ms): 100
```

```
Up Delay (ms): 0
```

```
Down Delay (ms): 0
```

```
Slave Interface: em1
```

```
MII Status: up
```

```
Speed: 1000 Mbps
```

```
Duplex: full
```

```
Link Failure Count: 0
```

```
Permanent HW addr: e4:43:4b:04:5b:a8
```

```
Slave queue ID: 0
```

```
Slave Interface: em2
```

```
MII Status: up
```

```
Speed: 1000 Mbps
```

```
Duplex: full
```

```
Link Failure Count: 0
```

```
Permanent HW addr: e4:43:4b:04:5b:a9
```

```
Slave queue ID: 0
```

```
[root@NWAPPLIANCE5847 ~]# █
```

14. Reboot the host.

15. Verify if the bonding interface is active using the following command:

```
ethtool eth0 | grep -i 'link detected'
```

This returns 'Link detected: yes'

16. After the bonding interface is configured, run `nwsetup-tui` to bootstrap or orchestrate the node. In the **Network Platform Network Configuration** prompt, select the `eth0` interface as the network interface.
 - a. If **Use DHCP** is selected, after bootstrap or orchestration of the nodes, perform the following:
 - i. Edit the bond interface file using the following command:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```
 - ii. Delete the `NETMASK` attribute

Note: The `NETMASK` attribute value should not conflict with `NETMASK` defined in the `dhcp` server for this network.

 - i. Save the file.
 - b. If **Static IP Configuration** is selected, the **Subnet Mask** corresponds to the `NETMASK` attribute in the bond interface (`/etc/sysconfig/network-scripts/ifcfg-eth0`) definition. For example, `NETMASK=23` corresponds to `NETMASK =255.255.254.0`.

Note: The `NETMASK` value is not automatically updated when the **Subnet Mask** value is set. These two attributes values should not be in conflict.

 - i. After running `nwsetup-tui`, you must delete `NETMASK` attribute from the bonding interface `ifcfg-eth0`.

Example for Bonding `em3` or `em4` (10G fiber interfaces)

The following is an example for bonding `em3` or `em4` (10G fiber interfaces) for use as management interface '`eth0`'

Warning: Do not run `nwsetup-tui` before configuring NIC bonding.

1. Log into host through Integrated Dell Remote Access Controller (iDRAC) or console connection.
2. List the interfaces using the following command:

```
ifconfig -a
```

Make sure that `em1`, `em2`, `em3`, `em4`, and `lo` are listed.
3. Verify that the `eth3` and `eth4` interface types are 10G fiber.

```
ethtool <Interface name>
```

For example, `ethtool em3`
4. Enable the bonding using the following command:

```
modprobe --first-time bonding
```

5. Verify if the bonding is enabled using the following command:

```
modinfo bonding
```

```
[root@NWAPPLIANCE30202 network-scripts]# modinfo bonding
filename:           /lib/modules/3.10.0-1160.11.1.el7.x86_64/kernel/drivers/net/bonding/bonding.ko.xz
author:             Thomas Davis, tadavis@lbl.gov and many others
description:        Ethernet Channel Bonding Driver, v3.7.1
version:            3.7.1
license:            GPL
alias:              rtnl-link-bond
retpoline:         Y
rhelversion:        7.9
srcversion:         3B2F8F8533AEAE2EB01F706
depends:
intree:            Y
vermagic:           3.10.0-1160.11.1.el7.x86_64 SMP mod_unload modversions
signer:             CentOS Linux kernel signing key
sig_key:            CE:19:A5:22:D5:5C:85:59:DF:08:5B:03:96:45:91:52:2B:41:E9:03
sig_hashalgo:      sha256
```

6. Create bonding definition file.

- a. `cd /etc/sysconfig/network-scripts/`

- b. `vi ifcfg-eth0`

Add the following attribute in the file:

```
DEVICE=eth0
TYPE=Bond
BONDING_MASTER=yes
IPADDR=<ip address of the host>
```

IMPORTANT: This IP address MUST be assigned during `nwsetup-tui` network configuration.

```
NETMASK=<subnet NETMASK>
```

```
GATEWAY=192.x.x.x
BONDING_OPTS="mode=1 miimon=100"
BOOTPROTO=none
NAME=eth0
ONBOOT=yes
```

- c. Save the file

7. Open the interface definition file for `em3` using the following command:

```
vi /etc/sysconfig/network-scripts/ifcfg-em3
```

- a. Make sure the following attributes in the file are as below:

- i. `BOOTPROTO=none`
- ii. `ONBOOT=yes`

- b. Add the below attributes to the end of the file:

- i. `MASTER=eth0`
- ii. `SLAVE=yes`

- c. Delete the following attributes in the file:

- i. `HWADDR` (mac address) line
- ii. `IPADDR` (if exists)

- iii. NETMASK (if exists)
 - iv. GATEWAY (if exists)
 - d. Save the file
8. Open the interface definition file for em4 using the following command:
- ```
vi /etc/sysconfig/network-scripts/ifcfg-em4
```
- a. Make sure the following attributes in the file are as below:
    - i. BOOTPROTO=none
    - ii. ONBOOT=yes
  - b. Add the below attributes to the end of the file:
    - i. MASTER=eth0
    - ii. SLAVE=yes
  - c. Delete the following attributes in the file:
    - i. HWADDR (mac address) line
    - ii. IPADDR (if exists)
    - iii. NETMASK (if exists)
    - iv. GATEWAY (if exists)
  - d. Save the file
9. Open the interface definition file for em1 using the following command:
- ```
vi /etc/sysconfig/network-scripts/ifcfg-em1
```
- a. Make sure the following attributes in the file are as below:
ONBOOT=no
 - b. Save the file.
10. Open the interface definition file for em2 using the following command:
- ```
vi /etc/sysconfig/network-scripts/ifcfg-em2
```
- a. Make sure the following attributes in the file are as below:  
ONBOOT=no
  - b. Save the file.
11. Restart the network service using the following command:
- ```
service network restart
```
12. Verify that em3, em4 and bond interface is active using the following command:
- ```
service network status
```
13. check the status of bond interface (ifcfg-eth0) using the following command:
- ```
cat /proc/net/bonding/eth0
```
- Make sure that em0,em3, em4 are listed and Bonding Mode is 'fault-tolerance (active-backup)' and Fiber = 10000.

14. Disable em1 and em2 configuration using the following command (This removes the config file for em1 and em2):

```
echo "DEVICE=em1" > /etc/sysconfig/network-scripts/ifcfg-em1
echo "DEVICE=em2" > /etc/sysconfig/network-scripts/ifcfg-em2
```

- a. Restart the network service using the following command:

```
service network restart
```

15. Reboot the host.

16. Verify if the bonding interface is active using the following command:

```
ethtool em1 | grep -i 'link detected' shall return 'Link detected: yes'
```

17. After the bonding interface is configured, run `nwsetup-tui` to bootstrap or orchestrate the node. In the **Network Platform Network Configuration** prompt, select the eth0 interface as the network interface.

- a. If **Use DHCP** is selected, after bootstrap or orchestration of the nodes, perform the following:

- i. Edit the bond interface file using the following command:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

- ii. Delete the **NETMASK** attribute

Note: The **NETMASK** attribute value should not conflict with **NETMASK** defined in the dhcp server for this network.

- i. Save the file.

- b. If **Static IP Configuration** is selected, the **Subnet Mask** corresponds to the **NETMASK** attribute in the bond interface (`/etc/sysconfig/network-scripts/ifcfg-eth0`) definition. For example, `NETMASK=23` corresponds to `NETMASK =255.255.254.0`.

Note: The **NETMASK** value is not automatically updated when the **Subnet Mask** value is set. These two attributes values should not be in conflict.

- i. After running `nwsetup-tui`, you must delete **NETMASK** attribute from the bonding interface `ifcfg-eth0`.

Revision History

Date	Description
June 27, 2018	Series 6 Hosts Hardware Setup Guide for NetWitness® Platform version 11.1.0.2 and later
July 17, 2018	Moved the PERC H840 RAID controller to slot 4 for the Series 6 Hybrid host.
July 31, 2018	Added information for ESA physical hosts for NetWitness® Platform version 11.2 and later. Added instructions for NetWitness® Platform version 10.6.5.2 and later.
October 17, 2018	Added SKUs to Hardware specifications. Added information about the inverted PERC H840 card in the R740xd Hybrid, which reverses the ports. Port 0 is on the right and port 1 is on the left on the R740xd Hybrid. You must attach cables to the R740xd with the connector's blue tab on the bottom.
February 9, 2019	Made adjustments and updated titles for additional installation tasks to further clarify the versions needed for those tasks.
April 10, 2019	Added additional hard drive details to the Hardware specifications. NetWitness Platform 11.3 and later supports Hybrid host software on the Dell PowerEdge R640. Additional external storage is required.
July 17, 2019	Added a Series 6 Hardware Specifications table, which replaces the individual hardware specification tables. Added UEBA to the S6 Hardware Description. Renamed the "Connect the Host to the Network" section to "Connect to the Series 6 Hardware Console" and shortened it.
July 29, 2019	Corrected the Series 6 hard drive specifications in the Series 6 Hardware Specifications table. The NL-SAS drives listed should all show 7.2K (not 7.5K).
October 22, 2019	Added support for Series 6E self-encrypted drive (SED) hardware.
February 12, 2020	Added Supported SFPs & Add-On Cards to the Series 6 Hardware Specifications table.