



# Storage Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Contact Information**

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

## **Trademarks**

For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **License Agreement**

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

## **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 RSA Link. 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**

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

May 2019

# Contents

---

<b>Storage Overview .....</b>	<b>5</b>
Storage Terms and Abbreviations .....	5
<b>RSA NetWitness Platform Storage Requirements .....</b>	<b>7</b>
Storage Requirements .....	7
Performance Recommendations .....	7
Recommended Storage Allocation Per NetWitness Host .....	8
Input/Output Operations Per Second .....	8
General Description of How NetWitness Platform Hosts Store Data .....	9
Decoder Hosts .....	9
Concentrator Host .....	9
Archiver Host .....	10
Hybrid Hosts .....	10
Options for SAN Configurations .....	10
<b>Using the REST API to Configure Configuration .....</b>	<b>11</b>
Configure Storage with REST API .....	11
REST API Storage Configuration Commands .....	13
Commands for Direct-Attached RAID Volumes .....	13
Commands for Allocating Block Devices as Storage .....	13
Commands for Allocating Storage to Services .....	13
Create RAID Volumes for Direct-Attached Storage (PowerVault & DAC) .....	13
Allocating SAS Enclosures .....	14
Using Self-Encrypting Drives .....	15
Prepare Virtual or Cloud Storage .....	15
Allocate Block Devices (Direct Attached or Virtual Storage) .....	16
Usage .....	16
NetWitness Service Volume Reference .....	17
Allocate Storage to a Service (All External Storage Devices) - srvAlloc .....	19
<b>Prepare Unity Storage .....</b>	<b>20</b>
Task 1 - Access Unisphere User Interface (UI) .....	21
Task 2 - Create Pools .....	22
Task 3 - Create LUNS .....	25
Task 4 - Register Hosts .....	27
Task 5 - Assign LUNS to Hosts .....	29
Task 6 - Install PowerPath .....	32

**Migrate Data to Another Storage Type ..... 33**

    Data on DAC Before Move to PowerVault ..... 33

    Data on PowerVault After Move from DAC ..... 35

**Enable or Validate Encryption to Existing PowerVault (encryptSedVd.py) ..... 36**

**Revision History ..... 38**

## Storage Overview

---

This guide provides you with storage requirements and the instructions on how to allocate storage for physical (DACs, PowerVaults, Unity) and virtual storage devices for RSA NetWitness Platform. It also includes the following topics.

- Detect Encryption on Existing PowerVault
- Migrate Data to Another Device

Refer to the following Hardware Setup Guides for information on how to connect these device to RSA NetWitness Platform Core and Hybrid physical hosts:

- 60-Drive DAC Setup Guide - RSA Link <https://community.rsa.com/docs/DOC-44956>
- 15-Drive DAC Setup Guide - RSA Link <https://community.rsa.com/docs/DOC-44957>
- PowerVault (MD 1400) Setup Guide - RSA Link <https://community.rsa.com/docs/DOC-94091>

## Storage Terms and Abbreviations

Term	Description
CPU	Central Processing Unit
EPS	Events Per Second
VMware ESX	Enterprise-class, type-1 hypervisor, Supported versions - 6.5, 6.0 and 5.5
GB	Gigabyte. 1GB = 1,000,000,000 bytes
Gb	Gigabit. 1Gb = 1,000,000,000 bits.
Gbps	Gigabits per second or billions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
GHz	GigaHertz 1 GHz = 1,000,000,000 Hz
IOPS	Input/Output Operations Per Second
Mbps	Megabits per second or millions of bits per second. It measures bandwidth on a digital data transmission medium such as optical fiber.
NAS	Network Attached Storage
OVF	Open Virtualization Format
OVA	Open Virtual Appliance. For purposes of this guide, OVA stands for Open Virtual Host.
RAM	Random Access Memory (also known as memory)
SAN	Storage Area Network
SSD/EFD HDD	Solid-State Drive/Enterprise Flash Drive Hard Disk Drive

Term	Description
SCSI	Small Computer System Interface
SCSI (SAS)	Point-to-point serial protocol that moves data to and from computer storage devices such as hard drives and tape drives.
TB	Terabyte. It equals <b>1000<sup>4</sup></b> bytes.
vCPU	Virtual Central Processing Unit (also known as a virtual processor)
vRAM	Virtual Random Access Memory (also known as virtual memory)
RSA NetWitness UEBA	RSA NetWitness User and Entity Behavior Analysis
Hyper-V	Microsoft Hyper Visor, Supported version 2016 Server
VHDX	Hyper-V virtual hard disk

## RSA NetWitness Platform Storage Requirements

---

This section contains generic RSA NetWitness Platform storage requirements. Contact your NetWitness Platform representative for a detailed analysis of the current and future storage requirements for your NetWitness Platform deployment.

### Storage Requirements

General specifications for core NetWitness Platform Hosts:

- IO size 490/Dec
- Block size 128K
- Response/Latency < 20ms
- Decoder 10/90 read/write (low random I/O)
- Concentrator 50/50 read/write (high random I/O)

RAID Group	Suitable Volumes
NL-SAS or 10K SAS	All Packet Decoder volumes All Log Decoder volumes All Archiver volumes Concentrator meta volume
SSD	Concentrator index volume

### Performance Recommendations

RSA recommends that Packet and Log Decoders receive two LUNs or Block Devices, one for Packet data, the other for all other databases. This allows you to segregate the high-bandwidth Packet Database from the other databases so they do not compete for I/O bandwidth with other activity.

Concentrators require a separate SSD-based index volume for best performance. You must house this index volume on a different RAID group than the Concentrator Meta database volume, which you can stored on NL-SAS. Archivers can use a single large NL-SAS storage volume per appliance.

## Recommended Storage Allocation Per NetWitness Host

Host Type	First LUN/Block Device	Second LUN/Block Device
Decoder	Meta/Session Volume (smaller volume)	Packet Volume (large volume)
Log Decoder	Meta/Session Volume (medium-sized volume)	Packet Volume (medium-sized volume)
Concentrator	Meta Volume (large volume)	Index Volume (smaller SSD volume)
Archiver	Data Archive Volume (large volume)	Not used

## Input/Output Operations Per Second

The following table lists the IOPS requirements for the Decoder and Concentrator hosts.

Logs	Log Decoder	Concentrator
10K EPS	400	8,000
20K EPS	550	10,300
25K EPS	1,200	10,800

Packets	Network Decoder	Concentrator
1Gbps	600	6,050
2 Gbps	950	8,300
4 Gbps	1,650	12,800
6 Gbps	2,400	17,300
8 Gbps	3,200	21,800



## General Description of How NetWitness Platform Hosts Store Data

In most deployments, NetWitness Platform Decoders, Log Decoders, Concentrators, Archivers, and Hybrid hosts require external storage to house their data. Each host uses the external storage in different ways and with different expectations on throughput and performance of the external storage. Some hosts have a higher occurrence of sequential writes and some hosts have a higher occurrence of random reads and writes.

### Decoder Hosts

Log Decoders and Network Decoders capture data and parse meta. The difference between these two hosts is in the type of data they capture:

- Log Decoder captures logs.
- Network Decoder captures packets.

Both Log Decoders and Network Decoders parse out meta data from the raw captured traffic. The meta data is then aggregated to a Concentrator for indexing. The host requires storage to house the raw payload data (raw packets or raw logs) and a cache for the meta extracted during data capture for Concentrator aggregation.

Your retention requirements is a key factor in determining the amount of storage you need for the raw packets or raw logs. In most deployments, you add storage over time based on increased retention requirements and increased capture rates. The storage for the raw data must support a high amount of sequential writes with random reads. Especially in the case of higher speed Network Decoder environments, it is recommended to have a minimum of two partitions exposed to the host to support the throttling between partitions for reads and writes.

The meta cache on a Decoder is generally fixed in size but you can expand it to support additional cache the possible loss of connectivity between the Decoder and a corresponding Concentrator. The meta cache must support a random IOPS rate for sustained writes from the Decoder of meta extracted and the corresponding reads from the Concentrator as meta is aggregated to a Concentrator.

### Concentrator Host

A Concentrator aggregates and indexes the meta data from a Decoder. Both the meta and index storage needs are scaled based on your NetWitness Platform deployment retention requirements. Similar to raw data stored on the Decoders, you may need to increase the storage for both meta data and index data over time to meet your retention requirements.

The meta storage houses all meta data extracted from either a Network Decoder or Log Decoder. Although the ratio of how much meta is extracted may change, the expectations for performance against meta storage is the same for both packet capture and log capture environments. The meta storage must support a sustained amount of sequential writes with random reads of meta data.

The index storage houses the live index generated from the meta data aggregated to a Concentrator. The size of the index is directly related to the size of the meta store. In addition to supporting IOPS for sustained writes, the index also needs to support a much higher rate IOPS for reads than meta based on interactive queries run through analyst interaction and reports and alerts.

## Archiver Host

The Archiver host requires a single partition for both meta and raw log storage. The storage pool deals primarily with sequential writes for long term data written from a Log Decoder or Network Decoder and random reads for reports and analysis.

## Hybrid Hosts

A Hybrid hosts two or more services on a single host. For example, a:

- Network Hybrid hosts both the Decoder and Concentrator services handling packets exclusively. It captures packet data and indexes this data to the Concentrator service. Expectations for storage performance match what is outlined for a dedicated Network Decoder host and dedicated Concentrator host.
- Log Hybrid hosts both the Log Decoder and Concentrator services handling logs exclusively. It captures log data and indexes the data to a Concentrator service. Expectations for performance match what is outlined for a dedicated Log Decoder and dedicated Concentrator.

## Options for SAN Configurations

If you want to use a Storage Area Network (SAN) , use the same basic drive groups and partition organization that you use for the other RSA storage devices. Depending on the SAN configuration and overhead, SAN configurations may require more enclosures and drives to operate with the same performance as on PowerVault or DAC. When deciding whether to use SAN, PowerVault, or DAC, any additional overhead on the SAN will be important to determine the minimum storage required.

## Using the REST API to Configure Configuration

---

In NetWitness Platform 11.3 and later releases, you use the REST API for all storage configuration operations. This section describes how to:

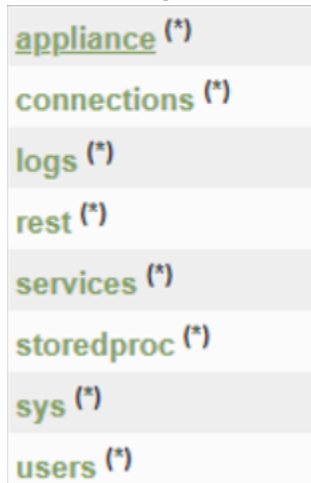
- [Configure storage with the REST API commands](#) (including a [list of these commands](#)).
- [Create RAID volumes for direct-attached storage](#) (that is, DACs & PowerVaults).
- [Allocate block devices for direct-attached or virtual storage](#).
- [Allocate storage to a service](#) (all external storage devices)

### Configure Storage with REST API

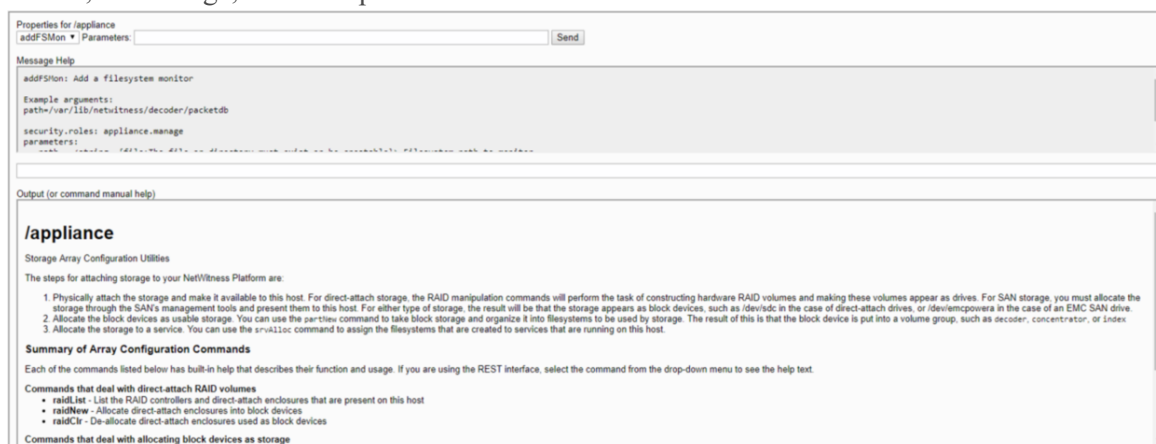
The following steps summarize how to configure storage for your NetWitness Platform hosts. See the detailed steps for the later in this section for the storage device you are configuring.

1. Physically attach the storage and make it available to this host.
  - For direct-attach storage, the RAID manipulation commands construct the hardware RAID volumes and make these volumes appear as drives.
  - For SAN storage, you must allocate the storage through the SAN management tools and present them to this host.
  - After you attach either type of storage, the storage appears as block devices (that is, `/dev/sdc` for direct-attach drives, or `/dev/emcpowera` for an EMC SAN drive. Attaching storage to a virtual or cloud instance also presents a block device to the host.
2. Log into the REST API Interface.
  - a. Open a Browser and specify the ip-address of the host using the correct port (for example, use port **50106** for the Network Decoder).  
`https://<decoder-ip-address>:50106`

- b. Log in with the `admin` account credentials.  
The following REST API menu is displayed.



- c. Click on the `(*)` next to **appliance** to access the REST command set.  
The **Properties for /appliance** dialog is displayed under the initial REST menu. The **Output (or command manual help)** section describes the commands that the REST API can send to the device, their usage, and their parameters.



## REST API Storage Configuration Commands

Each of the commands listed below has built-in help that describes their function and usage. If you are using the REST interface, select the command from the drop-down menu to see the help text.

### Commands for Direct-Attached RAID Volumes

- `raidLst` - List the RAID controllers and direct-attach enclosures that are present on this host.
- `raidNew` - Allocate direct-attached enclosures to block devices.

### Commands for Allocating Block Devices as Storage

- `devlSt` - List available block devices on the host.
- `partNew` - Allocate partitions on a block device and create volume groups.
- `vgs` - Summarize how block devices are organized into volume groups.

### Commands for Allocating Storage to Services

- `srvList` - List services on the host and their allocated storage paths.
- `srvAlloc` - Allocate a volume group to a service.
- `srvFree` - Remove a volume group from a service.

## Create RAID Volumes for Direct-Attached Storage (PowerVault & DAC)

NetWitness Platform hardware uses direct-attached SAS drives for storage. These drives are housed in a SAS enclosure. SAS enclosures are shelves of drives attached to the NetWitness node by a cable connected to the SAS host bus adapter.

SAS enclosures are also known as other names, such as "DAC" (Direct-Attached Capacity), or "JBOD" (Jumbo Box of Disks), or "Dell PowerVault".

NetWitness Platform utilizes Dell PERC SAS host bus adapters. NetWitness Platform devices typically include two SAS host bus adapters. One is used for controller drives that are internal to the NetWitness Node, and another is used for controlling drives attached to the SAS enclosures. The internal controller and drives are configured when the node is built, but the external SAS enclosures are not. This command is used to configure the external SAS enclosures.

This command works with the following SAS enclosure types:

- EMC ESAS 15-drive enclosures
- EMC ESAS 60-drive enclosures
- Dell PowerVault 12-drive enclosures

**Note:** EMC 60-drive enclosures are logically organized as four separate 15-drive sub-enclosures. They behave as if there are four 15-drive enclosures, each of which can be configured independently.

## Allocating SAS Enclosures

This command operates on entire enclosures. It can configure an enclosure to perform one of the pre-determined roles within a NetWitness Platform node.

To allocate an enclosure, you must identify it by specifying the controller it is attached to and the Enclosure ID.

You can identify the controllers and enclosures that are attached to the system by using the `raidList` command. In the following example, Controller 1 does not display any block devices. This indicates the array is not configured.

Properties for /appliance  
 Parameters:

Message Help  

```
raidList: list drive shelves attached to this appliance
security.roles: appliance.manage
```

Output (or command manual help)  

```
Controller 0, Enclosure 32
Vendor: DP
Model: BP13G+EXP
In Use: true
Drives: 931.511 GB x 2
        1.818 TB x 2
Devices: sda
        sdb

Controller 1, Enclosure 82
Vendor: DELL
Model: MD1400
In Use: false
Drives: 10.691 TB x 12
Devices:

Controller 1, Enclosure 13
Vendor: DELL
Model: MD1400
In Use: false
Drives: 10.691 TB x 12
Devices:
```

You must select a RAID layout scheme for the Enclosure. The following tables show you the supported allocation schemes.

Scheme	Drives Required	Allocation
decoder	12 or 15 HDDs	3x drives in RAID 5 for decodersmall, all remaining drives in RAID 5 for decoder
log decoder	12 or 15 HDDs	Same as decoder
archiver	12 or 15 HDDs	All drives in RAID 6 for archiver or decoder database volume

Scheme	Drives Required	Allocation
network hybrid	12 or 15 HDDs	3x drives in RAID 5 for meta expansion, all remaining drives in RAID 5 for packet expansion
log hybrid	12 or 15 HDDs	Half of the drives in RAID 5 for meta expansion, half the drives in RAID 5 for packet expansion
concentrator	3 or more SSDs, 3 or more HDDs	All SSDs in RAID 5 for index, all HDDs in RAID 6 for meta

After the controller, enclosure and scheme are identified, execute the `raidNew` command to create RAID Volumes. For example:

```
send /appliance raidNew controller=1 enclosure=82 scheme=decoder
preferSecure=false
```

Add the `commit=1` parameter to actually execute this operation. Execute the `raidList` command to list the created block devices.

Proceed to [Allocate Block Devices](#), after the `raidNew` command is successful.

## Using Self-Encrypting Drives

If the `raidNew` command detects self-encrypting drives and a security key has been set on the controller, the `raidNew` command will attempt to create a secure array. To set a security key on the controller, use the `raidKey` command. For example:

```
send /appliance raidKey controller=1 key=myPassssphrase keyId=1
```

To create an unsecured (that is, unencrypted) array on physical devices attached to a controller with a security key set, specify `preferSecure=false` when using `raidNew`.

## Prepare Virtual or Cloud Storage

Virtual or Cloud NetWitness Hosts need block storage attached. Make sure that the allocated storage meets all of the [RSA NetWitness Platform Storage Requirements](#). Specifically, make sure that:

- You have at least two Block Devices are created for Decoders (meta /session and packet volumes)
- You have at least two block devices are created for Concentrators (index and meta volumes)
- Ensure block devices can meet the minimum IOPS for expected ingestion rates

Attach the allocated storage to the NetWitness Host by following the hosting platforms native procedure.

- VmWare – Vsphere Console (add disk to VM)
- Hyper-V – Manager Console (add disk to VM)
- Azure – Add Managed Disks to virtual instance.
- AWS – Add EBS Storage to virtual instance.

After the storage is attached to the virtual host, proceed to [Allocate Block Devices](#).

## Allocate Block Devices (Direct Attached or Virtual Storage)

The `partNew` command prepares a storage device to use in NetWitness Platform. It performs the following tasks.

1. Creates the partition table on the block device.
2. Creates the Linux Volume Manager physical device partition.
3. Creates a volume group containing the physical device.
4. Creates logical volumes in the volume group.
5. Creates XFS filesystems on each logical volume.
6. Creates `/etc/fstab` entries for each logical volume.
7. Mounts each logical volume.

### Usage

You must provide the block device name, for example, `sdc`, `/dev/sdc`, or `/dev/emcpowera`. Use the `devlist` command to locate unused block devices.

#### Output (or command manual help)

```
sda: vendor=DELL model="PERC H730P Mini" size="931 GB" used=1
sdb: vendor=DELL model="PERC H730P Mini" size="1.81 TB" used=1
sdc: vendor=DELL model="PERC H830 Adp" size="21.38 TB" used=1
sdd: vendor=DELL model="PERC H830 Adp" size="85.53 TB" used=1
```

You must provide a name for the service that will be used with the storage, for example, "decoder" or "concentrator" and you have the option of providing the volume type. The default volume type has the same name as the service.

By default, the `partNew` command does not make changes. It displays the actions that will be taken if you commit the command string. To actually make the changes to the system, add the `commit=true` parameter to the command. For example, to assign devices `sdd` and `sde` to Decoder:

```
send /appliance partNew name=sdc service=decoder volume=decodersmall
send /appliance partNew name=sdd service=decoder volume=decoder
```

**Note:** Note that you must create the `decodersmall` volume before the `decoder` volume because it holds the small filesystem mounted at `/var/netwitness/decoder`. For example to assign device `sdc` to archiver:

```
send /appliance partNew name=sdc service=archiver
```

Note that we do not need to specify a volume type. It is assumed that the volume type is `archiver`.

Execute the `vgs` command. This command enumerates all the volume groups on this host. In addition, it displays the physical volumes that the volume group consists of, and the logical volumes within the volume group. The output will validate the `partNew` command created the appropriate Logical Volumes.

Go to [Allocate Storage to a Service](#) to complete the storage configuration.



## NetWitness Service Volume Reference

### Service Volume Names

Service	Volume Name	Filesystems Created
decoder	decoder	packetdb
decoder	decodersmall	decoder root, index, sessiondb, metadb
logdecoder	logdecoder	packetdb
logdecoder	logdecodersmall	logdecoder root, index, sessiondb, metadb
concentrator	concentrator	concentrator root, metadb, sessiondb
concentrator	index	index
archiver	archiver	database

### Volume Sizing

Volume	Filesystem	Mount Point	Size
decodersmall	decoroot	/var/netwitness/decoder	10 GB
decodersmall	index	/var/netwitness/decoder/index	30 GB
decodersmall	sessiondb	/var/netwitness/decoder/sessiondb	600 GB
decodersmall	metadb	/var/netwitness/decoder/metadb	100% of free space on decodersmall volume
decoder	packetdb	/var/netwitness/decoder/packetdb	100% of free space on decoder volume
logdecodersmall	decoroot	/var/netwitness/logdecoder	10 GB
logdecodersmall	index	/var/netwitness/logdecoder/index	30 GB
logdecodersmall	sessiondb	/var/netwitness/logdecoder/sessiondb	600 GB
logdecodersmall	metadb	/var/netwitness/logdecoder/metadb	100% of free space on logdecodersmall volume
logdecoder	packetdb	/var/netwitness/logdecoder/packetdb	100% of free space on logdecoder volume
concentrator	root	/var/netwitness/concentrator	30 GB
concentrator	sessiondb	/var/netwitness/concentrator/sessiondb	600 GB
concentrator	metadb	/var/netwitness/concentrator/metadb	100% of free space on concentrator volume

Volume	Filesystem	Mount Point	Size
index	index	/var/netwitness/concentrator/index	100% of free space on index volume
archiver	database	/var/netwitness/archiver/database	100% of free space on archiver volume

## Allocate Storage to a Service (All External Storage Devices) - `srvAlloc`

The `srvAlloc` command configures services on a host to use storage in a volume group. You must provide the name of the service to configure and the volume group to assign to the service (the service you provide must be installed on the host).

**Note:** By default, the `srvAlloc` command does not make changes. You must append the `commit=true` parameter to the command string to actually make the changes to the system and restart the specified service after making changes.

Use the `srvLst` command to see a list of services installed on this host. The `srvLst` command communicates with the service through the SSL port. You install a Category on a host. A Category can be a single service, or multiple related services, located on the same host. The following table lists the services by Category.

Category	Services	Encrypted SSL Port
Archiver	Archiver	56008
Concentrator	Concentrator	565005
Log Collector	Log Collector	56001
Log Decoder	Log Collector Log Decoder	56001 56002
Network Decoder		56004

## Prepare Unity Storage

You must work with your Dell EMC Storage Engineer to allocate storage within your Unity environment for the RSA NetWitness Platform and ensure the allocated storage meets all of the RSA NetWitness Platform Storage Requirements. Specifically, make sure that:

- You have at least two LUNS created for Decoders (meta /session and packet volumes).
- You have at least two LUNS created for Concentrators (index and meta volumes).
- Ensure block devices can meet the minimum IOPS for expected ingestion rates.

You must add every RSA NetWitness host that uses the Unity storage as a host within the Unity interface. After you create hosts and LUNs, you must assign the LUNs to the hosts. Assigning the LUNs to hosts makes the storage visible to the hosts so they can locate the storage through the host-based Dell EMC PowerPath software.

**Note:** A Dell EMC engineer will configure the following Unity Array.

You need to perform the following tasks to prepare Unity Storage.

[Task 1 - Access Unisphere User Interface \(UI\)](#)

[Task 2 - Create Pools](#)

[Task 3 - Create LUNS](#)

[Task 4 - Register Hosts](#)

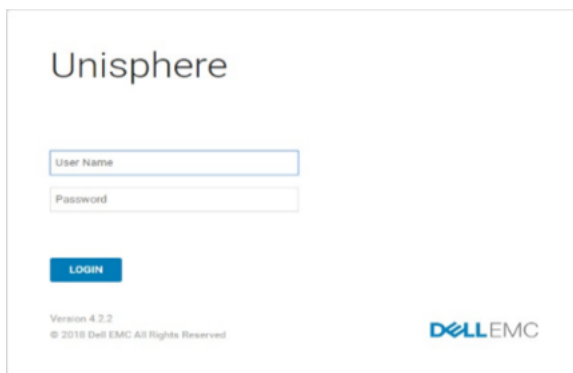
[Task 5 - Assign LUNS to Hosts](#)

[Task 6 - Install PowerPath](#)

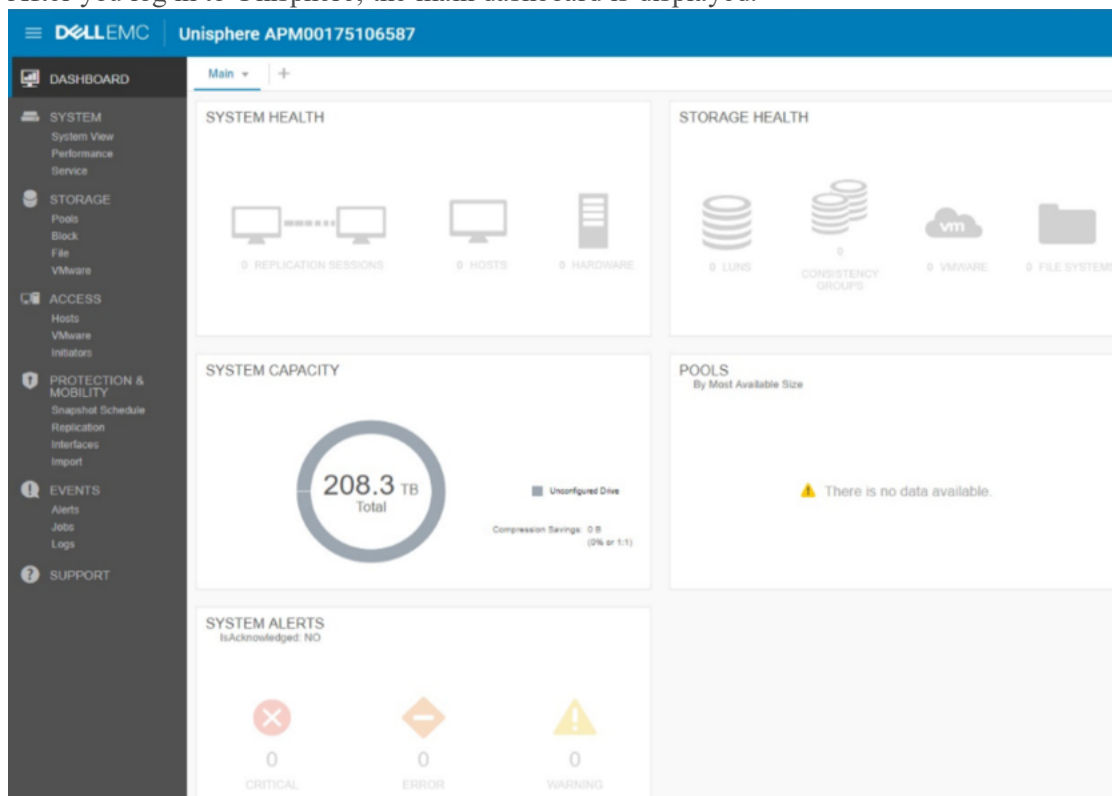
## Task 1 - Access Unisphere User Interface (UI)

1. Connect your workstation on the same subnet as the UNITY.
2. Open a browser and go to **http://<unisphereIP>** to connect to the Unisphere UI.
3. Log in with the credentials provided by the Dell EMC CE. The default credentials are **admin/Password123#**.

**Note:** Unisphere will ask you to change password the first time log in. It also asks you to install the license before you can configure array (Dell EMC CE may do this for you. You must get the new admin password from them).



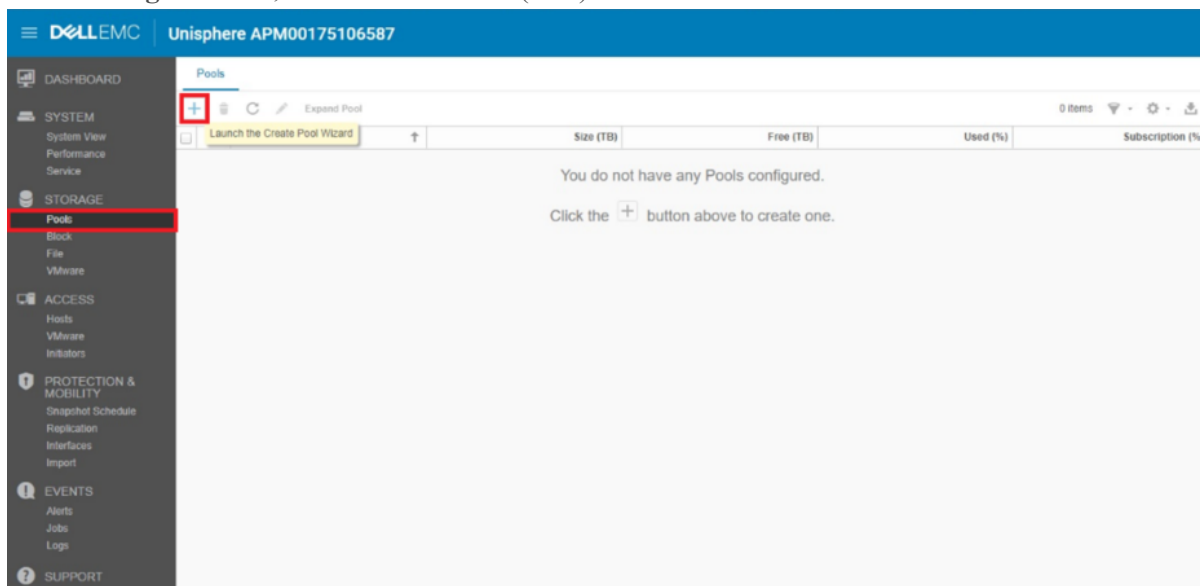
After you log in to Unisphere, the main dashboard is displayed.



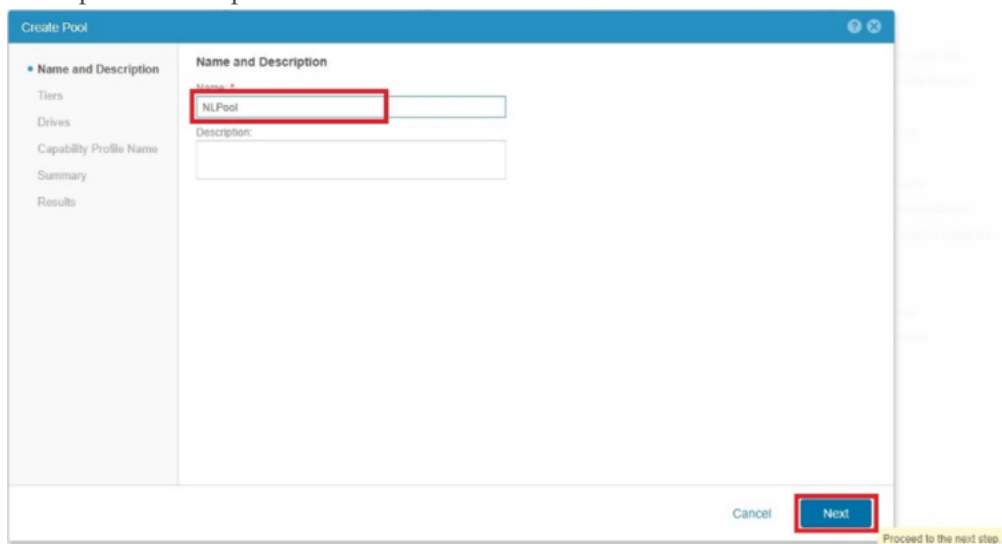
## Task 2 - Create Pools

The NetWitness configuration consists of two different pools. One pool is dedicated to the NL-SAS drives and the other pool is dedicated to the SSDs.

1. From **Storage Section**, click > **Pools** >  (Add) to launch the Create Pool Wizard.



2. Enter in a name for the pool (for example, **NLPool**) and click **Next**. Optionally, you can also enter a description for the pool.



3. Select **Capacity Tier** under **Tier** for the tier type (drive type) and click **Change**.

**Create Pool**

✓ Name and Description  
• Tiers  
Drives  
Capability Profile Name  
Summary  
Results

**Select Storage Tiers**

Available Tiers

Tier	Drive Type	Unused Drives	Unused Capacity (GB)
<input type="checkbox"/> Extreme Performance Tier	SAS FLASH	1	356.7
<input type="checkbox"/> Performance Tier	SAS	6	3,301.8
<input checked="" type="checkbox"/> <b>Capacity Tier</b>	NL SAS	40	229,121.7

☐ Use FAST Cache

**Selected Tiers**

**Capacity Tier**  
RAID 6 (6+2), Maximum Usable Capacity 128.9 TB

[Change](#)

**Extreme Performance Tier**  
Provides very fast access times for resources demanding the quickest response time. Databases can achieve their best performance when using this tier.

**Performance Tier**  
Provides high, all-around performance with consistent response times, high throughput, and good bandwidth. Appropriate for database resources accessed centrally through a network.

**Capacity Tier**  
Provides high storage capacity with generally lower performance. Appropriate for storing large amounts of primarily static data (such as video, audio, and image files) for users and applications without strict performance requirements.

Cancel [Back](#) [Next](#)

4. Choose the RAID type and from the drop down and select the RAID size.  
The RAID type and size are a customer preference. The only requirement is to make sure you have enough IOPS within the pool to accommodate the log or packet capture and queries. In the following example, a **RAID 5 (8+1)** configuration is selected, however some customers may prefer a **RAID 6 (10+2 or 12+2)**.
5. Make sure you have the correct Raid type and size selected.

**Create Pool**

✓ Name and Description  
• Tiers  
Drives  
Capability Profile Name  
Summary  
Results

**Select Storage Tiers**

Available Tiers

Tier	Drive Type	Unused Drives	Unused Capacity (GB)
<input type="checkbox"/> Extreme Performance Tier	SAS FLASH	1	356.7
<input type="checkbox"/> Performance Tier	SAS	6	3,301.8
<input checked="" type="checkbox"/> <b>Capacity Tier</b>	NL SAS	40	229,121.7

☐ Use FAST Cache

**Selected Tiers**

**Capacity Tier**  
RAID 5 (8+1), Maximum Usable Capacity 171.9 TB

[Change](#)

**Extreme Performance Tier**  
Provides very fast access times for resources demanding the quickest response time. Databases can achieve their best performance when using this tier.

**Performance Tier**  
Provides high, all-around performance with consistent response times, high throughput, and good bandwidth. Appropriate for database resources accessed centrally through a network.

**Capacity Tier**  
Provides high storage capacity with generally lower performance. Appropriate for storing large amounts of primarily static data (such as video, audio, and image files) for users and applications without strict performance requirements.

Cancel [Back](#) [Next](#)

Proceed to the next step.

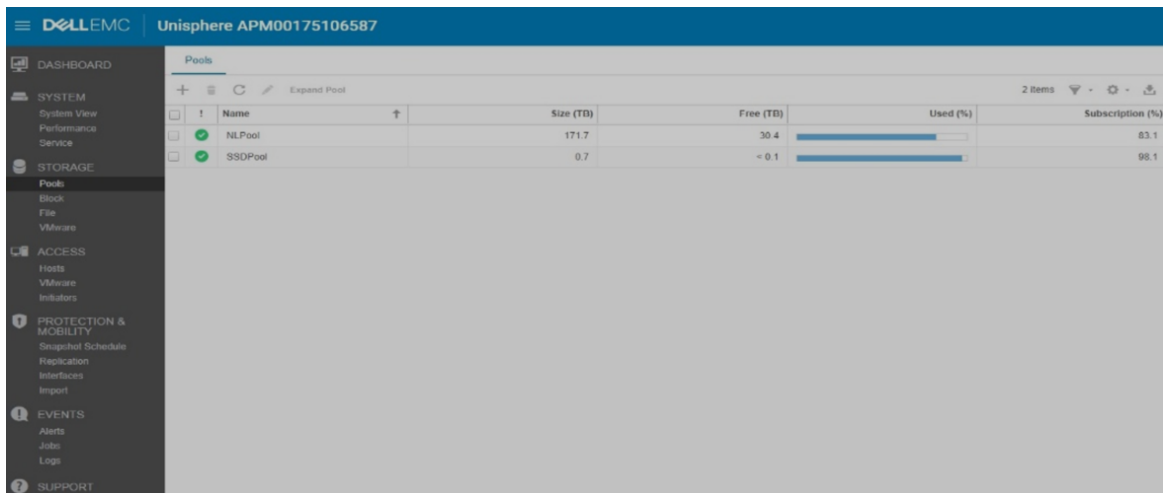
6. Choose the number of drives you want to add into the pool and click **Next**.

7. Skip the **VMware Capability** section and click **Next**.

8. Make sure that everything is correct on the Summary tab, and click **Finish**.
9. Create another pool for the SSDs using steps 2 – 8.
- Enter in a name for the other pool (for example, **SDDPool**) and click **Next**. Optionally, you can also enter a description for the pool.
  - Select **Extreme Performance Tier** under **Tier** for the tier type (drive type) and click **Change**.
  - Choose the RAID type and from the drop down, select the RAID size, and click **OK**.

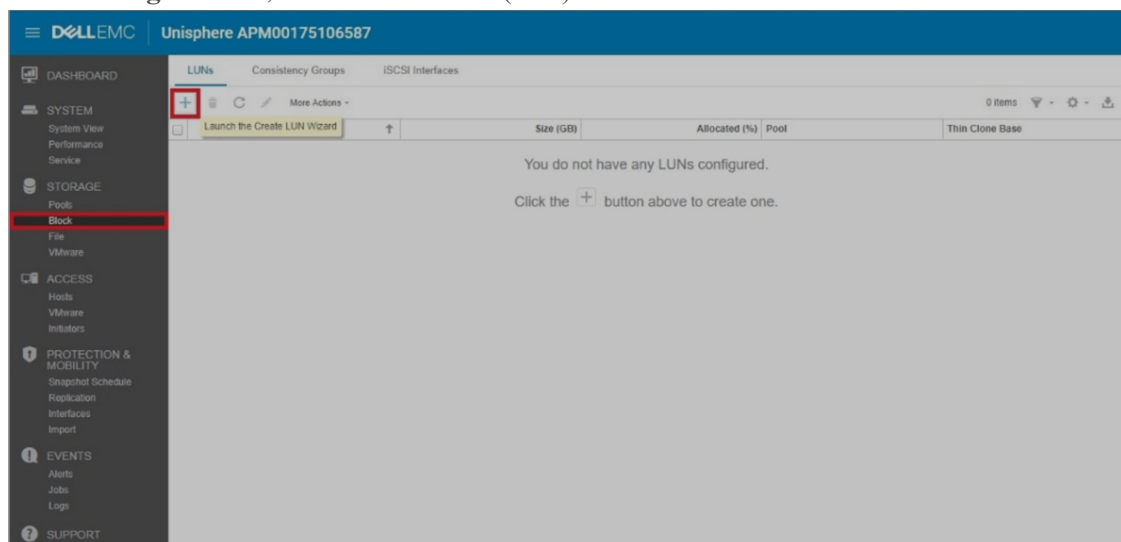
**Note:** Raid 5 (4+1) RAID Configuration is different then Capacity Tier.





### Task 3 - Create LUNS

1. From **Storage** section, click **Block** >  (Add) to launch the **Create LUN Wizard**.



The table below lists all of the possible LUNS you may need to create. The ConIndex is the only LUN you need to assign to the SSD Pool. Make sure that the LUN sizes do not exceed what is listed below.

DecoderLarge01	75 TB orLess	NL Pool	No
DecoderSmall01	20 TB or Less	NL Pool	No
Concentrator01	15 TB or Less	NL Pool	No
Archiver01	75 TB or Less	NL Pool	No
ConIndex01	3 TB or Less	<b>SSD Pool</b>	No

2. Enter the LUN Name from the list. Optionally, you can enter a description of LUN.
3. Select the appropriate pool from the list on the drop-down menu.
4. Deselect the **Thin** checkbox (These will be fully provisioned LUNs).
5. Select **Next** to proceed to the next menu.

**Create LUNs**

**Configure LUN(s)**

Number of LUNs: 1

Name: **DecoderLarge01**

Description:

Pool: **NLPool (Capacity Tier, 171.9 TB free)**

Tiering Policy: Start High Then Auto-Tier

Size: **20 TB**

☒ Thin

Host I/O Limit: No Limit

**Next**

Proceed to the next step.

6. Click **Next** until you get to the summary section.
7. Verify that the **Name**, **Pool**, **Size** and **Thin** selections are all correct.
8. Click **Finish** to complete LUN creation.

**Create LUNs**

**Summary**

**Name and Description**

Name: **DecoderLarge01**

Description:

**LUN Configuration**

Pool: **NLPool**

Size: **20.0 TB**

Thin: **No**

Compression: No

Tiering Policy: Start High Then Auto-Tier

Host I/O Limit: No Limit

**Host Access**

Access has not been configured for any hosts.

**Snapshot**

No snapshot schedule will be assigned to this LUN.

**Replication**

No replication is being created

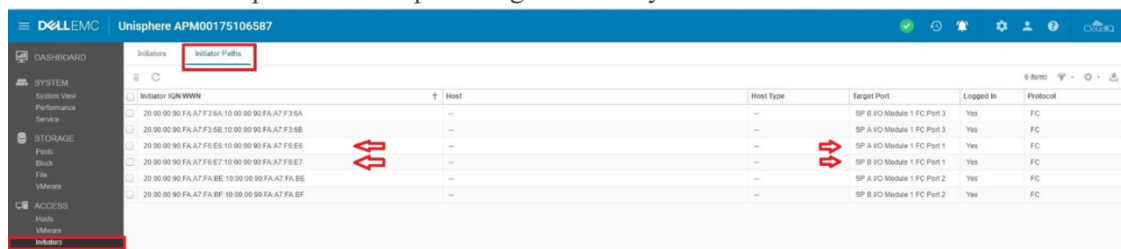
**Finish**

- Repeat steps 2- 8 for the remaining LUN creations.

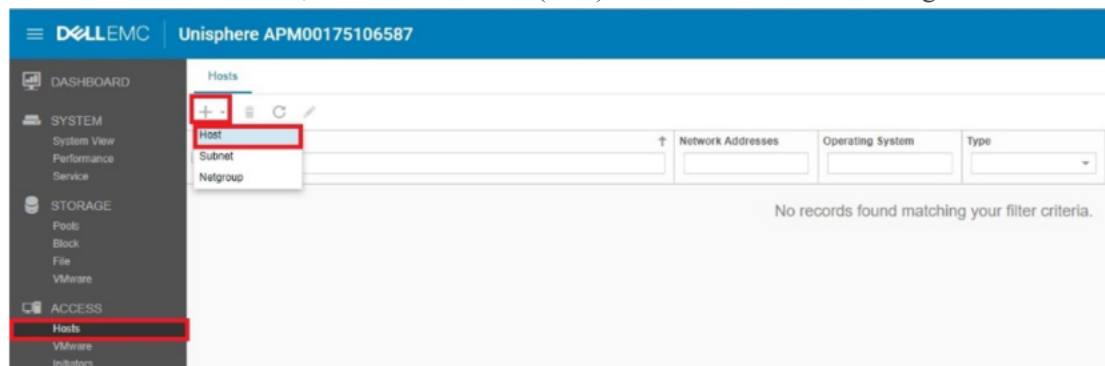
## Task 4 - Register Hosts

Before proceeding, record the hostname and IP address of the Head Unit and make sure that the HBAs in the head unit are properly cabled to the UNITY.

- From the Access section, click **Initiators**.
- Under the **Initiator Paths** tab, make sure that the correct HBAs are selected that you will use to register the Head Unit.  
You should see two initiators per Head Unit. This represents the fiber connection from port 1 to SPA and port 1 to SPB. If you have multiple head units, the easiest method is to power each down and then power them up and register one by one.



- From the Access section, click **Hosts** > **+** (Add) > **Host** to add a host configuration.



- Enter the Hostname of the Head Unit.
- Under **Operating System**, select **Linux** from the drop down menu.
- Enter the IP address of the Head Unit.

7. Click **Next** to proceed to the next section.

**Add a Host**

**Specify a Name and Additional Information**

Name:

Description:

Operating System:

Network Address:

Tenant:

Cancel **Next**

Proceed to the next step.

① While the host operating system information is not required, providing it will allow for more specific setup and troubleshooting instructions.

② In order to customize access to NFS shares, the Network Address (name or IP address) is required. Port information is not allowed.

Network Address examples:  
IPv4 address: 192.168.1.2  
IPv6 address: FE80:3202:B3FF:FE1E:8329  
Host name: hostname

③ Tenant information is not required. To create a tenant, select the Tenants tab for a file system.

8. In the Initiators section, select the two initiators that correspond to the correct port associated with the Head Unit and click **Next** to proceed.

**Add a Host**

**Select Discovered Initiators or Manually Add Initiators**

Automatically Discovered Initiators

Initiator IQN/WWN	Connected To
<input checked="" type="checkbox"/> 20:00:00:90:FA:A7:F5:E6:10:00:00:90:FA:A7:F5:E6	SP A iO Module 1 FC Port 1
<input type="checkbox"/> 20:00:00:90:FA:A7:FA:BF:10:00:00:90:FA:A7:FA:BF	SP B iO Module 1 FC Port 2
<input type="checkbox"/> 20:00:00:90:FA:A7:F3:6A:10:00:00:90:FA:A7:F3:6A	SP B iO Module 1 FC Port 3
<input checked="" type="checkbox"/> 20:00:00:90:FA:A7:F3:6A:10:00:00:90:FA:A7:F3:6A	SP B iO Module 1 FC Port 3

Manually Added Initiators

+ -

☐ Protocol ↑ Initiator IQN/WWN

No initiators have been manually added yet. Click the + button to manually add an initiator.

Cancel **Back** **Next**

Proceed to the next step.

① The host uses initiator(s) to access the storage resources.

Select from the list of initiators the system has auto-discovered or click the "+" button to manually add an initiator if they are not connected yet.

- Make sure that the **Name**, **OS**, **IP** and **WWNs** are correct and click **Finish**.

**Add a Host**

✓ Name  
✓ Initiators  
• Summary  
Results

**Review the host configuration**

Name: **SSDecoder**  
Description:  
Operating System: **Linux**  
Network Addresses: **10.25.66.32**  
Tenant:

Initiators to be registered with this host

Protocol	Initiator IQN/WWN
FC	20 00 00 90 FA A7 F5 E6 10 00 00 90 FA A7 F5 E6
FC	20 00 00 90 FA A7 F5 E7 10 00 00 90 FA A7 F5 E7

Cancel Back **Finish**

- Repeat steps 2-9 for all Head Units.
- In the Initiators section, select the two initiators that correspond to the correct port associated with the Head Unit. Then click “Next” to proceed.

## Task 5 - Assign LUNS to Hosts

- From the **Access** section, click **Hosts**, select the head unit (for example, **Decoder**) and click



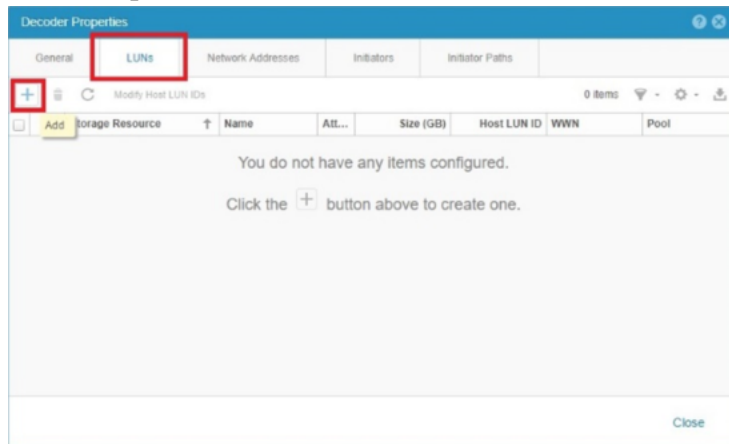
(edit) to view and edit details for the selected host.

**Dell EMC Unisphere APM00175106587**

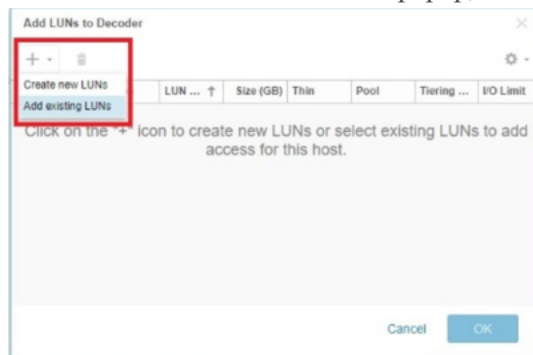
**Hosts**

Name	Network Addresses	Operating System	Type	Tenant	LUNs	Initiators	Initiator Paths
Decoder	---	Linux	Manual	---	0	2	2

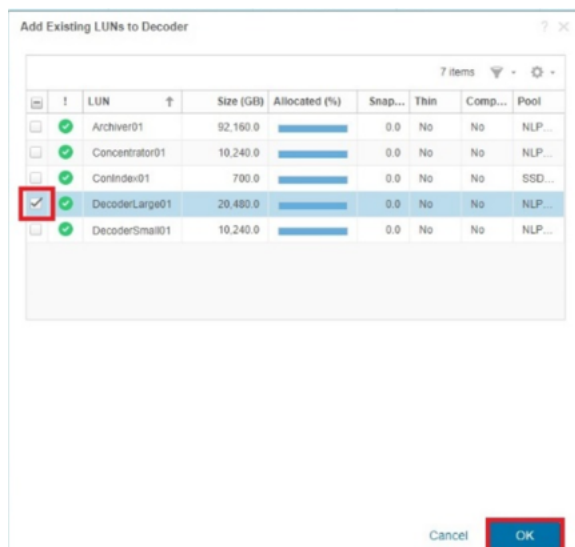
2. In the **Properties** section, select the **LUNS** tab and click  (Add icon).



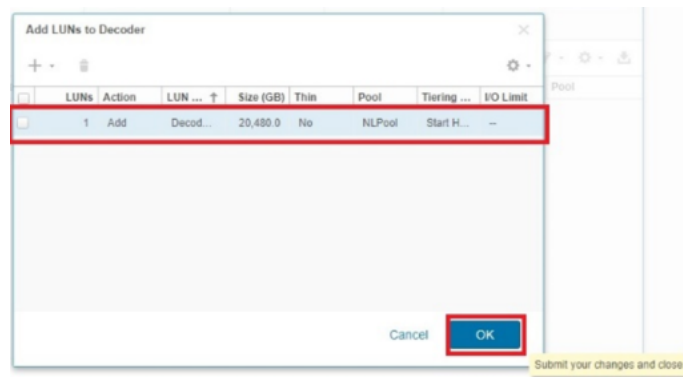
3. From the **Add LUNs to <Host>** popup, click  > **Add existing LUNs**.



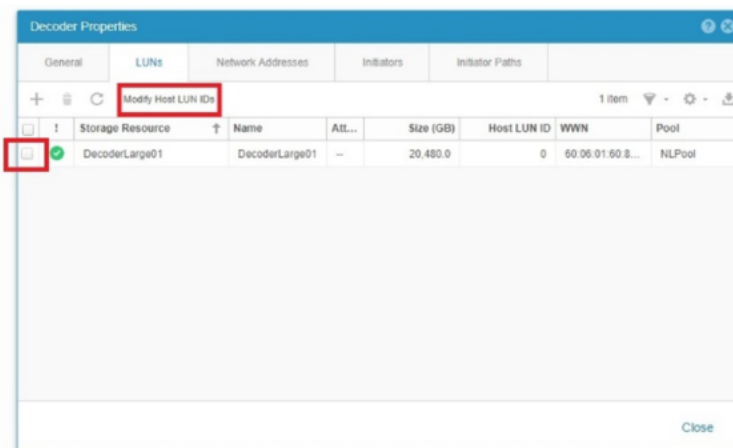
4. Select the LUN to add to the Head Unit and **OK**.



5. Make sure that the correct LUN was added to the host and click **OK**.



6. (OPTIONAL) If you need to modify the HLU (Host LUNN Unique ID):
- Select the LUN you want to change.
  - Click **Modify Host LUN IDs**.



7. Click  (edit), change the HLU to the number you want, and click **OK**.

## Task 6 - Install PowerPath

1. Make sure that the Emulex ports on the Decoder host are attached to the Unity.
2. Log in to `root` on the Decoder attached to the Unity with the `admin` credentials.
3. Install PowerPath and register the EMC PowerPath licenses for Unity hardware.

```
yum install DellEMCPower.LINUX-6.4.0.00.00-95.RHEL7.x86_64.rpm
```

**Note:** When you purchase an RSA Provided Unity, PowerPath licenses are sent to you. You can download PowerPath at [support.dell.com](http://support.dell.com).

4. Make sure that all the PowerPath connections are correct.

```
powermt display dev=all
```

The following output is an example of valid PowerPath connections.

```
=====
--- Host ---
### HW Path          I/O Paths    - Stor -  -- I/O Path --  -- Stats ---
                                Interf.  Mode    State    Q-I/Os Errors
=====
    15 lpfc           sde       SP A6    active  alive     0      0
    18 lpfc           sdg       SP B6    active  alive     0      0

Pseudo name=emcpowerb
Unity ID=APM00174407815 [Host_62]
Logical device ID=600601609D9046006996745A46B60AB6 [DecoderSmall101]
state=alive; policy=CLAROpt; queued-I/Os=0
Owner: default=SP A, current=SP A      Array failover mode: 4
=====
--- Host ---
### HW Path          I/O Paths    - Stor -  -- I/O Path --  -- Stats ---
                                Interf.  Mode    State    Q-I/Os Errors
=====
    15 lpfc           sdd       SP A6    active  alive     0      0
    18 lpfc           sdf       SP B6    active  alive     0      0
```

5. Verify that the PowerPath license is installed using the `emcpreg` command.

```
[root@NWAPPLIANCE24932 ~]# emcpreg -list
```

```
Key BQPO-DB4M-VFC2-Q24R-ML9Z-EQTU
```

```
Product: PowerPath
```

```
Capabilities: A1
```

6. Add the following string to the `/etc/lvm/lvm.conf` file to filter the LVM (Logical Volume Manager) so that it ignores duplicate volumes.

```
filter = [ "a|^/dev/sda2$|", "a|^/dev/sdb1$|",
"a|^/dev/emcpower.*|", "r|.*/|" ]
```

7. Reboot the Decoder.
8. Complete the instructions in [Allocate Block Devices \(Direct Attached or Virtual Storage\)](#) to complete storage configuration.



## Migrate Data to Another Storage Type

The following procedure describes how to move data from one type of external storage device to another. The procedure uses "moving data from 2 DACs to 2 PowerVaults" as an example.

Refer to the Hardware Setup Guides on RSA Link

(<https://community.rsa.com/community/products/netwitness/hardware-setup-guides>) for detailed instructions for setting up RSA NetWitness Platform host and storage hardware.

### Data on DAC Before Move to PowerVault

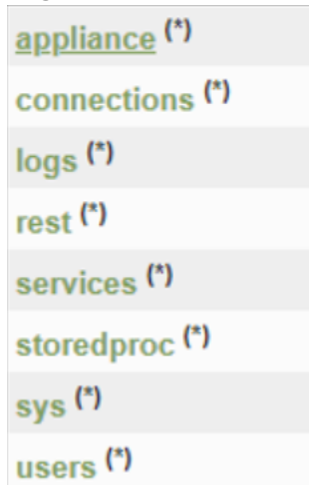
Before you move data from 2 DACs to 2 PowerVaults, a table, similar to the following table, is displayed if you run the `pvs` (Physical Volume Size) command from the Decoder Linux console (or SSH to the Decoder) with 2 DACs attached and configured to the Decoder. The column headings are Physical Volume (PV), Volume Group (VG), Linux Format (Fmt), Linux Attribute (Attr), Physical Volume Size (PSize), and Physical Volume Free Space (PFree).

PV	VG	Fmt	Attr	PSize	PFree
/dev/sda2	netwitness_vg00	lvm2	a--	<930.00g	0
/dev/sdb1	netwitness_vg00	lvm2	a--	<1.82t	0
/dev/sdc	decodersmall	lvm2	a--	<5.46t	0
/dev/sdd	decoder	lvm2	a--	<27.29t	0
/dev/sde	decodersmall0	lvm2	a--	<5.46t	0
/dev/sdf	decoder0	lvm2	a--	<27.29t	0

Complete the following steps to move data from a DAC to a PowerVault.

1. Attach two PowerVaults to a separate PERC controller on the Decoder.
2. Create the devices.
  - a. Open a Browser and specify the ip-address of the Network Decoder and port **50106** to access the REST tool.

- b. Log in with the `admin` account credentials.



- c. Click on the (\*) next to **appliance** to access the REST command set.
- d. Under **Properties for /appliance**, select `raidNew`, specify `controller=<PowerVault-controller-id>` `enclosure=<PowerVault-enclosure-id>` `scheme=decoder` `preferSecure=false`, and click **Send**.

**Note:** Only specify `preferSecure=false` if the PowerVault drives are not SED drives.

- e. Specify `controller=<PowerVault-controller-id>` `enclosure=<PowerVault-enclosure-id>` `scheme=decoder` `preferSecure=false` `commit=1` and click **Send**.
- f. Run `raidLst` to display the Controller/Enclosure combination with the new PowerVault enclosures.

In the following example, the output shows `dev/sdg` and `/dev/sdh` on **Controller 2, Enclosure 246**.

```
Controller 2, Enclosure 246
Vendor:  DELL
Model:   MD1400
In Use:  true
Drives: 10.691 TB x 12
Devices: sdg
         sdh
```

3. Go to the Decoder Linux console or SSH to the Decoder and run the following commands.

```
parted -s /dev/sdg mklabel gpt
parted -s -a optimal /dev/sdg mkpart LVM 0% 100%
pvcreate -f /dev/sdg
```

If the volume is created successfully, the following message is displayed.

```
Physical volume "/dev/sdg" successfully created
```

4. Run the following command string to extend the DAC volume group (**decoder**, **decodersmall**) to the Powervault Physical volume.

```
vgextend decoder /dev/sdg
```

5. Run the following command string to move the data from the DAC to the PowerVault. In this following command string, the DAC is **/dev/sdc** and the PowerVault is **/dev/sdg**.

```
pvmove /dev/sdc /dev/sdg
```

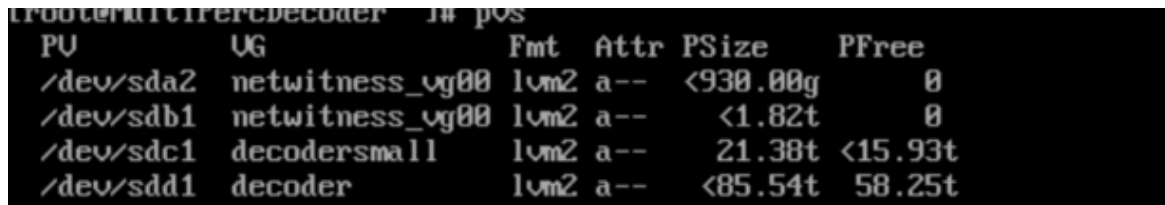
**Note:** Depending on the amount of data on the drives, the move can take two or more hours to complete. For example, in a test, it took four hours to move one TB of data.

6. After the move is complete, run the following commands to reduce and remove the DAC drive.

```
vgreduce decoder /dev/sdc
pvremove /dev/sdc
reboot
```

7. Detach the physical connections from the DACs to the host.

- a. Verify that the Physical volumes are moved from the DACs to the PowerVaults.
  - a. Restart the host and verify that the **/etc/fstab** file is correct.
  - b. Run the **pvs** command and make sure that the **PSize** and **PFree** values are correct on the PowerVault.



PV	VG	Fmt	Attr	PSize	PFree
/dev/sda2	netwitness_vg00	lvm2	a--	<930.00g	0
/dev/sdb1	netwitness_vg00	lvm2	a--	<1.82t	0
/dev/sdc1	decodersmall	lvm2	a--	21.38t	<15.93t
/dev/sdd1	decoder	lvm2	a--	<85.54t	58.25t

## Data on PowerVault After Move from DAC

After you move data from 2 DACs to 2 PowerVaults, a table, similar to the following table, is displayed if you run the **pvs** (Physical Volume Size) command from the Decoder Linux console (or SSH to the Decoder) with 2 PowerVaults attached and configured to the Decoder. The column headings are Physical Volume (PV), Volume Group(VG), Linux Format (Fmt), Linux Attribute (Attr), Physical Volume Size (PSize), and Physical Volume Free Space(PFree).

PV	VG	Fmt	Attr	PSize	PFree
/dev/sda2	netwitness_vg00	lvm2	a--	<930.00g	0
/dev/sdb1	netwitness_vg00	lvm2	a--	<1.82t	0
/dev/sdc1	decodersmall	lvm2	a--	21.38t	<15.93t
/dev/sdd1	decxoder	lvm2	a--	<85.54t	58.25t

## Enable or Validate Encryption to Existing PowerVault (encryptSedVd.py)

You may have set up a PowerVault, but you do not know if it has encryption. The `encryptSedVd.py` script:

- Validates that the PowerVault, attached to your Core host, has the correct setup for encryption.
- Encrypts unencrypted drives.

The following scenarios are examples of why you would use the `encryptSedVd.py` script.

- You want to know if a PowerVault has encryption. In this case, if the script determines that the PowerVault does not have encryption, it gives you the opportunity to encrypt the PowerVault.
- You set up a PowerVault without encryption and you want to encrypt it.

You will find this script in the `rsa-sa-tools` directory for releases 11.3.0.0 and later. The following directory is for 11.3.0.0.

`rsa-sa-tools-11.3.0.0-1903082015.5.e6581a4.el7.noarch.rpm`

The following procedure illustrates how to use the script.

1. Log in as `root`.
2. Change the directory to the `rsa-sa-tools` RPM base directory:

```
cd /opt/rsa/saTools/supportScript/
```

3. Execute the following command:

```
OWB_ALLOW_NON_FIPS=1 ./encryptSedVd.py
```

The script tells you if the disks are encrypted or not encrypted.

- If the drives are encrypted, the script displays the following message.  
No unencrypted RAID virtual drives with SED physical drives found.
- If the drives are not encrypted, the script identifies the unencrypted drives as shown in the following example.  
2 unencrypted RAID virtual drive(s) found on adapter: 1  
Enable disk encryption y/n?

4. (Conditional) If the drives are not encrypted and you want to encrypt them:

- a. Type `y` and press Enter in response to the Enable disk encryption y/n? to enable encryption.

You must enter a pass phrase if you get the following prompt.

This PERC adapter does not have a security key set.

Enter a Passphrase for the encryption key between 8 and 32 characters in length,

with a mix of lower, upper and non-alphanumeric characters?

- b. Type the `<passphrase>`, for example `nFreDaW$792`, and press Enter.  
The following prompt is displayed.

Please re-enter passphrase again for validation?

- c. Type the <passphrase>, for example nFreDaW\$792, and press Enter.

The following prompt is displayed.

Please re-enter passphrase again for validation?

- d. Type the <passphrase> again, for example nFreDaW\$792, and press Enter.

The following output and prompt is displayed.

Enter an optional ID string for the security key less than 256 characters or press Enter for none?

- e. Press Enter if you do not want an optional ID string.

The following output and prompt is displayed.

```
*****
```

```
*****
```

The Passphrase for the security key \*Must\* be securely backed up in case of PERC adapter hardware failure, should this occur, data on all encrypted disks will be unrecoverable.

Current Passphrase ('Quoted'): '<passphrase>'

Entered KeyID ('Quoted'): ''

```
*****
```

```
*****
```

Enter y to confirm that you backed up the Passphrase or press Enter to cancel?

- f. Type y and press Enter to confirm that you backed up the Passphrase.

The script tells that it encrypted the PowerVault as shown in the following example.

Successfully set encryption for all SED capable RAID virtual drives found

## Revision History

---

Revision	Date	Description	Author
1.0	28-May-19	First Edition	IDD
1.1	31-May-19	Minor corrections	IDD