Upgrade Guide

HGST Active Archive System SA-7000

September 2015

1ET0077

Revision 1.1

Long Live Data ™ | www.hgst.com

Copyright

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: HGST a Western Digital company PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer or express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HGST may make improvements or changes in any products or programs described in this publication at any time.

It is possible that this publication may contain reference to, or information about, HGST products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that HGST intends to announce such HGST products, programming, or services in your country.

Technical information about this product is available by contacting your local HGST representative or on the Internet at: www.hgst.com/support

HGST may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

HGST, a Western Digital company
3403 Yerba Buena Road
San Jose, CA 95135
Produced in the United States

Long Live Data™ is a trademark of HGST, Inc. and its affiliates in the United States and/or other countries.

HGST trademarks are authorized for use in countries and jurisdictions in which HGST has the right to use, market and advertise the brands.

Other product names are trademarks or registered trademarks of their respective owners.

One MB is equal to one million bytes, one GB is equal to one billion bytes, one TB equals 1,000GB (one trillion bytes) and one PB equals 1,000TB when referring to storage capacity. Usable capacity will vary from the raw capacity due to object storage methodologies and other factors.

References in this publication to HGST products, programs or services do not imply that HGST intends to make these available in all countries in which HGST operates.

Product information is provided for information purposes only and does not constitute a warranty.

Information is true as of the date of publication and is subject to change. Actual results may vary. This publication is for general guidance only. Photographs may show design models.

Contents

List of Figures

List of Tables

1 About this Guide

Topics:

- Conventions
- Storage Notations
- Admonitions
- Related Documents

This guide provides instructions for Active Archive System software and firmware updates, and hardware upgrades.

1.1 Conventions

Element	Sample Notation
OS shell or Q-Shell commands (user input)	`rm -rf /tmp`
OS shell or Q-Shell system output	`Installation successful!`

Commands longer than one line are split with "\"	`q.dss.manage.setPermissions('/manage', \`
	`[....])`

User-supplied values	*`ManagementNodeVirtualIPAddress`* or `<ManagementNodeVirtualIPAddress>`
File and directory names	The file `aFile.txt` is stored in `/home/user`.
Any graphical user interface label	Click **OK**.
Keyboard keys and sequences	To cancel the operation, press `Ctrl+c`.
Menu navigation in a GUI	Navigate to **Dashboard** > **Administration** > **Hardware** > **Servers**.

1.2 Storage Notations

Convention	Prefix	Size (bytes)
KB	kilobyte	1,000
KiB	kibibyte	1,024
MB	megabyte	1,000,000
MiB	mebibyte	1,048,567
GB	gigabyte	1,00,000,000
GiB	gibibyte	1,073,741,824
TB	terabyte	1,000,000,000,000
TiB	tibibyte	1,099,511,627,776

- Sizes of disks are expressed with *SI prefixes* (kilo, mega, tera, peta, exa)
- Space, size of partitions and file systems are expressed with the *binary prefixes* (kibi, mebi, tebi, pebi, exbi)
- A comma (",") is used for digit grouping, for example 1,000 is 1 thousand.
- A period (".") is used as decimal mark, for example 12.5 %.

1.3 Admonitions

Type	Usage
Note:	Indicates extra information that has no specific hazardous or damaging consequences.
Tip:	Indicates a faster or more efficient way to do something.
Caution:	Indicates an action that, if taken or avoided, may result in hazardous or damaging consequences.
Warning:	Indicates an action that, if taken or avoided, may result in data loss or unavailability.

1.4 Related Documents

For more information about the Active Archive System, please consult the following documents:

- The *HGST Active Archive System Administration Guide* explains how to use the Active Archive System interfaces for executing system management, monitoring, and analytics tasks.
- The *HGST Active Archive System API Guide* provides a reference for the Active Archive System S3 API.
- The *HGST Active Archive System FRU Replacement Guide* provides procedures for replacing hardware components of the Active Archive System.
- The *HGST Active Archive System Installation Guide* provides instructions for the installation of the Active Archive System in the data center, and its initial bringup.
- The *HGST Active Archive System Release Notes* provide important information about changes, new features, and known limitations.
- The *HGST Active Archive System Site Requirements Document* contains data center requirements for the Active Archive System.
- The *HGST Active Archive System Troubleshooting Guide* provides help for issues you might encounter.
- The *HGST Active Archive System Upgrade Guide* provides instructions for software and firmware updates, and system expansion.

For the latest or online version of any of these documents, visit http://www.hgst.com/support.

2 Disclaimers

Topics:

- Regulatory Statement of Compliance

The following chapter describes the Regulatory Statement of Compliance and Safety Compliance for the Active Archive System.

2.1 Regulatory Statement of Compliance

Product Name: **Active Archive System**
Regulatory Model: **SA-7000 series**
EMC Emissions: **Class A**

This product has been tested and evaluated as Information Technology Equipment (ITE) at accredited third-party laboratories for all safety, emissions and immunity testing required for the countries and regions where the product is marketed and sold. The product has been verified as compliant with the latest applicable standards, regulations and directives for those regions/countries. The suitability of this product for other product categories other than ITE, may require further evaluation.

The product is labeled with a unique regulatory model and regulatory type that is printed on the label and affixed to every unit. The label will provide traceability to the regulatory approvals listed in this document. The document applies to any product that bears the regulatory model and type names including marketing names other than those listed in this document.

2.1.1 Restricted Access Location

The Active Archive System is intended for installation in a server room or computer room where at least one of the following conditions apply:

- access can only be gained by SERVICE PERSONS or by USERS who have been instructed about the restrictions applied to the location and about any precautions that shall be taken and/or
- access is through the use of a TOOL or lock and key, or other means of security, and is controlled by the authority responsible for the location.

2.1.2 Safety Compliance

The following table outlines how the Active Archive System is being designed to pass the product safety requirements:

Country/Region	**Authority or Mark**	**Standard**
Australia/New Zealand	CB report, CB certificate	AS/NZS 60950.1
Canada/North America	NRTL	CSA C22.22 No. 60950-1-07
Customs Union/Russia, Kazakhstan, Belarus, Armenia	EAC	TR CU 004/2011
European Union	CE	EN 60950-1
International		IEC60950, CB report and Certificate to include all country national deviations
United States/North America	NRTL	UL 60950-1
Mexico	NYCE or NOM	NOM-019-SCFI-1998

Country/Region	Authority or Mark	Standard
Brazil	INMETRO	IEC 60950-1
Taiwan	BSMI	CNS14336
Ukraine	UKrTEST or equivalent	4467-1:2005
Moldova	INSM	SM SR EN60950-1
Serbia	KVALITET	SRPS EN60950:2010
India	BIS	IS 13252 (Part 1):2010

Table 1: Product Safety Compliance

2.1.3 Electromagnetic Compatibility Agency Requirements

The following table outlines how the Active Archive System is being designed to comply with the Electromagnetic Compatibility (EMC) agency requirements:

Country/Region	Authority or Mark	Standard	Status
Australia/New Zealand	C-tick or A-tick	AS/NZS CISPR22	Complete
Canada/North America	Industry Canada	ICES-003	Complete
Customs Union/Russia, Kazakhstan, Belarus, Armenia	EAC	TR CU 020/2011	Complete
European Union	CE	EN55022, EN55024 including EN61000-3-2, EN61000-3-3	Complete
International		CISPR22, CISPR24	Complete
Japan	VCCI	V-3:2014	Complete
United States/North America	FCC	FCC Part 15	Complete
Taiwan	BSMI	CNS13438	Complete
Korea	MSIP	KN22, KN24	Complete
Ukraine	UKrTEST or equivalent	4467-1:2005	Complete
Serbia	KVALITET	CISPR22	Complete
Brazil	INMETRO		Complete

Table 2: Product EMC/Immunity Compliance

3 Safety and Regulatory

Topics:

The following chapter provides safety and regulatory information for the Active Archive System.

3.1 Optimizing Location

Failure to recognize the importance of optimally locating your product and failure to protect against electrostatic discharge (ESD) when handling your product can result in lowered system performance or system failure.

Do not position the unit in an environment that has extreme high temperatures or extreme low temperatures. Be aware of the proximity of the unit to heaters, radiators, and air conditioners. For more information on ambient operating conditions and environment, see: General Site Requirements.

Position the unit so that there is adequate space around it for proper cooling and ventilation. Consult the product documentation for spacing information.

Keep the unit away from direct strong magnetic fields, excessive dust, and electronic/electrical equipment that generate electrical noise.

3.2 Safety Warnings and Cautions

To avoid personal injury or property damage, before you begin installing the product, read, observe, and adhere to all of the following safety instructions and information. The following safety symbols may be used throughout the documentation and may be marked on the product and / or the product packaging.

CAUTION Indicates the presence of a hazard that may cause minor personal injury or property damage if the CAUTION is ignored.

WARNING Indicates the presence of a hazard that may result in serious personal injury if the WARNING is ignored.

Indicates potential hazard if indicated information is ignored.

Indicates shock hazards that result in serious injury or death if safety instructions are not followed.

Indicates do not touch fan blades, may result in injury.

Indicates disconnect all power sources before servicing.

3.3 Electrostatic Discharge

⚠ **CAUTION**

Electrostatic discharge can harm delicate components inside HGST products.

Electrostatic discharge (ESD) is a discharge of stored static electricity that can damage equipment and impair electrical circuitry. It occurs when electronic components are improperly handled and can result in complete or intermittent failures

Wear an ESD wrist strap for installation, service and maintenance to prevent damage to components in the product. Ensure the antistatic wrist strap is attached to a chassis ground (any unpainted metal surface). If possible, keep one hand on the frame when you install or remove an ESD-sensitive part.

Before moving ESD-sensitive parts placed it in ESD static-protective bags until you are ready to install the part.

3.4 Rackmountable Systems

CAUTION

Always install rack rails and storage enclosure according to applicable product documentation. Follow all cautions, warnings, labels and instructions provided with the product and the rackmount instructions.

Reliable earthing of rack-mounted equipment should be maintained.

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Observe the maximum rated ambient temperature, which is specified in the product documentation.

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

3.5 Power Connections

Be aware of the ampere limit on any power supply or extension cables being used. The total ampere rating being pulled on a circuit by all devices combined should not exceed 80% of the maximum limit for the circuit.

CAUTION The power outlet must be easily accessible close to the unit.

⚠ Always use properly grounded, unmodified electrical outlets and cables. Ensure all outlets and cables are rated to supply the proper voltage and current.

⚡ This unit has more than one power supply connection; both power cords must be removed from the power supplies to completely remove power from the unit. There is no switch or other disconnect device.

3.6 Power Cords

Use only tested and approved power cords to connect to properly grounded power outlets or insulated sockets of the rack's internal power supply.

If an AC power cord was not provided with your product, purchase one that is approved for use in your country.

CAUTION To avoid electrical shock or fire, check the power cord(s) that will be used with the product as follows:

- The power cord must have an electrical rating that is greater than that of the electrical current rating marked on the product.
- Do not attempt to modify or use the AC power cord(s) if they are not the exact type required to fit into the grounded electrical outlets.
- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground.
- The power supply cord(s) is / are the main disconnect device to AC power. The socket outlet(s) must be near the equipment and readily accessible for disconnection.

3.7 Safety and Service

All maintenance and service actions appropriate to the end-users are described in the product documentation. All other servicing should be referred to a HGST-authorized service technician.

To avoid shock hazard, turn off power to the unit by unplugging both power cords before servicing the unit. Use extreme caution around the chassis because potentially harmful voltages are present.

When replacing a hot-plug power supply, unplug the power cord to the power s upply being replaced before removing it from the Storage Enclosure.

The power supply in this product contains no user-serviceable parts. Do not open the power supply. Hazardous voltage, current and energy levels are present inside the power supply. Return to manufacturer for servicing.

Use caution when accessing part of the product that are labeled as potential shock hazards, hazardous access to moving parts such as fan blades or caution labels.

4 HGST Regulatory Statements

Topics:

The following chapter provides regulatory statements for the Active Archive System.

HGST Storage Enclosures are marked to indicate compliance to various country and regional standards.

Note: *Potential equipment damage:* Operation of this equipment with cables that are not properly shielded and not correctly grounded may cause interference to other electronic equipment and result in violation of Class A legal requirements. Changes or modifications to this equipment that are not expressly approved in advance by HGST will void the warranty. In addition, changes or modifications to this equipment might cause it to create harmful interference.

4.1 FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Any modifications made to this device that are not approved by HGST may void the authority granted to the user by the FCC to operate equipment.

4.2 FCC Verification Statement (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates and can radiate radio frequency energy, and if not installed and used in accordance with the Active Archive System User Guide, it may cause harmful interference to radio communications.

4.3 ICES-003 (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le Ministre Canadian des Communications.

English translation of the notice previous:

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Canadian Department of Communications.

4.4 CE Notices (European Union), Class A ITE

Marking by the symbol indicates compliance of this system to the applicable Council Directives of the European Union, including the EMC Directive (2004/108/EC) and the Low Voltage Directive (2006/95/EC). A “Declaration of Conformity” in accordance with the applicable directives has been made and is on file at HGST Europe.

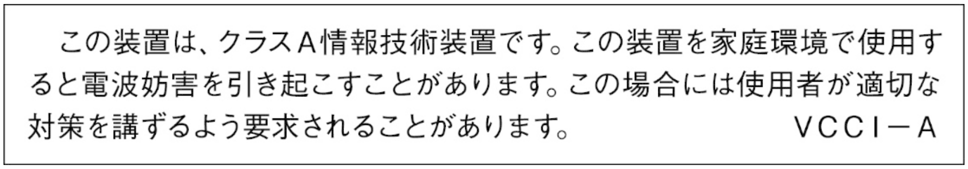
4.5 Europe (CE Declaration of Conformity)

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Canadian Department of Communications.

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le Ministre Canadian des Communications.

4.6 Japanese Compliance Statement, Class A ITE

The following Japanese compliance statement pertains to VCCI EMI regulations:

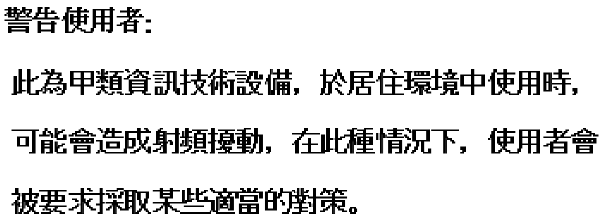


この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

English translation:

This is a Class A product based on the Technical Requirement of the Voluntary Control Council for Interference by Information Technology (VCCI). In a domestic environment, this product may cause radio interference, in which case the user may be required to take corrective actions.

4.7 Taiwan Warning Label Statement, Class A ITE



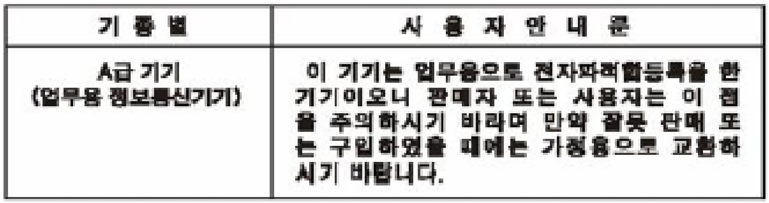
警告使用者:

此為甲類資訊技術設備，於居住環境中使用時，
可能會造成射頻擾動，在此種情況下，使用者會
被要求採取某些適當的對策。

English translation:

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take adequate measures.

4.8 KCC Notice (Republic of Korea Only), Class A ITE



기 종 별	사 용 자 안 내 문
A급 기기 (업무용 정보통신기기)	이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

English translation:

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this device is not suitable for your use, you may exchange it for a non-business device.

5 Software Updates

Topics:

The software update process is non disruptive. There is no downtime during software updates.

Software Update Workflow

1. Follow the pre update procedure in Prerequisites on page 18.
2. Download and extract the latest patch as explained in Downloading the Update Patch on page 19.
3. Run the update script as explained in Running the Update Script on page 19.
4. When the update script finishes, re-run the update script with the `-r` option as explained in Running the Update Script with the -r Option without Restarting the Client Daemons on page 21 in order to:

   A. Restart the client daemons.

   B. Restart all Controller Nodes.
5. Follow the post update procedure in Mandatory Actions to be Completed after the Update on page 22.

5.1 Updating the Active Archive System

5.1.1 Prerequisites

Before you start the software update, check the following:

1. Run a health check on your environment and resolve all issues that are identified:
   - If you do not have external public internet connectivity, invoke `q.amplistor.healthCheck(check_public_connectivity=False)`.
   - If you are connected to the external network, invoke `q.amplistor.healthCheck()`.
2. If there are events indicating that a MetaStore is lagging behind, refrain from upgrading and make sure that none of your MetaStores are lagging behind. Check for events, similar to the following:

   ```
   Node node_name on MetaStore metastore_name is lagging number_of_keys keys.
   ```
3. If there are any bad or degraded disks, decommission them before you start the update.
4. Replace decommissioned disks that are boot disks:
   - In the CMC, navigate to **Dashboard** > **Administration** > **Hardware** > **Disks** > **Decommissioned**.
   - On the **Nodes** page, select the desired node.
   - Click **Disks**.
   - Under logical disks, check on `md0` and `md1` if any of the decommissioned disks belongs to the RAID configuration.
5. Ensure that all MetaStores are up and that none of them are degraded.
6. In the list of **Unmanaged Devices**, look for nodes which have the status **ACTIVE**.

   Do not skip this check, since you may run different OS versions in your setup. This may lead to different behaviors.

   - Either clean up these nodes through the Q-Shell:

     ```
     q.amplistor.cleanupMachine('MAC_address_of_host')
     ```

     or
   - Clean up these nodes through the CMC: **Dashboard** > **Administration** > **Hardware** > **Servers** > **Unmanaged Devices**); or

- Initialize the nodes.

5.1.2 Downloading the Update Patch

To download the latest patch, proceed as follows:

1. Download the latest tarball from http://www.hgst.com/support.
2. Check the md5 hash.
3. Put the downloaded tarball on the Management Node in the root home directory.
4. Extract the package:

```
tar -xzvf Patch_Name.tgz -C /opt/qbase3/
```

5.1.3 Running the Update Script

The update script, `apply_package.py`, updates a software patch on all nodes sequentially. This is an automatic process that does not require human interaction. The update process consists of the following phases:

1. Update of the Management Node. This typically takes a couple of minutes.
2. Update of all Storage and Controller Nodes. This takes 2-3 minutes per Storage Node. After the update of each Storage Node, the Storage Node is automatically restarted if the patch changed the underlying Linux kernel.
3. Update of the Arakoon MetaStores, if the patch changed the system MetaStores.
4. Update of the CMC, if the patch changed it. This typically takes about 5 minutes.
5. Restart of the storage daemons. This takes 5-6 minutes per Storage Node.

When the update script finishes, you must do two manual steps:

1. Restart the client daemons. You do this by re-running the update script with the `-r` option. Pick a low peak hour for this, or modify your client application to stop writes to the Controller Nodes whose client daemon is being restarted. This takes a couple of seconds per client daemon.
2. Restart all Controller Nodes. This takes 2-5 minutes per Controller Node.

`apply_package.py` has the following options:

Option	Description
`-h, --help`	Show this help message and exit.
`-p PATCHNAME, --patchname=PATCHNAME`	Patch name to install.
`-d, --debug`	Enable debug logging.
`-f, --force`	Force patch installation.
`-r, --restart_clientdeamons`	Restart DSS clientdaemons on all Controller Nodes.
`-c, --complete_dss_upgrade`	Complete the DSS update.
`-l, --list`	List available patches and exit.
`-o, --one_ctrl`	Force update for environments having only one Controller Node.
`-O, --readonly`	Set if we need to protect data in syncstores setting them readonly during upgrade

Tracing the Progress of an Update

The progress of the update can be followed on any of the nodes via the following file:

```
/mnt/sandboxtmp/logging/release_name_date__hour.log
```

To run the update script, proceed as follows:

1. Open a screen session on the Management Node:

   ```
   screen -S MyUpdateSession
   ```

2. Execute the update script.
   Assuming you downloaded the update patch and extracted it to `/opt/qbase3`, do the following:

   ```
   cd /opt/qbase3/utils/
   ./apply_package.py -d -O -p Patch_Name
   ```

   This installs the necessary packages on all nodes, sets the MetaStores to read-only and restarts the Storage Nodes. The upgrade leaves the client daemons running.

   Note: If you want less verbosity in the logging, omit the `-d` parameter.

3. At the end of running this command, you are asked to restart the Controller Nodes of your environment:

   ```
   Please reboot following controller nodes if they were not rebooted yet

   [<list of Controller Nodes>]
   ```

   Note: In the course of the update, you will get this message each time you run the `apply_package.py` script. You need to restart the Controller Nodes only *one time*, thus you may ignore the following reboot messages.

   Restart the Management Node first.

4. When your Management Node is restarted, restart the other Controller Nodes via the CMC.

   Caution: Restart *one* Controller Node at a time. Wait until the Controller Node is fully operational before restarting the next Controller Node.

5. When all Controller Nodes are restarted, log into the Management Node.

6. Open a screen session on the Management Node.

   ```
   screen -S MyUpdateSession
   ```

7. Re-run the update script with the `-r` and `-c` options, you no longer need the `-O` option.

   Note: Do not skip this command, even though you have restarted your Controller Nodes in the previous steps.

   This will automatically restart all client daemons one by one.

   ```
    cd /opt/qbase3/utils/
   ./apply_package.py -rc -p Patch_Name
   ```

   Note: Restarting your client daemons will cancel any ongoing read or write operations towards that daemon. Restarting a daemon only takes a couple of seconds. If you like to have control over the restart of the client daemons, follow the procedure in Running the Update Script with the -r Option without Restarting the Client Daemons on page 21 and then execute this step again.

   The update of the Management Node will take about 5 minutes. During this update, the CMC might not be available.

After the Management Node has been updated, the CMC will become available again, but you may receive PostgreSQL related exceptions when logging into the CMC and when browsing to new events. You can ignore these messages until the update is completed.

The start of the update is identified by following event:

```
Upgrade started for Patch_Name
```

The end of the update is identified by following event:

```
Upgrade completed for Patch_Name
```

While the update of the database is ongoing, retrieving the actual disk safety from the CMC is not possible.

Any event that occurs between the start and end point of the update script can safely be ignored.

5.1.4 Running the Update Script with the -r Option without Restarting the Client Daemons

When running the upgrade script with the `-r` option (as shown in the previous paragraph), all client daemons will restart one by one (not all at once), but it does not check whether a client daemon is processing requests or not. In case you want fine-grained control over the restart of the client daemons, follow this procedure:

1. Restart the client daemons one by one via the Q-Shell:

   ```
   q.dss.clientdaemon.restartOne('client_daemon_guid')
   ```

   The client daemon GUIDs can be retrieved with `q.dss.clientdaemons.getStatus()`, where the keys of the returned dict are the GUIDs of the client daemons.
2. Open the log file `/opt/qbase3/log/dss/clientdaemons/`*`client_daemon_guid`*`/clientx.log`.
3. At the end of that file, look up the section that starts with *`Month day timestamp`*` info [None] Received sigterm. Cancelling all managers` and ends with *`Month day timestamp`*` info [None] server: initialization successful`.

   There are a large amount of lines in between, but as you can see in the following sample log, the timestamp difference between start and end is very small.

   ```
   Dec 23 10:53:34.4046 info [None] Received sigterm. Canceling all managers.
   Dec 23 10:53:34.4047 error [None] statistics log manager: failed: Lwt.Canceled
   Dec 23 10:53:34.4048 error [None] sync manager: failed: Lwt.Canceled
   Dec 23 10:53:34.4048 error [None] BlockStore Id Checker: failed: Lwt.Canceled
   Dec 23 10:53:34.4049 info [None] server at inet:127.0.0.1:23510, fd 9:
                                    canceling connection threads
   Dec 23 10:53:34.4049 info [None] server at inet:127.0.0.1:23510, fd 9:
                                    joining canceled connection threads
   Dec 23 10:53:34.4049 error [None] server at inet:127.0.0.1:23510, fd 9:
                                     end of server, closing socket: Lwt.Canceled:
   Dec 23 10:53:34.4050 info [None] node connection manager: end
   Dec 23 10:53:34.4050 info [None] server at inet:0.0.0.0:8080, fd 10:
                                    connection timeout monitoring thread: canceling

   ...

   Dec 23 10:53:34.5005 info [None] "/opt/qbase3/cfg/dss/clientdaemons/\
                                     e2c345ce-cc23-496e-9429-11de771539b3.cfg":
                                     section "[brand]",
                                     entry "product_version": value "3.6.0"

   ...
   ```

```
Dec 23 10:53:34.6902 info [None] S3 connection manager: initializing
Dec 23 10:53:34.6905 info [None] S3 connection manager: start
Dec 23 10:53:34.6908 info [None] S3 connection manager: initialization successful
Dec 23 10:53:34.6912 info [None] Encryption library initialized
Dec 23 10:53:34.6916 info [None] codec: initializing
Dec 23 10:53:34.6925 info [None] codec: initialization successful
Dec 23 10:53:34.6928 info [None] statistics log manager: start
Dec 23 10:53:34.6931 info [None] sync manager: start
Dec 23 10:53:34.6934 info [None] sync_manager[None]: sleeping 10000000.000000s
Dec 23 10:53:34.6937 info [None] BlockStore Id Checker: start
Dec 23 10:53:34.6939 info [None] BlockStore Id Checker
Dec 23 10:53:34.6941 info [None] Installing signal handler on managers
Dec 23 10:53:34.6944 info [None] server: initialization successful
```

4. Validate that the **product version number** in the log file is correct.

```
...
Dec 23 10:53:34.5005 info [None] "/opt/qbase3/cfg/dss/clientdaemons/\
                                  e2c345ce-cc23-496e-9429-11de771539b3.cfg":
                                  section "[brand]",
                                  entry "product_version": value "3.6.0"
...
```

5. Repeat the above steps for *all* client daemons on a Controller Node.
6. Once you have restarted all client daemons of the Controller Node, you can set a flag to indicate that the Controller Node does not need to be restarted
   a) In a terminal of the Controller Node, navigate to the directory `/opt/qbase3/var/patches/AmpliStor_3.6.0/`.
   b) Create the file `.dss_upgrade_compeleted`, the patch name may vary in rebranded version:

   ```
   touch /opt/qbase3/var/patches/AmpliStor_3.6.0/.dss_upgrade_completed
   ```

   c) Repeat this procedure for all Controller Nodes.
7. Run the upgrade script with the `-r` option to omit the restarting of the client daemons. The only remaining activity is to complete the upgrade from step 11 as mentioned in Running the Update Script on page 19.

5.1.5 Mandatory Actions to be Completed after the Update

5.1.5.1 Creating New Certificates

After updating the software, you have to upload new certificates through the CMC as follows. This is due to a security breach in the OpenSSL package.

1. In the CMC, navigate to: **Dashboard** > **Administration** > **Management** > **Interfaces** > **Certificates**.
2. For each Controller Node, click **Select File**.
3. Select the desired, valid HTTPS certificate.
4. Click **Upload File**.

5.1.5.2 Clearing the Browser Cache

Clear your browser cache, so that the new version of the CMC (a `.swf` file) is downloaded. The new version is capable of reading and displaying the changed functionality.

Clearing the browser cache means logging out from the CMC, closing the tab/window, opening up your browser-specific cache control settings, and clearing them.

Review the tuning recommendations as described in *Tuning the Active Archive System* in the *HGST Active Archive System Administration Guide*.

5.1.5.3 Removing Old Patches

You can remove old Active Archive System patches in your root file system to free up disk space. To remove old patches:

1. Open an SSH session to a Controller Node, and exit the OSM menu.
   The Linux prompt appears.
2. At the Linux prompt, navigate to `/opt/qbase3/var/patches`.
3. Look up the list of available patches.
   For example,

```
~# du -sh *
1.5M    ./AmpliStor_3.2.1
573M    ./AmpliStor_3.3.2
1.4G    ./AmpliStor_3.4.0
1.2G    ./AmpliStor_3.4.1
1.0G    ./AmpliStor_3.4.2
1.3G    ./AmpliStor_3.4.3
1.1G    ./AmpliStor_3.5.0
```

4. You can safely remove all older version except for the three most recent.
   For example,

```
rm -rf AmpliStor_3.2.1 AmpliStor_3.3.2 AmpliStor_3.4.0 AmpliStor_3.4.1
```

5.1.5.4 Confirming Patch Installation

When the upgrade has been completed for all nodes, confirm if the package has been installed.

1. Clean your browser cache so that the new `CMC.swf` gets loaded correctly into the browser.
2. Check the version in the CMC by navigating to **Dashboard** > **Upper Right Corner of Dashboard** > **About**.
3. In the same **About** box, you can see the list of different patches that have been applied. To see the details about a patch, open it. Details are displayed such as:

```
Package dss [version: 4.0.0, build: 21]
```

When a patch is not completely installed, you see following event in your events log in the CMC:

```
Found a partially installed patch: Active Archive System_4.0.0
```

5.1.6 Troubleshooting Software Update Issues

5.1.6.1 Software Updates

Problem	**Recommended Action**
Cannot find log files related to Active Archive System updates.	Look in `/opt/qbase3/var/log/` . You might need to run the log collector tool to populate this file. For more information on running the log collector tool, see *Logging* in the *HGST Active Archive System Administration Guide*.
PostgreSQL related exceptions are observed when logging into the CMC and when browsing to new events	After the Management Node has been updated, the CMC will become available again, but you may receive PostgreSQL related exceptions when logging into the CMC and when browsing to new events. You can ignore these messages until the update is completed. The start of the update is identified by following event: `Upgrade started for Patch_Name`

Problem	Recommended Action
	The end of the update is identified by following event: `Upgrade completed for Patch_Name`
A software update failed.	In case the update was unable to complete on a certain node, the update script, `apply_package.py`, will automatically stop upgrading. If this happens, proceed as follows: **1.** Check the logs and confirm which nodes have been updated and which have not. **2.** Spot the node where the failure happened and ensure the problem is resolved. **3.** Execute the update tool again on the Management Node: `/opt/qbase3/bin/python /opt/qbase3/utils/apply_package.py -p AmpliStor_3.6.0`
A software update on a system with offline nodes failed.	To perform an update on an environment with offline Storage Nodes, keep the following in mind: • The update will fail on the offline node. • Either resolve the issue or decommission the node. To perform an update on an environment with offline Controller Nodes, keep the following in mind: • The update script, `apply_package.py`, checks if the MetaStore clusters are complete (complete means having three members). • If the Controller Node is part of a MetaStore cluster, the update will fail. • Resolve the issue with the Controller Node or replace the Controller Node.

5.2 Updating Arakoon

5.2.1 Rolling Upgrades

Since the Arakoon protocol does not support the concept of versions, Arakoon is updated by a rolling update. This process is based upon the Paxos algorithm. To update Arakoon, proceed as follows.

The three Arakoon nodes communicate to each other over dedicated network ports.

1. The first step is to change the port of the first (non-master) node so that it does not participate in the quorum anymore.
2. The software of this node is updated to the new version and the node is restarted and running the new version.
3. These two steps are repeated for the second node. This node will now be able to communicate to the first node and they will elect a master among them and be able to make progress, after the first node has caught up from the second.
4. As a last step, the third node is also updated and restarted.
5. Finally the third node catches up and the cluster is fully in sync again.

5.3 Updating the Telemetry Collection Feature

5.3.1 Running the Telemetry Collection Update Script

This section is under development.

6 Firmware Updates

Topics:

6.1 Updating LSI Firmware

Contact HGST support.

6.2 Updating Intel NIC Firmware

Contact HGST support.

6.3 Updating the SuperMicro BIOS

Contact HGST support.

6.4 Updating the SuperMicro IPMI

Contact HGST support.

6.5 Updating Storage Enclosure Basic IOC Firmware

1. Set the user MetaStore to read only.

a) Log into the CMC.

b) Navigate to **Dashboard** > **Administration** > **Storage Management** > **MetaStores**.

c) In the **Status** column of the user MetaStore, select the **READONLY** option.

d) Check the job to make sure it is done.

2. Disable the `Aggregate Storagepool Info` policy on the Management Node.

```
api = i.config.cloudApiConnection.find('main')
polguid = api.policy.find(name='monitoring_storagepool')['result'][0]
api.policy.updateModelProperties(polguid,
 status=str(q.enumerators.policystatustype.DISABLED))
quit()
```

3. Transfer the new firmware, *`firmware_filename`*, to the Storage Node.

4. Open an SSH session to the Storage Node and shutdown services on it.

```
qshell -c "q.manage.servers.all.stop()"
```

5. Unmount all Storage Enclosure Basic partitions on the Storage Node.

```
mount | egrep 'dss|sandboxtmp' | awk '{print $3}' | xargs umount
```

Important: You cannot start the firmware update until all partitions are unmounted.

6. Run the following command to get the Storage Enclosure Basic device path and **device name**:

```
lsscsi -g | grep STOR
```

7. Run the following command to ensure that you can communicate with the Storage Enclosure Basic:
Replace *device_name* with the value returned from step 6.

```
sg_ses /dev/device_name -p 3
```

For example,

```
sg_ses /dev/sg42
```

8. Run the following command to obtain the status of the Storage Enclosure Basic and current firmware version:

```
sg_ses /dev/device_name -p 3
```

For example,

```
sg_ses /dev/sg42 -p 3
```

9. Start the actual firmware update.

```
sg_ses_microcode /dev/device_name -m 0xe -b 512 -N -I firmware_filename -vv
```

10. Once the update completed, reset the Storage Enclosure Basic as follows:

a) Send the reboot command.

Note: Wait 1 minute for this comment to complete.

```
sg_ses_microcode /dev/device_name -m 0xf
```

b) Get the device name.

```
lsscsi -g | grep STOR
```

c) Confirm that all devices are up.

```
sg_ses  /dev/device_name  -p 3
```

d) Make sure both expanders have the right firmware.

```
sg_ses  /dev/device_name  -p 7
```

11. Reboot the Storage Node.

```
reboot
```

Important: Wait until the Storage Node comes back up. Partitions are mounted and services are started automatically.

12. Repeat steps 3 to 11 for each of the remaining Storage Nodes.
13. Once all Storage Nodes have been rebooted, enable the aggregate storage pool info policy on the Management Node.

    ```
    api = i.config.cloudApiConnection.find('main')
    polguid = api.policy.find(name='monitoring_storagepool')['result'][0]
    api.policy.updateModelProperties(polguid,
     status=str(q.enumerators.policystatustype.ACTIVE))
    ```

14. Once all the Storage Enclosure Basic storage arrays have been updated and the Storage Nodes rebooted (one at a time) and back online, set the user MetaStore to read/write mode.
    a) Log into the CMC.
    b) Navigate to **Dashboard** > **Administration** > **Storage Management** > **MetaStores**.
    c) In the **Status** column of the user MetaStore, select the **READ/WRITE** option.

6.6 Updating Storage Enclosure Basic Drive Firmware

1. Download and install Hugo on the system
2. Download the desired firmware to the same Controller Node.
3. Use the `scp` command to transfer the firmware to the Storage Node associated with the drives you want to update.
4. Start Hugo
5. Display current firmware version.
6. Update the firmware.
7. Display the firmware version again to confirm that the update succeeded.

7 System Expansion

Topics:

An Active Archive System *cluster* contains 2 racks.

Terminology

The *primary management rack* is the existing rack that is currently live.

The *new rack* is the additional rack that is being added.

Expectations

- The field engineer must perform the following steps on the primary management rack:
  1. Log into the primary management rack's Controller Node and run a health check.
  2. Update the configuration of both TOR switches on the primary management rack.
- The primary management rack does not require any down time during the expansion procedure.
- The expansion procedure does not require any down time for the primary management rack.
- The expansion procedure does not interfere with existing operations.
- The expansion procedure takes 12+ hours for each new rack added.

Assumptions

- The new rack has had its hardware, firmware, and BIOS settings validated at the factory.
- On the primary management rack, the Management Node is online, and none of the services are being reported as down.

> **Important:** Racks must be located within the cable length specified in Preparations on page 28.

7.1 Preparations

Obtain the items listed in the table below.

Item	Available From	Details
IP addresses for the 3 Controller Nodes on public network #1, and IP addresses for the 3 Controller Nodes on public network #2	Customer or data center administrator.	You need a total **6** new public IP addresses.
Private IP addresses for the 3 Controller Nodes on the new rack	Customer	You need a total **6** new private IP addresses.
IPMI IP addresses for the 9 nodes on the new rack		You need a total **9** new IPMI IP addresses.
The serial number of the new rack	http://www.hgst.com/support	The serial number of the new rack is in a CSV file. Download this file onto your laptop.

Item	Available From	Details
Hostname prefix for the new rack.	Customer	The hostname prefix must match the hostname used on the primary management rack.
Physical rack number for the new rack	Customer	The name to be used for the new rack (for example, `R02`).
Name of public network #1, and name of public network #2	Customer	
QSFP+ transceivers	Upgrade kit from HGST	Part number: `AFBR-79EQDZ` Description: `40GBASE-SR4 - Avago4` Quantity: **4**
Fibre cable for Storage Interconnect	Upgrade kit from HGST	Part number: `MPO-LL7EAP005MCS-2` Description: `5m MTP cable` Quantity: **2**
RJ45 (CAT6) cable for Ethernet connection		You need a total of **1** cable, to connect laptop to the Storage Interconnect / Controller Nodes.
Keyboard (USB) and monitor (VGA)	Data center administrator	Required for troubleshooting.
IP address of the Management Node of the primary management rack	Data center administrator	
Passwords for Controller Nodes and Storage Interconnect switches of the primary management rack	Data center administrator	
Installation of new rack (moving the new rack into place and bolting it down)	Data center administrator	Ensure that the new rack is moved to the desired location and bolted down.
Support tools	http://www.hgst.com/support	Download `hgst_health_check.py` and `hgst_configuration_diff.py` onto your laptop.

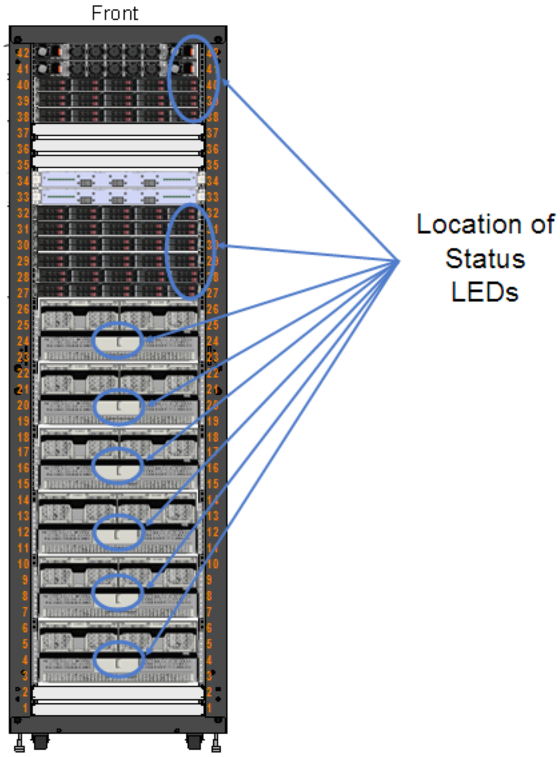
7.2 Executing Preliminary Checks on the New Rack

Follow these steps to ensure that the new rack is fully functional and has not been damaged during shipping/transportation.

1. Connect the external power cords of the new rack to two different distribution networks.
   The system begins to power up automatically as soon as the power cords are connected. The intelligent PDUs control the power-on sequence. The power-on sequence takes approximately 2 minutes.
2. Confirm that all hardware components power up in the correct order.

Observe the status LEDs on the components illuminating in the following order. There is a gap (in seconds) between each segment.

Figure 1: Status Lights on the Active Archive System



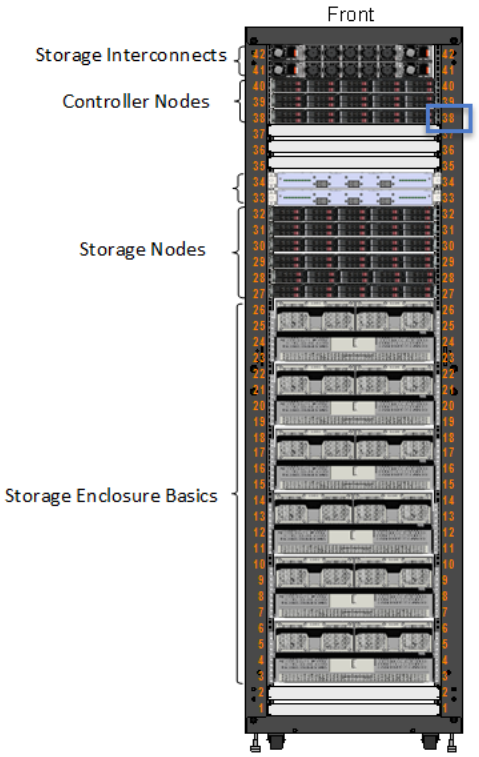
a) Storage Interconnect
b) Controller Nodes
c) Storage Enclosure Basic storage arrays
d) Storage Nodes

3. Connect your laptop to Controller Node 01 (CN01) at **U38** on the new rack.

a) Identify location **U38** on the new rack.

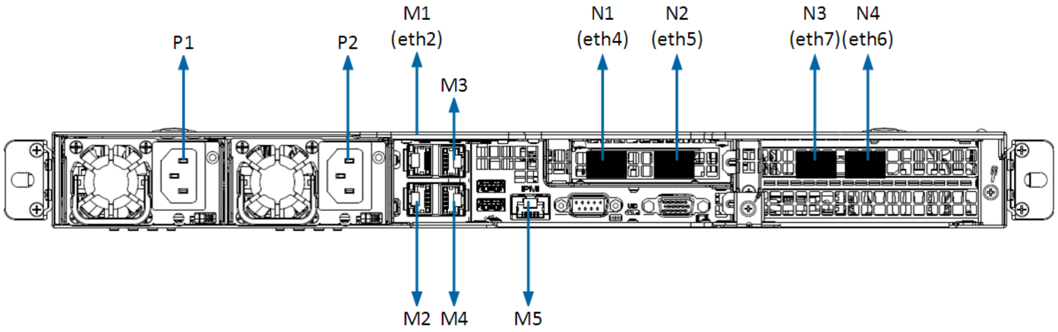
Rack unit labels are only visible from the front of the rack. Refer to the figure below for help in identifying location **U38**.

Figure 2: Location of U38 in the Rack



b) Connect your RJ45 (CAT6) cable to your laptop's Ethernet port and to the port on Controller Node 01 that is labeled **M1** in the figure below.

Figure 3: Controller Node, Back



c) Give your laptop an IP address in the same range as the default IP address of Controller Node 01; in other words, `192.168.107.1/24`.

Example:

Laptop IP address: `192.168.107.20`
Subnet mask: `255.255.255.0`
Gateway: `192.168.107.1` (Use the default IP address of Controller Node 01, as the gateway).

d) Ping the default IP address of Controller Node 01, `192.168.107.1/24`, to confirm that you can reach it.

e) Open an SSH session to the default IP address of Controller Node 01, `192.168.107.1`.
The login prompt appears.

f) Log in using the default credentials (username `root`, password `HGST`).

The end user license agreement (EULA) appears.

g) Press `Enter` to view the end user license agreement (EULA).

h) Accept the EULA.

```
Do you accept the EULA [Default: Yes]:
```

Type `Yes` or press `Enter` to accept the EULA. If you do not accept the EULA, the configuration wizard exits.

i) Complete the configuration wizard by typing the following at each prompt, to ensure no configuration changes are done.

- At the prompt `Do you accept the EULA [Default: Yes]:`, type `Yes`.
- At the prompt `Do you agree to allow the system to send out system telemetry and logs? [Default: Yes]:`, type `Yes`.
- At the prompt `Enter the current password for the administrator account:`, type the default password for `admin` (`HGST`).
- At the prompt `Enter a new password for the administrator account:`, type the default password for `admin` (`HGST`).
- At the prompt `Enter the current root password for the machines:` type the default password for `admin` (`HGST`).
- At the prompt `Would you like to use SSL for the user interface [Default: No]:` , type `No`.
- At the prompt `Currently configuring location. Proceed? [Default: Yes]:` , type **`No`**.
- At the prompt `Currently configuring notification. Proceed? [Default: Yes]:` , type **`No`**.
- At the prompt `Currently configuring s3. Proceed? [Default: Yes]:` , type **`No`**.
- At the prompt `Currently configuring networking. Proceed? [Default: Yes]:` , type **`No`**.
- At the prompt `Do you want to apply these changes [Default: Yes]:` , type `Yes`.

4. Generate a new CSV file from the CSV file located on the new rack.

a) When the configuration wizard is completed, transfer the file it generated, `initialize_complete.csv`, from Controller Node 01 on the new rack onto your laptop.
For example,

```
scp root@192.168.107.1:/opt/qbase3/cfg/
initialize_complete.csv some_dir/expansion_rack.csv
```

b) Get the MAC address and IP address from Controller Node 01 on the new rack.

c) Open an SSH session to Controller Node 01 on the new rack, using its default IP address, `01. 192.168.107.1`.

Log in using the default credentials (username `root`, password `HGST`).

The OSMI menu appears.

d) Exit the OSMI menu.
The Linux prompt appears.

e) At the Linux prompt, run the `ifconfig` command.

f) From the output of `ifconfig` fill in the following table:

NIC	IP Address	MAC Address
`Eth4`		
`Eth5`		
`Eth6`		
`Eth7`		

g) Exit the SSH session.

h) Modify **expansion_rack.csv** with information from the above table, as follows:

    Insert a new row right after the first row.
    Under the `Node Type` column, type `CPU`.
    Under the `Datacenter` column, type `DC01`.
    Under the `Rack` column, type `DC01-LR07`.
    Under the `MAC1` column, type the MAC address in for `eth6` from the table above.
    Under the `Lan1` column, type `DC01 Pubic2_lan`.
    Under the `IP1` column, type the IP Address for `eth6` from the table above.
    Under the `MAC2` column, type the MAC Address for `eth5` from the table above.
    Under the `Lan2` column, type `DC01 Storage1_lan`.
    Under the `IP2` column, type the IP address for `eth5` from the table above.
    Under the `MAC3` column, type the MAC Address for `eth7` from the table above.
    Under the `Lan3` column, type `DC01 Storage2_lan`.
    Under the `IP3` column, type the IP Address for `eth7` from the table above.
    Under the `MAC4` column, type the MAC Address for `eth4` from the table above.
    Under the `Lan4` column, type `DC01 Public1_lan`.
    Under the `IP4` column, type the IP Address for `eth4` from the table above.

i) Save and close the file.

5. Verify the health of the new rack.

a) Using `scp`, transfer the script `hgst_health_check.py` from your laptop to Controller Node 01 on the new rack.

b) Navigate to the destination directory where the script was transferred to, and make the script executable.

```
chmod +x hgst_health_check.py
```

c) Run `hgst_health_check.py` on the new rack to ensure that all hardware/software is functional.

```
python hgst_health_check.py
```

This runs for about 15 minutes and displays its progress. Upon completion, `hgst_health_check.py` generates a log file, `hgst_healthcheck.log`, with all the information it displayed onscreen. If it finds errors, it prints the details about the errors and also provides instructions for an interactive shell.

Important: If `hgst_health_check.py` reports any errors, contact HGST support.

d) Once the health check is complete, exit the SSH session and disconnect your laptop from the new rack.

6. Power off all Controller and Storage Nodes in the new rack.

Press the power button on the front control panel of each node.

Important: It is important to power off all the nodes to avoid IP conflicts.

7. Verify the health of the primary management rack.

a) Open an SSH session to the IP address of the Management Node of the primary management rack.

b) Using `scp`, transfer the script `hgst_health_check.py` from your laptop to the Management Node of the primary management rack.

c) Navigate to the destination directory where the script was transferred to, and make the script executable.

```
chmod +x hgst_health_check.py
```

d) Run `hgst_health_check.py` on the primary management rack to ensure that all hardware/software is functional.

```
python hgst_health_check.py
```

This runs for about 15 minutes and displays its progress. Upon completion, `hgst_health_check.py` generates a log file, `hgst_healthcheck.log`, with all the information it displayed onscreen. If it finds errors, it prints the details about the errors and also provides instructions for an interactive shell.

Important: If `hgst_health_check.py` reports any errors, contact HGST support.

e) Once the health check is complete, exit the SSH session.

Important: All racks must pass the system health check before proceeding further.

7.3 Configuring the TOR Storage Interconnect Switches

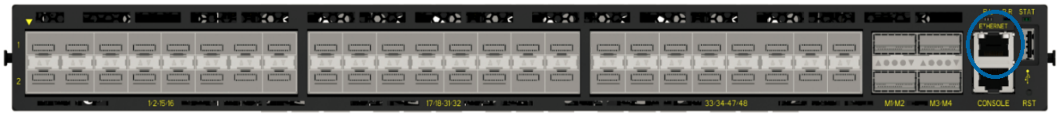
Reconfigure both TOR Storage Interconnect switches on the primary management rack and the new rack as follows.

Note: In the examples shown, `rack03` is the primary management rack, and `rack13` is the new rack.

1. Connect your laptop to the management port (`ETHERNET`) on TOR switch 1 (lower).

a) Connect your RJ 45 (CAT6) from your laptop's Ethernet port to the port on the switch labeled `ETHERNET` in the figure below on the master rack.

Figure 4: TOR Switch, Ethernet Port



b) Give your laptop an IP address in the same range as the default IP address of the switch; in other words, `192.168.123.20/24`.

Example:

Laptop IP address: `192.168.123.20`
Subnet mask: `255.255.255.0`
Gateway: `192.168.123.1` (Use the default IP address of the switch, as the gateway).

c) Ping the default IP address of the switch, (`192.168.123.123/ 192.168.123.123`), to confirm that you can reach it.

2. Reconfigure TOR switch 1 on the primary management rack.

a) Open a `TELNET` session to the default IP address of switch 1, `192.168.123.123`.
The login prompt appears.

b) Log in using the default credentials (username `admin`, there is no default password set, so press `Enter` to continue.
The switch command prompt appears.

c) Enter the following commands to reconfigure TOR switch 1 on the primary management rack.

```
enable
configure
interface 0/49,0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
no spanning-tree bpdufilter
exit
exit
write memory
```

Verify the above configuration is done as in the example below:

```
(rack03-sw01) (Config)#show running-config interface vlan 100
interface vlan 100
routing
ip address dhcp
ip address  172.16.1.50  255.255.192.0  secondary
exit

(rack03-sw01) (Config)#show running-config interface 0/49
interface  0/49
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit

(rack03-sw01) (Config)#show running-config interface 0/51
interface  0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit
```

d) Exit the `TELNET` session.

3. Reconfigure TOR switch 2 on the primary management rack.

a) Open a `TELNET` session to the default IP address of switch 2, `192.168.123.123`.
The login prompt appears.

b) Log in using the default credentials (username `admin`, no password).
The switch command prompt appears.

c) Enter the following commands to reconfigure TOR switch 2 on the primary management rack.

```
enable
configure
interface 0/49,0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
no spanning-tree bpdufilter
exit
exit
write memory
```

Verify the above configuration is done as in the example below:

```
(rack03-sw02) #show running-config interface vlan 100
interface vlan 100
routing
ip address dhcp
ip address  172.16.101.50  255.255.192.0  secondary
exit

(rack03-sw02) #show running-config  interface 0/49
interface  0/49
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit

(rack03-sw02) #show running-config  interface 0/51
interface  0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit
(rack03-sw02) #
```

d) Exit the `TELNET` session.

4. Repeat the steps above for configuring the TOR switches on the new rack.

a) Connect your RJ 45 (CAT6) from your laptop's Ethernet port to the port on the switch labeled `ETHERNET` in the figure below on the master rack.

b) Give your laptop an IP address in the same range as the default IP address of switch 1 (lower); in other words, `192.168.123.20/24`.

Example:

Laptop IP address: `192.168.123.20`
Subnet mask: `255.255.255.0`
Gateway: `192.168.123.1` (Use the default IP address of the switch, as the gateway).

c) Ping the default IP address of the above switch, (`192.168.123.123/192.168.123.123`), to confirm that you can reach it.

5. Reconfigure TOR switch 1 on the new rack.

a) Open a `TELNET` session to the default IP address of switch 1 on the new rack, `192.168.123.123`.
The login prompt appears.

b) Log in using the default credentials (username `admin`, no password).
The switch command prompt appears.

c) Enter the following commands to reconfigure TOR switch 1 on the new rack.

```
enable
configure
interface 0/49,0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
no spanning-tree bpdufilter
exit
interface vlan 100
no ip address  172.16.1.50  255.255.192.0  secondary
ip address  172.16.2.50  255.255.192.0  secondary
exit
exit
write memory
```

Verify the above configuration is done as in the example below:

```
interface vlan 100
routing
ip address dhcp
ip address  172.16.2.50  255.255.192.0  secondary
```

```
exit

(rack13-sw01) #show running-config interface 0/49
interface  0/49
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit

(rack13-sw01) #show running-config interface 0/51
!Current Configuration:
interface  0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit
```

d) Exit the `TELNET` session.

6. Reconfigure TOR switch 2 on the new rack.

a) Open a `TELNET` session to the default IP address of switch 2 on the new rack, `192.168.123.123`.
The login prompt appears.

b) Log in using the default credentials (username `admin`, no password).
The switch command prompt appears.

c) Enter the following commands to reconfigure TOR switch 2 on the new rack.

```
enable
configure
interface 0/49,0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
no spanning-tree bpdufilter
exit
interface vlan 100
no ip address  172.16.101.50  255.255.192.0  secondary
ip address  172.16.102.50  255.255.192.0  secondary
exit
exit
write memory
```

Verify the above configuration is done as in the example below:

```
(rack13-sw02) #show running-config interface vlan 100
interface vlan 100
routing
ip address dhcp
ip address  172.16.102.50  255.255.192.0  secondary
exit

(rack13-sw02) #show running-config interface 0/49
interface  0/49
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit

(rack13-sw02) #show running-config interface 0/51
interface  0/51
vlan pvid 100
vlan acceptframe vlanonly
vlan ingressfilter
vlan participation include 100
vlan tagging 100
exit
```

d) Exit the `TELNET` session.

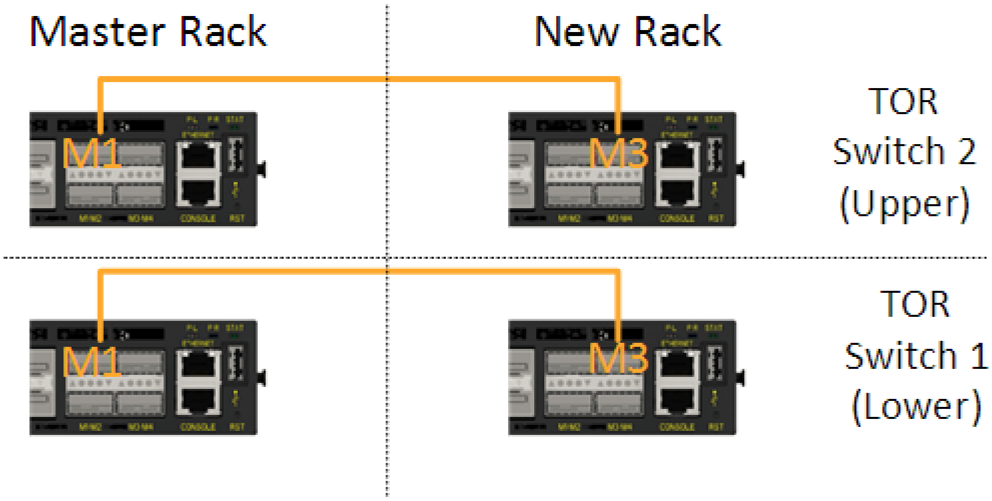
7.4 Interconnecting the TOR Switches

Connect the new rack to your existing rack(s) as follows.

1. Connect transceivers to all the TOR switches as follows:
   - Rack 1, switch 1(lower), plug QSFP+ module into port 49 (Upper left QSFP+ port) of switch
   - Rack 1, switch 2(upper), plug QSFP+ module into port 49 (Upper left QSFP+ port) of switch
   - Rack 2, switch 1(lower), plug QSFP+ module into port 51 (Upper right QSFP+ port) of switch
   - Rack 2, switch 2(upper), plug QSFP+ module into port 51 (Upper right QSFP+ port) of switch
2. Interconnect the TOR switches of both racks.
   - Connect MTP/MPO cable from port 49 (M1) (rack 1/switch 1) to port 51 (M3) (rack 2/switch 1)
   - Connect MTP/MPO cable from port 49 (M1) (rack 1/switch 2) to port 51 (M3) (rack 2/switch 2)

   Refer to the diagram below.

   Figure 5: Connecting the QSFP+ Ports on the Storage Interconnect Switches



3. Verify link status and switch connectivity.

   a) From the both the rack's TOR switch 1 and 2, verify the link status.

```
(rack03-sw01) #show interfaces status | include 0/49
0/49                                    Up      40G Full    40G Full    40G-
BaseSX          Inactive
(rack03-sw02) #show interfaces status | include 0/49
0/49                                    Up      40G Full    40G Full    40G-
BaseSX          Inactive
New RACK
```

```
(rack13-sw01) #show interfaces status | include 0/51
0/51                                     Up      40G Full    40G Full    40G-
BaseSX          Inactive
(rack13-sw02) #show interfaces status | include 0/51
0/51                                     Up      40G Full    40G Full    40G-
BaseSX          Inactive
```

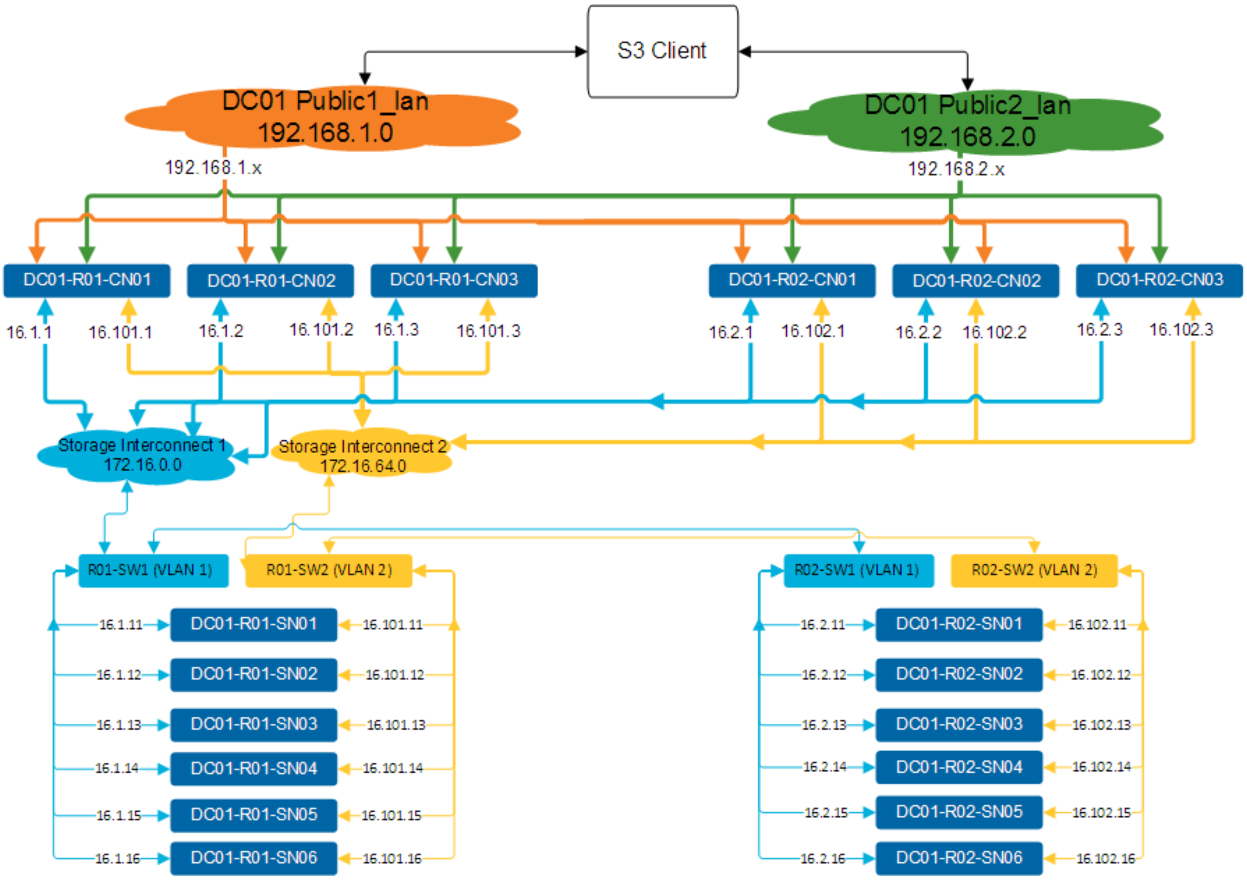
The LED corresponding to the ports should be green.

b) Do a ping test from the primary management rack TOR switches to the IP address of the VLAN interface as shown in the example below.
For example,

```
(rack03-sw01) #show running-config interface vlan 100
interface vlan 100
routing
ip address dhcp
ip address  172.16.1.50  255.255.192.0  secondary
exit

(rack03-sw01) #ping 172.16.2.50
Pinging 172.16.2.50 with 0 bytes of data:
Reply From 172.16.2.50: icmp_seq = 0. time= 0 usec.
Reply From 172.16.2.50: icmp_seq = 1. time= 0 usec.
Reply From 172.16.2.50: icmp_seq = 2. time= 0 usec.
----172.16.2.50 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0

(rack03-sw02) #show running-config interface vlan 100
interface vlan 100
routing
ip address dhcp
ip address  172.16.101.50  255.255.192.0  secondary
exit

(rack03-sw02) #ping 172.16.102.50
Pinging 172.16.102.50 with 0 bytes of data:
Reply From 172.16.102.50: icmp_seq = 0. time= 0 usec.
Reply From 172.16.102.50: icmp_seq = 1. time= 0 usec.
Reply From 172.16.102.50: icmp_seq = 2. time= 0 usec.
----172.16.102.50 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

```
exit
```

Figure 6: Network Connectivity for Data Center 1 (DC01), Racks 1 and 2 (R01 and RC02), with Default IP Addresses

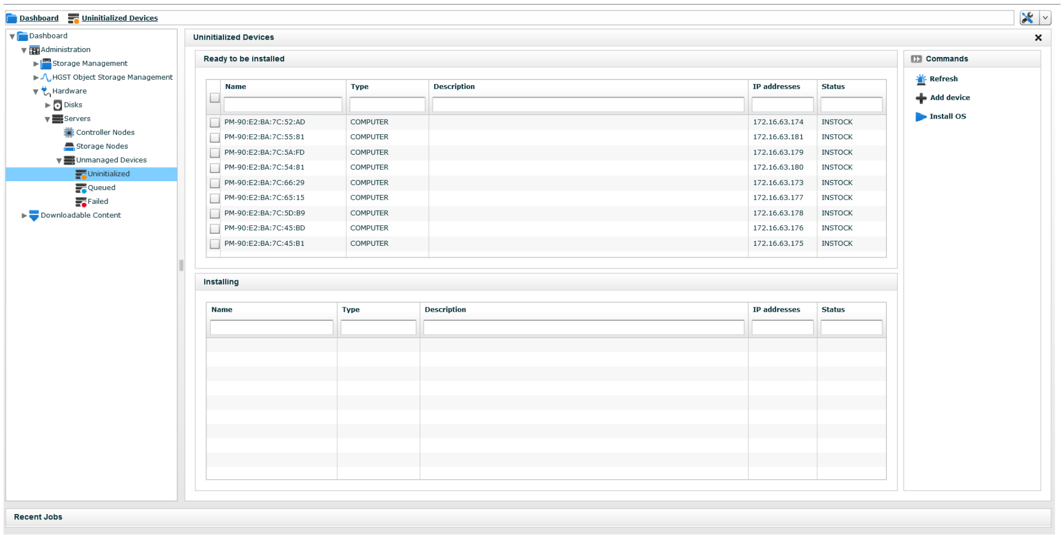


7.5 Installing the Active Archive System Software

1. Power on the new rack servers by pressing the power button on the front control panel of the servers. The servers automatically PXE boot to the existing Management Node.
2. Log into the CMC.
3. In CMC navigate to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Unmanaged Devices** > **Uninitialized**.

The successfully PXE booted nodes on the new rack appear with hostnames in the format `PM-`*`mac_address`* and status **INSTOCK**. Wait for 5 minutes. Verify all nine systems are displayed in the CMC.

Figure 7: Uninitialized Devices Displayed in the CMC



Uninitialized Devices

Ready to be installed

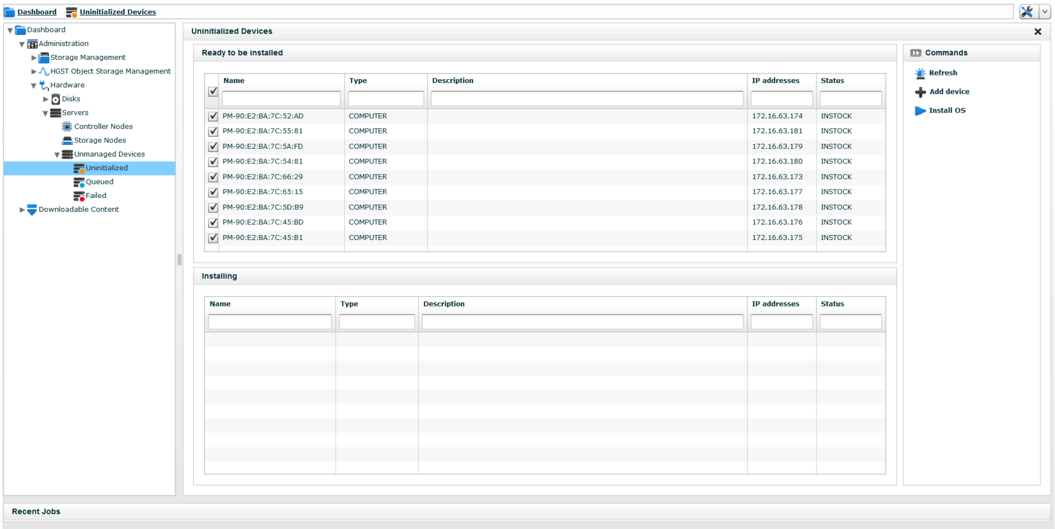
□	Name	Type	Description	IP addresses	Status
□	PM-90:E2:BA:7C:52:AD	COMPUTER		172.16.63.174	INSTOCK
□	PM-90:E2:BA:7C:55:81	COMPUTER		172.16.63.181	INSTOCK
□	PM-90:E2:BA:7C:5A:FD	COMPUTER		172.16.63.179	INSTOCK
□	PM-90:E2:BA:7C:54:81	COMPUTER		172.16.63.180	INSTOCK
□	PM-90:E2:BA:7C:66:29	COMPUTER		172.16.63.173	INSTOCK
□	PM-90:E2:BA:7C:65:15	COMPUTER		172.16.63.177	INSTOCK
□	PM-90:E2:BA:7C:5D:B9	COMPUTER		172.16.63.178	INSTOCK
□	PM-90:E2:BA:7C:45:BD	COMPUTER		172.16.63.176	INSTOCK
□	PM-90:E2:BA:7C:45:B1	COMPUTER		172.16.63.175	INSTOCK

Installing

Name	Type	Description	IP addresses	Status

4. Select the check boxes of all **INSTOCK** nodes.

Figure 8: Selecting all INSTOCK Nodes in the CMC



Uninitialized Devices

Ready to be installed

☑	Name	Type	Description	IP addresses	Status
☑	PM-90:E2:BA:7C:52:AD	COMPUTER		172.16.63.174	INSTOCK
☑	PM-90:E2:BA:7C:55:81	COMPUTER		172.16.63.181	INSTOCK
☑	PM-90:E2:BA:7C:5A:FD	COMPUTER		172.16.63.179	INSTOCK
☑	PM-90:E2:BA:7C:54:81	COMPUTER		172.16.63.180	INSTOCK
☑	PM-90:E2:BA:7C:66:29	COMPUTER		172.16.63.173	INSTOCK
☑	PM-90:E2:BA:7C:65:15	COMPUTER		172.16.63.177	INSTOCK
☑	PM-90:E2:BA:7C:5D:B9	COMPUTER		172.16.63.178	INSTOCK
☑	PM-90:E2:BA:7C:45:BD	COMPUTER		172.16.63.176	INSTOCK
☑	PM-90:E2:BA:7C:45:B1	COMPUTER		172.16.63.175	INSTOCK

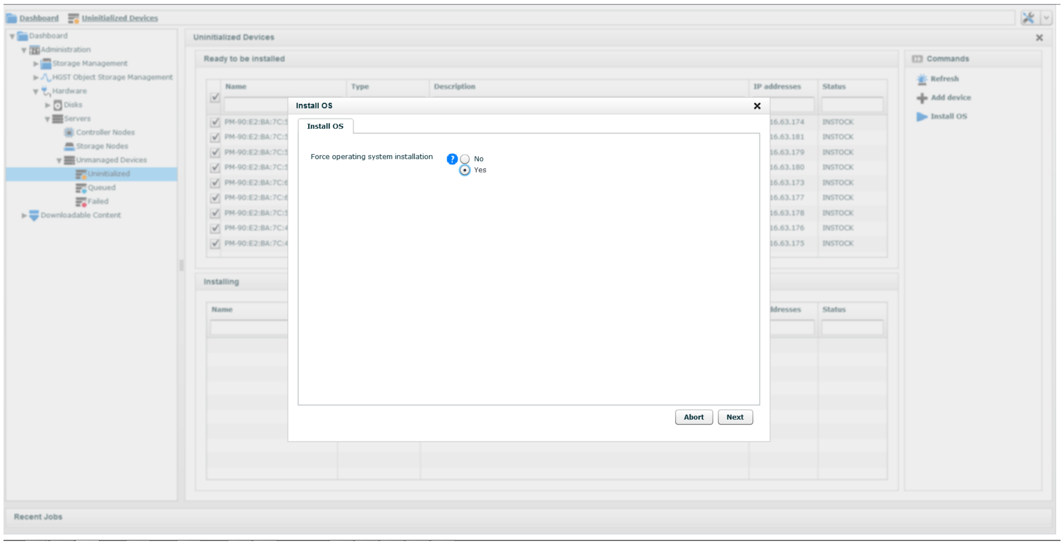
Installing

Name	Type	Description	IP addresses	Status

5. Click **Install OS** in the right pane.

6. Select the **Yes** radio button at the **Force operation system installation** prompt.

Figure 9: Selecting the Force operation system installation Option in the CMC

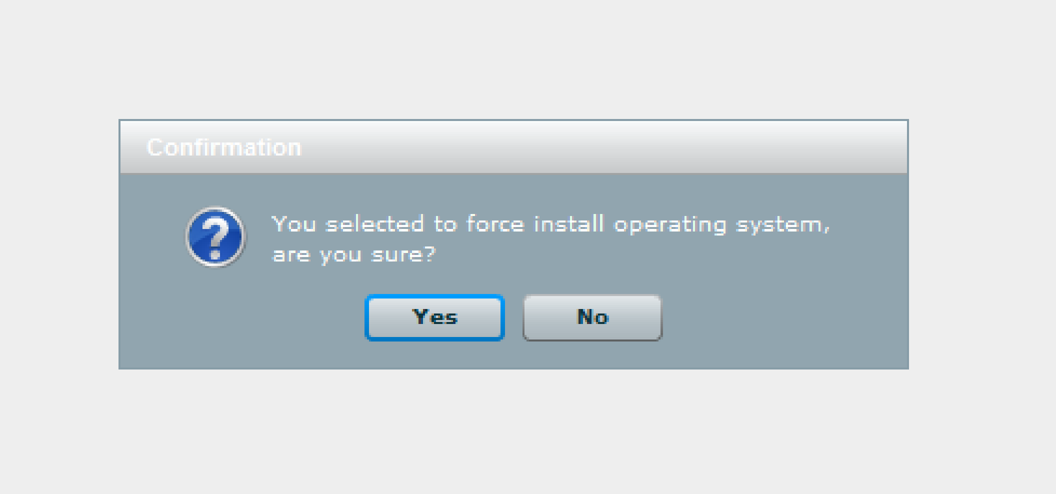


Name	IP addresses	Status
☑ PM-90:E2:BA:7C:5	16.63.174	INSTOCK
☑ PM-90:E2:BA:7C:5	16.63.181	INSTOCK
☑ PM-90:E2:BA:7C:5	16.63.179	INSTOCK
☑ PM-90:E2:BA:7C:5	16.63.180	INSTOCK
☑ PM-90:E2:BA:7C:6	16.63.173	INSTOCK
☑ PM-90:E2:BA:7C:6	16.63.177	INSTOCK
☑ PM-90:E2:BA:7C:5	16.63.178	INSTOCK
☑ PM-90:E2:BA:7C:4	16.63.176	INSTOCK
☑ PM-90:E2:BA:7C:4	16.63.175	INSTOCK

Force operating system installation ○ No ● Yes

7. Select **Next**.
8. Select **Yes** for confirmation.

Figure 10: Confirming OS Installation

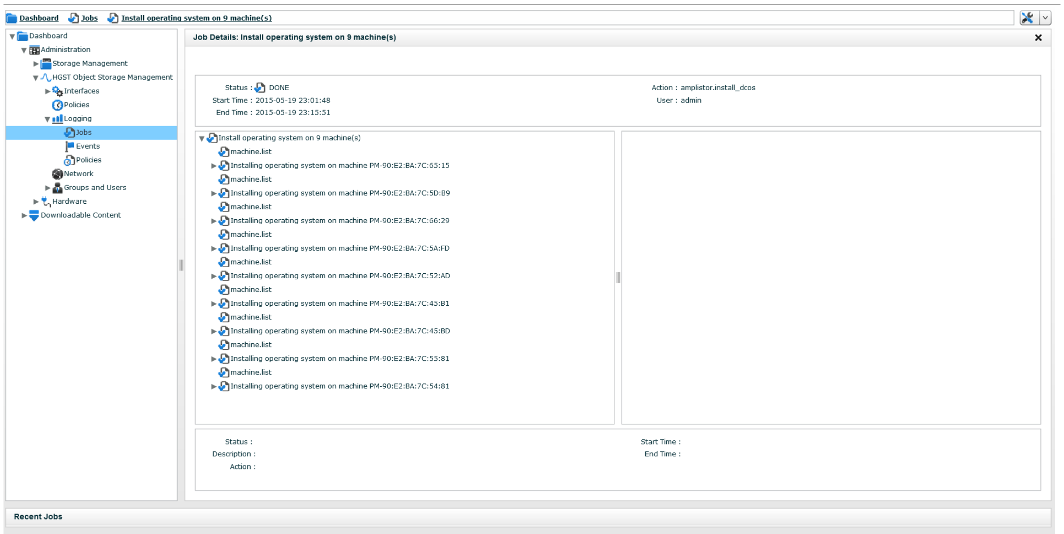


You selected to force install operating system, are you sure?

9. Monitor the `Install operating system on 9 machine(s)` job in **Dashboard** > **Administration** > **HGST Object Storage Management** > **Logging** > **Jobs**.
10. Verify that the `Initialize Node` completes successfully.

The Status field will have a blue checkmark and the text **Done**.

Figure 11: Details of a Node Initialization Job in the CMC



Job Details: Install operating system on 9 machine(s)

Status : DONE
Start Time : 2015-05-19 23:01:48
End Time : 2015-05-19 23:15:51
Action : amplistor.install_dcos
User : admin

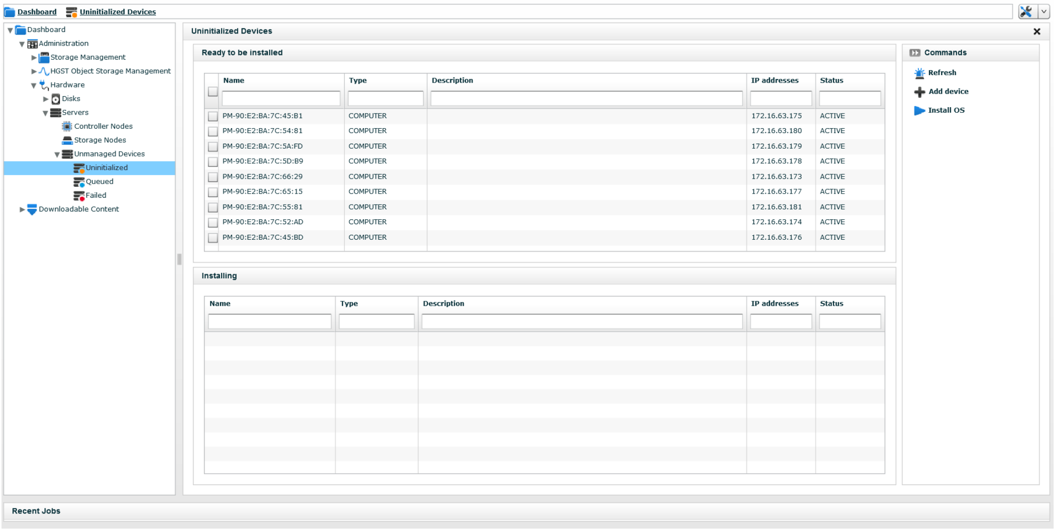
```
Install operating system on 9 machine(s)
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:65:15
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:5D:B9
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:66:29
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:5A:FD
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:52:AD
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:45:B1
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:45:BD
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:55:81
    machine.list
    Installing operating system on machine PM-90:E2:BA:7C:54:81
```

Status :
Description :
Action :
Start Time :
End Time :

It takes about 45 minutes for this job to complete.

11. Validate that once the job completes successfully, all nine nodes have status **ACTIVE** in **Dashboard** > **Administration** > **Hardware** > **Servers** > **Unmanaged Devices** > **Uninitialized**.

Figure 12: Successful Node Initialization Job in the CMC



Uninitialized Devices

Ready to be installed

□	Name	Type	Description	IP addresses	Status
□	PM-90:E2:BA:7C:45:B1	COMPUTER		172.16.63.175	ACTIVE
□	PM-90:E2:BA:7C:54:81	COMPUTER		172.16.63.180	ACTIVE
□	PM-90:E2:BA:7C:5A:FD	COMPUTER		172.16.63.179	ACTIVE
□	PM-90:E2:BA:7C:5D:B9	COMPUTER		172.16.63.178	ACTIVE
□	PM-90:E2:BA:7C:66:29	COMPUTER		172.16.63.173	ACTIVE
□	PM-90:E2:BA:7C:65:15	COMPUTER		172.16.63.177	ACTIVE
□	PM-90:E2:BA:7C:55:81	COMPUTER		172.16.63.181	ACTIVE
□	PM-90:E2:BA:7C:52:AD	COMPUTER		172.16.63.174	ACTIVE
□	PM-90:E2:BA:7C:45:BD	COMPUTER		172.16.63.176	ACTIVE

Installing

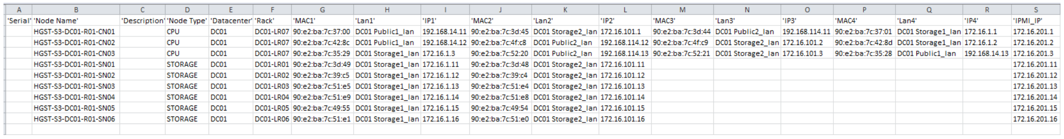
Name	Type	Description	IP addresses	Status

7.6 Initializing the Multi Rack System

1. Download the CSV file from HGST to your laptop.

2. Open the CSV using Microsoft Excel.

Figure 13: CSV File



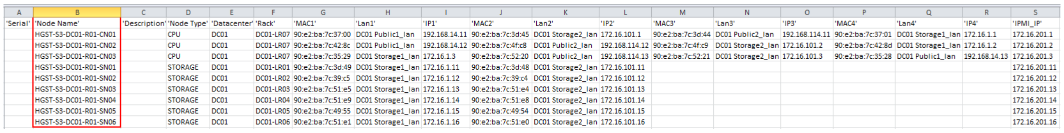
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
'Serial'	'Node Name'	'Description'	'Node Type'	'Datacenter'	'Rack'	'MAC1'	'Lan1'	'IP1'	'MAC2'	'Lan2'	'IP2'	'MAC3'	'Lan3'	'IP3'	'MAC4'	'Lan4'	'IP4'	'IPMI_IP'
	HGST-S3-DC01-R01-CN01		CPU	DC01	DC01-LR07	90:e2:ba:7c:37:00	DC01 Public1_lan	192.168.14.11	90:e2:ba:7c:3d:45	DC01 Storage2_lan	172.16.101.1	90:e2:ba:7c:3d:44	DC01 Public2_lan	192.168.114.11	90:e2:ba:7c:37:01	DC01 Storage1_lan	172.16.1.1	172.16.201.1
	HGST-S3-DC01-R01-CN02		CPU	DC01	DC01-LR07	90:e2:ba:7c:42:8c	DC01 Public1_lan	192.168.14.12	90:e2:ba:7c:4f:c8	DC01 Public2_lan	192.168.114.12	90:e2:ba:7c:4f:c9	DC01 Storage2_lan	172.16.101.2	90:e2:ba:7c:42:8d	DC01 Storage1_lan	172.16.1.2	172.16.201.2
	HGST-S3-DC01-R01-CN03		CPU	DC01	DC01-LR07	90:e2:ba:7c:35:29	DC01 Storage1_lan	172.16.1.3	90:e2:ba:7c:52:20	DC01 Public2_lan	192.168.114.13	90:e2:ba:7c:52:21	DC01 Storage2_lan	172.16.101.3	90:e2:ba:7c:35:28	DC01 Public1_lan	192.168.14.13	172.16.201.3
	HGST-S3-DC01-R01-SN01		STORAGE	DC01	DC01-LR01	90:e2:ba:7c:3d:49	DC01 Storage1_lan	172.16.1.11	90:e2:ba:7c:3d:48	DC01 Storage2_lan	172.16.101.11							172.16.201.11
	HGST-S3-DC01-R01-SN02		STORAGE	DC01	DC01-LR02	90:e2:ba:7c:39:c5	DC01 Storage1_lan	172.16.1.12	90:e2:ba:7c:39:c4	DC01 Storage2_lan	172.16.101.12							172.16.201.12
	HGST-S3-DC01-R01-SN03		STORAGE	DC01	DC01-LR03	90:e2:ba:7c:51:e5	DC01 Storage1_lan	172.16.1.13	90:e2:ba:7c:51:e4	DC01 Storage2_lan	172.16.101.13							172.16.201.13
	HGST-S3-DC01-R01-SN04		STORAGE	DC01	DC01-LR04	90:e2:ba:7c:51:e9	DC01 Storage1_lan	172.16.1.14	90:e2:ba:7c:51:e8	DC01 Storage2_lan	172.16.101.14							172.16.201.14
	HGST-S3-DC01-R01-SN05		STORAGE	DC01	DC01-LR05	90:e2:ba:7c:49:55	DC01 Storage1_lan	172.16.1.15	90:e2:ba:7c:49:54	DC01 Storage2_lan	172.16.101.15							172.16.201.15
	HGST-S3-DC01-R01-SN06		STORAGE	DC01	DC01-LR06	90:e2:ba:7c:51:e1	DC01 Storage1_lan	172.16.1.16	90:e2:ba:7c:51:e0	DC01 Storage2_lan	172.16.101.16							172.16.201.16

3. Update the hostname prefix and the rack identifier for each node in the second column.
   a) Replace the prefix `HGST-S3` in each field with the hostname already in use on the existing rack(s).

   You can find the hostname of the system by logging into the CMC and navigating to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Controller Nodes**.

   b) In the CSV file, replace `R01` with the physical rack number that is being added. For example, if this is the second rack, replace `R01` with `R02`.

Figure 14: CSV File, Hostnames for the New Rack



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
'Serial'	'Node Name'	'Description'	'Node Type'	'Datacenter'	'Rack'	'MAC1'	'Lan1'	'IP1'	'MAC2'	'Lan2'	'IP2'	'MAC3'	'Lan3'	'IP3'	'MAC4'	'Lan4'	'IP4'	'IPMI_IP'
	HGST-S3-DC01-R01-CN01		CPU	DC01	DC01-LR07	90:e2:ba:7c:37:00	DC01 Public1_lan	192.168.14.11	90:e2:ba:7c:3d:45	DC01 Storage2_lan	172.16.101.1	90:e2:ba:7c:3d:44	DC01 Public2_lan	192.168.114.11	90:e2:ba:7c:37:01	DC01 Storage1_lan	172.16.1.1	172.16.201.1
	HGST-S3-DC01-R01-CN02		CPU	DC01	DC01-LR07	90:e2:ba:7c:42:8c	DC01 Public1_lan	192.168.14.12	90:e2:ba:7c:4f:c8	DC01 Public2_lan	192.168.114.12	90:e2:ba:7c:4f:c9	DC01 Storage2_lan	172.16.101.2	90:e2:ba:7c:42:8d	DC01 Storage1_lan	172.16.1.2	172.16.201.2
	HGST-S3-DC01-R01-CN03		CPU	DC01	DC01-LR07	90:e2:ba:7c:35:29	DC01 Storage1_lan	172.16.1.3	90:e2:ba:7c:52:20	DC01 Public2_lan	192.168.114.13	90:e2:ba:7c:52:21	DC01 Storage2_lan	172.16.101.3	90:e2:ba:7c:35:28	DC01 Public1_lan	192.168.14.13	172.16.201.3
	HGST-S3-DC01-R01-SN01		STORAGE	DC01	DC01-LR01	90:e2:ba:7c:3d:49	DC01 Storage1_lan	172.16.1.11	90:e2:ba:7c:3d:48	DC01 Storage2_lan	172.16.101.11							172.16.201.11
	HGST-S3-DC01-R01-SN02		STORAGE	DC01	DC01-LR02	90:e2:ba:7c:39:c5	DC01 Storage1_lan	172.16.1.12	90:e2:ba:7c:39:c4	DC01 Storage2_lan	172.16.101.12							172.16.201.12
	HGST-S3-DC01-R01-SN03		STORAGE	DC01	DC01-LR03	90:e2:ba:7c:51:e5	DC01 Storage1_lan	172.16.1.13	90:e2:ba:7c:51:e4	DC01 Storage2_lan	172.16.101.13							172.16.201.13
	HGST-S3-DC01-R01-SN04		STORAGE	DC01	DC01-LR04	90:e2:ba:7c:51:e9	DC01 Storage1_lan	172.16.1.14	90:e2:ba:7c:51:e8	DC01 Storage2_lan	172.16.101.14							172.16.201.14
	HGST-S3-DC01-R01-SN05		STORAGE	DC01	DC01-LR05	90:e2:ba:7c:49:55	DC01 Storage1_lan	172.16.1.15	90:e2:ba:7c:49:54	DC01 Storage2_lan	172.16.101.15							172.16.201.15
	HGST-S3-DC01-R01-SN06		STORAGE	DC01	DC01-LR06	90:e2:ba:7c:51:e1	DC01 Storage1_lan	172.16.1.16	90:e2:ba:7c:51:e0	DC01 Storage2_lan	172.16.101.16							172.16.201.16

4. Update the public LAN names to match your network LAN names.
   a) Open an SSH session to the Management Node, and exit the OSMI shell.
   b) Enter the Q-Shell.

```
sudo /opt/qbase3/qshell
```

   c) Execute the following Python code to get a list of your LAN names and which eth device the LAN is being used on.

   Copy and paste these lines into the shell one line at a time. Each line is automatically indented as needed.

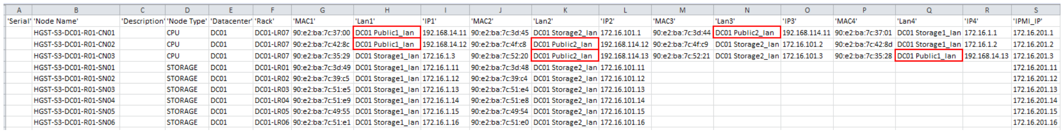
```
api = i.config.cloudApiConnection.find('main')
mguid = api.amplistor.getApplianceInfo()['result']['machineguid']
machine_nics = api.machine.getObject(mguid).nics
public_lans = api.lan.find(publicflag=True)['result']
for nic in machine_nics:
    if nic.ipaddressguids:
        lguid = api.ipaddress.list(nic.ipaddressguids[0])['result'][0]['languid']
     if lguid in public_lans:
         lan_name = api.lan.list(languid=lguid)['result'][0]['name']
      print "%s : %s" % (nic.name, lan_name)
```

   The output is similar to what is shown below:

```
eth6 : name_of_network1
eth4 : name_of_network2
```

   d) Replace all references to `DC01 Public1_lan` with the value returned for `eth4`. In the sample output, this is *`name_of_network2`*.
   e) Replace all references to `DC01 Public2_lan` with the value returned after `eth6`. In the sample output, this is *`name_of_network1`*.

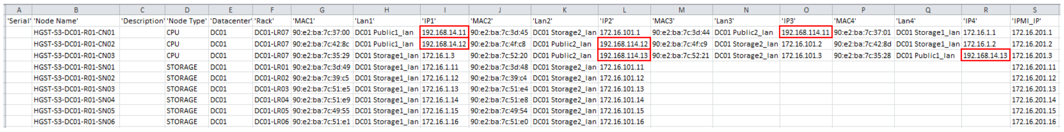
Figure 15: CSV File, Network Names



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
'Serial'	'Node Name'	'Description'	'Node Type'	'Datacenter'	'Rack'	'MAC1'	'Lan1'	'IP1'	'MAC2'	'Lan2'	'IP2'	'MAC3'	'Lan3'	'IP3'	'MAC4'	'Lan4'	'IP4'	'IPMI_IP'
	HGST-S3-DC01-R01-CN01		CPU	DC01	DC01-LR07	90:e2:ba:7c:37:00	DC01 Public1_lan	192.168.14.11	90:e2:ba:7c:3d:45	DC01 Storage2_lan	172.16.101.1	90:e2:ba:7c:3d:44	DC01 Public2_lan	192.168.114.11	90:e2:ba:7c:37:01	DC01 Storage1_lan	172.16.1.1	172.16.201.1
	HGST-S3-DC01-R01-CN02		CPU	DC01	DC01-LR07	90:e2:ba:7c:42:8c	DC01 Public1_lan	192.168.14.12	90:e2:ba:7c:4f:c8	DC01 Public2_lan	192.168.114.12	90:e2:ba:7c:4f:c9	DC01 Storage2_lan	172.16.101.2	90:e2:ba:7c:42:8d	DC01 Storage1_lan	172.16.1.2	172.16.201.2
	HGST-S3-DC01-R01-CN03		CPU	DC01	DC01-LR07	90:e2:ba:7c:35:29	DC01 Storage1_lan	172.16.1.3	90:e2:ba:7c:52:20	DC01 Public2_lan	192.168.114.13	90:e2:ba:7c:52:21	DC01 Storage2_lan	172.16.101.3	90:e2:ba:7c:35:28	DC01 Public1_lan	192.168.14.13	172.16.201.3
	HGST-S3-DC01-R01-SN01		STORAGE	DC01	DC01-LR01	90:e2:ba:7c:3d:49	DC01 Storage1_lan	172.16.1.11	90:e2:ba:7c:3d:48	DC01 Storage2_lan	172.16.101.11							172.16.201.11
	HGST-S3-DC01-R01-SN02		STORAGE	DC01	DC01-LR02	90:e2:ba:7c:39:c5	DC01 Storage1_lan	172.16.1.12	90:e2:ba:7c:39:c4	DC01 Storage2_lan	172.16.101.12							172.16.201.12
	HGST-S3-DC01-R01-SN03		STORAGE	DC01	DC01-LR03	90:e2:ba:7c:51:e5	DC01 Storage1_lan	172.16.1.13	90:e2:ba:7c:51:e4	DC01 Storage2_lan	172.16.101.13							172.16.201.13
	HGST-S3-DC01-R01-SN04		STORAGE	DC01	DC01-LR04	90:e2:ba:7c:51:e9	DC01 Storage1_lan	172.16.1.14	90:e2:ba:7c:51:e8	DC01 Storage2_lan	172.16.101.14							172.16.201.14
	HGST-S3-DC01-R01-SN05		STORAGE	DC01	DC01-LR05	90:e2:ba:7c:49:55	DC01 Storage1_lan	172.16.1.15	90:e2:ba:7c:49:54	DC01 Storage2_lan	172.16.101.15							172.16.201.15
	HGST-S3-DC01-R01-SN06		STORAGE	DC01	DC01-LR06	90:e2:ba:7c:51:e1	DC01 Storage1_lan	172.16.1.16	90:e2:ba:7c:51:e0	DC01 Storage2_lan	172.16.101.16							172.16.201.16

5. Update the public IP assignments to match your desired IPs for each system.

Figure 16: CSV File, Public IP Assignments

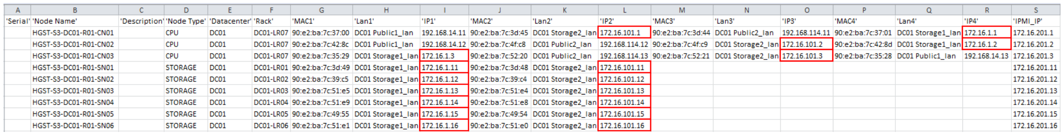


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
'Serial'	'Node Name'	'Description'	'Node Type'	'Datacenter'	'Rack'	'MAC1'	'Lan1'	'IP1'	'MAC2'	'Lan2'	'IP2'	'MAC3'	'Lan3'	'IP3'	'MAC4'	'Lan4'	'IP4'	'IPMI_IP'
	HGST-S3-DC01-R01-CN01		CPU	DC01	DC01-LR07	90:e2:ba:7c:37:00	DC01 Public1_lan	192.168.14.11	90:e2:ba:7c:3d:45	DC01 Storage2_lan	172.16.101.1	90:e2:ba:7c:3d:44	DC01 Public2_lan	192.168.114.11	90:e2:ba:7c:37:01	DC01 Storage1_lan	172.16.1.1	172.16.201.1
	HGST-S3-DC01-R01-CN02		CPU	DC01	DC01-LR07	90:e2:ba:7c:42:8c	DC01 Public1_lan	192.168.14.12	90:e2:ba:7c:4f:c8	DC01 Public2_lan	192.168.114.12	90:e2:ba:7c:4f:c9	DC01 Storage2_lan	172.16.101.2	90:e2:ba:7c:42:8d	DC01 Storage1_lan	172.16.1.2	172.16.201.2
	HGST-S3-DC01-R01-CN03		CPU	DC01	DC01-LR07	90:e2:ba:7c:35:29	DC01 Storage1_lan	172.16.1.3	90:e2:ba:7c:52:20	DC01 Public2_lan	192.168.114.13	90:e2:ba:7c:52:21	DC01 Storage2_lan	172.16.101.3	90:e2:ba:7c:35:28	DC01 Public1_lan	192.168.14.13	172.16.201.3
	HGST-S3-DC01-R01-SN01		STORAGE	DC01	DC01-LR01	90:e2:ba:7c:3d:49	DC01 Storage1_lan	172.16.1.11	90:e2:ba:7c:3d:48	DC01 Storage2_lan	172.16.101.11							172.16.201.11
	HGST-S3-DC01-R01-SN02		STORAGE	DC01	DC01-LR02	90:e2:ba:7c:39:c5	DC01 Storage1_lan	172.16.1.12	90:e2:ba:7c:39:c4	DC01 Storage2_lan	172.16.101.12							172.16.201.12
	HGST-S3-DC01-R01-SN03		STORAGE	DC01	DC01-LR03	90:e2:ba:7c:51:e5	DC01 Storage1_lan	172.16.1.13	90:e2:ba:7c:51:e4	DC01 Storage2_lan	172.16.101.13							172.16.201.13
	HGST-S3-DC01-R01-SN04		STORAGE	DC01	DC01-LR04	90:e2:ba:7c:51:e9	DC01 Storage1_lan	172.16.1.14	90:e2:ba:7c:51:e8	DC01 Storage2_lan	172.16.101.14							172.16.201.14
	HGST-S3-DC01-R01-SN05		STORAGE	DC01	DC01-LR05	90:e2:ba:7c:49:55	DC01 Storage1_lan	172.16.1.15	90:e2:ba:7c:49:54	DC01 Storage2_lan	172.16.101.15							172.16.201.15
	HGST-S3-DC01-R01-SN06		STORAGE	DC01	DC01-LR06	90:e2:ba:7c:51:e1	DC01 Storage1_lan	172.16.1.16	90:e2:ba:7c:51:e0	DC01 Storage2_lan	172.16.101.16							172.16.201.16

6. Update the private IP assignments to match the rack's public IPs based which number physical rack is being added.

Use the included rack IP guide to determine which "private" IP addresses should be assigned to each system. Use the `Left IPs` for "DC01 Storage1_lan". Use the `Right IPs` for the "DC01 Storage2_lan".

Figure 17: CSV File, Private IP Assignments

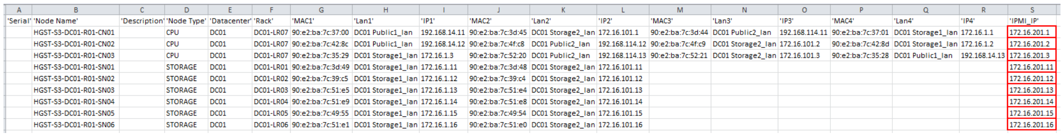


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
'Serial'	'Node Name'	'Description'	'Node Type'	'Datacenter'	'Rack'	'MAC1'	'Lan1'	'IP1'	'MAC2'	'Lan2'	'IP2'	'MAC3'	'Lan3'	'IP3'	'MAC4'	'Lan4'	'IP4'	'IPMI_IP'
	HGST-S3-DC01-R01-CN01		CPU	DC01	DC01-LR07	90:e2:ba:7c:37:00	DC01 Public1_lan	192.168.14.11	90:e2:ba:7c:3d:45	DC01 Storage2_lan	172.16.101.1	90:e2:ba:7c:3d:44	DC01 Public2_lan	192.168.114.11	90:e2:ba:7c:37:01	DC01 Storage1_lan	172.16.1.1	172.16.201.1
	HGST-S3-DC01-R01-CN02		CPU	DC01	DC01-LR07	90:e2:ba:7c:42:8c	DC01 Public1_lan	192.168.14.12	90:e2:ba:7c:4f:c8	DC01 Public2_lan	192.168.114.12	90:e2:ba:7c:4f:c9	DC01 Storage2_lan	172.16.101.2	90:e2:ba:7c:42:8d	DC01 Storage1_lan	172.16.1.2	172.16.201.2
	HGST-S3-DC01-R01-CN03		CPU	DC01	DC01-LR07	90:e2:ba:7c:35:29	DC01 Storage1_lan	172.16.1.3	90:e2:ba:7c:52:20	DC01 Public2_lan	192.168.114.13	90:e2:ba:7c:52:21	DC01 Storage2_lan	172.16.101.3	90:e2:ba:7c:35:28	DC01 Public1_lan	192.168.14.13	172.16.201.3
	HGST-S3-DC01-R01-SN01		STORAGE	DC01	DC01-LR01	90:e2:ba:7c:3d:49	DC01 Storage1_lan	172.16.1.11	90:e2:ba:7c:3d:48	DC01 Storage2_lan	172.16.101.11							172.16.201.11
	HGST-S3-DC01-R01-SN02		STORAGE	DC01	DC01-LR02	90:e2:ba:7c:39:c5	DC01 Storage1_lan	172.16.1.12	90:e2:ba:7c:39:c4	DC01 Storage2_lan	172.16.101.12							172.16.201.12
	HGST-S3-DC01-R01-SN03		STORAGE	DC01	DC01-LR03	90:e2:ba:7c:51:e5	DC01 Storage1_lan	172.16.1.13	90:e2:ba:7c:51:e4	DC01 Storage2_lan	172.16.101.13							172.16.201.13
	HGST-S3-DC01-R01-SN04		STORAGE	DC01	DC01-LR04	90:e2:ba:7c:51:e9	DC01 Storage1_lan	172.16.1.14	90:e2:ba:7c:51:e8	DC01 Storage2_lan	172.16.101.14							172.16.201.14
	HGST-S3-DC01-R01-SN05		STORAGE	DC01	DC01-LR05	90:e2:ba:7c:49:55	DC01 Storage1_lan	172.16.1.15	90:e2:ba:7c:49:54	DC01 Storage2_lan	172.16.101.15							172.16.201.15
	HGST-S3-DC01-R01-SN06		STORAGE	DC01	DC01-LR06	90:e2:ba:7c:51:e1	DC01 Storage1_lan	172.16.1.16	90:e2:ba:7c:51:e0	DC01 Storage2_lan	172.16.101.16							172.16.201.16

7. Update the IPMI IP assignments to match the rack's IPMI IPs based upon which number physical rack is being added.

Use the included rack IP guide to determine which "private" IP addresses should be assigned to each system. Use the "IPMI" IP's for the column "IPMI_IP".

Figure 18: CSV File, IPMI IP Assignments



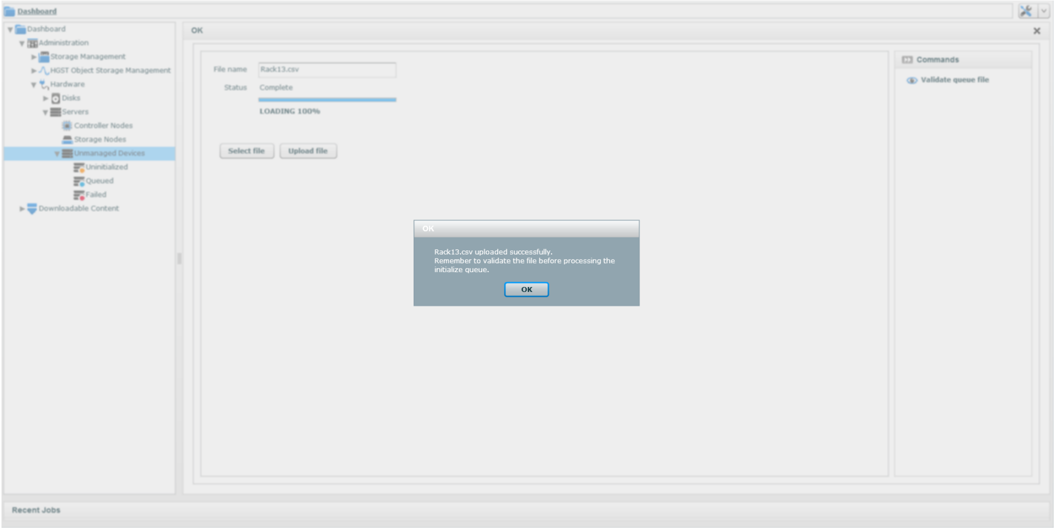
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
'Serial'	'Node Name'	'Description'	'Node Type'	'Datacenter'	'Rack'	'MAC1'	'Lan1'	'IP1'	'MAC2'	'Lan2'	'IP2'	'MAC3'	'Lan3'	'IP3'	'MAC4'	'Lan4'	'IP4'	'IPMI_IP'
	HGST-S3-DC01-R01-CN01		CPU	DC01	DC01-LR07	90:e2:ba:7c:37:00	DC01 Public1_lan	192.168.14.11	90:e2:ba:7c:3d:45	DC01 Storage2_lan	172.16.101.1	90:e2:ba:7c:3d:44	DC01 Public2_lan	192.168.114.11	90:e2:ba:7c:37:01	DC01 Storage1_lan	172.16.1.1	172.16.201.1
	HGST-S3-DC01-R01-CN02		CPU	DC01	DC01-LR07	90:e2:ba:7c:42:8c	DC01 Public1_lan	192.168.14.12	90:e2:ba:7c:4f:c8	DC01 Public2_lan	192.168.114.12	90:e2:ba:7c:4f:c9	DC01 Storage2_lan	172.16.101.2	90:e2:ba:7c:42:8d	DC01 Storage1_lan	172.16.1.2	172.16.201.2
	HGST-S3-DC01-R01-CN03		CPU	DC01	DC01-LR07	90:e2:ba:7c:35:29	DC01 Storage1_lan	172.16.1.3	90:e2:ba:7c:52:20	DC01 Public2_lan	192.168.114.13	90:e2:ba:7c:52:21	DC01 Storage2_lan	172.16.101.3	90:e2:ba:7c:35:28	DC01 Public1_lan	192.168.14.13	172.16.201.3
	HGST-S3-DC01-R01-SN01		STORAGE	DC01	DC01-LR01	90:e2:ba:7c:3d:49	DC01 Storage1_lan	172.16.1.11	90:e2:ba:7c:3d:48	DC01 Storage2_lan	172.16.101.11							172.16.201.11
	HGST-S3-DC01-R01-SN02		STORAGE	DC01	DC01-LR02	90:e2:ba:7c:39:c5	DC01 Storage1_lan	172.16.1.12	90:e2:ba:7c:39:c4	DC01 Storage2_lan	172.16.101.12							172.16.201.12
	HGST-S3-DC01-R01-SN03		STORAGE	DC01	DC01-LR03	90:e2:ba:7c:51:e5	DC01 Storage1_lan	172.16.1.13	90:e2:ba:7c:51:e4	DC01 Storage2_lan	172.16.101.13							172.16.201.13
	HGST-S3-DC01-R01-SN04		STORAGE	DC01	DC01-LR04	90:e2:ba:7c:51:e9	DC01 Storage1_lan	172.16.1.14	90:e2:ba:7c:51:e8	DC01 Storage2_lan	172.16.101.14							172.16.201.14
	HGST-S3-DC01-R01-SN05		STORAGE	DC01	DC01-LR05	90:e2:ba:7c:49:55	DC01 Storage1_lan	172.16.1.15	90:e2:ba:7c:49:54	DC01 Storage2_lan	172.16.101.15							172.16.201.15
	HGST-S3-DC01-R01-SN06		STORAGE	DC01	DC01-LR06	90:e2:ba:7c:51:e1	DC01 Storage1_lan	172.16.1.16	90:e2:ba:7c:51:e0	DC01 Storage2_lan	172.16.101.16							172.16.201.16

8. Create a job on the initialization queue.

a) In the CMC, browse to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Unmanaged Devices**.

b) Click **Select file** and choose your modified CSV.

Figure 19: Creating a Job in the Initialization Queue in the CMC



File name: Rack13.csv

Status: Complete

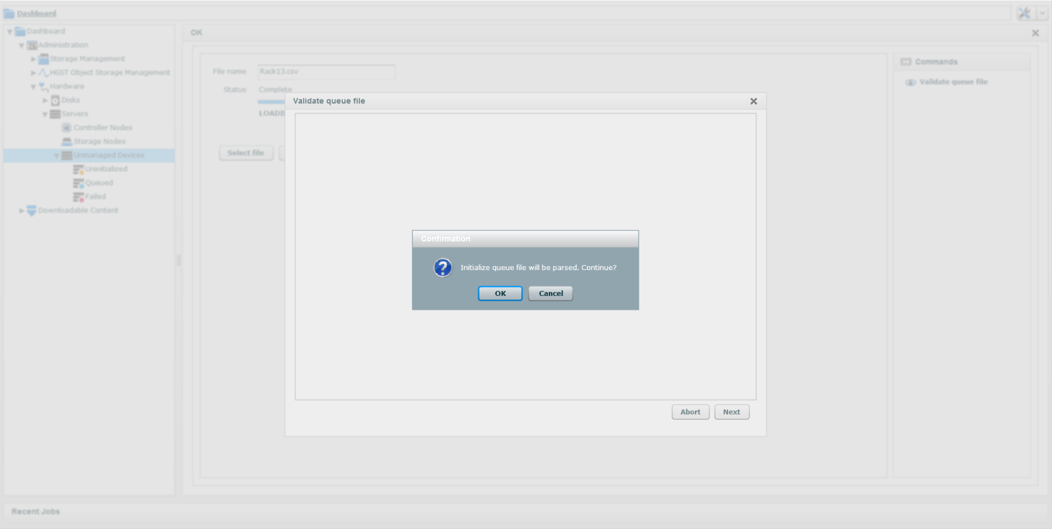
LOADING 100%

Rack13.csv uploaded successfully.
Remember to validate the file before processing the initialize queue.

c) Click **Upload queue**.

d) Click **Validate queue file** (CSV file).

Figure 20: Verifying the CSV File in the CMC



File name: Rack13.csv

Status: Complete

Validate queue file

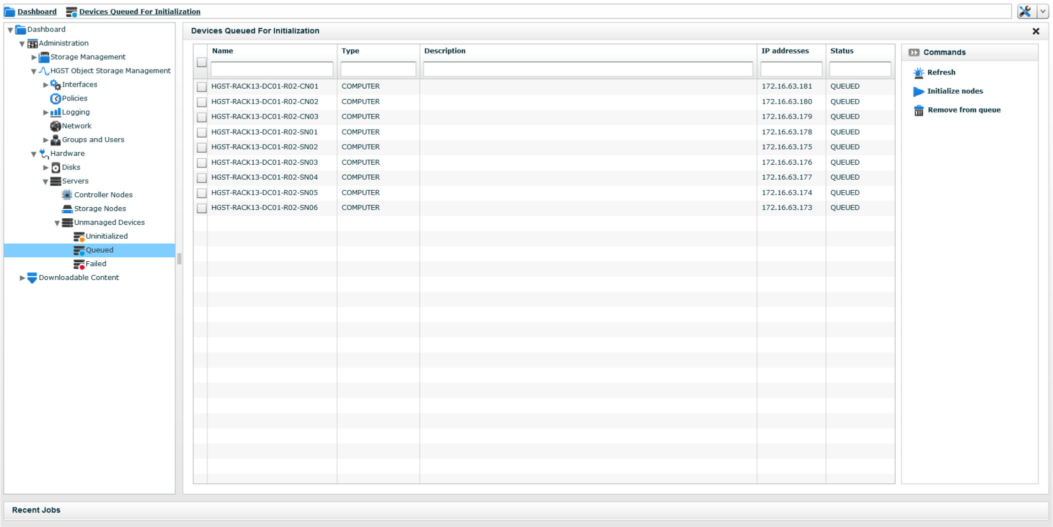
Confirmation

Initialize queue file will be parsed. Continue?

9. Start the processing of the initialization queue.

a) In the CMC, browse to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Unmanaged Devices** > **Queued**.

Figure 21: Devices Queued for Initialization in the CMC

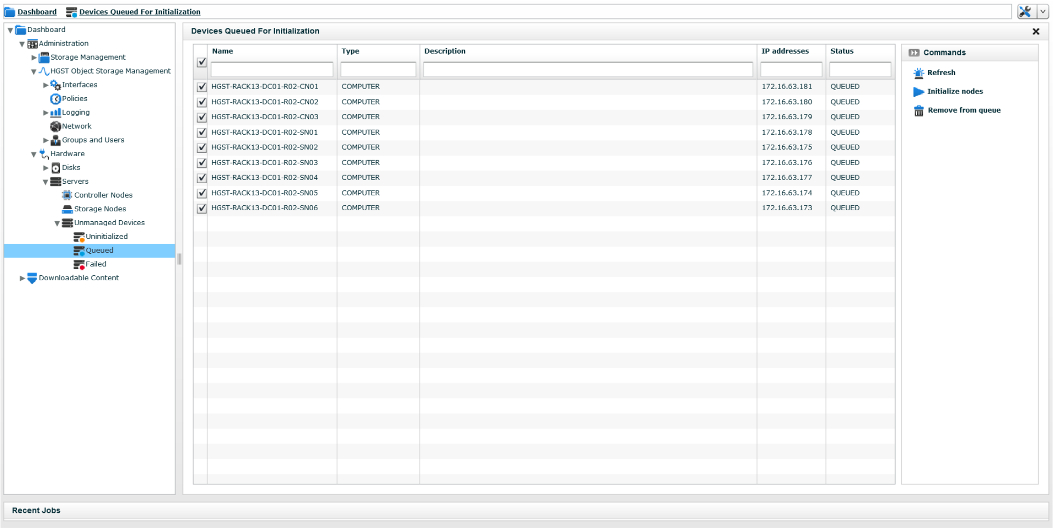


Devices Queued For Initialization

Name	Type	Description	IP addresses	Status
HGST-RACK13-DC01-R02-CN01	COMPUTER		172.16.63.181	QUEUED
HGST-RACK13-DC01-R02-CN02	COMPUTER		172.16.63.180	QUEUED
HGST-RACK13-DC01-R02-CN03	COMPUTER		172.16.63.179	QUEUED
HGST-RACK13-DC01-R02-SN01	COMPUTER		172.16.63.178	QUEUED
HGST-RACK13-DC01-R02-SN02	COMPUTER		172.16.63.175	QUEUED
HGST-RACK13-DC01-R02-SN03	COMPUTER		172.16.63.176	QUEUED
HGST-RACK13-DC01-R02-SN04	COMPUTER		172.16.63.177	QUEUED
HGST-RACK13-DC01-R02-SN05	COMPUTER		172.16.63.174	QUEUED
HGST-RACK13-DC01-R02-SN06	COMPUTER		172.16.63.173	QUEUED

b) Select the check boxes next to all nine queued servers.

Figure 22: Selecting the Nodes to Add to the Initialization Queue in the CMC

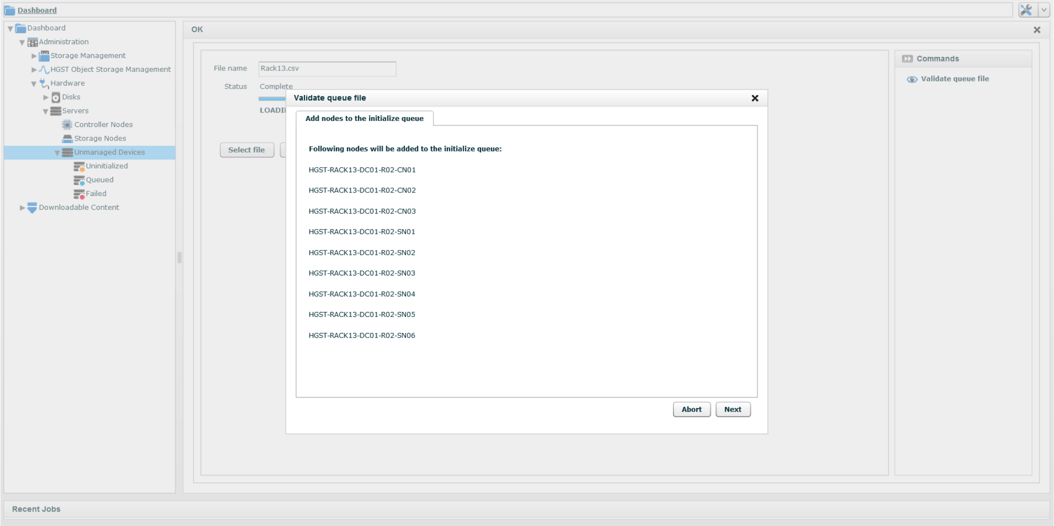


Devices Queued For Initialization

☑	Name	Type	Description	IP addresses	Status
☑	HGST-RACK13-DC01-R02-CN01	COMPUTER		172.16.63.181	QUEUED
☑	HGST-RACK13-DC01-R02-CN02	COMPUTER		172.16.63.180	QUEUED
☑	HGST-RACK13-DC01-R02-CN03	COMPUTER		172.16.63.179	QUEUED
☑	HGST-RACK13-DC01-R02-SN01	COMPUTER		172.16.63.178	QUEUED
☑	HGST-RACK13-DC01-R02-SN02	COMPUTER		172.16.63.175	QUEUED
☑	HGST-RACK13-DC01-R02-SN03	COMPUTER		172.16.63.176	QUEUED
☑	HGST-RACK13-DC01-R02-SN04	COMPUTER		172.16.63.177	QUEUED
☑	HGST-RACK13-DC01-R02-SN05	COMPUTER		172.16.63.174	QUEUED
☑	HGST-RACK13-DC01-R02-SN06	COMPUTER		172.16.63.173	QUEUED

c) Click **Initialize nodes** in the right side **Commands** pane.

Figure 23: Starting the Initialization Queue in the CMC



File name Rack13.csv

Status Complete

Validate queue file

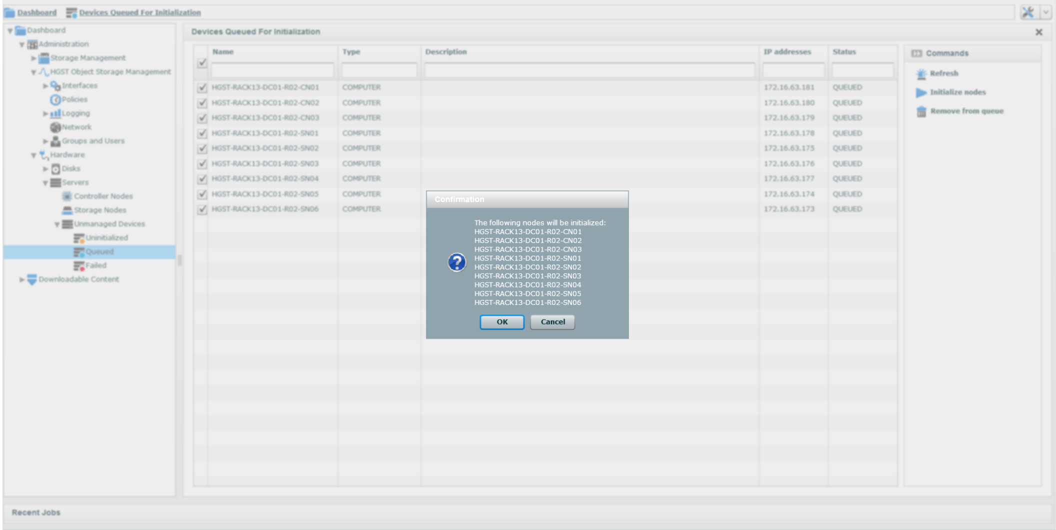
Add nodes to the initialize queue

Following nodes will be added to the initialize queue:

HGST-RACK13-DC01-R02-CN01
HGST-RACK13-DC01-R02-CN02
HGST-RACK13-DC01-R02-CN03
HGST-RACK13-DC01-R02-SN01
HGST-RACK13-DC01-R02-SN02
HGST-RACK13-DC01-R02-SN03
HGST-RACK13-DC01-R02-SN04
HGST-RACK13-DC01-R02-SN05
HGST-RACK13-DC01-R02-SN06

Abort Next

Figure 24: Confirming the Initialization Queue in the CMC



Devices Queued For Initialization

☑	Name	Type	Description	IP addresses	Status
☑	HGST-RACK13-DC01-R02-CN01	COMPUTER		172.16.63.181	QUEUED
☑	HGST-RACK13-DC01-R02-CN02	COMPUTER		172.16.63.180	QUEUED
☑	HGST-RACK13-DC01-R02-CN03	COMPUTER		172.16.63.179	QUEUED
☑	HGST-RACK13-DC01-R02-SN01	COMPUTER		172.16.63.178	QUEUED
☑	HGST-RACK13-DC01-R02-SN02	COMPUTER		172.16.63.175	QUEUED
☑	HGST-RACK13-DC01-R02-SN03	COMPUTER		172.16.63.176	QUEUED
☑	HGST-RACK13-DC01-R02-SN04	COMPUTER		172.16.63.177	QUEUED
☑	HGST-RACK13-DC01-R02-SN05	COMPUTER		172.16.63.174	QUEUED
☑	HGST-RACK13-DC01-R02-SN06	COMPUTER		172.16.63.173	QUEUED

Confirmation

The following nodes will be initialized:
HGST-RACK13-DC01-R02-CN01
HGST-RACK13-DC01-R02-CN02
HGST-RACK13-DC01-R02-CN03
HGST-RACK13-DC01-R02-SN01
HGST-RACK13-DC01-R02-SN02
HGST-RACK13-DC01-R02-SN03
HGST-RACK13-DC01-R02-SN04
HGST-RACK13-DC01-R02-SN05
HGST-RACK13-DC01-R02-SN06

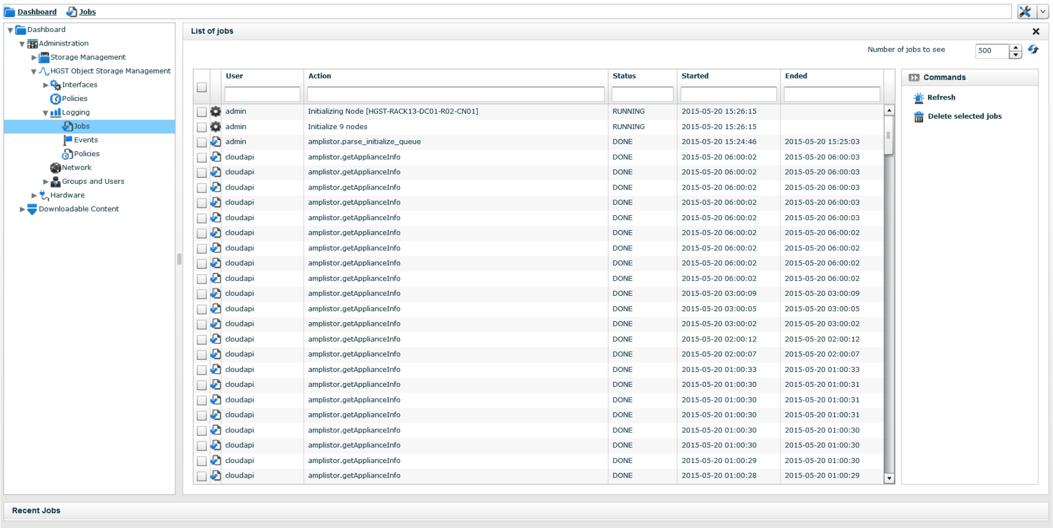
OK Cancel

10. In the CMC, browse to **Dashboard** > **Administration** > **HGST Object Storage Management** > **Management** > **Logging** > **Jobs** and monitor the status of the initialization jobs.

Note: Initialization takes about 10 hours.

When an initialization job is done, its **Status** field has a blue check mark and the text **Done** as shown below.

Figure 25: Job Status in the CMC



	User	Action	Status	Started	Ended
□	admin	Initializing Node [HGST-RACK13-DC01-R02-CN01]	RUNNING	2015-05-20 15:26:15	
□	admin	Initialize 9 nodes	RUNNING	2015-05-20 15:26:15	
□	admin	amplistor.parse_initialize_queue	DONE	2015-05-20 15:24:46	2015-05-20 15:25:03
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:03
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:03
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:03
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:03
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:03
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:02
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:02
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:02
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 06:00:02	2015-05-20 06:00:02
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 03:00:09	2015-05-20 03:00:09
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 03:00:05	2015-05-20 03:00:05
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 03:00:02	2015-05-20 03:00:02
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 02:00:12	2015-05-20 02:00:12
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 02:00:07	2015-05-20 02:00:07
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:33	2015-05-20 01:00:33
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:30	2015-05-20 01:00:31
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:30	2015-05-20 01:00:31
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:30	2015-05-20 01:00:31
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:30	2015-05-20 01:00:30
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:30	2015-05-20 01:00:30
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:29	2015-05-20 01:00:30
□	cloudapi	amplistor.getApplianceInfo	DONE	2015-05-20 01:00:28	2015-05-20 01:00:29

Figure 26: Controller Nodes After Initialization

Figure 27: Storage Nodes After Initialization

7.7 Configuring the System

Edit the `post_install.ini` file on the Management Node to include additional MetaStores as follows.

1. Open an SSH session to the Management Node of the primary management rack.
   The OSMI menu appears.
2. Exit the OSMI menu.
3. Open the file `/opt/unattended_install/post_install/conf/post_install.ini`.
4. At the bottom of the file, add four new sections for the MetaStores, with the following caveats:
   a) Increment the suffix on each section label (`metastore`*N*).

      For example, when adding a second rack, the section labels must be `metastore5`, `metastore6`, `metastore7`, and `metastore8` respectively.

   b) Increment the suffix on each value of `name` (`objects`*N*).

      For example, when adding a second rack, the values of `name` must be `objects5`, `objects6`, `objects7`, and `objects8` respectively.

   c) Copy the same values for `size` and `allocation` from `[metastore1]` to `[metastore5]`, `[metastore2]` to `[metastore6]`, from `[metastore3]` to `[metastore7]`, and from `[metastore4]` to `[metastore8]`.

      Note: Your values for `size` and `allocation` may differ from the example below.

      For example,

```
[metastore1]
name=objects1
size=156000
```

```
allocation=AUTO
spread=HGST-S3-DC01-R01-CN01|DC01-LR07|DC01|ata3||HGST-S3-DC01-R01-CN02|DC01-LR07|
DC01|ata3||HGST-S3-DC01-R01-CN03|DC01-LR07|DC01|ata3
...
[metastore5]
name=objects5
size=156000
allocation=AUTO
spread=MY-PRIVATE-CLOUD-DC01-R02-CN01|DC01-LR07|DC01|ata3||MY-PRIVATE-CLOUD-DC01-
R02-CN02|DC01-LR07|DC01|ata3||MY-PRIVATE-CLOUD-DC01-R02-CN03|DC01-LR07|DC01|ata3
```

d) Change each value of `spread` in your new `[metastore`*`N`*`]` sections as follows:

- Replace `HGST-S3` with the hostname as shown in the Linux prompt on the Management Node. (The hostname is the part of the prompt before `-DC01`).
- Replace `R01` with the physical rack number that is being added. For example, if this is your second rack, replace `R01` with `R02`.

  For example,

  ```
  spread=MY-PRIVATE-CLOUD-DC01-R02-CN01|DC01-LR07|DC01|ata6||MY-PRIVATE-CLOUD-
  DC01-R02-CN02|DC01-LR07|DC01|ata6||MY-PRIVATE-CLOUD-DC01-R02-CN03|DC01-LR07|
  DC01|ata6
  ```

Your final `post_install.ini` should now look like this (when adding a second rack):

```
[metastore1]
name=objects1
size=156000
allocation=AUTO
spread=HGST-S3-DC01-R01-CN01|DC01-LR07|DC01|ata3||HGST-S3-DC01-R01-CN02|DC01-LR07|
DC01|ata3||HGST-S3-DC01-R01-CN03|DC01-LR07|DC01|ata3
[metastore2]
name=objects2
size=204500
allocation=AUTO
spread=HGST-S3-DC01-R01-CN01|DC01-LR07|DC01|ata4||HGST-S3-DC01-R01-CN02|DC01-LR07|
DC01|ata4||HGST-S3-DC01-R01-CN03|DC01-LR07|DC01|ata4
[metastore3]
name=objects3
size=204500
allocation=AUTO
spread=HGST-S3-DC01-R01-CN01|DC01-LR07|DC01|ata5||HGST-S3-DC01-R01-CN02|DC01-LR07|
DC01|ata5||HGST-S3-DC01-R01-CN03|DC01-LR07|DC01|ata5
[metastore4]
name=objects4
size=204500
allocation=AUTO
spread=HGST-S3-DC01-R01-CN01|DC01-LR07|DC01|ata6||HGST-S3-DC01-R01-CN02|DC01-LR07|
DC01|ata6||HGST-S3-DC01-R01-CN03|DC01-LR07|DC01|ata6
[metastore5]
name=objects5
size=156000
allocation=AUTO
spread=MY-PRIVATE-CLOUD-DC01-R02-CN01|DC01-LR07|DC01|ata3||MY-PRIVATE-CLOUD-DC01-
R02-CN02|DC01-LR07|DC01|ata3||MY-PRIVATE-CLOUD-DC01-R02-CN03|DC01-LR07|DC01|ata3
[metastore6]
name=objects6
size=204500
allocation=AUTO
spread=MY-PRIVATE-CLOUD-DC01-R02-CN01|DC01-LR07|DC01|ata4||MY-PRIVATE-CLOUD-DC01-
R02-CN02|DC01-LR07|DC01|ata4||MY-PRIVATE-CLOUD-DC01-R02-CN03|DC01-LR07|DC01|ata4
```

```
[metastore7]
name=objects7
size=204500
allocation=AUTO
spread=MY-PRIVATE-CLOUD-DC01-R02-CN01|DC01-LR07|DC01|ata5||MY-PRIVATE-CLOUD-DC01-
R02-CN02|DC01-LR07|DC01|ata5||MY-PRIVATE-CLOUD-DC01-R02-CN03|DC01-LR07|DC01|ata5
[metastore8]
name=objects8
size=204500
allocation=AUTO
spread=MY-PRIVATE-CLOUD-DC01-R02-CN01|DC01-LR07|DC01|ata6||MY-PRIVATE-CLOUD-DC01-
R02-CN02|DC01-LR07|DC01|ata6||MY-PRIVATE-CLOUD-DC01-R02-CN03|DC01-LR07|DC01|ata6
```

5. At the top of the file, replace the word `True` with `False` in the following lines, if it is not already done.

```
SET_CMC_PASSWORD = False
CHANGE_MGMT_HOST_NAME = False
EXTEND_SYSTEM_METASTORES = False
SET_ROOT_PASSWORD = False
CREATE_DEFAULT_POLICY = False
CONFIGURE_S3 = False
WRITE_CONFIG_WIZARD_STARTUP_SCRIPT = False
CONFIGURE_PHONE_HOME = False
UPDATE_MPT3SAS = False
```

6. Save and close the file.
7. Run the post-install script using the following command.
   Replace *`machine_name`* with the hostname as shown in the Linux prompt on the Management Node.

```
/opt/qbase3/bin/python /opt/unattended_install/post_install/post_install.py \
--hostname "machine_name" --config /opt/unattended_install/post_install/conf/
post_install.ini
```

7.8 Configuring Telemetry Collection

The telemetry collection feature automatically installs itself on new nodes, but you must mount the directory it needs on all nodes in the new rack. To do this, proceed as follows.

1. Get the IP addresses for all Controller and Storage Nodes in the new rack.
   a) Log into the CMC.
   b) Navigate to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Controller Nodes**
   c) Write down the IP address for each Controller Node.
   d) Navigate to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Storage Nodes**
   e) Write down the IP address for each Storage Node.
   f) Log out of the CMC.
2. Open an SSH session to the Management Node, and exit the OSMI menu.
3. At the Linux prompt on the Management Node, do the following:
   a) Force the telemetry collection to scan for new nodes:

```
/opt/hawk/callhome/callhome.py --upgrade
```

   b) Open an SSH session to Controller Node 2 using the IP address you obtained for it from the CMC in step 1.
   The OSMI menu appears.
   c) Exit the OSMI menu.
   The Linux prompt appears.

d) At the Linux prompt, run the following command:

```
sudo mount /mnt/hawk
```

e) Exit the SSH session to Controller Node 2.

4. Repeat step 3 for Controller Node 3 and Storage Nodes 1-6.
5. Exit the SSH session to the Management Node.

7.9 Installing Hugo

You must install Hugo on all the Storage Nodes of the new rack.

1. Download the Hugo `.deb` package from the HGST customer support portal, and transfer the Hugo `.deb` package to all Storage Nodes of the new rack.
   a) Log into the CMC.
   b) Navigate to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Storage Nodes**
   c) Write down the IP address for each Storage Node.
   d) Log out of the CMC.
   e) Download the Hugo .deb package from the HGST customer support portal.
   f) Using `scp`, transfer the Hugo .deb package to the Management Node.
   g) Open an SSH session to the Management Node, and exit the OSMI menu.
   h) At the Linux prompt, use `scp` to transfer the Hugo `.deb` package to Storage Nodes 1-6 of the new rack, `/root` directory, (one at a time).
2. At the Linux prompt on the Management Node, do the following:
   a) Open an SSH session to Storage Node 1.
   b) Add the following lines at the end of the file `~/.bashrc`:

```
# HUGO env variable
HGST_LICENSE_ACCEPTED=1
export HGST_LICENSE_ACCEPTED
```

   c) Save the file.
   d) Run the following command:

```
source ~/.bashrc
```

   e) Run the following command to install Hugo:

```
dpkg -i Hugo_version
```

   f) Verify that Hugo is installed:

```
hugo v
```

   This command returns the version of Hugo that is installed.
3. Repeat step 2 for Storage Nodes 2-6.

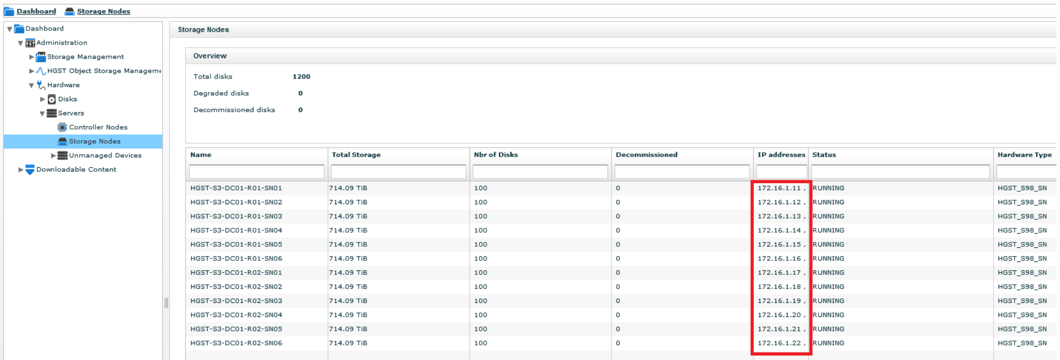
7.10 Setting Queue Depth

After you add a rack to the Active Archive System, you must check that the `max_queue_depth` setting on all drives in all Storage Enclosure Basic arrays is set to 128, and update it if not.

1. Log into the CMC.
2. Navigate to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Storage Nodes**

3. Write down the IP address for each Storage Node.

Figure 28: IP Addresses of Storage Nodes



Total disks	1200
Degraded disks	0
Decommissioned disks	0

Name	Total Storage	Nbr of Disks	Decommissioned	IP addresses	Status	Hardware Type
HGST-S3-DC01-R01-SN01	714.09 TiB	100	0	172.16.1.11 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R01-SN02	714.09 TiB	100	0	172.16.1.12 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R01-SN03	714.09 TiB	100	0	172.16.1.13 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R01-SN04	714.09 TiB	100	0	172.16.1.14 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R01-SN05	714.09 TiB	100	0	172.16.1.15 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R01-SN06	714.09 TiB	100	0	172.16.1.16 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R02-SN01	714.09 TiB	100	0	172.16.1.17 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R02-SN02	714.09 TiB	100	0	172.16.1.18 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R02-SN03	714.09 TiB	100	0	172.16.1.19 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R02-SN04	714.09 TiB	100	0	172.16.1.20 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R02-SN05	714.09 TiB	100	0	172.16.1.21 ,	RUNNING	HGST_S98_SN
HGST-S3-DC01-R02-SN06	714.09 TiB	100	0	172.16.1.22 ,	RUNNING	HGST_S98_SN

4. At the Linux prompt on the Management Node, do the following:

a) Open an SSH session to Storage Node 1.

b) Check the queue depth of all the drives connected to this Storage Node by executing the following command:

```
cat /sys/block/*/device/queue_depth|sort|uniq -c
```

For example,

```
root@HGST-S3-DC01-R01-SN01:~#  cat /sys/block/*/device/queue_depth|sort|uniq
 -c
     98 254
      2 31
```

The sample output above indicates that there are 98 drives with queue_depth of `254`, and 2 drives with queue_depth of `31`.

c) If the queue depth of any drive is not `128`:
Create the file `/etc/modprobe.d/mpt3sas.conf` with the following text:

```
options mpt3sas max_queue_depth=128
```

The run the following commands at the Linux prompt:

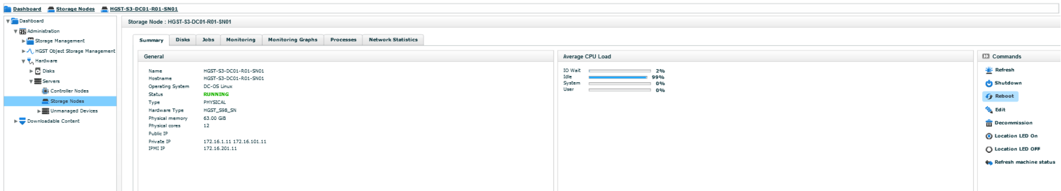
```
depmod -a
update-initramfs -u
```

d) Reboot the Storage Node from the CMC.

Navigate to **Dashboard** > **Administration** > **Hardware** > **Servers** > **Storage Nodes**, and click **Reboot**.

> **Important:** You **must wait** until the CMC indicates that the Storage Node is fully up (the **Status** field is **RUNNING**) and the **Disk Safety** on the CMC dashboard is **5**.

Figure 29: IP Addresses of Storage Nodes



Name	HGST-S3-DC01-R01-SN01
Hostname	HGST-S3-DC01-R01-SN01
Operating System	DC-OS Linux
Status	RUNNING
Type	PHYSICAL
Hardware Type	HGST_S98_SN
Physical memory	63.00 GiB
Physical cores	12
Public IP	
Private IP	172.16.1.11 172.16.101.11
IPMI IP	172.16.201.11

5. Repeat step 4 for Storage Nodes 2-6.

7.11 Running Post Validation Checks

After you add a rack to the Active Archive System, you must do some post validation steps.

Prerequisites

- The new rack must be fully configured with all the required software installed, system configurations done, and relevant cabling connecting it to the primary management rack.
- The `hgst_configuration_diff.py` script must be run on the primary management rack's Management Node.

> **Warning:** The following post validation steps must succeed before declaring full functionality of the added rack. Failure to follow these steps could result in data center failure.

1. Using `scp`, transfer the script `hgst_configuration_diff.py` from your laptop to the Management Node.
2. Navigate to the destination directory where the script was transferred to, and make the script executable.

```
chmod +x hgst_configuration_diff.py
```

3. Run `hgst_configuration_diff.py --factory` on the Management Node.

```
./hgst_configuration_diff.py --factory
```

This command creates two new system configuration files:

/opt/qbase3/utils/factory_config_settings.pickle

System configuration file with current machine settings in machine readable format

/opt/qbase3/utils/factory_config_settings.txt

System configuration file with current machine settings in human readable format

4. Log into all Controller Nodes to verify that these two configuration files have been copied to each node under `/opt/qbase3/utils`.
5. Run `hgst_configuration_diff.py --altconfig` on the Management Node to create a working copy of the current configuration.

```
./hgst_configuration_diff.py --altconfig newfilename_with_timestamp
```

This command generates two files:

/opt/qbase3/utils/*newfilename_with_timestamp*.pickle

System configuration file with current machine settings in machine readable format

/opt/qbase3/utils/*newfilename_with_timestamp*.txt

System configuration file with current machine settings in human readable format

6. Run `hgst_configuration_diff.py --config` on the Management Node to compare the pickle file from step 3 to the pickle file from the previous step.

```
./hgst_configuration_diff.py \
--config /opt/qbase3/utils/factory_config_settings.pickle\
--compare /opt/qbase3/utils/newfilename_with_timestamp.pickle
```

This is a sanity check to verify that there are no differences in the two configuration files.

7.12 Rechecking System Health

Recheck system health to ensure that all the components are working.

1. Run hgst_health_check.py on the new expanded system.

   ```
   python hgst_health_check.py
   ```

   This runs for about 15 minutes and displays its progress. Upon completion, hgst_health_check.py generates a log file, hgst_healthcheck.log, with all the information it displayed onscreen. If it finds errors, it prints the details about the errors and also provides instructions for an interactive shell.

   Important: If hgst_health_check.py reports any errors, contact HGST support.

2. Save the files generated by hgst_health_check.py.

Index