Elastic Storage Server
Version 5.1

Quick Deployment Guide

SC27-8580-08

Elastic Storage Server
Version 5.1

Quick Deployment Guide

SC27-8580-08

Note
Before using this information and the product it supports, read the information in "Notices" on page 63.

This edition applies to version 5.x of the Elastic Storage Server (ESS) for Power, and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments; see the topic "How to submit your comments" on page viii. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Tables

About this information

This information guides you in quickly installing, or upgrading to, version 5.x of the Elastic Storage Server (ESS).

For detailed ESS installation and upgrade information, see *Deploying the Elastic Storage Server*.

Who should read this information

This information is intended for experienced system installers and upgraders who are familiar with ESS systems.

Prerequisite and related information

ESS information

The ESS 5.1 library consists of these information units:

- *Deploying the Elastic Storage Server*, SC27-6659
- *Elastic Storage Server: Quick Deployment Guide*, SC27-8580
- *Elastic Storage Server: Problem Determination Guide*, SA23-1457
- *IBM Spectrum Scale RAID: Administration*, SC27-6658
- *IBM ESS Expansion: Quick Installation Guide (Model 084)*, SC27-4627
- *IBM ESS Expansion: Installation and User Guide (Model 084)*, SC27-4628

For more information, see IBM® Knowledge Center:

http://www-01.ibm.com/support/knowledgecenter/SSYSP8_5.1.0/sts51_welcome.html

For the latest support information about IBM Spectrum Scale™ RAID, see the IBM Spectrum Scale RAID FAQ in IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSYSP8/sts_welcome.html

Related information

For information about:

- IBM Spectrum Scale, see IBM Knowledge Center:
  http://www.ibm.com/support/knowledgecenter/STXKQY/ibmspectrumscale_welcome.html
- IBM POWER8® servers, see IBM Knowledge Center:
  http://www.ibm.com/support/knowledgecenter/POWER8/p8hdx/POWER8welcome.htm
- The DCS3700 storage enclosure, see:
  - *System Storage® DCS3700 Quick Start Guide*, GA32-0960-03:
    http://www.ibm.com/support/docview.wss?uid=ssg1S7004915
  - *IBM System Storage DCS3700 Storage Subsystem and DCS3700 Storage Subsystem with Performance Module Controllers: Installation, User's, and Maintenance Guide* , GA32-0959-07:
    http://www.ibm.com/support/docview.wss?uid=ssg1S7004920
- The IBM Power Systems™ EXP24S I/O Drawer (FC 5887), see IBM Knowledge Center :
  http://www.ibm.com/support/knowledgecenter/8247-22L/p8ham/p8ham_5887_kickoff.htm
- Extreme Cluster/Cloud Administration Toolkit (xCAT), go to the xCAT website :

http://sourceforge.net/p/xcat/wiki/Main_Page/

Conventions used in this information

Table 1 describes the typographic conventions used in this information. UNIX file name conventions are used throughout this information.

Table 1. Conventions

Convention	Usage
bold	**Bold** words or characters represent system elements that you must use literally, such as commands, flags, values, and selected menu options. Depending on the context, **bold** typeface sometimes represents path names, directories, or file names.
bold underlined	**bold underlined** keywords are defaults. These take effect if you do not specify a different keyword.
`constant width`	Examples and information that the system displays appear in `constant-width` typeface. Depending on the context, `constant-width` typeface sometimes represents path names, directories, or file names.
italic	*Italic* words or characters represent variable values that you must supply. *Italics* are also used for information unit titles, for the first use of a glossary term, and for general emphasis in text.
<*key*>	Angle brackets (less-than and greater-than) enclose the name of a key on the keyboard. For example, **<Enter>** refers to the key on your terminal or workstation that is labeled with the word *Enter*.

\	In command examples, a backslash indicates that the command or coding example continues on the next line. For example:
	`mkcondition -r IBM.FileSystem -e "PercentTotUsed > 90" \`
	`-E "PercentTotUsed < 85" -m p "FileSystem space used"`

{*item*}	Braces enclose a list from which you must choose an item in format and syntax descriptions.
[*item*]	Brackets enclose optional items in format and syntax descriptions.
<**Ctrl-***x*>	The notation <**Ctrl-***x*> indicates a control character sequence. For example, <**Ctrl-c**> means that you hold down the control key while pressing <**c**>.
item...	Ellipses indicate that you can repeat the preceding item one or more times.
|	In *synopsis* statements, vertical lines separate a list of choices. In other words, a vertical line means *Or*. In the left margin of the document, vertical lines indicate technical changes to the information.

How to submit your comments

Your feedback is important in helping us to produce accurate, high-quality information. You can add comments about this information in IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSYSP8/sts_welcome.html

To contact the IBM Spectrum Scale development organization, send your comments to the following email address:

scale@us.ibm.com

Chapter 1. Deploying the Elastic Storage Server - for experienced users

This topic includes a concise set of deployment instructions for those who are familiar with Elastic Storage Server (ESS) systems.

In these instructions:

- All version numbers shown are examples. The version depends on the release and edition that is being deployed.
- All package names shown are examples. The package name depends on the architecture of the node and the edition that is being deployed.
- Node names `ems1`, `gssio1`, and `gssio2` are examples. Each environment could have its own unique naming conventions.

Follow these high-level steps:

1. Complete the prerequisite tasks.
2. Unpack the ESS install/upgrade software from FixCentral at http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%2Bdefined%2Bstorage&product=ibm/StorageSoftware/IBM+Spectrum+Scale+RAID&release=All&platform=All&function=all
3. Obtain the kernel update errata, if required. Kernel Errata and other required update packages are provided in the `/home/deploy` directory of the management server node when shipped from factory. Kernel updates can be also obtained from the Red Hat support page.
4. Complete one of the following tasks:
   a. Install the ESS system.
   b. Upgrade the ESS system.

After the system is deployed and GUI is set up, the following optional tasks can be performed:

- **Set up the management server node (EMS) and deploy I/O server nodes with the ESS Installation and Deployment Toolkit**: To facilitate some steps of installation and deployment tasks, ESS release 5.x ships with the ESS Installation and Deployment Toolkit. The toolkit is a menu-driven interface that can be optionally used to set up the management server node and deploy I/O server nodes. To start the toolkit, issue the **`gssutils`** command at the command line. Refer to the **`gssutils`** man page for details.
  1. The toolkit can be used to help and simplify some of the steps; however, this document and CLI should be used as the primary installation and deployment instructions and method.
  2. The steps for installing the management server software (provided in the section titled “Install the management server software ” on page 3) must be done outside of the toolkit.
  3. Cleaning of the xCAT configuration and associated configurations (provided in step 2. of the section titled “Install the ESS system” on page 3) must be done outside of the toolkit.
  4. Review this guide to become familiar with the steps before using the toolkit.
- **Call home configuration:** Call home, through the attached HMC node, is supported for the servers in the IBM Elastic Storage™ Server (5146-GLx and 5146-GSx only). When properly enabled and configured, server platform events (power, cooling, processor, memory) are automatically reported to IBM when they reach a service action required state.

  For 5146-GLx and 5146-GSx, ESS 5.x also ships with Electronic Service Agent™, which when properly configured can provide Call home capability for drives that needs to be replaced in the attached enclosures.

Note: Errors associated with devices and adapters within the servers, or any errors associated with the expansion I/O drawers and drives are not supported in this initial release.

A Lab Based Services engagement is required to configure and initialize the call home application after installing or upgrading to ESS 5.x. Contact your IBM Sales representative to arrange this engagement.

Complete the prerequisite tasks

Complete these tasks before proceeding:

1. Ensure nodes are properly prepared for deployment.
   - The management server node and I/O server node network requirements are met with correct `/etc/hosts` entries in EMS node. Review and address the items described in Table 3 on page 35.For detailed information on network topology, see Figure 1 on page 32 and Figure 2 on page 32.
   - HMC is properly configured for the management server node and I/O server nodes and partition names are correctly set. To apply the HMC V8 update, use the following resources:
     – HMC V8 upgrade procedure: https://www-01.ibm.com/support/docview.wss?uid=nas8N1020108
     – HMC V8 860 files: ftp://public.dhe.ibm.com/software/server/hmc/network/v8860/
     – HMC V8 860 SP1 ISO: ftp://public.dhe.ibm.com/software/server/hmc/updates/HMC_Update_V8R860_SP1.iso

     After upgrading, the HMC configuration should be similar to:
     Version: 8 Build Level: 20170302.1 Serial Number: 2137FCD
     Release: 8.6.0 Base Version: V8R8.6.0 Service Pack: 1

     Note: This is not applicable for the PPC64LE platform.
   - Nodes are powered up
2. Obtain the following packages and place them under the `/home/deploy` directory.
   - The Red Hat Enterprise Linux 7.2 ISO image file (For example, `rhel-server-7.2-ppc64-dvd.iso` or `rhel-server-7.2-ppc64le-dvd.iso`) or DVD for 64-bit IBM Power Systems architecture. The ISO or DVD is used to upgrade the management server node as well as upgrade or deploy I/O server nodes.

     You can obtain these ISOs as follows:
     – For the PPC64BE ISO, go to this URL: Red Hat Enterprise Linux 7.2 ISO PPC64BE
     – For the PPC64LE ISO, do the following:
       a. Log in to the Red Hat Network website.
       b. Select **Download** > **Red Hat Enterprise Linux** > **Red Hat Enterprise Linux 7.2 Binary DVD for Little Endian**
   - The ESS software archive. For example:
     PPC64BE packages: `gss_install-5.1.1_ppc64_datamanagement_20170519T103358Z.tgz` or `gss_install-5.1.1_ppc64_standard_20170519T103358Z.tgz`
     PPC64LE packages: `gss_install-5.1.1_ppc64le_datamanagement_20170519T102516Z.tgz`or `gss_install-5.1.1_ppc64le_standard_20170519T102516Z.tgz`
     You can download these packages from FixCentral at http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%2Bdefined%2Bstorage&product=ibm/StorageSoftware/IBM+Spectrum+Scale+RAID&release=All&platform=All&function=all.
   - The required kernel update errata, if required.
   - The systemd update.

     Important: Doing the systemd update is mandatory and the systemd update must be applied to each ESS node.
     For more information, see Appendix H, “Obtaining systemd update for system upgrades,” on page 55.

- The mpt3sas driver package (`mpt3sas-13.100.00.00-1.el7_2.src.rpm`). **This is not applicable for the PPC64BE platform.**
- The system firmware update. For more information, see Appendix E, "Updating the system firmware," on page 49.

Note: The kernel errata and the mpt3sas driver packages are available in the `/home/deploy` directory by default.

3. Review the list of known issues for the ESS version you are installing.
   See Appendix A, "Known issues," on page 25 for more information.

Install the management server software

Note: The package name depends on the platform and the edition on which you are installing the software.

1. Unpack the ESS software archive:
   ```
   tar -zxvf gss_install-5.1.1_ppc64_datamanagement_20170519T103358Z.tgz
   ```
2. Check the MD5 checksum:
   ```
   md5sum -c gss_install-5.1.1_ppc64_datamanagement_20170519T103358Z.md5
   ```
3. Make sure the `/opt/ibm/gss/install` directory is clean:
   ```
   /bin/sh gss_install-5.1.1_ppc64_datamanagement_20170519T103358Z --remove
   ```
4. Extract the ESS packages and accept the license as follows. By default, it is extracted to the `/opt/ibm/gss/install` directory:
   ```
   /bin/sh gss_install-5.1.1_ppc64_datamanagement_20170519T103358Z --text-only
   ```
5. For install and deployment, see "Install the ESS system."
   To upgrade an existing ESS system, see "Upgrade the ESS system" on page 11..

Install the ESS system

Follow these steps to perform a new installation of the ESS software on a management server node and I/O server nodes. Node host names **ems1**, **gssio1**, and **gssio2** are examples. Each environment could have its own unique naming conventions. For an xCAT command such as **updatenode**, use an xCAT host name. For the IBM Spectrum Scale commands (those start with mm), use an IBM Spectrum Scale host name. For example, **ems1** is an xCAT host name (typically a hostname associated with the management interface) and **ems1-hs** is the corresponding IBM Spectrum Scale host name (typically a host name associated with the high speed interface).

1. Make the **gssdeploy** script executable:
   ```
   chmod +x /opt/ibm/gss/install/samples/gssdeploy
   ```
2. Clean the current xCAT installation and associated configuration to remove any preexisting xCAT configuration, and then address any errors before proceeding:
   ```
   /opt/ibm/gss/install/samples/gssdeploy -c
   ```
3. Run the following command:
   ```
   /opt/ibm/gss/install/installer/gssinstall -m /opt/ibm/gss/install/manifest -u
   ```
4. Copy the **gssdeploy.cfg** configuration file to the `/var/tmp` directory:
   ```
   cp /opt/ibm/gss/install/samples/gssdeploy.cfg /var/tmp
   ```

   `/var/tmp` is a sample directory name. You can specify a different directory name. Do not copy the **gssdeploy.cfg** configuration file to the `/tmp` directory because the **gssdeploy** script uses the `/tmp/gssdeploy` directory and the `/tmp` directory might get cleaned up in case of a system reboot.

5. If deploying on the **PPC64LE** platform, gather information for the `gssdeploy.cfg` configuration file using the following commands when you are in close proximity with the rack containing the nodes:
   a. Scan the nodes in the FSP subnet range:

      ```
      /var/tmp/gssdeploy -f FSP_Subnet_Range
      ```

      FSP_Subnet_Range is the FSP management node interface subnet range. For example, `10.0.0.0/24`. It is recommended to use the IP address `10.0.0.1` for the management interface, if possible.

      Note: The **gssdeploy -f** command first determines if a DHCP server is running on the network. If the DHCP sever is not running, it prompts you to start one so that the I/O server nodes can obtain addresses. Select `Y` to start the DHCP server when prompted.

      This command scans the specified subnet range to ensure that only the nodes on which you want to deploy are available. These include I/O server nodes and management server node (EMS).

      This command also returns the following:

      - Serial numbers and FSP numbers of the nodes in the building block
      - Serial numbers and IP addresses of I/O server nodes in the building block

      Note: Do not proceed to the next step until FSP IP addresses and serial numbers of all known nodes are visible using the **gssdeploy -f** script.
   b. Physically identify the nodes in the rack:

      ```
      /var/tmp/gssdeploy -i
      ```

      With the -i option, *Node_IP*, *Default_Password*, and *Duration* need to be provided as input, where:

      - *Node_IP* is the returned FSP IPMI IP address of the node obtained by using the **gssdeploy -f** command.
      - *Default_Password* is the default password of the node, which is `PASSW0RD`
      - *Duration* is the time duration in seconds for which the LED on the node should blink.

      After you issue this command, the LED blinks on the specified node for the specified duration. You can identify the node in the rack using the blinking LED.

      Depending on the order of a node in the rack, its corresponding entry is made in the `gssdeploy.cfg` file. For example, for the bottommost node in the rack, its corresponding entry is put first in `gssdeploy.cfg`.
6. Update the `gssdeploy.cfg` file according to your requirements and the gathered information.

   The options that you can specify in the `gssdeploy.cfg` file include:

   - Whether use DVD for installation: `RHEL_USE_DVD`

     The default option is to use ISO.
   - If DVD, then device location: `RHEL_DVD`
   - Mount point to use for RHEL media: `RHEL_MNT`
   - ISO location: `RHEL_ISODIR`

     The default location is `/opt/ibm/gss/iso`.
   - ISO file name: `RHEL_ISO`
   - EMS host name: `EMS_HOSTNAME`
   - Network interface for xCAT management network: `EMS_MGTNETINTERFACE`
   - Network interface for FSP network: `FSP_MGTNETINTERFACE` [**Not applicable for PPC64BE**]
   - FSP default IPMI password: `FSP_PASSWD` [**Not applicable for PPC64BE**]
   - HMC host name: `HMC_HOSTNAME` [**Not applicable for PPC64LE**]
   - HMC default user ID: `HMC_ROOTUID` [**Not applicable for PPC64LE**]
   - HMC default password: `HMC_PASSWD`[**Not applicable for PPC64LE**]
   - I/O server user ID: `IOSERVERS_UID`

- I/O server default password: `IOSERVERS_PASSWD`
- I/O server serial numbers: `IOSERVERS_SERIAL` [**Not applicable for PPC64BE**]
- I/O server node names: `IOSERVERS_NODES`
  For example, gssio1 gssio2
- Deployment OS image: `DEPLOY_OSIMAGE`

Note: For PPC64LE, there must be a one-to-one relationship between serial number and node in `gssdeploy.cfg` and for every node specified in `gssdeploy.cfg`, there must be a matching entry in `/etc/hosts`.

7. Perform precheck to detect any errors and address them before proceeding further:
   ```
   /opt/ibm/gss/tools/samples/gssprecheck -N ems1 --pre --install --file /var/tmp/gssdeploy.cfg
   ```

   Note: gssprecheck gives hints on ways to fix any discovered issues. It is recommended to review each found issue carefully though resolution of all might not be mandatory.
8. Verify that the ISO is placed in the location specified in the `gssdeploy.cfg` configuration file and then run the **gssdeploy** script:
   ```
   /var/tmp/gssdeploy -x
   ```

   Note: To perform I/O server discovery task this step will power cycle the I/O server nodes specified in the `gssdeploy.cfg` file.
9. Back up the xCAT database and save it to a location not on the management server node:
   ```
   dumpxCATdb -p /var/tmp/db
   tar -zcvf xCATDB-backup.tar.gz /var/tmp/db
   ```
10. Log out and then log back in to acquire the environment updates.
11. Set up the Kernel Errata repository and complete the steps for Installing the Errata Kernel Update.
12. Update the management server node. Here **ems1** is the xCAT host name. This step installs the kernel, uninstalls OFED, installs IBM Spectrum Scale, and applies the IBM Spectrum Scale profile.

    ```
    updatenode ems1 -P gss_updatenode
    ```

    Use **systemctl reboot** to reboot the management server node and run this step again as shown below. This additional step rebuilds OFED for new kernel and builds GPFS™ portability layer (GPL) for IBM Spectrum Scale.
    ```
    updatenode ems1 -P gss_updatenode
    ```
13. Update OFED on the management server node:

    ```
    updatenode ems1 -P gss_ofed
    ```
14. Update the IP RAID Adapter firmware on the management server node:
    ```
    updatenode ems1 -P gss_ipraid
    ```
15. If deploying on the PPC64LE platform, rebuild the mpt3sas RPM, which is located in the `/home/deploy` directory, by default:
    ```
    /bin/rpmbuild --rebuild /home/deploy/mpt3sas-13.100.00.00-1.el7_2.src.rpm
    ```
    This step creates two RPMs.
    a. Copy these RPMs in the kernel directory:
       ```
       cp -p /root/rpmbuild/RPMS/ppc64le/kmod-mpt3sas-13.100.00.00-1.el7.ppc64le.rpm ${KERNEL_DIR}
       cp -p /root/rpmbuild/RPMS/ppc64le/mpt3sas-debuginfo-13.100.00.00-1.el7.ppc64le.rpm ${KERNEL_DIR}
       ```
       `${KERNEL_DIR}` is `/install/gss/otherpkgs/rhels7/ppc64le/kernel`.
       ```
       cd ${KERNEL_DIR} ; createrepo .
       yum clean all
       ```
16. Use **systemctl reboot** to reboot the management server node.

Deploy the I/O server nodes

1. Before initiating the deployment of the I/O server nodes, do the following:
   a. Verify that the running kernel level is 55.3 using the **uname -a** command.
   b. Verify that there are no repository errors using the **yum repolist** command.
   c. Ensure that the attached storage enclosures are powered off.
2. Run the **gssinstallcheck** script:

   ```
   gssinstallcheck -N ems1
   ```

   This script is used to verify IBM Spectrum Scale profile, OFED, and kernel. etc.
   a. Check for any error with the following:
      1) Installed packages
      2) Linux kernel release
      3) OFED level
      4) IPR SAS FW
      5) IPR SAS queue depth
      6) System firmware
      7) System profile setting
      8) Host adapter driver

   Ignore other errors that may be flagged by the **gssinstallcheck** script. They will go away after the remaining installation steps are completed.
3. Run the **gssprecheck** script in full install mode and address any errors:

   ```
   /opt/ibm/gss/tools/samples/gssprecheck -N ems1 --install --file /var/tmp/gssdeploy.cfg
   ```

   Note: gssprecheck gives hints on ways to fix any discovered issues. It is recommended to review each found issue carefully though resolution of all might not be mandatory.
4. Deploy on the I/O server nodes using the customized deploy script:

   ```
   ./gssdeploy -d
   ```

5. After a duration of about five minutes, run the following command:

   ```
   nodestat gss_ppc64
   ```

   After running the command, the output displays the OS image name or packages being installed. For example:
   PPC64LE installations:

   ```
   node: rhels7.2-ppc64le-install-gss
   node: rhels7.2-ppc64le-install-gss
   ```

   PPC64BE installations:

   ```
   node: rhels7.2-ppc64-install-gss
   node: rhels7.2-ppc64-install-gss
   ```

   After about 30 minutes, the following output displays:

   ```
   node: sshd
   node: sshd
   ```

   The installation is complete when **nodestat** displays `sshd` for all I/O server nodes. Here **gss_ppc64** is the xCAT node group containing I/O server nodes. To follow the progress of a node installation, you can tail the console log by using the following command:

   ```
   tailf /var/log/consoles/NodeName
   ```

   where *NodeName* is the node name.

Note: Make sure the xCAT post-installation script is complete before rebooting the nodes. You can check xCAT post process running on the I/O server nodes as follows:

```
xdsh gss_ppc64 "ps -eaf | grep -v grep | grep xcatpost"
```

If there are any processes still running, wait for them to complete.

6. At the end of the deployment, wait for approximately five minutes and reboot the node:

   ```
   xdsh gss_ppc64 systemctl reboot
   ```

7. Once rebooted, verify the installation by running **gssinstallcheck:**

   ```
   gssinstallcheck -G ems1,gss_ppc64
   ```

   Check for any error with the following:

   a. Installed packages
   b. Linux kernel release
   c. OFED level
   d. IPR SAS FW
   e. IPR SAS queue depth
   f. System firmware
   g. System profile setting
   h. Host adapter driver

Ignore other errors that may be flagged by the **gssinstallcheck** script. They will go away after the remaining installation steps are completed.

Check the system hardware

After the I/O server nodes have been installed successfully, power on the attached enclosures. Wait approximately five to 10 minutes from power on for discovery to complete before moving on to the next step. Here is the list of key log files that should be reviewed for possible problem resolution during deployment.

- By default `/var/log/message` log from all I/O server nodes are directed to the message log in the EMS node.
- The gssdeploy log is located at `/var/log/gss`
- The xCAT log is located at `/var/log/xcat`
- Console outputs from the I/O server node during deployment are located at `/var/log/consoles`

1. Run **gssstoragequickcheck**:

   ```
   gssstoragequickcheck -G gss_ppc64
   ```

2. Run **gss_sashba script**:

   ```
   updatenode gss_ppc64 -P gss_sashba
   ```

3. Run **gssfindmissingdisks**:

   ```
   gssfindmissingdisks -G gss_ppc64
   ```

   If **gssfindmissingdisks** displays an error, run **mmgetpdisktopology** and pipe it to **topsummary** on each I/O server node to obtain more information about the error:

   ```
   mmgetpdisktopology > /var/tmp/<node>_top.out
   topsummary <node>_top.out
   ```

4. Run **gsscheckdisks**:

   ```
   GSSENV=INSTALL gsscheckdisks -G gss_ppc64 --encl all --iotest a --write-enable
   ```

Attention: When run with **--iotest w** (write) or **--iotest a** (all), **gsscheckdisks** will perform write I/O to the disks attached through the JBOD. This will overwrite the disks and will result in the loss of any configuration or user data stored on the attached disks. **gsscheckdisks** should be run only during the installation of a building block to validate that read and write operations can be performed to the attached drives without any error. The **GSSENV** environment variable must be set to **INSTALL** to indicate that **gsscheckdisks** is being run during installation.

5. Check for any hardware serviceable events and address them as needed. To view the serviceable events, issue the following command:

   ```
   gssinstallcheck -N ems1,gss_ppc64 --srv-events
   ```

   If you want to view detailed information about any of the displayed events on the PPC64LE architecture, you can use the following command:

   ```
   gssinstallcheck --platform-events EVENT
   ```

   On the PPC64BE architecture, use HMC to obtain detailed information about the displayed events.

   Note: During the initial deployment of the nodes on the PPC64BE platform, SRC BA15D001 might be logged as a serviceable event by Partition Firmware. This is normal and should be cleared after the initial deployment. For more information, see Appendix A, "Known issues," on page 25.

Note: Configure the node to connect to the Red Hat network and apply the latest security patches, if needed.

Set up the high-speed network

Set up the high-speed network that will be used for the cluster data communication. Update your `/etc/hosts` file with high-speed network entries showing the high-speed IP address and corresponding host name. Copy the modified `/etc/hosts` to I/O server nodes of the cluster. With the Ethernet high-speed network, you can use the **gssgennetworks** script to create a bonded Ethernet interface over active (up) high-speed network interfaces. See Appendix D, "Installation: reference," on page 39.

1. Update `/etc/hosts` file with high-speed hostname entries in the management server node and copy the modified `/etc/hosts` file to the I/O server nodes as follows:

   ```
   xdcp gss_ppc64 /etc/hosts /etc/hosts
   ```

2. To see the current set of active (up) interfaces on all nodes, run:

   ```
   gssgennetworks -N ems1,gss_ppc64 --suffix=-hs
   ```

   Where ems1 is the name of the management server node and gss_ppc64 is the I/O server node group and -hs is the node name suffix of the high-speed host name.

3. To create a bonded (Ethernet-only) interface, in all nodes, run:

   ```
   gssgennetworks -N ems1,gss_ppc64 --suffix=-hs --create-bond
   ```

   The script sets `miimon` to `100`, the bonding mode to `802.3ad` (LACP), and `xmit_hash_policy` to `layer2+3`. In some network configurations xmit_hash_policy of layer3+4 may provide a better load balancing of the traffic over the slave interfaces of the bond. You can change the xmit_hash_policy as follows once the bond is created.

   ```
   nmcli c mod bond-bond0 +bond.option xmit_hash_policy=layer3+4
   ```

   where bond-bond0 is the bonded interface.

   The other bond options are left with the default values, including `lacp_rate` (the default is `slow`). For proper network operation, the Ethernet switch settings in the networking infrastructure must match the I/O server node interface bond settings. If the Ethernet switch and network infrastructure cannot support bonding mode 802.3ad (LACP), another bonding mode can be selected. For more information, see the **gssgennetworks** man page.

   See Appendix D, "Installation: reference," on page 39 for information on how to set up networking.

   Note: If using bonded IP over IB, do the following:

Ensure that the **CONNECTED_MODE=yes** statement exists in the corresponding slave-bond interface scripts located in /etc/sysconfig/network-scripts directory of the management server and I/O server nodes. These scripts are created as part of the IP over IB bond creation. An example of the slave-bond interface with the modification is shown below.

```
TYPE=Infiniband         <= change from Ethernet to Infiniband
NAME=bond-slave-ib0     <= bond-slave-ib0 is the slave connection
UUID=86c0af63-4b6c-475c-a724-0fb074dc9092
DEVICE=ib0              <= slave interfaceONBOOT=yes
MASTER=bond0            <= master bond interface
SLAVE=yes
CONNECTED_MODE=yes      <= do not comment out this statement on RHEL 7.2
NM_CONTROLLED=yes       <= add this line
```

Run the following command:`nmcli c reload bond-bond0`

Here **bond-bond0** is the connection name of the bond.

4. Once the high-speed network is set up, stress test the high-speed network as follows:

   ```
   GSSENV=TEST gssnettest -N ems1,gss_ppc64 --suffix=-hs
   ```

   where ems1 is the management server node name and gss_ppc64 is the I/O server node group and -hs is the nodename suffix of the high-speed host name. This test should only be run in a test environment as it can highly stress the high-speed network.

Create the cluster, recovery groups, and file system

1. Create the GPFS cluster:

   ```
   gssgencluster -C test01 -G gss_ppc64 --suffix=-hs --accept-license
   ```

   In this example, `test01` is used as the cluster name and `-hs` is used as the suffix of the host name.
2. Create the recovery groups:

   ```
   gssgenclusterrgs -G gss_ppc64 --suffix=-hs
   ```
3. Create the vdisks, NSDs, and file system:

   ```
   gssgenvdisks --create-vdisk --create-nsds --create-filesystem --contact-node gssio1
   ```
4. Add the management server node to the cluster:

   ```
   gssaddnode -N ems1 --cluster-node gssio1 --suffix=-hs --accept-license --no-fw-update
   ```

   In this example, the management server hostname is `ems1` with a suffix of `-hs` (`ems1-hs`) in the high-speed network. The **--no-fw-update** option is used because the management server node does not contain a SAS adapter or attached drives.

Check the installed software and system health

1. Run **gssinstallcheck** on the management server:

   ```
   gssinstallcheck -N ems1
   ```
2. Run **gssinstallcheck** on the I/O server nodes:

   ```
   gssinstallcheck -G gss_ppc64
   ```
3. Shut down GPFS in all nodes and reboot all nodes.
   a. Shut down GPFS all nodes:

      ```
      mmshutdown -a
      ```
   b. Reboot all server nodes:

      ```
      xdsh gss_ppc64 "systemctl reboot"
      ```
   c. Reboot the management server node:

      ```
      systemctl reboot
      ```
4. After reboots, run the following command (**Not applicable for PPC64LE**):

```
gssinstallcheck -G gss_ppc64 --phy-mapping
```

Ensure that the phy mapping check is OK.

5. Restart GPFS in all nodes and wait for all nodes to become active:

```
mmstartup -a
```

6. Mount the filesystem and perform a stress test. For example, run:

```
mmmount gpfs0 -a
gssstress /gpfs/gpfs0 gssio1 gssio2
```

In this example, **gssstress** is invoked on the management server node. It is run on I/O server nodes `gssio1` and `gssio2` with `/gpfs/gpfs0` as the target path. By default gssstress runs for 20 iterations and can be adjusted using the -i option (type **gssstress** and press Enter to see the available options). During the I/O stress test, check for network error by running from another console:

```
gssinstallcheck -N ems1,gss_ppc64 -–net-errors
```

7. Perform a health check. Run:

```
gnrhealthcheck
/usr/lpp/mmfs/bin/mmhealth node show -N all --verbose
```

Address any issues that are identified.

8. Check for any open hardware serviceable events and address them as needed. The serviceable events can be viewed as follows:

```
gssinstallcheck -N ems1,gss_ppc64 --srv-events
```

If you want to view detailed information about any of the displayed events on the PPC64LE architecture, you can use the following command:

```
gssinstallcheck --platform-events EVENT
```

On the PPC64BE architecture, use HMC to obtain detailed information about the displayed events.

Note: During initial deployment of the nodes, SRC BA15D001 may be logged as serviceable event by Partition Firmware. This is normal and should be cleared after the initial deployment. For more information, see Appendix A, “Known issues,” on page 25.

9. Verify that NTP is set up and enabled.
   a. On the management server node verify that `/etc/ntp.conf` is pointing to the management server node itself over the management interface.
   b. Restart NTP daemon on each node.

```
xdsh <ems>,gss_ppc64 "systemctl restart ntpd"
```

   c. Verify that NTP is setup correctly by running the following checks:
      - Verify that offset is 0.

```
xdsh ems1,gss_ppc64 "ntpq -p"
```

      - Verify that NTP is enabled and synchronized.

```
xdsh ems1,gss_ppc64 "timedatectl status" | grep -i NTP
```

      - Verify that the timezone is set correctly on each node.

```
xdsh ems1,gss_ppc64 "timedatectl status"  | grep -i zone
```

Install the ESS GUI

Important: Complete all of the following steps carefully including the steps for configuring **mmperfmon** and restricting certain sensors to the management server node (EMS) only.

1. Generate performance collector on the management server node by running the following command. The management server node must be part of the ESS cluster and the node name must be the node name used in the cluster (e.g., ems1-hs).

```
mmperfmon config generate --collectors ems1-hs
```

2. Set up the nodes in the *ems nodeclass* and *gss_ppc64 nodeclass* for performance monitoring running the following command.

   ```
   mmchnode --perfmon -N ems,gss_ppc64
   ```

3. Capacity and fileset quota monitoring is not enabled in the GUI by default. You must correctly update the values and restrict collection to the management server node only.
   a. To modify the GPFS Disk Capacity collection interval, run the following command:

      ```
      mmperfmon config update GPFSDiskCap.restrict=EMSNodeName
               GPFSDiskCap.period=PeriodInSeconds
      ```

      The recommended period is 86400 so that the collection is done once per day.
   b. To restrict GPFS Fileset Quota to run on the management server node only, run the following command:

      ```
      mmperfmon config update GPFSFilesetQuota.restrict=EMSNodeName
      ```

      Here the *EMSNodeName* must be the name shown in the **mmlscluster** output.

      Note: To enable quota, the filesystem quota checking must be enabled. Refer **mmchfs -Q** and **mmcheckquota** commands in the *IBM Spectrum Scale: Command and Programming Reference*.
4. Verify that the values are set correctly in the performance monitoring configuration by running the **mmperfmon config show** command on the management server node. Make sure that `GPFSDiskCap.period` is properly set, and `GPFSFilesetQuota` and `GPFSDiskCap` are both restricted to the management server node only.

   Note: If you are moving from manual configuration to auto configuration then all sensors are set to default. Make the necessary changes using the **mmperfmon** command to customize your environment accordingly. For information on how to configure various sensors using **mmperfmon**, see Manually installing IBM Spectrum Scale GUI.
5. Start the performance collector on the management server node:

   ```
   systemctl start pmcollector
   ```

6. Enable and start gpfsgui:

   ```
   systemctl enable gpfsgui.service
   systemctl start gpfsgui
   ```

7. To launch the ESS GUI in a browser, go to: `https://EssGuiNode` where ESSGuiNode is the hostname or IP address of the management server node for GUI access. To log in, type admin in the User Name field and your password in the Password field on the login page. The default password for admin is admin001. Walk through each panel and complete the GUI Setup Wizard.

This completes the installation task of the ESS system. After completing the installation, apply security updates available from Red Hat.

For information on applying optimized configuration settings to a set of client nodes or a node class, see "Adding IBM Spectrum Scale nodes to an ESS cluster" on page 46.

Upgrade the ESS system

During the upgrade process if a step fails, it must be addressed before moving to the next step. Follow these steps to perform an upgrade of the ESS system. **This section applies to the PPC64BE architecture.**

Note: For considerations and instructions to upgrade a cluster that contains ESS and protocol nodes, see Chapter 2, "Upgrading a cluster containing ESS and protocol nodes," on page 19. You can decide when to upgrade the ESS system in such a cluster. You can either upgrade protocol nodes first and then the ESS system or you can upgrade the ESS system first, followed by the protocol nodes.

Prerequisites and supported upgrade paths

Before you begin the upgrade procedure, do the following:

- Ensure that the Red Hat Enterprise Linux (RHEL) 7.2 PPC64 server ISO (for example, `RHEL-7.2-20151030.0-Server-ppc64-dvd1.iso`) is available in the `/opt/ibm/gss/iso` directory as specified in the `gssdeploy.cfg` configuration file.
- Disable the subscription manager and any external repositories by issuing the following commands on each node that you want to upgrade:

```
subscription-manager config --rhsm.manage_repos=0
yum clean all
```

The following upgrade paths are supported:

- ESS version 4.5.x, 4.6.x, or 5.0.x to version 5.1.x on PPC64BE.

Note: For upgrading to ESS 5.1.x from version 4.0.x or earlier, contact IBM Support.

Important:

If you are not upgrading to ESS 5.1.x, ensure that you have the following version installed to avoid system stability or functional issues:

- If you have 4.5.x installed: ESS 4.5.2 or later
- If you have 5.0.x installed: ESS 5.0.1 or later

Prepare the system for upgrade

1. Perform a health check by issuing the following command:

   ```
   gnrhealthcheck
   ```

   Address any issues that are identified.
2. Wait for any of these commands that are performing file system maintenance tasks to complete:
   mmadddisk
   mmapplypolicy
   mmcheckquota
   mmdeldisk
   mmfsck
   mmlssnapshot
   mmrestorefs
   mmrestripefile
   mmrestripefs
   mmrpldisk
3. Stop the creation and deletion of snapshots using **mmcrsnapshot** and **mmdelsnapshot** during the upgrade window.

Upgrading from ESS 5.0.x, ESS 4.6.x, and ESS 4.5.x

Perform the following steps if you are upgrading from ESS 5.0.x, ESS 4.6.x, and ESS 4.5.x :

1. Check for any hardware serviceable events from the HMC:

   ```
   gssinstallcheck -G ems1,gss_ppc64 --srv-events
   ```

   Address any hardware issues identified in the serviceable events.
2. Check for any deployment errors:

   ```
   gssinstallcheck -G ems1,gss_ppc64
   ```
3. Make the **gssdeploy** script executable:

```
chmod +x /opt/ibm/gss/install/samples/gssdeploy
```

4. If you are upgrading from ESS 4.6.x or ESS 4.5.x, perform cleanup and save a backup copy of the xCAT database:

   ```
   /opt/ibm/gss/install/samples/gssdeploy -c -r /var/tmp/xcatdb
   ```

5. Update ESS repositories on the management server node:

   ```
   cd /opt/ibm/gss/install
   installer/gssinstall -m manifest -u
   ```

6. If you are upgrading from ESS 4.6.x or ESS 4.5.x, copy the `gssdeploy.cfg` configuration file to the `/var/tmp` directory:

   ```
   cp /opt/ibm/gss/install/samples/gssdeploy.cfg /var/tmp
   ```

7. If you are upgrading from ESS 4.6.x or ESS 4.5.x, customize the `gssdeploy.cfg` configuration file according to your environment. For information about the contents of `gssdeploy.cfg`, see "Install the ESS system" on page 3.

Update the management server node

1. On the management server node, stop GUI services, and save performance monitoring collector and sensor configuration files:

   ```
   systemctl stop gpfsgui
   cp /opt/IBM/zimon/ZIMonCollector.cfg /var/tmp
   cp /opt/IBM/zimon/ZIMonSensors.cfg /var/tmp
   ```

2. If you are upgrading from ESS 4.6.x or ESS 4.5.x, install tools and xCAT and restore the xCAT database:

   ```
   /var/tmp/gssdeploy -x -r /var/tmp/xcatdb
   ```

3. Perform precheck to detect any errors and address them before proceeding further:

   ```
   /opt/ibm/gss/tools/samples/gssprecheck -N ems1 --upgrade --file /var/tmp/gssdeploy.cfg
   ```

   Note: **`gssprecheck`** gives hints on ways to fix any discovered issues. It is recommended to review each found issue carefully though resolution of all might not be mandatory.

4. Shut down IBM Spectrum Scale on the management server node while making sure quorum is still maintained:

   ```
   mmshutdown
   ```

5. If you have not installed the kernel update, complete the following steps:
   a. Obtain and package the kernel update. For more information, see Appendix F, "Obtaining kernel for system upgrades," on page 51.
   b. Stage the kernel update for installation. For more information, see Appendix G, "Instructions for installing the ESS Red Hat Linux Errata Kernel Update," on page 53.

   If you have already installed the kernel update, skip this step.

6. Update the management server node:

   ```
   updatenode ems1 -P gss_updatenode
   ```

   Use **`systemctl reboot`** to reboot the management server node and complete this step again as follows:

   ```
   updatenode ems1 -P gss_updatenode
   ```

   This additional step rebuilds OFED for the new kernel and builds GPFS Portability Layer (GPL) for IBM Spectrum Scale, if required.

7. Update OFED on the management server node:

   ```
   updatenode ems1 -P gss_ofed
   ```

8. Update IP RAID Adapter firmware on the management server node:

   ```
   updatenode ems1 -P gss_ipraid
   ```

9. Ensure that the **CONNECTED_MODE=yes** statement exists in the corresponding slave-bond interface scripts located in `/etc/sysconfig/network-scripts` directory of the ems1 node. An example of the slave-bond interface with the modification is as follows.

```
TYPE=Infiniband
NAME=bond-slave-ib0
UUID=86c0af63-4b6c-475c-a724-0fb074dc9092
DEVICE=ib0
ONBOOT=yes
MASTER=bond0
SLAVE=yes
CONNECTED_MODE=yes       <= do not comment out this statement on RHEL 7.2
NM_CONTROLLED=yes
```

10. Use **`systemctl reboot`** to reboot the management server node.
11. Perform the following steps to upgrade IBM Spectrum Scale RAID configuration parameters.

```
/opt/ibm/gss/tools/samples/gssupg511.sh -b ems1-hs,gss_ppc64
/opt/ibm/gss/tools/samples/gssupg511.sh -c
```

12. Start IBM Spectrum Scale on the management server node:

```
mmstartup
```

13. Verify that IBM Spectrum Scale is in the active state before upgrading the I/O server nodes:

```
mmgetstate
```

    Do not proceed if the system is not active.
14. Ensure that the management server node is fully updated and active:

```
gssinstallcheck -N ems1
```

Update the I/O server nodes

Repeat the following steps for each I/O server node, one node at a time.

1. Before shutting down GPFS on any I/O server node, run precheck from the management server node:

```
/opt/ibm/gss/tools/samples/gssprecheck -N IO_NODE --upgrade --file /var/tmp/gssdeploy.cfg
```

   Note: `gssprecheck` gives hints on ways to fix any discovered issues. It is recommended to review each found issue carefully though resolution of all might not be mandatory.
2. Move the cluster and file system manager role to another node if the current node is a cluster manager or file system manager.
   a. To find the cluster and file system managers, run:

```
mmlsmgr
```

   b. To change the file system manager, run:

```
mmchmgr gpfs0 gssio2-hs
```

      In this example, `gssio2-hs` is the new file system manager of file system `gpfs0`.
   c. To change the cluster manager, run:

```
mmchmgr -c gssio2-hs
```

      In this example, `gssio2-hs` is the new cluster manager.
3. Move the recovery group in the current I/O server node to the peer I/O server node in the same building block.
   a. To list the recovery groups, run:

```
mmlsrecoverygroup
```

   b. To list the active server, primary server, and secondary server, run:

```
mmlsrecoverygroup rg_gssio1-hs -L | grep active -A2
```

c. To move the recovery group from the current active I/O server node (`rg_gssio1-hs`) to the peer I/O server node (`gssio2-hs`) in the same building block, run the following commands in the shown order:

```
mmchrecoverygroup rg_gssio1-hs --active gssio2-hs

mmchrecoverygroup rg_gssio1-hs --servers gssio2-hs,gssio1-hs
```

4. After confirming that the recovery group has been successfully moved to the peer I/O server node, unmount all GPFS file systems if mounted, and shut down IBM Spectrum Scale on the current I/O server node while maintaining quorum:

```
mmunmount all -N CurrentIoServer-hs
mmshutdown -N CurrentIoServer-hs
```

5. Run **updatenode**:

```
updatenode CurrentIoServer -P gss_updatenode
```

Reboot the I/O server node and complete this step again if you are instructed to do so in the **updatenode** output. Reboot the I/O server node as follows :

```
xdsh CurrentIoServer "systemctl reboot"
```

6. Update OFED.

```
updatenode CurrentIoServer -P gss_ofed
```

7. Update IP RAID FW in the I/O Server node that is being upgraded.

```
updatenode CurrentIoServer -P gss_ipraid
```

8. Ensure that the **CONNECTED_MODE=yes** statement exists in the corresponding slave-bond interface scripts located in `/etc/sysconfig/network-scripts` directory of the *CurrentIOServer* node. An example of the slave-bond interface with the modification is as follows.

```
TYPE=Infiniband
NAME=bond-slave-ib0
UUID=86c0af63-4b6c-475c-a724-0fb074dc9092
DEVICE=ib0
ONBOOT=yes
MASTER=bond0
SLAVE=yes
CONNECTED_MODE=yes       <= do not comment out this statement on RHEL 7.2
NM_CONTROLLED=yes
```

9. Reboot the I/O server node as follows:

```
xdsh CurrentIoServer "systemctl reboot"
```

10. Update the SAS host adapter firmware on *CurrentIoServer*:

```
CurrentIoServer$ mmchfirmware --type host-adapter
```

Here CurrentIOServer is an I/O server node and the command is run on the I/O server node.

11. Update the node configuration:

```
/opt/ibm/gss/tools/samples/gssupg511.sh -s CurrentIoServer-hs
```

This command is run from the EMS node.

12. Run phy check and ensure that the phy mapping is OK:

```
gssinstallcheck -N CurrentIoServer --phy-mapping
```

13. Start IBM Spectrum Scale on the I/O server node:

```
mmstartup -N CurrentIoServer-hs
```

Once the IBM Spectrum Scale daemon is successfully started, move back the recovery group that was moved to the peer I/O server node of the same building block in Step 3c above. Move back the cluster manager and the file system manager if required that was moved to the other nodes in step 2.

14. Wait until the I/O server can be seen active from the management server node, using the following command:

    ```
    mmgetstate
    ```

    The management server must be already running for issuing this command.

15. Run **gssinstallcheck** from the management server node:

    ```
    gssinstallcheck -N IO_NODE
    ```

16. Repeat preceding steps for the peer I/O server node of the same building block.
17. Repeat all steps in this section for each additional building block.

Update the enclosure and drive firmware

1. To update the storage enclosure firmware, run the following command from one I/O Server node of each building block:

   ```
   CurrentIoServer$ mmchfirmware --type storage-enclosure
   ```

2. To update the drive firmware, run the following command from **each** I/O Server node of each building block:

   ```
   CurrentIoServer$ mmchfirmware --type drive
   ```

   The drive update can take some time to complete. You can update the drives more quickly by taking the system offline (shutting down IBM Spectrum Scale) and using the **--fast-offline** option.

Check the installed software and system health

1. Perform a health check:

   ```
   gnrhealthcheck
   /usr/lpp/mmfs/bin/mmhealth node show -N all --verbose
   ```

2. Check for any hardware serviceable events and address them as needed. To view the serviceable events, issue the following command:

   ```
   gssinstallcheck -N ems1,gss_ppc64 --srv-events
   ```

   Note: During the initial deployment of the nodes, SRC BA15D001 might be logged as a serviceable event by Partition Firmware. This is normal and should be cleared after the initial deployment. For more information, see Appendix A, “Known issues,” on page 25.

Note: Some of these steps might fail if they are already implemented in previous versions of ESS. If you see any failures indicating **mmperfmon** has already been configured, ignore these failure messages and continue with the remaining steps.

Upgrading GUI

Upgrading from ESS 5.0.x, ESS 4.6.x, and ESS 4.5.x

Perform the following steps to upgrade from ESS 5.0.x, ESS 4.6.x, and ESS 4.5.x :

1. Generate performance collector on the management server node by running the following command. The management server node must be part of the ESS cluster and the node name must be the node name used in the cluster (e.g., ems1-hs).

   ```
   mmperfmon config generate --collectors ems1-hs
   ```

2. Set up the nodes in the *ems nodeclass* and *gss_ppc64 nodeclass* for performance monitoring running the following command.

```
mmchnode --perfmon -N ems,gss_ppc64
```

3. Capacity and fileset quota monitoring is not enabled in the GUI by default. You must correctly update the values and restrict collection to the management server node only.
   a. To modify the GPFS Disk Capacity collection interval, run the following command:
      ```
      mmperfmon config update GPFSDiskCap.restrict=EMSNodeName
               GPFSDiskCap.period=PeriodInSeconds
      ```
      The recommended period is 86400 so that the collection is done once per day.
   b. To restrict GPFS Fileset Quota to run on the management server node only, run the following command:
      ```
      mmperfmon config update GPFSFilesetQuota.restrict=EMSNodeName
      ```
      Here the *EMSNodeName* must be the name shown in the **mmlscluster** output.

      Note: To enable quota, the filesystem quota checking must be enabled. Refer **mmchfs -Q** and **mmcheckquota** commands in the *IBM Spectrum Scale: Command and Programming Reference*.
4. Verify that the values are set correctly in the performance monitoring configuration by running the **mmperfmon config show** command on the management server node. Make sure that `GPFSDiskCap.period` is properly set, and `GPFSFilesetQuota` and `GPFSDiskCap` are both restricted to the management server node only.

   Note: If you are moving from manual configuration to auto configuration then all sensors are set to default. Make the necessary changes using the **mmperfmon** command to customize your environment accordingly. For information on how to configure various sensors using **mmperfmon**, see Manually installing IBM Spectrum Scale GUI.
5. Start the performance collector on the management server node:
   ```
   systemctl start pmcollector
   ```
6. Enable and start gpfsgui:
   ```
   systemctl enable gpfsgui.service
   systemctl start gpfsgui
   ```
7. To launch the ESS GUI in a browser, go to: `https://EssGuiNode` where ESSGuiNode is the hostname or IP address of the management server node for GUI access. To log in, type admin in the User Name field and your password in the Password field on the login page. The default password for admin is admin001. Walk through each panel and complete the GUI Setup Wizard.

After the GUI is up and running, do the following:

1. Enable the subscription manager by issuing the following commands on the upgraded nodes:
   ```
   subscription-manager config --rhsm.manage_repos=1
   yum clean all
   ```
2. Obtain the systemd update and apply it on each node. For more information, see Appendix H, "Obtaining systemd update for system upgrades," on page 55 and Appendix I, "Instructions for installing the ESS Red Hat Linux systemd update," on page 57.

This completes the upgrade task of the ESS system. For information on applying optimized configuration settings to a set of client nodes or a node class, see "Adding IBM Spectrum Scale nodes to an ESS cluster" on page 46.

Chapter 2. Upgrading a cluster containing ESS and protocol nodes

The procedure for upgrading a cluster containing ESS and protocol nodes comprises several phases. Although the protocol node upgrade procedure is detailed here, the same procedure can be tweaked and used for client and NSD nodes as well.

1. "Planning the upgrade"
2. "Performing upgrade prechecks" on page 20
3. "Upgrading protocol nodes using the installation toolkit" on page 22
4. "Upgrading OFED, OS, and kernel errata on protocol nodes" on page 23

   This phase comprises the following steps.

   a. Uninstalling OFED
   b. Upgrading OS and rebooting the system
   c. Upgrade kernel and rebooting the system
   d. Upgrading firmware
   e. Build the GPFS portability layer
   f. Installing OFED and rebooting the system
5. "Upgrading ESS" on page 24
6. "Upgrading HMC in PPC64BE systems" on page 24

Planning the upgrade

Before scheduling an upgrade of a cluster containing ESS and protocol nodes, planning discussions must take place to know the current cluster configuration and to understand which functions might face an outage.

The planning phase comprises of the following steps.

1. Note all products and functions currently installed in the cluster being upgraded.
   - SMB
   - NFS
   - cNFS
   - Object
   - TCT
   - AFM
   - Encryption
   - CES Groups
   - IBM Spectrum Protect™
   - DMAPI flag for file systems
   - IBM Spectrum Archive™ EE
   - GUI - How many and which nodes?
   - Performance monitoring collectors - How many and where are they located?
   - Performance monitoring sensors - Are they installed on all nodes?
   - Which nodes run more than one of these functions?
2. Understand the source version and the number of hops needed to move to the target code version across all nodes and functions.

3. Understand if the IBM Spectrum Scale installation toolkit can be used on the protocol nodes and also understand how the installation toolkit performs the upgrade. For information about installation toolkit limitations, see Limitations of the installation toolkit.

   Note: This instruction set assumes that the installation toolkit is being used for protocol nodes.
4. Set expectations for functional currency and outages. For more information, see IBM Spectrum Scale FAQ.
5. Obtain the necessary packages. For more information, see "Complete the prerequisite tasks" on page 2.
6. Decide the upgrade sequence.
7. Decide whether operating system, driver, or firmware updates are needed on protocol nodes. This includes OFED, Power® firmware, x86 firmware. When making this decision, be aware that tools normally used within ESS might not be available to assist with automating these efforts outside of the ESS nodes.

Performing upgrade prechecks

The precheck phase assists with the planning phase and it can be done on a cluster without any harm. It might be useful to run through the precheck steps the day before an upgrade is scheduled, or earlier, to guard against any unexpected situations that might lead to an upgrade failure.

1. Identify the protocol nodes to be upgraded.
2. Verify that a base OS repository exists, and if it does not exist, configure one on all protocol nodes. The repository must reflect the current OS or kernel on the nodes and not the version being upgraded to. The OS upgrade will be done after the IBM Spectrum Scale upgrade using the installation toolkit.
   a. Check the current OS and kernel level.

      ```
      uname –a
      cat /etc/*release*
      ```
   b. Check the existing repositories.

      ```
      yum repolist
      ```
   c. Pick a file to install for testing the repository and use **yum install** to try the installation. Enter `no` on the confirmation prompt. If the repository for your current base OS does not exist, create one as follows.
      1) Mount the installation image by issuing one of the following command depending on the media type.
         - If using an ISO, issue this command:

           ```
           mount -o loop RHEL7.2.iso /mnt
           ```
         - If using DVD media, issue this command:

           ```
           mount -o loop /dev/sr0  /mnt
           ```
      2) Copy the `media.repo` file from the `/mnt` directory to `/etc/yum.repos.d` and change its permissions.

         ```
         cp /mnt/media.repo /etc/yum.repos.d/rhel72dvd.repo
         chmod 644 /etc/yum.repos.d/rhel72dvd.repo
         ```
      3) Open the file in an editor.

         ```
         vi /etc/yum.repos.d/rhel72dvd.repo
         ```
      4) Configure the following settings in the file.

         ```
         gpgcheck=1
         enabled=1
         baseurl=file:///mnt/
         gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
         ```
      5) Clear the caches.

```
yum clean all
subscription-manager clean
```

6) Verify that you can obtain the packages list from the repository.

```
yum list --noplugins
```

Note: When creating a repository, make sure to give it a new name that is different than any existing repositories. This reduces the possibility of yum caching errors.

Note: These steps will vary for SLES 12 nodes and zypper repositories.

3. Verify and, if needed, configure promptless ssh on all protocol nodes and ESS nodes (EMS and I/O server nodes).

   Important: Verify the following combinations.

   - All nodes must be able to ssh to themselves and all other nodes using the IP
   - All nodes must be able to ssh to themselves and all other nodes using the host name
   - All nodes must be able to ssh to themselves and all other nodes using the FQDN

   If your IBM Spectrum Scale cluster version is 4.2.2 or later, you can use the **mmnetverify** command to check for promptless ssh access among nodes.
4. Verify that the contents of the `/etc/hosts` file on each protocol nodes are in the following format:

   ```
   <IP> <FQDN> <alias>
   ```
5. Verify that firewall ports required for the necessary functions are open. For more information, see Securing the IBM Spectrum Scale system using firewall.
6. Download the new IBM Spectrum Scale self-extracting package using the sub-steps and then place it on the protocol node that you plan to designate as the installer node.
   a. Go to the IBM Spectrum Scale page on Fix Central, select the new **spectrumscale** package and then click **Continue**.
   b. Choose the download option **Download using Download Director** to download the new **spectrumscale** package and place it in the wanted location on the install node.
7. Extract the new IBM Spectrum Scale self-extracting package by using the package name (for example, `/tmp/Spectrum_Scale_Protocols_Standard-4.2.3.0_x86_64-Linux_install`).

   This creates a new directory structure (`/usr/lpp/mmfs/4.2.3.0/`).
8. In the installation toolkit, enter the configuration to mirror the current cluster configuration.
   - Do not input the EMS or I/O nodes from the ESS system.
   - If the installation toolkit was previously used, the old clusterdefinition.txt file can be copied to the new code location as follows.

     ```
     cp –p /usr/lpp/mmfs/4.2.2.1/installer/configuration/clusterdefinition.txt \
     /usr/lpp/mmfs/4.2.3.0/installer/configuration
     ```
   - Input any protocol or non-protocol nodes on which you plan to use the installation toolkit:

     ```
     /usr/lpp/mmfs/4.2.3.0/installer/spectrumscale node add
     ```
   - Input the existing CES shared root file system into the installation toolkit:

     ```
     /usr/lpp/mmfs/4.2.3.0/installer/spectrumscale config protocols -f cesshared -m /ibm/cesshared
     ```
   - Input the existing CES IPs (**mmces address list**) into the installation toolkit:

     ```
     /usr/lpp/mmfs/4.2.3.0/installer/spectrumscale config protocols -e CESIP1,CESIP2,CESIP3
     ```
   - It is not required to input NSD or file system information.
   - Disable performance monitoring so that the installation toolkit does not add more collectors to the protocols nodes since the collector should already exist on the ESS configuration.

     ```
     ./spectrumscale config perfmon -r off
     ```
   - If the installation toolkit must be setup from scratch, you can refer to this example:

```
./spectrumscale setup –s 192.168.10.1                    ## IP of installer node that all other nodes can get to
./spectrumscale node add node1.gpfs.net –a -p            ## designates this node as the node
                                                         ## that runs mm commands for the installer.
                                                         ## Also designates it as a protocol node
./spectrumscale node add node2.gpfs.net -p
./spectrumscale node add node3.gpfs.net –p
./spectrumscale node add node4.gpfs.net                  ## example of a client node
./spectrumscale enable smb                               ## if SMB is active
./spectrumscale enable nfs                               ## if NFS is active
./spectrumscale enable object                            ## if Object is active
./spectrumscale config protocols -e CESIP1,CESIP2,CESIP3          ## CES-IPs gathered from mmces address list
./spectrumscale config protocols -f cesshared -m /ibm/cesshared   ## FS name and mount point for CES shared root
./spectrumscale config perfmon –r off                   ## turn off perfmon recofig so it doesn't interfere with the ESS
./spectrumscale node list                               ## list out the node config afterwards
./spectrumscale config protocols                        ## shows the protocol config
```

Note: The installation toolkit can be used for tasks other than upgrade, such as adding new protocols and protocol nodes. If you are planning to do this in the future, you will need to expand the preceding example to input configuration details necessary for each future action. For more information, see Protocols Quick Overview Guide.

9. Run the installation toolkit upgrade precheck.

   ```
   ./spectrumscale upgrade –precheck
   ```

   A successful precheck implies that you are ready for using the installation toolkit to perform the upgrade.
10. Double check networking and bonding modes that are in use and save this information in case it is needed later.
11. Check the level of OFED drivers and place the latest OFED package on the nodes, if using Infiniband adapters.

Upgrading protocol nodes using the installation toolkit

Use these steps to upgrade protocol nodes using the installation toolkit.

Before proceeding with the upgrade using the installation toolkit, ensure that the toolkit is set up. For more information, see this step of the precheck task.

This phase of the upgrading a cluster containing ESS and protocol nodes procedure is dependent on the successful completion of the planning and precheck phases.

1. Run the installation toolkit upgrade precheck.

   ```
   ./spectrumscale upgrade --precheck
   ```

   If the precheck is successful, proceed to the next step.
2. Run the installation toolkit upgrade procedure.

   ```
   ./spectrumscale upgrade
   ```

   When this procedure is done, components including base GPFS and protocols will have been upgraded on all protocol nodes that were specified to the installation toolkit. This step does not need to be repeated on each node unless only a subset of nodes were specified to the installation toolkit.
3. Check whether the performance monitoring RPMs did not upgrade due to the `config perfmon –r off` flag being used for installation toolkit. If that is the case, you need to copy the performance monitoring RPMs (`/usr/lpp/mmfs/4.2.3.2/zimon_rpms` or `/usr/lpp/mmfs/4.2.3.2/zimon_debs`) from the installer node to each node and manually upgrade each node by issuing a command similar to the following.

   ```
   yum localinstall gpfs.gss.pmsensors-4.2.3.0.el7.x86_64.rpm
   ```
4. Verify that the performance monitoring sensors point to the performance monitoring collector service running on the EMS node.

```
mmperfmon config show
```

Assuming that the **mmperfmon config generate** was run to configure the collectors, it might be needed to point the performance monitoring sensors back to the performance monitoring collector on the EMS node.

```
mmchnode --perfmon -N NodeTobeAdded
```

Upgrading OFED, OS, and kernel errata on protocol nodes

Use these steps to upgrade OFED, OS, and kernel errata on protocol nodes as part of upgrading a cluster containing ESS and protocol nodes.

This phase is not required but it is advisable to match OFED, OS, and kernel errata across all nodes within a cluster to help with performance and to ease debugging. As a part of this procedure, ensure the following:

- Always upgrade IBM Spectrum Scale on protocol nodes prior to OFED, OS, and kernel errata.
- If kernel errata is for a new OS (RHEL7.2 vs RHEL7.1), always update the OS before the kernel errata.
- When taking nodes offline to update OFED, OS, and kernel errata, ensure the following:
  - Quorum does not break
  - Enough NSD nodes remain up to access NSDs
  - The remaining nodes can handle the desired workload

Repeat the following steps on each node.

1. Uninstall the OFED drivers as follows.
   a. Obtain and extract OFED drivers.
   b. Suspend CES on the node being upgraded.
      ```
      mmces node suspend -N NodeBeingUpgraded
      ```
   c. Shut down GPFS on the node being upgraded.
      ```
      mmshutdown -N NodeBeingUpgraded
      ```
   d. Find the uninstallation script within the OFED drivers package and execute it on the node being upgraded..
      ```
      mount –o loop mellanox_iso_name /media
      cd /media
      ./uninstall.sh
      ```
2. Create a local repository for the OS upgrade. For information on creating a base RHEL repository, see these steps in the precheck task.

   A repository must be created so that the OS can be upgraded. This repository can be DVD or ISO based. Make sure that you remove any repositories pointing to old OS versions.
3. Upgrade the OS.
   ```
   yum upgrade
   ```
   Review the `yum upgrade` output for any errors that might need to be resolved prior to rebooting and ensure that a clean yum upgrade operation was completed and that it was successful. Reboot the node after OS upgrade.
   ```
   shutdown -r now
   ```
4. Update the kernel errata. For more information, see Appendix F, “Obtaining kernel for system upgrades,” on page 51 and Appendix G, “Instructions for installing the ESS Red Hat Linux Errata Kernel Update,” on page 53. Reboot the node after kernel errata update.
   ```
   shutdown -r now
   ```
5. Update the Power8 and x86 firmware. For information on updating Power8 firmware, see Appendix E, “Updating the system firmware,” on page 49 and ESS Installation and Deployment Blog.

   x86 firmware update is dependent on the manufacturer, model, and type.

6. Build the GPFS portability layer using the **mmbuildgpl** command. For more information, see Building the GPFS portability layer.
7. Install the latest OFED drivers.

   Note: Do this step only after the OS and kernel are at the latest levels. The OFED level is tied to the kernel so if the kernel changes afterwards, this step might need to be repeated.

   a. Create an updated ISO file for the currently active kernel..

      ```
      mount –o loop mellanox_iso_name /media
      /media/mlnx_add_kernel_support.sh –m /media --make-iso –y --distro rhel7.2 --kmp
      ```

      Ensure that the Linux distribution matches exactly.

   b. Install the OFED drivers from the newly created ISO.

      ```
      umount /media
      mount –o loop newlybuilt_iso_name /media
      cd /media
      ./mlnxofedinstall –q --force
      ```

   Reboot the node after the driver update.

   ```
   shutdown -r now
   ```

8. Verify that GPFS is active on the node and then resume CES.

   ```
   mmgetstate -a
   mmces node resume -N NodeBeingUpgraded
   mmces node list
   mmces service list -a
   mmces address list
   ```

9. Repeat the preceding steps on all non-ESS nodes that the EMS does not upgrade.

Upgrading ESS

While upgrading a cluster containing ESS and protocol nodes, an upgrade of the ESS system itself might occur either before or after the upgrade of protocol nodes. If not yet done, proceed with an upgrade of the ESS system.

For detailed information on the ESS upgrade procedure, see “Upgrade the ESS system” on page 11.

Upgrading HMC in PPC64BE systems

While upgrading a cluster containing ESS and protocol nodes, if you had not upgraded HMC before applying the Power8 system firmware, you can proceed with upgrading HMC after the ESS upgrade completes.

To apply the HMC V8 update, use the following resources:

- HMC V8 upgrade procedure: https://www-01.ibm.com/support/docview.wss?uid=nas8N1020108
- HMC V8 860 files: ftp://public.dhe.ibm.com/software/server/hmc/network/v8860/
- HMC V8 860 SP1 ISO: ftp://public.dhe.ibm.com/software/server/hmc/updates/HMC_Update_V8R860_SP1.iso

Appendix A. Known issues

This topic describes known issues for ESS.

ESS 5.1.x issues

The following table describes known issues in ESS 5.1.x and how to resolve these issues. Depending on which fix level you are installing, these might or might not apply to you.

Table 2. Known issues in ESS 5.1.x

Issue	Environment affected	Description	Resolution or action

The **gssgennetworks** script requires high-speed host names to be derived from I/O server (xCAT) host names using suffix, prefix, or both.	High-speed network generation
	Type: Install
	Version: Advanced or Standard
	Arch: Big Endian or Little Endian
	Affected nodes: I/O server and EMS nodes
		gssgennetworks requires that the target host name provided in -N or -G option are reachable to create the high-speed network on the target node. If the xCAT node name does not contain the same base name as the high-speed name you might be affected by this issue. A typical deployment scenario is:
		gssio1 // xCAT name
		gssio1-hs // high-speed
		An Issue scenario is:
		gssio1 // xCAT name
		foo1abc-hs // high-speed name
			Create entries in the /etc/hosts with node names that are reachable over the management network such that the high-speed host names can be derived from it using some combination of suffix and/or prefix. For example, if the high-speed host names are foo1abc-hs, goo1abc-hs:
			1. Add foo1 and goo1 to the /etc/hosts using management network address (reachable) in the EMS node only.
			2. Use: **gssgennetworks -N foo1,goo1 – suffix abc-hs --create-bond**
			3. Remove the entries foo1 and goo1 from the /etc/hosts file on the EMS node once the high-speed networks are created.
			Example of how to fix (/etc/hosts):
			// Before
			<IP><Long Name><Short Name> 192.168.40.21 gssio1.gpfs.net gssio1 192.168.40.22 gssio2.gpfs.net gssio2 X.X.X.X foo1abc-hs.gpfs.net foo1abc-hs X.X.X.Y goo1abc-hs.gpfs.net goo1abc-hs
			// Fix
			192.168.40.21 gssio1.gpfs.net gssio1 foo1 192.168.40.22 gssio2.gpfs.net gssio2 goo1 X.X.X.X foo1abc-hs.gpfs.net foo1abc-hs X.X.X.Y goo1abc-hs.gpfs.net goo1abc-hs
			gssgennetworks -N foo1, goo1 --suffix=abc-hs --create-bond

Running **gssutils** over PuTTY might shows horizontal lines as “qqq” and vertical lines as “xxx”.	ESS Install and Deployment Toolkit Type: Install or Upgrade Version: Advanced or Standard Arch: Big Endian or Little Endian Affected Nodes: EMS and I/O server nodes	PuTTY translation default Remote Character set UTF-8 might not translate horizontal line and vertical character sets correctly.	1. On the PuTTY terminal Window > Translation, change Remote character set from UTF-8 to ISO-8859-1:1998 (Latin-1, West Europe) (this should be first option after UTF-8). 2. Open session.

Table 2. Known issues in ESS 5.1.x (continued)

Issue	Environment affected	Description	Resolution or action
gssinstallcheck might flag an error regarding page pool size in multi-building block situations if the physical memory sizes differ.	Software Validation Type: Install or Upgrade Arch: Big Endian or Little Endian Version: Advanced or Standard Affected nodes: I/O server nodes	**gssinstallcheck** is a tool introduced in ESS 3.5, that helps validate software, firmware, and configuration settings. If adding (or installing) building blocks of a different memory footprint installcheck will flag this as an error. Best practice states that your I/O servers must all have the same memory footprint, thus pagepool value. Page pool is currently set at ~60% of physical memory per I/O server node. Example from **gssinstallcheck**: [ERROR] pagepool: found 142807662592 expected range 147028338278 - 179529339371	1. Confirm each I/O server node's individual memory footprint. From the EMS, run the following command against your I/O xCAT group: **xdsh gss_ppc64 "cat/ proc/meminfo | grep MemTotal"** **Note:** This value is in KB.If the physical memory varies between servers and/or building blocks, consider adding memory and re-calculating pagepool to ensure consistency. 2. Validate the pagepool settings in IBM Spectrum Scale: **mmlsconfig | grep -A 1 pagepool** **Note:** This value is in MB. If the pagepool value setting is not roughly ~60% of physical memory, then you must consider recalculating and setting an updated value. For information about how to update the pagepool value, see IBM Spectrum Scale documentation on IBM Knowledge Center.
Syslog might indicate `systemd` errors related to disk devices appearing twice with different `sysfs` paths.	Message logging Type: Install or Upgrade Arch: Big Endian or Little Endian Version: Advanced or Standard Affected nodes: I/O server nodes	On a running system, syslog (journal or dmesg) might show a flood of warnings related to enclosure disks appearing twice with different sysfs paths. This is simply a warning and has no effect on system operation. Suppressing the messages is important to keeping the system clean of invalid issues. Updating systemd resolves this problem.	To resolve this issue, connect your nodes to the Red Hat network (RHN) using the supplied license. Update the following RHBA (or higher for systemd): https://rhn.redhat.com/errata/RHBA-2017-1311.html **yum update --advisory=RHBA-2017-1311**

Table 2. Known issues in ESS 5.1.x (continued)

Issue	Environment affected	Description	Resolution or action
The GUI might display the long-waiters warning: `Spectrum Scale long-waiters monitoring returned unknown result`	GUI Type: Upgrade Arch: Big Endian Version: Advanced or Standard Affected nodes: ALL	Upon new installs (or upgrades) to ESS 5.1.x, the GUI might show an error due to a bad return code from **mmhealth** in its querying of long-waiters information. `/usr/lpp/mmfs/bin/mmdiag --deadlock Failed to connect to file system daemon: No such process RC=50`	There is no current workaround but it is advised to verify on the command line that no long-waiters exist. If the system is free from this symptom, mark the event as read on the GUI by clicking under the Action column. Doing so will clear the event.
Creating small file systems in the GUI (below 16G) will result in incorrect sizes	GUI Type: Install or Upgrade Arch: Big Endian or Little Endian Version: Advanced or Standard Affected nodes: ALL	When creating file systems in the GUI smaller than 16GB (usually done to create CES_ROOT for protocol nodes) the size will come out larger than expected. **gssgenvdisks** also has this problem for those used to the command-line method of creating file systems.	There is currently no resolution. The smallest size you might be able to create is 16GB. Experienced users may consider creating a customer `vdisk.stanza` file for specific sizes you require.
Creating file systems in the GUI might immediately result in lack of capacity data	GUI Type: Install or Upgrade Arch: Big Endian or Little Endian Version: Advanced or Standard Affected nodes: ALL	When creating file systems in the GUI you might not immediately see the capacity data show up.	You may wait up to 24 hours for the capacity data to display or simply visit the command line which should accurately show the file system size.

Table 2. Known issues in ESS 5.1.x (continued)

Issue	Environment affected	Description	Resolution or action

The GUI might show 'unknown' hardware states for storage enclosures and Power 8 servers in the ESS building block.
Part info and firmware levels under the **Hardware Details** panel might also be missing.
	GUI
	Type: Upgrade
	Arch: Big Endian
	Version: Advanced or Standard
	Affected nodes: ALL
		The ESS GUI (running on the EMS) might show 'unknown' under the Hardware panel for the ESS building block members.
		
		The ESS GUI might also be missing information under Part Info and Firmware version within the **Hardware Details** panel.
			The workaround for this issue is the following:
			1. Login to the EMS
			2. Run the following in order:
			`/usr/lpp/mmfs/gui/cli/runtask RECOVERY_GROUP`
			`/usr/lpp/mmfs/gui/cli/runtask DISK_ENCLOSURES`
			`/usr/lpp/mmfs/gui/cli/runtask ENCLOSURE_FW`
			`/usr/lpp/mmfs/gui/cli/runtask CHECK_FIRMWARE`
			
			After running, the GUI should refresh with the issues resolved.

Canceling disk replacement through GUI leaves original disk in unusable state	GUI Type: Install or Upgrade Arch: Big Endian or Little Endian Version: Advanced or Standard Affected nodes: NA	Canceling a disk replacement can lead to an unstable system state and must not be performed. However, if you did this operation, use the provided workaround.	Do not cancel disk replacement from the GUI. However, if you did, then use the following command to recover the disk took state: **`mmchpdisk <RG> --pdisk <pdisk> --resume`**
Under **Monitoring** > **Hardware details**, you might see enclosures missing location information.	GUI Type: Install or Upgrade Arch: Big Endian or Little Endian Version: Advanced or Standard Affected nodes: NA	After install or upgrade to ESS 5.1.x, you might see missing location information for the enclosures in your system. This is not reflective of the true frame U location which can be observed in the **Monitoring** > **Hardware details** panel.	The current workaround is to wait up to 24 hours for the GUI services to refresh. After this period you will see the enclosure location information fill in.
The GUI wizard might start again after completing the initial setup.	GUI Type: Install Arch: Big Endian Version: Advanced or Standard Affected nodes: NA	After completing the GUI wizard setup on ESS 5.1.x Big Endian, you might see the start screen again.	If you see the GUI wizard start screen a second time, type the address of the EMS into the browser and press enter. https://<ip of EMS over management network> You will then be taken to the GUI home screen.

Table 2. Known issues in ESS 5.1.x (continued)

Issue	Environment affected	Description	Resolution or action
Upon upgrades to ESS 5.1.x Big Endian, you might notice missing pools and users in the **Monitoring** > **Capacity** GUI panel	GUI Type: Upgrade Arch: Big Endian Version: Advanced or Standard Affected nodes: NA	You might notice one or more missing pools or users after upgrading to ESS 5.1.x Big Endian in the **Monitoring** > **Capacity** GUI panel. You may also see missing capacity and throughput data under the **Monitoring** > **Nodes** panel.	There is currently no resolution or workaround.Try waiting 24 hours for the GUI to refresh. To confirm your pools are available, run the **mmlspool <filesystem>** command.
Upon upgrades to ESS 5.1.x Big Endian, you might see nodes in the degraded state yet no events show any issue.	GUI Type: Upgrade Arch: Big Endian Version: Advanced or Standard Affected nodes: I/O server nodes	Under the **Monitoring** > **Nodes** panel, you might see your I/O server nodes in the degraded state. Upon clicking each node, you will notice no serviceable events.	There is currently no resolution or workaround.Try waiting 24 hours for the GUI to refresh its internal data.

Appendix B. Networking requirements for ESS

This topic describes the networking requirements for installing ESS.

Note: The references to HMC are not applicable for the PPC64LE platform.

Networking requirements

The following networks are required:

- **Service network**

  This network connects the flexible service processor (FSP) on the management server and I/O server nodes (with or without the HMC, depending on the platform) as shown in blue in Figure 1 and 2 on the following pages.
- **Management and provisioning network**

  This network connects the management server to the I/O server nodes (and HMCs, if available) as shown in yellow in in Figure 1 and 2 on the following pages. The management server runs DHCP on the management and provisioning network. If a management server is not included in the solution order, a customer-supplied management server is used.
- **Clustering network**

  This high-speed network is used for clustering and client node access. It can be a 10 Gigabit Ethernet (GbE), 40 GbE, or InfiniBand network. It might not be included in the solution order.
- **External and campus management network**

  This public network is used for external and campus management of the management server, the HMC (if available), or both.

Figure 1, Network Topology, is a high-level logical view of the management and provisioning network and the service network for an ESS building block (on **PPC64BE**) .

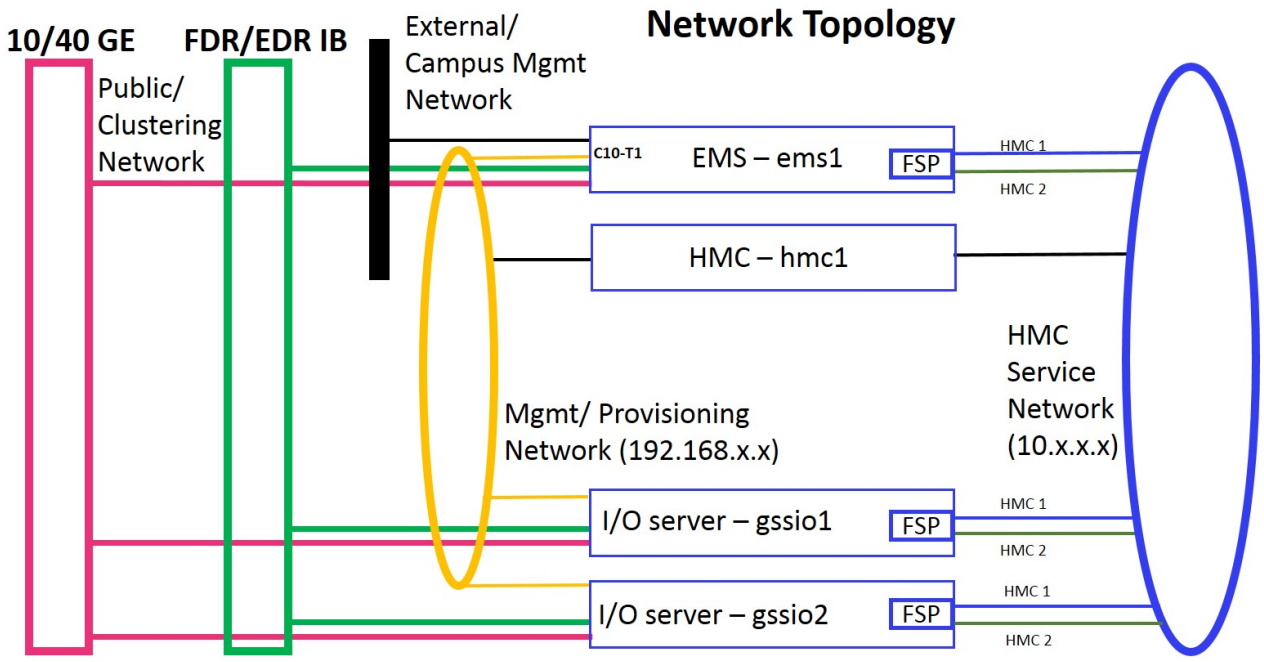

Figure 1. The management and provisioning network and the service network: a logical view (on **PPC64BE***)*

Figure 2, Network Topology, is a high-level logical view of the management and provisioning network and the service network for an ESS building block (on **PPC64LE**).

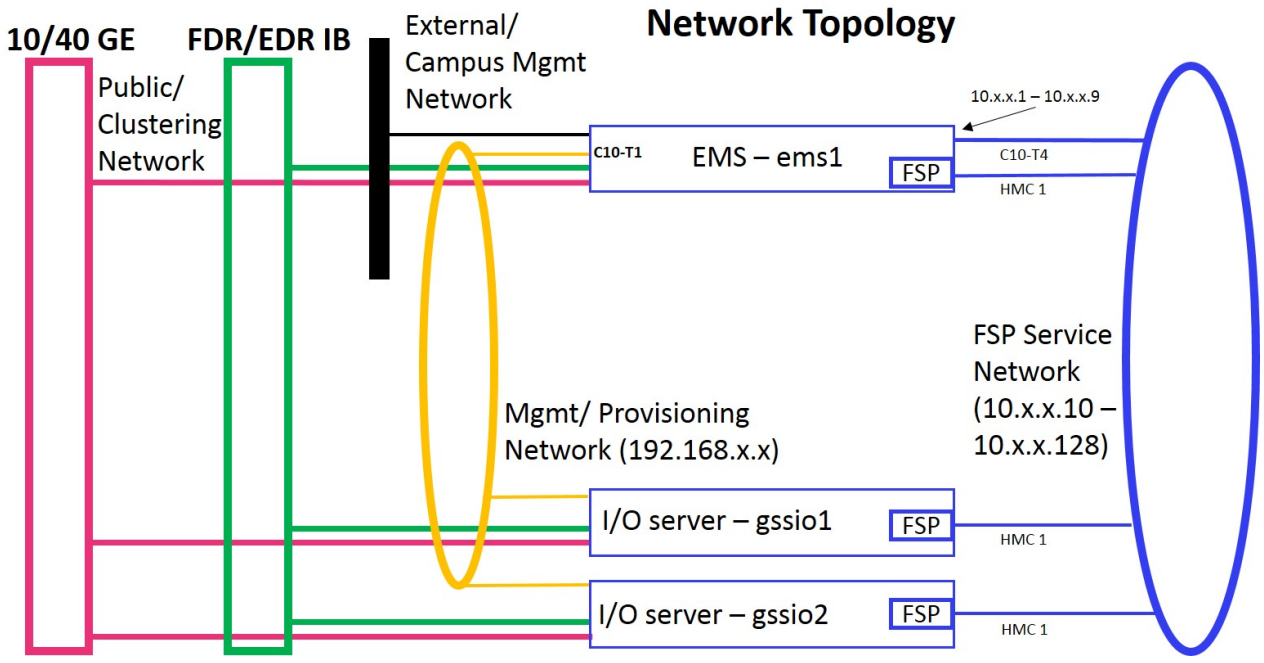

Figure 2. The management and provisioning network and the service network: a logical view (on **PPC64LE***)*

The management and provisioning network and the service network must run as two non-overlapping networks implemented as two separate physical networks or two separate virtual local-area networks (VLANs).

The HMC, the management server, and the switches (1 GbE switches and high-speed switches) might not be included in a solution order in which an existing or customer-supplied HMC or management server is used. Perform any advance planning tasks that might be needed to access and use these solution components.

Appendix C. Pre-installation tasks for ESS

This topic provides the pre-installation tasks required for ESS.

Note: The references to HMC are not applicable for the PPC64LE platform.

Table 3. Pre-installation tasks

ESS component	Description	Required actions	System settings
1. Service network **Note:** This network varies depending on the platform (PPC64BE or PPC64LE).	**HMC service network:** This private network connects the HMC with the management server's FSP and the I/O server nodes. The service network must not be seen by the OS running on the node being managed (that is, the management server or the I/O server node). The HMC uses this network to discover the management server and the I/O server nodes and perform such hardware management tasks as creating and managing logical partitions, allocating resources, controlling power, and rebooting. **Note:** HMC is not applicable for the PPC64LE platform. **FSP service network:** This private network connects the FSP interface on EMS and the I/O server nodes. The service network must be seen by the OS running on the EMS node but not by the I/O server nodes being managed.	Perform any advance planning tasks that might be needed to access and use the HMC if it is not part of the solution order and a customer-supplied HMC will be used. Set up this network if it has not been set up already.	Set the HMC to be the DHCP server for the service network.
2. Management and provisioning network	This network connects the management server node with the HMC (when present) and the I/O server nodes. It typically runs over 1Gb. • This network is visible to the OS that is running on the nodes. • The management server uses this network to communicate with the HMC (when present) and to discover the I/O server nodes. • The management server will be the DHCP server on this network. There cannot be any other DHCP server on this network. • This network is also used to provision the node and therefore deploy and install the OS on the I/O server nodes.	Perform any advance planning tasks that might be needed to access and use the management server if it is not part of the solution order and a customer-supplied management server will be used. Set up this network if it has not been set up already.	
3. Clustering network	This network is for high-performance data access. In most cases, this network is also part of the clustering network. It is typically composed of 10GbE, 40GbE, or InfiniBand networking components.	Set up this network if it has not been set up already.	

Table 3. Pre-installation tasks (continued)

ESS component	Description	Required actions	System settings
4. Management network domain	The management server uses this domain for the proper resolution of hostnames.	Set the domain name using *lowercase* characters. Do *not* use any uppercase characters.	Example: `gpfs.net`
5. HMC node (IP address and hostname) **Note:** HMC is not applicable for the PPC64LE platform.	The IP address of the HMC node on the management network has a console name, which is the hostname and a domain name. • This IP address must be configured and the link to the network interface must be up. • The management server must be able to reach the HMC using this address.	Set the fully-qualified domain name (FQDN) and the hostname using *lowercase* characters. Do *not* use any uppercase characters. Do *not* use a suffix of `-en`*x*, where *x* is any character. Do *not* use an _ (underscore) in the hostname.	Example: IP address: `192.168.45.9` Hostname: `hmc1` FQDN: `hmc1.gpfs.net`
6. Management server node (IP address)	The IP address of the management server node has an FQDN and a hostname. • This IP address must be configured and the link to the network interface must be up. • The management network must be reachable from this IP address.	Set the FQDN and hostname using *lowercase* characters. Do *not* use any uppercase characters. Do *not* use a suffix of `-en`*x*, where *x* is any character. Do *not* use an _ (underscore) in the hostname.	Example: IP address: `192.168.45.10` Hostname: `ems1` FQDN: `ems1.gpfs.net`
7. I/O server nodes (IP addresses)	The IP addresses of the I/O server nodes have FQDNs and hostnames. • These addresses are assigned to the I/O server nodes during node deployment. • The I/O server nodes must be able to reach the management network using this address.	Set the FQDN and hostname using *lowercase* characters. These names must match the name of the partition created for these nodes using the HMC. Do *not* use any uppercase characters. Do *not* use a suffix of `-en`*x*, where *x* is any character. Do *not* use an _ (underscore) in the host name.	Example: I/O server 1: IP address: `192.168.45.11` Hostname: `gssio1` FQDN: `gssio1.gpfs.net` I/O server 2: IP address: `192.168.45.12` Hostname: `gssio2` FQDN: `gssio2.gpfs.net`
8. Management server node management network interface (PPC64BE) Management server node FSP network interface (PPC64LE)	The management network interface of the management server node must have the IP address that you set in item 6 assigned to it. This interface must have only one IP address assigned. For the PPC64LE system, one additional interface is assigned to FSP network. This interface must have only one IP address assigned.	To obtain this address, run: `ip addr`	Example: `enP7p128s0f0`

Table 3. Pre-installation tasks (continued)

ESS component	Description	Required actions	System settings
9. HMC (**hscroot** password) **Note:** HMC is not applicable for the PPC64LE platform.		Set the password for the **hscroot** user ID.	Example: `abc123` This is the default password.
10. I/O servers (user IDs and passwords)	The user IDs and passwords of the I/O servers are assigned during deployment.		Example: User ID: `root` Password: `cluster` (this is the default password)
11. FSP IPMI password	The IPMI password of the FSP. FSP IPMI of all the nodes assumed to be identical.		Example: `PASSW0RD`
12. Clustering network (hostname prefix or suffix)	This high-speed network is implemented on a 10Gb Ethernet, 40Gb Ethernet or InfiniBand network.	Set a hostname for this network. It is customary to use hostnames for the high-speed network that use the prefix and suffix of the actual hostname. Do *not* use a suffix of `-en`*x*, where *x* is any character.	Examples: Suffixes: `-bond0`, `-ib`, `-10G`, `-40G` Hostnames with a suffix: `gssio1-ib`, `gssio2-ib`
13. High-speed cluster network (IP address)	The IP addresses of the management server nodes and I/O server nodes on the high-speed cluster network have FQDNs and hostnames. In the example, `172.10.0.11` is the IP address that the GPFS daemon uses for clustering. The corresponding FQDN and hostname are `gssio1-ib` and `gssio1-ib.data.net`, respectively.	Set the FQDNs and hostnames. Do *not* make changes in the `/etc/hosts` file for the high-speed network until the deployment is complete. Do *not* create or enable the high-speed network interface until the deployment is complete.	Example: Management server: IP address: `172.10.0.10` Hostname: `ems1-ib` FQDN: `ems1-ib.gpfs.net` I/O server 1: IP address: `172.10.0.11` Hostname: `gssio1-ib` FQDN: `gssio1-ib.data.net` I/O server 2: IP address: `172.10.0.12` Hostname: `gssio2-ib` FQDN: `gssio2-ib.data.net`

Table 3. Pre-installation tasks (continued)

ESS component	Description	Required actions	System settings
14. Red Hat Enterprise Linux 7.2	The Red Hat Enterprise Linux 7.2 DVD or ISO file is used to create a temporary repository for the xCAT installation. xCAT uses it to create a Red Hat Enterprise Linux repository on the management server node.	Obtain this DVD or ISO file and download. For more information, see the Red Hat Enterprise Linux website: **http://access.redhat.com/products/red-hat-enterprise-linux/**	Example: `RHEL-7.2-20150219.1-Server-ppc64-dvd1.iso` **Note:** The Red Hat Enterprise Linux 7.2 ISO name depends on the architecture (PPC64BE or PPC64LE).
15. Management network switch	The switch that implements the management network must allow the Bootstrap Protocol (BOOTP) to go through.	Obtain the IP address and access credentials (user ID and password) of this switch. Some switches generate many Spanning Tree Protocol (STP) messages, which interfere with the network boot process. You need to disable STP to mitigate this.	
16. Target file system	You need to provide information about the target file system that is created using storage in the ESS building blocks. This information includes name, block size, file system size, RAID code, etc. This information you is passed on to **gssgenvdisks** to create the customer file system.	Set the target file system name, the mount point, the block size, the number of data NSDs, and the number of metadata NSDs.	Example: `Block size = 8M, #datansd=4, #metadatansd=2`

Appendix D. Installation: reference

This topic provides information on creating a bonded interface with Ethernet, adding IBM Spectrum Scale nodes to an ESS cluster, and node name considerations.

bonded interface

A bonded interface with Ethernet

Starting with ESS 3.5, you can use a script to help you quickly create a bonded interface with Ethernet. See the man page for the **gssgennetworks** command for more information. Otherwise, complete the following steps.

Connect the network cables to the corresponding switch. Check that the links are up at the device level. To create a bonding, add connections for the master, add connections for the slave, bring up the connection for the slaves, and then bring up the connection for the master (bond). Run:

```
ibdev2netdev
```

The system displays output similar to this:

```
[root@gssio2 ~]# ibdev2netdev

mlx4_0 port 1 ==> enp1s0 (Up)
mlx4_0 port 2 ==> enp1s0d1 (Up)
mlx5_0 port 1 ==> ib0 (Down)
mlx5_0 port 2 ==> ib1 (Down)
mlx5_1 port 1 ==> ib2 (Down)
mlx5_1 port 2 ==> ib3 (Down)
```

This example shows two 10GbE network ports that are up and are connected to the switch properly. Now you will create a bond with these two ports.

Check the connection and make sure there are no connections defined for these ports. You can do this using network manager connection and device commands.

To check the connection, run:

```
nmcli -p c
```

The system displays output similar to this:

```
[root@gssio2 ~]# nmcli -p c

================================================================================
                        NetworkManager connection profiles
================================================================================
NAME             UUID                                  TYPE            DEVICE
--------------------------------------------------------------------------------
enp1s0d1         6d459dc7-db53-43d4-9236-8257ee900aae  802-3-ethernet  --
enP7p128s0f2     72b6533e-6eaa-4763-98fa-0b4ed372e377  802-3-ethernet  --
enP7p128s0f3     1b0a97e7-1b90-4d26-89cf-8f4fc8e5a00e  802-3-ethernet  --
enP7p128s0f1     5dffee0e-b0b6-4472-864e-acc2dc0cc043  802-3-ethernet  --
enp1s0           060d342f-3388-4e9f-91bb-13c3aa30847f  802-3-ethernet  --
GSS enP7p128s0f0 5f755525-2340-7e18-ef9d-0d4bfdba4c30  802-3-ethernet  enP7p128s0f0
```

To check the device, run:

```
nmcli -p d
```

The system displays output similar to this:

```
[root@gssio2 ~]# nmcli -p d

============================================================
                    Status of devices
============================================================
DEVICE        TYPE        STATE         CONNECTION
------------------------------------------------------------
enP7p128s0f0  ethernet    connected     GSS enP7p128s0f0
enP7p128s0f1  ethernet    disconnected  --
enP7p128s0f2  ethernet    disconnected  --
enP7p128s0f3  ethernet    disconnected  --
enp1s0        ethernet    disconnected  --
enp1s0d1      ethernet    disconnected  --
ib0           infiniband  disconnected  --
ib1           infiniband  disconnected  --
ib2           infiniband  disconnected  --
ib3           infiniband  disconnected  --
lo            loopback    unmanaged     --
```

As you can see, there is no connection defined for the devices and the device state is down. Add a connection for the bond `bond0`. In this case, specify `802.3ad` for the Link Aggregation Control Protocol (LACP) and an IPv4 address of `172.16.45.22/24`. For the bonding parameters, specify a `miimon` value of 100 milliseconds (msec).

```
[root@gssio2 ~]# nmcli c add type bond ifname bond0 miimon 100 mode 802.3ad ip4 172.16.45.22/24

Connection 'bond-bond0' (c929117b-6d92-488d-8bcb-d98e7e0c8b91) successfully added.
```

Note that by default, `xmit_hash_policy` is set to `layer2`. For optimal performance, you might want to set it to `layer3+4`, as follows:

```
nmcli c mod bond-bond0 +bond.option xmit_hash_policy=layer3+4
```

To view the connection properties, run:

```
nmcli c show bond-bond0
```

Add connections for the slaves:

```
[root@gssio2 ~]# nmcli c add type bond-slave ifname enp1s0 master bond0

Connection 'bond-slave-enp1s0' (d9e21d55-86ea-4551-9371-1fc24d674751) successfully added.

[root@gssio2 ~]# nmcli c add type bond-slave ifname enp1s0d1 master bond0

Connection 'bond-slave-enp1s0d1' (8432645a-5ddc-44fe-b5fb-2884031c790c) successfully added.
```

Bring the connection up for the slaves:

```
[root@gssio2 ~]# nmcli c up bond-slave-enp1s0d1

Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/4)

[root@gssio2 ~]# nmcli c up bond-slave-enp1s0

Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/6)
```

Bring the connection up for bond-bond0:

```
[root@gssio2 ~]# nmcli c up bond-bond0

Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/7)
```

Finally, make sure the appropriate bond devices have been created:

```
[root@gssio2 ~]# cat /proc/net/bonding/bond0

Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: IEEE 802.3ad Dynamic link aggregation
Transmit Hash Policy: layer2 (0)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

802.3ad info
LACP rate: slow
Min links: 0
Aggregator selection policy (ad_select): stable
Active Aggregator Info:
      Aggregator ID: 1
      Number of ports: 1
      Actor Key: 33
      Partner Key: 1
      Partner Mac Address: 00:00:00:00:00:00

Slave Interface: enp1s0
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: f4:52:14:df:af:74
Aggregator ID: 1
Slave queue ID: 0

Slave Interface: enp1s0d1
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: f4:52:14:df:af:75
Aggregator ID: 2
Slave queue ID: 0
```

Changing the MTU

To change the maximum transmission unit (MTU), follow these steps:

1. Create a file, copy the following script into it, and save the file in the `/etc/NetworkManager/dispatcher.d` directory of the nodes where bonding is run If the executable (**x**) bit gets reset, use **chmod +x** to make the file executable. The `/opt/ibm/gss/tools/samples` directory includes the **mtuset** script for your use.

```
#!/bin/sh
INTERFACE_NAME_REGEX="^bond?"
if [[ $CONNECTION_ID =~ $INTERFACE_NAME_REGEX ]]; then
        if [[ $2 == up ]]; then
                MTU=$(awk -F "=" '($1 ~ "^MTU") {print $NF}' /etc/sysconfig/network-scripts/
ifcfg-$CONNECTION_ID)
                if [[ $MTU > 0 ]] && [[ $MTU != 1500 ]]; then
                        logger -s "Setting MTU of $CONNECTION_ID to $MTU..."
                        if /usr/sbin/ip link set dev $1 mtu $MTU ; then
                                logger "Successfully set MTU of $CONNECTION_ID to $MTU"
                        else
                                logger "Failed to set MTU of $CONNECTION_ID to $MTU"
                        fi
                fi
        fi
fi
```

See **https://access.redhat.com/solutions/1309583** for more information.

2. Add the MTU parameter value to the bond's interface configuration file. To set an MTU of 9000, specify:

   ```
   MTU=9000
   ```

   For example, add **MTU=9000** to `ifcfg-bond-bond0`, `ifcfg-bond-slave-xxxx`, and `ifcfg-bond-slave-yyyy`. The script shown in the previous step checks for the MTU setting and uses **ip link set** to set them appropriately. The script assumes that the bond connection starts with `bond?-xxxx`. Make changes in the scripts as needed.

3. To enable the network manager dispatch service in each node, run these commands:

   ```
   [root@gssio2 network-scripts]# systemctl enable NetworkManager-dispatcher.service
   [root@gssio2 network-scripts]# systemctl start NetworkManager-dispatcher.service
   ```

4. To restart networking, run:

   ```
   systemctl reboot
   ```

   While restarting networking, you could lose the connection to the I/O server nodes. Use **rcons** to establish the console connection, if needed.

   a. Open a console to each node. For example, run:

      ```
      rcons gssio1
      ```

      If **rcons** does not open, the console server is probably not running. To restart it at the management server node, run:

      ```
      makeconservercf NodeName
      ```

      or

      ```
      makeconservercf NodeGroup
      ```

      Log in to the console. The default user ID is **root** and the default password is **cluster**.

   b. To disconnect from the console server, press **<Ctrl-e> c .** (period).

Bonding with InfiniBand

Connect the InfiniBand cables to the corresponding switch. Check that the links are up at the device level. To create a bonding, add connections for the master and for the slave. You will have to modify the network script file and reload the connections in Network Manager. After the connections are reloaded, bonding should be available. When the system is restarted or rebooted, it could take some time (more than five minutes) before the bonding interface is ready. Check the device status on each node to make sure all of the links are up. Run:

```
ibdev2netdev
```

The system displays output similar to this:

```
[root@gssio2 ~]# ibdev2netdev

mlx5_0 port 1 ==> ib0 (Up)
mlx5_0 port 2 ==> ib1 (Up)
mlx5_1 port 1 ==> ib2 (Up)
mlx5_1 port 2 ==> ib3 (Up)
mlx5_2 port 1 ==> ib4 (Up)
mlx5_2 port 2 ==> ib5 (Up)
```

You can also use **ibstat**.

Check the connection using `nmcli c` and make sure there is no existing bond already defined in these interfaces. Add the bond connection first. In this example, active-backup mode is selected. In IP over InfiniBand (IPoIB), only active-backup bond is supported. Run:

```
nmcli c add type bond ifname bond0 mode
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]# nmcli c add type bond ifname bond0 mode

active-backup ip4 172.16.45.22/24
Connection 'bond-bond0' (66f182d1-d0da-42cf-b4c9-336d5266bbe7) successfully
added.
```

Add the slave connections as follows. In this example, `ib0` and `ib1` are the slave devices. Make appropriate changes as needed. First, run:

```
nmcli c add type bond-slave ifname ib0 master bond0
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]#  nmcli c add type bond-slave ifname ib0 master bond0

Connection 'bond-slave-ib0' (86c0af63-4b6c-475c-a724-0fb074dc9092) successfully added.
```

Next, run:

```
nmcli c add type bond-slave ifname ib1 master bond0
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]#  nmcli c add type bond-slave ifname ib1 master bond0

Connection 'bond-slave-ib1' (1d0cb5c3-268d-487c-9e40-7c0cf268150f) successfully added.
```

To check the connections, run:

```
nmcli c
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]# nmcli c

NAME              UUID                                  TYPE            DEVICE
GSS enP7p128s0f0  5f755525-2340-7e18-ef9d-0d4bfdba4c30  802-3-ethernet  enP7p128s0f0
bond-slave-ib1    1d0cb5c3-268d-487c-9e40-7c0cf268150f  802-3-ethernet  --
bond-slave-ib0    86c0af63-4b6c-475c-a724-0fb074dc9092  802-3-ethernet  --
bond-bond0        66f182d1-d0da-42cf-b4c9-336d5266bbe7  bond            bond0
enP7p128s0f1      2eb8617f-5c7d-4d68-a7fe-88a030fdb28b  802-3-ethernet  --
enP7p128s0f3      7dea32aa-caa1-4016-9414-a47c62de27e9  802-3-ethernet  --
enP7p128s0f2      4416229e-2233-414f-b3ad-929c54c15f27  802-3-ethernet  --
```

You can see that the slave connections are created, but there are no devices for these connections.

To check the devices, run:

```
nmcli d
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]# nmcli d

DEVICE        TYPE        STATE         CONNECTION
bond0         bond        connected     bond-bond0
enP7p128s0f0  ethernet    connected     GSS enP7p128s0f0
enP7p128s0f1  ethernet    disconnected  --
enP7p128s0f2  ethernet    disconnected  --
enP7p128s0f3  ethernet    disconnected  --
ib0           infiniband  disconnected  --
ib1           infiniband  disconnected  --
ib2           infiniband  disconnected  --
```

```
ib3           infiniband  disconnected  --
ib4           infiniband  disconnected  --
ib5           infiniband  disconnected  --
lo            loopback    unmanaged     --
```

The devices `ib0` and `ib1` are disconnected (this is the view from Network Manager).

Check `/etc/sysconfig/network-scripts` directory for the network script for each of the connections that were just created.

```
-rw-r--r--  1 root root   354 Jan 19 04:12 ifcfg-bond-bond0
-rw-r--r--  1 root root   121 Jan 19 04:12 ifcfg-bond-slave-ib0
-rw-r--r--  1 root root   121 Jan 19 04:12 ifcfg-bond-slave-ib1
```

You need to make some changes to the slave connection scripts (`ifcfg-bond-slave-ib0` and `ifcfg-bond-slave-ib1`). In most cases, the master bond interface script remains unchanged:

```
cat ifcfg-bond-bond0
```

```
DEVICE=bond0
BONDING_OPTS=mode=active-backup
TYPE=Bond
BONDING_MASTER=yes
BOOTPROTO=none
IPADDR0=172.16.45.22
PREFIX0=24
GATEWAY0=172.6.45.20
DEFROUTE=yes
NAME=bond-bond0
UUID=66f182d1-d0da-42cf-b4c9-336d5266bbe7
ONBOOT=yes
```

Modify the first slave-bond interface script as indicated in bold typeface:

```
TYPE=Infiniband                 <= change from Ethernet to Infiniband
NAME=bond-slave-ib0
UUID=86c0af63-4b6c-475c-a724-0fb074dc9092
DEVICE=ib0
ONBOOT=yes
MASTER=bond0
SLAVE=yes
NM_CONTROLLED=yes               <= add this line
```

Modify the second slave-bond interface script as indicated in bold typeface:

```
TYPE=Infiniband                 <= change from Ethernet to Infiniband
NAME=bond-slave-ib1
UUID=1d0cb5c3-268d-487c-9e40-7c0cf268150f
DEVICE=ib1
ONBOOT=yes
MASTER=bond0
SLAVE=yes
NM_CONTROLLED=yes               <= add this line
```

Now reload the connections:

```
[root@gssio2 network-scripts]# nmcli c reload
```

To check the connections, run:

```
nmcli c
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]# nmcli c
```

```
NAME              UUID                                  TYPE            DEVICE
GSS enP7p128s0f0  5f755525-2340-7e18-ef9d-0d4bfdba4c30  802-3-ethernet  enP7p128s0f0
```

```
bond-slave-ib1    1d0cb5c3-268d-487c-9e40-7c0cf268150f  infiniband      ib1
bond-slave-ib0    86c0af63-4b6c-475c-a724-0fb074dc9092  infiniband      ib0
bond-bond0        66f182d1-d0da-42cf-b4c9-336d5266bbe7  bond            bond0
enP7p128s0f1      2eb8617f-5c7d-4d68-a7fe-88a030fdb28b  802-3-ethernet  --
enP7p128s0f3      7dea32aa-caa1-4016-9414-a47c62de27e9  802-3-ethernet  --
enP7p128s0f2      4416229e-2233-414f-b3ad-929c54c15f27  802-3-ethernet  --
```

Now you can see that the bond slave connections have devices assigned to them.

To check the devices, run:

```
nmcli d
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]# nmcli d

DEVICE        TYPE        STATE         CONNECTION
bond0         bond        connected     bond-bond0
enP7p128s0f0  ethernet    connected     GSS enP7p128s0f0
ib0           infiniband  connected     bond-slave-ib0
ib1           infiniband  connected     bond-slave-ib1
enP7p128s0f1  ethernet    disconnected  --
enP7p128s0f2  ethernet    disconnected  --
enP7p128s0f3  ethernet    disconnected  --
ib2           infiniband  disconnected  --
ib3           infiniband  disconnected  --
ib4           infiniband  disconnected  --
ib5           infiniband  disconnected  --
lo            loopback    unmanaged     --
```

This shows that devices `ib0` (connection name: `bond-slave-ib0`) and `ib1` (connection name: `bond-slave-ib1`) are now connected.

To check the `bond0` state in the `proc` file system, run:

```
cat /proc/net/bonding/bond0
```

The system displays output similar to this:

```
[root@gssio2 network-scripts]# cat /proc/net/bonding/bond0

Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup) (fail_over_mac active)
Primary Slave: None
Currently Active Slave: ib0
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: ib0
MII Status: up
Speed: 40000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: a0:00:00:27:fe:80
Slave queue ID: 0

Slave Interface: ib1
MII Status: up
Speed: 40000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: a0:00:00:29:fe:80
Slave queue ID: 0
```

To ping the other node on the same bonded network, run:

```
ping 172.16.45.22
```

The system displays output similar to this:

```
[root@gssio1 ~]# ping 172.16.45.22

PING 172.16.45.22 (172.16.45.22) 56(84) bytes of data.
64 bytes from 172.16.45.22: icmp_seq=1 ttl=64 time=8.52 ms
64 bytes from 172.16.45.22: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 172.16.45.22: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 172.16.45.22: icmp_seq=4 ttl=64 time=0.042 ms
64 bytes from 172.16.45.22: icmp_seq=5 ttl=64 time=0.043 ms
64 bytes from 172.16.45.22: icmp_seq=6 ttl=64 time=0.040 ms
```

Adding IBM Spectrum Scale nodes to an ESS cluster

IBM Spectrum Scale node configuration is optimized for running IBM Spectrum Scale RAID functions.

1. ESS cluster node configuration is optimized for running IBM Spectrum Scale RAID functions. Protocols, other gateways, or any other non-ESS services must not be run on ESS management server nodes or I/O server nodes. In a cluster with high IO load, avoid using ESS nodes as cluster manager or filesystem manager. For optimal performance the NSD client nodes accessing ESS nodes should be properly configured. ESS ships with **gssClientConfig.sh script** located in `/usr/lpp/mmfs/samples/gss/` directory. This script can be used to configure the client as follows:

   ```
   /usr/lpp/mmfs/samples/gss/gssClientConfig.sh <Comma Separated list of
   client nodes or nodeclass>
   ```

   You can run the following to see configuration parameter settings without setting them:

   ```
   /usr/lpp/mmfs/samples/gss/gssClientConfig.sh -D
   ```

   After running this script, restart GPFS on the affected nodes for the optimized configuration settings to take effect.
2. When IBM Spectrum Scale nodes deployed with protocols are added to the ESS cluster, quorum, cluster manager, and filesystem manager functions should be moved from the ESS to the protocol nodes after adding protocol nodes to the cluster.

For information about adding an IBM Spectrum Scale protocol node to an ESS cluster, see:

- Overview of the IBM Spectrum Scale installation toolkit
- Preparing a cluster that contains ESS for adding protocols
- Spectrum Scale Protocols Quick Overview

Node name considerations

Carefully select the hostname, suffix, and prefix of the management server and I/O server so that the hostname used in the high-speed network and by the ESS cluster can be generated from the suffix or prefix.

High-speed hostnames

Example 1:

```
a-bcd-edf-1
a-bcd-edf-2
a-bcd-edf-3
a-bcd-edf-4
```

Here, `a-bcd-` is the prefix and `edf-1`, `edf-2`, `edf-3`, and `edf-4` are the xCAT names of the nodes.

Example 2:

```
1-a-bcd-edf
2-b-bcd-edf
3-c-bcd-edf
4-d_bcd_edf
```

Here, `-edf` is the suffix and `1-a-bcd`, `2-a-bcd`, `3-a-bcd`, and `4-a-bcd` are the xCAT names of the nodes.

If possible, avoid using high-speed node names with variations at the beginning and the end, such as:

```
A-a-bcd-edf-1
B-b-bdc-edf-2
C-c-bcd-edf-3
D-d-bcd-edf-4
```

In such cases, use the **-N** option and specify the node list with the **gssgencluster** and **gssgenclusterrgs** commands. The node names must be reachable from the management server node. xCAT requires that the target nodes be part of a node group and a warning might be issued if the hostname is not defined as an xCAT object.

Example:

1. The xCAT hostnames are **gssio1**, **gssio2**, **gssio3**, and **gssio4**.
2. The high-speed hostnames are **A-test1**, **B-test2**, **C-test3**, **D-test4**. These hostnames are reachable from the management server node. They are not defined in xCAT.

Run:

```
gssgencluster -C test01 -N A-test1,B-test2,C-test3,D-test4
```

Appendix E. Updating the system firmware

Use this information to obtain and apply the system firmware updates.

The system firmware packages are available in the `/opt/ibm/gss/install/firmware` directory of the management server node in newly shipped systems.

- System firmware update files for PPC64BE for updating using HMC:

  ```
  01SV860_103_056.xml
  01SV860_103_056.rpm
  ```

- System firmware update file for PPC64LE for updating using the command line:

  ```
  01SV860_103_056.img
  ```

You can obtain the firmware update packages as follows:

1. Go to the FixCentral website.
2. Download the POWER8 System Firmware SV860_103 (FW860.20) package.

After installing or updating to ESS 5.1.x, you might notice an uninstalled RPM in the firmware group.

```
Checking installed packages...
================================================================
 [INFO]: [EMS] Group firmware RPMs:  Not Inst:  1, Current:  0, New:  0, Old:  0
 [INFO]: [EMS] Group gpfs RPMs:      Not Inst:  0, Current: 16, New:  0, Old:  0
 [INFO]: [EMS] Group gss RPMs:       Not Inst:  0, Current:  3, New:  0, Old:  0
 [INFO]: [EMS] Group gui RPMs:       Not Inst:  0, Current:  2, New:  0, Old:  0
 [INFO]: [EMS] Group ofed RPMs:      Not Inst:  0, Current:  1, New:  0, Old:  0
 [INFO]: [EMS] Group xcat-core RPMs: Not Inst:  0, Current:  8, New:  0, Old:  0
 [INFO]: [gssio1] Group firmware RPMs:  Not Inst:  1, Current:  0, New:  0, Old:  0
 [INFO]: [gssio1] Group gpfs RPMs:      Not Inst:  0, Current: 16, New:  0, Old:  0
 [INFO]: [gssio1] Group gss RPMs:       Not Inst:  0, Current:  1, New:  0, Old:  0
 [INFO]: [gssio1] Group ofed RPMs:      Not Inst:  0, Current:  1, New:  0, Old:  0
 [INFO]: [gssio2] Group firmware RPMs:  Not Inst:  1, Current:  0, New:  0, Old:  0
 [INFO]: [gssio2] Group gpfs RPMs:      Not Inst:  0, Current: 16, New:  0, Old:  0
 [INFO]: [gssio2] Group gss RPMs:       Not Inst:  0, Current:  1, New:  0, Old:  0
 [INFO]: [gssio2] Group ofed RPMs:      Not Inst:  0, Current:  1, New:  0, Old:  0
```

This NOT_INST error implies that the new firmware RPM is not installed yet.

Depending on your platform, use one of the following sets of steps for updating system firmware.

- Update the system firmware on PPC64LE systems as follows.
  1. Unpack the `*img` file in the `/tmp/fwupdate` directory.

     ```
     cd /opt/ibm/gss/install/firmware/
     rpm -ivh 01SV860_103_056.rpm
     ```

  2. Shutdown IBM Spectrum Scale and stop any ongoing I/O on the node.
  3. Verify the firmware level.

     ```
     update_flash -v -f /tmp/fwupdate/01SV860_103_056.img
     ```

  4. Update the system firmware.

     ```
     update_flash -f /tmp/fwupdate/01SV860_103_056.img
     ```

     After issuing this command, the node reboots and updates the firmware. It could take up to 30 minutes for the node to reboot with the new firmware level. You can then run **gssinstallcheck** on the node to verify if the firmware is successfully updated.

To update system firmware on PPC64BE systems, you must use HMC and you must upgrade your HMC to 860 SP1 before updating system firmware. For information about upgrading HMC, see HMC V8 Upgrade Procedure.

- Update the system firmware on PPC64BE systems as follows.
  1. Power down the system.
  2. From the HMC navigation area, click **Updates**.
  3. Using SFTP, point to the `/opt/ibm/gss/install/firmware` directory on the EMS node. The following files should be present:

     ```
     01SV860_103_056.xml
     01SV860_103_056.rpm
     ```

     Note: For updating the system firmware using HMC, if SFTP to the EMS node does not work, move the `*rpm` and the `*xml` files to a server which is accessible using FTP or SFTP.
  4. Select the update file and update the system firmware. It could take up to 30 minutes to update the firmware using HMC.

Appendix F. Obtaining kernel for system upgrades

For new system installation, the kernel is shipped with the system. However, for upgrades, you need to obtain and package the kernel update, and then follow the kernel update installation procedure.

You must have a EUS license to download the kernel from Red Hat Network.

Use the following steps during an upgrade to obtain and package the kernel update.

1. Clear the version locks.

   ```
   yum versionlock clear
   ```

2. Connect the management server node to the Red Hat Network.

   ```
   subscription-manager register --username=<X> --password=<Y>
   subscription-manager list --available // list pools
   subscription-manager attach --pool=<X>
   ```

   Or

   ```
   subscription-manager attach --auto
   ```

3. Create a directory for the kernel update package.

   For PPC64BE, issue:

   ```
   mkdir -p /tmp/kernel/RHBA-2017-1711-72-BE/
   ```

   For PPC64LE, issue:

   ```
   mkdir -p /tmp/kernel/RHBA-2017-1711-72-LE/
   ```

4. List all repositories and enable the repositories that are disabled, as required.

   ```
   yum repolist all
   yum-config-manager --enable rhel*
   ```

   Or

   ```
   subscription-manager config --rhsm.manage_repos=1
   ```

5. Download the kernel update package.

   For PPC64BE, issue:

   ```
   yum update *327.55.3* --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-BE
   yum update kmod-20-9.el7.ppc64.rpm --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-BE
   yum update perf-3.10.0-327.55.3.el7.ppc64.rpm --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-BE
   yum update python-perf-3.10.0-327.55.3.el7.ppc64.rpm --downloadonly --downloaddir=/tmp/RHBA-2017-1711-72-BE
   ```

   For PPC64LE, issue:

   ```
   yum update *327.55.3* --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-LE
   yum update kmod-20-9.el7.ppc64le.rpm --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-LE
   yum update perf-3.10.0-327.55.3.el7.ppc64le.rpm --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-LE
   yum update python-perf-3.10.0-327.55.3.el7.ppc64le.rpm --downloadonly --downloaddir=/tmp/kernel/RHBA-2017-1711-72-LE
   ```

   The command-line kernel download method might fail if a newer kernel is available. In that case, use these steps.

   a. Use one of the following steps depending on your platform:
      - For PPC64BE, go to the following URL: https://access.redhat.com/search/#/?q=kernel*327*55*.2*ppc64.rpm&p=1&srch=any&documentKind=
      - For PPC64LE, go to the following URL: https://access.redhat.com/search/#/?q=kernel*327*55*.2*ppc64le.rpm&p=1&srch=any&documentKind=

   b. Search for the required or any additional RPMs listed in Appendix G, “Instructions for installing the ESS Red Hat Linux Errata Kernel Update,” on page 53 and download them.

6. Package the directory.

For PPC64BE, issue:

```
cd /tmp/kernel ; tar -zcvf RHSA-2017-1711-72-BE.tgz RHBA-2017-1711-72-BE
```

For PPC64LE, issue:

```
cd /tmp/kernel ; tar -zcvf RHBA-2017-1711-72-LE.tar.gz RHBA-2017-1711-72-LE
```

7. Disable the Red Hat Network connection on the management server node.

```
subscription-manager config --rhsm.manage_repos=0
yum clean all
```

Continue with the kernel update installation steps for `RHBA-2017-1711-72-BE.tar.gz` or `RHBA-2017-1711-72-LE.tar.gz`. For more information, see Appendix G, “Instructions for installing the ESS Red Hat Linux Errata Kernel Update,” on page 53.

Appendix G. Instructions for installing the ESS Red Hat Linux Errata Kernel Update

This topic provides instructions for installing the Red Hat Linux Errata Kernel Update for ESS.

At the time of shipping from factory, most current recommended kernel errata and associated RPMs are provided in the `/home/deploy` directory. It is highly recommended to limit errata updates applied to the Red Hat Enterprise Linux operating system used in the ESS solution to security errata or errata updates requested by service. For more information visit Red Hat's solution article on applying only security updates: https://access.redhat.com/solutions/10021.

Kernel errata updates can be obtained from Red Hat network (RHN) using the supplied license: https://rhn.redhat.com/errata/rhel-server-7.2.eus-errata-security.html.

For information about the kernal update for the current release, see https://rhn.redhat.com/errata/RHBA-2017-1711.html.

Perform the following steps to prepare for installation of the ESS Red Hat Linux Errata Kernel Update. This example shows errata update (RHSA-2017-1711) provided in the `/home/deploy` directory of the EMS node when shipped from factory.

The following packages are provided in `RHBA-2017-1711-72-BE.tar.gz`:

- `kmod-20-9.el7.ppc64.rpm`
- `kernel-abi-whitelists-3.10.0-327.55.3.el7.noarch.rpm`
- `kernel-bootwrapper-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-debug-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-debug-devel-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-devel-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-headers-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-doc-3.10.0-327.55.3.el7.noarch.rpm`
- `kernel-tools-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-tools-libs-3.10.0-327.55.3.el7.ppc64.rpm`
- `kernel-tools-libs-devel-3.10.0-327.55.3.el7.ppc64.rpm`
- `perf-3.10.0-327.55.3.el7.ppc64.rpm`
- `python-perf-3.10.0-327.55.3.el7.ppc64.rpm`

The following packages are provided in the `RHBA-2017-1711-72-LE.tar.gz`:

- `kmod-20-9.el7.ppc64le.rpm`
- `kernel-abi-whitelists-3.10.0-327.55.3.el7.noarch.rpm`
- `kernel-bootwrapper-3.10.0-327.55.3.el7.ppc64le.rpm`
- `kernel-3.10.0-327.55.3.el7.ppc64le.rpm`
- `kernel-debug-3.10.0-327.55.3.el7.ppc64le.rpm`

| kernel-debug-devel-3.10.0-327.55.3.el7.ppc64le.rpm

| kernel-devel-3.10.0-327.55.3.el7.ppc64le.rpm

| kernel-headers-3.10.0-327.55.3.el7.ppc64le.rpm

| kernel-doc-3.10.0-327.55.3.el7.noarch.rpm

| kernel-tools-3.10.0-327.55.3.el7.ppc64le.rpm

| kernel-tools-libs-3.10.0-327.55.3.el7.ppc64le.rpm

| kernel-tools-libs-devel-3.10.0-327.55.3.el7.ppc64le.rpm

| perf-3.10.0-327.55.3.el7.ppc64le.rpm

| python-perf-3.10.0-327.55.3.el7.ppc64le.rpm

1. Copy RPMs and setup repository:
   a. Unpack the Errata Kernel archive on the management server node.
      ```
      $ cd /var/tmp
      ```
      For PPC64BE, issue:
      ```
      $ tar -zxvf RHBA-2017-1711-72-BE.tar.gz
      ```
      For PPC64LE, issue:
      ```
      $ tar -zxvf RHBA-2017-1711-72-LE.tar.gz
      ```
   b. Set up the management server node Kernel repository:
      ```
      $ /opt/ibm/gss/xcat/bin/gssxcatconfig -k
      ```
   c. Remove old RPMs from the kernel repository directory.
      For PPC64BE, issue:
      ```
      $ cd /install/gss/otherpkgs/rhels7/ppc64/kernel/
      $ rm -f *.rpm
      ```
      For PPC64LE, issue:
      ```
      $ cd /install/gss/otherpkgs/rhels7/ppc64le/kernel/
      $ rm -f *.rpm
      ```
   d. Copy the Errata Kernel RPMs into the repository directory.
      For PPC64BE, issue:
      ```
      $ cd /install/gss/otherpkgs/rhels7/ppc64/kernel/
      $ cp /var/tmp/RHBA-2017-1711-72-BE/*.rpm .
      ```
      For PPC64LE, issue:
      ```
      $ cd /install/gss/otherpkgs/rhels7/ppc64le/kernel/
      $ cp /var/tmp/RHBA-2017-1711-72-LE/*.rpm .
      ```
2. Update the Kernel repository information.
   For PPC64BE, issue:
   ```
   $ cd /install/gss/otherpkgs/rhels7/ppc64/kernel/
   $ createrepo .
   ```
   For PPC64LE, issue:
   ```
   $ cd /install/gss/otherpkgs/rhels7/ppc64le/kernel/
   $ createrepo .
   ```
3. After doing these steps, return to the corresponding install or upgrade task and install the kernel update using the **updatenode** command. For more information, see “Install the ESS system” on page 3 and “Upgrade the ESS system” on page 11.

Appendix H. Obtaining systemd update for system upgrades

For new system installation, the systemd update is shipped with the system and it is available in the `/home/deploy` directory.. However, for upgrades, you need to obtain and package the systemd update, and then follow the systemd update installation procedure.

You must have a EUS license to download the systemd update from Red Hat Network.

Use the following steps during an upgrade to obtain and package the systemd update.

1. Clear the version locks.

   ```
   yum versionlock clear
   ```

2. Connect the management server node to the Red Hat Network.

   ```
   subscription-manager register --username=<X> --password=<Y>
   subscription-manager list --available // list pools
   subscription-manager attach --pool=<X>
   ```

   Or

   ```
   subscription-manager attach --auto
   ```

3. Create a directory for the systemd update package.

   For PPC64BE, issue:

   ```
   mkdir -p /tmp/systemd/RHBA-2017-1311-BE/
   ```

   For PPC64LE, issue:

   ```
   mkdir -p /tmp/systemd/RHBA-2017-1311-LE
   ```

4. List all repositories and enable the repositories that are disabled, as required.

   ```
   yum repolist all
   yum-config-manager --enable rhel*
   ```

   Or

   ```
   subscription-manager config --rhsm.manage_repos=1
   ```

5. Download the kernel update package.

   For PPC64BE, issue:

   ```
   yum update systemd*219-30.el7_3.9* --downloadonly –downloaddir=/tmp/systemd/RHBA-2017-1311-BE
   yum update libgudev1-219-30.el7_3.9.ppc64.rpm --downloadonly –downloaddir=/tmp/systemd/RHBA-2017-1311-BE
   yum update libgudev1-devel-219-30.el7_3.9.ppc64.rpm --downloadonly –downloaddir=/tmp/systemd/RHBA-2017-1311-BE
   ```

   For PPC64LE, issue:

   ```
   yum update systemd*219-30.el7_3.9* --downloadonly –downloaddir=/tmp/systemd/RHBA-2017-1311-LE
   yum update libgudev1-219-30.el7_3.9.ppc64le.rpm --downloadonly –downloaddir=/tmp/systemd/RHBA-2017-1311-LE
   yum update libgudev1-devel-219-30.el7_3.9.ppc64le.rpm --downloadonly –downloaddir=/tmp/systemd/RHBA-2017-1311-LE
   ```

   The command-line kernel download method might fail if a newer kernel is available. In that case, use these steps.

   a. Use one of the following steps depending on your platform:
      - For PPC64BE, go to the following URL: https://access.redhat.com/search/#/?q=systemd*219-30.el7_3.9*ppc64.rpm&p=1&srch=any&documentKind=
      - For PPC64LE, go to the following URL: https://access.redhat.com/search/#/?q=systemd*219-30.el7_3.9*ppc64le.rpm&p=1&srch=any&documentKind=

   b. Search for the required or any additional RPMs listed in Appendix I, “Instructions for installing the ESS Red Hat Linux systemd update,” on page 57 and download them.

6. Package the directory.

For PPC64BE, issue:

```
cd /tmp/systemd ; tar -zcvf systemd-RHBA-2017-1311-73-BE.tar.gz RHBA-2017-1311-BE
```

For PPC64LE, issue:

```
cd /tmp/systemd ; tar -zcvf systemd-RHBA-2017-1311-73-LE.tar.gz RHBA-2017-1311-LE
```

7. Disable the Red Hat Network connection on the management server node.

```
subscription-manager config --rhsm.manage_repos=0
yum clean all
```

Continue with the systemd update installation steps for `systemd-RHBA-2017-1311-73-BE.tar.gz` or `systemd-RHBA-2017-1311-73-LE.tar.gz`. For more information, see Appendix I, "Instructions for installing the ESS Red Hat Linux systemd update," on page 57.

Appendix I. Instructions for installing the ESS Red Hat Linux systemd update

This topic provides instructions for installing the Red Hat Linux systemd update for ESS.

It is highly recommended to limit errata updates applied to the Red Hat Enterprise Linux operating system used in the ESS solution to security errata or errata updates requested by service. For more information visit Red Hat's solution article on applying only security updates: https://access.redhat.com/solutions/10021.

Perform the following steps to prepare for installation of the ESS Red Hat Linux systemd update. This example shows systemd update (RHBA-2017-1311) provided in the `/home/deploy` directory of the EMS node when shipped from factory.

The following packages are provided in `systemd-RHBA-2017-1311-73-BE.tar.g`:

```
systemd-219-30.el7_3.9.ppc64.rpm
systemd-devel-219-30.el7_3.9.ppc64.rpm
systemd-debuginfo-219-30.el7_3.9.ppc64.rpm
systemd-journal-gateway-219-30.el7_3.9.ppc64.rpm
systemd-libs-219-30.el7_3.9.ppc64.rpm
systemd-networkd-219-30.el7_3.9.ppc64.rpm
systemd-python-219-30.el7_3.9.ppc64.rpm
systemd-resolved-219-30.el7_3.9.ppc64.rpm
systemd-sysv-219-30.el7_3.9.ppc64.rpm
libgudev1-219-30.el7_3.9.ppc64.rpm
libgudev1-devel-219-30.el7_3.9.ppc64.rpm
```

The following packages are provided in the `systemd-RHBA-2017-1311-73-LE.tar.g`:

```
systemd-219-30.el7_3.9.ppc64le.rpm
systemd-devel-219-30.el7_3.9.ppc64le.rpm
systemd-debuginfo-219-30.el7_3.9.ppc64le.rpm
systemd-libs-219-30.el7_3.9.ppc64le.rpm
systemd-networkd-219-30.el7_3.9.ppc64le.rpm
systemd-python-219-30.el7_3.9.ppc64le.rpm
systemd-resolved-219-30.el7_3.9.ppc64le.rpm
systemd-sysv-219-30.el7_3.9.ppc64le.rpm
libgudev1-219-30.el7_3.9.ppc64le.rpm
libgudev1-devel-219-30.el7_3.9.ppc64le.rpm
```

1. Copy the tarball to the `/var/tmp` directory.
2. Extract the tarball using one of the following commands.

   For PPC64BE, issue:

```
$ tar -zxvf systemd-RHBA-2017-1311-73-BE.tar.gz
```

For PPC64LE, issue:

```
$ tar -zxvf systemd-RHBA-2017-1311-73-LE.tar.gz
```

3. Update the repository information.

   For PPC64BE, issue:

   ```
   $ cd /var/tmp/RHBA-2017-1311-BE
   $ createrepo .
   ```

   For PPC64LE, issue:

   ```
   $ cd /var/tmp/RHBA-2017-1311-LE
   $ createrepo .
   ```

4. Install the systemd update RPMs.

   Note: Before issuing the **yum -y install** command, ensure that any Red Hat Network subscriptions are disabled.

   For PPC64BE, issue:

   ```
   $ cd /var/tmp/RHBA-2017-1311-BE
   $ yum -y install *rpm
   ```

   For PPC64LE, issue:

   ```
   $ cd /var/tmp/RHBA-2017-1311-LE
   $ yum -y install *rpm
   ```

5. After doing these steps, return to the corresponding install or upgrade task. For more information, see "Install the ESS system" on page 3 and "Upgrade the ESS system" on page 11.

Note: This update needs to be performed on every node in the building block including the management server node. Restarting IBM Spectrum Scale on the updated nodes is not required.

Appendix J. Instructions for updating the mpt3sas driver

If the kernel is modified on the I/O server nodes, you need to rebuild and reload the mpt3sas driver.

Note: If you need to maintain file system access, ensure that you follow the same steps that you need to perform before doing upgrade including:

- Before shutting down GPFS, ensure that quorum is maintained
- Move the recovery groups
- Move the cluster or file system manager

After the kernel is updated and the nodes are rebooted, do the following.

1. Shutdown GPFS on the node.

   mmshutdown -N *NODE*
2. Copy the mpt3sas src RPM from `/home/deploy` on the management server node to the I/O server nodes.
3. Rebuild the RPMs for the running kernel.

   ```
   /bin/rpmbuild --rebuild SRC_RPM_LOCATION/mpt3sas-13.100.00.00-1.el7_2.src.rpm
   ```

   This command creates two RPMs.
4. Unload the current mpt3sas driver.

   ```
   rmmod mpt3sas
   ```
5. Install the RPMs.

   ```
   rpm -Uvh /root/rpmbuild/RPMS/ppc64le/kmod-mpt3sas*rpm
   rpm -Uvh /root/rpmbuild/RPMS/ppc64le/mpt3sas*rpm
   ```
6. Load the updated modules.

   ```
   modprobe mpt3sas
   ```
7. Verify that the module is loaded.

   ```
   modinfo mpt3sas
   ```
8. Verify the disks are visible by issuing the **lsscsi** or the **lsblk** commands..

Appendix K. Shutting down and powering up ESS

The ESS components and frame may need to be powered off in cases such as data center maintenance, relocation, or emergencies. Use the following information to shut down and power up ESS.

Shutting down ESS

1. Verify that the file systems are not needed by users during the time the system will be unavailable.
2. If you are using a remote cluster to mount the ESS file system, unmount the file system by issuing the **mmumount** command from the remote client nodes.
3. Shut down the nodes using the **mmshutdown -N** command. For example:

   ```
   mmshutdown -N ems1,gssio1,gssio2
   ```

4. If other nodes are attached and ESS nodes are the only quorum and manager nodes, it is recommended that you use the **mmshutdown -a** command to shut down the entire cluster.
5. Verify that IBM Spectrum Scale is shut down on the I/O nodes by issuing the **mmgetstate -a** command.
6. Power off the EMS and I/O nodes by issuing the **mmshutdown -h now** command on each individual node.

   If you are using the Big Endian (BE) platform:

   a. The EMC LPAR, I/O node1 LPAR, and I/O node 2 LPAR will be shut down after you issue the **shutdown -h now**.
   b. Use the HMC to shut down the physical servers.
   c. Verify that the power light on the front of the frame is blinking after the LPARs are shut down.

   If you are using the Big Endian (BE) platform and the HMC resides within this frame:

   a. Power off the HMC. If the HMC controls servers that are outside of this frame, plan appropriately before shutting down.

   If you are using the Little Endian (LE) platform:

   a. The EMC LPAR, I/O node1 LPAR, and I/O node 2 LPAR will be completely shut down after you issue the **shutdown -h now** command.
   b. Verify that the power light on the front of the frame is blinking.
7. Power off all storage by flipping the power switches to off.
8. Before shutting off power to the frame, verify there are no components within the frame that are relied on by external infrastructure such as IB or Ethernet switches. If any of these exist and hardware outside of the frame needs access, plan appropriately before shutting off power to the frame.

Powering up ESS

1. Verify that power is connected to the frame.
2. Turn on all PDUs within the ESS frame.
3. Power on the components in the following order.

   If you are using the Big Endian (BE) platform:

   a. Power on the HMC.
   b. Power on the storage drawers by flipping the power switches on each storage module to on.
   c. Power on the EMS node, I/O node 1 and I/0 node 2.
   d. Wait for the HMC to come online and log in.
   e. Wait for the EMS node, I/O node 1 and I/0 node 2 to be accessible to the HMC.
   f. Once the EMS sees that node, I/O node 1 and I/0 node 2 are powered on, move to the LPAR view for each and power on the associated LPARs:

EMS LPAR

1/O node 1 LPAR

I/O node 2 LPAR

g. Once all LPARs are powered on, ssh to the EMS node and verify that IBM Spectrum Scale has come online by issuing **mmgetstate -N ems1,gssio1,gssio2**. If IBM Spectrum Scale does not automatically start, start it manually by issuing **mmstartup -N ems1,gssio1,gssio2.**

h. Issue the **gnrhealthcheck** and the **mmhealth cluster show** commands, and check the GUI event logs.

If you are using the Little Endian (LE) platform:

a. Power on the storage drawers by flipping the power switches on each storage module to on.

b. Power on the EMS node, I/O node 1 and I/0 node 2.

c. Once all LPARs are powered on, ssh to the EMS node and verify that IBM Spectrum Scale has come online by issuing **mmgetstate -N ems1,gssio1,gssio2**. If IBM Spectrum Scale does not automatically start, start it manually by issuing **mmstartup -N ems1,gssio1,gssio2.**

d. Issue the **gnrhealthcheck** and the **mmhealth cluster show** commands, and check the GUI event logs.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21,

Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information 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. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Dept. 30ZA/Building 707
Mail Station P300

2455 South Road,
Poughkeepsie, NY 12601-5400
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment or a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Glossary

This glossary provides terms and definitions for the ESS solution.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window):

http://www.ibm.com/software/globalization/terminology

B

building block
A pair of servers with shared disk enclosures attached.

BOOTP
See *Bootstrap Protocol (BOOTP)*.

Bootstrap Protocol (BOOTP)
A computer networking protocol thst is used in IP networks to automatically assign an IP address to network devices from a configuration server.

C

CEC See *central processor complex (CPC)*.

central electronic complex (CEC)
See *central processor complex (CPC)*.

central processor complex (CPC)
A physical collection of hardware that consists of channels, timers, main storage, and one or more central processors.

cluster
A loosely-coupled collection of independent systems, or *nodes*, organized into a network for the purpose of sharing resources and communicating with each other. See also *GPFS cluster*.

cluster manager
The node that monitors node status using disk leases, detects failures, drives recovery, and selects file system managers. The cluster manager is the node with the lowest node number among the quorum nodes that are operating at a particular time.

compute node
A node with a mounted GPFS file system that is used specifically to run a customer job. ESS disks are not directly visible from and are not managed by this type of node.

CPC See *central processor complex (CPC)*.

D

DA See *declustered array (DA)*.

datagram
A basic transfer unit associated with a packet-switched network.

DCM See *drawer control module (DCM)*.

declustered array (DA)
A disjoint subset of the pdisks in a recovery group.

dependent fileset
A fileset that shares the inode space of an existing independent fileset.

DFM See *direct FSP management (DFM)*.

DHCP See *Dynamic Host Configuration Protocol (DHCP)*.

direct FSP management (DFM)
The ability of the xCAT software to communicate directly with the Power Systems server's service processor without the use of the HMC for management.

drawer control module (DCM)
Essentially, a SAS expander on a storage enclosure drawer.

Dynamic Host Configuration Protocol (DHCP)
A standardized network protocol that is used on IP networks to dynamically distribute such network configuration parameters as IP addresses for interfaces and services.

E

Elastic Storage Server (ESS)
A high-performance, GPFS NSD solution

made up of one or more building blocks that runs on IBM Power Systems servers. The ESS software runs on ESS nodes - management server nodes and I/O server nodes.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process. See also *file encryption key (FEK)*, *master encryption key (MEK)*.

ESS See *Elastic Storage Server (ESS)*.

environmental service module (ESM)
Essentially, a SAS expander that attaches to the storage enclosure drives. In the case of multiple drawers in a storage enclosure, the ESM attaches to drawer control modules.

ESM See *environmental service module (ESM)*.

Extreme Cluster/Cloud Administration Toolkit (xCAT)
Scalable, open-source cluster management software. The management infrastructure of ESS is deployed by xCAT.

F

failback
Cluster recovery from failover following repair. See also *failover*.

failover
(1) The assumption of file system duties by another node when a node fails. (2) The process of transferring all control of the ESS to a single cluster in the ESS when the other clusters in the ESS fails. See also *cluster*. (3) The routing of all transactions to a second controller when the first controller fails. See also *cluster*.

failure group
A collection of disks that share common access paths or adapter connection, and could all become unavailable through a single hardware failure.

FEK See *file encryption key (FEK)*.

file encryption key (FEK)
A key used to encrypt sectors of an individual file. See also *encryption key*.

file system
The methods and data structures used to control how data is stored and retrieved.

file system descriptor
A data structure containing key information about a file system. This information includes the disks assigned to the file system (*stripe group*), the current state of the file system, and pointers to key files such as quota files and log files.

file system descriptor quorum
The number of disks needed in order to write the file system descriptor correctly.

file system manager
The provider of services for all the nodes using a single file system. A file system manager processes changes to the state or description of the file system, controls the regions of disks that are allocated to each node, and controls token management and quota management.

fileset A hierarchical grouping of files managed as a unit for balancing workload across a cluster. See also *dependent fileset*, *independent fileset*.

fileset snapshot
A snapshot of an independent fileset plus all dependent filesets.

flexible service processor (FSP)
Firmware that provices diagnosis, initialization, configuration, runtime error detection, and correction. Connects to the HMC.

FQDN
See *fully-qualified domain name (FQDN)*.

FSP See *flexible service processor (FSP)*.

fully-qualified domain name (FQDN)
The complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name.

G

GPFS cluster
A cluster of nodes defined as being available for use by GPFS file systems.

GPFS portability layer
The interface module that each

installation must build for its specific hardware platform and Linux distribution.

GPFS Storage Server (GSS)
A high-performance, GPFS NSD solution made up of one or more building blocks that runs on System x servers.

GSS See *GPFS Storage Server (GSS)*.

H

Hardware Management Console (HMC)
Standard interface for configuring and operating partitioned (LPAR) and SMP systems.

HMC See *Hardware Management Console (HMC)*.

I

IBM Security Key Lifecycle Manager (ISKLM)
For GPFS encryption, the ISKLM is used as an RKM server to store MEKs.

independent fileset
A fileset that has its own inode space.

indirect block
A block that contains pointers to other blocks.

inode The internal structure that describes the individual files in the file system. There is one inode for each file.

inode space
A collection of inode number ranges reserved for an independent fileset, which enables more efficient per-fileset functions.

Internet Protocol (IP)
The primary communication protocol for relaying datagrams across network boundaries. Its routing function enables internetworking and essentially establishes the Internet.

I/O server node
An ESS node that is attached to the ESS storage enclosures. It is the NSD server for the GPFS cluster.

IP See *Internet Protocol (IP)*.

IP over InfiniBand (IPoIB)
Provides an IP network emulation layer on top of InfiniBand RDMA networks, which allows existing applications to run over InfiniBand networks unmodified.

IPoIB See *IP over InfiniBand (IPoIB)*.

ISKLM
See *IBM Security Key Lifecycle Manager (ISKLM)*.

J

JBOD array
The total collection of disks and enclosures over which a recovery group pair is defined.

K

kernel The part of an operating system that contains programs for such tasks as input/output, management and control of hardware, and the scheduling of user tasks.

L

LACP See *Link Aggregation Control Protocol (LACP)*.

Link Aggregation Control Protocol (LACP)
Provides a way to control the bundling of several physical ports together to form a single logical channel.

logical partition (LPAR)
A subset of a server's hardware resources virtualized as a separate computer, each with its own operating system. See also *node*.

LPAR See *logical partition (LPAR)*.

M

management network
A network that is primarily responsible for booting and installing the designated server and compute nodes from the management server.

management server (MS)
An ESS node that hosts the ESS GUI and xCAT and is not connected to storage. It can be part of a GPFS cluster. From a system management perspective, it is the central coordinator of the cluster. It also serves as a client node in an ESS building block.

master encryption key (MEK)
A key that is used to encrypt other keys. See also *encryption key*.

maximum transmission unit (MTU)
The largest packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network, such as the Internet. The TCP uses the MTU to determine the maximum size of each packet in any transmission.

MEK See *master encryption key (MEK)*.

metadata
A data structure that contains access information about file data. Such structures include inodes, indirect blocks, and directories. These data structures are not accessible to user applications.

MS See *management server (MS)*.

MTU See *maximum transmission unit (MTU)*.

N

Network File System (NFS)
A protocol (developed by Sun Microsystems, Incorporated) that allows any host in a network to gain access to another host or netgroup and their file directories.

Network Shared Disk (NSD)
A component for cluster-wide disk naming and access.

NSD volume ID
A unique 16-digit hexadecimal number that is used to identify and access all NSDs.

node An individual operating-system image within a cluster. Depending on the way in which the computer system is partitioned, it can contain one or more nodes. In a Power Systems environment, synonymous with *logical partition*.

node descriptor
A definition that indicates how IBM Spectrum Scale uses a node. Possible functions include: manager node, client node, quorum node, and non-quorum node.

node number
A number that is generated and maintained by IBM Spectrum Scale as the cluster is created, and as nodes are added to or deleted from the cluster.

node quorum
The minimum number of nodes that must be running in order for the daemon to start.

node quorum with tiebreaker disks
A form of quorum that allows IBM Spectrum Scale to run with as little as one quorum node available, as long as there is access to a majority of the quorum disks.

non-quorum node
A node in a cluster that is not counted for the purposes of quorum determination.

O

OFED See *OpenFabrics Enterprise Distribution (OFED)*.

OpenFabrics Enterprise Distribution (OFED)
An open-source software stack includes software drivers, core kernel code, middleware, and user-level interfaces.

P

pdisk A physical disk.

PortFast
A Cisco network function that can be configured to resolve any problems that could be caused by the amount of time STP takes to transition ports to the Forwarding state.

R

RAID See *redundant array of independent disks (RAID)*.

RDMA
See *remote direct memory access (RDMA)*.

redundant array of independent disks (RAID)
A collection of two or more disk physical drives that present to the host an image of one or more logical disk drives. In the event of a single physical device failure, the data can be read or regenerated from the other disk drives in the array due to data redundancy.

recovery
The process of restoring access to file system data when a failure has occurred. Recovery can involve reconstructing data or providing alternative routing through a different server.

recovery group (RG)
A collection of disks that is set up by IBM Spectrum Scale RAID, in which each disk is connected physically to two servers: a primary server and a backup server.

remote direct memory access (RDMA)
A direct memory access from the memory of one computer into that of another without involving either one's operating system. This permits high-throughput, low-latency networking, which is especially useful in massively-parallel computer clusters.

RGD See *recovery group data (RGD)*.

remote key management server (RKM server)
A server that is used to store master encryption keys.

RG See *recovery group (RG)*.

recovery group data (RGD)
Data that is associated with a recovery group.

RKM server
See *remote key management server (RKM server)*.

S

SAS See *Serial Attached SCSI (SAS)*.

secure shell (SSH)
A cryptographic (encrypted) network protocol for initiating text-based shell sessions securely on remote computers.

Serial Attached SCSI (SAS)
A point-to-point serial protocol that moves data to and from such computer storage devices as hard drives and tape drives.

service network
A private network that is dedicated to managing POWER8 servers. Provides Ethernet-based connectivity among the FSP, CPC, HMC, and management server.

SMP See *symmetric multiprocessing (SMP)*.

Spanning Tree Protocol (STP)
A network protocol that ensures a loop-free topology for any bridged Ethernet local-area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them.

SSH See *secure shell (SSH)*.

STP See *Spanning Tree Protocol (STP)*.

symmetric multiprocessing (SMP)
A computer architecture that provides fast performance by making multiple processors available to complete individual processes simultaneously.

T

TCP See *Transmission Control Protocol (TCP)*.

Transmission Control Protocol (TCP)
A core protocol of the Internet Protocol Suite that provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network.

V

VCD See *vdisk configuration data (VCD)*.

vdisk A virtual disk.

vdisk configuration data (VCD)
Configuration data that is associated with a virtual disk.

X

xCAT See *Extreme Cluster/Cloud Administration Toolkit*.

Printed in USA

SC27-8580-08