Power Systems

Configuring and managing an IBM PurePower System

Power Systems

Configuring and managing an IBM PurePower System

Note

Before using this information and the product it supports, read the information in "Safety notices" on page v, "Notices" on page 43, the *IBM Systems Safety Notices* manual, G229-9054, and the *IBM Environmental Notices and User Guide*, Z125–5823.

This edition applies to IBM Power Systems™ servers that contain the POWER8 processor and to all associated models.

Contents

Safety notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, safety information documentation is included in the publications package (such as in printed documentation, on DVD, or as part of the product) shipped with the product. The documentation contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information documentation. You should also refer to the safety information documentation any time you do not clearly understand any safety information in the U.S. English publications.

Replacement or additional copies of safety information documentation can be obtained by calling the IBM Hotline at 1-800-300-8751.

German safety information

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Laser safety information

IBM® servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

Laser compliance

IBM servers may be installed inside or outside of an IT equipment rack.

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **If IBM supplied the power cord(s), connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Do not attempt to switch on power to the machine until all possible unsafe conditions are corrected.**
- **Assume that an electrical safety hazard is present. Perform all continuity, grounding, and power checks specified during the subsystem installation procedures to ensure that the machine meets safety requirements.**
- **Do not continue with the inspection if any unsafe conditions are present.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

  To Disconnect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Remove the power cords from the outlets.**
  3. **Remove the signal cables from the connectors.**
  4. **Remove all cables from the devices.**

  To Connect:

  1. **Turn off everything (unless instructed otherwise).**
  2. **Attach all cables to the devices.**
  3. **Attach the signal cables to the connectors.**
  4. **Attach the power cords to the outlets.**
  5. **Turn on the devices.**

  Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching.

  (D005)

(R001 part 1 of 2):

DANGER: Observe the following precautions when working on or around your IT rack system:

- Heavy equipment–personal injury or equipment damage might result if mishandled.
- Always lower the leveling pads on the rack cabinet.
- Always install stabilizer brackets on the rack cabinet.
- To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.

- Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices.

- Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.
- Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.
- An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

(R001 part 2 of 2):

CAUTION:

- Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.
- Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.
- Consideration should be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.
- *(For sliding drawers.)* Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.

- *(For fixed drawers.)* This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.

CAUTION:
Removing components from the upper positions in the rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building.

- **Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must observe the following precautions:**
  - **Remove all devices in the 32U position (compliance ID RACK-001 or 22U (compliance ID RR001) and above.**
  - **Ensure that the heaviest devices are installed in the bottom of the rack cabinet.**
  - **Ensure that there are little-to-no empty U-levels between devices installed in the rack cabinet below the 32U (compliance ID RACK-001 or 22U (compliance ID RR001) level, unless the received configuration specifically allowed it.**
- **If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.**
- **If the rack cabinet you are relocating was supplied with removable outriggers they must be reinstalled before the cabinet is relocated.**
- **Inspect the route that you plan to take to eliminate potential hazards.**
- **Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.**
- **Verify that all door openings are at least 760 x 230 mm (30 x 80 in.).**
- **Ensure that all devices, shelves, drawers, doors, and cables are secure.**
- **Ensure that the four leveling pads are raised to their highest position.**
- **Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.**
- **Do not use a ramp inclined at more than 10 degrees.**
- **When the rack cabinet is in the new location, complete the following steps:**
  - **Lower the four leveling pads.**
  - **Install stabilizer brackets on the rack cabinet.**
  - **If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.**
- **If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.**

(R002)

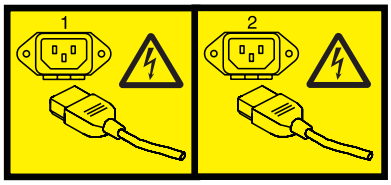
(L001)

DANGER: Hazardous voltage, current, or energy levels are present inside any component that has this label attached. Do not open any cover or barrier that contains this label. (L001)

(L002)

DANGER: Rack-mounted devices are not to be used as shelves or work spaces. (L002)

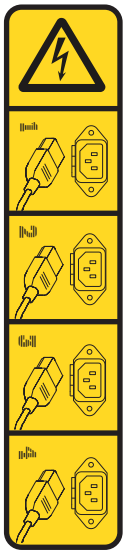
(L003)



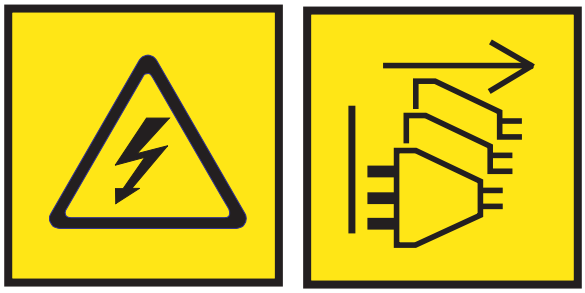
or

or

or



or



DANGER: Multiple power cords. The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. (L003)

(L007)

CAUTION: A hot surface nearby. (L007)

(L008)

CAUTION: Hazardous moving parts nearby. (L008)

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION:
This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.**

(C026)

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. Although shining light into one end and looking into the other end of a disconnected optical fiber to verify the continuity of optic fibers many not injure the eye, this procedure is potentially dangerous. Therefore, verifying the continuity of optical fibers by shining light into one end and looking at the other end is not recommended. To verify continuity of a fiber optic cable, use an optical light source and power meter. (C027)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

CAUTION:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do Not:
- **___ Throw or immerse into water**
- **___ Heat to more than 100°C (212°F)**
- **___ Repair or disassemble**

Exchange only with the IBM-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM part number for the battery unit available when you call. (C003)

(C048)
CAUTION regarding IBM provided VENDOR LIFT TOOL:

- **Operation of LIFT TOOL by authorized personnel only.**
- **LIFT TOOL intended for use to assist, lift, install, remove units (load) up into rack elevations. It is not to be used loaded transporting over major ramps nor as a replacement for such designated tools like pallet jacks, walkies, fork trucks and such related relocation practices. When this is not practicable, specially trained persons or services must be used (for instance, riggers or movers).**
- **Read and completely understand the contents of LIFT TOOL operator's manual before using. Failure to read, understand, obey safety rules, and follow instructions may result in property damage and/or personal injury. If there are questions, contact the vendor's service and support. Local paper manual must remain with machine in provided storage sleeve area. Latest revision manual available on vendor's web site.**
- **Test verify stabilizer brake function before each use. Do not over-force moving or rolling the LIFT TOOL with stabilizer brake engaged.**
- **Do not move LIFT TOOL while platform is raised, except for minor positioning.**
- **Do not exceed rated load capacity. See LOAD CAPACITY CHART regarding maximum loads at center versus edge of extended platform.**
- **Only raise load if properly centered on platform. Do not place more than 200 lb (91 kg) on edge of sliding platform shelf also considering the load's center of mass/gravity (CoG).**
- **Do not corner load the platform tilt riser accessory option. Secure platform riser tilt option to main shelf in all four (4x) locations with provided hardware only, prior to use. Load objects are designed to slide on/off smooth platforms without appreciable force, so take care not to push or lean. Keep riser tilt option flat at all times except for final minor adjustment when needed.**
- **Do not stand under overhanging load.**
- **Do not use on uneven surface, incline or decline (major ramps).**
- **Do not stack loads.**
- **Do not operate while under the influence of drugs or alcohol.**
- **Do not support ladder against LIFT TOOL.**
- **Tipping hazard. Do not push or lean against load with raised platform.**
- **Do not use as a personnel lifting platform or step. No riders.**
- **Do not stand on any part of lift. Not a step.**
- **Do not climb on mast.**
- **Do not operate a damaged or malfunctioning LIFT TOOL machine.**
- **Crush and pinch point hazard below platform. Only lower load in areas clear of personnel and obstructions. Keep hands and feet clear during operation.**
- **No Forks. Never lift or move bare LIFT TOOL MACHINE with pallet truck, jack or fork lift.**
- **Mast extends higher than platform. Be aware of ceiling height, cable trays, sprinklers, lights, and other overhead objects.**
- **Do not leave LIFT TOOL machine unattended with an elevated load.**
- **Watch and keep hands, fingers, and clothing clear when equipment is in motion.**
- **Turn Winch with hand power only. If winch handle cannot be cranked easily with one hand, it is probably over-loaded. Do not continue to turn winch past top or bottom of platform travel. Excessive unwinding will detach handle and damage cable. Always hold handle when lowering, unwinding. Always assure self that winch is holding load before releasing winch handle.**
- **A winch accident could cause serious injury. Not for moving humans. Make certain clicking sound is heard as the equipment is being raised. Be sure winch is locked in position before releasing handle. Read instruction page before operating this winch. Never allow winch to unwind freely. Freewheeling will cause uneven cable wrapping around winch drum, damage cable, and may cause serious injury. (C048)**

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM servers that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:

- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

The dc-powered system is intended to be installed in a common bonding network (CBN) as described in GR-1089-CORE.

Configuring and managing an IBM PurePower System

Learn how to configure and manage an IBM PurePower System™, and learn to use the PurePower Integrated Manager, monitor the system, and configure the network.

Accessing the PurePower Integrated Manager by using the flat panel rack-mounted monitor and keyboard

You can use the flat panel rack-mounted monitor and keyboard to access the PurePower Integrated Manager.

To access the PurePower Integrated Manager by using the flat panel rack-mounted monitor and keyboard, complete the following steps:

1. Power on the management nodes by pressing the buttons on the right side of the node chassis.
2. Wait 5 minutes for the management nodes to power on.
3. Slide out the console display and keyboard. Lift the display to access the keyboard.
4. The display powers on.
5. Press the **PRTSC** key to enable the KVM switch. The management nodes are displayed.
6. Press **Enter**.
7. Log in to the KVM console. The default user ID is `admin` and the password is `PASSW0RD` for the KVM hypervisor operating system (192.168.93.44).

   To change the default ID and password, select **Applications** > **System Tools** > **Settings** > **Users** and change the required fields.

   Note:

   To change the password for the PurePower Integrated Manager operating system (puremgrvm), complete the following steps:

   a. From the Red Hat Enterprise Linux (RHEL) KVM operating system desktop, select **Applications** > **Utilities** > **Terminal**.
   b. From the terminal session, run the following command: `ssh admin@192.168.93.46 PASSW0RD`
   c. From the puremgrvm operating system, run the following command: `passwd`

      Note: You will be prompted for the new password and confirmation.
   d. Exit the terminal session and return to console login screen. You can now log on by using the new password.
8. Double-click the PurePower Integrated Manager icon to start the PurePower Integrated Manager user interface.
9. Log in to the PurePower Integrated Manager user interface.

   Note: The default ID and password is `admin/PASSW0RD`.
10. The PurePower Integrated Manager Home window opens.
11. In the left-hand navigation area, click the **Hardware Inventory** icon. The Hardware Inventory screen displays information about hardware resources.
12. Check the Nagios interface to ensure that the components of the system are functioning properly. To access Nagios, complete the following steps:
    a. Click **Home**.

b. From the PurePower Integrated Manager Home screen, click **puremgra**. The Nagios Core manager window opens.
c. Log in to Nagios Core manager.

   Note: The default ID and password is `nagiosadmin/PASSW0RD`.

Installing customer supplied hardware for a PurePower System

Space is reserved at the top of your IBM Enterprise rack for customer supplied hardware. For example, the hardware can include switches or tape drives.

To install customer supplied hardware for a PurePower System, complete the following steps:

1. Select the hardware you want to install.
2. Follow the instructions that are provided with the hardware to install and configure the hardware.

Adding an expansion rack to your PurePower System configuration

You can use the PurePower Integrated Manager to add an expansion rack to your PurePower System configuration.

Note: The terms *expansion rack* and *extension rack* are interchangeable in this topic.

To add an expansion rack to your PurePower System configuration, complete the following steps:

1. Log in to the PurePower Integrated Manager with your username and password.
2. Click the **Hardware Inventory** icon. The Hardware Inventory window is shown.
3. Click **Add Rack**. The Add Rack Definition window is shown.
4. On the Rack Details window, enter the following information:

   Note: The Label field is required, the remaining fields are optional.
   - Type a name for the new rack in the **Label** field.
   - Type the name of the appropriate data center in the **Data Center** field.
   - Type the appropriate location in the **Location** field.
   - Add any notes in the **Notes** field.
5. Choose from the following options:
   - If you do not want to configure rack connections, clear the **Include rack connections** check box.
   - If you want to configure rack connections, leave the **Include rack connections** check box selected.
6. Click **Next**.
   - If you cleared **Include rack connections**, the Summary window is shown. Continue with step 7 on page 3.
   - If you selected **Include rack connections**, the Connection Profile window is shown. Complete the following steps:
     a. Click **Select Profile** and navigate to the connection profile file that you received with the rack. The connection profile file contains device configuration information for each resource in the rack.
     b. Click **Next**. The Confirm Connections window is shown.
     c. Click **Confirm Connection**. The physical connections between the managing rack and the rack extension are verified. This action can take several minutes.
     d. Click **Next**. The Configure Network window is shown.

e. On the Configure Network window, you can either specify the default network address that you want to use when you add devices, or use the default network address 192.168.92.xxx by clearing the **Specify default network address** box.
f. Click **Next**. The Summary window is shown.
g. Review the information that is shown. Continue with step 7.

7. Click **Finish**. A new rack tab is added to the hardware inventory, and resources are added to the rack.

For details about editing the properties of an existing rack, moving devices from one rack to another, or removing a rack, see Managing racks by using the PurePower Integrated Manager.

Adding the PurePower System to your network

Learn how to add the PurePower System to your network.

Configuring the network by using the PurePower Integrated Manager

Learn how to configure the network by using the PurePower Integrated Manager.

Note: You cannot use the PurePower Integrated Manager to change the 1 Gb management switch or the 40 Gb data network switch configurations for virtual LANs (VLANs), link aggregations, port settings, and so on.

To configure the network, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Hardware Inventory** icon.
3. Click the tab for the rack for which you want to configure the network.
4. Under Resources, click **Configure Network**. The Configure Network window is shown.
5. Select one or more of the following options:
   - Make necessary changes to the subnet mask that is used. The subnet mask establishes the range of addresses that are valid.
   - If a gateway is used, click **Specify a gateway for all resources**, and then specify the IP address of the gateway.
   - Specify a value for each octet of the IP address for each device in the rack.

     Note: You can also set an initial value for each selected device in the table. For example, if you set a new value for your subnet mask and gateway on your rack, you could then set all your devices' addresses to be in a range. For example, 9.27.20.x to 9.27.21.x.

     To do this, you would put the value 9 and 27 in the **host prefix** field, and select **Apply Prefix to Selected Resources**. The table updates with the correct values for the selected resources.
   - To apply a global network address scheme, set the subnet mask, update the network address field as needed, and select **Apply Prefix to Selected Resources**. The addresses of each resource are updated based on the network address.

     Note: If you set a new value for your subnet mask and gateway on your rack, you could then set all your devices' addresses to be in a particular range. For example, if your want a range of 9.27.20.x to 9.27.21.x, you would put the value 9 and 27 in the **host prefix** field, and select **Apply Prefix to Selected Resources**. The table updates with the correct values for the selected resources.
6. Click **OK**. The PurePower Integrated Manager is updated to access the resources in the rack at the addresses provided.

Special considerations

If you update the NTP Server IP address or the KVM Host OS IP address (for example, 192.168.93.44 (purekvma) or 192.168.93.144 (purekvmb)), you might need to manually update the following devices in the PurePower System rack.

The default IP addresses for a PurePower System are contained in the 192.168.93.x (255.255.240.0) subnet. If required, this default network address range can be changed.

In the PurePower Integrated Manager user interface, if the rack network switch, storage area network (SAN) switch, and IBM Storwize® V7000 management IP are changed, you must complete some steps manually.

The default Primary NTP Server for the PurePower System rack is the PureKVM A-Side Host OS (192.168.93.44), Secondary NTP Server for the PurePower System rack is the PureKVM B-Side OS (192.168.93.144). If the PurePower Integrated Manager user interface changed the KVM Host OS IP, then you must complete the following manual steps to update the rack switches and other devices, and to point to the new IP address defined for the PureKVM Host OS serving the NTP role.

IBM System Storage® SAN-48B-5

tsclockserver 192.168.93.44 <=== Use the new IP address for the KVM Host OS

Lenovo RackSwitch G8052

ntp primary server 192.168.93.44 <=== Use the new IP address for the Side A KVM Host OS

ntp secondary server 192.168.93.144 <=== Use the new IP address for the Side B KVM Host OS

Mellanox MSX1710-BS2F2 switches

en

conf t

ntp enable

ntp server 192.168.93.44 <=== Use the new IP address for the KVM Host OS write memory

V7000 **chsystem -ntpip 192.168.93.44** <=== Use the new IP address for the KVM Host OS

FS900 **chsystem -ntpip 192.168.93.44** <=== Use the new IP address for the KVM Host OS

HMC **chhmc -c xntp -s enable**

chhmc -c xntp -s add -a 192.168.93.44 -i eth1 <=== Verify that eth1 is 192. interface used

VIOS OS

echo "server 192.168.93.44 <=== Use the new IP value for the KVM Host OS

driftfile /etc/ntp.drift

tracefile /etc/ntp.trace" > /tmp/ntp.conf

cp /tmp/ntp.conf /home/padmin/config/ntp.conf

stopsrc -s xntpd

startsrc -s xntpd -a '-c /home/padmin/config/ntp.conf'

If the PurePower Integrated Manager user interface was used to change the gateway for the PurePower System rack and the value that is specified for the gateway is required to be changed back to 0.0.0.0, it is necessary to perform the actions on each individual device in the PurePower System rack.

To match the new subnet required, it is also necessary to manually perform the following steps:

1. On the PureKVM Host OS, modify **/data/purekvm/recovery_volume.properties** to include the new IP address scheme.
2. On the PowerVC Guest OS, first update the /etc/hosts with the new IP address, then run the **# /usr/bin/powervc-config general ip** command on the PowerVC Guest OS.

IP address schema for an IBM PurePower System multiple-rack configuration

The IBM PurePower System multiple-rack configuration includes a primary rack and up to seven expansion racks. The expansion racks are shipped with default IP addresses 192.168.92.x.

Note: The terms *expansion rack* and *extension rack* are interchangeable in this topic.

The primary rack is shipped with the default IP address 192.168.93.x and a subnet mask 255.255.240.0. This setting provides IP addresses in the range 192.168.80.1 – 192.168.95.254. You can use the following addresses for each rack, with the same private address scheme:

Table 1. IP addresses for an IBM PurePower System multiple-rack configuration

Rack	IP address
Primary rack	192.168.93.x
Expansion rack 1	192.168.94.x
Expansion rack 2	192.168.95.x
Expansion rack 3	192.168.80.x
Expansion rack 4	192.168.81.x
Expansion rack 5	192.168.82.x
Expansion rack 6	192.168.83.x
Expansion rack 7	192.168.84.x

Working with operating systems

Learn about creating custom certificate authority certificates, identifying operating system ports, setting up SELinux, and getting fixes for your PurePower System operating systems.

Managing the PurePower Integrated Manager guest operating system

Learn how to create custom certificate authority certificates and identify operating system ports.

Note: Any user ID that is created on the PurePower Integrated Manager guest operating system can be used to log in to the PurePower Integrated Manager web interface and perform any action from the web interface. Accounts that are created on the PurePower Integrated Manager guest operating system need to be restricted to only users that need to manage the devices of the PurePower System.

Creating custom certificate authority certificates

The Pure Manager (puremgrvm) web server configures HyperText Transfer Protocol Secure (HTTPS) by using self-signed X.509 certificates. You can replace the created certificates with custom certificate authority (CA) certificates.

Type the following commands to create custom certificates:

```
etc/httpd/conf.d/puremgr.conf
/etc/pki/tls/certs/puremgr.crt
/etc/pki/tls/private/puremgr.key
```

Identifying IP addresses, user IDs, and passwords

Learn about the default IP addresses, user IDs, and passwords that are available in the PurePower System.

Table 2. List of IP addresses, user IDs, and passwords (primary node management)

	IP address	Default user ID	Default password
PureKVM-A	192.168.93.44	root	PASSW0RD
		admin	PASSW0RD
PureMgr VM-A	192.168.93.46	root	PASSW0RD
		admin	PASSW0RD
PowerVC VM-A	192.168.93.45	root	PASSW0RD
Service VM-A	192.168.93.47	root	PASSW0RD
HMC virtual appliance-A	192.168.93.61	hscroot	abc1234
		hscpe	abc1234

Table 3. List of IP addresses, user IDs, and passwords (secondary node management)

	IP address	Default user ID	Default password
PureKVM-B	192.168.93.144	root	PASSW0RD
		admin	PASSW0RD
PureMgr VM-B	192.168.93.146	root	PASSW0RD
		admin	PASSW0RD
PowerVC VM-B	192.168.93.145	root	PASSW0RD
Service VM-B	192.168.93.147	root	PASSW0RD
HMC virtual appliance-B	192.168.93.161	hscroot	abc1234
		hscpe	abc1234

Identifying operating system ports

Learn about the operating system ports, including the PureKVM host operating system ports, the PurePower Integrated Manager guest operating system ports, the Service guest operating system ports, the PowerVC guest operating system ports, and the HMC virtual appliance guest operating system ports.

Identifying the PureKVM host operating system ports:

Learn about the PureKVM host operating system ports, including the traffic direction, port, usage, and protocol.

Table 4. PureKVM host operating system ports

Traffic direction	Port	Usage	Protocol
Inbound	22	Linux operating system	SSH
Inbound	123 / User datagram protocol (UDP)	Linux operating system	NTP
Outbound	22	Linux operating system	SSH
Outbound	123 / UDP	Linux operating system	NTP

Identifying the PurePower Integrated Manager guest operating system ports:

Learn about the PurePower Integrated Manager guest operating system ports, including the traffic direction, port, usage, and protocol.

Table 5. PurePower Integrated Manager guest operating system ports

Traffic direction	Port	Usage	Protocol
Loopback	8080 / transmission control protocol (TCP)	Apache HTTPd web server	HTTP
Loopback	8282 / TCP	Python REST server	HTTP
Inbound	443 (SSL) / TCP	Apache HTTPd web server	HTTPS
Inbound	22 / TCP	Linux operating system	SSH
Inbound	22 / TCP	Linux operating system	SSH
Inbound	5666 / TCP	Nagios NRPE	Private
Inbound	161 / user datagram protocol (UDP) [1]	Nagios SNMP	SNMP
Inbound	162 (SSL) / UDP [1]	Nagios SNMP	SNMP
Inbound	3260 / TCP	PureMgr	iSCSI
Inbound	25 TCP	Nagios notifications	SMTP
Inbound	110 / TCP	Nagios notifications	POP3
Inbound	995 (SSL) / TCP	Nagios notifications	POP3
Inbound	143 / TCP	Nagios notifications	IMAP
Inbound	993 (SSL) / TCP	Nagios notifications	IMAP
Inbound	123 / UDP	Linux operating system	NTP
Outbound	162 (SSL) / UDP [1]	Nagios SNMP	SNMP
Outbound	161 / UDP [1]	Nagios SNMP	SNMP
Outbound	5666 / TCP	Nagios NRPE	Private
Outbound	110 / TCP	Nagios Notifications	POP3
Outbound	25 / TCP	Nagios Notifications	SMTP
Outbound	995 (SSL)	Nagios Notifications	POP3
Outbound	143 / TCP	Nagios notifications	IMAP
Outbound	993 (SSL) / TCP	Nagios notifications	IMAP
Outbound	22	Linux operating system	SSH
Outbound	443 (SSL) / TCP	Apache HTTPd web server	HTTPS
Outbound	3260 / TCP	PureMgr	iSCSI
Outbound	123 / UDP	Linux OS	NTP
[1] If you want, ports 161 / UDP and 162 / UDP that are used for SNMPv1/v2 can be disabled.			

Identifying the Service guest operating system ports:

Learn about the Service guest operating system ports, including the traffic direction, port, usage, and protocol.

Table 6. Service guest operating system ports

Traffic direction	Port	Usage	Protocol
Inbound	22	Linux operating system	SSH
Inbound	123 / user datagram protocol (UDP)	Linux operating system	NTP
Inbound	5666 / Transmission control protocol (TCP)	Nagios NRPE	Private
Inbound	67 / UDP	POWER8® service processor IPs	DHCP
Inbound	68 / UDP	POWER8 service processor IPs	DHCP
Outbound	22	Linux operating system	SSH
Outbound	123 / UDP	Linux operating system	NTP
Outbound	5666 / TCP	Nagios NRPE	Private
Outbound	67 / UDP	POWER8 service processor IPs	DHCP
Outbound	68 / UDP	POWER8 service processor IPs	DHCP

Identifying the PowerVC guest operating system ports:

Learn about the PowerVC guest operating system ports, including the traffic direction, port, and protocol.

Table 7. PowerVC guest operating system ports

Traffic direction	Port	Protocol
Inbound	80 [1]	HTTP
Inbound	443	HTTPS
Inbound	5000	HTTPS
Inbound	5470	HTTPS
Inbound	5671	AMQPS
Inbound	8428	HTTPS
Inbound	8774	HTTPS
Inbound	8777	HTTPS
Inbound	9000	HTTPS
Inbound	9292	HTTPS
Inbound	9696	HTTPS
Inbound	35357	HTTPS
Inbound	123 / UDP	NTP
Outbound	22	SSH
Outbound	389	LDAP
Outbound	636	LDAPS
Outbound	12443	HTTPS
Outbound	123 / UDP	NTP
[1] Only redirects to port 443. You can disable it if you want users to use port 443 only.		

Identifying the HMC virtual appliance guest operating system ports:

Learn about the Hardware Management Console (HMC) virtual appliance guest operating system ports, including ports and usage.

Table 8. HMC virtual appliance guest operating system ports

Port	Service
443	Secure Web Access
8443	Secure Web Access
9960	Secure Web-Access
12443	Secure Web-Access
80	Web Access
30000, 30001	Nets (HMC-FSP SSL communications)
2300 (non-SSL), 2301 (SSL)	5250
22	Secure Shell
icmp echo	Ping
5989	Open Pegasus
9900:UDP	FCS Datagram
9920	FCS
657:UDP, 657:TCP	RMC
1701:UDP	L2TP
500:UDP, 4500:UDP, ESP	Internet VPN Service Management Connection
427:UDP	SLP
12347:UDP, 12348:UDP	RSCT Peer Domains
161:TCP 151: UDP	SNMP Agent
9090, 9940, and 30000 through 30009	WEB-SM
9735	TTY
9443	Secure ASMI (introduced at V5R1.0)
4411	Bob Cat
4412	Eclipse
2302	TTY Proxy
9197, 9198	CIM Indicator
5988	CIM
8899	Cluster Ready Hardware Server
25 (configurable)	SMTP
162:TCP, 162:UDP	SNMP Traps
123:UDP	NTP
2049	NFS
23	Telnet

For more information about HMC virtual appliance firewall considerations, see HMC Firewall Information.

Setting up SELinux

Security-Enhanced Linux (SELinux) on the hypervisor must be disabled or the permissions must be set up correctly.

1. To set SELinux to permissive, type the following command:
   ```
   sed -i s/^SELINUX=.*$/SELINUX=permissive/ /etc/selinux/config
   setenforce 0
   ```
2. To set SELinux to disabled, type the following command:
   ```
   sed -i s/^SELINUX=.*$/SELINUX=disabled/ /etc/selinux/config
   ```
3. After you run a command, restart the system to save the changes permanently.
4. After you restart the system, you can use the **getenforce** command to see the SELinux status.

Getting operating system fixes for the PurePower System

Learn how to get fixes for the AIX® and the Red Hat Enterprise Linux (RHEL) operating system.

Getting AIX operating system fixes for the PurePower System

Learn how to get fixes for the AIX operating system.

To get fixes for the AIX operating system, complete the following steps:

1. Go to the Fix Central website.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **System p**.
4. From the **Product** list, select **AIX**.
5. From the **Version** list, select the current AIX version.
6. Click **Continue** and follow the on-screen instructions to download and install fixes to your operating system.

Getting Linux operating system fixes for the PurePower System

Learn how to get fixes for Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) operating systems.

Important: Power® versions of RHEL (pRHEL) and Intel versions of RHEL (xRHEL) are available. The guest operating system on the PurePower Integrated Manager is running on Intel RHEL 7.X. Any virtualized deployments on POWER8 processor-based servers are running logical partitions on Power RHEL for big endian (BE) or little endian (LE).

To get fixes for the RHEL or SLES operating systems, complete the following steps:

1. Choose from the following options:
   - If you are getting fixes for xRHEL, continue with step 2.
   - If you are getting fixes for pRHEL or SUSE, continue with step 3 on page 11.
2. If you are getting fixes for the xRHEL operating system that is running on your PurePower Integrated Manager, complete the following steps:
   a. Check for updates on the Red Hat subscription service.
   b. Download any needed Red Hat Packaging Manager (RPM) files.
   c. Follow the on-screen prompts.

   Important: It is mandatory that for each of the xRHEL Operating Systems (KVM Host OS, puremgr guest, service guest, and powervc guest) that the Red Hat Satellite Subscription Management services are utilized to perform all applicable Errata advisory updates to address fixes and security vulnerabilities as supported from Red Hat. For more information on how-to, consult your Red Hat Satellite Subscription services.

Please verify that your `recovery_volume.properties` file matches the latest configuration. For more information, see **Determining the hypervisor recovery volume characteristics** (http://www.ibm.com/support/knowledgecenter/POWER8/p8ef9/p8ef9_hypervisor_vm_disk_locations.htm). If you are not using the xRHEL samba rpm's, the xRHEL KVM Host must remove the samba rpm's due to known bugs (or update to latest fix level via RH Errata). On the KVM Host, use the **# rpm -e samba** command to remove the samba rpm's.

3. If you are getting fixes for the pRHEL or SLES operating system, complete the following steps:
   a. Go to the Fix Central website.
   b. Click the **Select product** tab.
   c. From the **Product Group** list, select **System p**.
   d. From the **Product** list, select **Linux**.
   e. Choose from the following options:
      - To update pRHEL: From the **OS level** list, select **Red Hat** and click **Continue**.
      - To update SLES: From the **OS level** list, select **SuSE** and click **Continue**.
   f. Follow the on-screen instructions to download and install fixes to your operating system.

Related information:

https://access.redhat.com/support/policy/updates/errata

Getting IBM i operating system fixes for the PurePower System

Learn how to get fixes for the IBM i operating system.

To get fixes for the IBM i operating system, complete the following steps:

1. Go to the Fix Central website.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **System i**.
4. From the **Product** list, select **IBM i**.
5. Click **Continue** and follow the on-screen instructions to download and install fixes to your operating system.

Managing security for the Pure Manager guest operating system

The Pure Manager guest operating system creates a **puremgradmin** group. A user of admin is created in the **puremgradmin** group with root level authority. The file and directory ownership of IBM included code is located in the **puremgradmin** group and root user.

For example:

```
-rwxr-xr-x. 1 root puremgradmin  1761 Sep 24 11:35 remove_rack
```

Any user ID that is created on the PurePower Integrated Manager guest operating system can be used to log in to the PurePower Integrated Manager web interface and perform any action from the web interface. Accounts that are created on the PurePower Integrated Manager guest operating system need to be restricted only to users that need to manage the devices of the PurePower System.

The Pure Manager guest operating system defines the following for backing up files:

```
[root@puremgrvm ~]# cat /etc/backup.conf
/opt/ibm/puremgr/data
/usr/local/nagios/etc
/usr/local/nagios/var
```

When a new update of the Pure Manager guest operating system is installed (through Fix Central), the `setupguests.sh -u` option is used. This option loads the archived backed up files from the Pure Manager

guest operating system and to the newly installed Pure Manager Guest operating system. This operation results in an upgrade of the Pure Manager guest operating system.

When the Pure Manager guest operating system is updated, the default user IDs and passwords are reset back to the factory settings.

PureKVM host operating system and SSH key exchanges

During the bare metal installation, the Red Hat Enterprise Linux (RHEL) 7.1 KVM host operating system exchanges Secure Shell (SSH) keys with the four guest operating systems (Pure Manager, PowerVC, HMC virtual appliance, and the service guest operating systems).

Note: The PureKVM host operating system supports only English characters (`LANG=C`). It does not support any mount point creations and other such creations that use any non-English-language or characters.

After you update each guest operating system through the Fix Central website, the **`setupguests.sh`** will also exchange SSH keys with each guest operating system. If required, the `ssh` file located in the `/root/.ssh/authorized_keys` path (Pure Manager, PowerVC, and service guest operating systems) or in `/home/hscroot/.ssh/authorized_keys2` path (HMC virtual appliance guest operating system) can be removed from each of the guest operating systems to remove the password-less SSH capabilities.

Getting fixes and checking compliance for the PurePower System

Learn how to get fixes and check compliance for the PurePower System.

Getting updates for the PurePower System

Use the Acquire updates window to download updates and to update the resources to the base version or the recommended version for the selected PurePower Integrated Manager version.

Note: For additional details about getting updates refer to the Learn more and Rack Update Guidance on-line help links on the Updates and Compliance window.

To get updates, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Updates and compliance** icon. The Updates and Compliance window is shown.
3. Select **Updates** from the View list.
4. Select the Resource Types for which you want to download updates.
5. Click **Download Updates**. The Download Updates window is shown.
6. In the Update Types area, choose either **base updates** or **recommended updates**. Depending on your selection, the most current update information is compiled.
7. Select the wanted fixes from the list of fixes that are shown.
8. Click **Download**. The download starts.
9. View and track the progress of firmware or software updates that are downloaded for various types of resources. The resource type is displayed as the parent

Getting fixes for the PurePower Integrated Manager

You can use the Fix Central website to get fixes for the PurePower Integrated Manager.

When service packs become available for the PurePower Integrated Manager, you can use the Fix Central website to get best practice information and download instructions.

To get fixes for the PurePower Integrated Manager firmware, complete the following steps:

1. Go to the Fix Central website.

2. Click the **Select product** tab.
3. From the **Product Group** list, select **PureSystems**.
4. From the **PureSystems** list, select **PurePower Systems**.
5. From the **PurePower Systems** list, select **Management devices**.
6. From the **Management devices** list, select **PurePower Management node**.
7. From the **PurePower Management node** list, select **8374-01M**.
8. From the **Installed Version** list, select the current version of your PurePower System.
9. Click **Continue** and follow the on-screen instructions to download and install firmware fixes to your system.

Checking the updates and compliance of devices in the PurePower System

Learn how to check and verify the version compliance of the existing firmware or software versions that are installed in the devices for the selected PurePower Integrated Manager version by using the Updates and Compliance page in the PurePower Integrated Manager.

Updates and Compliance of devices in a PurePower System rack

Use the Updates and Compliance window in the IBM PurePower Integrated Manager to view information about devices and to check version compliance of the existing firmware or software versions that are installed in the devices for the selected PurePower Integrated Manager version.

The Updates and Compliance window provides a comparison of the firmware or software version that are installed on the device and the base version and the recommended version. You can also download the firmware or software versions by using the links that are provided in the Base Version and Recommended Version columns (when an update is available).

The following fields are displayed in the Updates and Compliance window:

Table 9. Fields and controls for the Updates and Compliance window

Field	Description
Assess compliance for PurePower version	Selects the version of the PurePower Integrated Manager against which version compliance of the devices is to be assessed.
View	Toggle between the Compliance window and the Updates window.

The following fields are displayed in the Compliance window:

Table 10. Fields and controls for the Compliance window

Field	Description
Retrieve Recommendations	Retrieves the latest recommended firmware or software versions of PurePower System rack devices for all supported PurePower Integrated Manager releases from the Fix Level Recommendation Tool (FLRT). The date that is displayed below the table provides information about when the recommendations were last updated.

Table 10. Fields and controls for the Compliance window (continued)

Field	Description
Settings	You can change the modes for retrieving recommendations from the Fix Level Recommendation Tool (FLRT). The following are the possible modes for retrieving recommendations: • Online: This mode must be used when the PurePower Integrated Manager VM has internet access • Proxy: This mode must be used when the PurePower Integrated Manager VM does not have internet access, and another machine with internet access to which the virtual machine can connect is available. • Offline: This mode must be used when the PurePower Integrated Manager VM does not have access to internet and it is not connected to any machine that has internet access.
Retrieve Installed Version	Retrieves the currently installed version information for the selected device. If no devices are selected in the table, then the version information for all devices is retrieved.
Show/Hide Fix Details	Shows or hides the listing of all the firmware or software fixes for the installed version, base version, and recommended versions for the devices.
Assess compliance for PurePower version	Selects the version of the PurePower Integrated Manager against which version compliance of the devices is to be assessed.
Label	Displays the name of the device.
Type	Displays the type of device.
Rack - EIA Location	Specifies the rack label and the Electronic Industries Alliance (EIA) location within the rack.
IP Address	Displays the IP address of the device.
Installed Version	Displays the version of the firmware or software that is installed in the device.
Base Version	Displays the recommended firmware or software version at PurePower Integrated Manager release time.
Recommended Version	Displays the currently recommended firmware or software version.
Version Status	Displays the version status of the device. The possible values follow: • Up To Date: Device firmware or software version matches with the recommended version. • Update Available: Device firmware or software version matches with the base version and is different from the recommended version. • Update Required: Device firmware or software version is different from the supported versions, that is, from the base version and the recommended version. • Not Supported: The selected PurePower System version does not support the device. • Not Available: PurePower Integrated Manager cannot retrieve the installed version of the device firmware or software.

The following fields are displayed in the Updates window:

Table 11. Fields and controls in the Updates window

Field	Description
Download Updates	Prompts for the fixes to download for the selected resource type.
Remove Updates	Removes the selected updates from the view.
Refresh	Refreshes the fix information in the view.
Show/Hide Fix Details	Shows or hides the listing of all the firmware or software fixes for the installed version, base version, and recommended versions for the devices.
Resource Update	Lists resource types and any updates for those resource types.
Update Type	Indicates whether the update is a base update or a recommended update.
Download Size	Indicates the size of the update.
Download Status	Shows the download status for an update (100% indicates that an update has been downloaded).
Download Location	Lists the location of the update on the server.

Verifying the version compliance of the devices in a PurePower System rack

By using the Updates and Compliance page of the IBM PurePower Integrated Manager, you can check version compliance of the existing firmware or software versions that are installed in the PurePower System rack devices against the selected PurePower Integrated Manager version.

To verify the version compliance of the devices, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Open the Updates and Compliance page by clicking the icon on the left menu.
3. Select the version of the PurePower Integrated Manager to check version compliance from the **Assess compliance for PurePower version** list. This action is needed to ensure that the version compliance check is performed against the specific stack version that is selected.
4. Depending on your requirement, you can complete one of the following options:
   - If you have installed any device or firmware recently, or if you have not checked the current version information of any devices or firmware recently, click **Retrieve Installed Version**. The current version information of all the devices in the rack and the version compliance status is displayed.

     Note:

     – When the version status is displayed as **Update Required**, click the base or recommended version to download an update to the firmware (or software). After the updates are installed, return to the Updates and Compliance page and click **Retrieve Installed Versions** to obtain the latest details and check for version compliance.

     – When the version status is displayed as **Update Available**, click the recommended version to download an update to the firmware (or software). After the updates are installed, return to the Updates and Compliance page and click **Retrieve Installed Versions** to obtain the latest details and check for version compliance.
   - If you want to retrieve the latest recommended firmware or software versions for all supported releases from the Fix Level Recommendation Tool (FLRT) and verify version compliance, click **Retrieve Recommendations**. The latest versions are retrieved from FLRT and version compliance check is performed. The time stamp that is displayed below the table provides information about when the recommendations were retrieved last.

5. If the version compliance status is **Update Required or Update Available**, update the respective device firmware or software version to the supported version. It is recommended to update the firmware or software to the recommended version to obtain the latest fixes.

Recommendation retrieval modes

The Fix Level Recommendation Tool (FLRT) connection setup can be configured in the virtual machine (VM) that is installed with the PurePower Integrated Manager to retrieve the latest recommended firmware or software versions for all supported releases by using various retrieval modes. Online, proxy, and offline are the available modes in the PurePower Integrated Manager to retrieve recommendations. You can set the recommendation retrieval modes by using the PurePower Integrated Manager interface or by using the command line.

Online mode

Use the Online mode when the PurePower Integrated Manager VM has internet access. To set the recommendation retrieval mode to online, complete the following steps:

1. Choose from the following options:
   - To use the PurePower Integrated Manager, continue with step 2.
   - To use the command line, continue with step 6.
2. Log in to the PurePower Integrated Manager.
3. Click the **Updates and compliance** icon.
4. Click **Settings** and select the online option.
5. Click **OK**. This completes the steps to set the recommendation retrieval mode in the PurePower Integrated Manager.
6. At the command line, change the directory to the `bin` directory. Type the following command and press **Enter**:
   ```
   cd /opt/ibm/puremgr/bin
   ```
7. To set the mode to online, type the following command and press **Enter**:
   ```
   set_compliance_config -c online
   ```

Proxy mode

Use the Proxy mode when the PurePower Integrated Manager VM does not have internet access, and when you have another machine with internet access to which the virtual machine can connect to.

The following requirements must be met on the proxy machine to successfully retrieve information from the FLRT by using the proxy mode:

- Internet access
- Python 3.4
- Red Hat Enterprise Linux as the operating system
- The PurePower Integrated Manager VM must be able to connect to the proxy machine through Secure Shell (SSH)

To set the recommendation retrieval mode to proxy, complete the following steps:

1. Choose from the following options:
   - To use the PurePower Integrated Manager, continue with step 2.
   - To use the command line, continue with step 6 on page 17.
2. Log in to the PurePower Integrated Manager.
3. Click the **Updates and compliance** icon.
4. Click **Settings** and select the proxy option.

5. Click **OK**. This completes the steps to set the recommendation retrieval mode in the PurePower Integrated Manager.
6. At the command line, change the directory to the `bin` directory. Type the following command and press **Enter**:
   ```
   cd /opt/ibm/puremgr/bin
   ```
7. To set the mode to proxy, type the following command and press **Enter**:
   ```
   set_compliance_config -c proxy -i ip_address - u username
   ```

Where `ip_address` is the IP address of the proxy machine and `username` is the user name to log in to the proxy machine.

You are prompted to enter the password to connect to the proxy machine.

Offline mode

Use the Offline mode when the PurePower Integrated Manager VM does not have access to internet and it is not connected to the machine that has internet access.

To set the recommendation retrieval mode to offline, complete the following steps:

1. Choose from the following options:
   - To use the PurePower Integrated Manager, continue with step 2 on page 16.
   - To use the command line, continue with step 6.
2. Log in to the PurePower Integrated Manager.
3. Click the **Updates and compliance** icon.
4. Click **Settings** and select the offline option.
5. Click **OK**. This completes the steps to set the recommendation retrieval mode in the PurePower Integrated Manager.
6. At the command line, change the directory to the `bin` directory. Type the following command and press **Enter**:
   ```
   cd /opt/ibm/puremgr/bin
   ```
7. To set the mode to offline, type the following command and press **Enter**:
   ```
   set_compliance_config -c offline
   ```

Retrieving recommendations manually

When you are using the offline mode, you must manually download the fix level recommendations and transfer the fix to the PurePower Integrated Manager VM. You can use the same process when you encounter connection issues in the online or proxy mode.

To manually retrieve recommendations from the FLRT, complete the following steps:

1. Identify an internet machine that meets the following requirements:
   - Internet access
   - Python 3.4
   - Red Hat Enterprise Linux 7.1 or later as the operating system
   - Secure Shell (SSH) must be available and enabled
2. Transfer the file `offline_flrt_query_X.Y.Z.tar.gz` (where X.Y.Z is the version of the PurePower Integrated Manager) in the `/opt/ibm/puremgr/data` directory of the PurePower Integrated Manager VM to the `/tmp` folder in the machine.
3. Extract the file on the internet machine in the `/tmp` folder.
   ```
   tar -zxvf offline_flrt_query_1.1.0.tar.gz
   ```

4. An opt directory is created in the /tmp directory. Change the directory by running the following command:

   ```
   cd /tmp/opt/ibm/puremgr/bin
   ```

5. Run the **generate_stack_definition** script on the internet machine. For example,

   ```
   [root@ph-remote-server bin]# ./generate_stack_definition
   WARNING:root:flrt_query.write_parse_xml_response_to_file:: HMC base_link in
   PurePower stack version 1.3.0 is either not present or empty.
   ```

   After the script runs successfully, the following message is displayed:

   ```
   PurePower stack definitions file has been successfully created at
   /tmp/stack_definitions.json.flrt
   Successful.
   ```

   Note: Ignore any warning messages if the script completes successfully.

6. Copy the file with the flrt extension that is created by running the **generate_stack_definition** script to the PurePower Integrated Manager VM.
7. On the PurePower Integrated Manager VM, back up the existing stack definition file.

   ```
   cp /opt/ibm/puremgr/etc/stack_definitions.json /opt/ibm/puremgr/etc/
   stack_definitions_backup.json
   ```

8. On the PurePower Integrated Manager VM, overwrite the stack definition file with the file that was generated in the internet machine.

   ```
   cp /tmp/stack_definitions.json.flrt /opt/ibm/puremgr/etc/stack_definitions.json
   ```

Backing up the components of a PurePower System

You need to back up several components of a PurePower System, including the PurePower Integrated Manager, switch configurations, and the V7000 Controller and V7000 expansion unit.

Backing up and restoring the PurePower Integrated Manager hypervisor data

Learn how to back up and restore the PurePower Integrated Manager hypervisor data.

Backing up the PurePower Integrated Manager hypervisor data

The /data directory on the primary management node hypervisor is used as a local copy of the Guest operating system backup files (if the Guest operating system is set to back up files in the /etc/backup.conf file).

You can specify files and directories that you want to back up to the local hypervisor disk for each guest operating system. On each guest operating system, the/etc/backup.conf file contains a list of files or directories that are backed up based on a cron job in the hypervisor. You can customize the /etc/cron.d/purepower-backup job to run at any frequency you want. You can copy the guest operating system files to the hypervisor local disk by submitting an SSH rsync request. For information about customizing the cron job entry, see the README.backup file.

Note: If you want to manually perform the backup or replication operation, you can run the following command as a root user from the PurePower KVM Hypervisor operating system. Use 192.168.93.44 for the primary management node and 192.168.93.144 for the secondary management node.

/data/purekvm/bin/purepower_replicate.sh (This command is a symbolic link to the /data/purekvm/bin/backupdata.sh command. Both commands have the same capabilities).

The /data directory on the primary management node hypervisor is the first location of the backed up files or directories. If the **enable_external_recovery=true** parameter (which is the factory setting) is set in the /data/purekvm/recovery_volume.properties file, the recovery_volume.properties file defines where an extra external recovery volume is located and how to access it. The **volume_name** file is mounted on the

hypervisor, and then the hypervisor local disk replicates the proper `/etc/backup.conf` files to the `recovery_volume.properties` file that is specified on the same schedule as the `/etc/cron.d/purepower-backup` job.

If the **master=guest** parameter is defined in the `recovery_volume.properties` file, the guest operating system resynchronizes its files to the hypervisor local disk first, and if optionally configured, and then to the external recovery volume.

If the **master=other** parameter is defined in the `recovery_volume.properties` file, the contents of the external recovery volume are copied first to the `/data` file on the hypervisor and then copied to the guest operating systems.

The messages for the cron jobs and the **backupdata.sh** (the script that runs the nightly cron job) are logged in the `/var/log/messages` file on the KVM hypervisor operating system.

See the Exit Values for `rsync` calls that are logged to the `/var/log/messages` file on the PureKVM Host operating system. For more information, see the rsync website (https://download.samba.org/pub/rsync/rsync.html).

To mount the iSCSI volume group and to back up any data to meet local and global disaster recovery program requirements as per the customer data center guidelines, see the Recovering the hypervisor iSCSI volume topic.

The network, SAN, or IBM Storwize V7000 storage devices do not backup the configuration files automatically. If you backup the configuration files manually, and if the output files are stored in the appropriate `/etc/backup.conf` configuration file, the backup files can be archived by using the 'recovery volume' data to restore the data for use in a disaster recovery operation. The backed up configuration file must be setup and managed by the customer.

If a complete hardware failure or RAID failure of the local disk of the hypervisor occurs, an RHEL 7.1 operating system is needed to use the `purekvm.tgz` tool set. You can download the tool set from the Fix Central website, which allows a bare metal installation of the 8374-01M system after such hardware or disk failure is remediated. Customers must ensure to get access to the 'recovery' volume data to use it for rebuilding their configuration.

README.backup file

The README.backup file provides information about customizing the cron job entry.

To open the readme file, enter the following command:

```
# cat /data/purekvm/README.backup
```

The backup operation copies data from the guests into the `/data/<guest-name>` folder for safe keeping. If the **enable_external_recovery_volume** parameter is set to true in the **/recovery_volume.properties** file, the backup data also copies into the IBM Storwize V7000 storage device.

By default, a cron job entry is added to the `/etc/cron.d/purepower-backup` location.

The contents of the script is similar to the following example:

```
0 3 * * * root /data/purekvm/bin/backupdata.sh
```

In this example, the **backupdata.sh** script runs as root at 3 am every day. If you need to add additional cron job entries and edit the user cron job tab, you can use the **crontab -e** option for the root user.

You can edit the purepower-backup file to modify the time. The details of time must be specified in the following format:

```
* * * * * <command to execute>

      | | | | |

      | | | | |

      | | | |  --- day of the week (0-6). 0 is sunday and 6 is saturday

      | | |  ------- month (1-12)

      | |  ----------- day of month (1-31)

      |  --------------- hour (0-23) 0 is midnight, 23 is 11pm

       ------------------- minutes (0-59)
```

Examples:

- To run a command at 12 midnight and 12 noon, type **0 0,12 * * ***
- To run a command at 5 AM on weekdays, type **0 5 * * 1-5**
- To run a command every alternate hour, type **0 */2 * * ***

You can edit the /recovery_volume.properties file to modify the backup behavior.

Set the **enable_external_recovery_volume** parameter to true to copy the backup data to the external storage.

Cross mount management node recovery volume for redundancy

Learn how to enable the capability to mount the redundant side of the management node recovery volume. For example, to mount the recovery volume of the **Primary Management Node Side A** to the recovery volume of the **Secondary Management Node Side B** and then synchronize Side A recovery data with Side B to bring Side B up-to-date to take over the management capabilities.

Note: You must power off the system that is used as the source during the cross mount operation to prevent any possibility of data overwrites to the IBM Storwize V7000 recovery volume. Normal operations write only to the recovery volume during the nightly KVM host operating system cron job (the backupdata.sh job at 3 AM Coordinated Universal Time (UTC)) or by invoking the purepower_replicate.sh job as a ROOT user by using the command-line interface (CLI).

Important: If you updated the superuser password for the IBM Storwize V7000 on the KVM Host Side A, then you must manually set the KVM Host Side B before the Cross Mount steps are completed. Use the **pp_recvol_props** script to update the recovery_volume.properties file with the properly encoded password for the IBM Storwize V7000. For steps on how to update the **storage_password** in the recovery_volume.properties file, see **Determining the hypervisor recovery volume characteristics**(http://www.ibm.com/support/knowledgecenter/POWER8/p8ef9/p8ef9_hypervisor_vm_disk_locations.htm).

The management node recovery volumes can be cross mounted in two methods:

- Manual
- Automated

Manual cross mount

Setup to cross mount the recovery volume

On the IBM Storwize V7000 storage device:

To add a host mapping to Side B of Side A's **purepower_recoverya** volume to PureKVM Side B, complete the following steps:

1. Open a web browser and connect to your IBM Storwize V7000 web interface (https://192.168.93.8 superuser/passw0rd).
2. In the navigation area, click **Hosts**.

   Note: If you previously shut down the **purekvmb** host, then the **purekvmb** host will be offline.
3. Right-click the **purekvmb** host and select **Modify Mappings**.
4. Locate the **purepower_recoverya** volume from the list on the left and click the right arrows to add it to the list on the right.
5. Click **Apply**.
6. Click **Map All Volumes** in the warning message window about multiple hosts that are mapped to the same volume.

On the PureKVM Side B:

```
# iscsiadm -m discovery -t sendtargets -I purepower_iface -p 192.168.93.4
# iscsiadm -m session --rescan
# mkdir /recoverya
# mount /dev/sdc /recoverya <=== Retrieve the /dev/sdX value from "iscsiadm -m session -P 3" output

# vi /data/purekvm/recovery_volume.properties <=== Change master=other and
mount_point=/recoverya

# /data/purekvm/bin/purepower_replicate.sh <=== Run this command as ROOT to manually invoke the flow to
pull Side A data into Side B
```

Setup to restore the original mount of the recovery volume

On the IBM Storwize V7000 storage device:

To remove the host mapping on Side B's **purepower_recoverya** volume (**purekvmb** host must be mapped only to **purepower_recoveryb**), complete the following steps:

1. Open a web browser and connect to the web interface of the IBM Storwize V7000 storage device (https://192.168.93.8 superuser/passw0rd).
2. Click **Hosts**.
3. Right-click the **purekvmb** host and select **Modify Mappings**.
4. Locate the **purepower_recoverya** volume in the list on the right and click the left arrows to remove it from the list on the right.
5. Click **Apply**.
6. Click **Close** and then **Cancel** out of the Modify Host Mappings window.
7. In the navigation pane, click **Hosts** > **HostMappings** to verify that the **recoveryb** host is mapped only to the **purepower_recoveryb** volume.

On the PureKVM Side B:

```
# umount /recoverya
# rm -rf /recoverya
# vi /data/purekvm/recovery_volume.properties <=== Change master=guest and
mount_point=/recoveryb

# /data/purekvm/bin/purepower_replicate.sh<=== Run this command as ROOT to manually invoke the flow
for Side B to replicate out the newly obtained data from Side A
```

On the other virtual machines (VMs):

1. Check that all your Side B devices are in the Pure Manager that you want to monitor.

2. Perform any **sudo service puremgr restart** type operations to pick up the new data.
3. Perform any **Manual Restore of HMC virtual appliance POWER8 Profiles**.
4. Perform the manual PowerVC Restore process on the latest backup available. For information, see Recovering IBM Power Virtualization Center data.

Automated cross mount

From the PurePower Keyboard/Video/Mouse (KVM) console, complete the following steps:

1. Select the **IBM PPIM Cross Mount** shortcut on the RHEL desktop.

   You will be prompted with confirmation messages, the output on results, and further references to the Knowledge Center web links to perform any required or optional procedures.

On the other virtual machines (VMs):

1. Check that all your Side B devices are in the Pure Manager that you want to monitor.
2. Check that the PowerVC restoration was completed as required. The restoration is automatically done during automation of the cross mount.
3. Confirm that the HMC virtual appliance POWER8 profiles are as required. If any corrective actions are required, see HMC Manual Reference Pages - RSTPROFDATA.

Manual Restore of HMC virtual appliance POWER8 Profiles

You need to manually **scp** the `/recoveryX` POWER8 profiles to the Hardware Management Console (HMC) virtual appliance.

Recovering the hypervisor iSCSI volume

Learn how to manually mount and make copies of the hypervisor iSCSI volume.

To mount the iSCSI recovery volume, complete the following steps from the PureKVM hypervisor:

1. Run the following command:

   ```
   # iscsiadm -m discovery -t sendtargets -I purepower_iface -p 192.168.93.4
   ```

   The **iscsi-target** node is returned from the source in the IBM Storwize V7000.
2. Run the following command:

   ```
   # service iscsi restart
   ```

   View the device that is mounted by **iscsiadm**.
3. Run the following command:

   ```
   # iscsiadm -m session -P 3

     ************************
     Attached SCSI devices:
     ************************
     Host Number: 12
         State: running
     scsi12 Channel 00 Id 0 Lun: 0
     Attached scsi disk sdb
         State: running
   ```
4. Run the following command:

   ```
   # mount /dev/sdb /myrecovery
   ```

   Note: Make any necessary copies of the recovery volume data to the wanted location.

Determining the hypervisor recovery volume characteristics

Learn about the contents and layout of the 200 GB recovery volume.

1. Check each guest operating system `/etc/backup.conf` file for the specific files that are regularly being backed up.
2. On the PureKVM Host operating system, the `/var/log/messages` file shows the history on the cron job that is defined in `/etc/cron.d/purepower-backup`.
3. Review the default values of the `recovery_volume.properties` file. No changes should be made to the default values.

   The `recovery_volume.properties` is different for the primary management node (PUREKVMA) and for the secondary management node (PUREKVMB).

   The differences in the property files on each management node are related to the `active_recovery_volume` specification. The `active_recovery_volume` and the `secondary_recovery_volume` values are used to automate the cross mounting of the recovery volume on the two management nodes. If the primary management node is taken offline or is not usable for any reason, the recovery volume for each management node is stored on the IBM Storwize V7000 and the primary recovery volume which contains the active backed up data can be used to prime the secondary management node for the secondary management node to take over. The usage of primary and secondary management nodes is solely dependent upon the customer usage and licenses purchased. See the Cross Mount Automation section for details on how to perform the switching of the roles of the management nodes.

   PUREKVMA

```
# cat /data/purekvm/recovery_volume.properties
[recovery_volume]
enable_external_recovery_volume=true
master=guest
factory_reset=nonestorage_ip=192.168.93.8 <==== This is the IBM Storwize V7000 Cluster IP
storage_password=191665b00f94425b298cb49e0d88ecddc2c1cfe77672787e60e00a401a1fc0c8?
<=== If you are not using the PurePower Manager UI to update the V7000 superuser password,
<=== then use the pp_recvol_props script to update
<=== the storage_password to the encoded value. In normal operations you would use the
<=== PurePower Manager UI to update the V7000 superuser password and then this file would
<=== also be synchronized with that password change. If for some reason it is necessary to
<=== manually change the V7000 superuser password out-of-band of PurePower Manager UI, then
<=== this script method can be used.
storage_userid=superuser
iscsi_management_ip=192.168.93.4 <===== This is the IBM Storwize V7000 iSCSI interface
iscsi_hypervisor_ip=192.168.93.44
<=== This is the IP address of the PUREKVMA hypervisor adapter interface, which
<=== completes the iSCSI data communications
iscsi_hypervisor_interface=br1
iscsi_iface_name=purepower_iface
iscsi_management_subnet=255.255.240.0
iscsi_management_gateway=0.0.0.0
iscsi_port=3
svc_node_id=1
pool_name=CI_DISK_POOL
volume_name=purepower_recoverya
size_gb=200
powervc_gb=100
service_gb=10
puremgr_gb=40
vhmc_gb=10
iscsi_host_name=purekvma
mount_point=/recoverya
filesystem_format=ext3
```

   PUREKVMB

```
# cat /data/purekvm/recovery_volume.properties
[recovery_volume]
enable_external_recovery_volume=true
active_recovery_volume=mount_point1
secondary_recovery_volume=mount_point2
master=guest
storage_ip=192.168.93.8 <==== This is the IBM Storwize V7000 Cluster IP
```

```
storage_password=191665b00f94425b298cb49e0d88ecddc2c1cfe77672787e60e00a401a1fc0c8?
<=== If you are not using the PurePower Manager UI to update the V7000 superuser password,
<=== then use the pp_recvol_props script to update the storage_password
<=== to the encoded value. In normal operations you would use the PurePower Manager UI to update
<=== the V7000 superuser password and then this file would also be synchronized with that
<=== password change. If for some reason it is necessary to manually change the V7000 superuser
<=== password out-of-band of PurePower Manager UI then this script method can be used.
storage_userid=superuser
iscsi_management_ip=192.168.93.4 <===== This is the IBM Storwize V7000 iSCSI interface
iscsi_hypervisor_ip=192.168.93.144
<=== This is the IP address of the PUREKVMB hypervisor adapter interface, which
<=== completes the iSCSI data communications
iscsi_hypervisor_interface=br1
iscsi_iface_name=purepower_iface
iscsi_management_subnet=255.255.240.0
iscsi_management_gateway=0.0.0.0
iscsi_port=3
svc_node_id=1
pool_name=CI_DISK_POOL
volume_name1=purepower_recoveryb
volume_name2=purepower_recoverya
size_gb=200
powervc_gb=100
service_gb=10
puremgr_gb=40
vhmc_gb=10
iscsi_host_name=purekvmb
mount_point1=/recoveryb
mount_point2=/recoverya
filesystem_format=ext3
retry_count=5
retry_interval_secs=60
```

Backing up and restoring the PurePower Integrated Manager VM

Learn how to back up and restore the PurePower Integrated Manager virtual machine (VM).

To regularly run a cron job that backs up files as defined in each guest operating system in the `/etc/backup.conf` file, see “Backing up the PurePower Integrated Manager hypervisor data” on page 18.

If the hypervisor local disk fails, or there is some other reason that you need to complete a complete fresh installation and then manually use the 'recovery' volume, see “Backing up the PurePower Integrated Manager hypervisor data” on page 18 for backup instructions, and then restore the PurePower Integrated Manager VM by using this procedure.

To restore the PurePower Integrated Manager VM, complete the following steps:

1. Go to the Fix Central website. The Fix Central website has the complete set of files that are needed to complete a new installation.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **PureSystems**.
4. From the **Select from PureSystems** list, select **PurePower Systems**.
5. From the **Select from PurePower Systems** list, select **Management devices**.
6. From the **Select from Management devices** list, select **PurePower Management Node**.
7. From the **PurePower Management Node** list, select **8374-01M**.
8. From the **Installed Version** list, select the current version of your PurePower System.
9. Click **Continue**.
10. Select **Browse for fixes** and click **Continue**.
11. Select one of the following packages depending on your situation:

- **IBM® PurePower Manager Install Tools**: This package contains installation tools that are used for the installation of the PureKVM Host operating system and the four Guest operating systems.
- **IBM PurePower Integrated Manager Appliance**: This package contains the PurePower Integrated Manager guest operating system that can be used for a complete fresh installation of the operating system.
- **IBM PurePower Integrated Manager HMC Virtual Applicance**: This package contains the PurePower Integrated Manager HMC virtual appliance guest operating system that can be used for a complete fresh installation of the operating system.
- **IBM PurePower Integrated Manager PowerVC Appliance**: This package contains the PurePower Integrated Manager PowerVC guest operating system that can be used for a complete fresh installation of the operating system.
- **IBM PurePower Integrated Manager Service Application**: This package contains the PurePower Integrated Manager Service guest operating system that can be used for a complete fresh installation of the operating system.

Note: Refer to the readme file on each package for installation instructions.

Backing up and restoring the PurePower HMC virtual appliance

Learn how to back up and restore the PurePower Hardware Management Console (HMC) virtual appliance.

To regularly run a cron job that backs up files as defined in each guest operating system in the `/etc/backup.conf` file, see “Backing up the PurePower Integrated Manager hypervisor data” on page 18.

If the hypervisor local disk fails, or there is some other reason that you need to complete a complete fresh installation and then manually use the 'recovery' volume, see “Backing up the PurePower Integrated Manager hypervisor data” on page 18 for backup instructions, and then restore the PurePower HMC virtual appliance by using this procedure.

To restore the PurePower HMC virtual appliance, complete the following steps:

1. Go to the Fix Central website. The Fix Central website has the complete set of files that are needed to complete a new installation.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **PureSystems**.
4. From the **Select from PureSystems** list, select **PurePower Systems**.
5. From the **Select from PurePower Systems** list, select **Management devices**.
6. From the **Select from Management devices** list, select **PurePower Management Node**.
7. From the **PurePower Management Node** list, select **8374-01M**.
8. From the **Installed Version** list, select the current version of your PurePower System.
9. Click **Continue**.
10. Select **Browse for fixes** and click **Continue**.
11. Select one of the following packages depending on your situation:
    - **IBM® PurePower Manager Install Tools**: This package contains installation tools that are used for the installation of the PureKVM Host operating system and the four Guest operating systems.
    - **IBM PurePower Integrated Manager Appliance**: This package contains the PurePower Integrated Manager guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager HMC Virtual Applicance**: This package contains the PurePower Integrated Manager HMC virtual appliance guest operating system that can be used for a complete fresh installation of the operating system.

- **IBM PurePower Integrated Manager PowerVC Appliance**: This package contains the PurePower Integrated Manager PowerVC guest operating system that can be used for a complete fresh installation of the operating system.
- **IBM PurePower Integrated Manager Service Application**: This package contains the PurePower Integrated Manager Service guest operating system that can be used for a complete fresh installation of the operating system.

Note: Refer to the readme file on each package for installation instructions.

Backing up and restoring the PurePower Integrated Manager PowerVC VM

Learn how to back up and restore the PurePower Integrated Manager PowerVC virtual machine (VM).

To regularly run a cron job that backs up files as defined in each guest operating system in the `/etc/backup.conf` file, see "Backing up the PurePower Integrated Manager hypervisor data" on page 18.

If the hypervisor local disk fails, or there is some other reason that you need to complete a complete fresh installation and then manually use the 'recovery' volume, see "Backing up the PurePower Integrated Manager hypervisor data" on page 18 for backup instructions, and then restore the PurePower Integrated Manager PowerVC VM by using this procedure.

To restore the PurePower Integrated Manager PowerVC VM, complete the following steps:

1. Go to the Fix Central website. The Fix Central website has the complete set of files that are needed to complete a new installation.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **PureSystems**.
4. From the **Select from PureSystems** list, select **PurePower Systems**.
5. From the **Select from PurePower Systems** list, select **Management devices**.
6. From the **Select from Management devices** list, select **PurePower Management Node**.
7. From the **PurePower Management Node** list, select **8374-01M**.
8. From the **Installed Version** list, select the current version of your PurePower System.
9. Click **Continue**.
10. Select **Browse for fixes** and click **Continue**.
11. Select one of the following packages depending on your situation:
    - **IBM® PurePower Manager Install Tools**: This package contains installation tools that are used for the installation of the PureKVM Host operating system and the four Guest operating systems.
    - **IBM PurePower Integrated Manager Appliance**: This package contains the PurePower Integrated Manager guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager HMC Virtual Applicance**: This package contains the PurePower Integrated Manager HMC virtual appliance guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager PowerVC Appliance**: This package contains the PurePower Integrated Manager PowerVC guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager Service Application**: This package contains the PurePower Integrated Manager Service guest operating system that can be used for a complete fresh installation of the operating system.

    Note: Refer to the readme file on each package for installation instructions.

Backing up and restoring the PurePower Integrated Manager Service VM

Learn how to back up and restore the PurePower Integrated Manager Service virtual machine (VM).

To regularly run a cron job that backs up files as defined in each guest operating system in the `/etc/backup.conf` file, see “Backing up the PurePower Integrated Manager hypervisor data” on page 18.

If the hypervisor local disk fails, or there is some other reason that you need to complete a complete fresh installation and then manually use the 'recovery' volume, see “Backing up the PurePower Integrated Manager hypervisor data” on page 18 for backup instructions, and then restore the PurePower Integrated Manager Service VM by using this procedure.

To restore the PurePower Integrated Manager Service VM, complete the following steps:

1. Go to the Fix Central website. The Fix Central website has the complete set of files that are needed to complete a new installation.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **PureSystems**.
4. From the **Select from PureSystems** list, select **PurePower Systems**.
5. From the **Select from PurePower Systems** list, select **Management devices**.
6. From the **Select from Management devices** list, select **PurePower Management Node**.
7. From the **PurePower Management Node** list, select **8374-01M**.
8. From the **Installed Version** list, select the current version of your PurePower System.
9. Click **Continue**.
10. Select **Browse for fixes** and click **Continue**.
11. Select one of the following packages depending on your situation:
    - **IBM® PurePower Manager Install Tools**: This package contains installation tools that are used for the installation of the PureKVM Host operating system and the four Guest operating systems.
    - **IBM PurePower Integrated Manager Appliance**: This package contains the PurePower Integrated Manager guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager HMC Virtual Applicance**: This package contains the PurePower Integrated Manager HMC virtual appliance guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager PowerVC Appliance**: This package contains the PurePower Integrated Manager PowerVC guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager Service Application**: This package contains the PurePower Integrated Manager Service guest operating system that can be used for a complete fresh installation of the operating system.

    Note: Refer to the readme file on each package for installation instructions.

Backing up switch configurations to a server

Learn how to back up the SAN48b-5 (2498-F48), IBM G8052 (7120-48E), and Mellanox MSX1710 (8831-NF2) switch configurations.

Backing up the IBM G8052 (7120-48E) switch configuration to a server

Learn how to back up the IBM G8052 (7120-48E) switch.

To back up the IBM G8052 (7120-48E) switch, select one of the following procedures:

- To back up the G8052 switch configuration by using the output command, complete the following steps: Ouput a configuration backup copy of the IBM RackSwitch (7120-48E) Management Switch:
  1. Enter the following command:

     Note: This example is for the IBM G8052 Management Switch 1.

     ```
     192.168.93.44 - PureKVM RHEL Host OS
     192.168.93.83 - IBM G8052Management Switch 1
     192.168.93.81 - IBM G8052Management Switch 2
     ssh admin@192.168.93.83  pw=admin

     rackswitch1>   en
     Enable privilege granted.
     rackswitch1#   conf   t
     Enter configuration commands, one per line.  End with Ctrl/Z.

     rackswitch1(config)#  copy   running-config    sftp
     Address or name of remote host: 192.168.93.44
     Enter SFTP server port [22]:
     Destination file name: /data/backups/rackswitch1.txt
     User name: root
     Password:
     Connecting to 192.168.93.44...via port 22
     SFTP: User root logged in.
     Upload in progress
     Current config successfully sftp'd to 192.168.93.44:/data/backups/rackswitch1.txt
     ```
- To back up the G8052 switch configuration by using the G8052 command-line interface, complete the following steps:
  1. Log in to the switch.
  2. From the Configuration# prompt, enter the following command:

     ```
     rackswitch1>   en
     Enable privilege granted.
     rackswitch1#   conf   t
     ```

     ```
     ptcfg <FTP or TFTP server> <filename>
     ```

     Where `server`is the FTP/TFTP server, or IPv4 or IPv6 address or host name, and `filename` is the name of the target script configuration file.

     Note: For more information, see the IBM N/OS™ 7.4 Menu-Based CLI for the RackSwitch G8052.

Backing up the SAN58b-5 switch configuration to a server

Learn how to back up the SAN48b-5 (2498-F48) switch to a server by using interactive mode or the command line.

To back up the SAN58b-5 switch, select one of the following options:

- To upload a configuration file in interactive mode, complete the following steps:
  1. Verify that the File Transfer Protocol (FTP), Secure Shell File Transfer Protocol (SFTP), or Secure Copy Protocol (SCP) service is running on the host computer.
  2. Connect to the switch and log in as admin.
  3. Enter the **configUpload** command. Follow the on-screen prompts to back up the switch.
  4. Save the switch configuration information for future reference. The configuration file is printable, but check the number of pages of the file before printing the file.

     An example of the **configUpload** command on a switch without Admin Domains follows:

     ```
     switch:admin> configupload
     Protocol (scp, ftp, sftp, local) [ftp]: sftp
     Server Name or IP Address [host]: 10.1.2.3
     User Name [user]: UserFoo
     Path/Filename [<home dir>/config.txt]: switchConfig.txt
     ```

```
Section (all|chassis|FID# [all]): chassis
username@10.1.2.3's password:
Password: <hidden>
configUpload complete
```

- To upload a configuration file by using the command line, complete the following steps:
  1. Type the following command:
     ```
     [configupload [-all] [-p ftp | -ftp] [host,user,path[,passwd]]
     configupload [-all] [-p scp | -scp] [host,user,path]
     configupload [-all] [-p sftp | -sftp] [host,user,path]
     ```
  2. Use the following operands:

     host Specifies the name or the IP address of the external host to which the switch configuration must be uploaded. To specify the FTP server by name, you need to set up one or more Domain Name System (DNS) servers by using the **dnsConfig** command.

     user Specifies the login name for the external host.

     path Specifies the file name and path of the configuration file. Absolute path names might be specified by using a forward slash (/). If you use a relative path name, files are uploaded to the login account's home directory on UNIX hosts and into the directory on which the FTP server is running on Windows hosts. This operand is valid only when the file is uploaded to an external host.

     passwd
     Specifies the password of the account.

For more information, see Maintaining the Switch Configuration File in the Brocade Fabric OS Administrator's Guide.

Backing up the Mellanox MSX1710 (8831-NF2) switch configuration to a server

Learn how to back up the Mellanox MSX1710 (8831-NF2) switch configuration to a server.

You can create a new BIN configuration file, upload a BIN configuration file, create a new text-based configuration file, or upload a text-based configuration file.

1. Select from the following options:
   - To back up the Mellanox MSX1710 (8831-NF2) switch by using the graphical user interface (GUI), continue with step 2.
   - To back up the Mellanox MSX1710 (8831-NF2) switch by creating a BIN configuration file, continue with step 3.
2. To use the GUI, complete the following steps:
   a. Log in to the Mellanox switch by opening a web browser and entering the switch IP address (for example, https://192.168.93.35).
   b. Log in with the default login credential of admin/admin.
   c. Click **Setup** on the left of the top menu bar.
   d. Click **Configuration** on the left menu bar.
   e. Check the box for the file that is loading as running config.
   f. Click **Download** and select **Save File** to save the BIN file to your wanted location.
3. To create a new BIN configuration file, complete the following steps:
   a. Log in to the Mellanox MSX1710 (8831-NF2) switch as Admin.
   b. Type the following command:
      ```
      switch(config)#configuration upload my-filename
      scp://root@my-server/root/tmp/my-filename
      ```
   c. To upload a BIN configuration file from a switch to an external file server, complete the following steps:

1) Log in to the switch as Admin.
2) Type the following command:

```
switch (config) # configuration upload my-filename
scp://root@my-server/root/tmp/my-filename
```

d. To create a new text-based configuration file, complete the following steps:
   1) Log in to the switch as Admin.
   2) Type the following command:

```
switch (config) # configuration text generate active running save my-filename
```

e. To upload a text-based configuration file from a switch to an external file server, complete the following steps:
   1) Log in to the Mellanox MSX1710 (8831-NF2) switch as Admin.
   2) Type the following command:

```
switch (config) # configuration text file my-filename upload
scp://root@my-server/root/tmp/my-filename
```

Note: For more information, see the Mellanox MLNX-OS® User Manual for VPI.

Backing up and restoring the Storwize V7000 and Storwize V7000 expansion unit system configuration

Learn how to back up and restore the Storwize V7000 Controller and Storwize V7000 expansion unit system configuration.

The instructions to back up and restore the Storwize V7000 Controller and Storwize V7000 expansion unit are available on the Fix Central website.

Enter **IBM Storwize V7000** in the **Product selector** field and follow the on-screen instructions.

Backing up and restoring the IBM FlashSystem 900 storage enclosure system configuration

Learn how to back up and restore the IBM FlashSystem™ 900 storage enclosure system configuration

The instructions to back up and restore the IBM FlashSystem 900 storage enclosure system configuration are available on the Fix Central website.

Enter **IBM FlashSystem 900** in the **Product selector** field and follow the on-screen instructions.

Disaster recovery

Learn how to recover and rebuild your PurePower System in the unlikely event of a disaster.

In the unlikely event of a disaster that impacts your PurePower System, you can rebuild your PurePower System by completing the following steps:

1. Go to the Fix Central website. The Fix Central website has the complete set of files that are needed to complete a new installation.
2. Click the **Select product** tab.
3. From the **Product Group** list, select **PureSystems**.
4. From the **Select from PureSystems** list, select **PurePower Systems**.
5. From the **Select from PurePower Systems** list, select **Management devices**.
6. From the **Select from Management devices** list, select **PurePower Management Node**.
7. From the **PurePower Management Node** list, select **8374-01M**.
8. From the **Installed Version** list, select the current version of your PurePower System.

9. Click **Continue**.
10. Select **Browse for fixes** and click **Continue**.
11. Select one of the following packages depending on your situation:
    - **IBM® PurePower Manager Install Tools**: This package contains installation tools that are used for the installation of the PureKVM Host operating system and the four Guest operating systems.
    - **IBM PurePower Integrated Manager Appliance**: This package contains the PurePower Integrated Manager guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager HMC Virtual Applicance**: This package contains the PurePower Integrated Manager HMC virtual appliance guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager PowerVC Appliance**: This package contains the PurePower Integrated Manager PowerVC guest operating system that can be used for a complete fresh installation of the operating system.
    - **IBM PurePower Integrated Manager Service Application**: This package contains the PurePower Integrated Manager Service guest operating system that can be used for a complete fresh installation of the operating system.

    Note: Refer to the readme file on each package for installation instructions.

Managing an IBM PurePower System

The PurePower Integrated Manager is used to manage the components of the PurePower System.

Your PurePower System includes the PurePower Integrated Manager console. The PurePower Integrated Manager includes the following preintegrated resource managers:

- Virtualization management by using PowerVC
- Hardware management by using the PurePower Integrated Manager
- Converged infrastructure monitoring by using Nagios Core Open Source software

The PurePower Integrated Manager also provides the ability for you to complete system management tasks. You can track hardware inventory, monitor your systems, and manage your network.

The PurePower Integrated Manager includes the following capabilities:

- A single user interface to manage multiple compute, network, and storage resources.
- Cloud and virtualization integration by using the PowerVC.

Managing the hardware in your PurePower System by using the PurePower Integrated Manager

Learn how to manage the PurePower System hardware by using the PurePower Integrated Manager.

Viewing hardware inventory by using the PurePower Integrated Manager

You can use the hardware inventory page to view hardware inventory.

To view hardware inventory, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Hardware Inventory** icon. The Hardware Inventory window is shown.
3. Click the tab for the rack for which you want to view the inventory.
4. View the hardware inventory that is listed for the rack you selected. The inventory list includes the assigned label, the resource type, and the Electronic Industries Alliance (EIA) location. The list also

includes the user ID used to manage the resource, the machine type, and model number, the serial number of the resource (when applicable), the IP address that is associated with its management interface, and the installed version.

Adding a resource node by using the PurePower Integrated Manager

If the resource is not identified by the PurePower Integrated Manager when you add a new hardware resource to your IBM PurePower System, you must add the resource node to the hardware inventory in the PurePower Integrated Manager.

To add a resource node, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Hardware Inventory** icon.
3. Select the tab of the rack that contains the node that you want to add.
4. Click **Add** and enter the resource information:
   - Label
   - Rack-EIA location
   - IP address
   - User ID
   - Password
5. Click **OK**. The resource is added.

Notes:

- Both rack hardware resources and unmonitored resources can be added.
- The **Add Resource** function only adds the information about resources to the PurePower Integrated Manager and does not perform any configuration in the device you are adding.
- When you attempt to add a resource to the PurePower Integrated Manager, the IP address and credentials are used to access the resource. If either of those values are not correct, the **Add Resource** function fails, and an error message is displayed to help you resolve the problem.

Editing a resource node by using the PurePower Integrated Manager

You might need to change the inventory information in the PurePower Integrated Manager. For example, the user ID and password that is used to access the resource might have changed. The inventory information for a resource can be changed by editing the properties of that resource.

To edit a resource node, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Hardware Inventory** icon.
3. Select the tab of the rack that contains the node that you want to edit.
4. Select the resource node that you want to edit and click **Edit**. The Edit Resource window appears.
5. Edit the following fields as needed:
   - Label
   - Rack-EIA location
6. Select the appropriate action in the **Resource Access** section to update the User ID or Password.
7. Click **OK**. The changes are saved.

Notes:

- If the IP address of a resource needs to be changed, use the Configure Network interface to make the change to the PurePower Integrated Manager. The IP Address field on the Edit Resource window can only be used to update PurePower Integrated Manager with the actual IP address of

the resource if a change was made to the resource outside of the PurePower Integrated Manager. For instructions to configure the network, see Configuring the network by using the PurePower Integrated Manager.

- The Edit Resource window requires a value for the label and user ID fields. You can retain the default values that are displayed for those fields or you can change the values as needed, but you cannot remove the values. Additionally, if you change the default value of the user ID, you must provide the password for the new user ID that is used to manage the resource. If the user ID or password is not correct, the Edit Resource task fails and an error message is displayed to help you resolve the problem.
- If you are changing the password of the current user ID that is used to manage this resource, you need to enter the old password for the resource and the new password and confirm the new password to be used for this resource.

Removing a resource node by using the PurePower Integrated Manager

You might need to remove inventory information from the PurePower Integrated Manager for a resource. For example, a resource in your environment might be replaced. The inventory information for a resource can be removed from the PurePower Integrated Manager.

To remove a resource node, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Hardware Inventory** icon.
3. Select the tab of the rack that contains the node that you want to remove.
4. Select the resource node or nodes that you want to remove.
5. Select **Remove**. The Remove Resource pane is displayed.
6. Click **OK**. The resource is removed.

Managing virtual machines by using the PurePower Integrated Manager

You can use the PurePower Integrated Manager interface to list all virtual machines that are known to the PurePower Integrated Manager server, to specify the IP address for the managed virtual machines, to update the user name and password for the virtual machines, and to manage the virtual machines. When the PowerVC server is added to the PurePower Integrated Manager, you can view all the virtual machines that are listed in the Virtual Machines section.

All virtual machines (that are known to the PurePower Integrated Manager server) are listed in the Virtual Machines section in the PurePower Integrated Manager. The virtual machines are typically defined on a PowerVC server.

To add a new virtual machine to manage to the PurePower Integrated Manager inventory, complete the following steps:

1. Add the PowerVC server (on which the new virtual machines are defined) to the PurePower Integrated Manager. For instructions, see “Adding a resource node by using the PurePower Integrated Manager” on page 32.
2. Open the Virtual Machines section in the PurePower Integrated Manager.
3. Click **Recollect Machine Information**.

   Note: This task can take up to 2 minutes to complete.
4. When the virtual machine is listed, verify that it contains an IP address.

   Note: It is possible that the virtual machine that is listed does not contain an IP address. If an IP address is not listed, you cannot manage that virtual machine. To set an IP address for the virtual machine, select the virtual machine (without an IP address) and click **Set Address**.

5. Verify that the user ID and password to the virtual machine is current and valid.

   Note: The PurePower Integrated Manager uses the user ID and password that the PowerVC has for the virtual machine. If there is no user ID and password set or if it is out-of-date, then you cannot manage that virtual machine. To update the user ID and password, you can run the **Set User ID and Password** task from the PurePower Integrated Manager.
6. Select the virtual machine or machines that you want to manage and click the **Manage Monitoring Agent** button.
7. From the **Manage Monitoring Agent** window, select the appropriate agent to be deployed.

   Note: After the agent is deployed, the virtual machine is listed on the monitored hosts list.

Managing Power nodes and storage expansion units by using the PurePower Integrated Manager

You can use the PurePower Integrated Manager to provide inventory and inventory management support for Power nodes and storage expansion units.

The PurePower Integrated Manager supports inventory management for Power nodes and storage expansion devices. When you add a Hardware Management Console (HMC) by using the PurePower Integrated Manager graphical interface or command line interface (CLI), all Power nodes that are managed by the HMC are automatically added. When you add a storage controller, all storage expansions that are associated with the storage controller are automatically added. These devices can be removed by using the PurePower Integrated Manager graphical interface or command line interface.

Power nodes and storage expansion devices that are added to the inventory contain the following device information: device type, serial number, machine type, and model number.

Note: Other hardware devices might contain more device information, such as IP address, extra IP interfaces, and management user ID and password.

The tasks that are available (by using the graphical interface or CLI) for inventory management of Power nodes and storage expansion devices include the following tasks:

- **Change**: Changes the description of the label, rack, and rack location.
- **Remove**: Removes the selected device or devices.

If you need to physically remove Power nodes and storage expansion devices from the system, you must remove them from the inventory by using the **Remove** task. After the device is removed from the inventory and system, you can add them back to the system and inventory.

Note: Removing an HMC or storage controller from inventory does not automatically remove the associated Power nodes or storage expansions from inventory. The Power nodes or storage expansions can be removed independently.

Managing devices

You can use the PurePower Integrated Manager to manage devices. You can add racks, remove racks, edit the properties of a rack, or move a device from one rack to another. You can manage up to 400 devices. All these actions can be done using the PurePower Integrated Manager interface or the command line.

Managing devices by using the PurePower Integrated Manager

You can use the PurePower Integrated Manager interface or the command line to add, remove, and change devices.

To add, remove, or change devices, complete the following steps from the PurePower Integrated Manager:

1. To add a device, complete the following steps:
   a. Click **Hardware Inventory** to open the Hardware Inventory window.
   b. Select the tab of the rack that contains the device that you want to add.
   c. Click **Add**.
   d. Enter the requested information.
   e. On the confirmation window, click **OK**. The changes are saved.
2. To remove a device, complete the following steps:
   a. Click **Hardware Inventory** to open the Hardware Inventory window.
   b. Select the tab of the rack that contains the device that you want to remove.
   c. Select the device or devices you want to remove.
   d. Click **Remove**.
   e. On the confirmation window, click **OK**. The changes are saved.
3. To change a device, complete the following steps:
   a. Click **Hardware Inventory** to open the Hardware Inventory window.
   b. Select the tab of the rack that contains the device that you want to change.
   c. Select the device or devices you want to change.
   d. Click **Edit**.
   e. Enter the information to be changed.
   f. On the confirmation window, click **OK**. The changes are saved.

Managing devices by using the PurePower Integrated Manager command line

All device management operations can be completed from both the PurePower Integrated Manager graphical user interface and from the command line interface.

Note:

Bash command line rules apply and include the following rules:

- Output can be piped by using |.
- Parameters containing white spaces must be quoted by using either single quotation marks (') or double quotation marks (").
- Wildcard characters (*, ?) and special characters such as > < & $ and | must be escaped with a leading backslash (\).

To use the command line interface, complete the following steps:

1. Go to the command line:

   The command line interface can be started by starting an SSH session to the PurePower Integrated Manager.
2. Use the following commands and functions to manage devices:

Table 12. PurePower Integrated Manager commands and functions for device management, SNMP management, device access, and rack management

Command	Function
Device management	
add_device	Adds device for management. Adds a device to the inventory. Triggers monitoring configuration of device and Nagios plug-in configuration.

Table 12. PurePower Integrated Manager commands and functions for device management, SNMP management, device access, and rack management (continued)

Command	Function
change_device	Changes the user ID and password settings of a device, including the device password. Updates the password that is used for monitoring the device. Creates a user ID and password on the device. Changes the network for a device, including the IP address, subnet mask, and gateway address.
list_devices	Lists all or only a type of managed device with minimal or full details. Shows all the device types that are supported. **Note:** Not all devices that are listed are actively monitored. Some devices are listed for inventory management purposes only. For example, Nagios core is listed for launch integration only.
remove_device	Removes the managed device. Removes a device from inventory. Stops device monitoring and the associated Nagios plug-in.
SNMP management	
include_MIB	Lists all MIB files to the net_snmp log
set_snmp_proxy	Sets SNMP proxy for the device.
subsrcibe_snmp_server	Adds subscription for a new SNMP server.
Device access	
remote_access	Starts SSH shell for the device.
Rack management	
add_rack	Adds a rack element to which the devices can be assigned to.
change_rack	Change the rack label, data center, location, and notes for a rack.
list_racks	Provides a list of the managed racks.
remove_rack	Removes a rack element if no devices are assigned it. **Note:** To remove a rack element, all devices that are associated with the rack need to be removed first.
Updates and compliance	
retrieve_installed_version	Collects version information for the given PurePower System rack devices.
retrieve_recommendations	Retrieves recommended versions information for PurePower System rack devices.
assess_compliance	Assesses compliance for resources against the specific PurePower System stack version.
identify_updates	Retrieves the list of updates for the given resource types.
acquire_updates	Downloads the list of updates for PurePower System rack resources.
list_update_details	Lists the updates that are based on the PurePower System stack version for different resource types.
remove_updates	Removes the specified updates for the given resource types from the file system.

Managing racks by using the PurePower Integrated Manager

Learn how to manage racks by using the PurePower Integrated Manager.

You can use the command line to add, edit, and remove racks. You can use the PurePower Integrated Manager interface to add a rack, edit the properties of a rack, move a device from one rack to another rack, or remove a rack.

Adding an expansion rack to your PurePower System configuration:

You can use the PurePower Integrated Manager to add an expansion rack to your PurePower System configuration.

Note: The terms *expansion rack* and *extension rack* are interchangeable in this topic.

To add an expansion rack to your PurePower System configuration, complete the following steps:

1. Log in to the PurePower Integrated Manager with your username and password.
2. Click the **Hardware Inventory** icon. The Hardware Inventory window is shown.
3. Click **Add Rack**. The Add Rack Definition window is shown.
4. On the Rack Details window, enter the following information:

   Note: The Label field is required, the remaining fields are optional.
   - Type a name for the new rack in the **Label** field.
   - Type the name of the appropriate data center in the **Data Center** field.
   - Type the appropriate location in the **Location** field.
   - Add any notes in the **Notes** field.
5. Choose from the following options:
   - If you do not want to configure rack connections, clear the **Include rack connections** check box.
   - If you want to configure rack connections, leave the **Include rack connections** check box selected.
6. Click **Next**.
   - If you cleared **Include rack connections**, the Summary window is shown. Continue with step 7 on page 3.
   - If you selected **Include rack connections**, the Connection Profile window is shown. Complete the following steps:
     a. Click **Select Profile** and navigate to the connection profile file that you received with the rack. The connection profile file contains device configuration information for each resource in the rack.
     b. Click **Next**. The Confirm Connections window is shown.
     c. Click **Confirm Connection**. The physical connections between the managing rack and the rack extension are verified. This action can take several minutes.
     d. Click **Next**. The Configure Network window is shown.
     e. On the Configure Network window, you can either specify the default network address that you want to use when you add devices, or use the default network address `192.168.92.xxx` by clearing the **Specify default network address** box.
     f. Click **Next**. The Summary window is shown.
     g. Review the information that is shown. Continue with step 7 on page 3.
7. Click **Finish**. A new rack tab is added to the hardware inventory, and resources are added to the rack.

For details about editing the properties of an existing rack, moving devices from one rack to another, or removing a rack, see Managing racks by using the PurePower Integrated Manager.

Editing the properties of a rack by using the PurePower Integrated Manager:

Learn how to edit the properties of a rack by using the PurePower Integrated Manager.

You can use the PurePower Integrated Manager interface to edit the properties of a rack.

To edit the properties of a rack, complete the following steps:
1. Log in to the PurePower Integrated Manager with your username and password.
2. Click the **Hardware Inventory** icon.
3. Expand the **Details** section.
4. Click **Edit Details** and make the required changes.
5. Click **OK**. The changes are saved.

Moving a device from one rack to another rack by using the PurePower Integrated Manager:

Learn how to move a device from one rack to another rack by using the PurePower Integrated Manager.

Move a device from one rack to another rack in the PurePower Integrated Manager interface if it is not properly showing the actual configuration for a rack. For example, if someone physically moved a device from one rack to another and forgot to update the PurePower Integrated Manager.

To move a device from one rack to another rack, complete the following steps:
1. Log in to the PurePower Integrated Manager with your user name and password.
2. Click the **Hardware Inventory** icon.
3. Select the tab of the rack that contains the device that you want to move.
4. Select the device that you want to move.
5. Click **Edit**.
6. In the **Rack** area, select the rack into which you want to move the device.
7. Click **OK**. The changes are saved.

Removing a rack by using the PurePower Integrated Manager:

Learn how to remove a rack by using the PurePower Integrated Manager.

Note: A rack definition can only be removed from the PurePower Integrated Manager when there are no resources associated with it. If you need to remove a rack, you must first remove any resources that are associated with the rack. For instructions, see Removing a resource node by using the PurePower Integrated Manager.
You can use the PurePower Integrated Manager interface to remove a rack.

To remove a rack from the PurePower Integrated Manager interface, complete the following steps:
1. Log in to the PurePower Integrated Manager with your username and password.
2. Click the **Hardware Inventory** icon.
3. Select the tab of the rack that you want to remove.
4. Expand the **Details** section.
5. Click **Remove Rack**.
6. Click **OK**. The changes are saved.

Monitoring your system by using the Nagios Core manager within the PurePower Integrated Manager

The Nagios Core manager within your PurePower Integrated Manager can monitor many components of your IBM PurePower System and provide a central view of your entire IT operation. You can monitor up to 2000 hosts using the Nagios Core manager.

The following functions are included:

- Monitors all mission-critical infrastructure components, including, operating systems, network protocols, system metrics, and network infrastructure
- Provides a central view of your entire IT operations network and business processes.
- Alerts are delivered to you via email and SMS. Multi-user notifications ensure that alerts reach the attention of the right people.
- Event handlers can be set up so that you can automatically restart failed applications, services, servers, and devices when problems are detected.

Notes:

- The daily check for updates to the Nagios Core open source software is controlled by settings in the `/usr/local/nagios/etc/nagios.cfg` configuration file.
  - The **check_for_updates** setting controls if the check for updates should be completed.
  - The **bare_update_check** setting controls what additional information on the Nagios Core installation.

  Future updates to the Nagios Core monitoring software are distributed with the PurePower Integrated Manager.
- Some devices that are listed in the Nagios Core Services view show that the default status for TRAP devices is **PENDING** with a **?** next to the TRAP. On the Nagios Core, the **PENDING** status indicates that the Nagios Core is waiting to do a check on the device. The question mark indicates that a passive check occurred. When the device has an active alert, the Nagios Core receives the trap. Since this is a passive check, the **PENDING** status is the expected behavior for the Nagios Core.
- Devices that are listed in the Nagios Core Map view show a question mark (?) for the device. The question mark indicates that no specific device type image has been set for the devices in the Nagios Core. For the PurePower System, since every device is contained in the rack, the network map is static and the Map view is not expected to provide any additional information.
- To set up Nagios Core email notifications, customize the following command with your email information:

  `/usr/local/nagios/etc/objects/contacts.cfg`

Creating user IDs and passwords for the Nagios Core web interface

The default user ID used to log in to the PurePower Integrated Manager Nagios Core web interface is **nagiosadmin** and the password is **PASSW0RD** (with a zero). More accounts can be created, or the password can be updated by using the command line.

To create a new user ID or update a password, complete the following steps:

1. To create the joe_user user ID, complete the following steps:
   a. Type the following command and press Enter:
      `[root@puremgr ~]# htpasswd /usr/local/nagios/etc/htpasswd.users joe_user`
   b. When prompted, type a password and press Enter.
   c. When prompted, retype the password and press Enter.

   The following message is displayed - Adding password for user joe_user.
2. To update the password for the user ID for joe_user, follow these steps:
   a. Type the following command and press Enter:

```
[root@puremgr ~]# htpasswd /usr/local/nagios/etc/htpasswd.users joe_user
```

b. When prompted, type the new password and press Enter.

c. When prompted, retype the new password and press Enter.

The following message is displayed - Updating password for user joe_user.

3. To delete the joe_user user ID, type the following command and press Enter:

```
[root@puremgr ~]# htpasswd -D /usr/local/nagios/etc/htpasswd.users joe_user
Deleting password for user joe_user
```

The following message is displayed - Deleting password for user joe_user.

4. To specify a password by using the **-b** flag, type the following command and press Enter:

```
[root@puresecurity ~]# htpasswd -b /usr/local/nagios/etc/htpasswd.users new_userid my_password
```

The following message is displayed - Adding password for user new_userid.

Starting and using the Nagios Core manager from the PurePower Integrated Manager

After you start the Nagios Core manager from within the PurePower Integrated Manager, you can monitor your infrastructure.

To start and use the Nagios Core manager, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Home** icon.
3. To log in to the Nagios console, click the resource manager link that you want to work with under the Health Monitors area of the Home page. The Authentication Required window appears.
4. Type your user name and password and click **OK**. The Nagios Core window appears.
5. In the left menu under **Current Status**, select one of the following options:
   - Select **Hosts** to monitor the overall status of the devices in the rack.
   - Select **Services** to monitor in greater detail the status of the devices in the rack.

   Note: For more information about using the Nagios Core Manager, click **Documentation**. A list of available documents are shown.

Configuring the RHEL guest operating system

To monitor a remote Red Hat Enterprise Linux (RHEL) operating system, you must first configure it correctly.

To configure the RHEL guest operating system, complete the following steps:

1. Ensure that the host name is set properly, including the fully qualified domain name (fqdn).
2. Check and update the following files:
   - `/etc/hosts`
   - `/etc/hostname`
3. Update PERL, if necessary, by using the following command: **`yum update perl`**.
4. Open port 5666 to access the NRPE daemon from the PurePower Integrated Manager by using the following commands:

   a. `sed -i -e '/?.*INPUT.*REJECT.*icmp-host-prohibited/ s/?/#/' /etc/sysconfig/iptables`

   b. `iptables -A INPUT -s <pureMgr_IP> -p tcp -m tcp --dport 5666 -j ACCEPT`

   c. `service iptables save`

   d. `service iptables restart`

   Notes:

- If the `/var/log/puremgr_agent.log` log file on the RHEL guest operating system shows a message that the installation of `xinetd` failed, manually install `xinetd` by using the following command: **`yum install xinetd`**
- Use the following command to verify that the configuration on RHEL guest operating system on the PurePower System is correct:

  ```
  <puremgr_machine># /usr/local/nagios/ibexec/check_nrpe -H <rhel_guest_OS_IP>
  ```

  – If the **`check_nrpe`** command displays the following error message - No route to host *<rhel_guest_OS_IP>*, it means that the firewall settings are not correct on the RHEL guest operating system.

  – If the **`check_nrpe`** command displays the following error message - Could not complete SSL handshake, it means that the host name settings not proper on the RHEL guest operating system server or the PurePower System server.

  – If the **`check_nrpe`** command succeeds and shows output similar to NPRE v2.15, but displays the following error message - Return code of 255 is out of bounds, it means that the check_nrpe or check_linux_stats.pl are not available on the RHEL guest operating system (because of installation issues). It also means that the check_linux_stats.pl script is not run by the Nagios manager and NRPE because of configuration issues. See the `/var/log/puremgr_agent.log` log file for details about installation or configuration issues.
- Use the following command on the RHEL guest operating system to verify whether the check_linux_stats.pl nagios plug-in script is working correctly:

  ```
  <rhel_guest_OS>># /usr/local/nagios/ibexec/check_linux_status.pl -C -w 90 -c 100 CPU OK : idle
  100.00%90;100 user=0.00% system=0.00% iowait=0.00% steal=0.00%
  ```

Managing the virtualization management node by using the PowerVC manager

Learn how to manage the virtualization management node by using the PowerVC manager.

Managing and deploying workloads by using the PowerVC manager

The PowerVC manager within the PurePower Integrated Manager is used to manage your IBM PurePower System virtual resources.

The PowerVC offers the following functions:

- Simplified virtualization management for IBM Power Systems servers.
- Easily replicate virtual machines for consistency and fast deployment.
- Resource pooling and dynamic virtual machine (VM) placement.
- Monitor the utilization of the resources that are in your environment.

For optimal performance of PowerVC, consider the following limits:

- The PowerVC manager can manage a maximum of 30 Power nodes.
- Each Power node can have a maximum of 500 VMs.
- A maximum of 3000 VMs can exist on all of the combined Power nodes.
- A maximum of 500 VMs can be on all of the combined Power Nodes managed by one Hardware Management Console (HMC)

Starting the PowerVC manager from the PurePower Integrated Manager

You can start the PowerVC manager from the PurePower Integrated Manager.

To start the PowerVC manager, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Home** icon.

3. In the Virtualization Management area, click the label of the PowerVC resource you want. The PowerVC Login pane appears.
4. Type your user name and password and click **OK**. The PowerVC pane appears.

Requesting service for your IBM PurePower System

Learn how to request service for your IBM PurePower System.

To request service for your system, complete the following steps:

1. Log in to the PurePower Integrated Manager.
2. Click the **Service and Support** icon.
3. Select the tab for the rack that contains the resource for which you want to request service.
4. For the resource you want to request service for, click **Create Service**.
5. Follow the on-screen prompts.

   Note: When you request service, it might be necessary to attach service data to the request. To collect service data and download it to your browser, click **Collect Service Data**. It might take several minutes to complete the collection task.

Notices

This information was developed for products and services offered in the US.

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, MD-NC119
Armonk, NY 10504-1785
US

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 actual people or business enterprises is entirely coincidental.

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

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of IBM.

IBM has prepared this information for use with the specific machines indicated. IBM makes no representations that it is suitable for any other purpose.

IBM's computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check IBM's support websites for updated information and fixes applicable to the system and related software.

Homologation statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

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.

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

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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

Electronic emission notices

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Class A Notices

The following Class A statements apply to the IBM servers that contain the POWER8 processor and its features unless designated as electromagnetic compatibility (EMC) Class B in the feature information.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot

accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

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

VCCI Statement - Japan

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

The following is a summary of the VCCI Japanese statement in the box above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

（一社）電子情報技術産業協会　高調波電流抑制対策実施要領に基づく定格入力電力値：Knowledge Centerの各製品の仕様ページ参照

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：5（3相、ＰＦＣ回路付）
• 換算係数 ：0

Electromagnetic Interference (EMI) Statement - People's Republic of China

声　明

此为 A 级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

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

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Class B Notices

The following Class B statements apply to features designated as electromagnetic compatibility (EMC) Class B in the feature installation information.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

VCCI Statement - Japan

この装置は, クラスB情報技術装置です。この装置は, 家庭環境で使用することを目的としていますが, この装置がラジオやテレビジョン受信機に近接して使用されると, 受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI－B

Japan Electronics and Information Technology Industries Association Statement

This statement explains the Japan JIS C 61000-3-2 product wattage compliance.

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

This statement explains the Japan Electronics and Information Technology Industries Association (JEITA) statement for products less than or equal to 20 A per phase.

高調波電流規格　JIS C 61000-3-2 適合品

This statement explains the JEITA statement for products greater than 20 A, single phase.

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類　：6（単相、ＰＦＣ回路付）
• 換算係数　：0

This statement explains the JEITA statement for products greater than 20 A per phase, three-phase.

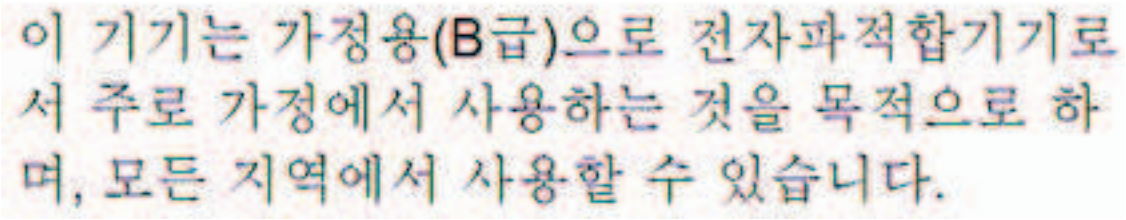
高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類　：5（3相、ＰＦＣ回路付）
• 換算係数　：0

IBM Taiwan Contact Information

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea



Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

Terms and conditions

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA