Hardware Management Console Readme

For use with Version 8 Release 8.4.0

Last updated: 19 February 2016

Contents

These special instructions contain the following information specific to HMC V8 R8.4.0 code level.

- Description
- Upgrade notes
- Enhancements and new function
- General fixes
- Known issues in HMC
- Web browser requirements
- Installation
- vHMC Installation
- National Language Support

PTF MH01559 HMC V8 R8.4.0 Recovery Media and Mandatory PTF MH01560

This package represents the Recovery image that can be used to upgrade your HMC from HMC V8 R8.2.0 or higher to HMC V8 R8.4.0. This package can also be used to install a clean version of HMC V8 R8.4.0. You can also reference this package by APAR MB03952 and PTF MH01559. The mandatory PTF is APAR MB03953 and PTF MH01560.

Note 1: During the upgrade to V8 R8.4.0, the local session will display a list of environment variables for hmcmanager (last line is "END ENV") for as long as 20 to 40 minutes without a screen change. Do not reboot HMC or power off; wait for the upgrade to complete.

Note 2: See Installation section for special install instructions for mandatory fix MH01560.

Package information				
Package name	**Size**	**Checksum (sha1sum)**	**APAR#**	**PTF#**
HMC_Recovery_V8R840_1.iso	3593261056	616c94cedc6102831a5dbc9219882bdeeface411	MB03952	MH01559
MH01560.iso Mandatory PTF	2283960320	d57ec00ef43e0b2886309c99f0836845d759a761	MB03953	MH01560
Splash Panel information (or lshmc -V output)				
After installing the Recovery package				

"version= Version: 8
Release: 8.4.0
Service Pack: 0
HMC Build level 20151007.6
","base_version=V8R8.4.0
"

After installing the Mandatory PTF

"version= Version: 8
  Release: 8.4.0
  Service Pack: 0
  HMC Build level 20151112.2
  MH01560: Required fix for HMC V8R8.4.0 (11-12-2015)
  ","base_version=V8R8.4.0
"

Upgrade notes

- The following Power8 systems are supported by this level of HMC V8 R8.3.0:
    o IBM Power System S812L (8247-21L)
    o IBM Power System S822L (8247-22L)
    o IBM Power System S822 (8284-22A)
    o IBM Power System S814 (8286-41A)
    o IBM Power System S824 (8286-42A)
    o IBM Power System S824L (8247-42L)
    o IBM Power System E870 Server (9119-MME)
    o IBM Power System E850, (8408-E8E)
    o IBM Power System E880 Server (9119-MHE)

- HMC V8 R8.4.0 continues to provide support for Power6 and Power7 based systems.

- POWER5 servers are not supported from HMC V8. Attempts to manage POWER5 servers will result in a connection state of Version Mismatch and connection_error_code "Connection not allowed 0009-0008-00000000".

- HMC V8 R8.4.0 supports the following HMC models:
    o Deskside: C08
    o Rack Mount: CR5, CR6, CR7, and CR8, CR9

- HMC V8 does not support models CR2, CR3, CR4 and C03, C04, C05, C06, C07.

- HMC V8 requires 2GB memory; 4GB memory is recommended, if you are running enhanced+ UI. If you run with **over 300 partitions**, it is recommended to have 8GB memory.

- The HMC must be version V8 R8.2.0 or later to be upgraded to HMC V8 R8.4.0. This requirement is enforced at install.

- When two HMCs manage the same server, both HMCs must be at the same version.

- When two HMCs manage the same server, both HMCs must be at the same version.A new management mode has been added to the HMC called PowerVM co-management. This feature allows the HMC and PowerVM NovaLink to both have a live management connection to the system.   This co-management support is currently a Technology Preview in HMC V8.840.0 and should not yet be used in a production environment. If a server is connected to two different versions (i.e. Version 7 and Version 8) of the HMC, the higher version HMC will upgrade the partition configuration (profile data of the system) to the latest version. After the partition configuration upgrade, lower levels of the HMC will not be able to interpret the data correctly. After the server is managed by the higher version of the HMC, you must first initialize the server before you can go back to the lower version of the HMC. You can restore a backup that is taken at the older level or re-create the partitions. If the server is not initialized, one of the following outcomes can occur depending on the version of the lower-level HMC:
  - HMC Version 7 Release 7.8.0 and 7.9.0 report a connection error of Version mismatch with reference code Save Area Version Mismatch if the server has been managed by Version 8.
  - HMC Version 7 Release 7.8.0 reports a connection error of Version mismatch with reference code Save Area Version Mismatch if the server has been managed by Release 7.9.0 or Version 8.
  - HMC Version 7 Release 7.7.0 and earlier might report a server state of Incomplete or Recovery if the server has been managed by a later version and / or release. In addition, partition configuration corruption may occur.

- It is recommended to have all connected VIOS servers on the latest level i.e. VIOS level 2.2.4.0. To have optimal performance from enhanced+ UI, make sure all VIOS are at 2.2.3.X level or above.

- All running partitions (AIX Linux and VIOS) should be at RSCT 3.2.0.6 or higher. Our recommendation is at a minimum for AIX 6.1 TL9 be at SP5 or higher, and AIX 7.1 TL3 be at SP5 or higher; these SP levels both contain RSCT 3.2.0.6.

- HMC Version 8.4.0 supports managing a maximum of 48 servers (non Power 595/780/795 models) or 32 IBM Power 595/780/795 servers with a maximum of 1024 partitions across the managed servers.

- **Call home changes in HMC V8R8.3.0 and later will impact upgrades from HMC V8R8.2.0**:
  - Call Home support for modem (dial-in via AT&T Global Network) and Internet VPN is disabled. The only supported method for Electronic Service Agent (ESA) connections for V8R8.3.0 and higher is "Internet".
  - The list of gateway IP addresses changed in HMC V8R8.3.0 and later. For a list of the new gateway access points see the "ESA for HMC Connectivity Security" document at http://www-01.ibm.com/support/esa/security.htm
  - The legacy internet proxy configuration was removed. If an internet proxy was configured at V8R8.2.0 or earlier, administrators should verify or re-configure the proxy as needed and test the configuration.
    - a. GUI Option: Go to Service Management -> Manage Outbound Connectivity
    - b. Click through Configure and click OK,
    - c. Then click OK again to exit the panel.
  - Users should test the HMC internet connectivity by submitting a test PMR.
  - For information on configuring Internet SSL Service and Support connection see http://www-01.ibm.com/support/knowledgecenter/8247-22L/p8hai/configuringthehmcasacall-homeserverusinglan-basedinternetandtlsssl.htm?cp=8247-22L&lang=en

Back to top

Enhancements and new function

New function or enhancement from V8R8.3.0:

- Login panel option updates: There are three login options:
    - Classic ==> The Classic interface provides access to all traditional functions of the HMC
    - Enhanced+ ==> The Enhanced+ interface provides access to the new HMC console GUI. This version is redesigned from the ground-up with a new look-and-feel, and interactions with an effort placed on simplification. It offers updated functions for managing PowerVM, managing partitions, template capture/deploy, virtual networking resource diagram, and an updated network install UI for partition OS and VIOS. These tasks are integrated into a dashboard view making it easy to view system resources, 'pin' frequently accessed pages, and search help topics.
    - Last Log In ==> This option opens the UI in the last Log In type. At installation, this option defaults to Classic mode.Call Home support for modem (dial-in via AT&T Global Network) and VPN will be removed.
- The Call-Home feature works entirely over SSL: https://w3-connections.ibm.com/blogs/5a65a241-60d9-4177-8cc4-d24fd24f2a26/entry/Beginning_with_HMC_version_830_0_Call_Home_feature_works_entirely_over_SSL?lang=en_us

- Remote Restart is supported when the source managed system is in Initializing state in addition to the other supported states.

New function or enhancement from V8R8.4.0:

- Introduced virtual storage topology diagram for:
    - Individual logical partitions that shows virtual storage resources specifically mapped to the partition.
    - A managed system that depicts a high-level view of the virtual storage on the system.
- The lspwrmgmt and chpwrmgmt command were enhanced to allow users to manageDynamic and Idle power saver tunable attributes from HMC and also through REST APIs.
- General enhancements to the Enhanced+ UI.
- New enhancements to support the inclusion of VIOS procs under Integrated Facilities for Linux (IFL):
    - New CoD messages and history messages have been added having the "Virtual IO Server" terminology in the message text. The label texts on GUI panels ,related with CoD procs, have been updated to include "VIOS" to show IFL procs. Commands lshwres and lscod have been updated to include new attribute with new terminology..
- Secure FTP key support has been added to the following GUI tasks: Back Up Management Console Data, Restore Management Console Data, Update HMC and Schedule Operations (Backup Critical Console Data).
- Secure FTP key generated with passphrase is supported only in command line,not in GUI tasks.
- HMC added support for virtual Network Interface Controller (vNIC), which is a type of virtual adapter that can be configured on client logical partitions to provide a network interface. Each vNIC client adapter is backed by an SR-IOV logical port that is owned by the VIOS. Client partitions with vNICs can be migrated, suspended, and remote restarted.
- Added support to allow user to specify MSP concurrency performance override value at each partition migration operation level. (This new function requires MSP at 2.2.4.0 level and PHYP at 840 level.)

- Added support to allow user to change the virtual switch name of a virtual ethernet adapter of a migrating partition. (The new function requires target VIOS partition at 2.2.4.0 level and target PHYP at 840 level.)
- Introduced Shared Storage Pool Multi Tier and Pool Mirroring support. VIOS with version 2.2.4.0 and above required for Multi Tier support. Pool Mirroring is supported from 2.2.3.X and above version of VIOS
- Certificate Revocation List (CRL) Management
  - Enable the user to view and manage the certificate revocation list (CRL) file that you obtain from the certificate authority (CA). CRL contains a list of certificates that are revoked, and the server that presents the certificate are no longer considered trustworthy. When the HMC establishes connection with any server entities, the certificate that is presented by the entity is validated with the recent CRL that is present on the HMC. In case any such endpoint is invalid the connection with the endpoint will be terminated and appropriate error message is displayed.
  - Import CRL
    - User can import a CRL file either from a removable media device on the console or from the local directory to the HMC.
  - Delete CRL
    - This allow the user to delete the CRL file that is stored on the HMC.
  - Import Repository
    - The existing Certificate infrastructure in HMC allow the user to import a CA signed public certificate in to HMC key-store. However there isn't an existing mechanism to import an external key-store containing private/public key pair or certificate chain to HMC. The new 'Import Repository' feature allow the user to import an external key-store containing certificates (private, public and certificate chain) to HMC.

[Back to top](#)

This package provides the following fixes:

General fixes

- Fixed an issue where the Format Media task's refresh button does not detect recently added media.
- Fixed an issue where the listing of applied PTF's does not show in the Enhanced UI.
- Fixed an issue where the display resolution of the TF4 monitor displays incorrectly due to an incorrect display resolution. Added new functionality for the user to be able to change the display configuration resolution
- Fixed an issue for a failure attempting to add a virtual ethernet adapter via DLPAR to a remote re-start lpar, user receives an HSCL294C error regarding VIOS backing device was not found.
- Fixed an issue where bkconsdata command over SFTP returns an incorrect error if "permission denied" is received from the target system
- Fixed an issue where XNTP entries could not be removed if the string had a trailing blank space.
- Fixed an issue with rsyslog writing warning messages to the /var/log/warn file.
- Fixed an issue where PCM graph does not render
- Fixed an issue where one cannot deploy the partition template with the default selection of the Virtual Fibre Channel configuration.

- Updated the repair procedure for non-concurrent high end System Node repairs
- Fixed an issue where inbound VPN connectivity fails with "Session completed unsuccessfully".
- Fixed a problem that occurs after a Power enterprise pool has been recovered (using chcodpool -o recover) when all of the servers in the pool configuration file used to do the recover are not connected to the master HMC. This problem causes no servers to be displayed on the Power enterprise pool GUI processor and memory resource pages and causes the **lscodpool --level sys -F** command to fail if compliance information is requested.
- Fixed an issue where errors in generating a Pool using Power Enterprise Pool functions were not properly reported.

Security Fixes

- Fixed multiple security vulnerabilites in curl: CVE-2014-3613, CVE-2014-3707, CVE-2014-8150, CVE-2015-3143, CVE-2015-3148, and CVE-2015-3153
- Fixed openssh vulnerability: CVE-2015-5600
- Fixed NTP vulnerabilities: CVE-2015-1798, CVE-2015-1799 and CVE-2015-3405
- Fixed autofs vulnerability: CVE-2014-8169
- Fixed Strongswan vulnerability : CVE-2015-4171

Command line changes

- The following commands have been enhanced to support SR-IOV virtual NICs: **chsyscfg, lssyscfg, mksyscfg, chhwres, lshwres, migrlpar, and lslparmigr**.
- The **migrlpar** command has been enhanced to allow virtual switch mappings to be specified for migrating partitions.
- The following commands have been enhanced to support the ability to migrate a partition when a Virtual I/O Server hosting the migrating partition's virtual SCSI and virtual fibre channel adapters on the source managed system is shutdown: **migrlpar, lslparmigr, lssyscfg, and refdev**.
- The **migrlpar** command has been enhanced to provide a concurrency level override for partition migration operations. The concurrency level is used to control the amount and configuration of resources allocated to partition migration operations by the Mover Service Partitions.
- The following commands have been enhanced to disable partition migration for a partition: **chsyscfg, lssyscfg, and mksyscfg**.
- A new option has been added to the **chsysstate** command to specify a VLAN ID to use when performing a network install of an IBM i partition.
- The **updhmc** command has been enhanced to support remote virtual media devices.
- NFS support has been added to the following commands: **getupgfiles** and **updhmc**.
- Secure FTP key support has been added to the following commands: **bkconsdata, getfile, getupgfiles, lslic, updhmc, and updlic**.
- Idle power saver support has been added to the **chpwrmgmt** command. In addition, the **chpwrmgmt** and **lspwrmgmt** commands have been enhanced to support configuring and displaying the dynamic and idle power saver parameters for a managed system.
- Additional I/O properties have been added to the **lshwres -r io --rsubtype slotchildren** command.
- The **chsyscfg -r sys** command has been enhanced to specify the boot mode and IPL source for a server when it is in the manufacturing default configuration.
- A new option has been added to the **updlic** command to purge firmware update files from the HMC hard disk repository, and a new option has been added to the **lslic** command to list the firmware update files that can be purged.

- The **chsacfg** command has been enhanced to support complete call-home configuration, and the lssacfg command has been enhanced to display complete call-home configuration.
- A new LPAR level attribute "**migration_disabled**" is introduced to disable/enable partition migration. If the attribute is disabled for a partition, Live Partition Mobility will fail.
  Examples:
    o Creation of Partition
      mksyscfg –r lpar –m <server name> -i "migration_disabled = <1/0>"
    o Modification of Partition
      chsyscfg–r lpar –m <server name> -i "migration_disabled = <1/0>"
    o Listing the partition properties
      lssyscfg -m <managed system> -r lpar -F migration_disabled

Back to top

Known issues in HMC

- On the Virtual HMC offering, call home for serviceable events with a failing MTMS of the HMC itself.is disabled. Those serviceable events should be manually reported to IBM software support.
- On the Virtual HMC offering, media loaded in the virtual CD/DVD device cannot be mounted.
- Serviceable event E35F0010 may be reported on an upgrade. This event indicates that an error occurred migrating the HMC user profile properties. Customized user profile settings will be lost and reset to their default.   To recover, edit the user profiles and reset the settings.
- In NIST mode:
    o Firefox ESR version 24 is not supported.
    o Oracle JRE 7 does not have matching NIST cipher so client browser using Oracle JRE 7 will not be able to open virtual terminal applet. As a workaround, upgrade to Oracle JRE 8.
    o RMC code on partition does not support two HMC connections with mixed configuration i.e. one HMC running in NIST mode and other one in non-NIST mode. Both the HMCs must be in the same mode.
    o HMC uses RSA 2048 type keys to communicate with LPARs. When user removes HMC V8 R8.4.0 and connects an older level HMC (i.e HMC V8 R8.2.0 or before), it will drive NIST mode on the LPARs to be disabled. However the LPARs would continue to use RSA 2048 type keys so there would be connection establishment issue. To resolve this problem, the LPAR admin should run '/usr/sbin/rsct/bin/chsecmode -c none -m rsa512' command on all the corresponding LPARs (This command can't be run if LPAR is running any HA software like TSA, PowerHA).
- In non-NIST mode:
    o Following ciphers are not supported although the available cipher list shows them.

      TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA

  Note this function is fully supported for all other Power systems assuming that the appropriate HMC, firmware and PowerVM levels installed.

- To ensure that the keyboard mapping is working properly for non-English keyboards, the codeset for the locale must be set to UTF-8. You can change the codeset by using the chhmc command. Example:
Set the locale to French with UTF-8 codeset for use with French keyboard.
chhmc -c locale -s modify -l fr_FR.UTF-8
Set the locale to English with UTF-8 codeset for use with French keyboard.
chhmc -c locale -s modify -l en_US.UTF-8

- HMC V8 R8.2.0 to V8 R8.4.0 upgrade script replaces the default templates during the upgrade process. Any changes performed on the V8 R8.2.0 default template will be overwritten. HMC V8 R8.2.0 to V8 R8.4.0 upgrade script will add the Quick Start Templates to the existing Template Library and the user can delete the older Starter Templates manually.
- VIOS installation is supported only through Add VIOS
- You cannot use the GUI to set a new master HMC for a Power enterprise pool when the new master HMC is not configured as the backup master HMC for the pool or if the new master HMC does not have valid backup data for the pool. You can perform this operation by running one of the following HMC commands:
chcodpool -o setmaster --mc this -p <pool name> -v -f <file>
            or
chcodpool -o setmaster --mc this --id <pool ID> -v -f <file>
- In Enhanced+ UI, Manage VIOS -> Add Logical Host Ethernet Adapter page once user has performed add and remove of same HEA port, the HMC does not display the port again for addition. As a workaround launch the Add Logical Host Ethernet Adapter page again.
- The Enhanced+ UI login mode does not support disconnected sessions like the Classic UI mode. In the Enhanced+ UI mode a session logoff is a logoff and a session disconnect is also a logoff. This means that the user cannot reconnect to the Enhanced+ UI session to resume the task(s) from where it had left off. Every login via the Enhanced+ mode creates a new session. For more details on long running tasks, please refer to the link below :
https://www-01.ibm.com/support/knowledgecenter/POWER8/p8eh6/p8eh6_loginmode.htm
- The "All Shared Storage Pool Clusters" will not launch successfully if any of the Virtual I/O Server managed by the HMC is not configured properly. This includes the Virtual I/O Servers that are not Nodes in the Shared Storage Pool Clusters in the HMC. Use ALL Systems relational view from which you can view all the partition grouped by System. In this view we can easily see the partition been migrated from one system to the other. In some rare situations, especially with a Firefox browser, the user maybe redirected to a second login page after having provided and validated credentials.
Then, providing the credentials again will fail. If this issue occurs the user should close and re-launch the browser to make it work.
- No local vterm when HMC is in NIST mode.
- Users can't update to 840 MPTF from USB. They can either use DVD install or network install.
- From the Enhanced+ HMC, click on HMC management icon in the toolbar, then open the Console Management page. Click the Schedule Operation link. The panel which is launched is not correct. In order to schedule an operation against the HMC, please use the Classic GUI.
- On physical console, vterm will not be launched In NIST mode. As a workaround, use vtmenu on physical console.
- Enabling or disabling service processor redundancy is only permitted when both Primary and Secondary Service Processors are at standby with Service Processor in Position A as Primary. The workaround is to set up FSP failover with the following command:
chsyscfg -m <server_name> -r sys -i "sp_failover_enabled=1"
- HMC V8 R8.2.0 or HMC V8 R8.3.0 to HMC V8 R8.4.0 upgrade results in the HMC calling home a E35F0012.

- When customers upgrade from V8 R8.1.0 to V8 R8.4.0 (V8 R8.1.0 to V8 R8.2.0/V8 R8.3.0 and then subsequent update to V8 R8.4.0 without login to UI), any users which existed in V8 R8.1.0 will remain but with default user settings.
- Opening multiple PCM Dashboard windows on the same browser will lead to a communication error on the window that was opened first. This is a known issue and the support for multiple PCM Dashboard windows on the same browser is planned for a follow-on release.
- System plan creation takes more time for P6 Systems
- After Templates copy to Templates Library/OS image page, the dashboard navigation is disabled. This is a known issue and work around is to open another window from the context menu and click on cancel will clear the navigation issue.
- If the System Templates deploy fails due to the installed VIOS going to Open Firmware state, then user can open Virtual Terminal for the VIOS and execute "boot" on the Open Firmware prompt to boot the VIOS.
- If after install no GUI launches, and you only see the CLI localhost login under the heading "Base release 7.4. Dev (hmc7_4p) on an x86_64", it's an indication that the HMC code is not installed, and only the Operating System has been put on disk. Causes could be that the date in UEFI is not the current date/year or DVD media issues. Set the date using the UEFI Setup Utility to be the current date and year, then attempt reinstall. Try different media if the date/year is correct.

[Back to top](#)

Web browser requirements

Learn about the requirements your web browser must meet to monitor and control the HMC.

HMC web browser support requires HTML 2.0, JavaScript 1.0, Java™ Virtual Machine (JVM), Java Runtime Environment (JRE) Version 8 or later, and cookie support in browsers that will connect to the HMC. Contact your support personnel to assist you in determining if your browser is configured with a Java Virtual Machine. The web browser must use HTTP 1.1. If you are using a proxy server, HTTP 1.1 must be enabled for the proxy connections. Additionally, pop-ups must be enabled for all HMCs addressed in the browser if running with pop-ups disabled.

The following browsers have been tested:

Google Chrome

HMC version 8.40 tested with Google Chrome version 43, 46 Beta. Google Chrome version 44 & 45 have known issues which prevents HMC Enhanced GUI to operate correctly, the recommended version is Chrome 43 or 46.

Microsoft Internet Explorer

HMC Version 8.4.0 supports Internet Explorer 11.0.

- If your browser is configured to use an Internet proxy, then local Internet addresses are included in the exception list. Consult your network administrator for more information. If you still need to use the

proxy to get to the Hardware Management Console, enable **Use HTTP 1.1 through proxy connections** under the **Advanced** tab in your Internet Options window.

- It is recommended to have:

    o Browser security setting in internet zone. If you are running security mode in "Local intranet" mode, make sure you do not have any setting to detect intranet network; disable Compatibility view.
    o Browser zoom setting to 100%.

Internet Explorer restriction

When trying to close an Enhanced+ modal popup window in Internet Explorer, a prompt window will appear with the question "The webpage you are viewing is trying to close the tab. Do you want to close this tab?" You must answer "No" to this question to close only the popup. Otherwise, the whole application will be closed.

Mozilla Firefox

HMC Version 8.4.0 supports Mozilla Firefox Version 31 and Mozilla Firefox Version 38 Extended Support Release (ESR). Ensure that the JavaScript options to raise or lower windows and to move or resize existing windows are enabled. To enable these options, click the Content tab in the browser's Options dialog, click Advanced next to the Enable JavaScript option, and then select the Raise or lower windows option and the Move or resize existing windows options. Use these options to easily switch between HMC tasks. For more information about the latest Mozilla Firefox ESR levels, see Security Advisories for Firefox ESR.

If you get certificate error while connecting Mozilla Firefox Version 24 to HMC, then change the certificate verification library by toggling the preference "security.use_mozillapkix_verification" to false in the about:config of Firefox browser. Refer below recommendation from Firefox forum https://support.mozilla.org/en-US/questions/1012036

Browser Cache & Application Cache Cleaning

Cache cleaning is not mandatory if the user has already cleaned the cache between 820 and 830.
It is mandatory only if moving from 820 to 840 directly.

In order to prevent from caching issue due to the 820 Enhanced+ GUI tech preview caching policy, please clear the Browser cache and Application.

In Microsoft Internet Explorer

Open the Browser
Select **Tools**
Select **Internet Options**
Under Browser History, select **Delete**
Check "**Temporary Internet files and websites files**" and "**Cookies and website data**"
Click on **Delete**

In Mozilla Firefox

1. In the top-right corner of the browser window click the **menu** button
   Choose **History**, and then **Clear Recent History.**
   In time range to clear, select "**Everything**"
   In the Details section, select "**Cookies**" and "**Cache**"
   Click on "**Clear now**"
2. In the top-right corner of the browser window click the menu button
   Choose **Options > Advanced > Network >**
   In "**Offline Web Content and User Data**" section click on "**Clear Now**"

In Google Chrome

1. In the top-right corner of the browser window, click the **Chrome menu**
   Choose **History**.
   Click the button **Clear browsing data**. A dialog will appear.
   From the drop-down menu, select "t**he beginning of time**."
   Check the boxes "**Cookies, site, and plug-in data**" and "**Cache**"
   Click the button **Clear browsing data**.
2. Open the following url with the Chrome browser: **chrome://appcache-internals/**
   If there is an entry related to the target hmc, click the corresponding "**Remove**" link

Other web browser considerations

Session cookies need to be enabled in order for ASMI to work when connected to HMC remotely. The ASM proxy code saves session information and uses it.

Internet Explorer

1. Click **Tools > Internet Options.**
2. Click the Privacy tab and select **Advanced**.
3. Determine whether **Always allow session cookies** is checked.
4. If not checked, select **Override automatic cookie handling** and **Always allow session cookies**.
5. For the First-party Cookies and Third-party Cookies, choose block, prompt, or accept. Prompt is preferred, in which case you are prompted every time a site tries to write cookies. Some sites need to be allowed to write cookies.

Firefox

1. Click **Tools > Options**.
2. Click the **Cookies** Tab.
3. Select **Allow sites to set cookies.**
   If you want to allow only specific sites, select Exceptions, and add the HMC to allow access.

Installation

Special Install Instructions for mandatory fix MH01560: This fix <u>must</u> be installed using the HMC updhmc command; not the GUI. See the updhmc "man" page (e.g. man updhmc) for further information and examples on using the command.

Installation instructions for HMC Version 8 upgrades and corrective service can be found at these locations:

[Upgrading or restoring HMC Version 8](#)

[Installation methods for HMC Version 8 fixes](#)

Instructions and images for upgrading via a remote network install can be found here:

[HMC V8 network installation images and installation instructions](#)

Installation methods for vHMC
http://www-01.ibm.com/support/knowledgecenter/HW4M4/p8hai/p8hai_installvhmc.htm

Virtual HMC (vHMC)

- The V8 R840 and higher versions of the HMC can be installed into virtual machine that is running on an x86 Hypervisor.
- The vHMC provides images in 2 additional formats to allows for quick deployment of the vHMC on either ESXi or KVM hypervisors
- A feature of the vHMC is the activation engine which allows you to preconfigure the HMC Console by passing configuration information to the HMC at the first boot of the HMC, when using these images.
- Please look at the Knowledge Center documentation that is provided with this Early Ship program for details on using the Activation Engine feature.
- Minimum requirements of vHMC:
  - 8GB of memory
  - 4 processors
  - 1 network interface, with a maximum of 4 allowed.
  - 160GB of disk space, recommend 700GB to get adequate PCM data
- The supported hypervisors are VMWARE ESXi 5.5 or higher   or KVM on Red hat RHEL 6.5 or higher
- The processor on the systems hosting vHMC must have either Intel VT-x or AMD-V Hardware Virtualization enabled.
- To see if you are running on a virtual HMC use the lshmc -v command. If it displays a UVMID field, then you are running in a virtual machine.

Example:
lshmc -v

"vpd=*FC ????????
*VC 20.0
*N2 Wed Aug 26 13:36:06 UTC 2015
*FC ????????
*DS Hardware Management Console

*TM Vb07-f21
*SE 6b4b9a5
*MN IBM
*PN N/A
*SZ 1044881408
*OS Embedded Operating Systems
*NA 127.0.0.1
*FC ????????
*DS Platform Firmware
*RM V8R8.4.0.0
*UVMID b07f:216b:4ce7:b9a5
"

- When deploying a virtual HMC, if the mac address is not specified, it will be generated by the hypervisor. Network configuration on the HMC relies on the value of MAC addresses. If you re-deploy a new virtual HMC and want to restore critical console data previously taken on a virtual HMC, ensure sure you are using the same MAC addresses.
- When using Activation Engine to setup NTP configuration, you must specify the NTP version value.
- The Activation Engine currently does not provide configuration of DHCP Server on virtual HMC.
- The number of Ethernet adapters (Virtual or Physical) defined to vHMC on KVM or ESX Hypervisors should correlate with vHMC Activation Engine(AE) vHMC-Conf.xml file.

Example KVM:
If a user defines 4 ethernet adapters in the domain.xml, they should define 4 ethernet adapters on AE vHMC-Conf.xml file with network values. In the case that they want an empty adapter, they have to use the following for each unused empty adapter:

```
<Ethernet>
      <Enable>Yes</Enable>
      <IPVersion>IPV4</IPVersion>
      <IPv4NetworkType>Static</IPv4NetworkType>
      <IPv4Address>0.0.0.0</IPv4Address>
      <IPv4Netmask>255.255.255.0</IPv4Netmask>
      <IPv4Gateway></IPv4Gateway>
      <IPv6NetworkType></IPv6NetworkType>
      <IPv6Address></IPv6Address>
      <IPv6Gateway></IPv6Gateway>
      <Hostname></Hostname>
  <Domain></Domain>
  <DNSServers></DNSServers>
      <Firewall>
            <PEGASUS>Enabled</PEGASUS>
            <RPD>Enabled</RPD>
            <FCS>Enabled</FCS>
            <I5250>Enabled</I5250>
            <PING>Enabled</PING>
            <L2TP>Disabled</L2TP>
            <SLP>Enabled</SLP>
            <RSCT>Enabled</RSCT>
```

```
            <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
            <SSH>Enabled</SSH>
            <VTTY>Disabled</VTTY>
            <NTP>Disabled</NTP>
            <SNMPTraps>Disabled</SNMPTraps>
            <SNMPAgents>Disabled</SNMPAgents>
        </Firewall>
    </Ethernet>
```

Back to top

National Language Support (Supported languages)

Languages	Locales
English	en_US,en_AU,en_BE,en_BE@preeuro,en_CA,en_GB,en_GB@euro,en_HK,en_IE,en_IE@preeuro,en_IN,en_N
Catalan	ca_ES, ca_ES@preeuro
German	de_DE, de_DE@preeuro, de_CH, de_AT, de_AT@preeuro, de_LU, de_LU@preeuro
French	fr_FR, fr_FR.UTF-8, fr_CH, fr_CA, fr_BE, fr_BE@preeuro, fr_LU, fr_LU@preeuro
Italian	it_IT, it_IT@preeuro, it_CH
Spanish	es_ES, es_ES@preeuro, es_AR, es_BO, es_CL, es_CO, es_CR, es_DO, es_EC,es_SV, es_GT, es_HN, es_M
Brazilian Portuguese	pt_BR
Portugal Portuguese	pt_PT, pt_PT@preeuro
Polish	pl_PL, pl_PL.UTF-8, pl_PL@euro,pl_PL@preeuro
Japanese	Ja_JP
Simplified Chinese	zh_CN, zh_SG
Traditional Chinese	zh_TW, zh_HK
Korean	ko_KR
Hungarian	hu_HU, hu_HU.UTF-8,hu_HU@euro,hu_HU@preeuro
Dutch	nl_NL, nl_NL@preeuro, nl_BE, nl_BE@preeuro
Russian	ru_RU
Czech	cs_CZ, cs_CZ.UTF-8,cs_CZ@euro,cs_CZ@preeuro
Slovakian	sk_SK, sk_SK.UTF-8,sk_SK@euro,sk_SK@preeuro