IBM PowerVM 1060.10 with VIOS 4.1.1 for Power10 and HMC 10.3.1062.1 for Power 9 Evaluated Configuration Guide

Revision 1.7

Jul 1st, 2025

Prepared By:
IBM
3605 US Hwy. 52 North
Rochester, MN   55901

Table of Contents

1 About This Information

This document provides comprehensive guidance on planning, installing, configuring, and managing logical partitioning on your Power server in support of a Virtualization Protection Profile (VPP) evaluation. You can view and download the document at: https://www.ibm.com/products/ibm-powervm under “Resources”.

The document describes the configuration for the IBM PowerVM 1060 with VIOS 4.1 for Power10 and HMC for POWER9 Security Target. The hardware and firmware allow you to set up more than one virtual machine on your server, so that you can run separate operating systems concurrently. Each virtual machine is called a *partition or logical partition (LPAR)*. The design of the architecture provides the following security features:

- The Hardware Management Console (HMC) firmware on a POWER9 server provides the user interfaces to configure the VIOS and virtual machines assigned to the Power10 server.
- The HMC, hardware and firmware on Power10 provide the operating system on each separate partition with the resources it needs to function
- The HMC, hardware and firmware keep the resources for each partition separate, so that they will not interfere with each other.

The IBM PowerVM 1060 with VIOS 4.1 for Power10 and HMC for POWER9 has been developed and evaluated in accordance with the Virtualization Protection Profile requirements listed below:

Objectives

- This certification permits a developer to gain assurance from positive security engineering based on good commercial development practices which, through rigorous, do not require substantial specialist knowledge, skills, and other resources.
- This certification is therefore applicable in those circumstances where developers or users require a level of independently assured security in conventional commodity targets of evaluation (TOE) and are prepared to incur additional security specific engineering costs.

Assurance components

- The evaluation provides assurance by an analysis of the security functions, guidance documentation, the high-level and low-level design of the TOE, to understand the security behavior. The analysis is supported by independent testing of the TOE security functions and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

VPP certification requires the following documentation:

- *Administrator Guidance*, which describes the tasks that a security administrator must perform to install and manage a VPP-evaluated system.
- *User Guidance*, which describes the user’s responsibilities for security. In this case, once a POWER server has been configured to run with multiple partitions, the user of the partition does not need to do anything to support security. All the security features are enforced by the firmware and hardware.

This information is designed to meet the VPP requirement for administrator guidance, when used together with the following documents:

- Installing and configuring the Hardware Management Console
- Managing the Hardware Mangement Console

- Problem analysis system parts and locations for the IBM Power Systems HMC
- Servicing the IBM Power Systems HMC
- Logical Partitioning
- Setting up the virtualization environment
- Managing the virtualization environment
- Monitoring the virtualization environment
- Virtual I-O Server
- Beginning troubleshooting and problem analysis

Note: Information about installing, configuring, managing, and servicing the HMC can all be accessed from the HMC itself. This information is part of the IBM Knowledge Center offering and is available on the internet. For example, information about Managing the HMC can be found in documents *PowerVM 3.1.3 POWER9 Managing the Hardware Management Console.pdf and PowerVM 3.1.3 Power10 Managing the Hardware Management Console.pdf*.

Information about creating a virtual computing environment on Power servers can be found in the document *PowerVM 3.1.3 Logical Partitioning.pdf*.
You should read these guides first, and you should consider it your primary source of information for setting up logical partitioning of your POWER server to meet the Virtualization Protection Profile security requirements that are listed in IBM PowerVM 1060 with VIOS 4.1 for Power10 and HMC for POWER9 Security Target.

2 Who should read this information

This information is intended for system administrators or security administrators that want to customize a Power server with Logical Partitioning within the valid VPP configuration. This information details the unique requirements of VPP security, and it is intended as a supplement to other manuals describing how you install and set up your system.

3 Overview of security features

There are four categories of security features provided by PowerVM and the HMC:

1. The Hardware Management Console (HMC) is used to manage the assignment of physical resources to the logical partitions (virtual machines). This include assignment of number of CPUs, amount of memory, Physical I/O adapters, virtual I/O devices and so on.

2. The Logical Partitioning Architecture implementation ensures that resources can be assigned to partitions by an authorized user and that those resources will not be accessible to other partitions.

3. The Logical Partitioning Architecture implementation ensures that communication between partitions can occur only using channels established by an authorized user.

4. The Logical Partitioning Architecture implementation ensures that each partition cannot access resources or communicate with other partitions except when explicitly allowed by an authorized user.

In addition, the following assumptions are made about the operating environment when the system is in operation. It is assumed that the user of the Target of Evaluation (TOE) is not willfully negligent or hostile and uses the TOE in compliance with the applied enterprise security policy and guidance. The assumptions include the following:

1. The system must be installed and configured in accordance with its guidance documents, including connecting appropriate device.

2. The system must be within a physical environment suitable to protect itself and its external connections from inappropriate access and modification.

3. The user of the VS is not willfully negligent or hostile and uses the VS in compliance with the applied enterprise security policy and guidance. At the same time, malicious applications could act as the user, so requirements which confine malicious applications are still in scope.

4. TOE Administrators are trusted to follow and apply all administrator guidance.

5. Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.

6. The platform has not been compromised prior to installation of the VS.

4 Target of Evaluation (TOE)

The IBM PowerVM 1060.10 with VIOS 4.1.1 for Power10 and HMC for POWER9 serves as the Target of Evaluation (TOE), incorporating firmware and software that deliver critical security protections within a computer system.

The TOE includes the following components:

- POWER9 CR2 HMC with firmware level HMC1061 (10.3.1062.1)
- Virtual I/O Server (VIOS) version 4.1.1
- Power10 S1024 (9105-42A) system with firmware level FW1060.10 (01ML1060_064_053)

POWER servers can be configured to house multiple independent systems within the same server. Each independent system within the server is called a partition. The partitions do not have to run the same type of operating system. During the configuration process, an administrator determines what resources within the server will be assigned to each independent partitions. There are many partition features. The following Logical Partitioning Architecture features are allowed in the evaluated configuration:

- Micro-partitioning: This feature allows a processor to be shared between two partitions. One partition may get 10% while another gets 90%.

- Virtual Ethernet: This feature provides optional communication between partitions
- The Logical Partitioning Architecture was evaluated independent of the OS in the partition. Any operating system may be installed in the partition.

Products that are included in the TOE have been evaluated and tested for Virtualization Protection Profile security compliance. Products that are not included in the TOE have not been evaluated for Virtualization Protection Profile security compliance. Because the TOE is a general building block, many installations require changes or additions to the evaluated configuration. Your security administrator should assess the security risk of any changes or additions to the TOE configuration.

4.1 Physical System security

To be within the evaluated configuration, the system must be in a secured room with limited and monitored access. The systems HMC appliance must also be in the same secured area. HMC has no mode like sleep or maintenance.

4.2 Hardware Management Console installation

A Virtualization Protection Profile compliant system must be configured by a Hardware Management Console (HMC). The HMC is directly connected to the system via a physical connection. The HMC is used to create and configure partitions (virtual machines) using interfaces GUI and CLI. HMC GUI uses https with TLS 1.2 based encryption. HMC CLI uses ssh based encrypted communication. The HMC utilizes several user roles to manage access and permissions. These roles include: hmcsuperadmin (Super Administrator), hmcpe (Product Engineer), hmcoperator (Operator), hmcservicerep (Service Representative), and hmcviewer (Viewer). The hmcsuperadmin has the highest level of access, while others have specific permissions based on their role. Details about each role are as follows:

1. **hmcsuperadmin** (Super Administrator):
   This role has the highest level of access and can perform all HMC management tasks, including managing user profiles and access.
2. **hmcpe** (Product Engineer):
   This role is typically used by service providers or internal engineers for debugging and problem determination.
3. **hmcoperator** (Operator):
   This role can perform basic HMC management tasks like starting, stopping, and managing logical partitions.
4. **hmcservicerep** (Service Representative):
   This role has access to tasks related to service and support, such as backing up HMC data.
5. **hmcviewer** (Viewer):
   This role allows users to view HMC interface and data but does not allow them to perform actions.

For the purposes of performing different operations the future section of document has steps shared to create hmcsuperadmin and hmcviewer users.

HMC Power 9 Appliance will be pre-loaded with the Base HMC Release **10.3.1050.0** version as part of Manufacturing.

6. On Power On, the HMC will be loaded with version 10.3.1050.0
7. User can login with the default user “hscroot” and default password “abc123”. On the first successful login the HMC will mandate the user to change the password. User can choose new password and proceed to next steps.
8. With the New Credentials HMC will guide the User to set the Network Settings for the HMC.
9. To Update the HMC to 10.3.1062.1 User has to update the following Update drivers:
10. First update image 10.3.1062.0
11. Update image 10.3.1062.1

Copy the update iso images to /home/hmcsuperadmin and follow below commands for HMC Installation from Local Disk:

```
updhmc -t disk -f /home/hmcsuperadmin/<install_update.iso>
```

Install Images are available at IBM Fix Central URL:
https://www.ibm.com/support/fixcentral/main/selectFixes?parent=powersysmgmntcouncil&product=ibm~hmc~9100HMCppc&release=V10R3&platform=Al

Examples:

10.3.1062.0 Update:
Use "updhmc" command below from remote terminal on HMC to install HMC with 10.3.1062.0 update Image

```
updhmc -t disk -f /home/hmcsuperadmin/MF71722-10.3.1062.0-2505290127-ppc64le.iso -r
```

10.3.1062.1 Update:
Use "updhmc" command below from remote terminal on HMC to install HMC with 10.3.1062.1 update Image

```
updhmc -t disk -f /home/hmcsuperadmin/MF71728-10.3.1062.1-2506170641-ppc64le.iso -r
```

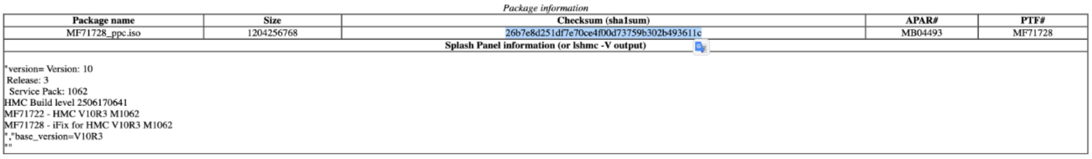
Use "lshmc" command below from remote terminal on HMC to list the installed HMC version:

```
lshmc -V
```

```
hscroot@hmc-mowgli1:~> lshmc -V
"version= Version: 10
 Release: 3
 Service Pack: 1062
HMC Build level 2506170641
MF71722 - HMC V10R3 M1062
MF71728 - iFix for HMC V10R3 M1062
","base_version=V10R3
"
```

Step to verify the hash for the HMC Update driver:

Using checksum command user can validate the Package information mentioned in the Fix Central for the downloaded iso update image. Use "sha1sum" command below from remote terminal where image is downloaded. HMC uses sha1 to generate checksum.



Package information

Package name	Size	Checksum (sha1sum)	APAR#	PTF#
MF71728_ppc.iso	1204256768	26b7e8d251df7e70ce4f00d73759b302b493611c	MB04493	MF71728
Splash Panel information (or lshmc -V output)				

```
"version= Version: 10
 Release: 3
  Service Pack: 1062
HMC Build level 2506170641
MF71722 - HMC V10R3 M1062
MF71728 - iFix for HMC V10R3 M1062
","base_version=V10R3
""
```

Figure 1

```
sha1sum MF71728-10.3.1062.1-2506170641-ppc64le.iso
26b7e8d251df7e70ce4f00d73759b302b493611c  MF71728-10.3.1062.1-2506170641-ppc64le.iso
```

Note: If the HMC prompts you with the message below during the update process, execute the reboot command.

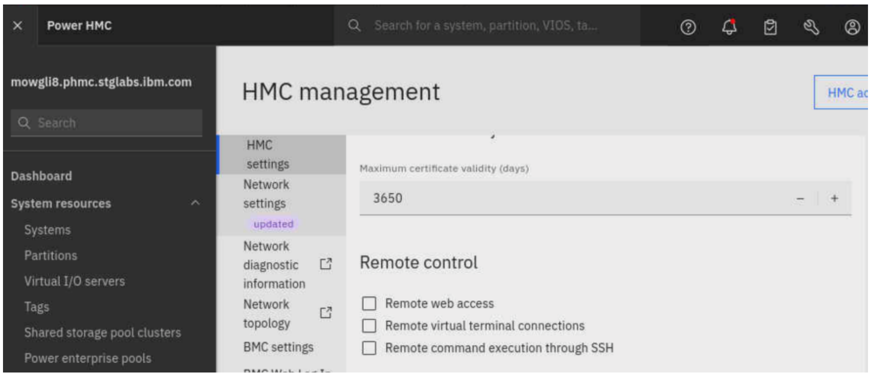
"A mandatory reboot is required but was not specified on the command syntax."

Reboot command: hmcshutdown -r -t now

4.3 Hardware Management Console (HMC) VPP Setup

HMC's Remote Administration methods of communication to enable:
To enable remote access following a fresh installation of the HMC, the super-admin user (hscroot) must activate Remote Web Access and Remote Command Execution (SSH) through the HMC's Local UI Console in the lab.

Using the default super-admin HMC user "hscroot", login via HMC Local Console UI and navigate to **HMC Management** -> **HMC Settings** under **Remote Control** and select both **Remote web access** & **Remote command execution through SSH** to enable.



Maximum certificate validity (days)

3650

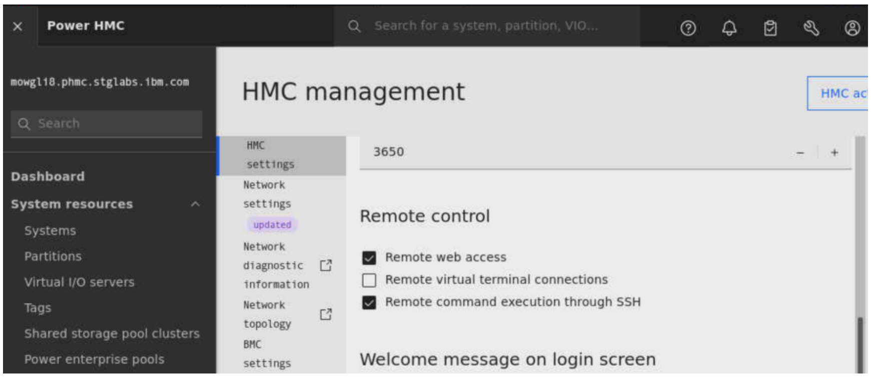
Remote control

□ Remote web access

□ Remote virtual terminal connections

□ Remote command execution through SSH

Figure 2



3650

Remote control

☑ Remote web access

□ Remote virtual terminal connections

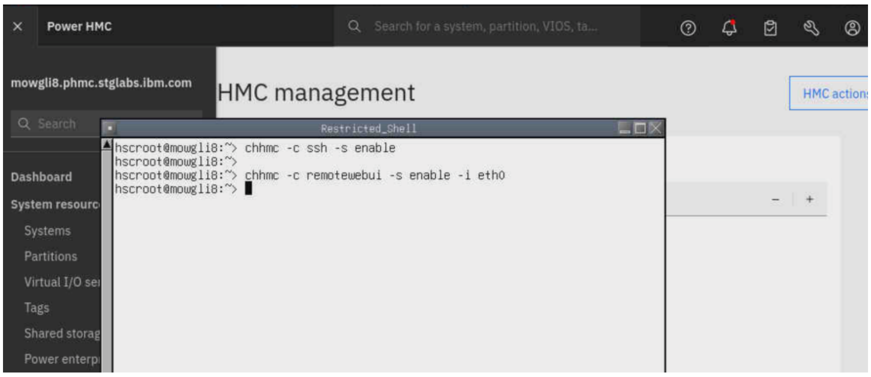
☑ Remote command execution through SSH

Welcome message on login screen

Figure 3

From the command line, to enable Remote Web UI and Remote Command Execution (SSH) follow below steps:

Access the HMC's Local Console UI: Navigate to **HMC Management -> HMC Actions** > **Open Restricted Shell Terminal**. This will launch the Restricted Shell, where you can run the necessary commands.



```
hscroot@mowgli8:~> chhmc -c ssh -s enable
hscroot@mowgli8:~>
hscroot@mowgli8:~> chhmc -c remotewebui -s enable -i eth0
hscroot@mowgli8:~>
```

Figure 4

The **hmcsuperadmin** can also enable and disable Web UI access and remote SSH using the following commands:

12. Command to enable or disable ssh:
    ->chhmc -c ssh -s <enable/disable>

13. Command to enable or disable remote webui:
    ->chhmc -c remotewebui -s <enable/disable> -i <interface>

14. List current status of ssh and remote webui:
    ->lshmc -r

Examples:
List current status of ssh and remote webui:
-> lshmc -r
ssh=**disable**,sshprotocol=2,sshusedns=enable,sshtimeout=0,**remotewebui**=**disable**,xntp=disable,xntpstatus=,xntpserver=,syslogserver=,syslogtcpserver=,syslogtlsserver=,altdiskboot=disable,ldap=disable,kerberos=disable,kerberos_default_realm=,kerberos_realm_kdc=,kerberos_clockskew=,kerberos_ticket_lifetime=,kpasswd_admin=,trace=,kerberos_trace_level=,kerberos_keyfile_present=,kerberos_auth_timeout=,security=nist_sp800_131a,sol=disabled,powerscuiagent=enable

Enable remote webui:
->chhmc -c remotewebui -s enable -i eth0

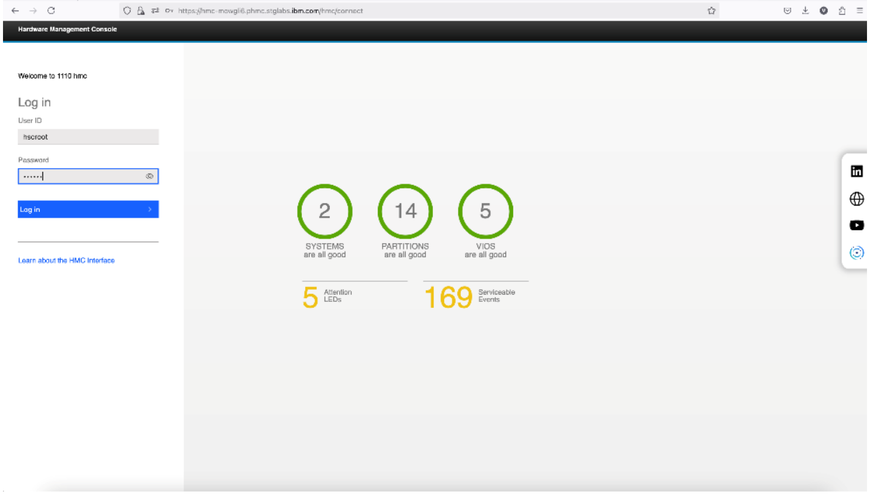
Enable remote ssh:
->chhmc -c ssh -s enable

Re-confirm enablement by listing current status of ssh and remote webui:
->lshmc -r
ssh=**enable**,sshprotocol=2,sshusedns=enable,sshtimeout=0,**remotewebui**=**enable**,xntp=disable,xntpstatus=,xntpserver=,syslogserver=,syslogtcpserver=,syslogtlsserver=,altdiskboot=disable,ldap=disable,kerberos=disable,kerberos_default_realm=,kerberos_realm_kdc=,kerberos_clockskew=,kerberos_ticket_lifetime=,kpasswd_admin=,trace=,kerberos_trace_level=,kerberos_keyfile_present=,kerberos_auth_timeout=,security=nist_sp800_131a,sol=disabled,powerscuiagent=enable

Steps to Launch Remote Web UI:

15. Open a web browser.
16. Enter the URL: Provide https://<IP> or https://<FQDN> (Fully Qualified Domain Name) of the target HMC in the address bar.
17. Ensure the HMC is pingable from the remote system from which you are attempting to launch the GUI.

    This will open the HMC GUI login page, where the user can enter their User ID and Password.


https://hmc-mowgli6.phmc.stglabs.ibm.com/hmc/connect
Hardware Management Console
Log in
Learn about the HMC Interface
SYSTEMS
are all good
PARTITIONS
are all good
VIOS
are all good
Attention
LEDs
Serviceable
Events

Welcome to 1110 hmc

User ID: hscroot

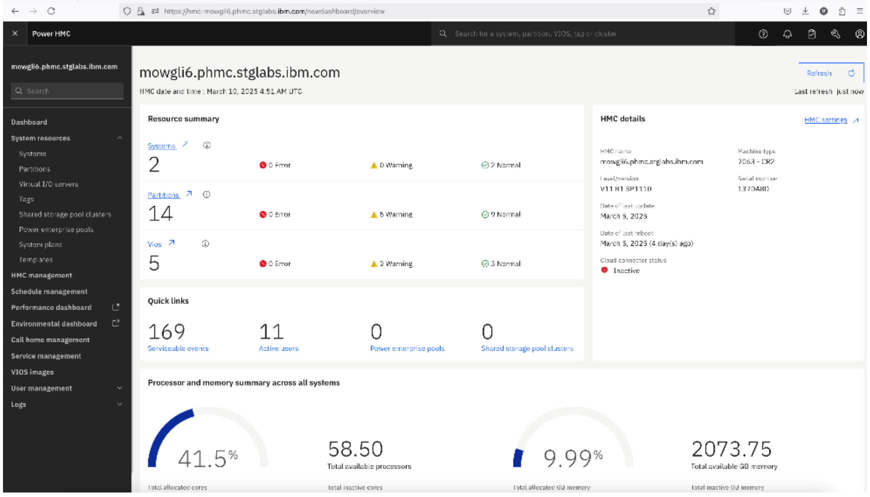
Password: ••••••

2 SYSTEMS are all good; 14 PARTITIONS are all good; 5 VIOS are all good

5 Attention LEDs; 169 Serviceable Events

Figure 5

After authenticating, the HMC GUI dashboard will be launched.



mowgli6.phmc.stglabs.ibm.com

HMC date and time : March 10, 2025 4.51 AM UTC

Last refresh just now

Resource summary

Systems 2	0 Error	0 Warning	2 Normal
Partitions 14	0 Error	5 Warning	9 Normal
Vios 5	0 Error	2 Warning	3 Normal

HMC details

HMC name: mowgli6.phmc.stglabs.ibm.com

Machine type: 7063 - CR2

Level/version: V11 R1 SP1110

Serial number: 137DA8D

Date of last update: March 5, 2025

Date of last reboot: March 5, 2025 (4 day(s) ago)

Cloud connector status: Inactive

Quick links

169 Serviceable events; 11 Active users; 0 Power enterprise pools; 0 Shared storage pool clusters

Processor and memory summary across all systems

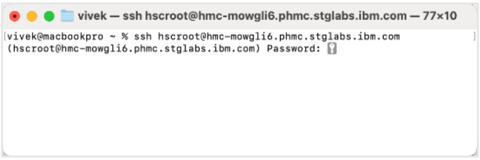
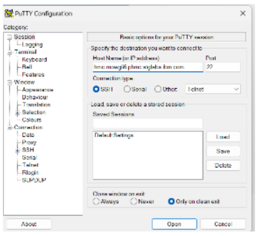
41.5% Total allocated cores; 58.50 Total available processors; Total inactive cores; 9.99% Total allocated GB memory; 2073.75 Total available GB memory; Total inactive GB memory

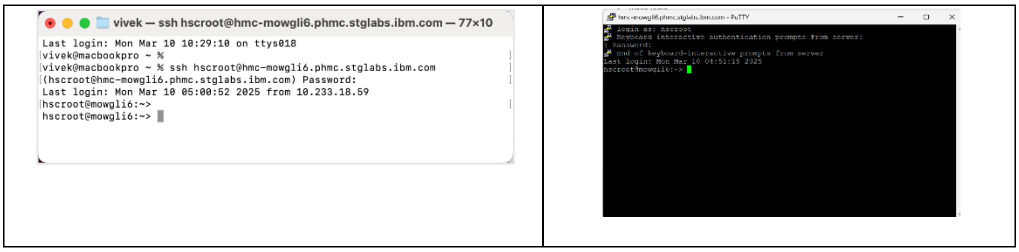
Figure 6

Steps to launch Remote Command Execution through SSH:

18. Launch Terminal from Linux / Mac or Putty from Windows.
19. Pass the HMC host name (FQDN) / IP and credentials to login from respective ssh terminals.

Linux box / Mac	Windows Putty

Syntax:
ssh hscroot@<HMC FQDN or HMC IP>

vivek — ssh hscroot@hmc-mowgli6.phmc.stglabs.ibm.com — 77×10
`vivek@macbookpro ~ % ssh hscroot@hmc-mowgli6.phmc.stglabs.ibm.com`
`(hscroot@hmc-mowgli6.phmc.stglabs.ibm.com) Password:`
	
	 PuTTY Configuration
	Category:
	Session
	Logging
	Terminal
	Keyboard
	Bell
	Features
	Window
	Appearance
	Behaviour
	Translation
	Selection
	Colours
	Connection
	Data
	Proxy
	SSH
	Serial
	Telnet
	Rlogin
	SUPDUP
	Load
	Save
	Delete
	About
	Open
	Cancel
	Basic options for your PuTTY session
	Specify the destination you want to connect to
	Host Name (or IP address): hmc-mowgli6.phmc.stglabs.ibm.com
	Port: 22
	Connection type: ● SSH ○ Serial ○ Other: Telnet
	Load, save or delete a stored session
	Saved Sessions
	Default Settings
	Close window on exit: ○ Always ○ Never ● Only on clean exit


vivek — ssh hscroot@hmc-mowgli6.phmc.stglabs.ibm.com — 77×10
hmc-mowgli6.phmc.stglabs.ibm.com - PuTTY

```
Last login: Mon Mar 10 10:29:10 on ttys018
vivek@macbookpro ~ %
vivek@macbookpro ~ % ssh hscroot@hmc-mowgli6.phmc.stglabs.ibm.com
(hscroot@hmc-mowgli6.phmc.stglabs.ibm.com) Password:
Last login: Mon Mar 10 05:00:52 2025 from 10.233.18.59
hscroot@mowgli6:~>
hscroot@mowgli6:~>
```

```
login as: hscroot
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Mon Mar 10 04:51:15 2025
hscroot@mowgli6:~>
```

Figure 7

4.3.1 Password Policy

This section outlines the procedure for enabling a dedicated password policy on the HMC. The password policy, titled "**HMC VPP Security Password Policy**" can be enabled by the hmcsuperadmin user.

Once enabled, this policy enforces the enhanced password standards to strengthen system security. The requirements include:

1. A minimum password length of 15 characters
2. At least one numeric digit
3. At least one uppercase letter

Command to apply "HMC VPP Security Password Policy" policy
->chpwdpolicy -o a -n "HMC VPP Security Password Policy"

Command to verify Policy Settings:
->lspwdpolicy -t p
active=1,name=HMC VPP Security Password Policy,description=,min_pwage=1,pwage=180,min_length=15,hist_size=10,warn_pwage=7,min_digits=1,min_uppercase_chars=1,min_lowercase_chars=6,min_special_chars=1,inactivity_expiration=180

4.3.2 User Creation

This section explains user creation commands from the HMC CLI and GUI.

To perform the following commands, ssh as the default super-admin HMC user "hscroot":

Commands to create product support user HSCPE and enable remote access for CLI and web ui:

20. ->mkhmcusr -u hscpe -a hmcpe --passwd makeitsimple -M 180 -d "HMC hscpe"
21. ->chhmcusr -i "name=hscpe,remote_webui_access=1,remote_ssh_access=1"

Commands to create HMC Viewer user and enable remote access for CLI and web ui:

22. ->mkhmcusr -u hmcviewer -a hmcviewer --passwd makeitsimple -M 180 -d "HMC Viewer"
23. ->chhmcusr -i "name=hmcviewer,remote_webui_access=1,remote_ssh_access=1"

Commands to create HMC Superadmin user and enable remote access for CLI and web ui:

24. ->mkhmcusr -u hmcsuperadmin -a hmcsuperadmin --passwd Howitsgoing@123 -d "HMCSuperAdmin"
25. ->chhmcusr -i "name=hmcsuperadmin,remote_webui_access=1,remote_ssh_access=1"

To perform the following actions from the GUI, login as the default super-admin HMC user "hscroot":

26. In the left navigation window select "**User Management**" & click on "**User Profiles**"

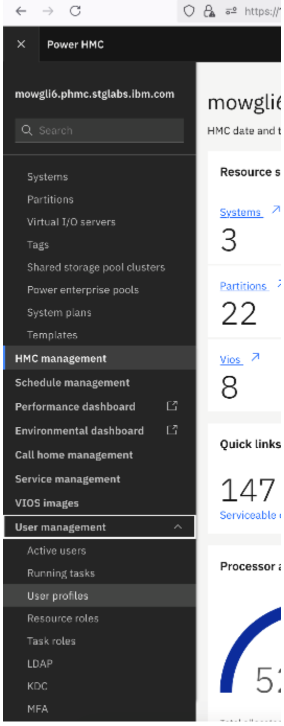
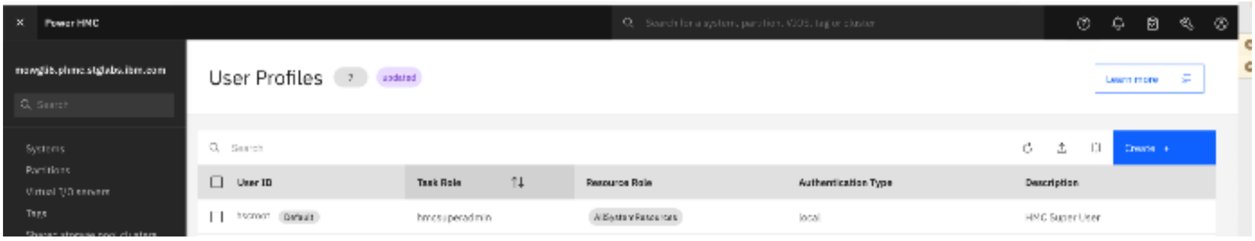


Figure 8

27. This will display the User Profiles page. To create a user click "**Create**":

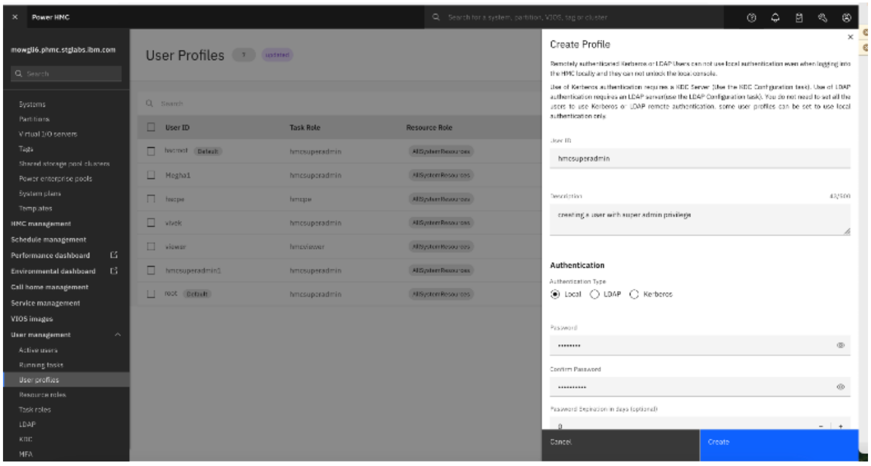


User Profiles 7 updated

User ID	Task Role	Resource Role	Authentication Type	Description
hscroot Default	hmcsuperadmin	AllSystemResources	local	HMC Super User

Figure 9

28. After click values as "User name", "Description", "Password" "Confirm Password"



Create Profile

Remotely authenticated Kerberos or LDAP Users can not use local authentication even when logging into the HMC locally and they can not unlock the local console.

Use of Kerberos authentication requires a KDC Server (Use the KDC Configuration task). Use of LDAP authentication requires an LDAP server(use the LDAP Configuration task). You do not need to set all the users to use Kerberos or LDAP remote authentication. some user profiles can be set to use local authentication only.

User ID: hmcsuperadmin

Description: creating a user with super admin privilege 43/500

Authentication

Authentication Type: ● Local ○ LDAP ○ Kerberos

Password: ••••••••

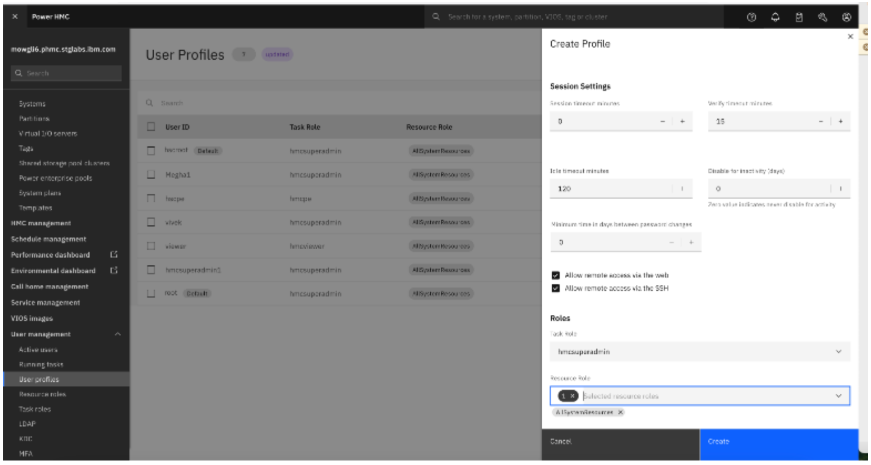
Confirm Password: ••••••••••

Password Expiration in days (optional): 0

Cancel Create

Figure 10

29. Select “Allow remote access via the web” and “Allow remote access via the SSH” check boxes. Additionally, select the appropriate “Task Role” and “Resource Role” & click “Create”



User ID	Task Role	Resource Role
hscroot Default	hmcsuperadmin	AllSystemResources
Megha1	hmcsuperadmin	AllSystemResources
hscpe	hmcpe	AllSystemResources
vivek	hmcsuperadmin	AllSystemResources
viewer	hmcviewer	AllSystemResources
hmcsuperadmin1	hmcsuperadmin	AllSystemResources
root Default	hmcsuperadmin	AllSystemResources

Create Profile

Session Settings

Session timeout minutes: 0

Verify timeout minutes: 15

Idle timeout minutes: 120

Disable for inactivity (days): 0

Zero value indicates never disable for activity

Minimum time in days between password changes: 0

☑ Allow remote access via the web

☑ Allow remote access via the SSH

Roles

Task Role: hmcsuperadmin

Resource Role: 1 × Selected resource roles

AllSystemResources ×

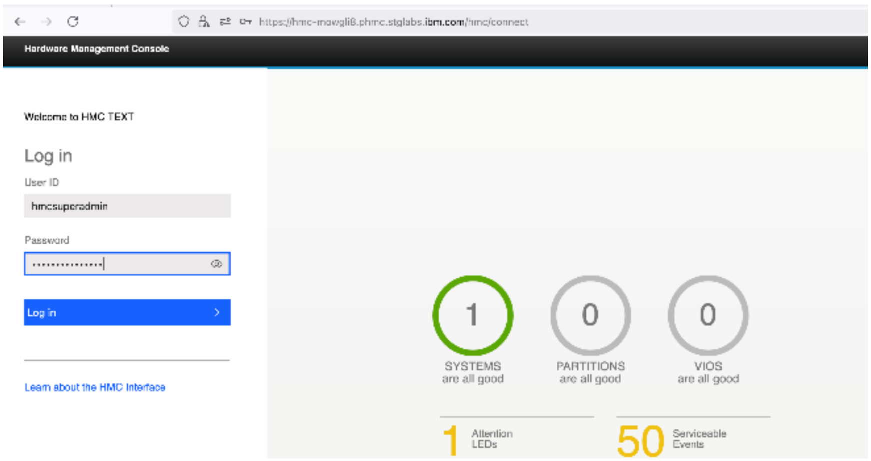
Figure 11

4.3.3 User login and session

This section provides details of login using newly created HMC SuperAdmin User “hmcsuperadmin” using CLI and GUI & enable sessions.

Run below command from remote system to connect to HMC command line (please refer **4.3.8** to enable public key-based authentication and **4.3.11** to enable public key-based login flow under **HMC as a Server**)
ssh -o HostKeyAlgorithms=+ssh-rsa hmcsuperadmin@<hmc_IP or hmc_FQDN>

Use the steps below from remote system browser to login to HMC using GUI
At the web browser address bar provide the IP or Fully Qualified Domain Name of the target HMC:
This will launch the following HMC GUI Login Page where user can enter the User ID and Password


https://hmc-mowgli6.phmc.stglabs.ibm.com/hmc/connect

User ID: hmcsuperadmin

Password: ••••••••••••••••

Figure 12

After Authenticating the user the HMC GUI dashboard will be launched:

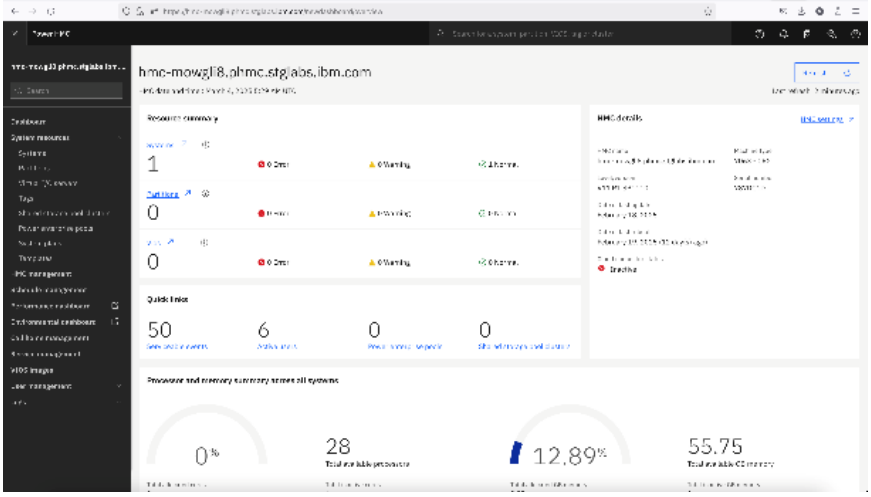


Figure 13

4.3.4 Inactivity timeout configuration for HMC users

This section provides details on configuration of remote connection inactivity on HMC. HMC user with task role “hmcsuperadmin” can configure the session parameters for any users.

Use below HMC command to configure remote connection timeout for inactive per user from remote terminal:

```
chhmcusr -i "name=<hmc_user>,inactivity_expiration=x"
```

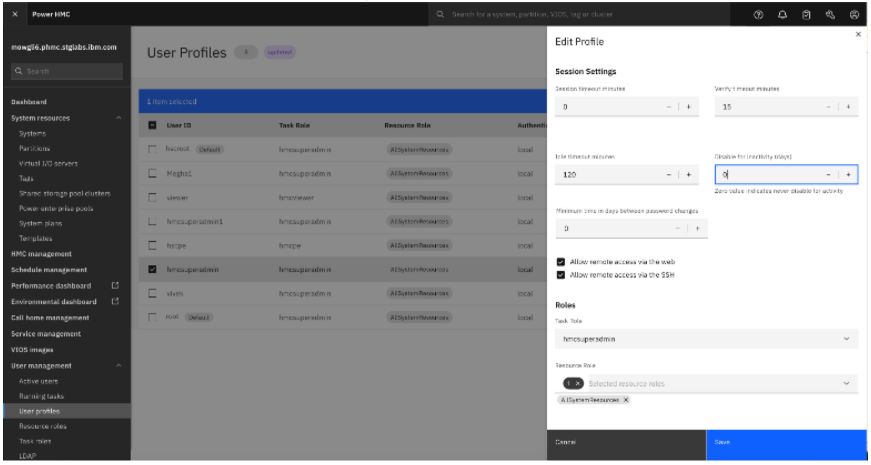
(x in days and 0 means never expire)

Note: Upon activating administrative policy, the policy supplied inactivity expiration will be considered for all HMC users

Use HMC GUI below to configure remote connection timeout for inactive per user from remote web browser:

From **User Profiles** under **User Management**, select a User and click Edit. This will display the **Edit Profile** where we can change the **Session Settings** for the User within the “**Disable for inactivity (days)**” field. See figure

Click the **Save** button when complete with your selections.


User Profiles

1 item selected

User ID	Task Role	Resource Role	Authenti
hscroot Default	hmcsuperadmin	AllSystemResources	local
Megha1	hmcsuperadmin	AllSystemResources	local
viewer	hmcviewer	AllSystemResources	local
hmcsuperadmin1	hmcsuperadmin	AllSystemResources	local
hscpe	hmcpe	AllSystemResources	local
hmcsuperadmin	hmcsuperadmin	AllSystemResources	local
vivek	hmcsuperadmin	AllSystemResources	local
root Default	hmcsuperadmin	AllSystemResources	local

Edit Profile

Session Settings

Session timeout minutes: 0

Verify timeout minutes: 15

Idle timeout minutes: 120

Disable for inactivity (days): 0

Zero value indicates never disable for activity

Minimum time in days between password changes: 0

☑ Allow remote access via the web

☑ Allow remote access via the SSH

Roles

Task Role: hmcsuperadmin

Resource Role: Selected resource roles

AllSystemResources

Figure 14

4.3.5 Lockout Policy configuration for HMC Users

This section provides details on configuring lockout policy for HMC users. HMC user with task role "hmcsuperadmin" can configure Lockout Policy.

Use the HMC Command below to configure lockout policy from remote terminal:

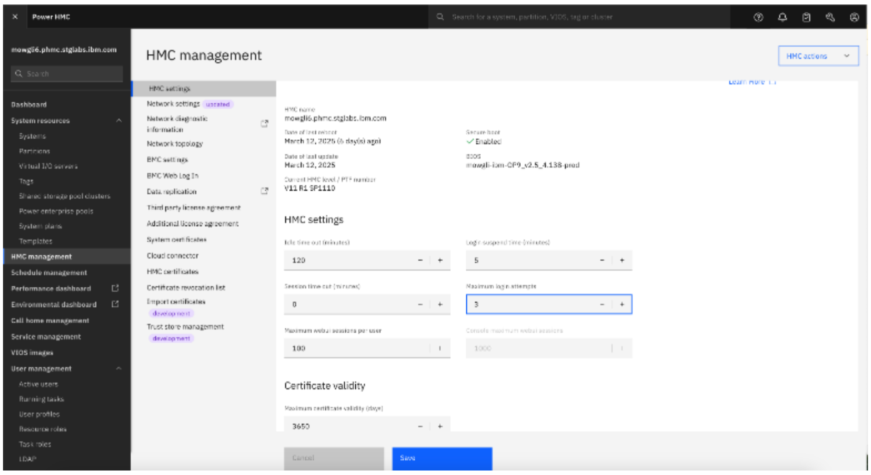
```
->chhmcusr -t default -i "max_login_attempts=x"
(where x is maximum number of times login attempts is allowed)
->chhmcusr -t default -i "login_suspend_time=y"
(where y is suspend time in minutes)
```

Use the HMC command to list all the HMC user information to confirm setting from remote terminal:

->lshmcusr -t default
session_timeout=0,idle_timeout=120,**max_login_attempts=3**,**login_suspend_time=5**,max_webui_sessions_per_user=100,max_webui_sessions=1000
(here, if the login password is wrong for 3 times continuously, then the user gets locked for 5 minutes)

Use HMC GUI to configure the lockout policy for a remote web browser:

1. Within **HMC Settings** under **HMC Management**, modify the "**Maximum login attempts**" field. Click **Save** when complete with your selections.



HMC management

HMC name
mowgli6.phmc.stglabs.ibm.com

Date of last reboot
March 12, 2025 (6 day(s) ago)

Secure boot
✓ Enabled

Date of last update
March 12, 2025

BIOS
mowgli-ibm-OP9_v2.5_4.138-prod

Current HMC level / PTF number
V11 R1 SP1110

HMC settings

Idle time out (minutes): 120

Login suspend time (minutes): 5

Session time out (minutes): 0

Maximum login attempts: 3

Maximum webui sessions per user: 100

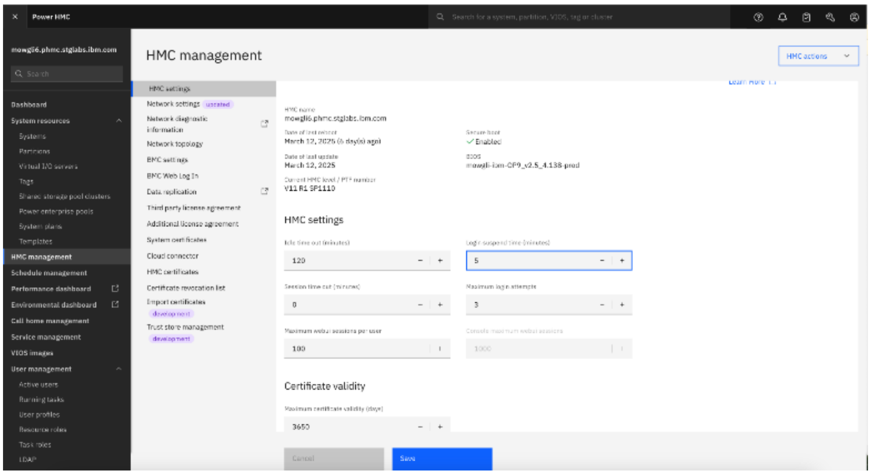
Console maximum webui sessions: 1000

Certificate validity

Maximum certificate validity (days): 3650

Figure 15

2. From **HMC Settings** under **HMC Management**, we can change the **HMC Settings** for "**Login suspend time (minutes)**". Click **Save** when complete with your selections.



HMC management

HMC name
mowgli6.phmc.stglabs.ibm.com

Date of last reboot
March 12, 2025 (6 day(s) ago)

Secure boot
✓ Enabled

Date of last update
March 12, 2025

BIOS
mowgli-ibm-OP9_v2.5_4.138-prod

Current HMC level / PTF number
V11 R1 SP1110

HMC settings

Idle time out (minutes): 120

Login suspend time (minutes): 5

Session time out (minutes): 0

Maximum login attempts: 3

Maximum webui sessions per user: 100

Console maximum webui sessions: 1000

Certificate validity

Maximum certificate validity (days): 3650

Figure 16

Use following HMC command to run from a “hmcsuperadmin” user to change the mentioned user password and also to unlock the mention user before its login suspend period has been elapsed:

```
->chhmcusr -i "name=<user_name>,passwd=<password>"
```

4.3.6 Banner and Welcome Text configuration on HMC for CLI and GUI

This section describes the banner or welcome text settings on the HMC.

Banner Text setting:
Use scp to copy the banner file from remote system to /tmp on the HMC, then deploy it:

```
->scp someID@someHost:/tmp/BannerFile.txt /tmp
```

Use the command below to configure the banner text on the HMC from a remote terminal:

```
->chusrtca -o ab -b /tmp/BannerFile.txt
```

(Pre-requisite: the file name with Banner content should be similar to "BannerFile.txt" and located within the /tmp/ directory)

Use the command below to remove banner text from HMC from remote terminal:

```
->chusrtca -c -b /tmp/BannerFile.txt
```

Removes banner text from the HMC. The banner text will no longer be displayed:

```
->chusrtca -o rb
```

Example banner text on HMC login using CLI from remote terminal:

```
-> ssh hscroot@<hmc hostname or ip address>
HMC Banner TEXT here
Password:
```

Notes: Ensure Banner Text has new line character, so it is not wrapped up.

```
-> cat /tmp/BannerFile.txt
TEST BANNER TEXT TESThscroot@mowgli2hmc:~>
-> cat /tmp/BannerFile.txt
TEST BANNER TEXT TEST by HMC IBM
->
```

Banner text is for SSH only, for GUI the Welcome Text is available which can be configured by both SSH command and GUI as shown below.

Welcome Text setting:
Use scp to copy the welcome text file to /tmp on the HMC, then deploy it:
->scp someID@someHost:/tmp/WelcomeFile.txt /tmp

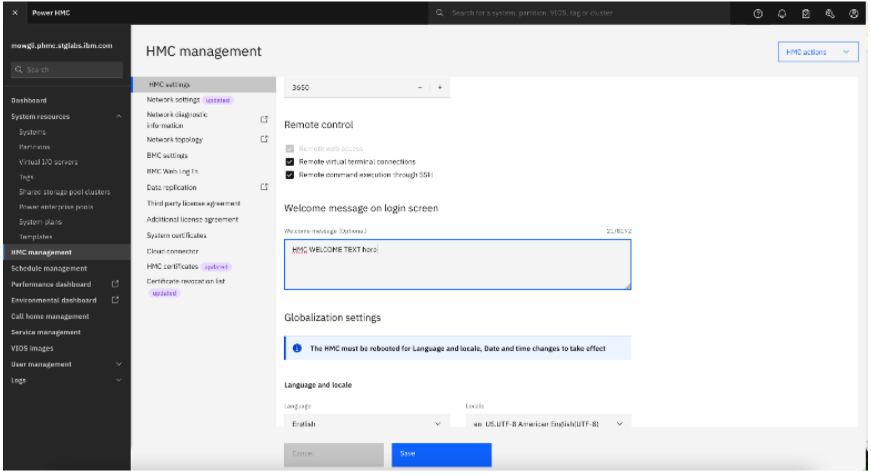
Use the command below to configure welcome text on HMC from remote terminal:
->chusrtca -o a -f /tmp/WelcomeFile.txt -c
(Pre-requisite: the file name with Banner content should be like "BannerFile.txt" and to be available in /tmp)

Use the command below to remove welcome text on HMC from remote terminal:
->chusrtca -c -b /tmp/BannerFile.txt

Removes banner text from the HMC. The banner text will no longer be displayed:
chusrtca -o r

Use the GUI below to configure welcome text on HMC from remote web browser:

1. Within **HMC Settings** under **HMC Management**, modify the **Welcome message on login screen** field. See figure



HMC management

3650

Remote control

☑ Remote web access
☑ Remote virtual terminal connections
☑ Remote command execution through SSH

Welcome message on login screen

Welcome message (Optional)
HMC WELCOME TEXT here

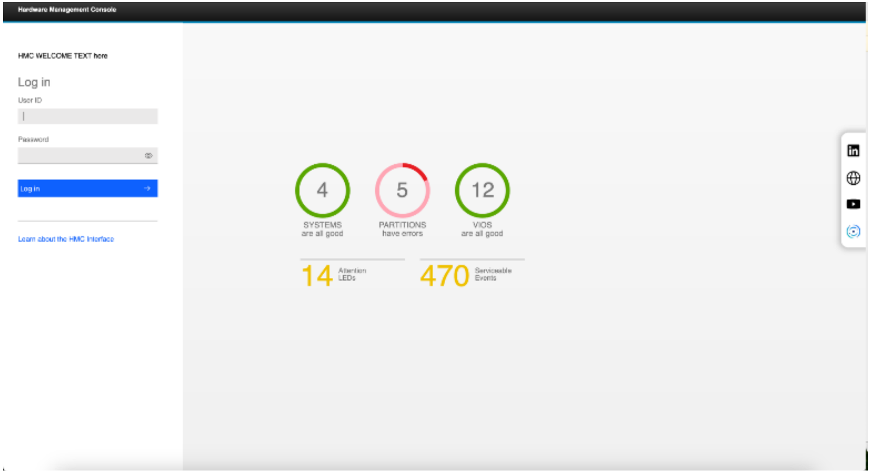
Globalization settings

The HMC must be rebooted for Language and locale, Date and time changes to take effect

Language and locale
Language: English
Locale: en_US.UTF-8 American English(UTF-8)

Figure 17

In the Login page above the “Log-in” text you will notice configured welcome message text.



HMC WELCOME TEXT here

Figure 18

4.3.7 SSH ciphers and algorithms configuration

This section explains the steps to enable and set various ssh configurations like ssh cipher, ssh mac, ssh key and ssh hostkey algorithms. The options to configure ssh is available only through HMC CLI and can be executed by “hmcsuperadmin” user. The ciphers setting used for HMC as SSH client or SSH server are same.

Command for SSH cipher setting:

- List ssh cipher
  ```
  -> lshmcencr -c ssh -t c
  "curr_encryptions=aes128-ctr,aes128-gcm@openssh.com,aes192-ctr,aes256-ctr,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com"
  ```

- Remove not required ssh cipher
  ```
  -> chhmcencr -c ssh -o r -e aes128-gcm@openssh.com,aes192-ctr,aes256-ctr,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com
  ```

- List configured aes128-ctr ssh cipher
  ```
  -:~> lshmcencr -c ssh -t c
  curr_encryptions=aes128-ctr
  ```

Command for SSH MAC setting:

- List ssh mac algorithms
  ```
  -> lshmcencr -c sshmac -t c
  "curr_encryptions=hmac-sha1,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-512-etm@openssh.com,umac-128-etm@openssh.com,umac-128@openssh.com,umac-64-etm@openssh.com,umac-64@openssh.com"
  ```

- Remove not required ssh mac algorithms
  ```
  -> chhmcencr -c sshmac -o r -e hmac-sha1,hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-512-etm@openssh.com,umac-128-etm@openssh.com,umac-128@openssh.com,umac-64-etm@openssh.com,umac-64@openssh.com
  ```

- List configured hmac-sha2-256 ssh mac algorithm
  ```
  -> lshmcencr -c sshmac -t c
  curr_encryptions=hmac-sha2-256
  ```

Command for SSH KEY setting:

- List ssh key algorithms
  ```
  -> lshmcencr -c sshkey -t c
  "curr_encryptions=curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,sntrup4591761x25519-sha512@tinyssh.org"
  ```

- Remove not required ssh key algorithms
  ```
  -> chhmcencr -c sshkey -o r -e "curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,sntrup4591761x25519-sha512@tinyssh.org"
  ```

- List configured ecdh-sha2-nistp256,ecdh-sha2-nistp384 ssh key algorithms
  ```
  -> lshmcencr -c sshkey -t c
  "curr_encryptions=ecdh-sha2-nistp256,ecdh-sha2-nistp384"
  ```

Command for SSH HOST KEY setting:

- List ssh host key algorithms
  ```
  -> lshmcencr -c sshhostkey -t c
  curr_encryptions="curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,sntrup4591761x25519-sha512@tinyssh.org,ssh-rsa
  ```

- Remove not required ssh host key algorithms
  ```
  -> chhmcencr -c sshhostkey -o r -e "ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-dss,ssh-dss-cert-v01@openssh.com,ssh-ed25519,ssh-ed25519-cert-v01@openssh.com"
  ```

- List configured ssh-rsa ssh host key algorithm
  ```
  -> lshmcencr -c sshhostkey -t c
  curr_encryptions=ssh-rsa
  ```

4.3.8 SSH authentication methods

This section explains the ssh authentication methods available on HMC. The options to configure ssh authentication is available only through HMC CLI and can be executed by "hmcsuperadmin" user.

Before proceeding with ssh configuration, check ssh service is enabled on HMc by using command below:
-> lshmc -r
ssh=enable,sshprotocol=2,sshusedns=enable,sshtimeout=0,remotewebui=enable

In case ssh is not enabled, use command below to enable:

```
-> chhmc -c ssh -s enable
```

HMC commands "lshmc -r " and "chhmc -c ssh" can be used from remote terminal to view and modify the changes respectively. Use double hyphen character as prefix to the option sshauth in the command.

Important Note: When using "public key" as authentication type, ensure an active ssh session of "hmcsuperadmin" user is running to copy keys. If authentication type is "public key" is selected without copying keys then only way to get back HMC will be through reinstallation.

Example commands:
Use command below on HMC to set authentication as password and publickey:
-> chhmc -c ssh -s modify **--sshauth passwd,publickey**

Use command below on HMC to set authentication as password:
-> chhmc -c ssh -s modify **--sshauth passwd** > support only **password**

Use command below on HMC to set authentication as publickey:
-> chhmc -c ssh -s modify **--sshauth publickey** > support only **publickey**

Use command below on HMC to list the status of setting:
-> lshmc -r -F **sshauth passwd,publickey/publickey/passwd**

please refer 4.3.11 to enable public key-based login flow under HMC as a Server

4.3.9 SSH Rekey configuration

This section provides details about SSH rekey configuration. Use double hyphen character as prefix to the option sshrekeylimit in the command.

Example commands:
Command to enable sshrekeylimit with 1G 1h:

```
-> chhmc -c ssh -s enable --sshrekeylimit enable
```

4.3.10 SSH Packet Size configuration

This section provides details about configuring HMC with ssh maximum packet length as 35k bytes. Once configuration is done, the packet containing more than 35K bytes, will be dropped or discarded. HMC reboot is required after the configuration. Use double hyphen character as prefix to the option sshrestrictedpkt in the command.

Run below commands to configure ssh maximum packet length to 35K bytes:

```
-> chhmc -c ssh -s modify --sshrestrictedpkt enable
```

Run below commands to configure ssh maximum packet length to default:

```
-> chhmc -c ssh -s modify --sshrestrictedpkt disable
```

Command to reboot HMC

```
hmcshutdown -r -t now
```

4.3.11 SSH Key Based Authentication configuration

This section explains details to enable SSH key based authentication when HMC acts as a Server and a Client.

HMC as a Server:
Run below command on Source linux system:

```
-> ssh-keygen -t rsa -b 2048 -f /home/<userhome>/.ssh/id_rsa  [updated to consider 2048 key]
```

Example commands:

```
-> ssh-keygen -t rsa -b 2048 -f /home/linuxuser/.ssh/id_rsa
```

List the public key by using the command below:

```
-> cat /home/linuxuser/.ssh/id_rsa.pud
```

Copy the public key from above command and use below commands to add the keys to HMC.
Start with login to HMC with IP address as hmcip using hmcsuperadmin user.

```
-> ssh hmcsuperadmin@hmcip
```

Add the copied public key by running below command on HMC

```
-> mkauthkeys -a "public key string obtained from source linux"
```

Example command:

```
-> mkauthkeys -a “ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCwClvBY22mltRsi076pDWiNHxbTDFm6lj9dq5M5D+a2
xLY8G7eJZthZQ5/kUHt6vz2G0OUss1AKd+1l1X5bZ9HM4+M0DTk0rx7hnY6nJ7z2HYlwDKBLDG7
ZUl8nxGancqoH6ZMrDbcX/FwNiKcO1ls6xB6pteHaMMHsvCn7fBGmp9aUWVTEoLxp4e3k8BkV6
X83Bio9vgbACdML5pvMg9zRVSVwRbTfvHZ5Vv2vSHsH88sPhZZSqFTkpJNq8WRGgN3FVLcER2
Tej0ypx3iNgkYWym6sLce0Y8D6eYyWK3IRubsbwaHIZqCk89/UF8Nc17B9iGx4fPlT+uy8du2Npg
```

```
BF7jT55pJ7wsWc1hseaxHjZuBpcdyqZzoRK+xk175VJdeJYz5PqBWziiSYzVlm9uWtuhhqHF1GDMj
CqvrV/tnacqEPWBevO8m8sCKuPjQUdGkYvZqVR0X2TcflINnVrajQPICJtcEpDXlbl766GSwj7De9X
NWlu2GdhVYpzJKRY0= hmcsuperadmin@hmcdomain”
```

List the added public key
Once public key is added, use HMC command as below to list the public key:

```
-> cat .ssh/authorized_keys2
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCwClvBY22mltRsi076pDWiNHxbTDFm6lj9dq5M5D+a2
xLY8G7eJZthZQ5/kUHt6vz2G0OUss1AKd+1l1X5bZ9HM4+M0DTk0rx7hnY6nJ7z2HYlwDKBLDG7
ZUl8nxGancqoH6ZMrDbcX/FwNiKcO1ls6xB6pteHaMMHsvCn7fBGmp9aUWVTEoLxp4e3k8BkV6
X83Bio9vgbACdML5pvMg9zRVSVwRbTfvHZ5Vv2vSHsH88sPhZZSqFTkpJNq8WRGgN3FVLcER2
Tej0ypx3iNgkYWym6sLce0Y8D6eYyWK3IRubsbwaHIZqCk89/UF8Nc17B9iGx4fPlT+uy8du2Npg
BF7jT55pJ7wsWc1hseaxHjZuBpcdyqZzoRK+xk175VJdeJYz5PqBWziiSYzVlm9uWtuhhqHF1GDMj
CqvrV/tnacqEPWBevO8m8sCKuPjQUdGkYvZqVR0X2TcflINnVrajQPICJtcEpDXlbl766GSwj7De9X
NWlu2GdhVYpzJKRY0= hmcsuperadmin@hmcdomain
```

Configure the host based key pairs
Remove all existing key pairs and configure only the supplied type
Use HMC command as below to reconfigure the existing host key pair to use only ssh-rsa after every reboot of HMC.

```
-> chhmc -c sshhostkeys -s modify --sshkeytype ssh-rsa
```

The modify and add operation of host keys requires HMC reboot

```
-> hmcshutdown -r -t now
```

Login from Source Linux to HMC after public key is copied
From source linux use below ssh command to login to HMC with public key:

```
-> ssh hmcsuperadmin@hmcip
```

HMC as a client

Run below command on Source HMC:

```
-> ssh-keygen -t rsa -b 2048 -f /home/<userhome>/id_rsa      [updated to consider 2048 key]
```

<u>Example command:</u>

```
-> ssh-keygen -t rsa -b 2048 -f /home/hmcsuperadmin/id_rsa
```

List the public key by using the command below:

```
-> cat /home/hmcsuperadmin/id_rsa.pud
```

On the Destination linux system, copy the public key and add to authorised keys on destination

```
-> ssh destmachineuser@destinationmachineip
-> vi ~/.ssh/authorized_keys
```

Add the copied public key string and save it

Login from Source HMC to Linux system after public key is copied
From source HMC use below ssh command to login to Linux with public key:

```
-> ssh –i /home/<userhome>/id_rsa destmachineuser@destinationmachineip
```

<u>Example command:</u>

```
-> ssh -i /home/hmcsuperadmin/id_rsa destmachineuser@destinationmachineip
```

Run below commands to remove the generated keys
In case the keys are no longer needed, use HMC command as below to remove them from user home location on HMC:

```
-> chhmc -c sshuserkeys -s remove -f /home/<userhome>/id_rsa
```

The remove operation of user specific keys requires HMC reboot

```
-> hmcshutdown -r -t now
```

Example command

```
-> chhmc -c sshuserkeys -s remove -f  /home/hmcsuperadmin/id_rsa.pub
chhmc -c sshuserkeys -s remove -f  /home/hmcsuperadmin/id_rsa
```

4.3.12 SSH known hosts management in local database

This section explains the details on SSH known hosts management in local database of individual HMC users. The HMC command chhmc can be used by “hmcsuperadmin” user to do the known host management.

Add public key:
Use HMC command as below to add public key of system as specified in hostname to known_hosts file under .ssh folder of user home directory during ssh login.

```
-> chhmc -c sshknownhosts -s add -h <hostname> -a <ipaddress>
```

Example command:

```
-> chhmc -c sshknownhosts -s add -h sample.com -a 9.0.0.1 --sshkeytype ssh-rsa
```

List public key:
Use HMC command as below list the known_hosts.

```
-> lshmc --sshknownhosts
```

Example command:

```
lshmc --sshknownhosts

"known_host=sample.com,9.0.0.1 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDn8/84f2yygvrb+EXHgwuZ6immjtGNW/2JMVaPyGzrF
cE+KZNJZiHVmzcy5BZ8l8msSLTO9hR6m5t9nBYO2lAnqpZDz/9ipi1uDpq+PwfQ/2RtcoPD5lk0Z6
Ca8gjFrD1NF34ZMX3LhEDMa2DH9uz4Q+ufiw7m2q4zxzFxrtJ2AMhL/IwOlj76d+OIgN3MYtKK0p
WkefNdicIwAG5TCupFS3s8JiuXj89Zg5B3D6xE2EyDdiw/BjUKiDMk8fnq30UM0rJ7G9Na6CPudb5
ynUpbLOb1RTUUHCvdteDagwOxg+hFzwoHvRGxuT2u0iI5oAc8jgksVb2Y/Fy2STon92mop4I+Pe
DyhdRXUVcDf7zbsX9XCuKsEjH5X9YAMM/3xxShHbQncZFE7xBi52Iwj11JL+klVPSdvkpVp/W3FY
ppRtUsTpFipxuIqmYxfBco5s3OEEd0XCnMpw2oYGPud7eTuPytEAetvJa9Fb9wAsPDFTxdAmsJgF
AhFlvY+ixat4k="
```

Remove public key:
Use HMC command as below to remove public key of system as specified in hostname to known_hosts file under .ssh folder of user home directory during ssh login.

```
-> chhmc -c sshknownhosts -s remove -h <hostname> -a <ipaddress>
```

Example command:

```
chhmc -c sshknownhosts -s remove -h sample.com -a 9.0.0.1
```

4.3.13 CA-Signed Certificate and ciphers setting for TLS

This section contains details of HMC's CA signed certificate and steps to do cipher settings for TLS. HMC uses RSA based certificates with 2048 key size. Users have no option to configure it with some other algorithm. User can choose key size from 2048 (default), 3072, and 4096 values. For TLS communication only the TLS 1.2 ciphers are in scope to be configured. ECDHE cipher uses secp256r1, secp384r1 and secp521r1 elliptic curves by default no explicit settings are required.

Use below HMC command to list TLS 1.2 ciphers of HMC:

```
-> lshmcencr -c webui -t c
"curr_encryptions=TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256"
```

Use below HMC command to remove the encryption/ciphers other than approved TLS encryption **"TLS_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**" and **"TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",** it will require to reboot HMC:

```
-> chhmcencr -c webui -o r -e
"TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256"

The Hardware Management Console will automatically be restarted after the encryption ciphers are changed. Are you sure you want to change the encryption ciphers (0 = no, 1 = yes)?
1
```

Note: TLS change (remove or add) in encryption ciphers will need a mandatory HMC restart to take effect. Passing "1" will restart the HMC automatically.

Re-confirm only supported ciphers are present for TLS communication using below command:

```
-> lshmcencr -c webui -t c
curr_encryptions=TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

4.3.13.1 CSR file

This section provides the details on the first step towards HMC TLS certificate creation which is to create CSR file. Use below HMC command to create CSR file:

```
-> mkhmccert -t ca -f <FILENAME>.csr -i
"org=CA_TEST,org_unit=HMC,country=US,state=TX,locality=Austin,email=support@aus.ibm.comi
```

,days_to_expire=365,ipaddrs=<HMCIP>,dns=localhost.blr.stglabs.ibm.com,common_name=<HMC_IP>,key_size=2048"

Explanation of mkhmccert command:

mkhmccert creates a Hardware Management Console (HMC) certificate.
Options:

-t The type of certificate to create. Valid values are **self** to create a self-signed certificate, and **ca** to create a certificate signing request (CSR) for the server where the Certificate Authority (CA) signed certificate will be issued.

-f The name of the file where the CSR is to be saved.

-l The location where the CSR is to be saved. Valid values are **usb** for a USB data storage device, and **sftp** for a secure FTP (SFTP) server. If this option is not specified, the CSR will be saved to the HMC hard disk.

-h The host name or IP address of the SFTP server where the CSR is to be saved.
This option is required when the CSR is to be saved on an SFTP server. Otherwise, this option is not valid.

-u The user ID to use to log in to the SFTP server.
This option is required when the CSR is to be saved on an SFTP server. Otherwise, this option is not valid.

--passwd The password to use to log in to the SFTP server.
If both this option and the **-k** option are omitted, you will be prompted to enter the password. The **–passwd** and **-k** options are mutually exclusive.
This option is only valid when the CSR is to be saved on an SFTP server.

-k The name of the file that contains the SSH private key. If the file name is not fully qualified, the file must exist in the user's home directory on the HMC.
Use the **ssh-keygen** command to generate the public and private SSH key pair. The **ssh-keygen** command is not allowed to write to the **.ssh** directory in the user's home directory on the HMC, so when you run the command on the HMC, you must specify both the directory and the file name for the private key. If you generate a key with a passphrase, you will be prompted to enter the passphrase when you run any HMC command that uses the key.
If both this option and the **–passwd** option are omitted and the CSR is to be saved on an SFTP server, you will be prompted to enter the password. The **-k** and **–passwd** options are mutually exclusive.
This option is only valid when the CSR is to be saved on an SFTP server.

-d The directory where the CSR is to be saved.

-i The input data for the command. The input data consists of attribute name/value pairs, which are in comma separated value (CSV) format.
The format of the input data is as follows:
*attribute-name***=***value***,***attribute-name***=***value***,**…
Note that certain attributes accept a comma separated list of values, as follows:
*attribute-name***=***value***,***value***,**… ,…
When a list of values is specified, the attribute name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a '#146; character.
Valid attribute names for this command:
org
org_unit
country
Two-character ISO country code
state
locality

days_to_expire
email
ipaddrs
Comma separated list
dns
Comma separated list
common_name
Only valid for a CSR
key_size
Only valid for a self-signed certificate
Valid values are **2048** (default), **3072**, and **4096**

--temp When creating a CSR, specify this option to create a temporary self-signed certificate to be used until the CA returns the signed certificate.
The HMC will automatically be restarted to apply for the temporary self-signed certificate.

-r Specify this option to cause the HMC to automatically be restarted without asking for confirmation after applying for a self-signed certificate.

--force Specify this option to allow a self-signed certificate to be created without a domain name.

--help Display the help text for this command and exit.

4.3.13.2 Apply certificate

Once a CRT or certificate has been received from CA authority, it can be applied on HMC by following steps as described in this section. This section provides details of applying for the certificate as received from CA authority.

The certificate attributes will be validated before the certificate is applied on HMC automatically using "chhmccert -o apply" HMC command.

User can validate HMC certificate using OCSP URL using HMC command. Use sample HMC command as below to validate certificate with OCSP URL.

```
-> chhmccert -o validate -t cacert -f CertificateFile -s SigningFile1,SigningFile2 -d <certificate_dir>
--ocsp <ocspurl>
```

In above command, the files CertificateFile , SigningFile1,SigningFile2 are certificate files. <certificate_dir> is the Directory where certificate files are copied. <ocspurl> is the URL of OCSP server

Option 1: Use the following command to apply the certificate stored in USB:

```
-> chhmccert -o apply -t cacert -f <FILENAME>.crt -l usb -d /media/sdbX/
```

Note: Where "X" for media device. The media device can be found by using HMC command "lsmediadev". The output of command will list the media (USB) device attached to the HMC.

Option 2: Use the following command to apply the certificate stored in HMC local path:

```
-> chhmccert -o apply -t cacert -f <FILENAME>.crt -d /home/<current user>/
```

Example command to list the Current Applied CA Certificate:

```
lshmccert -t currcert
-> type=ca,version=3,serial_num=170839,"issuer=CN=IBM INTERNAL INTERMEDIATE CA,
CN=IBM INTERNAL INTERMEDIATE CA, O=International Business Machines Corporation,
C=US","valid_from=Jan 9, 2025, 5:00:00 AM","valid_until=Jan 9, 2027, 4:59:59
```

AM","subject=CN=<IP>, CN=<IP>, OU=HMC, O=ibm.com, L=Austin, ST=TX, C=US","subject_alternative_names=DNS: localhost.blr.stglabs.ibm.com, IP: <IP>",key_size=2048

4.3.13.3 Archive certificate

HMC provides an option for users to archive currently applied certificates. The process will move the currently applied certificate as archived. There can be only one archive certificate on HMC. Once the certificate is archived the user will have the option to boot HMC using a self-signed certificate. Use HMC command as below to delete and archive the current certificate and restart the HMC without asking for confirmation:

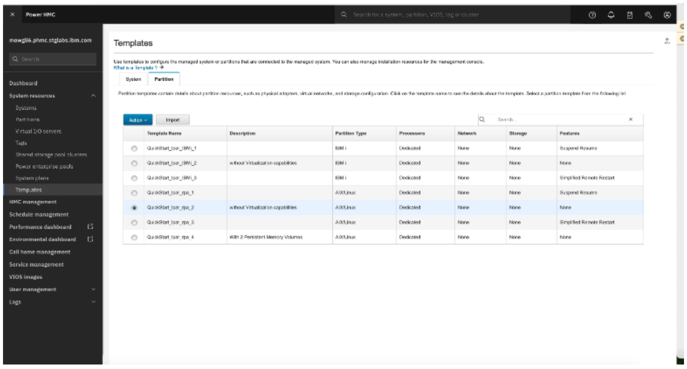
```
-> chhmccert -o archiverm -r
```

4.3.14 VM Configuration

This section has details on creating, configuring, and deleting Power VMs. AIX, Linux and IBM i are Power Architecture based Operating Systems designed to run for IBM Power servers. AIX, Linux and IBM i, are logical partitions (LPARs) that can be created and managed using the Hardware Management Console (HMC) on IBM Power Systems, enabling virtualization and resource sharing.

Refer to below screens to create VM using HMC GUI with "hmcsuperadmin" user login:

1. Select Templates Tab under System Resources. This will launch the Templates Panel and Select "**Partition**" Tab. Now "Select a Partition" of any type: **IBM i** or **AIX/Linux**



Templates

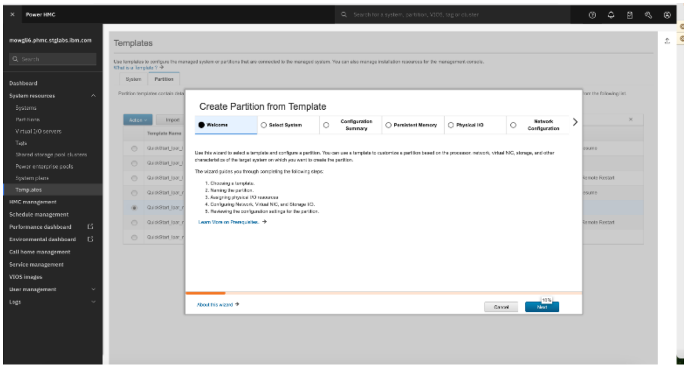
Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.
What is a Template ?

Partition templates contain details about partition resources, such as physical adapters, virtual networks, and storage configuration. Click on the template name to see the details about the template. Select a partition template from the following list.

	Template Name	Description	Partition Type	Processors	Network	Storage	Features
○	QuickStart_lpar_IBMi_1		IBM i	Dedicated	None	None	Suspend Resume
○	QuickStart_lpar_IBMi_2	without Virtualization capabilities	IBM i	Dedicated	None	None	None
○	QuickStart_lpar_IBMi_3		IBM i	Dedicated	None	None	Simplified Remote Restart
○	QuickStart_lpar_rpa_1		AIX/Linux	Dedicated	None	None	Suspend Resume
●	QuickStart_lpar_rpa_2	without Virtualization capabilities	AIX/Linux	Dedicated	None	None	None
○	QuickStart_lpar_rpa_3		AIX/Linux	Dedicated	None	None	Simplified Remote Restart
○	QuickStart_lpar_rpa_4	With 2 Persistent Memory Volumes	AIX/Linux	Dedicated	None	None	None

Figure 19

2. Select the **Action** button's drop down and Click on **Deploy** option. This will open the wizard to create a Partition / VM of that type. Click the Next button.



Create Partition from Template

Use this wizard to select a template and configure a partition. You can use a template to customize a partition based on the processor, network, virtual NIC, storage, and other characteristics of the target system on which you want to create the partition.

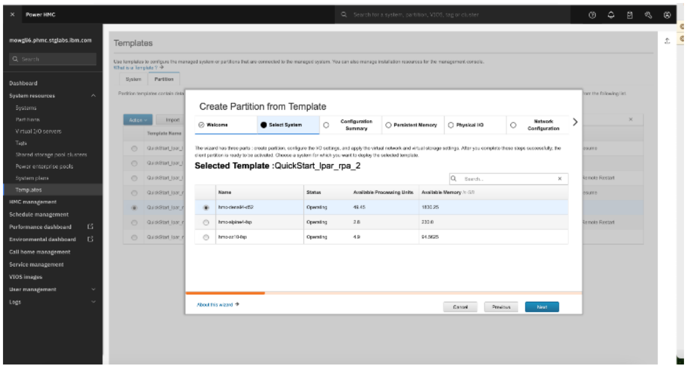
The wizard guides you through completing the following steps:

1. Choosing a template.
2. Naming the partition.
3. Assigning physical I/O resources
4. Configuring Network, Virtual NIC, and Storage I/O.
5. Reviewing the configuration settings for the partition.

Learn More on Prerequisites.

Figure 20

3. Select the System in which the VM / Partition needs to be created. Click Next button. For Persistent Memory tab also pass by clicking the Next button.



Create Partition from Template

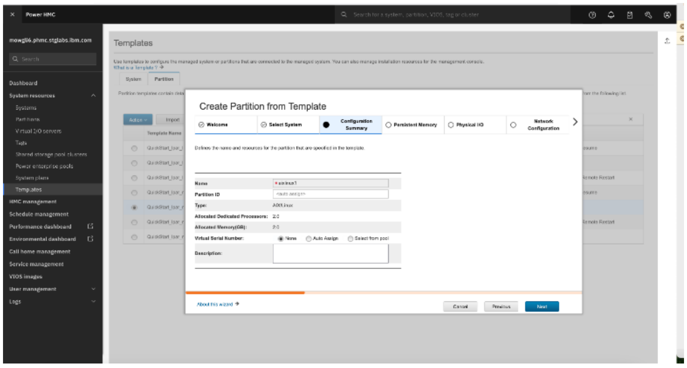
The wizard has three parts : create partition, configure the IO settings, and apply the virtual network and virtual storage settings. After you complete these steps successfully, the client partition is ready to be activated. Choose a system for which you want to deploy the selected template.

Selected Template : QuickStart_lpar_rpa_2

	Name	Status	Available Processing Units	Available Memory in GB
●	hmc-denali4-d52	Operating	49.45	1830.25
○	hmc-alpine4-fsp	Operating	2.8	232.0
○	hmc-zz10-fsp	Operating	4.9	94.5625

Figure 21

4. Configure the VM name, ID (if required). Click the Next button



Create Partition from Template

Defines the name and resources for the partition that are specified in the template.

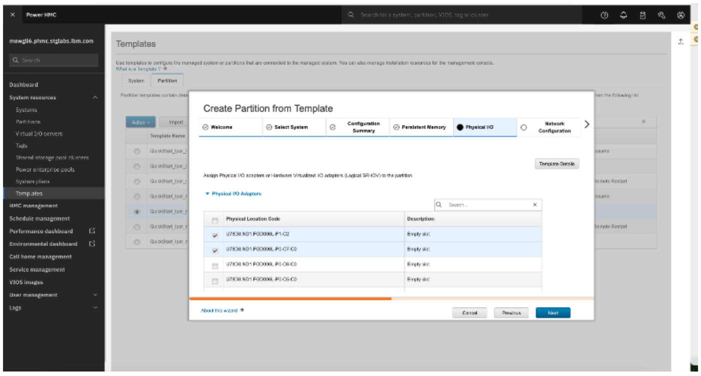
Name	* aixlinux1
Partition ID	<auto assign>
Type:	AIX/Linux
Allocated Dedicated Processors:	2.0
Allocated Memory(GB):	2.0
Virtual Serial Number:	● None ○ Auto Assign ○ Select from pool
Description:	

Figure 22

5. Select the Physical I/O adapters available in the selected System for the VM using the check box. For example, you may select slot number `P1-C0` to assign that slot to your partition.

   Access to certain adapters is denied, see below:
   a. PCIe4 4-port NVMe JBOF adapter (FC EJ1X and EJ1Y; CCIN 6B87)
   b. PCIe4 cable adapter (FC EJ24; CCIN 6B92)

   When complete, click the Next button.



Create Partition from Template

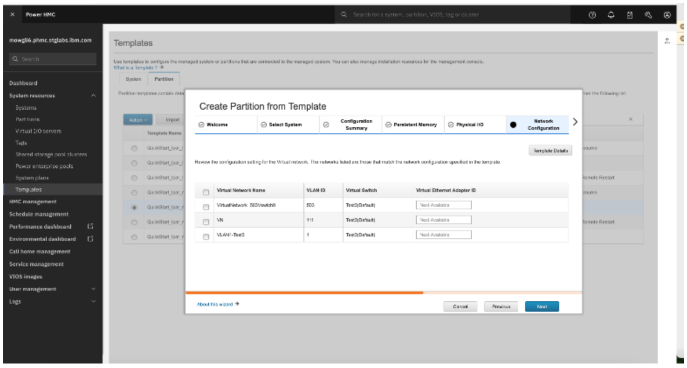
Assign Physical I/O adapters or Hardware Virtualized I/O adapters (Logical SR-IOV) to the partition.

Physical I/O Adapters

□	Physical Location Code	Description:
☑	U78D8.ND1.FGD006L-P1-C2	Empty slot
☑	U78D8.ND1.FGD006L-P0-C7-C0	Empty slot
□	U78D8.ND1.FGD006L-P0-C6-C0	Empty slot
□	U78D8.ND1.FGD006L-P0-C5-C0	Empty slot

Figure 23

6. Navigate to other Tabs like Network configuration and Virtual NIC Configuration by clicking the Next button.

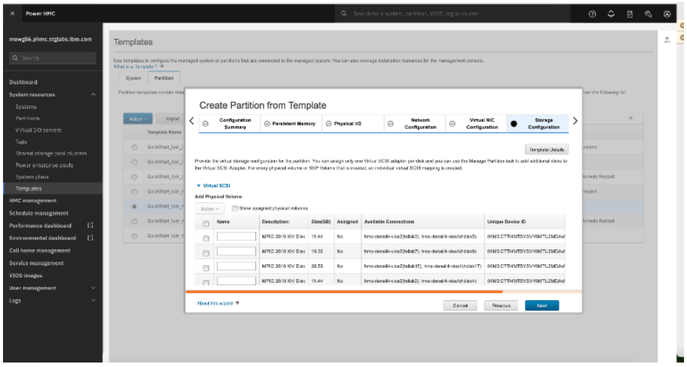


Review the configuration setting for the Virtual network. The networks listed are those that match the network configuration specified in the template.

□	Virtual Network Name	VLAN ID	Virtual Switch	Virtual Ethernet Adapter ID
□	VirtualNetwork_500/vswitch0	500	Test3(Default)	Next Available
□	VN	111	Test3(Default)	Next Available
□	VLAN1-Test3	1	Test3(Default)	Next Available

Figure 24

7. Select the Storage Configuration as applicable and Click the Next button.



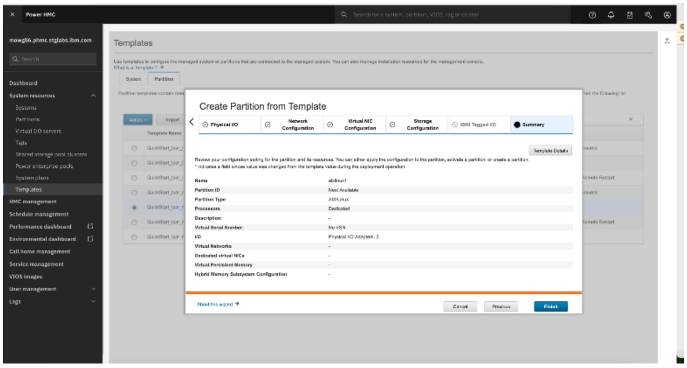
Provide the virtual storage configuration for the partition. You can assign only one Virtual SCSI adapter per disk and you can use the Manage Partition task to add additional disks to the Virtual SCSI Adapter. For every physical volume or SSP Volume that is created, an individual virtual SCSI mapping is created.

□ Show assigned physical volumes

□	Name	Description:	Size(GB)	Assigned	Available Connections	Unique Device ID
□		MPIO 2810 XIV Disk	11.44	No	hmc-denali4-vios2(hdisk3), hmc-denali4-vios1(hdisk5)	01M3CTTI4VTBYSVY0MTL2MDAx
□		MPIO 2810 XIV Disk	19.08	No	hmc-denali4-vios2(hdisk7), hmc-denali4-vios1(hdisk9)	01M3CTTI4VTBYSVY0MTL2MDAx
□		MPIO 2810 XIV Disk	28.59	No	hmc-denali4-vios2(hdisk15), hmc-denali4-vios1(hdisk17)	01M3CTTI4VTBYSVY0MTL2MDAx
□		MPIO 2810 XIV Disk	11.44	No	hmc-denali4-vios2(hdisk2), hmc-denali4-vios1(hdisk4)	01M3CTTI4VTBYSVY0MTL2MDAx

Figure 25

8. This tab shows the Summary of VM with configurations which is about to be created. Click the Finish button to create the VM.

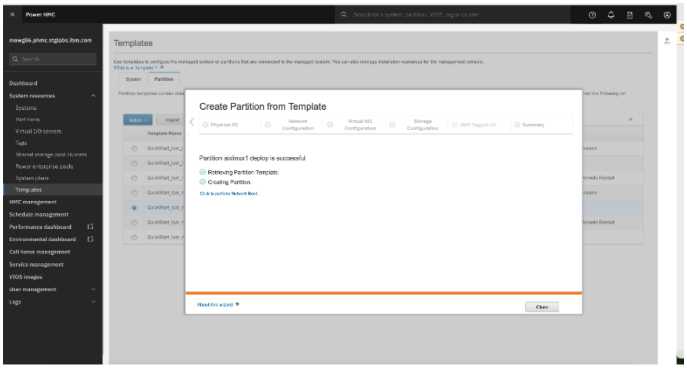


Review your configuration setting for the partition and its resources. You can either apply the configuration to the partition, activate a partition, or create a partition.
* Indicates a field whose value was changed from the template value during the deployment operation.

Name	abdlinux1
Partition ID	Next Available
Partition Type	AIX/Linux
Processors	Dedicated
Description:	-
Virtual Serial Number:	No VSN
I/O	Physical I/O Adapters: 2
Virtual Networks	-
Dedicated virtual NICs	-
Virtual Persistent Memory	-
Hybrid Memory Subsystem Configuration	-

Figure 26

9. All the selected configurations are applied, and the VM / Partition is created under the selected System. Click the Close button to close the tab.



Use templates to configure the managed system or partitions that are connected to the managed system. You can also manage installation resources for the management console.

Create Partition from Template

Partition aixlinux1 deploy is successful

- Retrieving Partition Template.
- Creating Partition.

Figure 27

Create VM using Command by "hmcsuperadmin" User:
In the following examples nested double quote characters are preceded by an escape character ('#146;). The escape characters are required to run commands locally on an HMC.

Create an AIX or Linux VM:

```
-> mksyscfg -r lpar -m system1 -i "name=aix_lpar2,profile_name=prof1,lpar_env=aixlinux,min_mem=256,desired_mem=1024,max_mem=1024,proc_mode=ded,min_procs=1,desired_procs=1,max_procs=2,sharing_mode=share_idle_procs,auto_start=1,boot_mode=norm,lpar_io_pool_ids=3,\"io_slots=21010003/3/1,21030003//0\",max_virtual_slots=20,\"virtual_fc_adapters=10/client/1//110//1,\"\"11/client/2//111/c0507609a405005a,c0507609a405005b/1\"\"\""
```

A "profile" refers to a configuration file that defines how a VM / logical partition (LPAR) or the managed system itself should be set up and activated, including resource allocation and startup attribute.
System Profile is an ordered list of partition profiles that the HMC uses to start logical partitions on a managed system in a specific configuration.
VM Profile is a record on the HMC that specifies a possible configuration for a logical partition, including the number of resources and startup attributes.

Create an IBM i VM profile:

```
->mksyscfg -r prof -m 9406-570*34134441 -i "name=prof2,lpar_id=3,min_mem=512,desired_mem=512,max_mem=1024,proc_mode=shared,min_procs=1,desired_procs=1,max_procs=2,min_proc_units=0.1,desired_proc_units=0.5,max_proc_units=1.5,sharing_mode=uncap,uncap_weight=128,auto_start=1,\"lpar_io_pool_ids=1,2\",\"io_slots=2101001B/1/1,2103001B/2/1,2105001B//0\",load_source_slot=2101001B,console_slot=hmc,max_virtual_slots=14,\"virtual_scsi_adapters=12/client/2//13/1,13/server////1\""
```

Create VM profiles using the configuration data in the file /tmp/profcfg:

```
->mksyscfg -r prof -m system1 -f /tmp/profcfg
```

Create a new VM profile by saving the current configuration of a partition:

```
->mksyscfg -r prof -m system1 -o save -p p1 -n newProfile
```

Create a system profile:

```
->mksyscfg -r sysprof -m system1 -i "name=sysprof1,\"lpar_names=lpar1,lpar2\",\"profile_names=prof1,prof1\""
```

Save the current configuration of a VM to an existing profile:

```
->mksyscfg -r prof -m system1 -o save -p aix1 -n activeProfile --force
```

Command to list the physical adapters:

```
->lshwres -m <system> -r io --rsubtype slot
->lshwres -m <system> -r io --rsubtype slot | grep lpar_id=none
```

```
hscroot@mowgli6:~> lshwres -m hmc-denali4-d52 -r io --rsubtype slot | grep lpar_id=none
unit_phys_loc=U78D8.ND0.FGD001L,bus_id=23,phys_loc=C7-
C0,drc_index=21010017,lpar_id=none,slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND0.FGD001L-P0-C7-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND0.FGD001L,bus_id=19,phys_loc=C3-
C0,drc_index=21010013,lpar_id=none,slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND0.FGD001L-P0-C3-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND0.FGD001L,bus_id=20,phys_loc=C4-
C0,drc_index=21010014,lpar_id=none,slot_io_pool_id=none,description=PCIe3 2 PORT 25/10 Gb
NIC&ROCE SFP28
ADAPTER,"feature_codes=58FB,EC2T,EC2U",pci_vendor_id=15B3,pci_device_id=1015,pci_subs_v
endor_id=1014,pci_subs_device_id=061E,pci_class=0200,pci_revision_id=00,bus_grouping=0,iop=
0,parent_slot_drc_index=none,drc_name=U78D8.ND0.FGD001L-P0-C4-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=0,dynamic_lpar_assignmen
t_capable=0
unit_phys_loc=U78D8.ND0.FGD001L,bus_id=26,phys_loc=C2,drc_index=2101001A,lpar_id=none,
slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND0.FGD001L-P1-
C2,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND0.FGD001L,bus_id=27,phys_loc=C3,drc_index=2101001B,lpar_id=none,
slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND0.FGD001L-P1-
C3,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND1.FGD006L,bus_id=38,phys_loc=C6-
C0,drc_index=21010026,lpar_id=none,slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND1.FGD006L-P0-C6-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND1.FGD006L,bus_id=39,phys_loc=C7-
C0,drc_index=21010027,lpar_id=none,slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND1.FGD006L-P0-C7-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND1.FGD006L,bus_id=34,phys_loc=C2-
C0,drc_index=21010022,lpar_id=none,slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
```

```
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND1.FGD006L-P0-C2-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND1.FGD006L,bus_id=37,phys_loc=C5-
C0,drc_index=21010025,lpar_id=none,slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND1.FGD006L-P0-C5-
C0,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
unit_phys_loc=U78D8.ND1.FGD006L,bus_id=42,phys_loc=C2,drc_index=2101002A,lpar_id=none,
slot_io_pool_id=none,description=Empty
slot,feature_codes=0,pci_vendor_id=FFFF,pci_device_id=FFFF,pci_subs_vendor_id=FFFF,pci_subs_
device_id=FFFF,pci_class=FFFF,pci_revision_id=FF,bus_grouping=0,iop=0,parent_slot_drc_index=
none,drc_name=U78D8.ND1.FGD006L-P1-
C2,interposer_present=0,interposer_pcie=0,lpar_assignment_capable=1,dynamic_lpar_assignmen
t_capable=1
hscroot@mowgli6:~>
```

Configure VM Command using "hmcsuperadmin" user:

Using profile**:**

```
-> chsyscfg -r lpar -m system1 -o apply -p p1 -n prof1
```

Modifying Profile:

```
-> chsyscfg -r prof -m sys1 -i "name=profile1,lpar_name=partition3,min_mem-
=256,desired_mem-=256,max_mem-=256,desired_procs=2"
```

Example command:

```
-> chsyscfg -r lpar -m hmc-denali4-d52 -o apply -p aix_test -n prof1
hscroot@mowgli6:~>
```

More Example command:

Change the managed system's user-defined name and power off policy:

```
-> chsyscfg -r sys -m 9406-570*89320051 -i "new_name=sys1, power_off_policy=1"
```

Change VM using the configuration data in the file /tmp/lparfile:

```
-> chsyscfg -r lpar -m sys1 -f /tmp/lparfile
```

Change the attributes of a shutdown VM by applying the profile prof1:

```
-> chsyscfg -r lpar -m system1 -o apply -p p1 -n prof1
```

Change a VM profile's memory amounts (reduce the profile's current memory amounts each by 256 MB), and number of desired processors:

```
-> chsyscfg -r prof -m sys1 -i "name=profile1, lpar_name=partition3,min_mem-
=256,desired_mem-=256,max_mem-=256,desired_procs=2"
```

Add 2 virtual fibre channel adapters with user-specified WWPNs to a VM profile:

```
-> chsyscfg -r prof -m mySys -i
"name=p1,lpar_name=lpar3,\"virtual_fc_adapters+=\"\"5/client//vios1/15/c0508301e9ac0008,
c0508301e9ac0009/1\"\",\"\"6/client//vios2/6/c0508301e9ac00a0,c0508301e9ac00a1/1\"\"
\""
```

Add a virtual NIC to a VM profile:

```
-> chsyscfg -r prof -m P9-1 -i
```

```
"name=prof1,lpar_id=1,\"vnic_adapters+=\"\"slot_num=11:backing_devices=sriov//1/3/2/10/1
/30,sriov//2/2/1/10/2/30\"\"\""
```

Change a system profile (add 2 new VM profiles):

```
-> chsyscfg -r sysprof -m sys1 -i
"name=sysprof1,\"lpar_names+=partition3,partition4\",\"profile_names+=3_prof1,4_defaultProf
\""
```

Create 2 VM's and configure same IO Adapter "U78D8.ND1.FGD006L" with DRC index "2101002B" to both VM and activate:

```
-> mksyscfg -m hmc-denali4-d52 -r lpar -i
"name=aix_test,profile_name=prof1,lpar_env=aixlinux,min_mem=256,desired_mem=1024,max_
mem=1024,proc_mode=ded,min_procs=1,desired_procs=1,max_procs=2,sharing_mode=share_idl
e_procs,auto_start=1,boot_mode=norm,lpar_io_pool_ids=3,io_slots=\"2101002B//0\""
```

```
-> mksyscfg -m hmc-denali4-d52 -r lpar -i
"name=aix_test2,profile_name=prof1,lpar_env=aixlinux,min_mem=256,desired_mem=1024,max_
mem=1024,proc_mode=ded,min_procs=1,desired_procs=1,max_procs=2,sharing_mode=share_idl
e_procs,auto_start=1,boot_mode=norm,lpar_io_pool_ids=3,io_slots=\"2101002B//1\""
```

Activating the VMs using HMC commands:

```
-> chsysstate -o on -r lpar -n aix_test -m hmc-denali4-d52 -f prof1
```

Delete VM Command using "hmcsuperadmin" user:

Option#1: Using VM name:

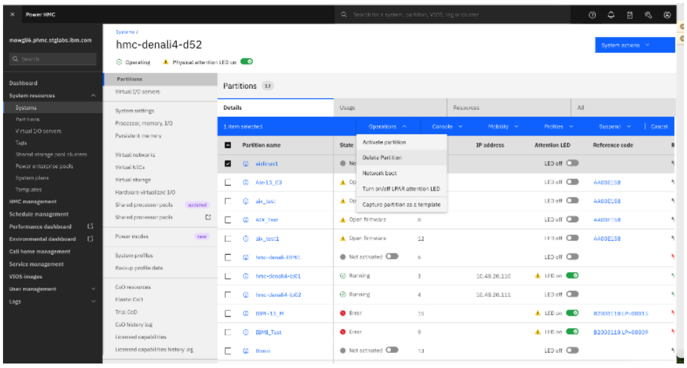
```
-> rmsyscfg -r lpar -m <systemName> -n <VMname>
```

Option#2: Using VM ID:

```
-> rmsyscfg -r lpar -m <systemName> --id <VM ID>
```

Delete VM from GUI with "hmcsuperadmin" user login:

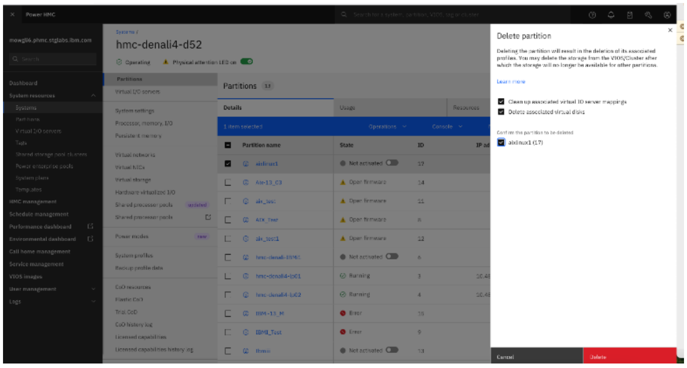
1. Select the Partition under the System its created. Click on the Operations drop down option and select " Delete Partition". This will launch the confirmation tab to the right



Partition name	State		IP address	Attention LED	Reference code
☑ aixlinux1	● No			LED off	
□ Aix-13_C3	Op			LED off	AA00E158
□ aix_test	Op			LED off	AA00E158
□ AIX_Test	Open firmware	8		LED off	AA00E158
□ aix_test1	Open firmware	12		LED off	AA00E158
□ hmc-denali-IBMi1	● Not activated	6		LED off	
□ hmc-denali4-lp01	Running	3	10.48.20.110	LED on	
□ hmc-denali4-lp02	Running	4	10.48.20.111	LED off	
□ IBM-13_M	Error	15		LED on	B2003110 LP=00015
□ IBMi_Test	Error	9		LED on	B2003110 LP=00009
□ Ibmiii	● Not activated	13		LED off	

Figure 28

2. In the Delete Partition / VM Confirmation tab select the VM name tab check box and click on Delete button



Delete partition

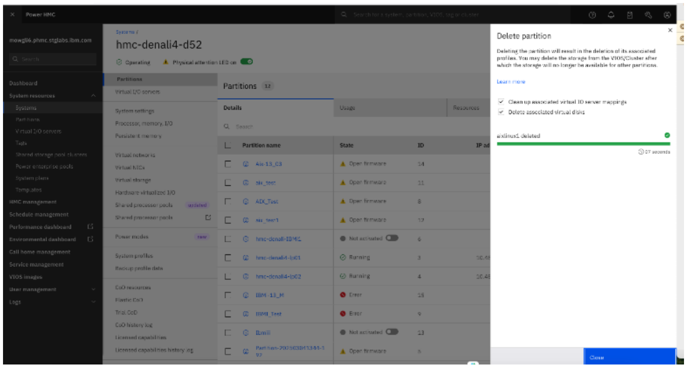
Deleting the partition will result in the deletion of its associated profiles. You may delete the storage from the VIOS/Cluster after which the storage will no longer be available for other partitions.

☑ Clean up associated virtual IO server mappings
☑ Delete associated virtual disks

Confirm the partition to be deleted
☑ aixlinux1 (17)

Figure 29

3. This will Delete the selected VM. Click on Close button to come out of this page.



Delete partition

Deleting the partition will result in the deletion of its associated profiles. You may delete the storage from the VIOS/Cluster after which the storage will no longer be available for other partitions.

☑ Clean up associated virtual IO server mappings
☑ Delete associated virtual disks

aixlinux1 deleted

07 seconds

More Example command:
Remove the VM aix1 and all of its associated virtual I/O server adapters and mappings from the associated Virtual I/O Servers, and delete the VM virtual disks:
-> rmsyscfg -r lpar -m system1 -n aix1 --vioscfg --vdisk -v

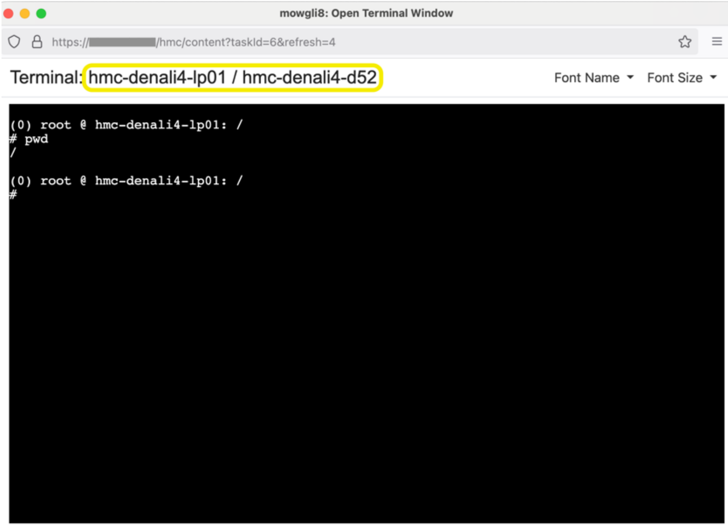
Remove the VM profile prof1 for VM lpar3:
-> rmsyscfg -r prof -m system1 -n prof1 -p lpar3

Remove the system profile sysprof1:
-> rmsyscfg -r sysprof -m 9406-520*34134441 -n sysprof1

Note: VM, Partition and LPAR refers to Power platform's Guest VM.

4.3.15 Guest VM Name Focus

This section contains details on getting Guest VM's name focus. Users can see the Guest VM name focused on top left of the Console Terminal along the System name.



https://[redacted]/hmc/content?taskId=6&refresh=4

Terminal: hmc-denali4-lp01 / hmc-denali4-d52

```
(0) root @ hmc-denali4-lp01: /
# pwd
/

(0) root @ hmc-denali4-lp01: /
#
```

Figure 30

4.3.16 XNTP service Enablement on HMC

This section describes the steps to enable XNTP service on HMC.

To Enable Network time Protocol use below HMC command:
-> chhmc -c xntp -s enable

To add a Network Time Protocol (NTP) server to your configuration file, you'll typically modify the ntp.conf file. This file contains the configuration settings for the NTP daemon, which is responsible for synchronizing your system's clock with a remote time source. **To add a Network Time Protocol server to the configuration file use below HMC command from remote terminal:**
-> chhmc -c xntp -s add -h mytimeserver.company.com

To add a Network Time Protocol server to the configuration file, using IP address and at the same time enable firewall access through network interface eth0:
-> chhmc -c xntp -s add -a 10.10.10.32 -i eth0

To remove a Network Time Protocol server from the configuration file:
-> chhmc -c xntp -s remove -h mytimeserver.company.com

4.3.17 Configure Removable Media for HMC

This section describes the steps to configure removable media on HMC from CLI. To list all the storage media devices that are available for use on the HMC use the command below from remote terminal using “hmcsuperadmin” user:
-> lsmediadev

Sample Output:
device=/dev/sda,type=6,description=disk drive

```
device=/dev/sdb1,mount_point=/media/sdb1,type=3,description=USB
device,label=WPUL,product=USB 2.0 FD,vendor=PNY
device=/dev/sdc1,mount_point=/media/sdc1,type=3,description=USB
device,label=STORE,product=STORE N GO,vendor=Verbatim
```

Format media command formats a USB device on the Hardware Management Console (HMC). The USB device can be formatted with the EXT4 or VFAT file system, which are the only file systems supported by USB devices used on the HMC. Once the operation is successful a return value of 0 will be returned.

Format a USB device with the VFAT file system:

```
-> formatmedia -r usb -d /dev/sdb1 -l BACKUP
```

Format a USB device with the EXT4 file system:

```
-> formatmedia -r usb -d /dev/sdb1 -t ext4 -l BACKUP
```

Format of media is only allowed to be executed by HMC Superadmin users. Below examples shows that “hmcsuperadmin” user can format.

User with Task Role- hmcsuperadmin will be able to execute format media command:

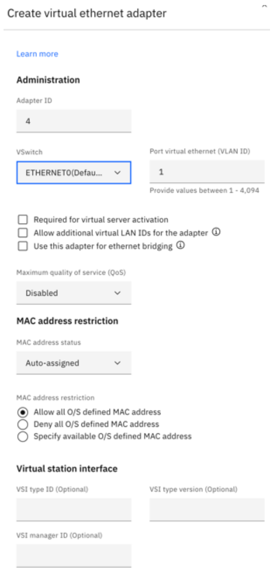
```
-> lsmediadev
device=/dev/sda,type=6,description=disk drive
device=/dev/sdb1,mount_point=/media/sdb1,type=3,description=USB
device,label=WPUL,product=USB 2.0 FD,vendor=PNY
device=/dev/sdc1,mount_point=/media/sdc1,type=3,description=USB
device,label=STORE,product=STORE N GO,vendor=Verbatim

->  formatmedia -r usb -d /dev/sdc1 -t ext4 -l STORE
```

4.3.18 Configure/De-configure Network for VM

This section explains the steps to configure network by “hmcsuperadmin” user using HMC GUI from remote web browser.

Physical Network Configuration:
To add a VM to a Physical Network follow below steps from GUI:
Navigate to the HMC GUI -> **Systems** -> (Select the system) -> **Partitions** -> (Select the check box next to the partition) -> **Profiles** -> **Manage Profiles** -> (Select the profile you would like to modify) -> **Virtual Adapters** -> **Create** -> **Create Ethernet Adapter** -> (Set settings similarly to the image below) -> **Save**



Create virtual ethernet adapter

Learn more

Administration

Adapter ID: 4

VSwitch: ETHERNET0(Defau...

Port virtual ethernet (VLAN ID): 1

Provide values between 1 - 4,094

□ Required for virtual server activation
□ Allow additional virtual LAN IDs for the adapter
□ Use this adapter for ethernet bridging

Maximum quality of service (QoS): Disabled

MAC address restriction

MAC address status: Auto-assigned

MAC address restriction

● Allow all O/S defined MAC address
○ Deny all O/S defined MAC address
○ Specify available O/S defined MAC address

Virtual station interface

VSI type ID (Optional)

VSI type version (Optional)

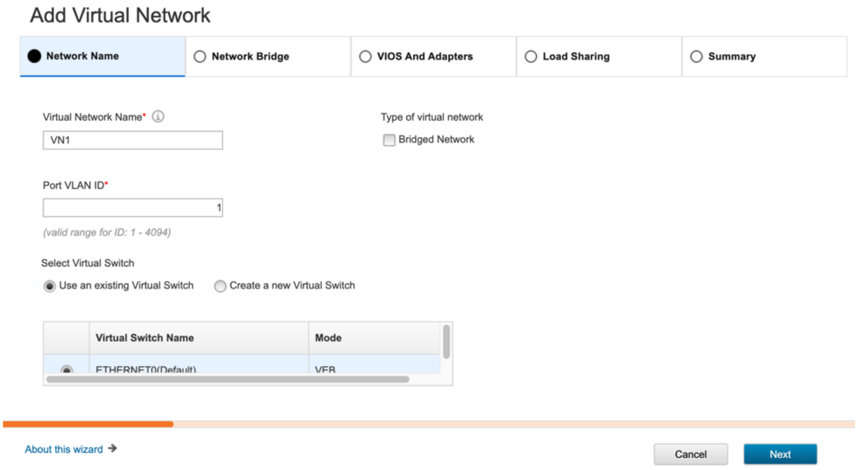
VSI manager ID (Optional)

Figure 31

Virtual Network Configuration:
A PowerVM virtual network allows connectivity between partitions on a server or, if bridged, across servers. You can create multiple virtual networks on a managed system and then connect partitions to those networks.

Via the HMC GUI, go to Systems -> (Select the system) -> Virtual Networks -> Add Virtual Network.

Set the Virtual Network Name, Port VLAN ID, select "Use an existing Virtual Switch", and verify "Bridged Network" is un-selected as shown below:



Add Virtual Network

● Network Name ○ Network Bridge ○ VIOS And Adapters ○ Load Sharing ○ Summary

Virtual Network Name*: VN1

Type of virtual network

□ Bridged Network

Port VLAN ID*: 1

(valid range for ID: 1 - 4094)

Select Virtual Switch

● Use an existing Virtual Switch ○ Create a new Virtual Switch

	Virtual Switch Name	Mode
●	ETHERNET0(Default)	VEB

Figure 32

After clicking "Next", you will be prompted to add the configuration.

To add a VM to a Virtual Network:
Navigate to the HMC GUI -> **Systems** -> (Select the system) -> **Partitions** -> (Select the partition) -> **Virtual Networks** -> **Attach Virtual Network** -> Select the Virtual Network name and click **OK**

Perform the above actions for any partition in which inter-VM communication is requested.

To remove a VM from a Virtual Network, and thus removing inter-VM communication:
HMC GUI, go to Systems -> (Select the system) -> Partitions -> (Select the partition) -> Virtual Networks -> (Select the Virtual Network name) -> Action -> Detach

4.3.19 Configure Physical Devices for VM

This section explains the steps to configure physical devices by "hmcsuperadmin" users using HMC GUI from remote web browser. This configuration ensures that physical device access is restricted to designated devices while restricting access to other VMs.

Using the HMC GUI, navigate to:
Systems -> (Select the system) -> (Check the box next to the partition to modify) -> **Profiles** -> **Manage Profiles** -> (Select the profile to modify) -> **Physical I/O** -> (Check the box next to the Location Code) -> Set "Added as" to "Required" -> Click **Add**.

When booting the partition, apply the modified profile. Setting the Location Code to "Required" ensures that no other partition with the same Location Code, marked as "Required," can boot.

4.3.20 Clearing logical volumes

This section explains how to clear all data within a logical volume. This is accomplished by utilizing the VIOS.

Add Physical Adapter via HMC

1. Navigate to **Virtual I/O Servers → VIOS225 → Physical I/O Adapter**
2. Click **Add Adapter**
3. Select the adapter
4. Click **Add Adapter** again, then **Save**

SSH to the VIOS partition
-> ssh padmin@viosip

Clear the Storage Device
To zero out a 1.53TB disk (1M × 1,526,185 blocks):
-> dd if=/dev/zero of=/dev/rhdiskx bs=1M count=1526185

4.3.21 Audit Function

This section provides details about various audit files on HMC and steps to offload log files to SFTP server. All the Audit logs to be exported to SFTP server manually. These audit files can then be imported back on HMC from the SFTP server. The audit log is a single file zip file and it's overwritten when regenerated. HMC logs have policies to rotate them and there will not be a situation where HMC is out of memory due to too many log files.

SFTP server Setup and Configuration:
A Linux system can be configured to act as a SFTP server as the SFTP functionality is built in within the standard SSH daemon which is readily available on most Linux distributions. There is no explicit setup and configuration needed on HMC to communicate to SFTP server.

Option#1: Importing and exporting audit log files using password

Command to export the Audit logs from HMC to SFTP Server using Password:

```
-> cpfile -t vpp -l r -f <file-name_withPath> -o export -h host-name -u user-ID [--passwd
    password]
```

Command to import the Audit logs from SFTP Server to HMC using Password:

```
-> cpfile -t vpp -l r -f <file-name_withPath> -o import -h host-name -u user-ID [--passwd
    password]
```

Option#2: Importing and exporting audit log files using public key
Command to export the Audit logs from HMC to SFTP Server using Public Key:

```
-> cpfile -t vpp -l r -f <file-name_withPath> -o export -h host-name -u user-ID -k [public key path]
```

Command to import the Audit logs from SFTP Server to HMC using Public Key:

```
-> cpfile -t vpp -l r -f <file-name_withPath> -o import -h host-name -u user-ID -k [public key path]
```

Example commands:

Option#1: Importing and exporting audit log files using password

Command to export the Audit logs from HMC to SFTP Server using Password:

```
-> cpfile -t vpp -l r -f /home/admin1/audit_4Mar2025_10AM.zip -o export -h 10.48.20.61 -u
admin1 --passwd admin
```

Command to import the Audit logs from SFTP Server to HMC using Password:

```
-> cpfile -t vpp -l r -f /home/admin1/audit_4Mar2025_10AM.zip -o import -h 10.48.20.61 -u
admin1 --passwd admin
```

Option#2: Importing and exporting audit log files using public key

Pre Requisite Step on HMC – To Enable Key Based Authentication
Generate pair of public and private keys on HMC:

```
-> ssh-keygen  -t rsa -f /home/<userhome>/id_rsa
```

Example: ssh-keygen -t rsa -f /home/hmcsuperadmin/id_rsa

List the public key and copy contents

```
-> cat /home/hmcsuperadmin/id_rsa.pud
```

Delete the public key when not needed:

```
-> chhmc -c sshuserkey -s remove -f /home/<userhome>/id_rsa
```

On Destination SFTP server system
Add the copied public key to authorised keys file by running below command:

```
-> ssh destmachineuser@destinationmachineip
-> vi ~/.ssh/authorized_keys
```

Add the copied public key to the above file and exit

Command to export the Audit logs from HMC to SFTP Server using Public Key:

```
-> cpfile -t vpp -l r -f /home/admin1/audit_4Mar2025_10AM.zip -o export -h 10.48.20.61 -u
admin1 -k /home/hmcsuperadmin/id_rsa
```

Command to import the Audit logs from SFTP Server to HMC using Public Key:
Follow Pre Requisite Step as above and then run below command on HMC.

```
-> cpfile -t vpp -l r -f /home/admin1/audit_4Mar2025_10AM.zip -o import -h 10.48.20.61 -u
admin1 -k /home/hmcsuperadmin/id_rsa
```

Sample Audit log files:

FFDC.log	Audit.log
GUIAudit.log	access_log
GUIFFDC.log	Security.log

GUISecurity.log	rmc_trace.*
HMC_events.html	ssl_error_log
iqyylog.log	ssl_request_log
secure	iqzdtrac.trm
ssl_access_log	messages
phyp	cimserver.log
VIOSCommunication.log	error_log

Note:

30. The file will be overwritten if the same name is used on remote SFTP server (Linux based).
31. When importing audit file to HMC from SFTP server, a directory gets created with the file name along with the time stamp.
32. As a best practice it is recommended to have a file name to include date time format for better tracking.
33. HMC and the SFTP server should be in the same network so that they are reachable to each other.

4.4 System firmware installation

The evaluated firmware level on Power10 is 01ML1060_064_053. This version has a sha256sum of *826871c1446a625f0e6dff6278892cebb34f5151645e403d959b05f98f7e1138*.

The certificate used to validate incoming firmware images are embedded into the system during the IBM manufacturing process and are not externally accessible. Digital signature verification is performed using the SHA-256 hashing algorithm to ensure the integrity and authenticity of the firmware image during installation; however, a manual check can be performed following these steps:

1. Upload the image to the HMC.
2. From the directory containing the image, run the following command:
   sha256sum <image>
3. Compare the resulting hash with the expected value to ensure integrity.

To verify the level of firmware on your system, follow these instructions:

1. From the HMC, In the navigation area, click the Resources icon, and then select All Servers.
2. Select the server for which you want to view system information.
3. In the menu pod, expand Actions and then expand Updates.
4. Select View system information
5. In the Specify LIC Repository window, select None – Display current values and click ok.

If the firmware level does not match the evaluated firmware level, you must install the evaluated firmware on your machine. The firmware is available for download from IBM fix central https://www.ibm.com/support/fixcentral/ . Enter your product, specify the base firmware release, ML1060 and specify the specific certified firmware level.

If you need to install the evaluated firmware on your machine, follow these instructions:

1. From the HMC, In the navigation area, click the Resources icon, and then select All Servers.
2. Select the server for which you want to update system information and click Actions > Updates.

3. Choose your source file location
4. Select Change Licensed Internal Code > for the Current Release or to a new Release based on the currently installed release.
5. Select an action from the list and click Ok.
6. When you complete this task, click Close.

Alternatively, the system firmware instillation can be performed via the BMC. If that is the approach desired, follow the steps below:

1. Verify the system is powered down
2. Click Operations > Firmware
3. Upload the .tar file downloaded from fix central
4. Click Start Update

4.5 VIOS installation

The VIOS level that will be used for the evaluation is VIOS 4.1. The flash image name is: Virtual_IO_Server_Base_Install_4.1.1.0_DVD_122024_122024_LCD8298701.iso with a sha256sum f85b70ea32c510e2dbcf6e4f2064a9aa7b34223e6ab5b497c726343802cdba97.

A manual check can be performed following these steps:

1. Upload the image to the HMC.
2. From the directory containing the image, run the following command: sha256sum <image>
3. Compare the resulting hash with the expected value to ensure integrity.

To verify the level of VIOS firmware on your system, follow these instructions:

6. From the HMC, In the navigation area, click the Resources icon, and then select All Servers.
7. Select the server for which you want to view system information.
8. In the system menu, select Virtual IO Server
9. Select the VIOS partition
10. Under VIOS Properties, the version is displayed

If the version does not match the evaluated firmware level, follow the steps below. This VIOS level is ordered and entitled with the purchase of a Power Server. The detailed steps to download the above image are given below:

1) Go to the Entitled Systems Support (ESS) www.ibm.com/servers/eserver/ess/ (see figure 1 in appendix)
2) If you have never been on the site before you must "attach" yourself to your IBM Customer Number.
    a) Click on "**My profile**".
    b) Click on "**Register customer number**".
    c) You may enter the country code/customer number combination or the HW/SW serial number of an IBM product purchased using that customer number. If you are the first to register for the customer, you will become the "primary" contact for that customer number and have to approve future requests to attach Web IDs to that customer number. If you are not the first, your request to attach the customer number will be sent to the current primary contact for that customer number. You can go no further until your IBM Web ID is associated with one or more customer numbers.
3) Select "**My entitled software**" for the initial ESS webpage

4) Enter OS category AIX, IBM i or Linux and specify OS level (see figure 2 in appendix)
5) Roll through the various software offerings and select 5765-VE4 PowerVM V4 (see figure 3 in appendix)
6) Select package 2282: IBM PowerVM V4 / VIOS 2282 v04.01.01,ENU,DVD (see figure 4 in appendix)
7) Agree to the terms and conditions for the software download (see figure 5 in appendix)
8) Select HTPS for download method (see figure 6 in appendix)
9) Select file Virtual_IO_Server_Base_Install_4.1.1.0_DVD_122024_122024_LCD8298701.iso (see figure 7 in appendix)
10) After uploading the above file to the HMC, follow the procedure outlined in the link below
    a) https://www.ibm.com/docs/en/power10?topic=mvis-activating-virtual-io-servers

4.5.1 Installation of iFixes within VIOS

AIX ifixes are digitally signed by IBM. The digital signatures are generated during the ifix creation process at IBM using an IBM private key specifically created for signing. The public key is provided with the evaluated configuration. This allows for verification of the signature of the ifix prior to installation.

First download the suma/emgr ifix from the link below. This ifix must be installed before the other ones.

https://aix.software.ibm.com/aix/efixes/Common_Criteria_Ifixes_AIX_73_TL3/SUMA_IFIX_CC.tar

-> *emgr_download_ifix -L <https_link> -P /tmp/*

The above command downloads the ifix and its signature in /tmp dir.

Untar the tar file and install the ifix.

-> */usr/sbin/emgr_sec <ifix_name.Z>*

The above command verifies the signature of ifix and installs the ifix.

On top of suma/emgr ifix, the following ifixes must be installed in the evaluated configuration:

https://aix.software.ibm.com/aix/efixes/security/openssl_fix44.tar

https://aix.software.ibm.com/aix/efixes/security/python_fix14.tar

https://aix.software.ibm.com/aix/efixes/security/openssh_fix18.tar

https://aix.software.ibm.com/aix/efixes/security/nim_fix.tar

https://aix.software.ibm.com/aix/efixes/security/libxml2_fix7.tar

https://aix.software.ibm.com/aix/efixes/Common_Criteria_Ifixes_AIX_73_TL3/dbg_ccssha.250326.epkg.Z

https://aix.software.ibm.com/aix/efixes/Common_Criteria_Ifixes_AIX_73_TL3/tmux35as0a.250318.epkg.Z

4.6 Partition the Server:

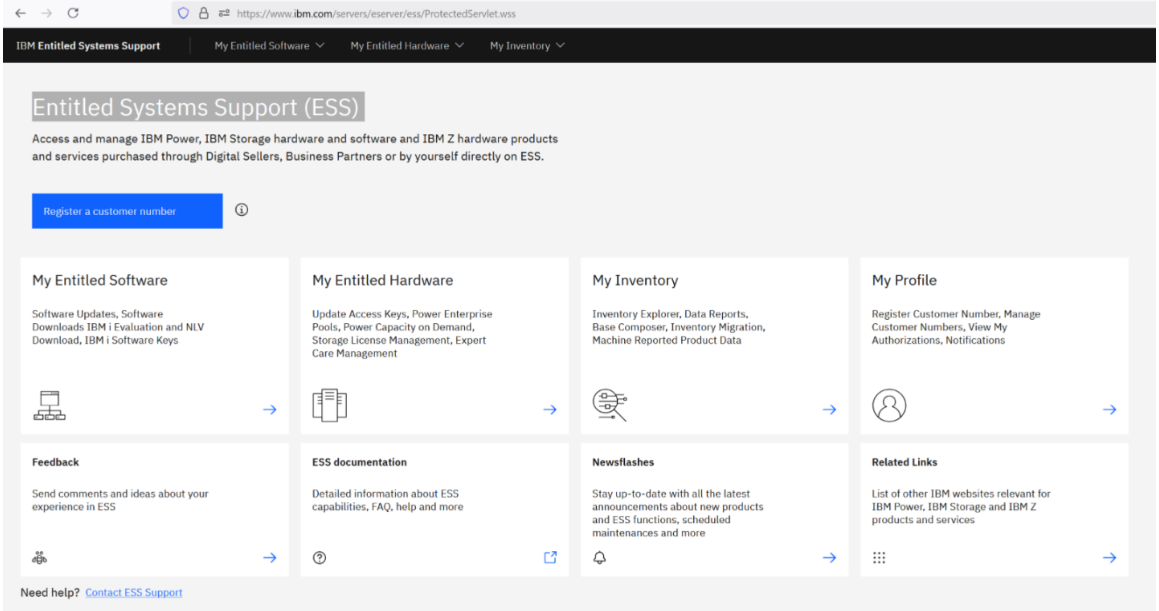
Additional information about how to setup, manage and monitor the virtualization environment can be found in the following documents:

- Setting up the virtualization environment
- Managing the virtualization environment
- Monitoring the virtualization environment

There are no special instructions for partitioning the server.

NOTE: The selection and installation of the individual operating systems for the partitions is outside the scope of this evaluation. The evaluated hardware and firmware are indifferent to the OS of the partition.

5 APPENDIX


https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss
IBM Entitled Systems Support
My Entitled Software
My Entitled Hardware
My Inventory
Register a customer number

Entitled Systems Support (ESS)

Access and manage IBM Power, IBM Storage hardware and software and IBM Z hardware products and services purchased through Digital Sellers, Business Partners or by yourself directly on ESS.

My Entitled Software

Software Updates, Software Downloads IBM i Evaluation and NLV Download, IBM i Software Keys

My Entitled Hardware

Update Access Keys, Power Enterprise Pools, Power Capacity on Demand, Storage License Management, Expert Care Management

My Inventory

Inventory Explorer, Data Reports, Base Composer, Inventory Migration, Machine Reported Product Data

My Profile

Register Customer Number, Manage Customer Numbers, View My Authorizations, Notifications

Feedback

Send comments and ideas about your experience in ESS

ESS documentation

Detailed information about ESS capabilities, FAQ, help and more

Newsflashes

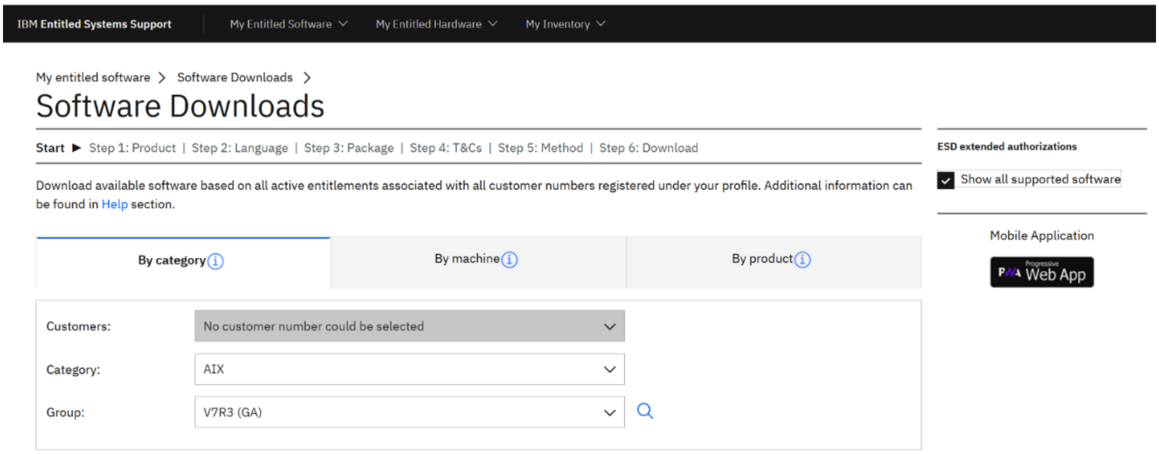
Stay up-to-date with all the latest announcements about new products and ESS functions, scheduled maintenances and more

Related Links

List of other IBM websites relevant for IBM Power, IBM Storage and IBM Z products and services

Need help? Contact ESS Support

Figure 1: IBM Entitled Systems Support (ESS)



Software Downloads

Start ▶ Step 1: Product | Step 2: Language | Step 3: Package | Step 4: T&Cs | Step 5: Method | Step 6: Download

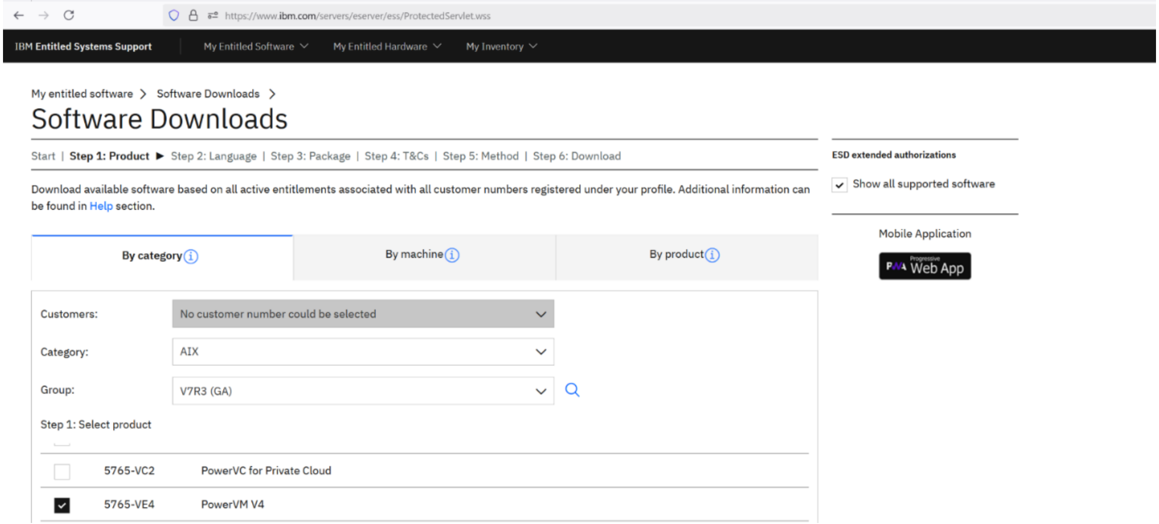
ESD extended authorizations

☑ Show all supported software

Download available software based on all active entitlements associated with all customer numbers registered under your profile. Additional information can be found in Help section.

Customers:	No customer number could be selected
Category:	AIX
Group:	V7R3 (GA)

Figure 2: Software Downloads



https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss

My entitled software > Software Downloads >

Software Downloads

Start | **Step 1: Product** ▶ Step 2: Language | Step 3: Package | Step 4: T&Cs | Step 5: Method | Step 6: Download

Download available software based on all active entitlements associated with all customer numbers registered under your profile. Additional information can be found in Help section.

Customers: No customer number could be selected

Category: AIX

Group: V7R3 (GA)

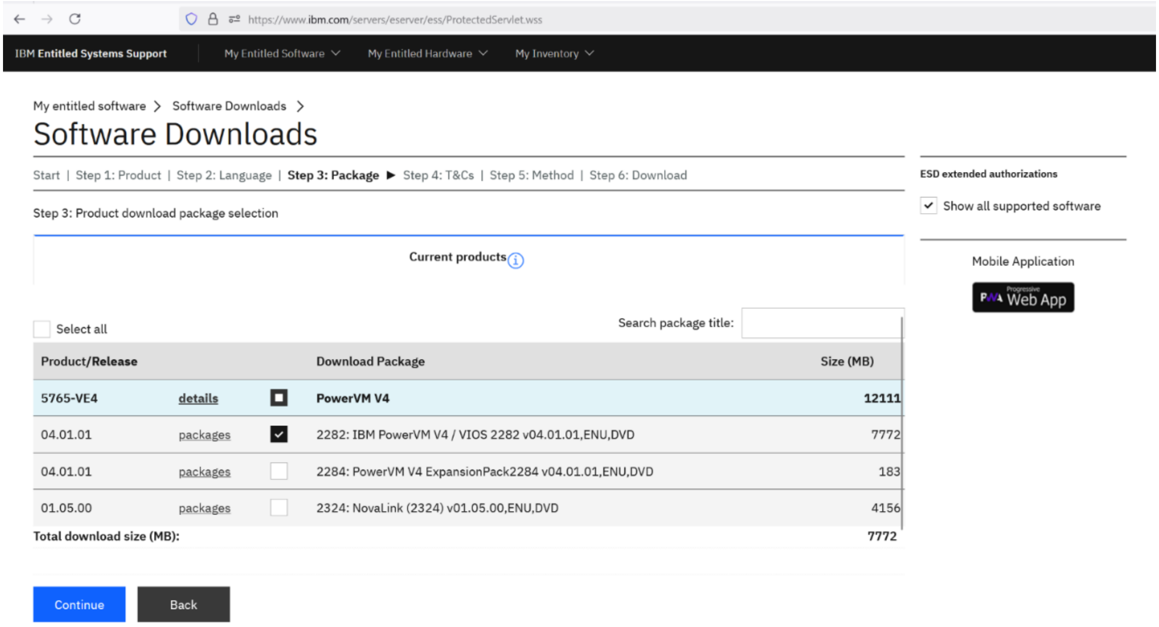
Step 1: Select product

□	5765-VC2	PowerVC for Private Cloud
☑	5765-VE4	PowerVM V4

ESD extended authorizations

☑ Show all supported software

Figure 3: Software Download - VIOS selection(Product)



https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss

My entitled software > Software Downloads >

Software Downloads

Start | Step 1: Product | Step 2: Language | **Step 3: Package** ▶ Step 4: T&Cs | Step 5: Method | Step 6: Download

Step 3: Product download package selection

□ Select all

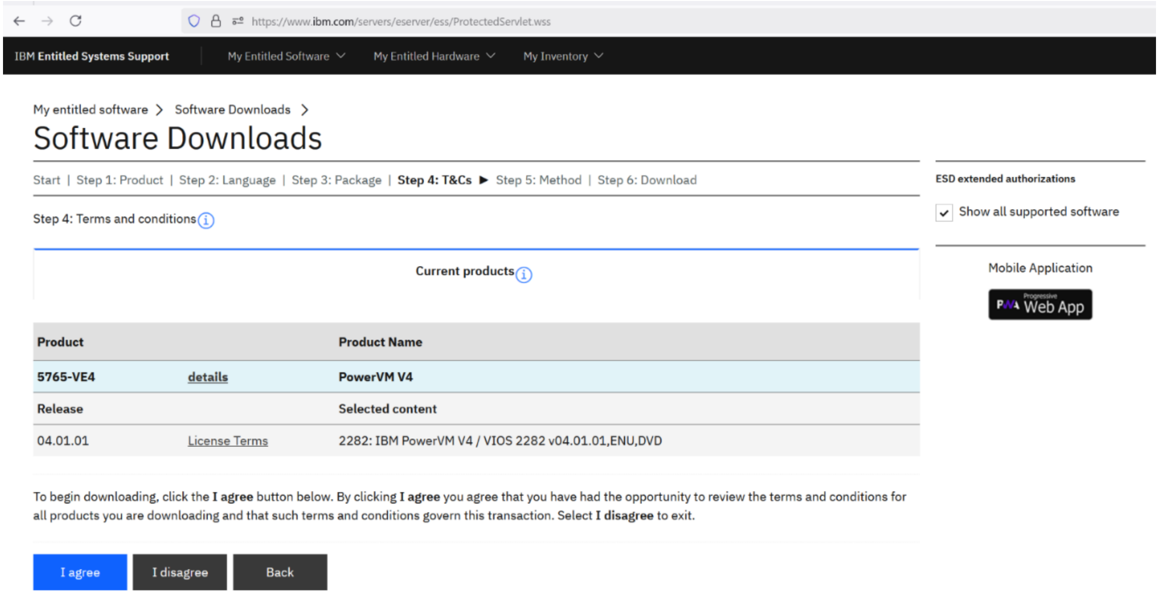
Search package title:

Product/Release			Download Package	Size (MB)
5765-VE4	details	■	**PowerVM V4**	12111
04.01.01	packages	☑	2282: IBM PowerVM V4 / VIOS 2282 v04.01.01,ENU,DVD	7772
04.01.01	packages	□	2284: PowerVM V4 ExpansionPack2284 v04.01.01,ENU,DVD	183
01.05.00	packages	□	2324: NovaLink (2324) v01.05.00,ENU,DVD	4156
Total download size (MB):				7772

ESD extended authorizations

☑ Show all supported software

Figure 4: Software Download - VIOS selection(Package)


https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss
IBM Entitled Systems Support
My Entitled Software
My Entitled Hardware
My Inventory
My entitled software > Software Downloads >
ESD extended authorizations
Mobile Application
Web App
I agree
I disagree
Back

Software Downloads

Start | Step 1: Product | Step 2: Language | Step 3: Package | **Step 4: T&Cs** ▶ Step 5: Method | Step 6: Download

Step 4: Terms and conditions

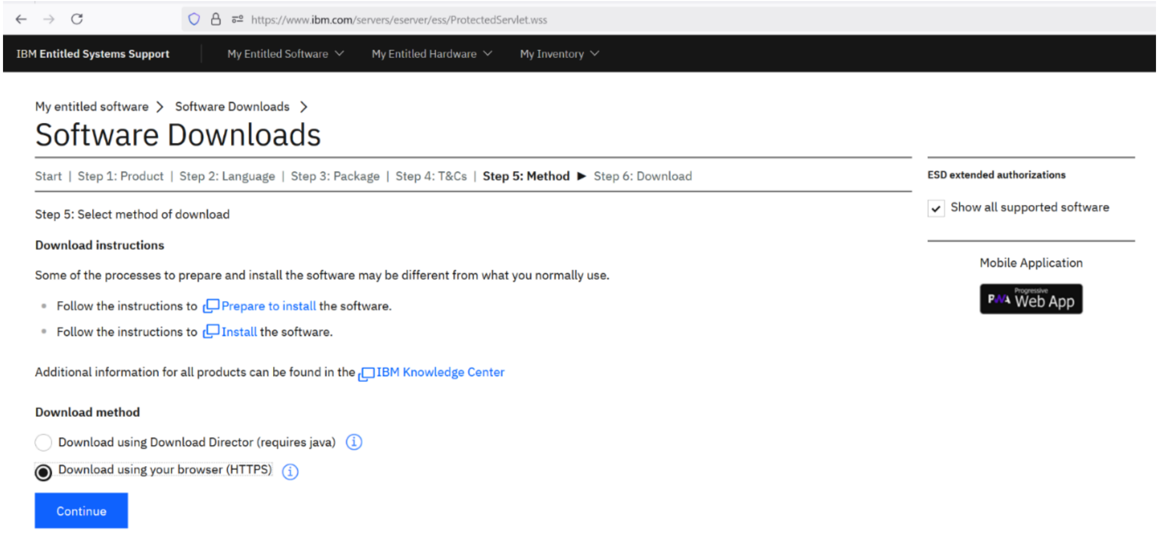
☑ Show all supported software

Current products

Product		**Product Name**
5765-VE4	details	**PowerVM V4**
Release		**Selected content**
04.01.01	License Terms	2282: IBM PowerVM V4 / VIOS 2282 v04.01.01,ENU,DVD

To begin downloading, click the **I agree** button below. By clicking **I agree** you agree that you have had the opportunity to review the terms and conditions for all products you are downloading and that such terms and conditions govern this transaction. Select **I disagree** to exit.

Figure 5: Software Download - VIOS selection(Terms and Conditions)


https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss
IBM Entitled Systems Support
My Entitled Software
My Entitled Hardware
My Inventory
My entitled software > Software Downloads >
ESD extended authorizations
Mobile Application
Web App
Continue

Software Downloads

Start | Step 1: Product | Step 2: Language | Step 3: Package | Step 4: T&Cs | **Step 5: Method** ▶ Step 6: Download

☑ Show all supported software

Step 5: Select method of download

Download instructions

Some of the processes to prepare and install the software may be different from what you normally use.

- Follow the instructions to Prepare to install the software.
- Follow the instructions to Install the software.

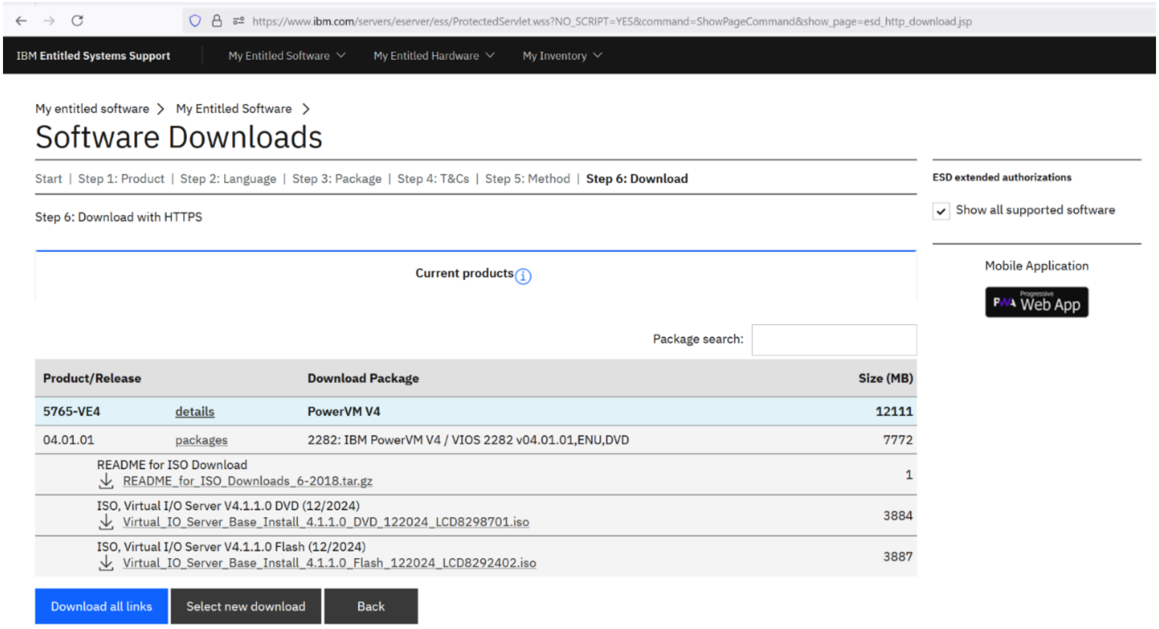
Additional information for all products can be found in the IBM Knowledge Center

Download method

○ Download using Download Director (requires java)

● Download using your browser (HTTPS)

Figure 6: Software Download - VIOS selection(Method of download)


IBM Entitled Systems Support
My Entitled Software
My Entitled Hardware
My Inventory
My entitled software > My Entitled Software >
Start | Step 1: Product | Step 2: Language | Step 3: Package | Step 4: T&Cs | Step 5: Method | Step 6: Download
ESD extended authorizations
Mobile Application
Web App
Download all links
Select new download
Back

https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss?NO_SCRIPT=YES&command=ShowPageCommand&show_page=esd_http_download.jsp

Software Downloads

Step 6: Download with HTTPS

☑ Show all supported software

Current products

Package search:

Product/Release		Download Package	Size (MB)
5765-VE4	details	PowerVM V4	12111
04.01.01	packages	2282: IBM PowerVM V4 / VIOS 2282 v04.01.01,ENU,DVD	7772
		README for ISO Download README_for_ISO_Downloads_6-2018.tar.gz	1
		ISO, Virtual I/O Server V4.1.1.0 DVD (12/2024) Virtual_IO_Server_Base_Install_4.1.1.0_DVD_122024_LCD8298701.iso	3884
		ISO, Virtual I/O Server V4.1.1.0 Flash (12/2024) Virtual_IO_Server_Base_Install_4.1.1.0_Flash_122024_LCD8292402.iso	3887

Figure 7: Software Download - VIOS selection(Download Image)