HMC 1060 Connectivity Security White Paper

IBM® Power8, Power9, and Power10 Processor-Based Systems and IBM Storage Systems DS8000

June 2024

Table of Contents

Introduction

This document describes data that is exchanged between the Hardware Management Console (HMC) and the IBM Service Delivery Center (SDC). In addition, it also covers the methods and protocols for this exchange. This includes the configuration of "Call Home" (Electronic Service Agent) on the HMC for automatic hardware error reporting. All the functionality that is described herein refers to Power Systems HMC and the HMC that is used for the IBM Storage System DS8000.

Terms and Definitions

Users should have a basic understanding of Internet Protocol (IP) networks and protocols. The following is a list of terms and acronyms used in this document.

Term	Definition
3DES	Triple DES
AES	Advanced Encryption Standard
AT&T	American Telephone & Telegraph
CHAP	Challenge Handshake Authentication Protocol
CHARM	Concurrent Hot Add Repair Maintenance
DES	Data Encryption Standard
ESP	Encapsulated Security Payload, Protocol 50
HMAC	Hashing Message Authentication Code
HMC	Hardware Management Console
IBM	International Business Machines
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
LIG	Local Interface Gateway
LPM	Live Partition Mobility
MD5	Message Digest Algorithm 5
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
PSK	Pre-Shared Key
RC4	Rivest Cipher 4
RFC	Request for change

SDC	Service Delivery Center
SNAT	Source Network Address Translation
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network

HMC Connectivity Methods

The HMC uses various methods to communicate back to IBM to match different client environments. This section outlines all the diverse ways in which an HMC can be configured to communicate with IBM.

Outbound Configurations

Outbound configurations are used to configure the HMC to connect back to IBM. The HMC uses the IBM Electronic Service Agent tool to connect to IBM for various situations including, but not limited to, reporting problems, reporting inventory, and transmitting error data. The Power HMC can also download system fixes. For more on the types of data that the HMC sends to IBM, see section Data & Information.

- The information in this section refers to the transactions initiated from the HMC. Outbound transactions (transactions initiated by the HMC) can receive data in response to a request. Examples of this would be fix download and update access key.

Internet Connectivity

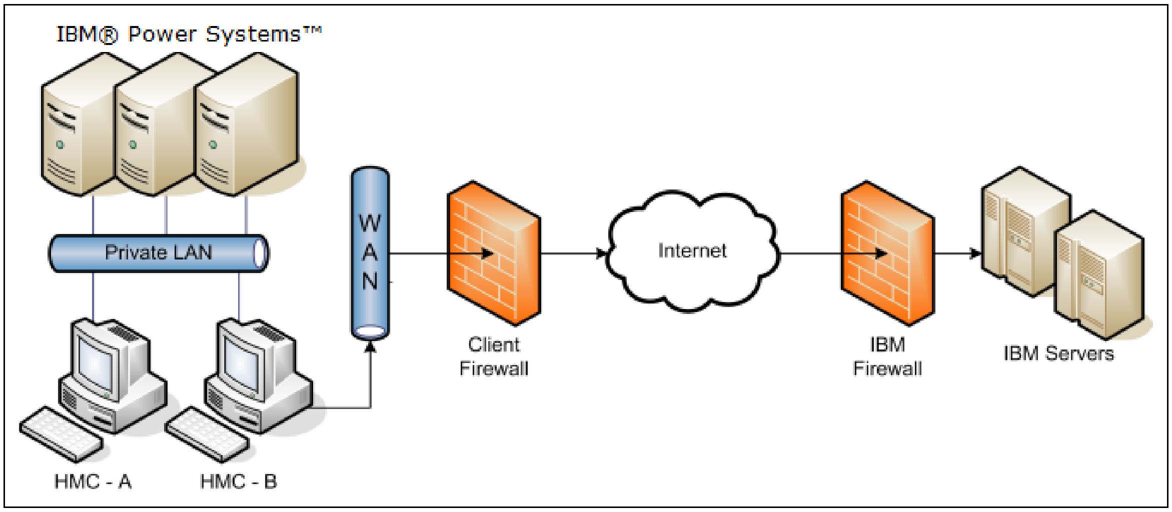
In this configuration, Electronic Service Agent on the HMC uses a client-provided internet connection to connect to IBM Support. All communications are handled through TCP sockets (which always originate from the HMC) and use SSL to encrypt the data that is being sent back and forth.

Optionally, the HMC can also be enabled to connect to the Internet through a client-configured SSL proxy server.

The HMC supports IP V6 connections.

Without proxy server

The following diagram shows the HMC connecting to IBM without a proxy server.



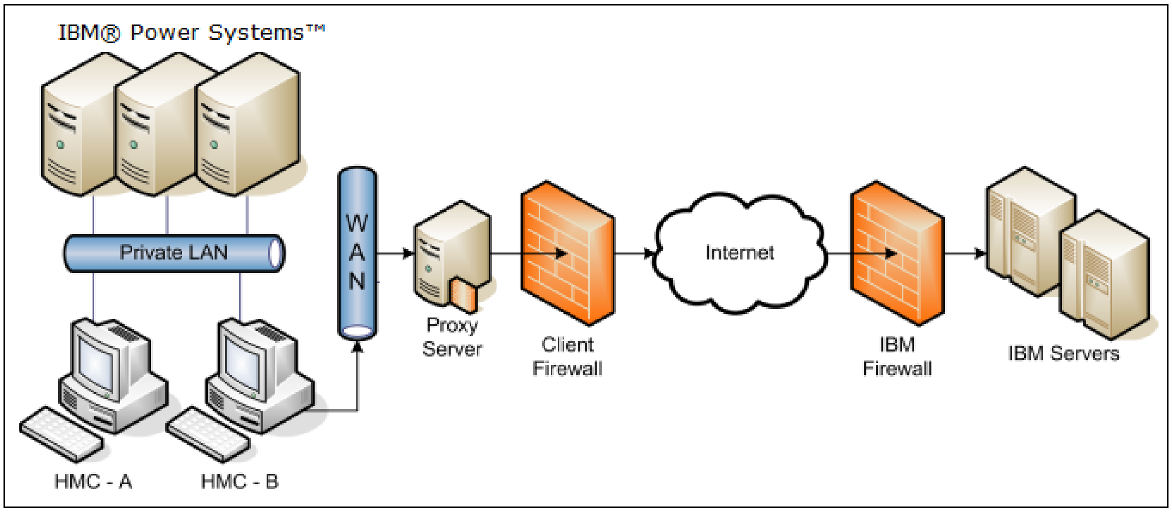
✚ Note: For DS8000, the private LAN and the HMC(s) are inside the machine.

In this setup the HMC connects through the client-provided internet connection by the default route. For this type of configuration, the client can optionally use a second network card to physically separate the local system network from the internet-enabled network.

For the HMC to communicate successfully, the client's external firewall must allow established TCP packets to flow freely on port 443. The use of Source Network Address Translation (SNAT) and masquerading rules to mask the HMC source IP address are both acceptable. The firewall may also limit the specific IP addresses to which the HMC can connect. Appendix contains the list of IP addresses.

With Proxy Server

The following diagram shows the HMC connecting to IBM using a client-provided proxy server.



✚ Note: For DS8000, the private LAN and the HMC(s) are inside the machine.

To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. Optionally, basic proxy authentication

(RFC #2617) may be configured so that the HMC authenticates before attempting to forward sockets through the proxy server.

For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. The proxy server may also limit the specific IP addresses to which the HMC can connect. Appendix contains the list of IP addresses.

Inbound Configurations

Configuring the Electronic Service Agent tool on your HMC enables outbound communications to IBM Support only. Electronic Service Agent is secure and does not allow inbound connectivity. However, HMC can configure customer-controlled inbound communications. Inbound connectivity configurations allow an IBM Service Representative to connect from IBM directly to your HMC or the systems that the HMC manages. The following sections describe two different approaches to remote service. Both approaches allow only a one-time use after enabling.

For DS8000, inbound connectivity is made to the HMC only. In addition to user id and password a remote user must pass a challenge/response type authentication before being granted access to the HMC.

- The information in this section refers to transactions initiated outside of the HMC. Outbound transactions (transactions initiated by the HMC) can receive data in response to a request. Examples of this would be fix download and update access key.

Internet Connectivity

In this configuration, IBM uses a client-provided Internet connection to connect to the Power HMC. All the communications are handled through TCP sockets (which always originate from the HMC) and they use SSL to encrypt the data that is being sent back and forth.

In addition to the support described in the previous paragraph, the DS8000 uses Assist-On-Site (AOS) for Internet SSL based connectivity into the HMC for problem determination and error recovery. For more information on AOS (AOS as a secure remote service solution) see, the IBM AOS Redbook.

- Starting with DS8880 R8.0 the modem is no longer an option for inbound connectivity.

Protocols and Encryption

This section describes the protocols, encryption algorithms, and security that the different communication methods use. It is intended to be a conceptual overview and does not provide implementation details for technologies.

SSL

The SSL sockets used by the HMC are Transport Layer Security (TLS) sockets (sometimes referred to as SSLv4). The initial handshake uses a public/private asymmetric 1024-bit key. After the handshake they negotiate bulk encryption which depends on the IBM server to which a connection is being made. IBM systems in the SDC use or a symmetric 256-bit Advanced Encryption Standard (AES) encryption.

Data and Information

This section outlines what data is sent and the reasons for sending data when the HMC connects to the IBM Service Delivery Center.

Reasons for connecting to IBM

- Reporting a problem with the HMC or one of the systems it is managing back to IBM
- Downloading fixes for systems the HMC manages (Power HMC only)
- Reporting inventory and system configuration information back to IBM
- Sending extended error data for analysis by IBM
- Closing out a problem that was previously open
- Reporting heartbeat and status of monitored systems
- Sending utilization data for system I/O, network, memory, and processors. (Power HMC only)
- Transmission of live partition mobility (LPM) data (Power HMC only)
- Track maintenance statistics (Power HMC)
- Transmission of de-configured resources (Power HMC only)
- Transmission of a request to IBM for a new Access Key
- Transmission of Disk Health report
- Transmission of FLRT report

Data Sent to IBM

This is a list of the files that may be sent to IBM, and short descriptions of the contents of those files. Along with the information contained in these files, the HMC also sends back client contact information, machine model and serial numbers, and debug traces for HMC software.

> None of the information or debug data sent to IBM contains client data.

Bulk data sent by Call Home is sent to the Customer Diagnostic Data Repository (CDDR). For more information on IBM Data Privacy policies, refer https://www.ibm.com/privacy/us/en/?lnk=flg-priv-usen

File	Description
actzuict.dat	Tasks performed
hmc.eed	HMC code level obtained from "lshmc -V" and connection information obtained from "lssysconn -r all"
iqyvpd.dat	Configuration information associated with the HMC
iqyvpdc.dat	Configuration information associated with the HMC

iqyycom0.log	HMC firmware log information backup0
iqyycom1.log	HMC firmware log information backup1
iqyycom2.log	HMC firmware log information backup2
iqyylog.log	HMC firmware log information
PMap.eed	Partition map, obtained from “lshsc -w -c machine”
problems.xml	XML version of the problems opened on the HMC for the HMC and the server
sys.eed	Output from the following commands: lssyscfg –r lpar –m $machine (Partition map) lshwres –r proc –m $machine --level lpar (Processor resources for each partition) lshwres –r mem –m $machine --level lpar (Memory resources for each partition) lshwres –r io –m $machine --rsubtype slot (I/O resources for each partition) lsdump –m $machine (Lists available dumps) lssyscfg –r sys –m $machine (Lists defined name and MTMS) lssyscfg –m $machine –r sysprof (Lists defined system profiles) lslic –m $machine –t syspower (CEC and Power LIC levels) lssyscfg –r cage –e $machine (Lists all the cages within the frame) lssyscfg –r frame –e $machine (List the frame info) lsdump –e $machine –s a (Lists all available dumps for side for this BPC) lsdump –e $machine –s b (Lists all available dumps for side b for this BPC) lshsc -i -a >> managedSystems
machType-Model_Serial.VPD.xml	Configuration information associated with the managed system
filetype.machineSerial .dumpID .yyyymmddhhmmss	Dump file type, set to one of the following: “SYSDUMP” for a platform system dump “FSPDUMP” for a FipS Service Processor dump “BMCDUMP” for a BMC SP dump “SMADUMP” for a SMA dump “PWRDUMP” for a power subsystem dump “LOGDUMP” for a platform event log entry dump “RSCDUMP” for a platform resource dump These dumps do not contain any client-related information.

acuppd.tgz	Output from the following commands: ps -AFLlww ls -lR /proc ls -R top -bn1 ipcs iqzzqtcs ifconfig iptables netstat -rn netstat -anpoee showTraceBuf all df -h The following files: /var/pcidata/biosinfo.log /var/pcidata/pcibusdata /var/log/messages* /var/log/hmc* /var/log/boot.msg /var/log/console.log /console///data/rcs/rcsControl.log /console///fix.logfile /console///fix/errorlog /console//data/iqyye4.log /console///core* /console//ffdc/core//* /console///javacore* /console///hs_err_pid* /console//data/iqyvpd* /console//data/actzuict.dat /console//data/iqzzspr.dat - (HMC Microcode system information manager data (used to control how the HMC functions)) /console//data/persist /console//data/ud//actwcud.dat /console//data//actzzmnd.dat /console//data/iqybrst.trm /console//data//actbrst.trm /console//data//builddate /bom/image.name

	/bom/distro_id /tmp/console/ud//* /tmp/console/xrtr-query*.txt /etc/host* /etc/fstab /etc/mtab /etc/protocols /etc/resolv.conf /etc/services /etc/syslog.conf /etc/sysconfig/network /etc/sysconfig/networking /proc/sys/fs/file-nr /var/log//mediasvcs.log
iqyypell.log	Platform error log sent in by the Operational Test.
cisaSW.xml	Software Service Information from an AIX LPAR. File is retrieved from the /var/esa/data directory on the LPAR.
ServiceData.xml	Summary of selective service operations.
yyyymmddhhmmss_FST.xml	CHARM data
gardRecord.xml	De-commissioned resources
LPMFFDC	LPM resiliency
/data/adm/esa/heartbeat/<TransactionId>/MachineType-Model_SerialNumber_Operating.iqyypell.log	The HMC ESA collects the heartbeat information and saves at this location
/data/adm/esa/hardware/<TransactionId>/MachineType-Model_SerialNumber.VPD.xml	The HMC ESA collects the hardware information and saves at this location
/data/adm/esa/software/<TransactionId>/MachineType-Model_SerialNumber_LPARID.xml	The HMC ESA collects the software information and saves at this location
/var/adm/esa/sysinfo/MachineType.Model.SerialNumber.*.Sysinfo.xml	The HMC ESA collects the System information for the HMC, CEC, and LPAR, and saves at this location.

/data/adm/esa/diskhealth/machineType_machineModel_machineSerial_lparid_DiskAnalytics_YYYYMMDDHHMMSSmmm.xml	The HMC ESA collects the disk health information for the AIX, VIOS, and Linux operating systems. Disk health information includes the most comprehensive information about the hard disks and solid-state disks inside the system and in external enclosures.
/data/adm/esa/flrt/machineType_machineModel_machineSerial_lparid_FLRT_YYYYMMDDHHMMSSmmm-lslpp.txt	The HMC ESA collects the FLRT-related data for the AIX and VIOS operating systems. FLRT (Fix Level Recommendation Tool) data includes update and upgrade recommendations. It provides a report with data to aid system administrators with service planning.
/data/adm/esa/flrt/machineType_machineModel_machineSerial_lparid_FLRT_YYYYMMDDHHMMSSmmm-emgr.txt	

Retention

When Electronic Service Agent on the HMC opens a problem report for itself, or one the systems that it manages, that report is called home to IBM. All the information in that report gets stored for up to 60 days after the closure of the problem.

Problem data that is associated with that problem report is also called home and stored. That information and any other associated packages will be stored for up to three days and then deleted automatically. Support Engineers who are actively working on a problem may offload the data for debugging purposes and then delete it when finished.

Hardware inventory reports and other various performance and utilization data may be stored for many years.

Data Received from IBM

When the HMC sends data to IBM for a problem, the HMC receives back a problem management hardware number. This number is associated with the serviceable event that is opened.

When fixes are requested, the fix is electronically downloaded.

When a new Access Key is requested, the new key is electronically downloaded.

Multiple HMCs

This section describes an environment with multiple HMCs configured with Outbound Connectivity.

- DS8000 supports one or two HMCs inside a DS8000. They will communicate with each other. It does not support HMCs from individual DS8000 to communicate with each other.

Discovery and Inter-Console Communication

Consoles can discover and communicate with each other. A console discovers other consoles by using a UDP broadcast (port 9900) on the subnet of each configured network card. A console also discovers any other console managing the systems it manages. Communication with any discovered console is established using an SSL socket (port 9920) with Diffie-Hellman key exchange.

Removing these ports from the HMC's firewall rules will prevent the HMCs on the subnet from being able to properly discover, communicate, and balance call-home requests among one another.

Call-Home Servers

A console automatically forwards its call-home requests to any discovered console that is configured as a call-home server. When more than one call-home server console is available, a brokering process involving inter-console communication selects a console to handle each request. Failures are automatically retried at the remaining call-home server consoles.

It is strongly preferred that all call home servers are at the same level to ensure compatibility.

- Call-Home server consoles handles only problem reporting or EED events for self and behalf of other HMCs in network. The periodic data (inventory or heartbeat) is handled only by the Call-Home Server HMC based on the following conditions that has connectivity to IBM.

- Call Home Server is enabled (or)

- Call Home Server disabled but discovery options are enabled, and outbound connectivity is configured.

Events Manager for Call Home - Power HMC

The Events Manager for Call Home allows you to register other HMCs. The Events Manager uses HTTPS requests for peer-to-peer communication. After registration, the event manager queries the registered HMC for any problem reporting events that are waiting to be called home to IBM and for any periodic data. The event manager allows the user to check the data that is being sent back to IBM and approve these events. After approval, the event manager notifies the registered HMC that it can proceed with the call home.

Appendix: IP addresses and Ports for IBM Connectivity

Overview

This appendix identifies the IP addresses and ports that are used by either a Power HMC or a Storage HMC when it is configured to use internet connectivity.

The list of required addresses varies based on the following factors:

1. Whether the device is a Power or a Storage HMC
2. The function that the current release of the HMC supports. For example, support for the new simplified call home connectivity.

If your HMC supports the simplified connectivity path, view the section Simplified Connectivity Options, else view section Traditional Connectivity Options to configure the IP addresses and ports.

Simplified Connectivity Options

A new Call Home server environment has been deployed that provides a front-end proxy to the current Call Home infrastructure. This environment simplifies the IT for Call Home customers by reducing the number of customers facing IBM servers, enabling IPv6 connectivity, and providing enhanced security by supporting NIST 800-131A. Customers will have fewer IBM addresses to open on their firewall. All Call Home internet traffic will flow through the Call Home proxy and then fan out to various internal IBM service providers.

Starting with DS8880 R8.0 the simplified connectivity options are used for outbound connectivity.

This list applies to all pre-defined ports and addresses used by the HMC, but not to those HMC functions which allow the entry of a target address / port.

Host Name	Current IP Address(es)	New IP Addresses	Port(s)	Protocol	Additional detail
esupport.ibm.com[1]	129.42.21.70 2607:f0d0:3901:33:129:42:21:70	192.148.6.11 2620:1f7:c010:1:1:1:1:11	443	HTTPS	From March 1, 2024: New IP enabled and returned from DNS. Current IP will be disabled and no longer returned from DNS.

[1] The HMC test connectivity function will test connectivity on all IP addresses, to ensure adequate fail over potential when the individual target endpoints are down for maintenance. Although opening all addresses is not required, the command tests for best practices which support 24x7 access.

Note: The IP addresses might change in the future; hence it is strongly recommended to use host names for firewall configuration instead of IP addresses.

Change in IP addresses in 2024. See below.

Name	IPv4	IPv6	Port(s)
esupport.ibm.com	192.148.6.11	2620:1f7:c010:1:1:1:1:11	443
From March 1, 2024: New IP enabled and returned from DNS. Current IP will be disabled and no longer returned from DNS.			

- esupport.ibm.com DNS will resolve to IPv4 address 192.148.6.11 instead of 129.42.21.70, 129.42.56.189, or 129.42.60.189 from March 1st, 2024. Corresponding IPv6 IP address also changes.
- esupport.ibm.com IPv4 address 129.42.56.189 and 129.42.60.189 will be disabled after June 30th, 2024. Corresponding IPv6 will also be disabled.
- The host name esupport.ibm.com will not change.
- After November 1st, 2024, all static IP access to esupport.ibm.com and www-945.ibm.com will be disabled.

Traditional Connectivity Options

This section of the appendix covers configuration for older versions of the HMC.

SSL Connectivity

Call home configuration download servers

The ECC protocol periodically checks if any of the IP addresses / ports used by SSL connectivity method have changed through the following IP addresses. Both addresses should be opened for total redundancy. This port is only used to download the address/port information used by Call Home transactions.

DNS name	IP address	Port(s)	Protocol(s)	Purpose
www-03.ibm.com	Akamai	443	https	Akamai enabled host does not have fixed IP address.

www6.software.ibm.com	170.225.126.56	443	https	Service provider file download

- Many ECC backend servers have moved to CIO Private Cloud (CPC) environment. Because of this, IP addresses have changed for few servers. The host names will remain the same. You can remove old (obsolete) IP addresses. The change in the IP addresses may impact the connections, so you may need to update the firewalls to accommodate these changes (allowing access to the new IP addresses).

Fix / Policy download Servers

The following IP addresses are used when applications are downloading updates (fixes or policy downloads) from IBM. Note that the system must be enrolled for communications to IBM, to request a download. The list of ports in section Problem / Inventory / Call Home Enrollment Servers must be reviewed.

DNS name	**IP address**	**Port(s)**	**Protocol(s)**	**Purpose**
delivery01-bld.dhe.ibm.com	170.225.126.67	443	HTTPS	Download fixes
delivery01-mul.dhe.ibm.com	170.225.126.68	443	HTTPS	Download fixes
delivery03.dhe.ibm.com	170.225.126.25	443	HTTPS	Download fixes
delivery03-bld.dhe.ibm.com	170.225.126.39 129.35.224.103	443	HTTPS	Download fixes
delivery03-mul.dhe.ibm.com	170.225. 126.40.126.40 129.35.224.113	443	HTTPS	Download fixes
delivery04-bld.dhe.ibm.com	170.225.126.45, 129.35.224.104	443	HTTPS	Download fixes
delivery04-mul.dhe.ibm.com	170.225.126.46 129.35.224.115	443	HTTPS	Download fixes
delivery04.dhe.ibm.com	170.225.126.44 129.35.224.105	443	HTTPS	Download fixes
deliverycb-bld.dhe.ibm.com	170.225.126.47	443	HTTPS	Download fixes
deliverycb-mul.dhe.ibm.com	170.225.126.48	443	HTTPS	Download fixes

download2.boulder.ibm.com	170.225.126.42	443	HTTPS	Download fixes
download3.boulder.ibm.com	170.225.126.24	443	HTTPS	Download fixes
download4.boulder.ibm.com	170.225.126.43	443	HTTPS	Download fixes

- Many IBM call home infrastructure servers have moved to cloud. Because of this, IP addresses have changed for a few servers. The host names will remain the same. You can remove old (obsolete) IP addresses.
- For the HMC versions 930 and above, the servers use HTTPS protocol for downloads, hence make sure to upgrade your HMC version to 930 and above.

Problem / Inventory / Call Home Enrolment Servers / Access Key

The following addresses are used for enrolling a system to communicate with IBM, for problem reporting and periodic transmissions such as inventory or heartbeat for Power data.

DNS name	IP address	Port(s)	Protocol(s)	Purpose
eccgw01.boulder.ibm.com	170.225.122.67	443	https	IBM electronic customer care gateway for system registration, sending of bulk data without a PMH, sending HW / SW inventory and downloading fixes.
	Host name is changed to eccgw.eastdata.ibm.com. However, eccgw01.boulder.ibm.com will act as an alias and can still be used by customers.			
eccgw02.rochester.ibm.com	170.225.123.67	443	https	IBM electronic customer care gateway for system registration, sending of bulk data without a PMH, sending HW / SW inventory and downloading fixes.
	Host name is changed to eccgw.southdata.ibm.com. However, eccgw02.rochester.ibm.com will act as an alias and can still be used by customers.			
	129.42.26.224 (current)	443	https	IBM gateway for problem reporting and access key when the system is

www-945.ibm.com (IPv4)	129.42.42.224 (current) 129.42.50.224 (current) 192.148.6.11 (new)			configured to use electronic customer care.
	170.225.123.67 (new)			From March 1st, 2024, this IP is being enabled for "static access only" to help ease the transition from static IP access to DNS access.
	From March 1st, 2024, www-945.ibm.com DNS will resolve to IPv4 address **192.148.6.11** instead of 129.42.42.224 or 129.42.26.224. Corresponding IPv6 changes as well. From June 30th, 2024, www-945.ibm.com IPv4 address **129.42.42.224** and **129.42.26.224** will be disabled. Corresponding IPv6 disabled as well.			
www-945.ibm.com (IPv6)	2620:0:6c4:1::1000 (current) 2620:0:6c0:1::1000 (current) 2620:0:6c2:1::1000 (current) 2620:1f7:c010:1:1:1:1:11 (new)	443	https	IBM gateway for problem reporting and access key when the system is configured to use electronic customer care

- Both IP addresses (207.25.252.197) & (129.42.160.51) must be OPEN for redundancy purposes.

Upload servers

The following servers are used for sending bulk data (i.e., logs / traces) when an error occurs, as well as sending up the periodic bulk data like inventory and heartbeat.

DNS name	IP address	Port(s)	Protocol (s)	Purpose
www6.software.ibm.com	170.225.126.56	443	https	Upload bulk data associated with status and problem reporting
www.ecurep.ibm.com	192.109.81.20	443	https	Upload bulk data associated with status and

				problem reporting
testcase.boulder.ibm.com	170.225.126.22	21	ftps	Upload bulk data associated with status and problem reporting

Remote Service HMC Port List

When an inbound remote service connection to the HMC is active, only the following ports are allowed through the firewall for TCP and UDP.

Ports	**Description**
22, 2301	Access to the HMC & 5250 Secure Terminal for IBMi
443	Web-based user interface (Power8).
123	NTP
161	SNMP Agent
162	SNMP Trap
427	SLP
443	HMC GUI & REST API
657	RMC
5,989	CIM (Legacy, Removed)
9,900	FCS: HMC-HMC Discovery
9920	FCS: HMC-HMC Communication
9960	VTerm Applet in GUI
12347, 12348	RSCT Peer Domain
17443	Redfish Event
11125 (tcp / udp)	PowerSC UI Agent
5026 (tcp / udp)	Call Home Server Proxy

- It is recommended to maintain only ssh (port 22), https (ports 443), and VTerm (9960) ports exposed to intranet. The other ports must be in private / isolated network. It is suggested to use a separate Ethernet port & VLAN for RMC (port 657), FCS (ports 9900 & 9920), and RSCT Peer Domain (12347, 12348).

More Information

You can find more information about several topics in the following locations.

- IBM Electronic Services web site – Contains more information about Electronic Service Agent.
- HMC Installation and Configuration Guide
- IBM Power Systems HMC Implementation and Usage Guide
- How to secure your HMC
- Call Home, Electronic Fix Distribution - Customer firewalls and proxies for the upcoming infrastructure changes.

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589

Produced in the United States of America
March 2024.

This document was developed for products and/or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products.

Questions on the capabilities of the non-IBM products should be addressed to the suppliers.

The IBM home page on the Internet can be found at http://www.ibm.com.

The IBM Power Systems page on the Internet can be found at https://www.ibm.com/in-en/it-infrastructure/power.

PSW03007-USEN-02