HMC 860 Connectivity Security White Paper

IBM Power6, Power7 and Power8 Processor-Based Systems and IBM Storage Systems DS8000

December 2017

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 version V6.1.0 and later as well as the HMC 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
VPN	Virtual Private Network
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 also has the ability to 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

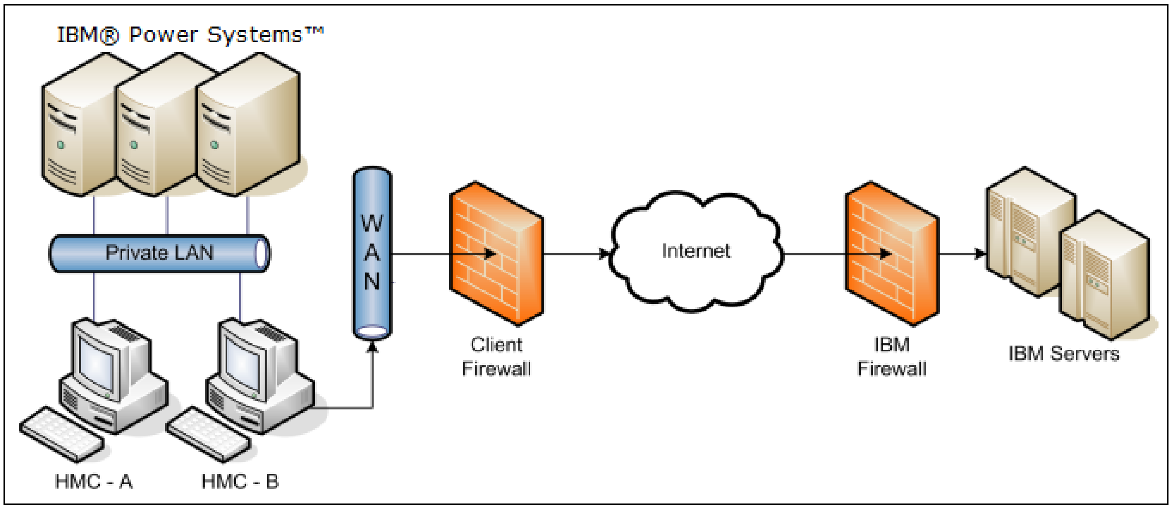
In this configuration, Electronic Service Agent on the HMC uses a client-provided internet connection to connect to IBM Support. All communications are handled through TCP sockets (which always originate from the HMC) and use SSL to encrypt the data that is being sent back and forth.

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.



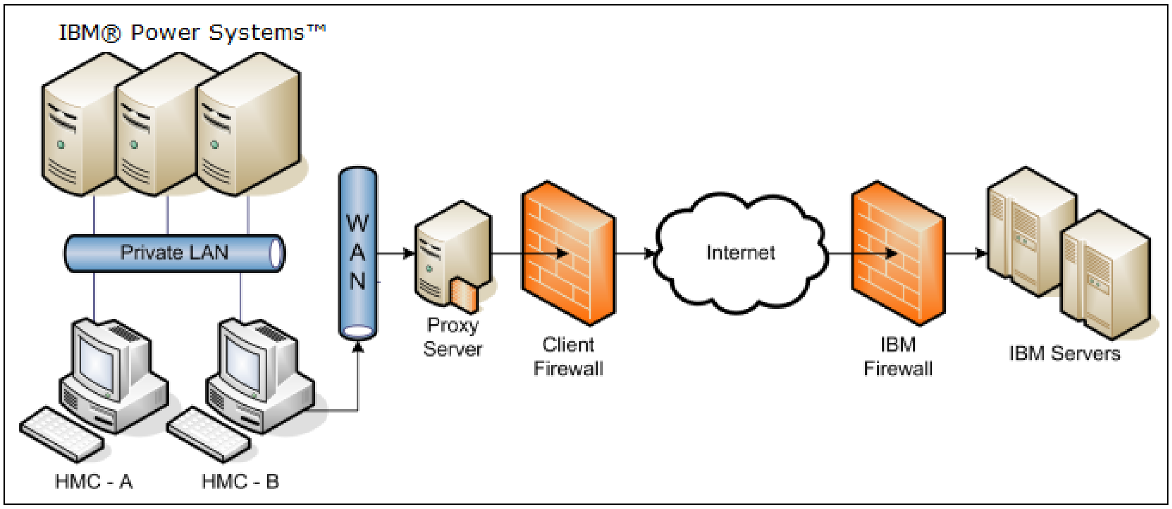
✚ Note: For DS8000, the private LAN and the HMC(s) are inside the machine.

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.

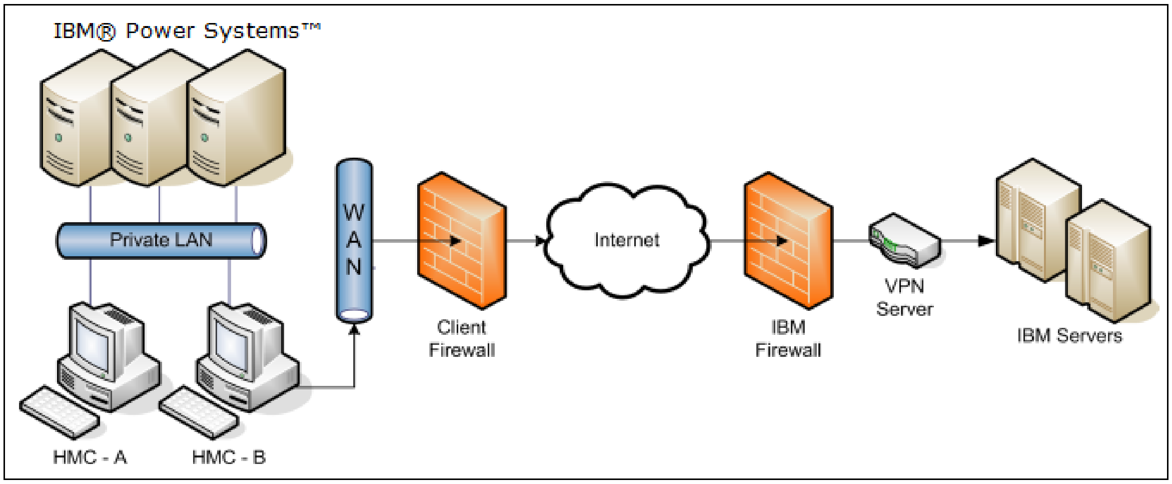
For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. The proxy server may also limit the specific IP addresses to which the HMC can connect. Appendix contains the list of IP addresses.

Internet Virtual Private Network (VPN) Connectivity for Power6, Power7, Power8 and DS8000

Important Note: Starting in 2015, new products will no longer have outbound VPN connectivity capabilities. Existing products with VPN support can continue to use that functionality until the end of life of that product.

Starting with DS8880 R8.0 the VPN is no longer an option for outbound connectivity.

The following diagram shows the HMC connecting to IBM using Internet VPN. This is similar to the Internet Connectivity in section Without proxy server, except that the connections are tunneled inside of another network layer. (This configuration is required to use the VPN Inbound Connectivity described in section VPN connectivity.)



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. When using this type of configuration on the Power HMC, the client can optionally use a second network card to physically separate the local system network from the Internet enabled network. For the DS8000, a second network card in the HMC is not supported. The preferred configuration is to have 2 separate HMCs, and each HMC can be connected to a different customer network.

Before the HMC tries to connect to the IBM servers, it first establishes an encrypted VPN tunnel between the HMC and the IBM VPN server gateway. The HMC initiates this tunnel using Encapsulated Security Payload (ESP, Protocol 50) and User Datagram Protocol (UDP). After it is established, all further communications are handled through TCP sockets, which always originate from the HMC.

For the HMC to communicate successfully, the client's external firewall must allow traffic for protocol ESP and port 500 UDP to flow freely in both directions. The use of SNAT and masquerading rules to mask the HMC's source IP address are both acceptable, but port 4500 UDP must be open in both directions instead of protocol ESP. The firewall may also limit the specific IP addresses to which the HMC can connect. VPN Server Address list section contains the list of IP addresses.

Customers can also configure the Power HMC's internal firewall, which applies to IP connections that go through the VPN tunnel.

Modem Connectivity for Power6, Power7 and DS8000

Although modem connectivity is still supported for some systems, its use is being deprecated and the support has been removed from Power8 and DS8880 R8.0 and later. IBM recommends the usage of internet connectivity for faster service, due to the size of error data files that may be sent to IBM Support. This configuration allows the HMC to use a modem to dial the AT&T global network and connect to the IBM service delivery center. The HMC automatically detects the modem when it boots up.

> For DS8000 the private LAN and the HMC(s) are inside the machine

In this scenario the HMC uses one of the configured phone numbers to dial the modem while connecting to the AT&T Global Network. After the modem connects, the HMC authenticates itself and establishes a Point-to-Point Protocol (PPP) session between the two modems. Finally, after the PPP session has finished, AT&T allows IP connections through a "Fenced Internet," which completes the network between the HMC and the IBM service delivery center.

All the communications between the HMC and the IBM servers are handled through TCP sockets. These sockets always originate from the HMC and use Secure Sockets Layer (SSL) to encrypt the data that is being sent back and forth.

The "Fenced Internet" connection uses a firewall to limit access between the HMC and the Internet. Specifically, it allows communication only between the HMC and a list of IBM IP addresses. All other access to and from the Internet is blocked.

> Customers can also configure the HMCs internal firewall on the Power HMC, which also applies to IP connections over the modem.

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.

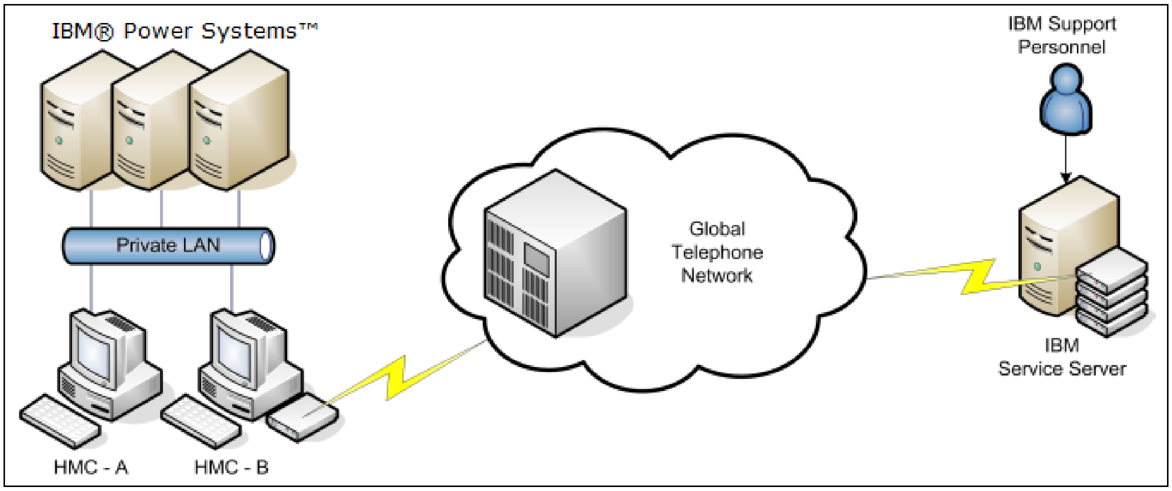
Internet Connectivity

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.

Modem connectivity for the Power HMC for Power6, Power7 and DS8000

The following diagram shows an inbound configuration using a modem.



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

For Power remote service over a modem, the modem must be set up to accept incoming phone calls. An IBM representative then logs into a special server and uses that to dial directly into the client's modem. After the modem answers, a PPP session is initiated, and the IBM representative must authenticate using credentials based on the value the client entered into the **PPP address** field on the **Customize Inbound Connectivity** panel.

After the PPP session is successfully initiated, the HMC creates an alternate IP address and attaches it to the virtual PPP network device for each partition to which the client has allowed access. Special routing rules are then placed to route network packets to those IP addresses and over to the intended partition.

Finally, if the client has disabled access to the HMC, firewall rules are put in place to block all traffic that goes to the HMC. If the client has allowed access to the HMC, then the firewall blocks all traffic except for packets targeting the ports outlined in section Remote Service HMC Port List. Note that these rules override any rules that client sets through the **Customize Network Settings** panel.

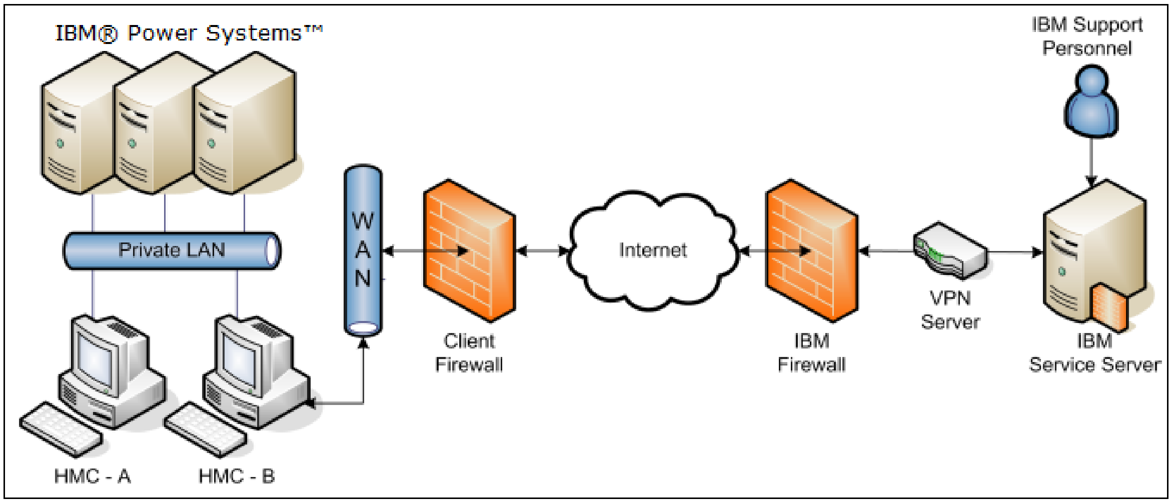
DS8000 uses a modem to provide inbound connectivity through an ASCII terminal emulation. In addition to user id and password a remote user must pass a challenge/response type authentication before being granted access to the HMC.

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

VPN connectivity for Power6, Power7, and Power8

Important Note: Starting in 2015, Power HMC will be limited to Internet VPN. Modem and pass-through VPN are no longer supported. Existing products with VPN support can continue to use that functionality until the end of life of that product.

The following diagram shows an inbound configuration using VPN.



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

A remote service VPN session can be initiated over a modem, Internet, or a pass-through i5/OS partition. In older versions that support Outbound VPN connectivity, at least one of these methods of connectivity must be configured through the **Outbound Connectivity** panel.

To initiate the VPN session, use the HMC web interface or the storage command line interface (SDCLI) or an inbound modem connection triggering the HMC to connect into the IBM VPN server as described in section Internet Virtual Private Network. The client must ensure the firewall has been properly configured to allow connections to the servers as listed in VPN Server Address list.

After the VPN session has been initiated, the HMC initiates additional L2TP+PPP tunnels for each partition to which the client has allowed access. Special routing rules are then put in place to route network packets on those tunnels over to the intended partitions.

Finally, if the client has disabled access to the HMC, firewall rules are put in place to block all traffic that goes to the HMC. If the client has allowed access to the HMC, then the firewall blocks all traffic except for packets targeting the ports outlined in section Remote Service HMC Port List. Note that these rules override any rules that client sets through the **Customize Network Settings** panel.

After the VPN session has been fully established, an authorized IBM Service Representative logs into the IBM Service Server and connects to the HMC through the VPN session. The IBM Service Server has a special firewall in place that keeps the client's VPN session completely separated from the IBM intranet. Access to the client's VPN session through the IBM Service Server is possible only through the use of special tools that require special authorization and knowledge to use.

DS8000 HMC and VPN connectivity

Starting in 2015, new products will no longer have inbound VPN connectivity capabilities. Existing products with VPN support can continue to use that functionality until the end of life of that product.

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

The HMC for DS8000 can be configured to allow specific, controlled, inbound connectivity for remote service through VPN. The VPN connection is always initiated from the HMC either via DSCLI or the service interface. For more information on DS8000 connectivity security, see VPN Security and Implementation.

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 particular technologies.

AT&T Global Network for Power6, Power7 and DS8000

When the HMC tries to connect to IBM using one of the phone numbers that is available from the Outbound Connectivity Modem panel, it is dialing into the AT&T Global Network Fenced Internet Remote Access Dial Service.

After the HMCs modem successfully connects into one of AT&T Local Interface Gateways (LIGs), it initiates a PPP session and authenticates with the server using a special account and user ID that are sent using Password Authentication Protocol (PAP). Upon successful authentication, the LIG assigns the HMC a dynamic IP address from a pool for the duration of the connection.

All packets that flow through the LIG from the HMC are inspected to ensure that the source of the packet is the assigned IP address and that the destination matches one of the authorized IBM servers or to one of the utility services provided by AT&T (such as domain name server). Return packets that flow through the LIG back to the HMC must have destinations that match the assigned IP addresses and the source must match the IBM server with which the IP addresses are communicating. Any packets that do not match these criteria are discarded.

SSL

The SSL sockets used by the HMC are actually 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 the 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.

VPN protocol for Power6, Power7, Power8 and DS8000

Starting in 2015, new products will no longer have inbound VPN connectivity capabilities. Existing products with VPN support can continue to use that functionality until the end of life of that product.

The VPN connection that is used by the HMC is an IP Security (IPSec) implementation in tunnel mode over a UDP socket that uses L2TP+PPP encapsulation for the actual data transmission. The VPN key exchange is done using Internet Key Exchange (IKE), which is authenticated as part of the ESP encryption by using a Pre-Shared Key (PSK). The ESP encryption uses a 192-bit Triple DES (3DES) encryption key with a 160-bit Message Digest Algorithm 5 (MD5) hash authentication key. The authentication and encryption keys are renegotiated at a random time interval around every 30 minutes.

After the IPSec tunnel has been properly established, the HMC creates an L2TP tunnel between itself and the VPN server. Within that tunnel the HMC then establishes one or more PPP sessions that the server authenticates using the Challenge Handshake Authentication Protocol (CHAP). All further HMC data sockets are then opened over one of the established PPP sessions.

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 performance and 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

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.***

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 of 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 a 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.
stats.send	Performance Management information from an AIX and/or Linux LPAR is retrieved for the /var/adm/perfmgr/daily/<hostname> directory on the LPAR
ServiceData.xml	Summary of selective service operations.
yyyymmddhhmmss_FST.xml	CHARM data
gardRecord.xml	De-commissioned resources
LPMFFDC	LPM resiliency
/var/adm/esa/heartbeat/<TransactionId>/MachineType-Model_SerialNumber_Operating.iqyypell.log	The HMC ESA collects the heartbeat information and saves at this location
/var/adm/esa/performance/<TransactionId>/MachineType-Model_SerialNumber_LPARID.pm_stats.send	The HMC ESA collects the performance management data and saves at this location
/var/adm/esa/hardware/<TransactionId>/MachineType-Model_SerialNumber.VPD.xml	The HMC ESA collects the hardware information and saves at this location
/var/adm/esa/software/<TransactionId>/MachineType-Model_SerialNumber	The HMC ESA collects the software information and saves at this location

_LPARID.xml	
/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.

Retention

When Electronic Service Agent on the HMC opens up 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

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 events that are waiting to be called home to IBM. 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 customer 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 allows the entry of a target address / port.

Host Name	IP Address(es)	Port(s)	Protocol	Additional detail
esupport.ibm.com[1]	129.42.56.189	443, 80	HTTPS (to IBM), HTTP (from IBM)	IPV4, Recommendation is that customers open the address range of 129.42.0.0 / 18 to minimize churn in the future if additional addresses are added.
	129.42.60.189			
	129.42.54.189			
	2620:0:6c0:200:129:42:56:189	443, 80	HTTPS (to IBM), HTTP (from IBM)	IPV6, Recommendation is that customers

[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.

	2620:0:6c2:200:129:42:60:189			open 2620:0:6c0: /45 to minimize churn in the future if additional addresses are added.
	2620:0:6c4:200:129:42:54:189			

Traditional Connectivity Options

This section of the appendix covers configuration for older versions of the HMC. In these older releases, there were two different connection paths to IBM, based on whether SSL connectivity or URSF has been chosen.

If you would like to use SSL, view section SSL Connectivity, else view section URSF (Universal Remote Support Function) with optional VPN (Virtual Private Networking) Connectivity.

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 been 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	204.146.30.17	443 and 80 (optional)	https and http	Service provider file download.
www6.software.ibm.com	170.225.15.41	443	https	Service provider file download

Fix / Policy download Servers

The following 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 should be reviewed.

DNS name	IP address	Port(s)	Protocol(s)	Purpose
download3.boulder.ibm.com	170.225.15.76	80	HTTP	Download fixes
download3.mul.ie.ibm.com	129.35.224.114	80	HTTP	Download fixes
delivery03.bld.dhe.ibm.com	170.225.15.103 129.35.224.103	80	HTTP	Download fixes
Delivery03.mul.dhe.ibm.com	129.35.224.113 170.225.15.113	80	HTTP	Download fixes

download4.boulder.ibm.com	170.225.15.107	80	HTTP	Download fixes
download4.mul.ie.ibm.com	129.35.224.107	80	HTTP	Download fixes
delivery04-bld.dhe.ibm.com	170.225.15.104, 129.35.224.104	80	HTTP	Download fixes
delivery04-mul.dhe.ibm.com	129.35.224.115, 170.225.15.115	80	HTTP	Download fixes
delivery04.dhe.ibm.com	129.35.224.105, 170.225.15.105	80	HTTP	Download fixes

Problem / Inventory / Call Home Enrollment 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, heartbeat or PM for Power data.

DNS name	IP address	Port(s)	Protocol(s)	Purpose
eccgw01.boulder.ibm.com	207.25.252.197	443	https	IBM electronic customer care gateway for system registration, sending of bulk data without a PMH, sending HW / SW inventory and downloading fixes.
eccgw02.rochester.ibm.com	129.42.160.51	443	https	IBM electronic customer care gateway for system registration, sending of bulk data without a PMH, sending HW / SW inventory and downloading fixes.
www-945.ibm.com	129.42.26.224 129.42.42.224 129.42.50.224	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 of 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	170.225.15.41	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	170.225.15.31	21	ftps	Upload bulk data associated with status and problem reporting

URSF (Universal Remote Support Function) with optional VPN (Virtual Private Networking) Connectivity

If you are using VPN or have not configured your system to use ECC, then the following is the list of addresses that must be opened.

Problem Reporting

IP address	Port	Purpose
198.74.67.240	19285	Problem Reporting
198.74.71.240	19285	Problem Reporting

Inventory, Heartbeat, and Diagnostic Data associated with Problem Reporting

Servers specific for North and South America

IP address	Port	Purpose	GEO / IOT
129.42.160.49		Legacy call home. Allow HMC access to IBM Service for North and South America	
207.25.252.204		Legacy call home. Allow HMC access to IBM Service for North and South America	

Servers for all other regions

IP address	Port	Purpose	GEO / IOT
129.42.160.50		Legacy call home. Allow HMC access to IBM Service for all other regions	
129.42.160.50		Legacy call home. Allow HMC access to IBM Service for all other regions	
207.25.252.205		Legacy call home. Allow HMC access to IBM Service for all other regions	

129.42.160.48	443	IBM Service to System Authentication Server. Legacy call home (SAS-1, SDR_2). Doc_Update_1	
207.25.252.200	443	IBM Service to System Authentication Server. Legacy periodic call home (SAS-2, SDR_1) - Doc_Update_2	

Remote Support

IP address	Port	Purpose
198.74.67.235	11111	Remote Support
198.74.71.235	11111	Remote Support

Download Power Firmware

IP address	Purpose
129.35.224.112	Download Power firmware using an anonymous HTTP connection in conjunction with port 80

VPN Server Address List

These IP addresses are used by an HMC when it is configured to use Internet VPN connectivity. All connections use protocol ESP and port 500 UDP, or ports 500 and 4500 UDP when a Network Address Translation (NAT) firewall is being used.

VPN Servers for All Regions

- 129.42.160.16
- 207.25.252.196

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, 23, 2125, 2300	These ports are used for access to the HMC.
9090, 9735, 9940, 30000-30009	These ports are used for Web-based System Manager (Power5).
443, 8443	These ports are used for Web-based user interface (Power6, Power7 and Power8).

More Information

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

- IBM Electronic Services web site – Contains more information about Electronic Service Agent.
- HMC Installation and Configuration Guide
- Redbook.
- Important Hardware Support Notice: IBM is discontinuing the use of analog dial up modems for service communications from our hardware. Dial connections use a modem connected to an analog phone line. These communications include automated calls for support as well as authorized transmission of error log data.

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

Produced in the United States of America
December 2017.

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 with the suppliers.

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

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

The IBM System I home page on the Internet may be found at: http://www.ibm.com/systems/i.

PSW03007-USEN-02