Cloud Management Console Cloud Connector Security White Paper

Aug 2020

Author:

Kevin Kenyon

kwkenyon@us.ibm.com

Manjunath Shanbhag

manjunathns@in.ibm.com

Table of Contents

Executive Overview

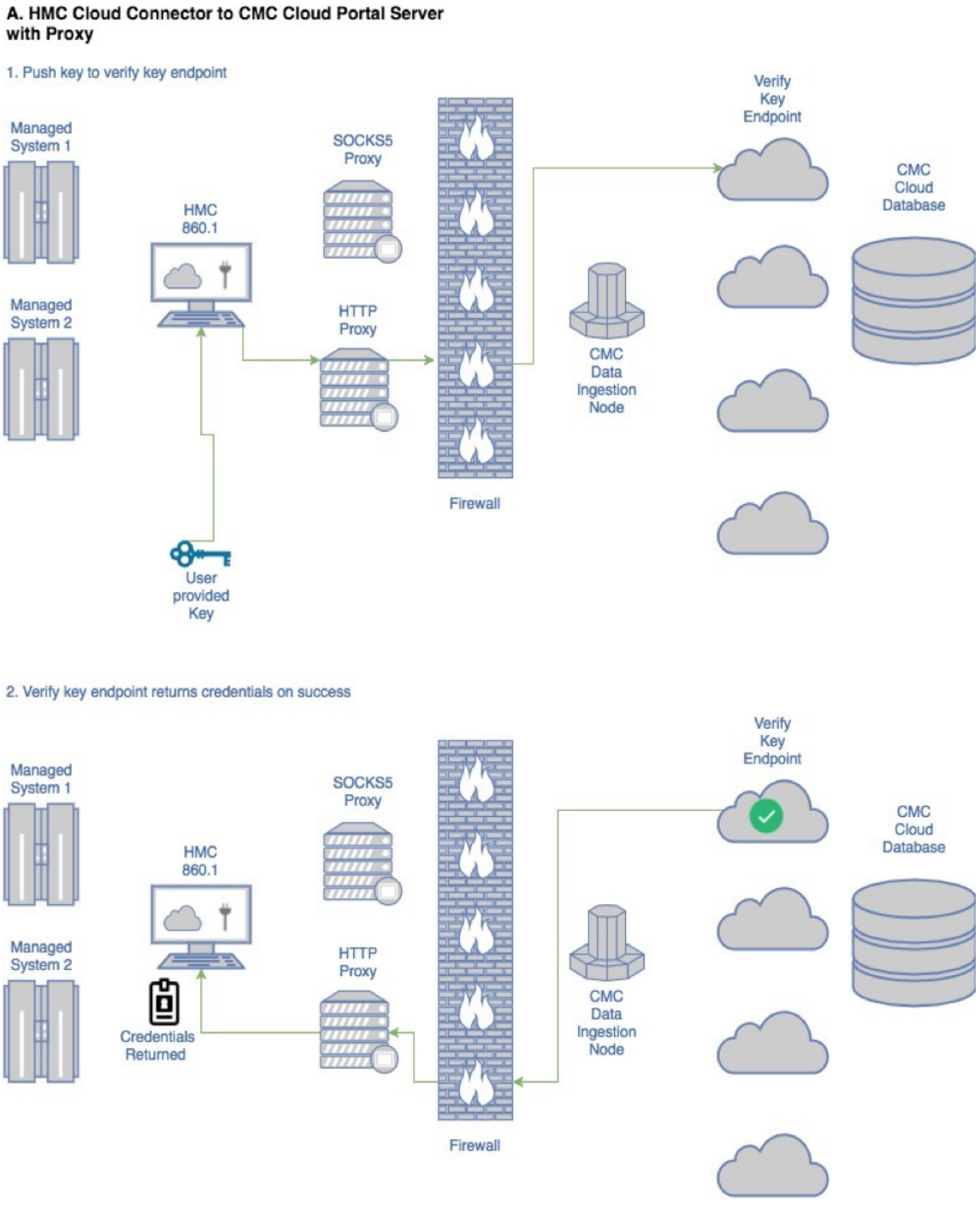
The HMC Cloud Connector is a Linux service that pushes data into the Cloud Management Console (CMC) database upon user enablement. Cloud connector utilizes a one-way push model: It initiates all outbound communication. This is not to be confused with one-way computer communication, which sends a message without waiting for a response. The typical request-response style is used but cloud connector is never the responder but always the requestor. For automatic network based configuration, where cloud connector pulls the configuration file from the cloud database, HTTPS is used; and for application data flow (push) between cloud connector and the CMC data ingestion node, TCP with SSL is used.

Cloud Connector is preinstalled in HMC, and can be started using the command with the key mentioned in the CMC->Settings->Cloud Connector Settings. Cloud Connector needs to connect to multiple end points and hence needs outbound connection to the IPs and Ports mentioned in the CMC->Settings->Cloud Connector Settings. If the HMCs do not have outbound connection to the endpoints, then proxies can be used for the connections.

Outbound Connections

A. HMC Cloud Connector to CMC Cloud Portal Server

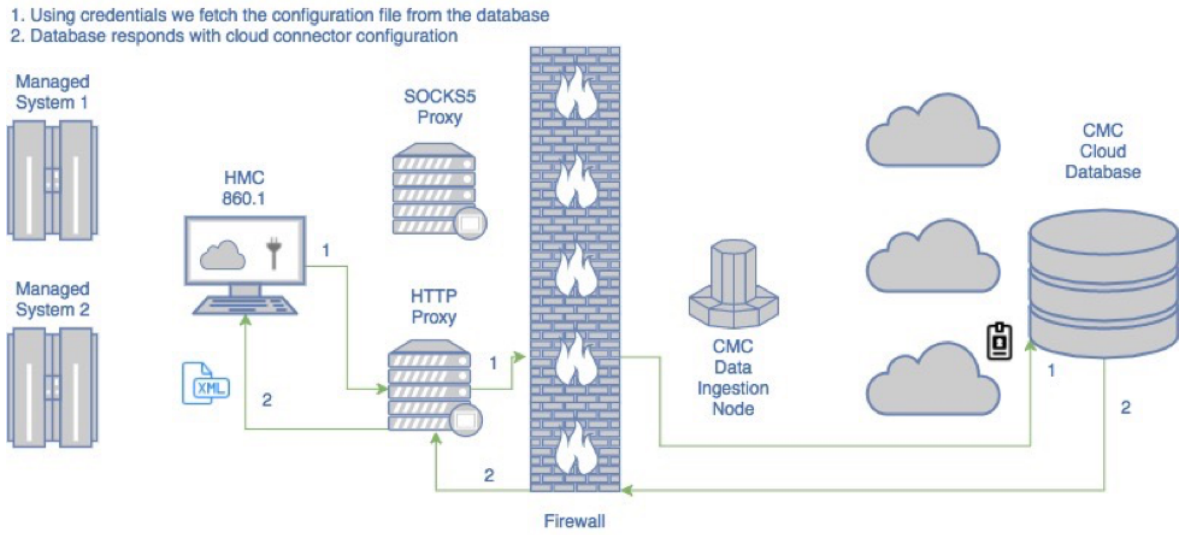
1. Given the user provided key, cloud connector establishes trust with the cloud portal via pushing the user provided key to a cloud portal key verification endpoint.
2. Given successful key verification, the CMC Cloud Portal Server returns credentials for pulling the cloud connector configuration file and SSL certificates.



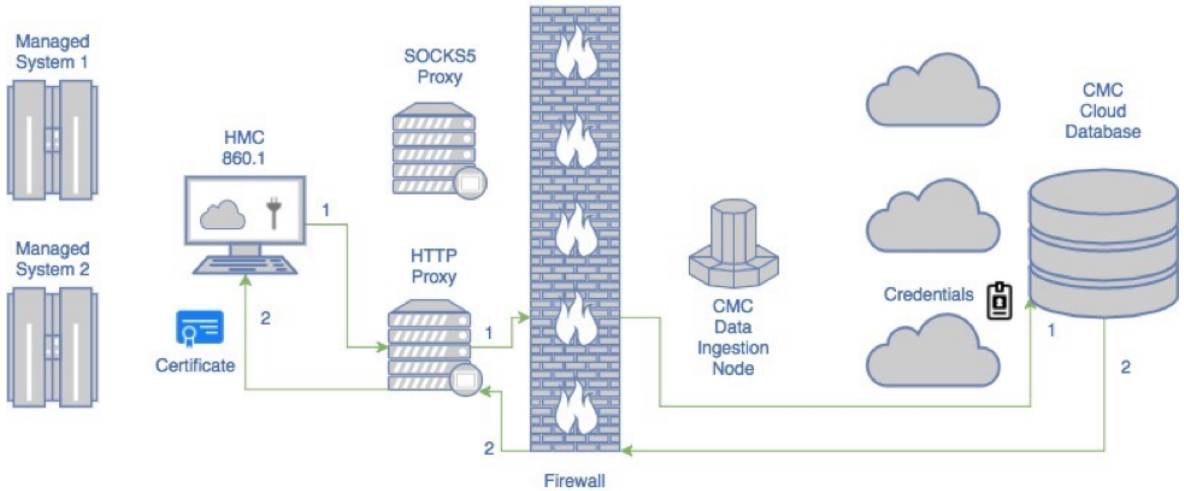
B. HMC Cloud Connector to CMC Cloud Database (Configuration/Certificates)

1. Given the credentials from connection A, the cloud connector pulls the customer specific cloud connector configuration file from the CMC Cloud Configuration Database
2. Given credentials from the configuration file collected with connection B1, the cloud connector pulls the SSL certificates and key from the CMC Cloud Certificate Database to secure the application data flow pipeline (connection C)

B1. HMC Cloud Connector to CMC Cloud Database

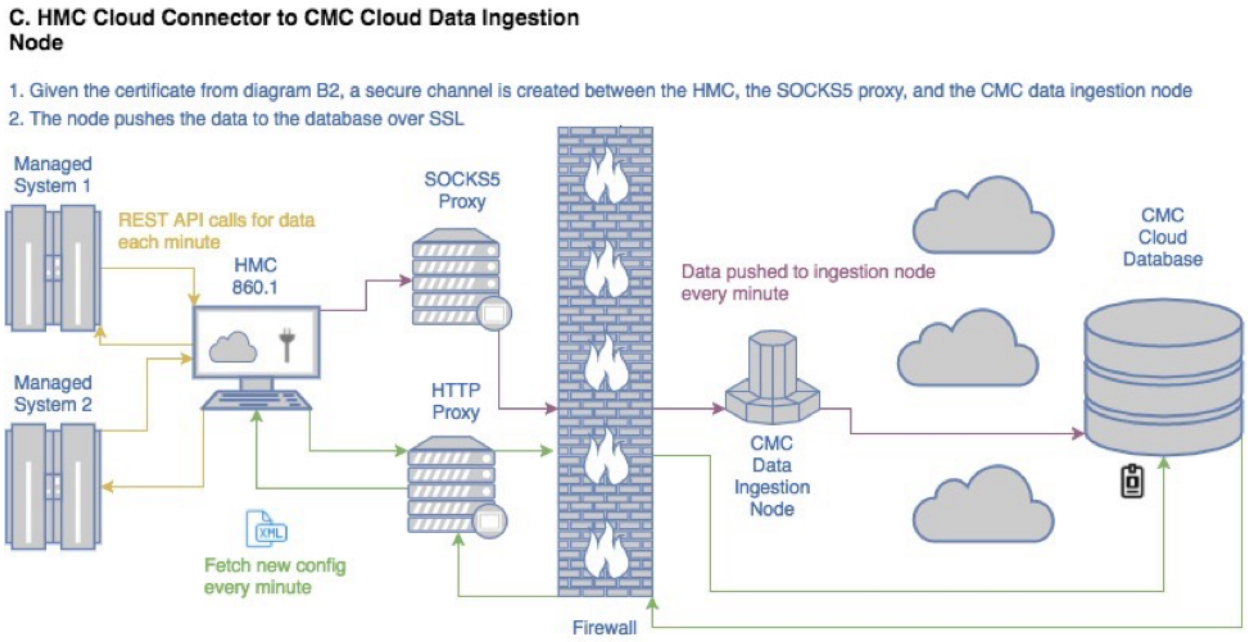


B2. HMC Cloud Connector to CMC Cloud Database



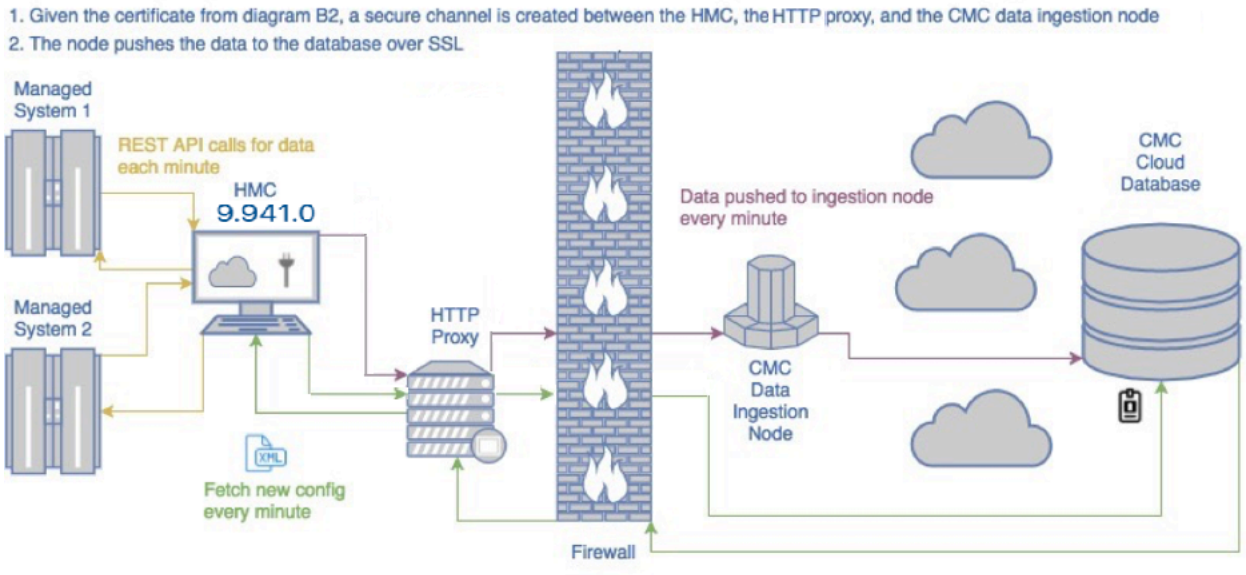
C. HMC Cloud Connector to CMC Cloud Data Ingestion Node

1. Given the SSL certificates from connection B2, a secure channel is created between the cloud connector and the CMC cloud data ingestion node through which cloud application data is pushed, such as Inventory data, Performance data, Logging data, and data related to any CMC app provided in the future. You can see that SOCKS5 proxy is used to establish the connection between HMC and ingestion node



2. With 9.1.941.0 version of HMC, cloud connector can be started only with HTTP proxy option. If the Cloud connector is started with only HTTP proxy, then it uses HTTP proxy to establish connection between HMC and ingestion node(as in connection D below). That removes the dependency on SOCKS5 proxy which was mandatory in the previous versions of HMC. Connection C option is still supported in current versions of the HMCs, when the Cloud Connector is started with both HTTP and SOCKS5 proxy options.

D. HMC Cloud Connector to CMC Cloud Data Ingestion Node



Secure Automatic Network Driven Cloud Connector Configuration

A. HMC Cloud Connector to CMC Cloud Portal Server

The startup key for the HMC based cloud connector (connector) is used to establish a valid connection between the connector and the CMC Cloud Portal Server (cloud portal) and between the connector and the configuration database (database). Once a valid connection is established to the cloud portal, credentials are returned to the cloud connector allowing for dynamic configuration and reconfiguration. To establish this connection, a security test is executed to assert that the startup key provided is valid. The test begins with a GET request from the connector to the cloud portal which will return a cross-site request forgery (XSRF) header. This XSRF header, along with a portion of the decoded key are then POST'ed to the same cloud portal endpoint. If the key is considered valid, the cloud portal will respond with a set of encoded credentials giving cloud connector access to a database containing the customers cloud connector configuration file.

All communication from the connector to the cloud portal are secured using the Transport Layer Security Version 1.2 protocol (TLSv1.2) and the SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher suite.

The complete list of enabled cipher suites for communication phase one to the cloud portal are listed below:

TLS_EMPTY_RENEGOTIATION_INFO_SCSV,
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
SSL_RSA_WITH_AES_256_CBC_SHA256,
SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
SSL_ECDH_RSA_WITH_AES_256_CBC_SHA384,
SSL_DHE_RSA_WITH_AES_256_CBC_SHA256,
SSL_DHE_DSS_WITH_AES_256_CBC_SHA256,
SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_AES_256_CBC_SHA,
SSL_ECDH_RSA_WITH_AES_256_CBC_SHA, SSL_DHE_RSA_WITH_AES_256_CBC_SHA,
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256, SSL_RSA_WITH_AES_128_CBC_SHA256,
SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
SSL_ECDH_RSA_WITH_AES_128_CBC_SHA256,
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256,
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256,
SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,

SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
SSL_RSA_WITH_AES_256_GCM_SHA384,
SSL_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
SSL_ECDH_RSA_WITH_AES_256_GCM_SHA384,
SSL_DHE_DSS_WITH_AES_256_GCM_SHA384,
SSL_DHE_RSA_WITH_AES_256_GCM_SHA384,
SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
SSL_RSA_WITH_AES_128_GCM_SHA256,
SSL_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
SSL_ECDH_RSA_WITH_AES_128_GCM_SHA256,
SSL_DHE_RSA_WITH_AES_128_GCM_SHA256,
SSL_DHE_DSS_WITH_AES_128_GCM_SHA256,

B. HMC Cloud Connector to CMC Cloud Database (Configuration/Certificates)

Once phase one communication with the cloud portal is completed, a secure SSL connection is then established between cloud connector and the cloud database to fetch the configuration file. This configuration file contains which cloud applications the customer has enabled, the data to push for those applications, what data to filter(not send to the cloud portal due to Managed System blocklisting and the data filter option to filter the System and Partition's IP address), and the internet protocol address (IP) of the cloud data ingestion node. In addition, it provides credentials for fetching an SSL certificate and key pair used in communication between the connector and the cloud data ingestion node. The credentials are used to access a separate database from the one used to fetch the configuration file. However, the underlying network location and mechanism used to fetch the certificates is the same. In short, an SSL connection is established and the data is returned to the connector. Every minute the cloud connector fetches a new configuration if it has changed.

All communication from the connector to the cloud database are secured using the Transport Layer Security Version 1.2 protocol (TLSv1.2).

C. HMC Cloud Connector to CMC Cloud Data Ingestion Node

Once the cloud connector is configured via the automated configuration process, it will begin collecting data and pushing that data to the data ingestion node. This channel is secured using SSL with mutual authentication using the certificate and key mentioned in the previous section. Using mutual authentication ensures that the connector only sends data to trusted data ingestion nodes. The certificate and key are stored on the HMC filesystem but are only accessible by the root user.

Fetching Data from HMC API

The final phase for data communication does not present a security risk but is worth discussing. The connector uses the HMC REST API to fetch inventory and performance data. Every minute new inventory data is fetched and saved to the filesystem for delivery to the data ingestion node. The data has to be saved to the filesystem because the data shipper code relies on this to keep track of what has or has not been successfully sent. For security, the files are only accessible to the root user as they contain all inventory associated to that HMC. If no new inventory data is present (that is, the inventory is the same) nothing is saved and shipped. Performance data is saved and shipped every minute unless performance collection is disabled.

To connect to the HMC API a special login procedure was built that only works for API calls originating from the HMC itself to its own localhost or 127.0.0.1 endpoint. Once the login query is completed, the HMC API server saves a login token (session cookie) to the HMC filesystem so that the connector can use it to make queries to the API without having to re-authenticate. This token may expire. If it does, a new one is generated and saved to the filesystem using the same mechanism. The token is only usable for queries to localhost. In other words, it cannot be hijacked and used for queries against the actual HMC hostname or IP from a remote server. Thus, it's only useful for services running on the HMC. The saved token is only accessible to the root user. TLS version 1.2 is used to fetch data from the HMC API. Since the requests initiate from the HMC themselves, this is an added security measure. In short, no man-in-the-middle attack is viable for requests coming from the HMC to the HMC.

There are some information (such as logging data), are not available through HMC REST APIs. Such data are saved in the HMC's filesystem, accessible only by the root user. Cloud Connector reads the data from such files, filters, and pushes the data to the ingestion node.

The application built in Cloud Management Console uses data from CMC Cloud Database. The apps needs data such as inventory, performance metrics, logging information etc. based on its use cases. This data is being pushed by cloud connector running in the HMC, which uses different REST API to fetch this information or the data saved by HMC in the filesystem. HMC provides rich set of REST APIs (https://www.ibm.com/support/knowledgecenter/TI0003M/p8ehl/concepts/ApiOverview.htm) , which provides information of partition, systems, IO, performance metrics etc. But Cloud Connector retrieves and pushes attributes required for the apps running in Cloud Management Console. Below is the consolidated list of attributes pushed by the Cloud Connector :

Inventory Attributes :

Resource	Attribute Name
ManagedSystem	SystemName
	State
	SystemFirmware
	SystemLocation
	Description
	SystemType

	MachineTypeModelAndSerialNumber.MachineType
	MachineTypeModelAndSerialNumber.Model
	MachineTypeModelAndSerialNumber.SerialNumber
	Hostname
	PrimaryIPAddress
	UUID
	RemainingHoursInMeteredPoolAuthPeriod
	PowerEnterprisePoolID
	ProcessorThrottling
	AssociatedSystemProcessorConfiguration.ConfigurableSystemProcessorUnits
	AssociatedSystemProcessorConfiguration.InstalledSystemProcessorUnits
	AssociatedSystemProcessorConfiguration.CurrentAvailableSystemProcessorUnits
	AssociatedSystemMemoryConfiguration.InstalledSystemMemory
	AssociatedSystemMemoryConfiguration.ConfigurableSystemMemory
	AssociatedSystemMemoryConfiguration.CurrentAvailableSystemMemory
	AssociatedSystemMemoryConfiguration.HugePageSize
	AssociatedSystemMemoryConfiguration.MemoryUsedByHypervisor
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.BusGroupingRequired
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.Description
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.FeatureCodes
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IOUnitPhysicalLocation
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCAdapterID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCIClass
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCIDeviceID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCISubsystemDeviceID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCIManufacturerID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCIRevisionID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCIVendorID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.PCISubsystemVendorID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.AlternateLoadSourceAttached
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.ConsoleCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.DirectOperationsConsoleCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.IOP
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.IOPInfoStale
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.IOPoolID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.LANConsoleCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.LoadSourceAttached
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.LoadSourceCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.OperationsConsoleAttached
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIBMiIOSlot.OperationsConsoleCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.AdapterID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.Description
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.DeviceName

	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.DynamicReconfigurationConnectorName
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.PhysicalLocation
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.UniqueDeviceID
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.LogicalPartitionAssignmentCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.RelatedIOAdapter.IOAdapter.DynamicPartitionAssignmentCapable
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.SlotDynamicReconfigurationConnectorIndex
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.SlotDynamicReconfigurationConnectorName
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.SlotPhysicalLocationCode
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.SRIOVCapableDevice
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.SRIOVCapableSlot
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.SRIOVLogicalPortsLimit
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.ParentDynamicReconfigurationConnectorIndex
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.ParentName
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PCIDeviceId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PCIVendorId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PCISubsystemDeviceId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PCISubsystemVendorId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PCIRevisionId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.ProgrammingInterfaceClass
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PCIClassCode
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.DeviceType
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PrimaryDeviceFunction
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.SerialNumber
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.FruNumber
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.PartNumber
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.CCIN
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.SlotChildId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.ParentSlotChildId
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.Size
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.SizeMetric
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.NumEnclosureBays
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.LocationCode
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.MicroCodeVersion
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.WWPN
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.WWNN
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.MacAddressValue
	AssociatedSystemIOConfiguration.IOSlots.IOSlot.IORDevices.IORDevice.Description
	PowerSupplies.PowerSupply.LocationCode
	PowerSupplies.PowerSupply.FruNumber
	PowerSupplies.PowerSupply.SerialNumber
	PowerSupplies.PowerSupply.State
	PowerSupplies.PowerSupply.Health
	PowerSupplies.PowerSupply.Description

	PowerSupplies.PowerSupply.MemberId
	FANs.FAN.LocationCode
	FANs.FAN.FruNumber
	FANs.FAN.SerialNumber
	FANs.FAN.State
	FANs.FAN.Health
	FANs.FAN.Description
	FANs.FAN.MemberId
SharedProcessorPool	AssignedPartitionsLinks
	CurrentReservedProcessingUnits
	MaximumProcessingUnits
	PoolID
	AvailableProcUnits
	PoolName
VirtualSwitch	SwitchID
	SwitchMode
	SwitchName
SharedMemoryPool	CurrentPoolMemory
LogicalPartition	PartitionID
	PartitionName
	PartitionState
	PartitionType
	ResourceMonitoringControlState
	ResourceMonitoringIPAddress
	PartitionUUID
	AssociatedManagedSystemLink
	PowerVMManagementCapable
	OperatingSystemVersion
	OperatingSystemType
	Description
	PartitionMemoryConfiguration.SharedMemoryEnabled
	PartitionMemoryConfiguration.CurrentMemory
	PartitionProcessorConfiguration.CurrentHasDedicatedProcessors
	PartitionProcessorConfiguration.CurrentDedicatedProcessorConfiguration.CurrentProcessors
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.AllocatedVirtualProcessors
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.CurrentProcessingUnits
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.RuntimeProcessingUnits
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.CurrentSharedProcessorPoolID

VirtualIOServer	PartitionID
	PartitionName
	PartitionState
	PartitionType
	PartitionUUID
	ResourceMonitoringControlState
	ResourceMonitoringIPAddress
	AssociatedManagedSystemLink
	PowerVMManagementCapable
	OperatingSystemVersion
	OperatingSystemType
	Description
	PartitionMemoryConfiguration.SharedMemoryEnabled
	PartitionMemoryConfiguration.CurrentMemory
	PartitionProcessorConfiguration.CurrentHasDedicatedProcessors
	PartitionProcessorConfiguration.CurrentDedicatedProcessorConfiguration.CurrentProcessors
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.AllocatedVirtualProcessors
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.CurrentProcessingUnits
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.RuntimeProcessingUnits
	PartitionProcessorConfiguration.CurrentSharedProcessorConfiguration.CurrentSharedProcessorPoolID
ManagementConsole	ManagementConsoleName
	MachineTypeModelAndSerialNumber.MachineType
	MachineTypeModelAndSerialNumber.Model
	MachineTypeModelAndSerialNumber.SerialNumber
	ManagedSystemsLinks
	NetworkInterfaces.ManagementConsoleNetworkInterface.InterfaceName
	NetworkInterfaces.ManagementConsoleNetworkInterface.NetworkAddress
	VersionInfo.BuildLevel
	VersionInfo.Maintenance
	VersionInfo.Minor
	VersionInfo.Release
	VersionInfo.Version
	VersionInfo.ServicePackName
	ProcConfiguration.NumberOfProcessors
	ProcConfiguration.ModelName
	ProcConfiguration.Architecture
	MemConfiguration.TotalMemory
	MemConfiguration.TotalSwapMemory
	UVMID
	IPAddress
Cluster	UUID

	ClusterName
	ClusterID
	RepositoryDisk.PhysicalVolume.Description
	RepositoryDisk.PhysicalVolume.UniqueDeviceID
	RepositoryDisk.PhysicalVolume.VolumeCapacity
	RepositoryDisk.PhysicalVolume.VolumeName
	RepositoryDisk.PhysicalVolume.VolumeState
	RepositoryDisk.PhysicalVolume.IsFibreChannelBacked
	RepositoryDisk.PhysicalVolume.StorageLabel
	ClusterSharedStoragePoolLink
	Node.Node.HostName
	Node.Node.PartitionID
	Node.Node.State
	Node.Node.VirtualIOServerLevel
	Node.Node.VirtualIOServerLink
	Node.Node.MachineTypeModelAndSerialNumber.MachineType
	Node.Node.MachineTypeModelAndSerialNumber.Model
	Node.Node.MachineTypeModelAndSerialNumber.SerialNumber
	ClusterCapabilities.IsTierCapable
	ClusterCapabilities.IsTierMirrorCapable
SharedStoragePool	UUID
	MultiDataTierConfigured
	MultiFailureGroupConfigured
	Capacity
	FreeSpace
	TotalLogicalUnitSize
	StoragePoolName
	UniqueDeviceID
	AssociatedClusterLink
	AssociatedTiersLinks
	PhysicalVolumes.PhysicalVolume.Description
	PhysicalVolumes.PhysicalVolume.UniqueDeviceID
	PhysicalVolumes.PhysicalVolume.VolumeCapacity
	PhysicalVolumes.PhysicalVolume.VolumeName
	PhysicalVolumes.PhysicalVolume.VolumeState
	PhysicalVolumes.PhysicalVolume.IsFibreChannelBacked
	PhysicalVolumes.PhysicalVolume.StorageLabel
Tier	UUID
	Name
	UniqueDeviceID
	Type

IsDefault
FreeSpace
OverCommitSpace
Capacity
FreeSpaceThreshold
OverCommitSpaceThreshold
TotalLogicalUnitSize
MirrorState
AssociatedSharedStoragePoolLink
FailureGroups.FailureGroup.Name
FailureGroups.FailureGroup.UniqueDeviceID
FailureGroups.FailureGroup.Capacity
FailureGroups.FailureGroup.State
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.Description
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.UniqueDeviceID
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.VolumeCapacity
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.VolumeName
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.VolumeState
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.IsFibreChannelBacked
FailureGroups.FailureGroup.PhysicalVolumes.PhysicalVolume.StorageLabel

Performance Metrics Attributes :

Metrics Resource	Attribute Name
ManagedSystemPreferences	SystemName
	SystemUUID
	IsAggregationEnabled
	SystemMTMS
	IsEnergyMonitorEnabled
	ConsoleMTMS
SharedStoragePoolPreferences	ClusterName
	PoolName
	PoolId
	ClusterId
	SSPUUID
	IsAggregationEnabled
	ConsoleMTMS
ManagedSystemMetrics	AssignedMemToLpars
	ConsoleMTMS
	HEAPort.DRCIndex
	HEAPort.ID
	HEAPort.PhysicalLocation

	HEAPort.ReceivedPackets
	HEAPort.ReceivedPackets
	HEAPort.SentBytes
	HEAPort.SentPackets
	Network.ReceivedBytes
	Network.ReceivedPackets
	Network.SentBytes
	Network.SentPackets
	SharedMemoryPool.AssignedMemToLpars
	SharedMemoryPool.AssignedMemToSysFirmware
	SharedMemoryPool.TotalMemory
	SharedProcessorPool.AssignedProcUnits
	SharedProcessorPool.AvailableProcUnits
	SharedProcessorPool.ConfiguredProcUnits
	SharedProcessorPool.ID
	SharedProcessorPool.Name
	SharedProcessorPool.UtilizedProcUnits
	SRIOVPort.DRCIndex
	SRIOVPort.ID
	SRIOVPort.PhysicalLocation
	SRIOVPort.ReceivedPackets
	SRIOVPort.ReceivedPackets
	SRIOVPort.SentBytes
	SRIOVPort.SentPackets
	Storage.NumOfReads
	Storage.NumOfWrites
	Storage.ReadBytes
	Storage.WriteBytes
	SystemAvailableMemory
	SystemAvailableProcUnits
	SystemConfigurabelProcUnits
	SystemConfigurableMemory
	SystemFWAssignedMem
	SystemMTMS
	SystemName
	SystemTotalMemory
	SystemTotalProcUnits
	SystemUtilizedProcUnits
	SystemUUID
LogicalPartitionMetrics	ConsoleMTMS
	EntitledProcunits
	ID

	LPARUUID
	MemMode
	Name
	Network.ReceivedBytes
	Network.ReceivedPackets
	Network.SentBytes
	Network.SentPackets
	ProcMode
	SRIOVLogicalPortMetrics.DRCIndex
	SRIOVLogicalPortMetrics.LocationCode
	SRIOVLogicalPortMetrics.PhysicalPortDRCIndex
	SRIOVLogicalPortMetrics.PhysicalPortID
	SRIOVLogicalPortMetrics.ReceivedBytes
	SRIOVLogicalPortMetrics.ReceivedPackets
	SRIOVLogicalPortMetrics.SentBytes
	SRIOVLogicalPortMetrics.SentPackets
	State
	Storage.NumOfReads
	Storage.NumOfWrites
	Storage.ReadBytes
	Storage.WriteBytes
	SystemName
	SystemUUID
	UtilizedProcUnits
	VFCAdapterMetrics.LocationCode
	VFCAdapterMetrics.NumOfReads
	VFCAdapterMetrics.NumOfWrites
	VFCAdapterMetrics.ReadBytes
	VFCAdapterMetrics.VIOSID
	VFCAdapterMetrics.WriteBytes
	VFCAdapterMetrics.WriteBytes
	VirtualEthMetrics.IsPVID
	VirtualEthMetrics.LocationCode
	VirtualEthMetrics.ReceivedBytes
	VirtualEthMetrics.ReceivedPackets
	VirtualEthMetrics.SentBytes
	VirtualEthMetrics.SentPackets
	VirtualEthMetrics.VLANId
	VirtualEthMetrics.VSwitchID
	VSCSIAadapterMetrics.LocationCode
	VSCSIAadapterMetrics.NumOfReads
	VSCSIAadapterMetrics.NumOfWrites
	VSCSIAadapterMetrics.ReadBytes

	VSCSIAadapterMetrics.VIOSID
VirtualIOServerMetrics	AssignedMemory
	ConsoleMTMS
	EntitledProcUnits
	FCAdapterMetrics.ID
	FCAdapterMetrics.LocationCode
	FCAdapterMetrics.NumOfReads
	FCAdapterMetrics.NumOfWrites
	FCAdapterMetrics.ReadBytes
	FCAdapterMetrics.WriteBytes
	ID
	Name
	Network.ReceivedBytes
	Network.ReceivedPackets
	Network.SentBytes
	Network.SentPackets
	NetworkAdapterMetrics.ID
	NetworkAdapterMetrics.LocaionCode
	NetworkAdapterMetrics.ReceivedBytes
	NetworkAdapterMetrics.ReceivedPackets
	NetworkAdapterMetrics.SentBytes
	NetworkAdapterMetrics.SentPackets
	SEA.BridgedAdapters
	SEA.LocaionCode
	SEA.ReceivedBytes
	SEA.ReceivedPackets
	SEA.SentBytes
	SEA.SentPackets
	SRIOVLogicalPortMetrics.DRCIndex
	SRIOVLogicalPortMetrics.LocationCode
	SRIOVLogicalPortMetrics.PhysicalPortDRCIndex
	SRIOVLogicalPortMetrics.PhysicalPortID
	SRIOVLogicalPortMetrics.ReceivedBytes
	SRIOVLogicalPortMetrics.ReceivedPackets
	SRIOVLogicalPortMetrics.SentBytes
	SRIOVLogicalPortMetrics.SentPackets
	State
	Storage.NumOfReads
	Storage.NumOfWrites
	Storage.ReadBytes
	Storage.WriteBytes
	SystemName

	SystemUUID
	SystemUUID
	UtilizedMemory
	VirtualEthMetrics.IsPVID
	VirtualEthMetrics.LocationCode
	VirtualEthMetrics.ReceivedBytes
	VirtualEthMetrics.ReceivedPackets
	VirtualEthMetrics.SentBytes
	VirtualEthMetrics.SentPackets
	VirtualEthMetrics.VLANId
	VirtualEthMetrics.VSwitchID
SharedStoragePoolMetrics	ReadBytes
	WriteBytes
	NodeMetrics.ReadBytes
	NodeMetrics.WriteBytes
	NodeMetrics.VIOSName
	NodeMetrics.ID
	NodeMetrics.SystemMTMS
	NodeMetrics.TierMetrics.ReadBytes
	NodeMetrics.TierMetrics.WriteBytes
	NodeMetrics.TierMetrics.TierName
	ClusterName
	PoolName
	PoolID
	ClusterID
	ConsoleMTMS

Attributes required for the Logging app are computed and stored in a file in the local file system of HMC. Cloud connector reads this attributes and pushes it to CMC Cloud Database. Below are the attributes required by the logging app :

SourceCEC
DestinationCEC
SourceHMCIP
DestinationHMCIP
OperationResult
PartitionName
HMCUser
OperationType
NumOfConcurrentOperations
IsRemoteOperation
ErrorCodes
AbortSide
SPPName
SourceCECName
DestinationCECName
SourcePrimaryMSPName
SourceSecondaryMSPName
DestinationPrimaryMSPName
DestinationSecondaryMSPName
TotalMemoryTransferData
ConsoleMTMS

StartSuspendDelta
SuspendResumeDelta
ResumeCompleteDelta
EstimatedLineSpeedInMbits
AverageResumeLatencyInMillis
BytesSentDuringSpeculative
BytesSentDuringSuspend
BytesSentDuringResume
BytesDirtyAtResume
BytesDemandPaged
MigrationDurationInTB
NumOfLPARVirtualAdapters
LparConfigValidationTime
LparCleanUpTime

Proxies

For all outbound connections, proxies can be configured to provide added security. For the connections between cloud connector and the cloud portal, and between cloud connector and the database, a HTTP proxy can be used. Till 9.1.941.0 version of HMC, only authentication scheme that is supported is Basic Authentication. With 9.1.941.1 version of HMC, Cloud Connector supports Kerberos, LDAP, Digest-md5 based proxy server authentication apart from Basic authentication. While starting Cloud Connector, an attribute can be specified on authentication type to be used for the proxy connection. Default authentication used is Basic. The credentials used for the initial HTTP CONNECT request from the cloud connector to the proxy using Basic Authentication will not be encrypted. Since this connection will occur behind the firewall, it does not present a security concern. Once the SSL tunnel is established, all data leaving the proxy will be properly encrypted using the mechanisms described in Outbound Connection section.

For the connection between cloud connector and the data ingestion node, a SOCKS5 proxy must be configured prior to HMC 9.1.941.0. Again, basic authentication is the only authentication mechanism that is supported. With 9.1.941.0 version of HMC, Cloud Connector can connect to ingestion node using HTTP proxy only. So it is not mandatory to use the SOCKS5 proxy to connect ingestion node with the 9.1.941.0 and beyond.

When a proxy is configured during start-up using a basic authentication credential, the password provided is encrypted using a shared secret between the HMC CLI code and the cloud connector process. From this secret, a key is generated using Password Based Encryption with the MD5 and DES algorithms. The key and a salt are used to encrypt the password. The encrypted password is then saved to the filesystem where it is only accessible by the root user. Once the cloud connector process begins running as root, it reads the encrypted key and decrypts it to construct the initial HTTP CONNECT request to the proxy server. For the SOCKS5 server the password is also encrypted in the initial phase where it is transferred from the HMC CLI to the cloud connector process. However, due to the constraints provided by our data shipper process, the SOCKS5 proxy password is stored in clear text in the data shipper configuration file. For added security, the file is only accessible to the root user. When Basic Authentication is used for the initial HTTP CONNECT request with cleartext, there is not an urgent need for the password to be encrypted at rest since a motivated attacker could simply capture the network packets and discover the credentials this way. However, since all of this occurs behind the firewall in a secured data center, the threat of an attacker having access to the HMC is minimal. If it does occur, greater risks than the discovery of the proxy password surely exist.

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. In some cases, the hardware product may not be new and may have been previously installed. Regardless, our warranty terms apply.

Information concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of the non-IBM products should be addressed with those suppliers.

All performance information was determined in a controlled environment. Actual results may vary. Performance information is provided “AS IS” and no warranties or guarantees are expressed or implied by IBM. Buyers should consult other sources of information, including system benchmarks, to evaluate the performance of a system they are considering buying.

When referring to storage capacity, 1 TB equals total GB divided by 1000; accessible capacity may be less.

The IBM home page on the Internet can be found at:

http://www.ibm.com

The IBM Power Systems home page on the Internet can be found at:

http://www.ibm.com/systems/power