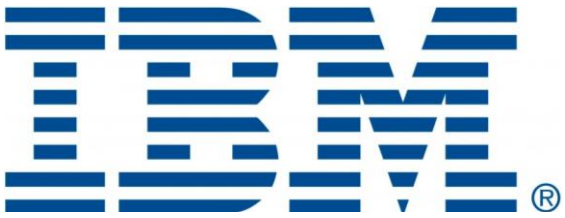


Connectivity Security White Paper

Microcode Data Collector 3.5.7

April 2018

Table of Contents

Introduction

This document describes the data that is exchanged between the Microcode Data Collector (MDC) and the IBM Service Delivery Center (SDC) and the methods and protocols for this exchange. The document includes the configuration of "Call Home" on the MDC installed device for automatic and manual collection of data and reporting. All the functionality that is described herein refers to MDC version 3.5.

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
AES	Advanced Encryption Standard
AMM	Advanced Management Module
HMC	Hardware Management Console
IP	Internet Protocol
MDC	Microcode Data Collector
SDC	Service Delivery Center
SNAT	Source Network Address Translation
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
WSH	Windows Scripting Host
WMI	Windows Management Instrumentation

Installation security considerations

MDC can be installed on any of the following operating environments. See MDC Setup Guide for details.

Windows

Management Requirements

- Some MDC functions are supported only when you run as an Administrator in Windows.

Internet access

The system on which you install MDC must have direct or SSL proxy internet access to support the automatic call home function. The function sends the collected report files to IBM.

AIX

Installation of MDC on AIX requires Root privileges.

Linux

Installation of MDC on Linux requires Root privileges.

MDC Connectivity Methods

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

Outbound Configurations

Outbound configurations are used to configure the MDC to connect back to IBM. The MDC connects to IBM for transmitting offering information. The types of data sent from MDC to IBM are covered in more detail in section – "Data sent to IBM from MDC".

Internet Connectivity

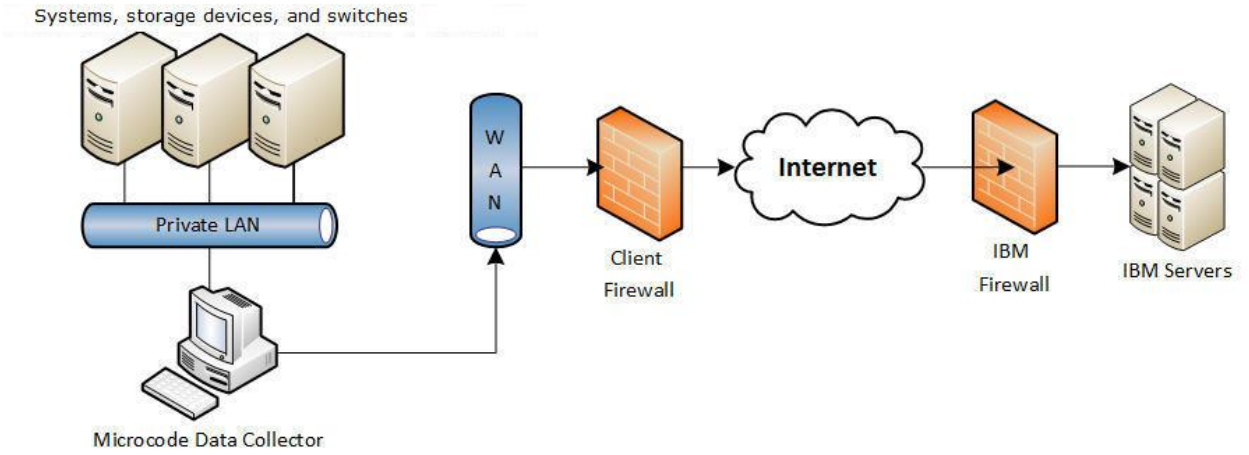
In this configuration, MDC uses a client-provided Internet connection to connect to IBM Support. All the communications are handled through TCP sockets (which always originate from the MDC). MDC uses SSL to encrypt the data that is being sent back and forth.

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

The MDC supports IP V4 connections.

Without Proxy Server

The following diagram shows an example of MDC connecting to IBM without a proxy server.

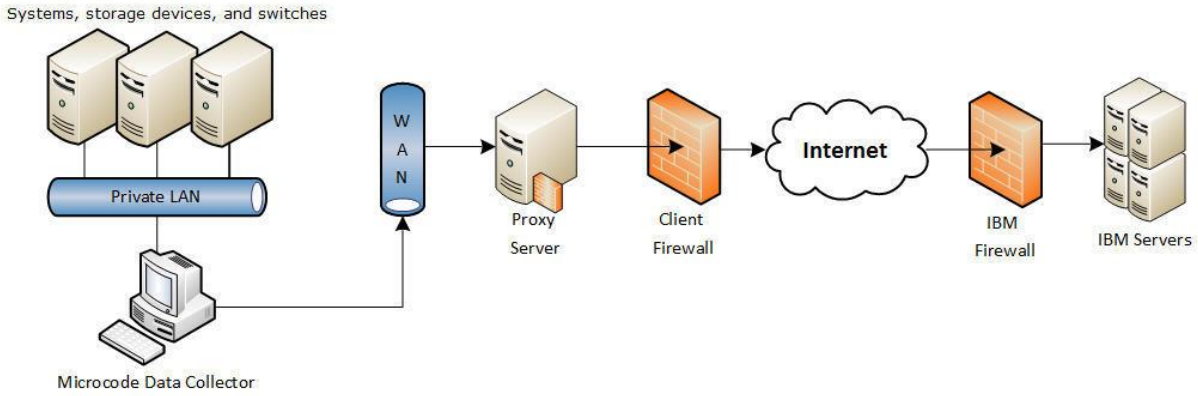


In this setup the MDC connects through the client-provided Internet connection by the default route.

For the MDC 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 MDC's source IP address are both acceptable.

With Proxy Server

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



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 MDC authenticates before it attempts to forward sockets through the proxy server.

Firewall Configurations

Simplified Connectivity

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, and enabling IPv6 connectivity. 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.

If you are installing MDC 3.5.1 or higher as the first install of MDC, configure the following IP addresses for MDC to communicate successfully over the client's firewall -

IP Address	Host Name	Port	Protocols	Purpose
129.42.54.189	esupport.ibm.com	443, 80	HTTPS	System configuration reporting, Fix download, Gateway, Problem Reporting, Service Providers, Status Reporting
129.42.56.189				
129.42.60.189				
2620:0:6c0:200:129:42:54:189				
2620:0:6c0:200:129:42:56:189				
2620:0:6c0:200:129:42:60:189				
170.225.15.31	testcase.boulder.ibm.com	21	ftps	Upload bulk data associated

				with status and problem reporting

- You must open the address range of 129.42.0.0 /18 to minimize churn in the future if additional addresses are added.

Traditional Connectivity

If you are installing MDC 3.5.1 or higher over a pre-existing version of MDC, this describes the current configuration. IBM recommends that you reconfigure as described under the 'Simplified connectivity' section, but this configuration will still work.

For the MDC to communicate successfully, the client's firewall must allow connections to port 443. The firewall must also allow specific IP addresses needed by MDC can connect. See the table below for the list of IP addresses –

IP Address	Host Name	Port	Protocols	Purpose
170.225.15.41	www6.software.ibm.com	443	HTTPS	System configuration reporting
192.109.81.20	www.ecurep.ibm.com	443	HTTPS	System configuration reporting
170.225.15.31	testcase.boulder.ibm.com	21	ftps	Upload bulk data associated with status and problem reporting
204.146.30.17	www.ibm.com	443	HTTPS	Request & request configuration updates
207.25.252.197	eccgw01.boulder.ibm.com	443	HTTPS	Upload data
129.42.160.51	eccgw02.rochester.ibm.com	443	HTTPS	Upload data
129.42.26.224 129.42.34.224 129.42.42.224	www-945.ibm.com	443		Problem reporting server v4
170.225.15.76	download3.boulder.ibm.com	80, 443		Fix download

129.35.224.114	download3.mul.ie.ibm.com	80, 443		Fix download
170.225.15.107	download4.boulder.ibm.com	80, 443		Fix download
129.35.224.107	download4.mul.ie.ibm.com	80, 443		Fix download
170.225.15.104 129.35.224.104	delivery04-bld.dhe.ibm.com	80, 443		Fix download (only applies to restricted updates)
129.35.224.115 170.225.15.115	delivery04-mul.dhe.ibm.com	80, 443		Fix download (only applies to restricted updates)
129.35.224.105 170.225.15.105	delivery04.dhe.ibm.com	80, 443		Fix download
170.225.15.103 129.35.224.103	delivery03-bld.dhe.ibm.com	80, 443		Fix download (only applies for dynamic ISOs through eFactory)
129.35.224.113 170.225.15.113	delivery03-mul.dhe.ibm.com	80, 443		Fix download (only applies for dynamic ISOs through eFactory)
170.225.15.124	dsw.boulder.ibm.com	80, 443		Fix download (only applies for entitled SWG updates)
129.35.224.124	dsw.mul.ie.ibm.com	80, 443		Fix download (only applies for entitled SWG updates)
170.225.15.108 129.35.224.108	dsw-bld.dhe.ibm.com	80, 443		Fix download (only applies for entitled SWG updates)
129.35.224.109 170.225.15.109	dsw-mul.dhe.ibm.com	80, 443		Fix download (only applies for entitled SWG updates)
129.35.224.110 170.225.15.110	dsw.dhe.ibm.com	80, 443		Fix download (only applies for entitled SWG updates)

129.35.224.103				

Inbound Configurations

Configuring the MDC will enable outbound communications to only IBM Support. MDC does not allow externally initiated inbound connectivity.

Service information exchanged with IBM

This section outlines the service information that is sent to IBM and the reasons for sending this information to IBM Service Delivery Center.

Reasons for Connecting to IBM

The reason for connecting to IBM is to transmit offering data to IBM.

Data sent to IBM from MDC

The table below lists the files that might be sent to IBM, and the short descriptions of the contents of those files. Along with the information contained in these files, the MDC also sends back client contact information, machine model and serial numbers, and debug traces for MDC software.

Device type	File	Description
IBM DS6000 and DS8000 Storage Systems.	dscli.cfg	File contains the data collection for the IBM DS6000 and DS8000 Storage Systems.
IBM XIV Storage Systems	xiv.cfg	File contains the data collection for the IBM XIV Storage Systems.
IBM XIV Storage Systems	xiv_snap_supportdata\system_xray_<machineType><machineModel><machineSerial>_yyyy-mm-dd-hhmm.tar.bz2	File contains the PSC data collection for the IBM XIV Storage Systems.
Systems running IBM Spectrum Virtualized Software	svc.cfg	File contains data collection for those storage devices which run IBM Spectrum Virtualized Software such as the IBM FlashSystem V9000, IBM San Volume Controller (SVC), IBM Storwize V3700 Disk System, IBM Storwize V7000, IBM Storwize V5000, IBM FlashSystem 840 / 900 Storage Controller Enclosure.
Systems running IBM Spectrum Virtualized Software	SVC_SNAP.<project>.svc.<modelType>.<SerialNo>.<timestamp>.tar.gz	File contains PSC data collection for those storage devices which run IBM Spectrum Virtualized Software such as the IBM FlashSystem V9000, IBM San Volume Controller (SVC), IBM Storwize V3700 Disk System, IBM Storwize V7000, IBM Storwize V5000, IBM FlashSystem 840 / 900 Storage Controller

		Enclosure.
IBM DS3000, DS4000 and DS5000 storage systems	smcli.cfg	File contains the data collection for the IBM DS3000, DS4000, and DS5000 storage systems.
IBM DS3000, DS4000 and DS5000 storage systems	smcli_supportdata\MDC.<project>.dsmidrange.<modelType>.<SerialNo>.<timestamp>.zip smcli_supportdata\MDC.<project>.pm.<modelType>.<SerialNo>.<timestamp>.txt	File contains the PSC data collection for the IBM DS3000, DS4000 and DS5000 storage systems.
IBM N Series Storage Systems.	nseries.cfg	File contains the data collection for the IBM N Series Storage Systems.
IBM ProtecTIER TS7610, TS7650 and TS7650G systems.	pt.cfg	File contains the data collection for the IBM ProtecTIER TS7610, TS7650 and TS7650G systems.
IBM ProtecTIER TS7610, TS7650 and TS7650G	ProtecTier_<hostname>_basic_<Mon>_<d>_<year>_<hh>_<mm>_<ss>_Report.tar	File contains the PSC data collection for the IBM ProtecTIER TS7610, TS7650 and TS7650G systems.
IBM 3494 and IBM 3953 Tape Libraries	lm.cfg	File contains the data collection for the IBM 3494 and IBM 3953 Tape Libraries.
IBM TS3500 Tape Libraries.	TS3500CLI.cfg	File contains the data collection for the IBM TS3500 Tape Libraries.
IBM TS3500 Tape Libraries.	TS3500.<projectName>.<hostname_or_ip>.<timestamp>.zip	File contains the PSC data collection for the IBM TS3500 Tape Libraries.
IBM SAN and LAN networking devices	sanswitch.cfg	File contains the data collection for the IBM SAN and LAN networking devices.
IBM SAN and LAN networking devices	SWITCH_SNAP.<project>.<switchType>.<MTMS>.hostname.<timestamp>.gz	File contains the PSC data collection for the IBM SAN and LAN networking devices.
IBM Power Systems that run AIX and AIX VIOS.	Rpt.VAP.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.<machineId>.<timeStamp>.tar.Z	File contains the data collection for the IBM Power Systems that run AIX and AIX VIOS.

IBM Power Systems (including Power LC) that host Linux operating system.	Rpt.VLP.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.<platform>.tar.Z	File contains the data collection for the IBM Power Systems that host Linux operating system.
IBM Power Systems that host IBM i operating systems	iseries.cfg	File contains the data collection for the IBM Power Systems that host IBM i operating systems.
IBM Power Systems that host IBM i operating systems	iseries_snap.MDC.<hostname>.<timestamp>.zip	File contains the PSC data collection for the IBM Power Systems that host IBM i operating systems.
IBM Hardware Management Consoles (HMCs).	hmc.cfg	File contains the data collection for the IBM Hardware Management Consoles (HMCs).
IBM Flex System Manager (FSM).	fsm.cfg	File contains the data collection for the IBM Flex System Manager (FSM).
IBM Bladecenter and Flex Chassis.	For AMM - bladeCenters\MDC.<projectName>.<type>.<modelnumber>.<serialNumber>.<timestamp>.service.txt For CMM - bladeCenters\MDC.<projectName>.<type>.<modelnumber>.<serialNumber>.<timestamp>.service.tgz	File contains the data collection for the IBM Bladecenter and Flex Chasis.
IBM System x devices.	dsa\<modelTypeNumber>_<serialNumber>_<yyyymmdd>-<hhmmss>.xml.gz	File contains the data collection for the IBM System x devices.
IBM System x devices that run Linux	Rpt.VLX.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.<platform>.tar.Z	File contains the data collection for the IBM System x devices that run Linux.
IBM ESXi hipervisors	dsa\<modelTypeNumber>_<serialNumber>_<yyyymmdd>-<hhmmss>.xml.gz	File contains the data collection for the IBM ESXi Systems.

IBM System z devices.	Rpt.VLZ.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.s39.tar.Z	File contains the data collection for the IBM System z devices.
SAP HANA / SAP BWA	<SAP_SystemID>_<hanaORbwa>_<bladeCenterMachineType>_<bladeCenterSerialNumber>_<yyyyMMddHHmmss>.zip	File contains the data collection for the SAP HANA / SAP BWA devices.

Data retrieved from IBM by MDC

MDC retrieves any MDC software updates from IBM, and information about the IP addresses / ports that are used when sending data to IBM. All communications are initiated by the customer machine having MDC, not by IBM.

Security Protocols and Encryption

Communication between MDC and IBM

Microcode Data Collector (MDC) primarily uses the HTTPS protocol for transmission of data between your site and the IBM Solution Delivery Center. The HTTP protocol serves as a backup path for downloading new configuration information when an appropriate HTTPS path cannot be established. Your data is never uploaded using the HTTP protocol.

HTTPS is achieved by encapsulating the HTTP application protocol within either the Transport Layer Security (TLSv1) cryptographic protocol or the Secure Socket Layer (SSLv3) cryptographic protocol.

Communication between MDC and the reporting end point

Passwords

All Device Passwords and passphrases for keys are encrypted using AES before saving to the file system.

Communication protocols used for various devices

IBM DS6000 and DS8000

MDC communicates through the IBM DS command line interface (DSCLI) for data collection from IBM DS6000 and DS8000 Storage Systems. MDC uses user ID/password based authentication to collect information for the IBM DS6000 and DS8000 Storage Systems.

IBM XIV Storage Systems

MDC communicates through the IBM XIV Storage System command-line interface (XCLI) for data collection from IBM XIV Storage Systems. The XCLI provides a mechanism for issuing commands to manage and maintain the XIV systems. MDC uses user ID/password based authentication to connect to the controllers physically that are located within IBM XIV Systems.

Systems running IBM Spectrum Virtualized Software

MDC uses SSH2 protocol [default port 22] with either public/private key or username/password based authentication to collect data from system running IBM Spectrum Virtualized Software.

IBM DS3000, DS4000 and DS5000

MDC communicates through the IBM system management command-line interface (SMCLI) for data collection from IBM DS3000, DS4000, and DS5000 storage systems. The SMCLI is a utility that you can use to perform system management tasks from the command line. MDC connects to the FAStT controllers of DS3000, DS4000, and DS5000 storage systems to collect data.

IBM N Series Storage Systems

MDC uses SSH [default port 22] or Telnet [default port 23] protocol with user ID/password based authentication to collect data from IBM N series Storage Systems that run on Data ONTAP OS. MDC also supports connecting to Remote LAN Management (RLM) and Service Processor (SP) firmware ports through SSH protocol. For RLM / SP, MDC logs in to the Data ONTAP through firmware and collects data.

IBM ProtecTIER Systems

MDC uses SSH protocol [default port 22] with user ID/password based authentication to collect data from IBM ProtecTIER TS7610, TS7650 and TS7650G systems.

IBM 3494 and IBM 3953 Tape Libraries

MDC uses Telnet protocol [default port 23] with user ID/password based authentication to collect data from IBM 3494 and IBM 3953 Tape Libraries. MDC communicates with the Library Mangers that are physically located inside IBM 3494 and IBM 3953 Tape Libraries.

IBM TS3500 Tape Libraries

MDC uses HTTP protocol [default port 80] and / or HTTPS protocol [default port 443] with user ID/password based authentication (optional) to collect data from IBM TS3500 Tape Libraries.

SAN / LAN Networking

MDC uses SSH [default port 22], Telnet protocol [default port 23] with user ID/password based authentication to collect data from SAN and LAN networking devices. MDC can collect data from BNT switch that is configured either through `ibmnos-cli` or `is-cli` interface.

IBM Power Systems

MDC uses SSH protocol [default port 22] with either user ID / password or public/private key based authentication to collect data from IBM Power systems. For user ID/password authentication, you can use 'padmin' user ID to collect data from VIOS and 'root' / sudo user ID (with root privileges) to collect data from AIX or Linux.

- Normal user (without any root access) credentials reports limited data collection on IBM Power Systems. For the commands which need root access, the execution result is not listed in the collection report. Normal user can run basic and extended collection on Power Linux but only basic collection on AIX.

IBM i Systems

MDC uses AS400 protocol with user ID/password based authentication to collect data from IBM i systems.

IBM HMCs

MDC uses SSH protocol [default port 22] with user ID/password based authentication to collect data from IBM Hardware Management Consoles (HMCs).

IBM Flex System Manager

MDC uses SSH protocol [default port 22] with user ID/password based authentication to collect data from IBM Flex System Manager (FSM).

IBM Bladecenter and Flex Chassis

MDC uses SSH protocol [default port 22] with user ID/password based authentication to collect data from Advanced Management Module (AMM) or Chassis Management Module (CMM) that is physically located on the chassis.

IBM System x

The Microcode Data Collector uses the Dynamic System Analysis (DSA) tool to collect data on System x systems. MDC uses SMB protocol [default port 445] authentication for Microsoft Windows, and SSH protocol [default port 22] for Linux. MDC can also function as a FTP Server to be used by the FTP client built into DSA while executing on the machine.

Many operations that MDC performs require access to resources that are not generally accessible by ordinary user accounts. Therefore, for all target platforms, the account names that you use to log onto remote machines must have administrative privileges on each of the target machines. For more information on target-specific requirements, see section For System x (Widnows).

ESXi

MDC uses SSH [default port 22] and HTTP protocol [default port 80] with user ID / password based authentication to collect data using DSA pointing to hypervisor. MDC connects to ESXi systems through IBM System x® (system to run DSA) machines to collect data.

Linux on System z

MDC uses SSH Protocol with user ID / password based authentication to collect data from System z (Linux) systems.

IBM SAP HANA / BWA

The IBM SAP HANA / BWA appliance consists of a BladeCenter (or Flex Chasis) including various System X blades or System x ITEs, Ethernet switch modules, and fiber channel switch modules. The switch modules can be from CISCO, QLogic, Brocade, or BNT.

MDC uses Linux user ID and password to authenticate and connect to all System x blades or servers. IBM SAP HANA / BWA appliance can collect data from System x devices, BladeCenter, SAN/LAN networking devices, DS3000, DS4000, and DS5000 devices.

- IBM SAP HANA appliance does not have any storage devices, but MDC supports to associate the storage devices to SAP HANA and collect data

Setting up public and private key authentication

To support secure data collection from systems running IBM Spectrum Virtualized Software and IBM Power Systems that are running AIX, Linux, or VIOS, you can use public and private key authentication over the SSH protocol. For information on generating public/private key pairs, see the MDC Setup Guide.

Key Management

The Key Management feature of MDC allows you to configure the private keys that are used to connect to the devices. You have to specify the location of the private key.

For example: c:\docume~1\Administrator\.ssh\id_private.

For the Public/private key authentication, you can also enter a passphrase. For example: mypassphrase.

Specifying a passphrase enhances the security of the private key file. A good passphrase contains both alphabetic and numeric characters and is at least 10 characters long.

Data Collection

The following table lists all the commands that are invoked on the respective devices to collect data. The table also describes the output file directory, where the data is stored and mapped for collecting data manually.

Device	Output file name	Commands
The respective output files for the following devices are stored in a zip file at this location: MDC_INSTALLED_LOCATION\collection\mdc\filename.zip		
IBM DS6000 and DS8000	dscli.cfg	DSCLI_DIR/bin/lshostvol.sh lssu lsserver -fmt delim -l $suid/0 lsserver -fmt delim -l $suid/1 lskey -fmt delim $suid lsfbvol -fmt delim -dev $suid -l showsu $suid showsi $suid lsstgencl -fmt delim -l $suid lsddm -fmt delim -l $suid lsioport -fmt delim -dev $suid -l lshostconnect -fmt delim -dev $suid -l lsarraysite -fmt delim -dev $suid -l lsarray -fmt delim -dev $suid -l lsrank -fmt delim -dev $suid -l
IBM XIV Storage Systems	xiv.cfg For PSC data, navigate to the folder: xiv_snap_supportdata\ system_xray_<machine Type><machine Model><machineSerial>_yyyy-mm-dd-hhmm.tar.bz2	version_get config_get vpd_config_get user_group_list user_list cg_list dm_list dest_list destgroup_list event_list event_list_uncleared rule_list smsgw_list smtpgw_list fc_connectivity_list fc_port_list host_connectivity_list component_list disk_list module_list service_list switch_list ups_list cluster_list host_list ipinterface_list ipinterface_list_ports

		mirror_list target_connectivity_list target_list target_port_list snap_group_list pool_list psu_list state_list system_capacity_list time_list reservation_key_list reservation_list vol_list support_center_list smtpgw_list internal=yes metadata_list node_list alive=no For PSC - vol_mapping_list system_logs_collect system_logs_get_status system_logs_get_file_fragment
Systems running IBM Spectrum Virtualized Software	svc.cfg For PSC data, navigate to the folder 'svc_snap_supportdata' to find an individual output file in this format for each device - \SVC_SNAP.<project>.svc.<modelType>.<SerialNo>.<timestamp>.tar.gz	lscluster lsnode lscontroller lscimomdumps lsclustercandidate lscopystatus lsdiscoverystatus lsemailuser lsfabric lsfcconsistgrp lsfcmap lsmdisk lshbaportcandidate lshost lsiogrp lsiogrpcandidate lslicense lsmdiskcandidate lsmdiskgrp lsmigrate lsnodecandidate lsrcconsistgrp lsrcrelationship lsrcrelationshipcandidate lsvdisk lsenclosure lsquorum lsdisk lsdrive lssnmpserver lshostiogrp lshostvdiskmap

		lsnodevpd lsenclosurecanister lsservicestatus lssystem For PSC - lsvdiskcopy lsvdiskdependentmaps lsvdiskextent lsvdiskfcmappings lsvdiskhostmap lsvdiskmember lsfreeextents lsmdiskextent lsmdiskmember lsiogrphost lsfcmapprogress svc_snap
IBM DS3000, DS4000 and DS5000	smcli.cfg For PSC data, navigate to the folder 'smcli_supportdata' to find an two output file in below formats for each device - \MDC.<project>.dsmidrange.<modelType>.<SerialNo>.<timestamp>.zip - \MDC.<project>.pm.<modelType>.<SerialNo>.<timestamp>.txt	show storageSubsystem summary show storageSubsystem healthStatus show storageSubsystem batteryAge show storageSubsystem hotSpareCoverage show allControllers show allHostPorts show allDriveChannels stats show allDrives show allLogicalDrives show storageSubsystem lunMappings show storageSubsystem hostTopology show storageSubsystem profile For PSC - save storageSubsystem supportdata on error stop set performanceMonitor interval=5 iterations=60 upload storageSubsystem file=\MDC.<project>.pm.<modelType>.<SerialNo>.<timestamp>.txt content=performanceStats
IBM NSeries Storage Systems	nseries.cfg	version version -b hostname uptime sysconfig -av sysconfig -c sysconfig -d sysconfig -h sysconfig -m sysconfig -M sysconfig -r sysconfig -t sysconfig -V storage show environment status environment status chassis all df -k

		aggr status -v aggr show_space vol status -v lun show -v all disk show -v ifconfig -a netstat -rn ifstat -a fcstat link_stats fcstat fcal_stats license bmc status cifs stat sasadmin dev_stats sasadmin adapter_state sasadmin expander_map sasadmin expander_phy_state sasadmin shelf sasadmin shelf_short sasadmin channels rdfile /etc/messages snap sched snap reserve snapmirror status snap list snap list -A snap reserve -A rlm status nfs status cifs shares dns info rdfile /etc/hosts rdfile /etc/nsswitch.conf nis info fcp show adapter iscsi initiator show qtree status options rdfile /etc/rc cf status cf monitor
IBM ProtecTIER Systems	pt.cfg For PSC data, navigate to the folder 'ptcli_supportdata' to find an individual output file in the following format for each device - ProtecTier_<hostname>_basic_	ping -w 5 172.31.1.1 telnet 172.31.1.1 /usr/sbin/dmidecode -s system-serial-number cat /opt/ras/persist/rsCerCfgAutorunMTM cat /opt/dtc/app/sys/verinfo /opt/ras/bin/rsCerCHDisplayMRPD /opt/ras/bin/versions For PSC - /opt/dtc/app/sbin/report_problem -inputfile <afile> -profile basic The contents of input file <afile> - Customer: MDC ProtecTIER server's OS is MDC Host OS is MDC Backup application is MDC Problem description: MDC

	<Mon>_<d>_<year>_<hh>_<mm>_<ss>_Report.tar Where, Mon – Month d – Day year – Year	
IBM 3494 and 3953 Tape Libraries	lm.cfg	CHKFINS FMTDBFLS.EXE TYPE FMTDBFLS.TXT
IBM TS3500 Tape Libraries	TS3500CLI.cfg For PSC data, navigate to the folder 'ts3500_extended_support_info' to find an individual output file in the following format for each device - \TS3500.<projectName>.<hostname_or_ip>.<timestamp>.zip	ViewLibraryVPD viewNodeCards viewDriveVPD **For PSC -** http://<host>/FS/LIBLG_00_MR http://<host>/FS/LIBLG_00_ER http://<host>/FS/LIBLG_00_VP http://<host>/FS/LIBLG_00_NV downloadLogs ALL **For Each of the Node -** http://<host>/FS/LIBLG_<Node>_EM http://<host>/FS/LIBLG_<Node>_EA **For each of the Tape Drive -** http://<host>/FS/DRIVE_DRIVE_<N>_<N+1> ; where N = (1 - 16)
SAN/LAN Networking	sanswitch.cfg For PSC data, navigate to the folder 'sansw_snap_supportdata' to find an individual output file in - the following format for each device - \SWITCH_SNAP.<project>.<switchType>.<MTMS>.hostname.<timestamp>.gz Where, switchType is Brocade, Cisco, Juniper	**For Brocade Switches** moreDisable date switchshow version firmwareshow switchstatusshow chassisshow tempshow sensorshow psshow fabricshow fabricswitchshow cfgshow nsshow portzoneshow porterrshow sfpshow diagshow dlsshow hashow memshow ipaddrshow slotshow

		PSC Command: snmpconfig --show snmpv1 snmpconfig --show snmpv3 supportShow **For Brocade-McData SAN Switches** show all **For Cisco Switches** terminal length 0 show switchname show wwn switch show wwn vsan-wwn show interface mgmt0 show hardware show environment show clock show cfs internal vsan database show interface brief show system health statistics show system resources show vsan show vsan membership show zone active show ip interface show topology show fcs database show fspf database show fcns database show flogi database show interface show version PSC Command: show tech-support **For Juniper Switches** show version show chassis hardware show interfaces **PSC Command -** request support information **For BNT Switches – IBM-NOSCLI mode** /info/sys/general /info/dump PSC Command: /stats/dump /cfg/cur **For BNT Switches – IBM-ISCLI mode** show information-dump PSC Command: show counters show running-config

<table>
<tr><td></td><td></td><td>For QLlogic Switches
show support</td></tr>
<tr><td rowspan="2">IBM Power Systems</td><td colspan="2">MDC 3.5.6 and higher versions support data collection by normal user (without any root access) on IBM Power Systems. The collection report that is run by normal user is a subset of the complete report run by root or sudo user.
Commands which need root access are indicated below.</td></tr>
<tr><td>For AIX

Rpt.VAP.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.<machineId>.<timeStamp>.tar.Z
where prowebId can be null</td><td>For AIX/VIOS

umask 002
hostname -s
host $HOST_SHORT | cut -f 1 -d " "
uname -m
pwd
which lsvpd
/usr/sbin/lsvpd (root)
lsattr -El sys0 -a systemid
lslpp -l perl.rte
lslpp -l bos.rte.serv_aid
whence powermt
whence dlnkmgr
whence gzip
oslevel
typeset -i OS_LEVEL
uname -x
uname -r
uname -v
lsdev -C

For each tape:
tapeutil -f /dev/$tape devinfo
tapeutil -f /dev/$tape path
tapeutil -f /dev/$smc inquiry
tapeutil -f /dev/$tape logpage 0x0C

cp /etc/objrepos/Cu*
cp /etc/objrepos/CD*
cp /usr/lib/objrepos/Pd*
cp /usr/lib/objrepos/fix*
cp /usr/lib/objrepos/history*
cp /usr/lib/objrepos/lag*
cp /usr/lib/objrepos/lpp*
cp /usr/lib/objrepos/product*
cp /usr/lib/objrepos/vendor*
cp /var/adm/ras/errlog
cp /var/adm/ras/errtmplt
cp /var/adm/ras/codepoint.cat
cp /var/adm/ras/bootlog
cp /etc/lpp/diagnostics/data/diagrpt*
bootinfo -r (root)
bootinfo -K (root)
/usr/sbin/prtconf
lslicense (root)</td></tr>
</table>

		svmon -G /usr/sbin/vmo -FL (root) /usr/sbin/ioo -FL (root) lvmo -v (root) For each lsvg: /usr/sbin/nfso -FL (root) /usr/sbin/schedo -FL (root) vmstat -v (root) oslevel -s instfix -iv |grep AIX_ML |awk ' /Not/ {print $5} ' instfix -iv |grep AIX_ML |awk ' /All/ {print $4} ' lssrc -a lsps -s lsps -a sysdumpdev -L (root) sysdumpdev -l (root) sysdumpdev -e (root) df lsfs mount lspv For each volume group vg using lsvg ls -la /dev/$vg lsvg $vg lsvg -l $vg lsvg -p $vg For each $spv using lspv lspv -l $spv lspv -p $spv lparstat -i lparstat -H lsslot -c slot lsslot -c phb lsslot -c pci lsslot -c port smtctl (root) lslpp -L emgr -l (root) emgr -lv3 (root) For each sissas device $device found using lsdev -C sissasraidmgr -Tl $device -j3 (root) sissasraidmgr -L -j1 -l $device (root) sissasraidmgr -Tl $device -j3 -o1 (root) lspath -F status:name:path_id:parent:connection -s All pcmpath query version pcmpath query adapter pcmpath query device pcmpath query adaptstats pcmpath query devstats pcmpath query portmap pcmpath query essmap

		pcmpath query wwpn fget_config -Av whence powermt version whence powermt display dev=all whence powermt display paths whence powermt display ports whence dlnkmgr view -sys -sfunc whence dlnkmgr view -sys -msrv whence dlnkmgr view -sys -pdrv whence dlnkmgr view -drv whence dlnkmgr view -lu whence dlnkmgr view -path /usr/lpp/EMC/Symmetrix/bin/inq.aix64_51 -sid -showvol For each line($line) of /usr/sbin/lsvpcfg datapath query adapter $line datapath query device $line datapath query adaptstats $line datapath query devstats $line For each root volume group($rvg) identified using lsvg | grep -v rootvg hd2vp $rvg /usr/sbin/lswpar -L /usr/sbin/lssrad -va /usr/sbin/lsrset -a -v exportfs lsfs -v nfs nfsstat nfsstat -m lppchk -v lscfg -vp /usr/sbin/lsmcode -A /usr/bin/fcstat netstat -v netstat -m netstat -in netstat -rn vmstat -I iostat -a iostat -RDTl mpstat -s mpstat -a cpuextintr_ctl -Q (root) /usr/bin/amepat /usr/sbin/lsnim -l /opt/ibm/mdc/system/bin/lsc -m /usr/sbin/raso -FL (root) /usr/sbin/bosdebug -L (root) /usr/sbin/chedition -l (root) /usr/esa/bin/esacli status (root) /usr/bin/rpm -qai (root) Some request from specific customers

		whence opcagt whence splunk /usr/lpp/OV/bin/opcagt -version `whence puppet` agent --version /splunk/splunkforwarder/bin/splunk --version For VIOS (In addition to above) /usr/ios/cli/ioscli ioslevel /usr/ios/cli/ioscli license /usr/ios/cli/ioscli lslparinfo /usr/ios/cli/ioscli lsfware /usr/ios/cli/ioscli lsmap -all -net /usr/ios/cli/ioscli lsmap -all /usr/ios/cli/ioscli lssw /usr/ios/cli/ioscli lstcpip -adapters /usr/ios/cli/ioscli lstcpip -state /usr/ios/cli/ioscli lstcpip -routtable /usr/ios/cli/ioscli lstcpip -adapters /usr/ios/cli/ioscli lspath /usr/ios/cli/ioscli lssp For each ethernet adapter /usr/ios/cli/ioscli entstat -all $ent for storagepools /usr/ios/cli/ioscli lssp -detail -sp /usr/ios/cli/ioscli viostat -path -adapter -sys /usr/ios/cli/ioscli lsnports /usr/ios/cli/ioscli lsmap -npiv -all /usr/ios/cli/ioscli lsmap -all -ams PSC DATA (VIOS and AIX) cp /etc/perf/daily - latest 6 files /usr/sbin/snap -gtnfpsABbLRwh -d tempDirectory (root)
IBM Power Systems	**For Linux** Rpt.VLP.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.<platform>.<timeStamp>.tar.gz where prowebId can be null	**Linux** hostname -s uname -m uname -a uname -p which lsvpd head -1 /etc/SuSE-release cat /etc/SuSE-release head -1 /etc/redhat-release cat /etc/redhat-release head -1 /etc/debian_version cat /etc/debian_version uname -rs cat /etc/lvm/lvm.conf dmsetup ls --tree (root) hostname ls -l /boot multipath -ll (root) parted -l (root) rpm -qa

		lszcrypt cat /etc/fstab df mount showmount -a lsqeth /proc/ppc64/lparcfg dmidecode ls -l /dev lspci (root) cat /proc/cmdline cat /proc/cpuinfo dmesg lsblk lsmod lsscsi ps -eLf swapon -s (root) sysctl -a (root) lsdasd lvs (root) pvs (root) vgs (root) cat /proc/meminfo cat /proc/slabinfo (root) free -m ipcs -a ifconfig -a (root) ip addr route -n (root) uptime lsdev lsfg -vp (root) lsvpd (root) lsmcode -A (root) /sbin/lvmdiskscan chkconfig --list systemctl list-unit-files chkconfig (root) systemctl list-unit-files For each tape($lmcp) identified using lsdev -Cc tape \| grep lmcp mtlib -l /dev/$lmcp –qL For each rmt tape mtlib -l /dev/$lmcp -f /dev/$rmt -qD mtlib -l /dev/$lmcp -qI -v mtlib -qC -sCCC -l/dev/$lmcp For each tape($smc) identified using lsdev -C \| grep smc tapeutil -f /dev/$smc devinfo tapeutil -f /dev/$smc path tapeutil -f /dev/$smc inquiry tapeutil -f /dev/$smc elementinfo tapeutil -f /dev/$smc devids tapeutil -f /dev/$smc inventory

		For each tape($rmt) identified using lsdev -C \| grep rmt tapeutil -f /dev/$rmt devinfo tapeutil -f /dev/$rmt path tapeutil -f /dev/$rmt logpage 0x0C PSC DATA (Linux) sosreport -l sosreport --batch supportconfig -D -b -t
IBM Power Systems	**For IBM i** C:\opt\ibm\mdc\collection\mdc\iseries.cfg For PSC data, navigate to the folder 'iseries_support data' to find an individual output file in the following format for each device - iseries_snap.MDC.<hostname>.<timestamp>.zip <modelNumber>.<machineType>.<machineSerialNumber>.<projectName>.DSPFMWTS.txt <modelNumber>.<machineType>.<machineSerialNumber>.<projectName>.DSPHDWRSC.txt <modelNumber>.<machineType>.<machineSerialNumber>.<projectName>.PRTERRLOG.txt <modelNumber>.<machineType>.<machineSerialNumber>.<projectName>.PTFGROUP.txt <modelNumber	**IBM i** DSPFMWTS DSPHDWRSC PRTERRLOG PTFGROUP DSPPTF

	>.<machineType>.<machineSerialNumber>.<projectName>.DSPPTF.txt	
IBM HMCs	hmc.cfg	lshmc -V uname -n lshsc -v lssyscfg -r sys lspartition -dlpar lssvcevents -t hardware -d 31 lssvcevents -t console -d 31 date netstat -in lshmc -b lshmc -n lshmcfs lslparmigr -r manager lssysconn -r all For each of the managed systems or lpars lshwres -m MANAGED_SYSTEM -r hea --rsubtype logical --level sys lshwres -m MANAGED_SYSTEM -r hea --rsubtype logical --level port lshwres -m MANAGED_SYSTEM -r hea --rsubtype phys --level sys lshwres -m MANAGED_SYSTEM -r io --rsubtype slot lshwres -m MANAGED_SYSTEM -r mem --level sys lshwres -m MANAGED_SYSTEM -r mem --level lpar lshwres -m MANAGED_SYSTEM -r mempool lshwres -m MANAGED_SYSTEM -r proc --level sys lshwres -m MANAGED_SYSTEM -r proc --level lpar lshwres -m MANAGED_SYSTEM -r procpool lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype eth --level sys lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype eth --level lpar lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype fc --level sys lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype fc --level lpar lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype scsi --level lpar lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype serial --level lpar lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype slot --level sys lshwres -m MANAGED_SYSTEM -r virtualio --rsubtype slot --level lpar lssyscfg -m MANAGED_SYSTEM -r lpar lssyscfg -m MANAGED_SYSTEM -r prof lsavailres -m MANAGED_SYSTEM lslic -m MANAGED_SYSTEM lslparmigr -m MANAGED_SYSTEM -r lpar

		lslparmigr -m MANAGED_SYSTEM -r sys lslparutil -r all -m MANAGED_SYSTEM -d 31 -s h
IBM Flex System Manager	fsm.cfg	lsconfig -V lsconfig -v smcli lsChassis
IBM BladeCenter and Flex Chassis	AMM - C:\opt\ibm\mdc\collection\bladeCenters\MDC.<projectName>.<type>.<model number>.<serialNumber>.<timestamp>.service.txt CMM - C:\opt\ibm\mdc\collection\bladeCenters\MDC.<projectName>.<type>.<model number>.<serialNumber>.<timestamp>.service.tgz Where, type is amm or cmm	info -T system:mm[1] info -T system displaysd -T system:mm[1] displaysd -u sftp://<cmmuser>:<cmmUserPassword>@<cmmHost>/service .tgz -T system:mm[1]
IBM System x	C:\opt\ibm\mdc\collection\dsa\<modelTypeNumber>_<serialNumber>_<yyyymmdd>-<hhmmss>.xml.gz Where modelTypeNumber and serialNumber will be unknown when dsa is unable to identify the value.	Executes DSA on the Systemx Devices For xLinux (In Addition to above) hostname -s uname -m uname -a uname -p head -1 /etc/SuSE-release cat /etc/SuSE-release head -1 /etc/redhat-release cat /etc/redhat-release head -1 /etc/debian_version cat /etc/debian_version uname -rs grep swap /etc/fstab /sbin/swapon -s ipcs -a ls -C /dev /sbin/lvmdiskscan /sbin/fdisk -l cat /etc/fstab mount df for each network obj($no) identified using ia rn an netstat -$no

		/sbin/ifconfig -a cat /etc/exports showmount -e showmount -a ls -alR /boot/* cat /etc/lilo.conf cat /etc/zipl.conf /sbin/lsmod modinfo -p dmesg rpm -qai cat /etc/crontab crontab -l cat /etc/security/limits.conf env java -version java -fullversion dmidecode PSC DATA: For Redhat sosreport –l sosreport --batch For Suse supportconfig -D -b –t
ESXi	dsa\<modelTypeNumber>_<serialNumber>_<yyyymmdd>-<hhmmss>.xml.gz Where modelTypeNumber and serialNumber will be unknown when dsa is unable to identify the value	Executes DSA on the “System to run DSA” device ppointing to ESXi device
Linux on System z	Rpt.VLZ.<prowebId>.<projectName>.<hostShortName>.<serialNumber>.s39.tar.Z Where, prowebId can be null	hostname -s uname -m uname -a uname -p head -1 /etc/SuSE-release cat /etc/SuSE-release head -1 /etc/redhat-release cat /etc/redhat-release head -1 /etc/debian_version cat /etc/debian_version uname -rs grep swap /etc/fstab /sbin/swapon -s

		ipcs -a ls -C /dev /sbin/lvmdiskscan /sbin/fdisk -l cat /etc/fstab mount df for each network obj($no) identified using ia rn an netstat -$no /sbin/ifconfig -a cat /etc/exports showmount -e showmount -a ls -alR /boot/* cat /etc/lilo.conf cat /etc/zipl.conf /sbin/lsmod modinfo -p dmesg rpm -qai cat /etc/crontab crontab -l cat /etc/security/limits.conf env java -version java -fullversion dmidecode PSC DATA: sosreport –l sosreport –batch supportconfig -D -b -t
SAP HANA / SAP BWA	<SAP_SystemID>_<hanaORbwa>_<bladeCenterMachineType>_<bladeCenterSerialNumber>_<yyyyMMddHHmmss>.zip - <hostName>_sapHanaBwa.log - <bladeCenterMachineType>_<bladeCenterSerialNumber>.txt - gpfs directory - gpfs.snapOut	**IBM System x (SUSE Linux)** IBM System x (SUSE Linux) supportconfig / supportconfig -A executes DSA on the System x Devices mppUtil -S On One of the System x Device gpfs.snap -a In addition to above, if it's a SAP BWA - Get host, default and custom ini files. /usr/sap/<SID>/TRX<instance_number>/hostname/*.ini – This can be multiple for each host /usr/sap/<SAPSID>/TRX<instance_number>/exe/config/*.ini /usr/sap/<SAPSID>/SYS/global/trex/config/custom/*.ini python_support/python serviceLoad.py -history=1 -export=serviceLoad.csv (From the directory /usr/sap/<SAP_SystemID>/exe/nuc/Linuxx86_64/trex-

	- sapBWAchecks directory - serviceLoad.csv - ini directory - hostname directory (*) - *.ini files - default directory - *.ini files - custom directory - *.ini files For each System x device , there will be directory as <Systemx HostName>_systemx - nts_<hostname>_<date>_<time>.tbz - <modelNumber>_<serialNumber>_<yyyymmdd>-<hhmmss>.xml.gz - mppUtil_output.txt For each BladeCenter, there will be directory as <BladeCenterHostName>_bladeCenter - service.txt For each DS3000, DS4000 and DS5000, there will be directory as <DS345KHostN	rev/python_support) IBM BladeCenter: info -T system:mm[1] info -T system displaysd -T system:mm[1] IBM DS3000, DS4000 and DS5000: save storageSubsystem supportdata clear allDriveChannels stats reset StorageSubsystem RLSBaseline reset StorageSubsystem SOCBaseline reset StorageSubsystem SASPHYBaseline Connects to each controller using telnet and then executes below commands: loadDebug iopPerfMonRestart socClearSYMbolErrorStats SAN/LAN Networking: Brocade Switches: moreDisable supportShow statsclear slotstatsclear Cisco Switches: terminal length 0 show tech-support clear counters interface all debug system internal clear-counters all QLlogic Switches: show support admin start set port clear admin end BNT Switches: IBM-NOSCLI mode: /info/sys/general ibmnos-cli verbose 0 lines 0 /m/tsdmp /stats/clrports ISCLI mode: iscli terminal-length 0 enable

	ame>_dsStorage - supportData.zip - supportData_afterClearCounters.zip For each SANLANNetworking, there will be directory as <SANLANNetworking HostName>_<brocade_qlogic_cisco_bnt> - sanswitch.cfg - sanswitch_afterClearCounters.cfg	show tech clear counters

For System x (Windows)

MDC requires Windows Scripting Host (WSH) or the Windows Management Instrumentation (WMI) service and VBScript to be enabled on the target. MDC requires Server Message Block (SMB) protocol on over TCP/IP for which, port 445 must not be blocked by firewalls or IP security policies.

See your OS firewall documentation to determine that these ports are not blocked for inbound requests.

MDC requires access to the hidden remote administrative disk share, for access to the system %TEMP% and other directories. Access to the Inter-process Communications share (IPC$) is also required for MDC to access remote registries. See the MDC Setup Guide for additional information.

Information specific to operating systems

Windows Server 2008

On Windows Server 2008 you might need to disable User Account Control if your account is not a domain administrator account. See the section on Windows Vista to learn how to disable User Account Control.

Windows Vista

The new User Account Control feature in Windows Vista requires users to perform several steps before MDC applications can communicate with Vista targets. See the MDC Setup Guide for instructions on how to set up your Vista account.

Windows 7

On Windows 7, the default startup type for the Remote Registry service is manual. The Remote Registry service must be running to enable MDC. For details on how to confirm this, see the MDC Setup Guide.

IBM Corporation
Marketing Communications
IBM Microcode Data Collector
Route 100
Somers, New York 10589

Produced in the United States of America
April 2018.