

IBM  
3.5.8.3

*Microcode Data Collector  
Setup Guide*



**Note**

Before using this information and the product it supports, read the information in [“Notices” on page 49.](#)

**July, 2024**

This edition applies to version 3, release 5, modification 8, of IBM® Microcode Data Collector and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2024.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Chapter 1. Microcode Data Collector.....</b>	<b>1</b>
What's new.....	1
Planning.....	1
Prerequisites.....	2
Supported devices.....	4
Using the Microcode Data Collector graphical user interface.....	4
Installing and upgrading Microcode Data Collector.....	4
Accessing the Microcode Data Collector graphical user interface.....	5
Collecting data.....	5
Identifying MDC managed devices.....	8
Scheduling tasks.....	8
Viewing the report files.....	9
Testing connectivity.....	10
Setting up IBM Power Systems (AIX, Linux, and VIOS).....	10
Setting up IBM Hardware Management Consoles (HMCs).....	12
Setting up IBM System x, Windows and ESX Server).....	13
Setting up ESXi.....	14
Setting up IBM BladeCenter and Flex System Enterprise Chassis.....	15
Setting up IBM Flex System Manager.....	16
Setting up IBM DS3000, DS4000, and DS5000 Storage Systems.....	17
Setting up IBM DS6000 and DS8000 Storage Systems.....	19
Setting up SAN/LAN Networking.....	20
Setting up Systems running IBM Spectrum Virtualized Software.....	21
Setting up IBM N series Storage Systems.....	22
Setting up IBM XIV Storage Systems.....	23
Setting up IBM TS3500 Tape Libraries.....	24
Setting up IBM ProtecTIER Systems.....	25
Setting up IBM 3494 and 3953 Tape Libraries.....	26
Setting up IBM i.....	27
Setting up IBM System z (Linux).....	28
Setting up IBM SAP HANA / BWA.....	29
Uninstalling.....	30
Using the Microcode Data Collector command-line interface (CLI).....	30
Installing Microcode Data Collector.....	30
Changing Microcode Data Collector settings.....	31
Collecting data.....	31
Sending data.....	32
Uninstalling Microcode Data Collector.....	32
Enabling call home for Tape Libraries.....	32
Troubleshooting.....	33
AIX VIOS Power System collection failed.....	33
MDC installation.....	33
Installation log.....	33
MDC log.....	33
MDC - Run as administrator.....	33
WMI repository.....	34
Test connection to ESXi fails.....	34
Unable to send files to IBM.....	34
TGRI0001E: The application might not establish a connection to 10.0.19.11.....	35
java.io.IOException: Connection failed with return code 5.....	35
Error while testing HMC connection with MDC.....	35

Uninstalling IBM Microcode Data Collector fails on Windows.....	35
Utility or Fileset not found on Power Systems (AIX / VIOS) .....	35
MDC Installation failed.....	36
No supported terminal types found.....	36
System x file not found.....	36
An error occurred when writing to the remote file.....	36
Error retrieving service.tgz file.....	36
Run collection failed on an AIX device.....	37
proweb.cfg file is very large.....	37
rksh: ioscli: not found.....	37
DSA compatibility check ... FAILED.....	37
Algorithm negotiation fail.....	37
Scenario: MyCompany deploys Microcode Data Collector.....	37
Setting up public and private key authentication.....	42
Creating public and private key pairs.....	43
Configuring public and private key authentication.....	44
Setting up target devices for System x (Windows).....	45
Operating systems information.....	45
Reconfiguring SSH client for VIOS server.....	46
<b>Notices.....</b>	<b>49</b>
Trademarks.....	49
Accessibility.....	50

# Chapter 1. Microcode Data Collector

Microcode Data Collector (MDC) collects microcode and support data from your systems for use by the IBM Premium Services support team.

The system on which MDC is installed connects to the configured systems to collect the microcode data. All the data that is collected is pulled to the system on which MDC is installed and is transmitted to IBM.

The data that is gathered is used by the IBM Premium Services support team and is treated as confidential by IBM. The data is not distributed, released, or otherwise made available for public use.

Refer to “[Supported devices](#)” on page 4 to learn which systems, products, or devices that MDC supports and what action to take for those systems, products, or devices.

**Note:** The systems or devices that you want to configure for data collection must be active and reachable on the network from the system on which Microcode Data Collector is installed.

## What's new

Microcode Data Collector (MDC) Version 3.5.8.3 includes the following.

- Removed log4j logging implementation for avoiding security vulnerabilities.
- Enhanced error messages that help in debugging issues.

## Planning

You can choose either a graphical user interface (GUI) or a command-line interface (CLI) to use Microcode Data Collector (MDC).

The following table differentiates the tasks that can be performed through GUI and CLI

Functionality	GUI	CLI
Install MDC	✓	✓
Identify and configure local system from which you want to collect data	✓	✓
Identify and configure remote systems from which you want to collect data	✓	✗
Specify contact information for your installation	✓	✓
Specify whether data is automatically or manually sent to IBM	✓	✓
Specify when the data is to be collected and sent to IBM	✓	✓
Specify the Internet connection path for the data transmission	✓	✗
Test the connection to IBM	✓	✓
Collect and send data to IBM	✓	✓
Run tailored collection	✓	✓
View reports list	✓	✗

Functionality	GUI	CLI
Perform MDC product updates (automatic)	✓	✓
Perform MDC product updates (manual)	✓	✗

If you do not have a graphics environment, you can use the MDC CLI. For more information, see [“Using the Microcode Data Collector command-line interface \(CLI\)”](#) on page 30.

## Prerequisites

Ensure that these requirements are met before you install Microcode Data Collector (MDC).

### Activation key

To use MDC, you must have a contract with the IBM Premium Services support team (Remote Advocate or Technical Relation Manager) through Microcode Support Services Offering (MSSO), Global Total Microcode Support (GTMS), Customer Technical Support (CTS), or Enhanced Technical Support (ETS). Based on the contract, you receive an activation key for MDC. Enter the activation key when you install MDC.

### Operating environment

MDC can be installed on any of the following operating environments. However, for a better user experience, it is recommended that you install MDC on Microsoft Windows.

- AIX 7.1, AIX 7.2 and later (Except Power 8 Little-Endian)

**Note:** Java™ 8 is shipped with this release of MDC. Java 8 works on AIX 6.1.5.0 and later.

- Microsoft Windows Server 2008
- Microsoft Windows 7
- Microsoft Windows 10

**Note:**

- Some MDC functions are supported only when you run as an Administrator in Windows.
- Java 8 is mandatory for Windows 10.

MDC can collect data from any of the following operating environments:

- Power 8 Big-Endian and Little-Endian
- Power 7, Power 6 Big-Endian and Little-Endian
- AIX 5.3 and later
- IBM i 6.1 and 7.1
- Virtual I/O Server (VIOS) 2.2.6 and later
- Microsoft Windows Server 2008
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- VMware vSphere Hypervisor 5.5 (u1), 5.1 (u2), 5.0 (u3)

**Note:** Collecting extended service information is not supported for XIV® storage systems when you run MDC on AIX.

## Hardware

This table defines the disk and memory requirements for a system that has MDC and all of the installed Storage Systems prerequisites (SMCLI, DSCLI, and XCLI).

Operating system	Disk	Memory
AIX	1.8 GB	700 MB
Windows	1.7 GB	650 MB

## 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 automatic call home function sends the collected report files to IBM.

## AIX

Installation of MDC on AIX requires the following:

- Root privileges
- A graphical environment such as the X Window System, if you are using the MDC graphical user interface.

### Notes:

- If you are using the dtsession window manager, your reports are not displayed correctly when you click **View Report List** on the **General tasks and settings** page.
- To view all screens correctly when you use Virtual Network Computing (VNC), use this command when you start VNC to set the minimum screen size to 1200 by 900:

```
-geometry 1200x900
```

- 3 GB of free space in the /opt directory
- Download the unzip utility for AIX at:  
[www.ibm.com/systems/power/software/aix/linux/toolbox/ezinstall.html](http://www.ibm.com/systems/power/software/aix/linux/toolbox/ezinstall.html)
- Ensure that you have the following filesets:
  - openssh.base.server
  - openssh.base.client

## Windows

- WMI (Windows Management Instrumentation) repository must be consistent. For more information on the steps to verify the WMI repository status, see [“WMI repository” on page 34](#).

## Accessibility

You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. If a screen reader is required, the Oracle Java Access Bridge must be installed on your Windows system. To install the Oracle Java Access Bridge, copy the `WindowsAccessBridge.dll` file from the `\accessbridge` folder in the `mdc.windows.zip` file to your `C:\WINDOWS\System32` directory and restart your screen reader before you install MDC.

MDC on Windows is tested with the JAWS screen reader on 32-bit Microsoft Windows XP with Service Pack 3.

## Online Help

Installing MDC on any of the operating systems (Windows or AIX) requires any of the following web browsers to view the online help.

- Mozilla Firefox
- Internet Explorer
- Google Chrome
- Microsoft Edge
- Netscape
- Opera

## Supported devices

MDC supports a wide variety of Power, Storage, Networking and x86 products.

Use the information in the [MDC Supported Device List](#) to identify what products or device types are supported by MDC.

## Using the Microcode Data Collector graphical user interface

---

Use this information to administer MDC using the graphical user interface.

## Installing and upgrading Microcode Data Collector

Use this information to install Microcode Data Collector (MDC) or to upgrade from a previous version of MDC.

### About this task

The contents of the MDC package install into the `/opt/ibm/mdc` or `c:\opt\ibm\mdc` directory. Contact the IBM Premium Services support team if you have questions about any files in this directory. Do not modify any files in the download package.

To install or upgrade MDC, follow these steps:

### Procedure

1. Download the installation archive file for your operating system from the following web page:  
[https://www.ibm.com/support/pages/esa/downloads\\_services.htm](https://www.ibm.com/support/pages/esa/downloads_services.htm)
2. Extract the installation files from the archive file.
3. Run the installation file for your operating system.

Platform	Installation file
AIX	install.sh
Windows	install.bat

**Note:** To install MDC on Windows system, right-click the `install.bat` file and select **Run as administrator** option. Else, you will not be able to perform all the functions of MDC and you will get a message - The installation has not been launched with Administrator privileges. Some functions might not be supported. Please refer setup guide for more information.

For more information, see [“MDC - Run as administrator”](#) on page 33.

If you have MDC version 3.3 or 3.4 running on your system, MDC 3.5 installer upgrades to MDC 3.5.

If you are installing for the first time, the MDC Installation wizard starts.

4. Read the License Agreement, the Non-IBM Terms and Conditions, and the License Information. Select **I accept both the IBM terms and the non-IBM terms**, and click **Next**.
5. Enter the activation key that you obtained from the IBM Premium Services support team and click **Next**.
6. Specify general settings and click **Next**.
7. Specify contact settings and click **Next**.
8. Specify scheduled task settings and click **Next**.
9. Specify connectivity settings and click **Next**.
10. Review the installation summary, make any necessary changes, and then click **Finish**.

## Accessing the Microcode Data Collector graphical user interface

Use this information to access the MDC graphical user interface.

### Before you begin

**Note:** Ensure **ulimit** value is *unlimited* in AIX systems.

To access the MDC graphical user interface, do one of the following tasks:

- For AIXun the following command:

```
/opt/ibm/mdc/MDC.sh
```

**Note:** Requires a graphical environment.

- For Windows, click **Start > All programs > IBM Microcode Data Collector > IBM Microcode Data Collector > Right-click > Run as administrator**.

**Note:** If you do not launch the MDC as an administrator, you can not perform few functions of MDC and you will get a warning message - The application has not been launched with Administrator privileges. Some functions might not be supported. Please refer setup guide for more information.

For more information, see “[MDC - Run as administrator](#)” on page 33.

**Tip:** You can also access the MDC graphical user interface by running the following command:

```
C:\opt\ibm\mdc\MDC.bat
```

## Collecting data

Use this information to understand how to collect and send data to IBM and perform updates.

### About this task

Use **General tasks and settings** page to collect and send data to IBM and perform updates.

If you have a Proactive System Check (PSC) contract, you can additionally collect the following types of information:

- Performance data for your IBM DS3000, DS4000, and DS5000 storage systems
- Extended service data for the following systems and devices:
  - Brocade, Cisco, Juniper storage area network (SAN), and local area network (LAN) devices, and Pure Flex top of rack (TOR) and BNT switch.
  - Systems running IBM Spectrum Virtualized Software
  - IBM XIV storage systems
  - IBM TS3500 tape libraries

MDC directly queries your tape libraries for detailed logs and drive memory dumps.

- IBM ProtecTIER Systems
- IBM Power Systems

Data can be collected and sent to IBM by following these steps.

## Procedure

- On **General tasks and settings** page, click **Run collection now** to perform a comprehensive collection and send the reports to IBM.

If **Call home mode** is set to **Automatic**, the data is collected and sent to IBM once a month according to the settings on the **Scheduled task settings** page. No further action is required.

If **Call home mode** is set to **Manual**, the data is collected but not sent to IBM. Continue with **Call home reports** step.

**Note:** For SAP HANA / BWA appliance, by default, the **Incident Report** option is executed during scheduled and manual collection of data.

- Click **Run tailored collection now**, the **Tailored Collection information** window displays. Tailored collection option allows you to run basic or extended collection on selected devices.

a) Select the **Collection Type** as **Other devices** or **SAP HANA / BWA**.

### Other devices

Select the system to collect information.

Click **Run collection now** to perform a comprehensive collection.

Click **Run extended collection now** to collect extended data for the selected system.

### SAP HANA / BWA

Select the system to collect information.

Enter the **PMR Id** (11-digit number) to associate the data that is collected, to the PMR.

Select the collection type as **Health Check** or **Incident Report**:

– The **Health Check** option involves the following steps to collect the data:

- a. Collects the extended data for all the devices and clears the history on the devices.
- b. Stops the MDC application for 3 hours during which no activity can be performed and displays a message - The collection is halted for 3 hours during which no action can be performed.
- c. Displays a message - The collection resumes after the halt period when the collection resumes.
- d. Starts the SAP HANA / BWA collector after 3 hours, to collect data for the second time on Switches and Data Storage devices.
- e. Associates the SAP HANA / BWA data with the specified PMR Id and sends to IBM, if the call home is automatic.

– The **Incident Report** option collects the data, associates it with the PMR Id, and sends to IBM.

Click **Run collection now** to collect the data.

b) Click **Close** to close the **Tailored Collection information** window.

- Click **Call home reports** to send previously collected reports to IBM.
- Click **View report list** to view a list of previously collected reports.
- Click **Perform Updates** to manually check and install, if there is a new version of MDC.
  - If there is a new MDC version available, you get a message - MDC Updates found!! Click OK to Install. Click **OK** to install the MDC update.
  - If there is no MDC update, you get a message - No MDC Updates found!!.

## Example

If you want to inspect the data that is contained in the reports, see [“Viewing the report files” on page 9](#).

## What to do next

You can also collect data using CLI. For information, see [“Collecting data” on page 31](#)

## General settings

### Procedure

- Enter the following information to collect and send data to IBM and also to perform MDC auto updates.

#### **IBM Customer Number**

Enter the customer number that is assigned to you by IBM.

#### **Project name**

Enter the name of the project that is assigned to you by IBM.

#### **Environment**

Specifies a marker type that is placed into the reports and are returned to IBM.

#### **Production**

Specifies a production environment.

#### **Test**

Specifies a test environment or prototype deployment.

#### **Call home mode**

##### **Automatic**

Specifies that reports are automatically sent to IBM immediately after a collection.

##### **Manual**

Specifies that reports are not automatically sent to IBM. This mode is useful if you want to collect and inspect the data, but not to send the data to IBM immediately. The data is in the following directories:

- For AIX

`/opt/ibm/mdc/collection/mdc`

- For Windows

`C:\opt\ibm\mdc\collection\mdc`

DSA data is in the following directories:

- For AIX

`/opt/ibm/mdc/collection/dsa`

- For Windows

`C:\opt\ibm\mdc\collection\dsa`

BladeCenter and Flex System Enterprise Chassis data is in the following directories:

- For AIX

`/opt/ibm/mdc/collection/bladeCenters`

- For Windows

`C:\opt\ibm\mdc\collection\bladeCenters`

#### **Auto Update mode**

Specifies the **Auto Update mode** options to update MDC automatically for a new version, if available.

### **Automatic**

Checks and installs the MDC updates automatically for every 7 days at 23:00 PM from the day you select this option. When selecting this option, ensure that the MDC installed system is in Charging mode (and not in Battery mode). If there are no updates, a message - No Updates Found is updated in the log file.

**Note:** If the MDC GUI is open or if there is any collection running at the time of auto-update, the auto-update is rescheduled to next day (same time) displaying a message - MDC GUI is open. Make sure to close MDC GUI to perform auto-update. Auto-update of MDC is rescheduled to tomorrow.

### **Manual**

Checks if there are any MDC updates available, automatically for every 7 days and displays a message on the collection console - MDC updates available. Click 'Perform Updates' to install MDC updates manually. Or select 'Automatic' option in the 'Auto Update mode' to perform the updates automatically..

### **None**

Specifies that MDC does not check for updates automatically. You must click **Perform Updates** to manually check MDC updates.

### **CTS/ETS ProwebId**

Provide your Proweb ID. This information is mandatory for Proweb customers. Leave it empty if you are not a Proweb customer.

## **Identifying MDC managed devices**

IBM uses this information to know number of devices and device types that are managed by MDC.

MDC identifies the new devices (that are not previously identified) based on the MTM details of the managed devices. MDC identifies the new device at the data collection time or at the heartbeat time. If a device is deleted, the device is removed from the list of MDC managed devices. For information on heartbeat settings, see [“Scheduling tasks” on page 8](#)

When you collect data for the devices, the identity of these devices is sent to IBM support to help them identify the devices for which the data collection is not started and / or failed to resolve any issues.

## **Scheduling tasks**

Use **Scheduled task settings** page to schedule the automatic data collection, call home, and heartbeat tasks.

### **Scheduled task settings**

#### **About this task**

If **Call home** mode is set to Automatic, the data is collected and sent to IBM every month according to the specified settings.

#### **Procedure**

To specify the scheduled task settings, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface” on page 5](#).

2. Click the **Scheduled task settings** tab.
3. Select **Enable** option under **Scheduled task settings** section to run the collection and call home monthly on the specified day and hour.
  - a) Select **Day of month**.
  - b) Select **Hour of day**.

4. Click **Apply** to save the settings.

## Heartbeat settings

### About this task

If **Call home** mode is set to **Automatic**, the data is collected and sent to IBM every month according to the specified settings.

### Procedure

To specify the scheduled task settings, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Scheduled task settings** tab.
3. Select **Enable Heartbeat** option under **Heartbeat settings** section to enable the heartbeat. Enabling the heartbeat pings the IBM server to specify that the MDC is live or reachable (though it is not running).

**Note:** If the heartbeat is disabled, the MDC installed device does not ping the IBM server.

4. Click **Apply** to save the settings.

## Viewing the report files

You can see the reports that are available and also inspect the data that is in the reports.

### About this task

### Procedure

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **General tasks and settings** tab.
3. On the **General Tasks** page, click **View report list**.

A list of reports that are received, but not yet transmitted are displayed.

### Results

Collected report files are contained in these directories:

- /opt/ibm/mdc/collection/mdc or c:\opt\ibm\mdc\collection\mdc
- /opt/ibm/mdc/collection/dsa or c:\opt\ibm\mdc\collection\dsa
- /opt/ibm/mdc/collection/bladeCenters or c:\opt\ibm\mdc\collection\bladeCenters
- /opt/ibm/mdc/collection/sapHanaBwa or c:\opt\ibm\mdc\collection\sapHanaBwa

The MDC log files are with the Storage system, and Management Console reports and are in the following directory:

/opt/ibm/mdc/collection/mdc or c:\opt\ibm\mdc\collection\mdc

## Testing connectivity

Use this information to test the connection to IBM.

### Procedure

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Connectivity settings** tab.
3. On the Connectivity settings page, click **Test connection to IBM**.

The IBM Microcode Data Collector Console window displays the test results.

Verify that you can connect to IBM.

## Setting up IBM Power Systems (AIX, Linux, and VIOS)

You can set up data collection for IBM Power Systems that is running AIX, Linux, Virtual I/O Server (VIOS). In addition to collecting data for the server itself, data is also collected for any IBM System Storage TS3100 Tape Library Express & TS3310 Tape Library when using the IBM Atape device driver.

### Before you begin

- MDC 3.5.6 and higher versions support data collection by normal user (without any root access) on IBM Power Systems. The normal user collects only a limited data. For complete data collection, login through sudo user.
- When your systems are running VIOS, set up data collection for all the VIOS partitions that are running on each Power System and for any partitions that own hardware.
- When you provide the credentials of a sudo user, ensure that sudo rpm is installed and configured for AIX, Linux for Power Systems. You can check whether sudo rpm is installed by running the **sudo** command. If sudo is installed, the system displays **sudo help** information, and if sudo is not installed, you get a message, sudo command does not exist. To configure login user to act as a sudo user, complete the following steps:
  1. Log in as root user.
  2. Run **visudo** command to open /etc/sudoers file that has **440** file permission.
  3. Verify the path of the **touch** command by using **which** command. For example, **which touch**. Use the following path to configure the command -
    - For AIX

```
Cmnd_Alias MDC_CMDS=/usr/bin/touch, /home/<login_user>/mdcworkdir/  
mdc_collection/system/bin/MDC.aix.vios.collector, /home/<login_user>/  
mdcworkdir/unix_utils.sh
```
    - For pLinux

```
Cmnd_Alias MDC_CMDS=/bin/touch, /home/<login_user>/mdcworkdir/  
mdc_collection/system/bin/MDC.pLinux.collector, /home/<login_user>/  
mdcworkdir/linux_utils.sh
```
  4. Add user privilege specification, **<login\_user> ALL=MDC\_CMDS**.
  5. Ensure that **targetpw** option is not set. This option is turned off by default. If the option is tuned on, you are required to enter the password of the user for whom you are acting as a sudo user.

For more information about sudo, see <http://www.sudo.ws/sudo/man/1.8.8/sudoers.man.html>.

6. On Linux for Power Systems, make clear if **requiretty** exists or not in **sudoers** file, if it does not exist or commented (disabled), then you can ignore this step. Else, if **requiretty** exists and is enabled, comment (disable) it and add a line as follows -

```
#Defaults requiretty
```

```
Defaults:<login_user> !requiretty
```

## About this task

MDC uses SSH2 protocol (only) with either user ID / password or public / private key based authentication to collect data from IBM Power Systems.

## Procedure

To set up data collection for your IBM Power Systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM Power Systems**.
4. Click the **IBM Power Systems** tab.

**Note:** Setting up IBM Power Systems requires knowledge of public and private key authentication. For information, see “[Setting up public and private key authentication](#)” on page 42.

5. On the **IBM Power Systems** page, click **New**.
  - a) In the **Enter a new IBM Power System** window, enter the following information:

### Enter IBM Power System host name or IP address

For example: 9.45.1.1.

### Enter userid

Enter `padmin` user ID to collect Microcode data from VIOS. Enter `root` or normal user or a sudo user ID to collect Microcode data from AIX or Linux for Power Systems.

### Note:

- A sudo user, belongs to sudo user list, who has permissions to run commands in root mode.
- 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.

### Working Directory

Select **/home** or **/tmp** working directory.

- If you select **/home**, a directory `/home/mdcworkdir` is created for a root user.
- If you select **/tmp**, a directory `/tmp/mdcworkdir` is created for a root user.

**Note:** For a non-root user, you cannot select a working directory, by default, a directory `/home/<user>/mdcworkdir` is created.

### Select authentication method

Select **Userid/password** or **Public/private key** authentication.

- If you select **Userid/password** authentication, **Enter password** to use for this authentication.

**Note:** If the user is a sudo user, you cannot use **Public/private key** authentication. You must select **Userid/password** authentication.

- If you select **Public/private key** authentication, **Select a private key** from the list of configured private keys.

**Note:** If a private key is not configured in the **Centralized Key Management** page, the **Public/private key** option is disabled.

- b) Click **OK**
6. If you have more systems, repeat these steps for each system.  
For information on configuring the private keys, see [“Configuring public and private key authentication” on page 44](#)
  7. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.  
Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM Hardware Management Consoles (HMCs)

You can set up data collection for IBM Hardware Management Consoles (HMCs).

### Before you begin

IBM HMC data collection uses Secure Shell (SSH2) protocol with user ID and password-based authentication to securely collect data for your HMC.

To enable this secure data collection, remote command execution must be enabled on the HMC. For information, see "Enabling and disabling HMC remote commands" at the following address:

[https://www.ibm.com/support/knowledgecenter/9009-22A/p9eh6/p9eh6\\_hmcrcce.htm](https://www.ibm.com/support/knowledgecenter/9009-22A/p9eh6/p9eh6_hmcrcce.htm).

To collect the utilization data, enable the data collection function on HMC by using the command **lslparutil**. For information, see "IVM lslparutil command" at the following address:

[https://www.ibm.com/support/knowledgecenter/9119-MHE/p8hcg/p8hcg\\_lslparutil.htm](https://www.ibm.com/support/knowledgecenter/9119-MHE/p8hcg/p8hcg_lslparutil.htm).

### Procedure

To set up data collection for your HMCs, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface” on page 5](#).

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM HMCs**.
4. Click the **IBM HMCs** tab.
5. On the **IBM HMCs** page, click **New**.
6. Enter the following information.

**IBM HMC host name or IP address**

For example: 9.45.1.1.

**User name**

Enter the user name to use when you access the HMC.

**Note:** The user name that you enter must have hmcoperator or higher authority.

**Password**

Enter the password to use when you access the HMC.

**Select Device Type**

Specify whether the system that you set up is in contract with IBM by using **Contract** or **Non-Contract** options.

**Note:** Microcode data is collected only from contract devices.

Click **OK**.

7. If you have more HMCs, repeat the steps for each.
8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM System x, Windows and ESX Server)

You can set up data collection for LENOVO System x systems that are running Linux, Microsoft Windows, and ESX Server. The Microcode Data Collector uses the Dynamic System Analysis (DSA) tool to collect data on System x systems.

### Before you begin

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 for IBM System x systems that are running Microsoft Windows, see [“Setting up target devices for System x \(Windows\)”](#) on page 45.

### About this task

You can collect secure data from a System x system by using the following method:

- The Secure Shell (SSH2) protocol for Linux and ESX Server and the Server Message Block (SMB) protocol for Windows

The Microcode Data Collector copies DSA to the System x system to collect data from the system. This is the recommended method. DSA is shipped with MDC for legacy IBM System x servers, but IBM does not provide the drivers that are required by the latest LENOVO System x systems. Get the latest (Lenovo DSA) drivers from the link- <https://datacentersupport.lenovo.com/us/en/downloads/DS504163> and place it in the `/opt/ibm/mdc/portable_dsa` location.

For information about DSA supported operating systems, refer to the DSA documentation at the following web page:

[www.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5084901](http://www.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5084901)

The SMB protocol requires access to port 445 on the remote host.

### Procedure

To set up data collection for your System x systems that are running Linux, Windows and ESX server, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM System x**.
4. Click the **IBM System x** tab.
5. On the **IBM System x** page, click **New**.
6. Enter the following information.

#### Enter IBM System x host name or IP address

For example: 9.45.1.1.

#### Enter user name

- For Linux and ESX Server, enter either **root** or a user name with root privileges.
- For Windows, enter either **Administrator** or a user name with Administrator privileges.

#### Enter password

Enter the password to use when you access this system.

### Select portable DSA version

Select the version of the IBM Dynamic System Analysis (DSA) tool that matches the operating system that is installed on this System x system.

**Note:** If you want to use a different DSA version, copy the file for that version into the following location:

`opt/ibm/mdc/portable_dsa`

This is the location that is specified for the `dsa.path` in the `opt/ibm/mdc/system/config/mdc.properties` file.

### Associated with SAP HANA / BWA Appliance

Select **Yes** to associate the IBM System x system with the SAP HANA / BWA appliance.

**Note:** If there is no single SAP HANA / BWA appliance configured on the MDC, or if the selected DSA is not SUSE Linux Enterprise Server (SLES) version, the **Yes** option is disabled.

If you select **Yes**, select the **SAP HANA / BWA Appliance System ID** from the list of available SAP HANA / BWA appliances. You can associate multiple SAP HANA / BWA appliances to a single System x system.

Click **OK**.

7. To test a specific system configuration, select the configuration and click **Test selected**. To test all the system configurations, click **Test all**.

Check the Microcode Data Collector Console window for test status messages.

## Setting up ESXi

You can set up Dynamic System Analysis (DSA) for IBM ESXi.

### About this task

MDC runs DSA to collect data from ESXi. MDC connects to ESXi systems through IBM System x<sup>®</sup> (system to run DSA) devices to collect data. Provide an IBM System x<sup>®</sup> device details with administrator or root privileges to run DSA.

MDC supports only IBM customized ESXi systems for collecting data. You can verify whether your ESXi system is IBM customized or not in any of the following two methods -

1. Log in to the ESXi system and run the command **`esxcli software vib list | grep ibmcustomization`**. If your ESXi system is IBM customized, you receive an output in this format  
`- ibmcustomization 2.0-3 IBM PartnerSupported 2013-03-25`
2. Enter the URL of your ESXi system in the browser. For example, `https://ipofESXiHostname/`. If your ESXi system is IBM customized, on the home page of your ESXi system, you can see this text  
`- You are running IBM Customized Image ESXi 5.0 Update 1 (based on ESXi 5.0 Update 1)`

### Procedure

You must enter the system details to run DSA. To set up data collection for your IBM ESXi, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **ESXi**.
4. Click the **ESXi** tab.
5. Under **System to run DSA**, enter the following information.

**Enter IBM System x host name or IP address**

For example: `9.3.21.123`.

**Enter user name**

For example: myuserid.

**Enter password**

For example: mypassword.

**Select portable DSA version**

Select a portable DSA version from the options.

Click **Apply**.

**Note:** For localhost (MDC installed System x / Windows device), the **user name** and **password** field entries are ignored.

6. You can create a new system configuration under **ESXi Hypervisor**. To create a new system configuration, follow these steps.

**Note:** The ESXi system must be connectable from the "System to run DSA" device.

a) Click **New**.

b) In the **Enter a new ESXi window**, enter the following information.

**Enter ESXi host name or IP address**

For example: 9.3.21.123.

**Enter user name**

For example: myuserid.

**Enter password**

For example: mypassword.

c) Click **OK**.

7. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM BladeCenter and Flex System Enterprise Chassis

You can set up data collection for IBM BladeCenter and Flex System Enterprise Chassis.

### Before you begin

Both IBM BladeCenter and IBM Flex System® Enterprise Chassis data collection use Secure Shell (SSH2) sessions to securely collect data from a management module such as the Advanced Management Module (AMM) or the Chassis Management Module (CMM) that is physically in your BladeCenter or Flex System Enterprise Chassis.

To enable this secure data collection, you must establish an SSH2 connection with the management module in your BladeCenter or Flex System Enterprise Chassis. For information, see "Secure Shell (SSH2) connection" at the following web address:

[http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.advmgtmod.doc/kp1bc\\_bc\\_cli\\_ssh.html](http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.advmgtmod.doc/kp1bc_bc_cli_ssh.html).

### Procedure

To set up data collection for your IBM BladeCenter and IBM Flex System Enterprise Chassis, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM BladeCenter and Flex Chassis**.
4. Click the **IBM BladeCenter and Flex Chassis** tab.

5. On the **IBM BladeCenter/Flex System Enterprise Chassis** page, click **New**.

6. Enter the following information.

**Enter BladeCenter/Flex System Enterprise Chassis host name or IP address**

For example: 9.45.1.1.

**Enter user name**

Enter the user name to use when accessing this BladeCenter or Flex System Enterprise Chassis.

**Enter password**

Enter the password to use when accessing this BladeCenter or Flex System Enterprise Chassis.

**Associated with SAP HANA / BWA Appliance**

Select **Yes** to associate the IBM BladeCenter with the SAP HANA / BWA appliance.

**Note:** If there is no single SAP HANA / BWA appliance configured on the MDC, the **Yes** option is disabled.

If you select **Yes**, select the **SAP HANA / BWA Appliance System ID** from the list of available SAP HANA / BWA appliances. You can associate multiple SAP HANA / BWA appliances to a single BladeCenter.

Click **OK**.

7. If you have additional BladeCenters or Flex System Enterprise Chassis, repeat the steps for each BladeCenter or Flex System Enterprise Chassis.

8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the Microcode Data Collector Console window for test status messages.

## Setting up IBM Flex System Manager

You can set up data collection for IBM Flex System Manager (FSM) systems.

### About this task

IBM FSM data collection uses Secure Shell (SSH2) protocol with user ID and password-based authentication to securely collect data for your FSM systems.

### Procedure

To set up data collection for your FSM systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5.

2. Click the **Identify systems** tab.

3. On the **Identify systems** page, select **IBM Flex System Manager**.

4. Click the **IBM Flex System Manager** tab.

5. On the **IBM Flex System Manager** page, click **New**.

6. Enter the following information.

**IBM FSM host name or IP address**

For example: 9.45.1.1.

**User name**

Enter the user name to use when you access the FSM system.

**Password**

Enter the password to use when you access the FSM system.

**Select Device Type**

Specify whether the system that you set up is in contract with IBM by using **Contract** or **Non-Contract** options.

**Note:** Microcode data is collected only from contract devices.

Click **OK**.

7. If you have more FSM systems, repeat the step for each system.
8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM DS3000, DS4000, and DS5000 Storage Systems

Use this information to set up data collection for IBM DS3000, DS4000, and DS5000 Storage Systems.

### Before you begin

To support data collection for IBM DS3000, DS4000 and DS5000 storage systems that are covered by your contract, you need the IBM DS Storage Manager that is installed on the same system on which Microcode Data Collector is installed. The IBM DS Storage Manager contains the SMCLI required by Microcode Data Collector.

**Note:** No support for data collection from IBM DS3000, DS4000 and DS5000 storage systems when running MDC on a Power Linux server as the SMCLI tool is not supported on Power Linux.

You can download the IBM DS Storage Manager from Fix Central. Depending upon the platform and version, the steps to install IBM DS Storage Manager are similar to the following:

1. Go to [www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral).
2. Click **IBM Sign in**. Sign in with your IBM ID. If you do not have an IBM ID, you can register to create one.
3. Under **Product Group** select **System Storage**.
4. Under **Select from System Storage** select **Disk systems**.
5. Under **Select from Disk systems**, select **Mid-range disk systems**.
6. Under **Select from Mid-range disk systems** select **DSxxxx** (where DSxxxx is your storage system).
7. Under **Release** select **DS\_SM\_vxx.xx.xx.xx** (select the latest).
8. Under **Platform** select the platform that matches where MDC is installed.
9. Click **Continue**.
10. Select the latest package and click **Continue**.
11. Select a download method and click **Continue**.
12. Click **Download now**.
13. Run the **SMIA-xxx-xx.xx.xx.xx** file that is contained in the downloaded compressed file.
14. Follow the installation wizard. Select **Custom** for installation type and click **Next**.
15. Select only the DS Storage Manager Client and click **Next**.
16. Select **Do not Automatically Start the Monitor** and click **Next**.
17. Click **Install**. When the installation program is finished, click **Done**.

### About this task

If you want to collect extended service information and performance data for your DS3000, DS4000, and DS5000 storage systems, click **Run extended collection now** on the **General tasks and settings** page. For more information, see [“Collecting data”](#) on page 5.

### Procedure

To set up data collection for your DS3000, DS4000 and DS5000 storage systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “Accessing the Microcode Data Collector graphical user interface” on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM DS3000, DS4000 and DS5000**.
4. Click the **IBM DS3000, DS4000 and DS5000** tab.
5. On the **IBM DS3000, DS4000 and DS5000** page, enter the SMCLI location or click **Browse** to locate the file.  
For example: C:/Progra~1/IBM\_DS/client/SMcli.exe (for Windows).

**Note:** If the CLI location is automatically filled, it means that the microcode Data Collector has detected the SMCLI location.

6. Click **New**.
7. Enter the following information.

**Enter primary FAStT Controller host name or IP address**

For example: 9.35.142.145.

**Enter secondary FAStT Controller host name or IP address**

For example: 9.35.142.146.

**Enter DS3000, DS4000, or DS5000 serial number**

**Note:** Use the serial number that is printed on the label on the back of the DS4000 controller unit (for DS4100, DS4300, DS4400, DS4500 and FAStT), or on the left front mounting bracket for DS3000, DCS3700, DS3950, DS4200, DS4700, DS4800, DS5020, DS5100, DS5300.

For example: 139801B.

**Enter Password**

Enter the password, only if it is set for the storage device.

**Associated with SAP HANA / BWA Appliance**

Select **Yes** to associate the DS3000, DS4000, or DS5000 storage systems with the SAP HANA / BWA appliance.

**Note:** If there is no single SAP HANA / BWA appliance that is configured on the MDC, the **Yes** option is disabled.

If you select **Yes**, enter the following information:

- Enter user name of both controllers
- Enter password of both controllers
- Select the **SAP HANA / BWA Appliance System ID** from the list of available SAP HANA / BWA appliances. You can associate multiple SAP HANA / BWA appliances to a single DS3000, DS4000, or DS5000 storage system.

Click **OK**.

8. If you have more systems, repeat from step “6” on page 18 for each system.
9. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.  
Check the **Microcode Data Collector Console** window for test status messages.

## What to do next

If the collection from DS3000, DS4000 and DS5000 storage systems does not collect any data due to network latency, you can increase the timeout in the C:\opt\ibm\mdc\system\config\commandTimeout.properties file. For example,

```
smcli.basic.command=120  
smcli.psc.command=1200  
smcli.performance.command=600
```

**Note:** The **smcli.basic.command** is used for basic collection and **smcli.psc.command**, **smcli.performance.command** are used along with basic in PSC collection.

# Setting up IBM DS6000 and DS8000 Storage Systems

You can set up data collection for IBM DS6000™ and DS8000® Storage Systems.

## Before you begin

To support data collection for IBM DS6000 and DS8000 Storage Systems that are covered by your contract, you need the IBM DS command-line interface (DSCLI) program installed on the same system on which Microcode Data Collector is installed. A Storage Management Console must also be active and be reachable on the network from this server. You can download the IBM DS command-line interface (DSCLI) program. For DS6000, the Storage Manager and DSCLI are bundled in a microcode package. For DS8000, the Storage Manager and DSCLI are contained in two separate images that are based on your version of microcode. The steps to download the IBM DS command-line interface (DSCLI) program are similar to the following:

1. Go to [www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral).
2. Click **IBM Sign in**. Sign in with your IBM ID. If you do not have an IBM ID, you can register to create one.
3. Under **Product Group** select **System Storage**.
4. Under **Select from System Storage** select **Disk systems**.
5. Under **Select from Disk systems**, select **Enterprise Storage Servers**.
6. Under **Select from Enterprise Storage Servers** select **DSxxxx** (where DSxxxx is your storage system).
7. Click **Continue**.
8. Select a DSCLI program and follow the directions to download and install.

## Procedure

To set up your IBM DS6000 and DS8000 Storage Systems for data collection, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM DS6000 and DS8000**.
4. Click the **IBM DS6000 and DS8000** tab.
5. On the **IBM DS6000 and DS8000** page, enter the DSCLI location or click **Browse** to locate the file.

**Note:** If the CLI location is automatically filled, then microcode Data Collector has detected the DSCLI location.

For example: `c:\Program~1\ibm\dsccli\dsccli.exe` (for Windows).

6. Click **New**.
7. Enter the following information.

**Enter Management Console host name or IP address**

For example: 9.35.142.145.

**Enter user name**

For example: myusername.

**Enter password**

For example: mypassword.

Click **OK**.

8. If you have more systems, repeat from step “6” on page 19 for each system.
9. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

# Setting up SAN/LAN Networking

You can set up data collection for storage area network (SAN) and local area network (LAN) devices.

## Before you begin

MDC can collect data from BNT switch that is configured either through **ibmnos-cli** or **is-cli** interface.

## About this task

If you want to collect extended service data for your SAN or LAN devices, click **Run extended collection now** on the **General tasks and settings** page. For more information, see [“Collecting data” on page 5](#).

## Procedure

To set up data collection for your SAN or LAN devices, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface” on page 5](#).

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **SAN/LAN Networking**.
4. Click the **SAN/LAN Networking** tab.
5. On the **SAN/LAN Networking** page, click **New**.
  - a) In the **Enter a new SAN/LAN device** window, enter the following information:

**Enter a device host name or IP address**

For example: 1.1.1.1.

**Enter user name**

For example: myusername.

**Enter password**

For example: mypassword.

**Select the device type**

Select **Brocade**, **Brocade-McData SAN**, **Cisco**, **Juniper**, **BNT**, or **QLogic**

**Note:** Select **Brocade** for IBM SAN switches.

**Select communication protocol**

Select **SSH** or **Telnet** protocol.

**Note:**

- BNT Switch supports only SSH (SSH2).
- SAP HANA / BWA appliance (with BNT, Brocade, QLogic, Cisco devices) supports only Telnet.
- Brocade, Brocade-McData SAN, Juniper, QLogic, and Cisco supports both SSH (SSH2) and Telnet.

**Associated with SAP HANA / BWA Appliance**

Select **Yes** to associate the SAN / LAN device with the SAP HANA / BWA appliance.

**Note:** If there is no single SAP HANA / BWA appliance that is configured on the MDC, the **Yes** option is disabled.

If you select **Yes**, select the **SAP HANA / BWA Appliance System ID** from the list of available SAP HANA / BWA appliances. You can associate multiple SAP HANA / BWA appliances to a single SAN / LAN device.

**Note:** You cannot associate *Brocade-McData SAN* and *Juniper* devices with SAP HANA / BWA appliances. The SAP HANA / BWA appliances can be connected only through Telnet.

**Important:** For setting up BNT, Cisco, Juniper, and QLogic switches, you can provide optional details like IBM device type, model, and serial number instead of communication protocol. To set up BNT, Cisco, Juniper, and QLogic switches, enter the following details:

- **Enter IBM machine type**
- **Enter IBM machine model**
- **Enter IBM machine serial**

b) Click **OK**

6. If you have more devices, repeat step “5” on page 20 for each device.

7. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

**Note:** If the device requires a password change, the test might fail.

## Setting up Systems running IBM Spectrum Virtualized Software

You can set up data collection for systems running IBM Spectrum Virtualized Software (SVS). The systems include IBM SAN Volume Controller, IBM Storwize, and IBM FLASH systems.

### Before you begin

Systems running IBM Spectrum Virtualized Software support both Username/password and Public/private key authentications. To support data collection by Public-Private key authentication, you need a public and private key pair. Install the public key on the IBM System Storage Productivity Center or the master console of the SAN Volume Controller cluster as follows:

1. Log in to the SAN Volume Controller Console

```
http://svc_console_host_name:9080/ics/Login
```

by using the admin user ID or a user ID with administrator authority.

2. Use the SAN Volume Controller Console interface to modify the user ID to add the public key file.
3. Copy the private key to a directory on the system on which MDC is installed.

To support data collection for IBM FLASH systems that are covered by your contract, you need a user ID and password authentication or a Public/private key authentication to log in to FLASH system.

### About this task

If you want to collect extended service data for your systems running IBM Spectrum Virtualized Software, click **Run extended collection now** on the **General tasks and settings** page. For more information, see “Collecting data” on page 5.

### Procedure

To set up data collection for your systems running IBM Spectrum Virtualized Software, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “Accessing the Microcode Data Collector graphical user interface” on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **Systems running IBM Spectrum Virtualized Software**.
4. Click the **Systems running IBM Spectrum Virtualized Software** tab.
5. On the **Systems running IBM Spectrum Virtualized Software** page, click **New**.
6. Enter the following information:

- a) **Enter the system running IBM Spectrum Virtualized Software IP address.**  
For example: 9.3.21.123.

b) **Enter userid**

The user Id provided should have the authorization to run the collection command list.

c) Select either **Userid/password** or **Public/private key** authentication.

- For **Userid/password** authentication, **Enter password** to use this authentication.
- For **Select a private key** authentication, Select a private key from the list of configured private keys.

**Note:** If a private key is not configured in the **Centralized Key Management** page, the **Public/private key** option is disabled.

d) Click **OK**.

7. If you have more systems, repeat from step “5” on page 21 for each system. For information on configuring the private keys, see “[Configuring public and private key authentication](#)” on page 44.

8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM N series Storage Systems

You can set up data collection for IBM N series Storage Systems.

### Before you begin

IBM N series Storage Systems are run on Data ONTAP Operating System, which is used to connect to the N series Systems and fetch the data. Generally, N series devices are equipped with firmware ports that function as remote management consoles. These consoles manage (for example, power ON / OFF) the N series devices. The IP address of the remote management port is different from the IP address of associated N series storage system.

The remote management port can be any one of the following depending upon the version of storage device:

- Remote LAN Management (RLM)
- Baseband Management Console (BMC)
- Service Processor (SP)

**Note:** MDC supports connecting to Remote LAN Management (RLM) and Service Processor (SP) firmware ports only.

### About this task

MDC uses SSH2 or Telnet protocol with user ID/password-based authentication to collect data from IBM N series Storage Systems that run on Data ONTAP OS. But to connect to the firmware ports, MDC supports only SSH2 protocol. For RLM / SP, MDC logs in to the Data ONTAP through firmware, and runs the **system console** command.

### Procedure

To set up data collection for your IBM N series Storage Systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Identify systems** tab.

3. On the **Identify systems** page, select **IBM N series Storage Systems**.

4. Click the **IBM N series Storage Systems** tab.

5. On the **IBM N series Storage Systems** page, click **New**. The **Enter a new IBM N series System** window displays.

6. Enter the following information:

**Enter N series Storage System node host name or IP address**

For example: 9.3.21.123.

**Select the mode of N series system**

Select **Data ONTAP** or **Firmware (SP/RLM)** protocol.

**Enter user name**

For example: myusername.

**Enter password**

For example: mypassword.

**Select communications protocol**

Select **SSH** or **Telnet** protocol.

**Note:** If **Firmware (SP/RLM)** mode of N series system is selected, the **Telnet** protocol is disabled. The provided user name and password are used to log in to firmware device. Then, from the firmware device, it connects to Data ONTAP with `root` user name and provided password. If this connection fails, the provided user name and password are used to connect to Data ONTAP from firmware. When a connection fails, you see this message on the console - `Cannot connect to system at: " + host.`

Click **OK**.

7. If you have more systems, repeat from step “5” on page 22 for each system.

8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM XIV Storage Systems

You can set up data collection for IBM XIV Storage Systems and A9000 Systems.

### Before you begin

To support IBM XIV Storage Systems that are covered by your contract, you must have the IBM XIV GUI installed on the same system on which Microcode Data Collector is installed. The IBM XIV GUI contains the XCLI required by the Microcode Data Collector.

**Note:** No support for data collection from IBM XIV Storage Systems when running MDC on a Power Linux server as the XCLI tool is not supported on Power Linux.

To download and install the IBM XIV GUI for your platform, follow these steps:

1. Go to [www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral).
2. Under **Product Group**, select **System Storage**.
3. Under **Select from System Storage**, select **Disk systems**.
4. Under **Select from Disk systems**, select **Enterprise Storage Servers**.
5. Under **Select from Enterprise Storage Servers**, select **XIV Storage System (2810, 2812)**.
6. Under **Installed Version**, select **3.1.1** or higher.
7. Under **Platform**, select the platform that matches where MDC is installed.
8. Click **Continue**.
9. Select the latest package and click **Continue**.
10. Sign in with your IBM ID. If you do not have an IBM ID, you can register to create one.
11. Select a download method and click **Continue**.
12. Review and agree to the terms and conditions to start the download.
13. Save the executable CLI file in the appropriate location as follows:

- For **AIX**: /root/IBM\_XIV\_Storage\_Management\_GUI
- For **Linux**: /root/IBM\_XIV\_Storage\_Management\_GUI
- For **Windows**: C:\Program Files\IBM\Storage\XIV\XIVGUI\

## About this task

If you want to collect extended service data for your IBM XIV storage systems, click **Run extended collection now** on the **General tasks and settings** page. For more information, see [“Collecting data” on page 5](#).

## Procedure

To set up data collection for your IBM XIV storage systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface” on page 5](#).

2. Click the **Identify systems** tab.

3. On the **Identify systems** page, select **IBM XIV Storage Systems**.

4. Click the **IBM XIV Storage Systems** tab.

5. Enter the XCLI location or click **Browse** to locate the file.

For example: C:\Program Files\IBM\Storage\XIV\XIVGUI\xcli.exe (for Windows).

**Note:** If the CLI location is automatically filled, the Microcode Data Collector has detected the XCLI location.

6. Click **New**.

7. Enter the following information.

**Enter XIV Controller 1 host name or IP address**

For example: 1.1.1.1.

**Optional: Enter XIV Controller 2 host name or IP address**

For example: 2.2.2.2.

**Optional: Enter XIV Controller 3 host name or IP address**

For example: 3.3.3.3.

**Enter user name**

For example: myusername.

**Enter password**

For example: mypassword.

Click **OK**.

8. If you have more systems, repeat from step [“6” on page 24](#) for each system.

9. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM TS3500 Tape Libraries

You can set up data collection for IBM TS3500 Tape Libraries.

### Before you begin

**Note:** This feature of setting up TS3500 tape libraries through MDC GUI is deprecated and it is preferred to enable call home for the product. For more information, see [“Enabling call home for Tape Libraries” on page 32](#).

To support data collection from your TS3500 tape libraries, these tape libraries must meet the following prerequisites:

- The TS3500 Tape Library must be at a firmware level 8xxx (or higher).
- The Advanced Library Management System (ALMS) must be installed and enabled.
- Java 5.0 or higher must be installed.

**Note:** Previous versions of the Microcode Data Collector required that the Secure Socket Layer (SSL) be disabled. Microcode Data Collector Version 3.3 allows SSL to be enabled and provides for the Keystore and Keystore password to be provided for each TS3500 tape library.

### About this task

If you want to collect extended service data for your TS3500 tape library, click **Run extended collection now** on the **General tasks and settings** page. For more information, see [“Collecting data” on page 5](#).

**Note:** For large tape libraries, collecting extended service information can take several hours.

### Procedure

To set up data collection for your TS3500 tape libraries, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface” on page 5](#).

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM TS3500 Tape Libraries**.
4. Click the **IBM TS3500 Tape Libraries** tab.
5. On the **IBM TS3500 Tape Libraries** page, click **New**.
6. Enter the following information.

**Enter IBM TS3500 Tape Library host name or IP address**

For example: 9 . 3 . 21 . 123.

**Enter user name**

For example: myuserid.

**Enter password**

For example: mypassword.

**Keystore location (if SSL enabled)**

Enter the full path and file name of the keystore file that contains the public and private key pair used with SSL.

**Keystore password**

Enter the keystore password used with SSL.

Click **OK**.

7. If you have more systems, repeat from step [“5” on page 25](#) for each system.
8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.  
Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM ProtecTIER Systems

You can set up data collection for IBM ProtecTIER Systems.

### Procedure

To set up data collection for your IBM ProtecTIER Systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface” on page 5](#).

2. Click the **Identify systems** tab.

3. On the **Identify systems** page, select **IBM ProtecTIER Systems**.
4. Click the **IBM ProtecTIER Systems** tab.
5. On the **IBM ProtecTIER Systems** page, click **New**.
6. Enter the following information.

**Enter ProtecTIER node host name or IP address**

For example: 9.3.21.123.

**Select ProtecTIER node number**

Set the ProtecTIER node number to 1 for unclustered environments. This is the typical configuration. A TS7650G can be clustered. If you have a TS7650G clustered environment, set the ProtecTIER node number to the actual node number.

**Enter ProtecTIER Manager version**

For example: 2.5.1.0.

**Tip:** The ProtecTIER Manager version is found on the ProtecTIER Manager **Help > About** screen.

**Enter user name**

For example: myuserid.

**Enter password**

For example: mypassword.

Click **OK**.

7. If you have more systems, repeat step “5” on page 26 for each system.
8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM 3494 and 3953 Tape Libraries

You can set up data collection for IBM 3494 and 3953 Tape Libraries.

### Before you begin

**Note:** This feature of setting up IBM 3494 and 3953 tape libraries through MDC GUI is deprecated and it is preferred to enable call home for the product. For more information, see [“Enabling call home for Tape Libraries”](#) on page 32.

### Procedure

To set up data collection for your IBM 3494 and 3953 tape libraries, follow these steps:

1. Access the Microcode Data Collector graphical user interface.
- Tip:** See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5.
2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM 3494 and 3953 Tape Libraries**.
4. Click the **IBM 3494 and 3953 Tape Libraries** tab.
5. On the **IBM 3494 and 3953 Tape Libraries** page, click **New**.
6. Enter the following information.

**Enter Library Manager host name or IP address**

For example: 1.1.1.1.

**Enter user name**

For example: myusername.

**Enter password**

For example: mypassword.

Click **OK**.

7. If you have more systems, repeat from step “5” on page 26 for each system.
8. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.  
Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM i

You can set up data collections for IBM i. MDC supports IBM i 6.1 and later versions.

### About this task

The Microcode Data Collector collects data from your IBM i systems. In addition to collecting data for the server itself, data is also collected for any local or remote IBM System Storage system unless the system is attached by NPIV (or vSCSI), in which case the adapter is owned by VIOS and the collection must be done through the VIO.

**Note:** If attachment type is unknown, data is collected from both the LPAR and the VIOS. For more information, see [IBM i Removable Media](#).

Provide the administrator or root privilege credentials of the IBM i systems from which you want to collect data.

### Procedure

To set up data collection for your IBM i, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM i**.
4. Click the **IBM i** tab.
5. On the **IBM i** page, under **IBM i Systems** click **New**.
6. Enter the following information.

**Enter IBM i host name or IP address**

For example: 9.3.21.123.

**Enter user name**

For example: myuserid.

**Enter password**

For example: mypassword.

**Select an Associated System**

Select the corresponding associated **HMC** or **FSM** and select **None** for self managed IBM i systems.

**Note:**

- HMC or FSM options are activated only if you have configured them in the IBM HMCs and IBM Flex System Manager® screens respectively.
- If multiple IBM HMCs are configured, and the **HMC** option is chosen, a list of HMC are shown. Select an HMC from the list.
- If multiple IBM FSMs are configured, and the **FSM** option is chosen, a list of FSM are shown. Select an FSM from the list.

Click **OK**.

7. To test a specific configuration, select the configuration and click **Test selected**. To test all the configurations, click **Test all**.

Check the **Microcode Data Collector Console** window for test status messages.

## Setting up IBM System z (Linux)

You can set up data collection for IBM System z systems that are running Linux operating system. The Microcode Data Collector runs a script file on System z systems and collects the data to `.tar.gz` file.

### Before you begin

Both root and sudo users can collect the Microcode data for System z systems.

- When you provide the credentials of a sudo user, ensure that sudo rpm is installed and configured for Linux for System z systems. You can check whether sudo rpm is installed by running the **sudo** command. If sudo is installed, the system displays **sudo help** information, and if sudo is not installed, you get a message, `sudo command does not exist`. To configure login user to act as a sudo user, complete the following steps.

- Log in as root user.
- Run **visudo** command to open `/etc/sudoers` file that has **440** file permission.
- Verify the path of the **touch** command by using **which** command. For example, **which touch**. Use this path to configure the command -

```
Cmdnd_Alias MDC_CMDS=/bin/touch, /home/<login_user>/mdcworkdir/  
mdc_collection/system/bin/MDC.zLinux.collector, /home/<login_user>/  
mdcworkdir/linux_utils.sh
```

- Add user privilege specification, **<login\_user> ALL=MDC\_CMDS**.
- Ensure that **targetpw** option is not set. This option is turned off by default. If the option is tuned on, you are required to enter the password of the user for whom you are acting as a sudo user.

For more information about sudo, see <http://www.sudo.ws/sudo/man/1.8.8/sudoers.man.html>.

- Check if **requiretty** option exists in `sudoers` file. If it does not exist or disabled, then you can ignore this step. Else, if the **requiretty** option exists and is enabled, then disable it and add a line as follows -

```
#Defaults requiretty
```

```
Defaults:<login_user> !requiretty
```

### About this task

Use Secure Shell (SSH2) protocol to authenticate yourself with a valid user ID and password and connect to the System z systems.

The Microcode Data Collector runs a script file on the System z system to collect data into a `.tar.gz` file and stores at `/opt/ibm/mdc/collection/mdc` directory. Any existing data in this directory is erased before the MDC saves the current data.

### Procedure

To set up data collection for your System z systems that are running Linux operating system, follow these steps:

- Access the Microcode Data Collector graphical user interface.

**Tip:** See “[Accessing the Microcode Data Collector graphical user interface](#)” on page 5.

- Click the **Identify systems** tab.
- On the **Identify systems** page, select **Linux on System z**.
- Click the **Linux on System z** tab.
- On the **IBM System z Linux systems** page, click **New**.
  - In the **Enter a new System z Linux system** window, enter the following information:

**Enter IBM System z Linux host name or IP address**

For example: 9.45.1.1.

**Enter user name**

Enter **root** or a sudo user ID to collect Microcode data.

**Note:** A sudo user who belongs to sudoer list and has permissions to run commands in root mode.

**Enter password**

Enter the password to use when you access this system.

b) Click **OK**

6. To test a specific system configuration, select the configuration and click **Test selected**. To test all the system configurations, click **Test all**.

Check the Microcode Data Collector console window for test status messages.

## Setting up IBM SAP HANA / BWA

You can set up data collection for IBM SAP HANA / BWA appliance that consists a BladeCenter (or Flex Chassis) with various System x blades or System x ITEs, Ethernet switch modules, and Fibre Channel switch modules.

### Before you begin

Before you begin SAP HANA collection, check for the latest DSA in Fix Central, and update the version of DSA in the MDC installation if necessary.

### About this task

Use 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 by using MDC you can associate the storage devices to SAP HANA and collect data.

**Note:** You must associate a BladeCenter to SAP HANA / BWA appliance to successfully collect and send data to IBM. SAP HANA / BWA appliance is identified with the associated BladeCenter. If you do not associate a BladeCenter to SAP HANA / BWA appliance, the data is collected for all the other associated devices but cannot be sent to IBM.

A new directory is created on the system that runs MDC at `C:\opt\ibm\mdc\tmp\sapHanaBwa` and `C:\opt\ibm\mdc\collection\sapHanaBwa` to maintain SAP HANA / BWA data. The `tmp` folder contains the data during collection. When the data is collected, it is moved to `collection` folder. A directory is created for SAP HANA / BWA appliance, for example, `C:\opt\ibm\mdc\tmp\sapHanaBwa\<SAPSID>`.

### Procedure

To set up data collection for your IBM SAP HANA / BWA appliances, follow these steps:

1. Access the Microcode Data Collector graphical user interface.

**Tip:** See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5.

2. Click the **Identify systems** tab.
3. On the **Identify systems** page, select **IBM SAP HANA / BWA**.
4. Click the **IBM SAP HANA / BWA** tab.
5. On the **IBM SAP HANA / BWA Appliance** page, click **New**.

a) In the **Enter a new IBM SAP HANA / BWA appliance** window, enter the following information:

- i) Enter **System Id**. For example: HANA03.
- ii) Enter **Instance Id**. For example: 02.

- iii) Select **Appliance Type**: HANA or BWA.
  - iv) Enter **Password for System Id admin (SAPSID>adm) user name**. The password must be the password of the user name **SAPSID>adm**. For example, password of the hana03adm user name.
  - b) Click **OK**.
6. When other devices are associated with the SAP HANA / BWA appliance, they are displayed in the **Configured Systems** section.

## Uninstalling

Use this information to uninstall Microcode Data Collector.

### Before you begin

Before uninstalling Microcode Data Collector, close the Microcode Data Collector graphical user interface window.

### Procedure

To uninstall Microcode Data Collector, choose from the following options:

- For AIX, run the following command:

```
/opt/ibm/mdc/bin/MDC.uninstall.sh
```

- For Windows, click **Start > All programs > IBM Microcode Data Collector > Uninstall IBM Microcode Data Collector**.

**Tip:** You can also uninstall Microcode Data Collector by running the following command:

```
C:\opt\ibm\mdc\system\bin\MDC.uninstall.bat
```

## Using the Microcode Data Collector command-line interface (CLI)

If you do not have a graphics environment, you can use the Microcode Data Collector (MDC) command-line interface (CLI) on AIX or Linux systems to do a subset of the tasks that you can do with the MDC graphical user interface.

### About this task

You can use the MDC CLI to perform the following tasks:

- Install MDC
- Specify contact information for your installation
- Specify whether data is automatically or manually sent to IBM
- Specify when the data is to be collected and sent to IBM
- Test the connection to IBM
- Collect and send data to IBM

## Installing Microcode Data Collector

Use this information to install or upgrade Microcode Data Collector (MDC).

### Procedure

To install MDC, follow these steps:

1. On the AIX command line, enter the following command:

```
./install.sh
```

2. IBM Microcode Data Controller Command Line wizard prompts for the following information.
  - a) Enter Y to continue installing MDC on the system.
  - b) Enter Y to accept the license terms and conditions.
  - c) Enter the activation key that is given to you along with your contract.
  - d) Enter **IBM Customer Number**
  - e) Enter **project name, CTS/ETS Proweb ID, contact name, contact phone, email address, city, Street Address, state or province, country number.**
  - f) Enter a (automatic) or m (manual) for **call home mode**.
  - g) Enter a (automatic) or m (manual) for **auto update mode**.
  - h) Enter p (production) or t (test) for **environment**.
  - i) Enter Y/y (yes) or N/n (no) to setup a scheduled task to run the collection monthly.
  - j) Enter Y/y (yes) or N/n (no) to enable a scheduled heartbeat task for MDC weekly.
  - k) The information summary of the MDC installation is displayed. Enter Y/y (yes) or N/n (no) to change your information. You get a message - The Microcode Data Collector is installing ... please wait.
  - l) After installation, enter Y/y (yes) or N/n (no) to run a connectivity test. You get the connectivity verification test results.
  - m) Enter Y/y (yes) or N/n (no) to run a data collection. A storage report is generated and if call home is set to automatic, the report is sent to IBM.
  - n) Command line installation is complete and you can use `/opt/ibm/mdc/MDC.sh` to run this command line wizard in future.

**Important:** A graphic environment is required to use the Microcode Data Collector Console.

## Changing Microcode Data Collector settings

Use this information to change contact information or other Microcode Data Collector (MDC) settings.

### Procedure

To change contact information or other MDC settings, follow these steps:

1. On the AIX command line, enter the following command:

```
./MDC.sh
```

2. Follow the prompts in the CLI wizard to change MDC settings.

## Collecting data

You can run Proactive System Check (PSC) by using CLI. Use either of the following methods to run PSC and send data to IBM.

### Running MDC.sh file

Run the MDC.sh file to run PSC and send data to IBM.

### Procedure

1. To run PSC collection and send data to IBM, run `/opt/ibm/mdc/MDC.sh`.

The following series of actions are prompted. Enter Y or N depending on the action you want to take.
2. Would you like to change your information? Enter Y or N. Change your information if your enter Y.
3. Would you like to run connectivity test? Enter Y or N.

4. Would you like to run collection now? Enter Y or N.
5. Would you like to run PSC collection now? Enter Y.  
Microcode Data Collector lists the systems for which you have PSC contract.
6. Enter the corresponding numbers of the systems for which you want to run PSC collection. For example, **1 2 4 6 7 8**.  
Microcode Data Collector runs the PSC collection for the systems you entered.

## Running MDC.PSC.collector.sh file

Run the MDC.PSC.collector.sh <file name> to run PSC and send data to IBM.

### Procedure

1. Create a text file with the data for collecting PSC for systems that are in contract. A sample file PSC\_DEVICES.txt is created for you at /opt/ibm/mdc/bin.
2. Enter the type of the system followed by host name in the file.  
For example, **XIV, hostname1**.  
Repeat this step for all the systems you want to run PSC collection.
3. Save the file.
4. Run the **/opt/ibm/mdc/MDC.PSC.collector.sh PSC\_DEVICES.txt** command to run PSC.  
Microcode Data Collector runs the PSC collection for the systems you entered in the file.

## Sending data

Use this information to collect and send data to IBM.

### Procedure

- To collect and send data to IBM, run **/opt/ibm/mdc/MDC.callhome**.  
The status of the transmission to IBM is displayed.

## Uninstalling Microcode Data Collector

Use this information to uninstall Microcode Data Collector (MDC).

### Procedure

- To uninstall MDC, run **/opt/ibm/mdc/bin/MDC.uninstall.sh**

## Enabling call home for Tape Libraries

---

MDC uses the Call Home functionality that is available in the IBM Tape Library products.

To enable data collection for contracts supported by the Microcode Data Collector, you need to configure call home in the product. For more information, see the following links:

- [https://www.ibm.com/support/knowledgecenter/STCMML8/com.ibm.storage.ts3500.doc/ipg\\_3584\\_remote\\_support.html](https://www.ibm.com/support/knowledgecenter/STCMML8/com.ibm.storage.ts3500.doc/ipg_3584_remote_support.html)
- [https://www.ibm.com/support/knowledgecenter/STQRQ9/com.ibm.storage.ts4500.doc/ts4500\\_ipg\\_3584\\_remote\\_support.html](https://www.ibm.com/support/knowledgecenter/STQRQ9/com.ibm.storage.ts4500.doc/ts4500_ipg_3584_remote_support.html)

## Troubleshooting

---

Use this information to troubleshoot MDC problems or MDC installation problems.

### AIX VIOS Power System collection failed

If AIX VIOS Power System collection is failing, and in MDC logs, if you find an error message that contains *(ERROR) (PowerSystemsCollector.collect) (53) scp: /tmp/mdc\_collection/system/bin/MDC.aix.vios.collector: No such file or directory*, go through the following steps:

1. Check the `/etc/ssh/sshd_config` file on the VIOS system for the parameter **PermitUserEnvironment** that must be set to 'yes'.
2. If the parameter **PermitUserEnvironment** is either commented or set to 'no', change the value to 'yes'.
3. Refresh the SSH by using the following Start & Stop commands:
  - - stopsrc -s sshd
  - - startsrc -s sshd
4. Run the MDC collection again for the system.

### MDC installation

MDC installation is not supported from a network drive. MDC must be installed from local drive and must be installed to C: on Windows or \ on UNIX, and AIX.

### Installation log

Use the installation log file to troubleshoot installation problems. You can find the installation log in the same directory as the installation program. For example, `c:\temp\mdc.windows\install.log`.

### MDC log

Use the MDC log file to troubleshoot general MDC problems. You can find the MDC log at `/opt/ibm/mdc/logs/hostname.log` or `c:\opt\ibm\mdc\logs\hostname.log`.

### MDC - Run as administrator

Install and start MDC as administrator. Else, you get a message -

```
The installation / application has not been started with Administrator
privileges. Some functions might not be supported. Refer setup guide for more
information.
```

If you do not install and start MDC as administrator, you cannot do the following functions of MDC -

- Collection from DS3000, DS4000, DS5000 devices
- Collection from DS6000, DS8000 devices
- Collection from XIV Storage Systems
- Scheduling of the following registration tasks with operating system fails -
  - Auto Update
  - Heartbeat
  - Device collection
- System x DSA collection for local devices
- ESXi collection where **System to Run DSA** is localhost

## WMI repository

If installation fails and `install.log` or the `mdc/logs` contain the message - Looks like Windows Management Instrumentation Repository is corrupt, verify the WMI Repository status link.

To verify the WMI repository status, follow these steps:

1. Start the command prompt (`cmd.exe`) through "Run as Administrator".
2. Run the `winmgmt /verifyrepository` command, for example, `C:\>winmgmt /verifyrepository`.
3. If the status is not "**WMI repository is consistent**", see the following links to fix the WMI Repository -
  - <http://blogs.technet.com/b/askperf/archive/2012/03/09/unable-to-connect-to-wmi-locally-win32-the-system-cannot-find-the-path-specified.aspx>
  - <http://blogs.technet.com/b/askperf/archive/2008/07/11/wmi-troubleshooting-the-repository-on-vista-server-2008.aspx>

## Test connection to ESXi fails

SSH2 is used to verify the correctness of authentication details, but not for collection. If the test connection to ESXi fails, you can see the message - **Connection failed with return code 2** in MDC log file (`/opt/ibm/mdc/logs/<machinName>.log`). To fix the error, follow these steps:

1. Verify whether the SSH2 connection is open on the ESXi device through PuTTY.
2. If SSH2 connection exists but the authentication fails, follow these steps:
  - a. Log in to the ESXi device through PuTTY.
  - b. Run the command - `vi /etc/ssh/sshd_config`.
  - c. Change the **PasswordAuthentication** from no to yes.
  - d. Save the changes and test the ESXi device from the MDC.

## Unable to send files to IBM

On the **Test connectivity** page, verify whether you are able to connect to all the IP addresses on the ports. If there are any failures, verify the firewall settings. If you are connecting MDC to IBM support through a firewall, configure the firewall to allow communication with IBM. Ensure that the IP addresses and port numbers have bidirectional communication open.

**Note:** IP addresses might change, so ensure that you use DNS names whenever possible. To refer the DNS names, go through the following steps:

1. Click **Connectivity settings** tab.
2. Click **Test connection to IBM**.
3. Refer the DNS names on the MDC console. For more information on firewall configurations, see [MDC\\_ConnectivitySecurityWhitepaper](#).

If all the settings are fine and still the error persists, follow these steps:

1. Stop MDC application.
2. Clear all log files in `C:\opt\ibm\mdc\callhome_support\log\*.log`.
3. Edit `C:\opt\ibm\mdc\callhome_support\eccBase.properties` file and change **TRACE\_LEVEL=SEVERE** to **TRACE\_LEVEL=INFO**.
4. Start MDC and test connectivity.
5. Close MDC.
6. Send `C:\opt\ibm\mdc\callhome_support\log\eccTrace***.log` files to IBM support.

7. Restore the log settings, edit C:\opt\ibm\mdc\callhome\_support\eccBase.properties file, and change **TRACE\_LEVEL=INFO** to **TRACE\_LEVEL=SEVERE**.

## TGRI0001E: The application might not establish a connection to 10.0.19.11

If any device involves connection to Telnet, SSH2, or SMB protocol and you get this error message, check whether the **10.0.19.11** IP address is reachable. Also, check whether the service (Telnet or SSH2) is enabled on the remote system and it accepts connection from the MDC installed system.

## java.io.IOException: Connection failed with return code 5

The authentication might be failed due to wrong user name or password. Double-check the user name or password.

## Error while testing HMC connection with MDC

If you get the following error, when testing the HMC connection,

```
2014-07-31 09:59:16: (INFO) (StorageCollector.authenticationTest) Testing:
device host name or IP
```

```
2014-07-31 09:59:31: (ERROR) (StorageCollector.authenticationTest) exception:
java.io.IOException: Connection failed with return code 2
```

follow the steps that are given in this link, to enable the SSH2 connection on HMC, so that MDC installed device can connect to HMC. [https://www-304.ibm.com/servers/resourcelink/lib03030.nsf/pages/howtousesthehardwaremanagementconsole/\\$file/remote\\_operations\\_enabling1.htm](https://www-304.ibm.com/servers/resourcelink/lib03030.nsf/pages/howtousesthehardwaremanagementconsole/$file/remote_operations_enabling1.htm).

## Uninstalling IBM Microcode Data Collector fails on Windows

If uninstalling IBM Microcode Data Collector fails on Windows, follow these steps to complete the uninstallation.

1. Ensure that you have no applications currently accessing the c:\opt\ibm\mdc directory.
2. Delete the c:\opt\ibm\mdc directory.
3. Delete the MicrocodeDataCollector scheduled task.
4. Delete the shortcut **Start > Program Files > IBM Microcode Data Collector**.

## Utility or Fileset not found on Power Systems (AIX / VIOS)

The following utility or fileset are mandatory for microcode data collection on Power Systems (AIX / VIOS). If you get any error that is related to the following utility or fileset, then you might need to install the respective utility or fileset.

AIX / VIOS
Utility <ul style="list-style-type: none"><li>• awk</li><li>• sed</li><li>• lsvpd</li><li>• lsattr</li></ul>
Fileset <ul style="list-style-type: none"><li>• perl.rte</li><li>• bos.rte.serv_aid</li></ul>

## MDC Installation failed

While you install MDC, if the installation is failed and you get the following message - Installation aborted because upgrade version 3.5.5 and installed version is same., then it might be due to the following two reasons:

1. The provided MDC version is already installed on your system.
2. The installable MDC.<platform>.zip file is extracted to /opt/ibm/mdc folder and the **install.sh** command is run to install.

To resolve this issue, uninstall MDC through the following steps and then extract the MDC.<platform>.zip installable file to a temporary folder and not to the /opt/ibm/mdc, which is the directory to which the MDC gets installed.

1. Close MDC and any other folders that are related to MDC.
2. Click **MDC.uninstall.sh** file.
3. Click **Yes** on confirmation and you a message - IBM Microcode Data Collector uninstall successful is displayed on successful uninstallation.
4. To verify, go to /opt/ibm and see that **mdc** folder is not displayed.

## No supported terminal types found

After you install MDC, when you try to view the MDC UI by running the **MDC.sh** command, you might get the following error message - No supported terminal types found.. To clear this error, ensure to install the *xterm* or *gnome* terminal on the MDC installed system.

## System x file not found

An error message similar to the following example might be displayed during MDC upload.

```
Missing a system x file in Archive Explorer
```

To troubleshoot the problem, run the collection as root user, so that the DSA will be collected and transmitted successfully. For more information, see section [“Setting up IBM System x, Windows and ESX Server”](#) on page 13.

## An error occurred when writing to the remote file

An error message similar to the following example might be displayed during MDC data collection from Power server.

```
(PowerSystemsCollector.collect) (53) CTGRI0006E An error occurred when writing to the remote file named /mdcworkdir/ibmast/general
```

```
(MetricsController.associateSystems) Could not enroll profile for 172.16.50.69 (POWERSYSTEM) - Serial is null
```

To troubleshoot the problem, increase the disk space of /opt directory up to 3 GB, on your system. For more information, see section [“Prerequisites”](#) on page 2.

## Error retrieving service.tgz file

An error message similar to the following example might be displayed during MDC data collection for BladeCenter and Flex System Enterprise Chassis.

```
Collecting for BladeCenter and Flex System Enterprise Chassis: flex01.....  
Error retrieving service.tgz file
```

To troubleshoot the problem, replace the host name with the IP address of the BladeCenter or Flex System Enterprise Chassis.

## Run collection failed on an AIX device

An error message similar to the following example might be displayed during MDC data collection on a remote AIX device.

```
(ERROR) (PowerSystemsCollector.collect) (50) ERROR: This application is already installed on this system.
```

The error is occurred because the MDC is installed on the remote system also. To troubleshoot the problem, uninstall MDC on the remote AIX system and run the collection.

## proweb.cfg file is very large

An error message similar to the following example might be displayed while sending data to Proweb.

```
proweb.cfg file appeared to be growing and taking up a lot of file space
```

To troubleshoot the problem, check whether there are two versions of the SDDPCM (Subsystem Device Driver Path Control Module) on AIX / VIOS system and ensure delete the old version and maintain the latest SDDPCM.

## rksh: ioscli: not found

An error message similar to the following example might be displayed during MDC data collection from Power 9 VIOS LPAR

```
Get the platform failed, Error message is: rksh: ioscli: not found
```

To troubleshoot the problem, reconfigure the SSH client according to the instructions in the section: [“Reconfiguring SSH client for VIOS server” on page 46](#)

## DSA compatibility check ... FAILED

An error message similar to the following example might be displayed in System x (7915-AC1) running SUSE L Enterprise Server 12 (x86\_64).

```
DSA compatibility check ... FAILED. Please check your DSA selection.
```

To troubleshoot the problem, Get the latest (Lenovo Dynamic System Analysis (DSA)) drivers from the link- <https://datacentersupport.lenovo.com/us/en/downloads/DS504163>.

## Algorithm negotiation fail

An error message similar to the following example might be displayed if you run the MDC application on an unsupported operating system.

```
"Algorithm negotiation fail"
```

To troubleshoot the problem, install and run MDC only on the supported operating environment. For more information, see [Operating Environment](#) section.

## Scenario: MyCompany deploys Microcode Data Collector

---

Use this scenario to help you configure and set up your environment.

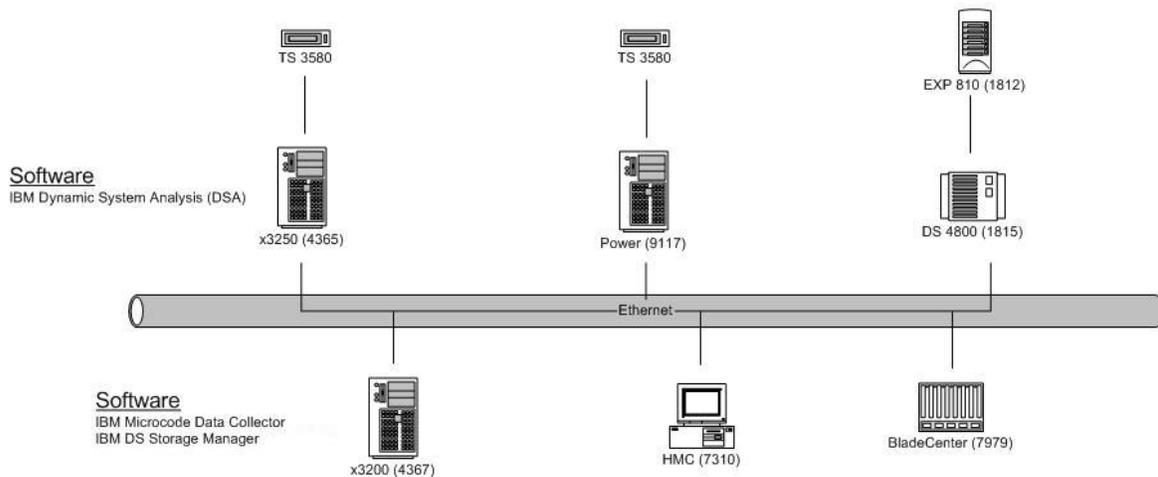
### Situation

MyCompany (a fictitious company) has a contract with the following system devices listed.

- 4365 (System x with SUSE Linux Enterprise Server 10)
- 7195 (System x with SUSE Linux Enterprise Server 12)
- 3580 (Tape drive that is attached to 4365)
- 9117 (Power System with AIX and VIOS LPARs)

- 3580 (Tape drive that is attached to 9117)
- 1815 (DS4800)
- 1812 (expansion enclosure that is attached to 1815)
- 4367 (System x with Windows 2003)
- 7310 (HMC)
- 7979 (Advanced Management Module (AMM) BladeCenter)

The following figure shows the configuration.



## Assumptions

MyCompany plans to:

- Install IBM Microcode Data Collector (MDC) on the 4367 system. MDC is being installed for the first time on the 4367 system.
- Install IBM DS Storage Manager on the 4367 system.
- Establish ssh connectivity with the 7310 HMC and 7979 BladeCenter Advanced Management Module (AMM).

The 3580 tape drive that is attached to the 4365 is automatically included in the collection. The 3580 tape drive that is attached to the 9117 on the AIX LPAR is included in the collection since the IBM Atape device driver is installed.

For the 7195 Lenovo System x system, get the suitable DSA driver from the link- <https://datacentersupport.lenovo.com/us/en/downloads/DS504163> and place it in the `/opt/ibm/mdc/portable_dsa` location.

## MDC installation

To install MDC, complete the following steps on 4367.

1. Download mdc.windows.zip from the following web page:  
[https://www.ibm.com/support/pages/esa/downloads\\_services.htm](https://www.ibm.com/support/pages/esa/downloads_services.htm)
2. Extract the installation files from the archive file.
3. Run the `install.bat` file. The MDC Installation wizard starts.
4. Read the License Agreement, the Non-IBM Terms and Conditions, and the License Information. Select **I accept both the IBM terms and the non-IBM terms**, and click **Next**.

5. Enter the activation key that you obtained from the IBM Premium Services support team and click **Next**.

6. On the **General Settings** page, enter the following information:

**IBM Customer Number**

12345

**Project name**

MyProject

**Environment**

Production

**Call home mode**

Automatic

**Auto Update mode**

Automatic

**CTS/ETS ProWeb ID**

Provide your Proweb ID. This information is mandatory for Proweb customers. Leave it empty if you are not a Proweb customer.

Click **Next**.

7. On the **Contact settings** page, enter the following information:

**Contact name**

John Smith

**Contact phone**

1234567890

**E-mail**

jsmith@mycompany.com

**Street**

12

**City**

Chicago

**State or province**

Illinois

**Country**

UNITED STATES

**Current Terms and Conditions**

Click **Current Terms and Conditions** to view the license information and also the GDPR compliant information.

Click **Next**.

8. On the **Scheduled tasks settings** page, specify the following:

**Enable**

Checked

**Day of month**

15

**Hour of day**

0

**Enable Heartbeat**

Checked

Click **Next**.

9. On the **Connectivity settings** page, select **Internet** and click **Next**.

10. Review the installation summary and click **Finish**. Leave **Launch the Microcode Data Collector when finished** checked.

11. When the Microcode Data Collector graphical user interface opens, click the **Connectivity settings** tab.
12. Click **Test connection to IBM**. The IBM Microcode Data Collector Console window opens and displays a successful connection to IBM.

## DS Storage Manager installation

To install DS Storage Manager, complete the following steps on 4367.

1. Go to [www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral).
2. Click **IBM Sign in**. Sign in with an IBM ID. If you do not have an IBM ID, you can register to create one.
3. Under **Product Group** select **System Storage**.
4. Under **Select from System Storage** select **Disk systems**.
5. Under **Select from Disk systems**, select **Mid-range disk systems**.
6. Under **Select from Mid-range disk systems** select **DS4800 Midrange Disk System**.
7. Under **Release** select **Disk-SM-v10.77.x5.28**.
8. Under **Platform** select **Windows 32-bit, x86**.
9. Click **Continue**.
10. Select **refresh pack: Disk-SM-Windows\_x64-Dec-2011-version-10.77.x5.28**.
11. Click **Continue**.
12. Click **Continue**.
13. Click **Download now**.
14. Double-click C:\Documents and Settings\Administrator\DownloadDirector\ibm\_sw\_ds3-5k\_10.77.xx.16\_windows\_intl386.zip
15. Navigate to WS03WS08\_10p77\_IA32/Windows.
16. Double-click SMIA-WS32-10.77.35.16.exe. The IBM Systems Storage DS Storage Manager window opens.
17. Click **OK**.
18. Click **Next**.
19. Click **Next**.
20. Select **I accept the terms of the License Agreement** and click **Next**.
21. Select **Custom** for installation type and click **Next**.
22. Select only the DS Storage Manager Client and click **Next**.
23. Select **Do not Automatically Start the Monitor** and click **Next**.
24. Click **Install**. When the installation program is finished, click **Done**.

## MDC configuration

To configure MDC, complete the following steps on 4367.

1. Access the Microcode Data Collector graphical user interface. See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5.
2. Click the **Identify Systems** tab.
3. On the **Identify Systems** page, make the following selections:
  - **IBM Power Systems**. A tab for the **IBM Power Systems** page is displayed. You can use this page to configure the 9117 LPARs.
  - **IBM HMCs**. A tab for the **IBM HMCs** page is displayed. You can use this page to configure the 7310.

- **IBM System x.** A tab for the **IBM System x** page is displayed. You can use this page to configure the 4365, 4367, and 7195 systems.
  - **IBM BladeCenter and Flex Chassis.** A tab for the **BladeCenters/Flex** page is displayed. You can use this page to configure the 7979.
  - **IBM DS3000, DS4000 and DS5000.** A tab for the **IBM DS3000, DS4000 and DS5000** page is displayed. You can use this page to configure the 1815.
4. Click the **IBM Power Systems** tab.
    - a. On the **IBM Power Systems** page, click **New**.
    - b. Enter `my9117a.mycompany.com` as the host name of the AIX LPAR of the MyCompany 9117.
    - c. Enter `root` as the user ID.
    - d. Enter `MyCompany4Ever` as the password and click **OK**.
    - e. Click **New**.
    - f. Enter `my9117v.mycompany.com` as the host name of the VIOS LPAR of the MyCompany 9117.
    - g. Enter `padmin` as the user ID.
    - h. Enter `MyVIOS4Ever` as the password and click **OK**.
    - i. Click **Test all**. Review the test results in the IBM Microcode Data Collector Console window.
  5. Click the **IBM HMCs** tab.
    - a. On the **IBM HMCs** page, click **New**.
    - b. Enter `my7310hmc.mycompany.com` as the host name of the 7310 MyCompany HMC.
    - c. Enter `mycompanyusername` as the user name
    - d. Enter `mycompanypassword` for the password and click **OK**.
    - e. Click **Test selected**. Review the test results in the IBM Microcode Data Collector Console window.
  6. Click the **IBM System x** tab.
 

Configure the 4365 System x system as follows:

    - a. On the **IBM System x** page, click **New**.
    - b. Enter `my4365.mycompany.com` as the host name of the 4365 System x system.
    - c. Enter `root` for the user name
    - d. Enter `myrootpassword` for the password.
    - e. Select portable DSA version `ibm_utl_dsa_dsy911-9.21_portable_sles10_i386.bin`.
    - f. Click **OK**.
    - g. Click **Test selected**. Review the test results in the IBM Microcode Data Collector Console window.

Configure the 4367 System x system as follows:

    - a. On the **IBM System x** page, click **New**.
    - b. Enter `my43657.mycompany.com` as the host name of the 4367 System x system.
    - c. Enter `Administrator` for the user name
    - d. Enter `myAdministratorpassword` for the password.
    - e. Select portable DSA version `ibm_utl_dsa_dsy911-9.21_portable_windows_i386.exe`.
    - f. Click **OK**.
    - g. Click **Test selected**. Review the test results in the IBM Microcode Data Collector Console window.

Configure the 7195 Lenovo System x system as follows:

    - a. On the **IBM System x** page, click **New**.
    - b. Enter `my43657.mycompany.com` as the host name of the 7195 System x system.
    - c. Enter `Administrator` for the user name.

- d. Enter myAdministratorpassword for the password.
  - e. Select portable DSA version lnvg\_y\_utl\_dsa\_dsala7j-10.4\_portable\_sles12\_x86-64.bin (that you have already downloaded from Lenovo site).
  - f. Click **OK**.
  - g. Click **Test selected**. Review the test results in the IBM Microcode Data Collector Console window.
7. Click the **IBM BladeCenter and Flex Chassis** tab.
    - a. On the **BladeCenters/Flex** page, click **New**.
    - b. Enter my7979hmc.mycompany.com as the host name of the 7979 BladeCenter Advanced Management Module (AMM).
    - c. Enter mycompanyusername as the user name
    - d. Enter mycompanypassword for the password and click **OK**.
    - e. Click **Test selected**. Review the test results in the IBM Microcode Data Collector Console window.
  8. Click the **IBM DS3000, DS4000 and DS5000** tab.
    - a. Verify that the Prerequisite CLI Location contains the location of the SMCLI: C:/Progra~1/IBM\_DS/client/SMcli.exe.
    - b. Click **Apply**.
    - c. Click **New**.
    - d. Enter my1815.mycompany.com as the host name of the MyCompany 1815.
    - e. Enter my1812.mycompany.com as the host name of the MyCompany 1812.
    - f. Enter 139801B as the serial number of the MyCompany 1815.
    - g. Click **OK**.
    - h. Click **Test all**. Review the test results in the IBM Microcode Data Collector Console window.

## Data collection

The data collection occurs automatically every month as follows:

1. The collection of the 4365 and 4367 begins on the 14th of the month when the scheduled task on each system starts to run.

The collected DSA data is sent to MDC.

Verify that the DSA data is received by MDC by clicking **General tasks and settings**, then clicking **View report list**. Look for the reports under **System x report(s) (DSA)**.

2. The collection of the 9117 and 1815 data begins on the 15th of the month.
3. Once the 9117 LPAR and 1815 data is collected, all the 4365, 4367, 9117, 3580, 1815, 1812, 7310, and 7979 data is sent to IBM.

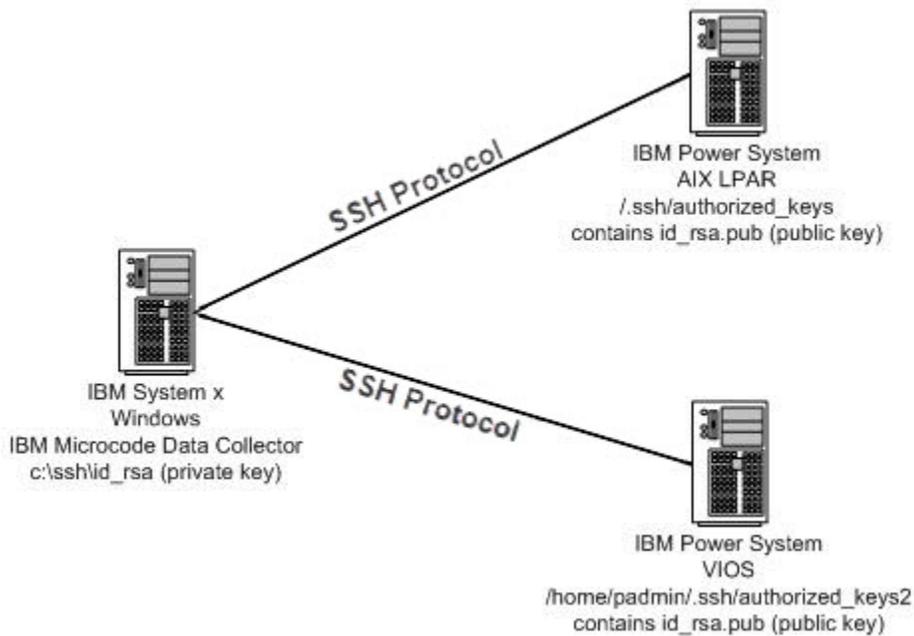
## Setting up public and private key authentication

---

To support secure data collection from IBM Power Systems that is running AIX, Linux, or VIOS, you can use public and private key authentication over the SSH2 protocol.

### Public and private key pair authentication

The following figure shows how this public and private key pair authentication works:



## Creating public and private key pairs

### Procedure

To create a public and private key pair on AIX, Linux, or VIOS, follow these steps:

1. On the command line, enter the command -

```
ssh-keygen -t rsa
```

**Tip:** On AIX, the SSH commands are in `/.ssh`. On Linux, the SSH commands are in `/root/.ssh`.

2. To use the default file and path name, press Enter.
3. Optional: Enter a passphrase.  
For example: MyCompany4Ever.

**Important:** Setting a passphrase enhances the security of the private key file. A good passphrase contains alphanumeric characters and is at least 10 characters long.

4. If necessary, enter the passphrase again.  
This operation creates the following files:

#### **/.ssh/id\_rsa**

This file is the private key file.

**Important:** Keep this file secure and protected.

#### **/.ssh/id\_rsa.pub**

This file is the public key file.

5. Append the contents of the public key file `id_rsa.pub` to the `authorized_keys` file `authorized_keys`, or `authorized_keys2`, as follows:

- On AIX or Linux:

```
cat /.ssh/id_rsa.pub >> /.ssh/authorized_keys
```

**Tip:** On AIX, both the `id_rsa.pub` file and the `authorized_keys` file are in `/.ssh`. On Linux, both the `id_rsa.pub` file and the `authorized_keys` file are in `/root/.ssh`.

- On VIOS:

```
cat /tmp/id_rsa.pub >> /home/padmin/.ssh/authorized_keys2
```

**Notes:**

- If the authorized\_keys file does not exist, create the file with the public key attached.
- If the authorized\_keys file exists, remove any old key entries for Microcode Data Collector from the file.
- Ensure that the permissions on this file are set to 600. To change the file permissions, run the **chmod** command as follows:
  - On AIX or Linux:

```
chmod 600 /.ssh/authorized_keys
```

**Tip:** On AIX, the authorized\_keys file is in /.ssh. On Linux, the authorized\_keys file is in /root/.ssh.

- On VIOS:

```
chmod 600 /home/padmin/.ssh/authorized_keys2
```

- Ensure that the owner of the file is root or admin. To change the owner of the file, run the **chown** command as follows:
  - On AIX or Linux:

```
chown root /.ssh/authorized_keys
```

- On VIOS:

```
chown padmin /home/padmin/.ssh/authorized_keys2
```

6. If you did not create the key pair on the system on which MDC is installed, create a C:\ssh directory on the system on which MDC is installed. And then, Copy the private key file id\_rsa to the c:\ssh directory on the system on which MDC is installed.

## Configuring public and private key authentication

---

### Procedure

To configure public and private key authentication for an IBM Power Systems, IBM SAN Volume Controller, and IBM Storwize systems, follow these steps:

1. Access the Microcode Data Collector graphical user interface. See [“Accessing the Microcode Data Collector graphical user interface”](#) on page 5
2. Click the **Centralized Key Management** tab.
3. Click **New**.
4. **Browse** the **Private Key Location**  
For example, /.ssh/key.
5. Optional: Enter the **Passphrase**.  
For example, mypassphrase.

**Important:** Specifying a passphrase enhances the security of the private key file. A good passphrase contains alpha numeric characters and is at least 10 characters long.

6. Click **OK**
7. If you have more keys, repeat from step [“3”](#) on page 44 for each key.
8. To delete a specific key, select the key and click **Delete**. Click **Yes** on the **Please confirm deletion** window.

## Setting up target devices for System x (Windows)

---

Use this information to set up System x systems that run on Windows for collecting data through MDC.

### About this task

Microcode Data Collector 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 over TCP/IP, for which port 445 must not be blocked by firewalls or IP security policies. Select **Disable NetBIOS over TCP/IP** in the **Control Panel** settings for the system's network connections properties (**Control Panel > Network and Dial-Up Connections (any connection) > Properties > Internet Protocol (TCP/IP) > Advanced > WINS > Disable NetBIOS over TCP/IP**).

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

To determine whether security policies are blocking these ports, click **Start > Settings > Control Panel > Administrative Tools**.

Choose the following navigation, which is based on whether your policies are stored locally or in an Active directory:

- **Locally stored policies:**

- Administrative Tools > Local Security Policy > IP Security Policies on Local Computer.

- **Policies stored in Active Directory:**

- Administrative Tools > Default Domain Security Settings > IP Security Policies on Active Directory
- Administrative Tools > Default Domain Controller Security Settings > IP Security Policies on Active Directory

Examine the IP security policies and edit or remove filters that block the ports. Ensure that port 445 currently used by MDC is not blocked.

The target device must have the Remote Registry service started (which is the default configuration) for MDC to connect to the target device.

MDC requires access to the hidden remote administrative disk share, for access to the system %TEMP% and other directories. Access to the Interprocess Communications share (IPC\$) is also required for MDC to access remote registries.

Before you access Interprocess Communications share (IPC\$), make sure that the Server service, **Control Panel > Administrative Tools > Services > Server** is started.

## Operating systems information

**Windows Server 2008:** On Windows Server 2008, you might need to disable **User Account Control**, if your account is not a domain user 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 you to do several steps before MDC can communicate with Vista targets.

If you have a domain user account, ensure that the local and the target devices are both members of a Windows domain.

If you are a member of a local administrators group and you use a local user account, complete the following steps to do administrative tasks on the target device:

1. Enable the built-in Administrator account and use it to connect. To enable the built-in Administrator account, open the Windows **Control Panel** and click **Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options**. Then, double-click **Accounts: Administrator account status** and select **enable**.
2. Disable User Account Control if a different Administrator user account is to be used to connect to the Vista target. To disable **User Account Control**,

- a. Open the Windows **Control Panel**
  - b. Click **Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options**
  - c. Double-click **User Account Control: Run all administrators in Admin Approval Mode** and select **disable**.
  - d. Restart your system
3. Disable **User Account Control** when you administer a workstation with a local user account (Security Account Manager user account). Otherwise, you cannot be a full administrator and cannot do administrative tasks. To disable User Account Control, perform the following steps:
- a. Click **Start > Run**
  - b. Type `regedit`, and then press **ENTER**
  - c. Locate and click this registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
  - d. If the `LocalAccountTokenFilterPolicy` registry entry does not exist, follow these steps:
    - i) On the **Edit** menu, point to **New**, and then click **DWORD Value**.
    - ii) Type `LocalAccountTokenFilterPolicy`, and then press **ENTER**.
    - iii) Right-click **LocalAccountTokenFilterPolicy**, and then click **Modify**.
    - iv) In the Value data box, type `1`, and then click **OK**
    - v) Restart your computer

**Note:** Alternatively, to manually modify the registry entry, use this command prompt -

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

**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.

To check whether the Remote Registry service is enabled and started:

1. Go to **Start**.
2. In the **Start Search** box, type `services.msc`. Press **ENTER**.
3. When Microsoft Management Console starts, in the console window, ensure that the service status is started. If not, right-click **Remote Registry**, and click **Start**.

To avoid problems with the manual startup, set the **Remote Registry service startup type** to automatic.

If you want to automatically start the service after the server start:

1. Right-click **Remote Registry** and select **Properties**.
2. In the Startup type option, choose **Automatic**.
3. Click **Apply** and **OK**

When the system starts up, Remote Registry starts automatically.



Figure 1. BMC

## Reconfiguring SSH client for VIOS server

---

To execute commands remotely to VIO server as `padmin` user via SSH, reconfigure the SSH client through the following steps:

1. Example of remote command execution failing from an SSH client to the padmin user on a VIO server.

SSH Client:

```
# ssh padmin@<VIO server> ioscli ioslevel
```

```
# ssh padmin@<VIO server> ioscli lslparinfo
```

```
rksh: ioscli: not found
```

2. Get to the root prompt on the VIO server.

```
$ whoami
padmin

$ oem_setup_env
#
```

3. Link /usr/ios/cli/environment to /home/padmin/.ssh/environment

```
# cat /usr/ios/cli/environment
PATH=/usr/ios/cli:/usr/ios/utills:/usr/ios/lpm/bin:/usr/ios/oem:/usr/ios/ldw/bin:$HOME

# ls -l /home/padmin/.ssh/environment (Link is not there).
/home/padmin/.ssh/environment not found

# cd /home/padmin/.ssh
# ln -sf /usr/ios/cli/environment environment
lrwxrwxrwx 1 root system 24 Dec 19 08:28 /home/padmin/.ssh/environment -> /usr/ios/cli/environment

# ls -l /home/padmin/.ssh/environment
lrwxrwxrwx 1 root system 24 Dec 19 08:28 /home/padmin/.ssh/environment -> /usr/ios/cli/environment
```

4. Edit /etc/ssh/sshd\_config. Uncomment the PermitUserEnvironment directive and change from its default of no to yes.

```
# vi /etc/ssh/sshd_config
```

Change from:

```
#PermitUserEnvironment no
```

Change to:

```
PermitUserEnvironment yes
```

5. Stop and restart sshd

```
# stopsrc -s sshd
# startsrc -s sshd
```

6. Test ssh remote command execution from SSH client to VIO server as the padmin user.

```
# ssh padmin@<VIO server> ioscli ioslevel
2.2.2.1
```

```
# ssh padmin@<VIO server> ioscli lslparinfo
1 VIO-Server-1
```

Successfully executed remote command as padmin user via ssh.

#### Note:

1. You can also configure SSH public/private keys between an SSH client and the VIO server for the padmin user to avoid having to supply the padmin password for each command execution.
2. From sshd man page:

```
PermitUserEnvironment
```

Specifies whether `~/.ssh/environment` and `environment=` options in `~/.ssh/authorized_keys` are processed by `sshd(8)`. The default is "no". Enabling environment processing might enable users to bypass access restrictions in some configurations by using mechanisms such as `LD_PRELOAD`.

## Notices

---

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

## Trademarks

---

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be

trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

## Accessibility

---

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties using the PDF files and want to request a Web-based format for a publication, mail a request to the following address:

International Business Machines Corporation  
Information Development  
Department GZW  
9000 South Rita Road  
Tucson, Arizona 85744-001 U.S.A

In the request, be sure to include the publication number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.



