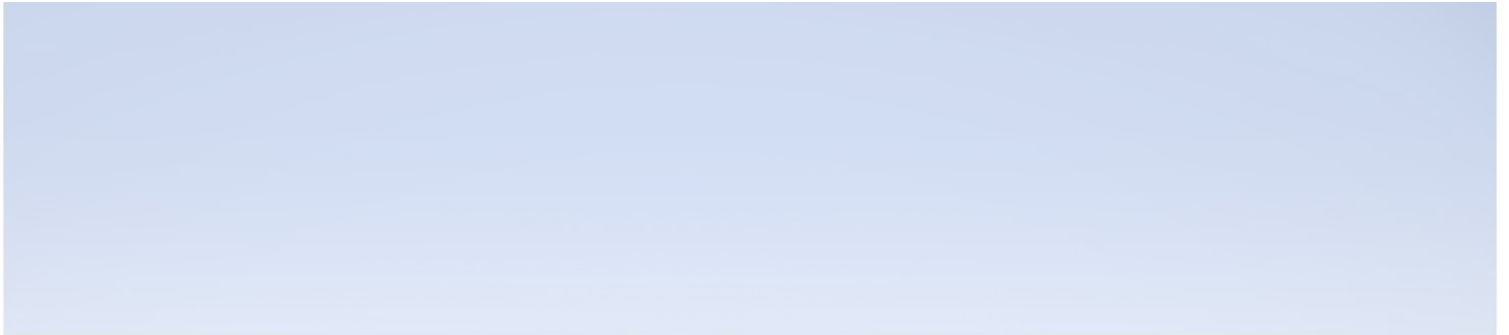# Diagnostics

Version 9.51, Released November 2018

Collector Installation Guide

Published November 2018

Legal Notices

Disclaimer

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Java is a registered trademark of Oracle and/or its affiliates.

Oracle® is a registered trademark of Oracle and/or its affiliates.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by the Spice Group (http://spice.codehaus.org).

For information about open source and third-party license agreements, see the *Open Source and Third-Party Software License Agreements* document.

Contents

Welcome To This Guide

Welcome to the Micro Focus Diagnostics Collector guide. This guide provides information about how to install and configure the Diagnostics collector.

How This Guide Is Organized

This guide contains the following chapters:

Diagnostics Documentation

Diagnostics includes the following documentation. Unless specified otherwise, the guides are in PDF format only and are available from the Software Support web site (https://softwaresupport.softwaregrp.com/) .

- **Diagnostics User Guide and Online Help:** Explains how to choose and interpret the Diagnostics views in the Diagnostics Enterprise UI to analyze your monitored applications. To access the online help for Diagnostics, choose **Help** > **Help** in the Diagnostics Enterprise UI. If Diagnostics is integrated with another Micro Focus Software product the online help is also available through that product's Help menu. The User Guide is a PDF version of the online help and their content is identical. The User Guide is available from the Diagnostics online help Home page, from the Windows Start menu (open **User Guide**), or from the Diagnostics Server installation directory.

- **Diagnostics Server Installation and Administration Guide:** Explains how to plan a Diagnostics deployment, and how to install and maintain a Diagnostics Server.

  The following Agent guides contain content that supports agent installation, setup and configuration.

  - **Diagnostics Java Agent Guide:** Describes how to install, configure, and use the Diagnostics Java Agent and the Diagnostics Profiler for Java.

  - **Diagnostics .NET Agent Guide:** Describes how to install, configure, and use the Diagnostics .NET Agent and Diagnostics Profiler for .NET.

- **Diagnostics Collector Guide:** Explains how to install and configure a Diagnostics Collector.

- **Diagnostics System Requirements and Support Matrixes Guide:** Describes the system requirements for the various Diagnostics components.

- **Release Notes:** Provides last-minute new information and known issues about each version of Diagnostics. The PDF file is also located in the Diagnostics installation disk root directory.

- **Diagnostics Data Model and Query API:** Describes the Diagnostics data model and the query API you can use to access the data. The guide is also available from the Diagnostics online help Home page.

- **Diagnostics Frequently Asked Questions (FAQ):** Gives answers to frequently asked questions. The FAQ is also available from the Diagnostics online help Home page.

Chapter 1: Installing Diagnostics Collectors

You can install Diagnostics Collector on Windows and UNIX machines.

This chapter includes:

About Installing the Diagnostics Collector

The Diagnostics Collector gathers data from remote systems. You can configure the Collector to collect performance data from the following types of active systems:

- SAP NetWeaver–ABAP
- Oracle Databases (including Oracle RAC)
- IBM WebSphere MQ
- TIBCO Enterprise Message Service (EMS)
- Software AG webMethods Broker
- SQL Server Databases
- VMware vCenter or VMware ESX Servers

During the installation of the Collector, you can choose to monitor any of these active systems. After the installation, you define instances of Oracle Databases, SQL Server systems, VMware vCenter or VMware ESX servers, IBM WebSphere MQ messaging systems, TIBCO EMS systems, Software AG webMethods Broker and SAP NetWeaver–ABAP systems to be monitored. Each monitored instance is represented by a probe entity. Multiple probes can be configured for each Collector.

> **Note:** The Collector can be installed on any machine. It does not necessarily have to be installed on the host machine of the SAP, Oracle, MQ, Tibco EMS, webMethods Broker, VMware or SQL Server

application. For Collector host system requirements, see "Requirements for the Diagnostics Collector Host" in the relevant version of the **Diagnostics System Requirements and Support Matrices Guide** on the Software Support site (https://softwaresupport.softwaregrp.com/group/softwaresupport/).

Requirements for the Diagnostics Collector Host

For Collector host system requirements, see "Requirements for the Diagnostics Collector Host" in the relevant version of the **Diagnostics System Requirements and Support Matrices Guide** on the Software Support site (https://softwaresupport.softwaregrp.com/group/softwaresupport/).

Launching the Diagnostics Collector Installer

The installation can be launched by downloading the installer from the Micro Focus Software Download Center, or by selecting it from the Diagnostics Downloads page in BSM/APM. This section describes how to access the installers and launch them on Windows and UNIX operating systems. For Linux, follow the UNIX instructions. For installing on other platforms, see "Installing the Diagnostics Collector Using the Generic Installer" on page 1.

To run a silent installation, see "Silent Installation of the Diagnostics Collector" on page 11.

To download the installer from the Micro Focus Software Download Center:

1. Access the Software Download Center at the Software Support web site (https://softwaresupport.softwaregrp.com/). This web site requires Passport login.

2. Locate the relevant **Diagnostics** information and select the appropriate link for downloading the Diagnostics Collector software.

3. Extract the contents of the downloaded .zip file.

4. Run the installer.

   On Windows platforms:

   Double-click the executable file **DiagCollector_<release number>_win64.exe**.

   On UNIX platforms:

   - To run the installer in graphical mode, set the display options as needed and then specify the **DiagCollector_<release number>_linux64_setup.bin** filename at the command prompt; for example:

     ```
     export DISPLAY=<hostname>:0.0
     ```

     The "xhost +" command must have been executed on the host where the installation is to be displayed (the <hostname> used in the export command).

   - To run the installer in console mode, specify the **DiagCollector_<release number>_<platform>_ setup** filename with the **-console** option, at the command prompt; for example:

     ```
     ./DiagCollector_9.51_linux64.bin -i -console
     ```

Continue with "Installing the Collector" on the next page.

To download the installer from the BSM/APM Diagnostics Downloads page:

1. In **APM**, select **Admin > Diagnostics** from the top menu and click the **Downloads** tab.

2. On the Downloads page, click the appropriate link to download the appropriate Collector installer.

> **Note:** The Collector installer is available in APM if it has been placed in the required directory for APM to access. After installing the Diagnostic Server, the Diagnostics Agent and Collector installers can be manually copied from the installation disk to the **<diag_server_install_dir>/html/opal/downloads** folder of the Diagnostics Server installation directory. For further information, see the Diagnostics Server Installation and Administration Guide.

Continue with "Installing the Collector" below

Installing the Collector

> **Note:** If there is a pre-existing installation of the Collector on the host machine, you must follow the instructions for upgrading the Collector instead of these install instruction, see "Upgrading the Collector" on page 30

After you launch the installer, the software license agreement opens.

To install a Collector:

1. Select a language and click **OK**.
    The Introduction window appears.

2. Click **Next**.
    The License Agreement window opens.

3. Accept the software license agreement.

    Read the agreement and select **I accept the terms of the license agreement**. In console mode press **Enter** to continue through the license agreement and when prompted, enter **1** to accept the agreement.

4. Click **Next** to continue. The Product Requirements window opens.

5. Click **Next** to continue. The Product Customization window opens.

6. Specify the location to install the Collector.

    In the **Installation Directory Name** box, accept the default directory, **C:\MercuryDiagnostics\Collector** or click **Browse** to navigate to another directory. In this documentation this directory is referred to as **<collector_install_dir>**.

    If the directory contains an existing installation of the Collector you want to upgrade, cancel this installation and follow the upgrade procedure for Collectors as described in "Upgrading the Collector" on page 30.

7. Click **Next** to continue. The Pre-Install Summary window opens.

8. Click **Install** to begin the installation process.

9. Assign a unique name to the Collector.
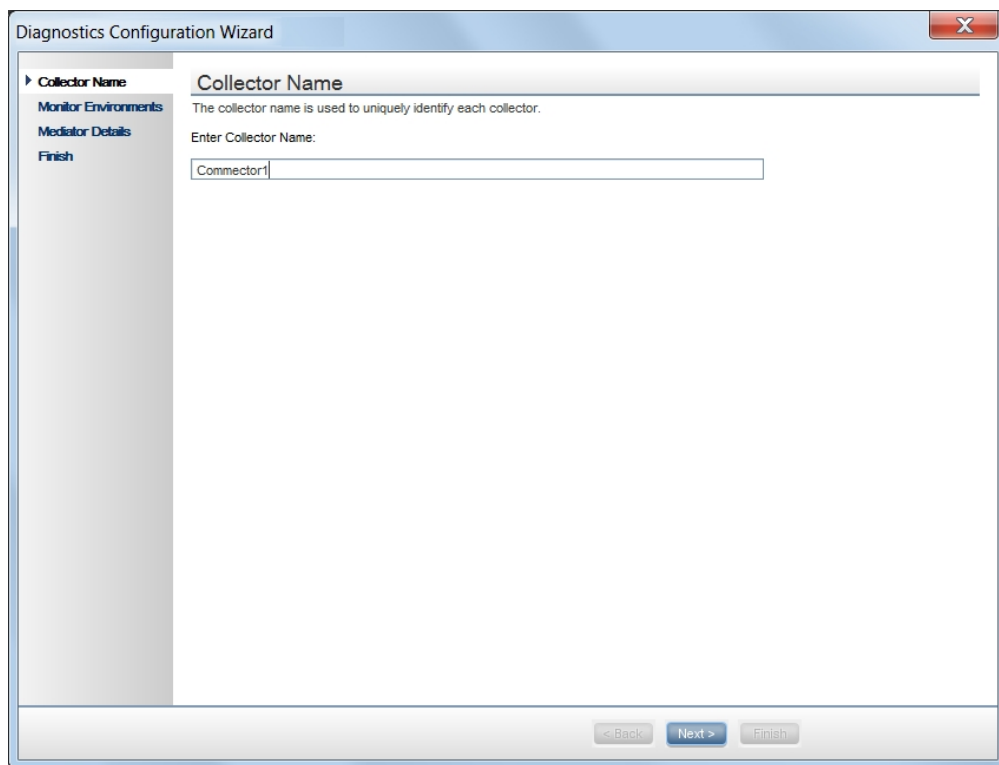
Assign a name to the Collector that uniquely identifies this specific Collector.

You can use **-** , **_** and all alphanumeric characters in the name.

Click **Next** to continue.

10. Select the environment to monitor.
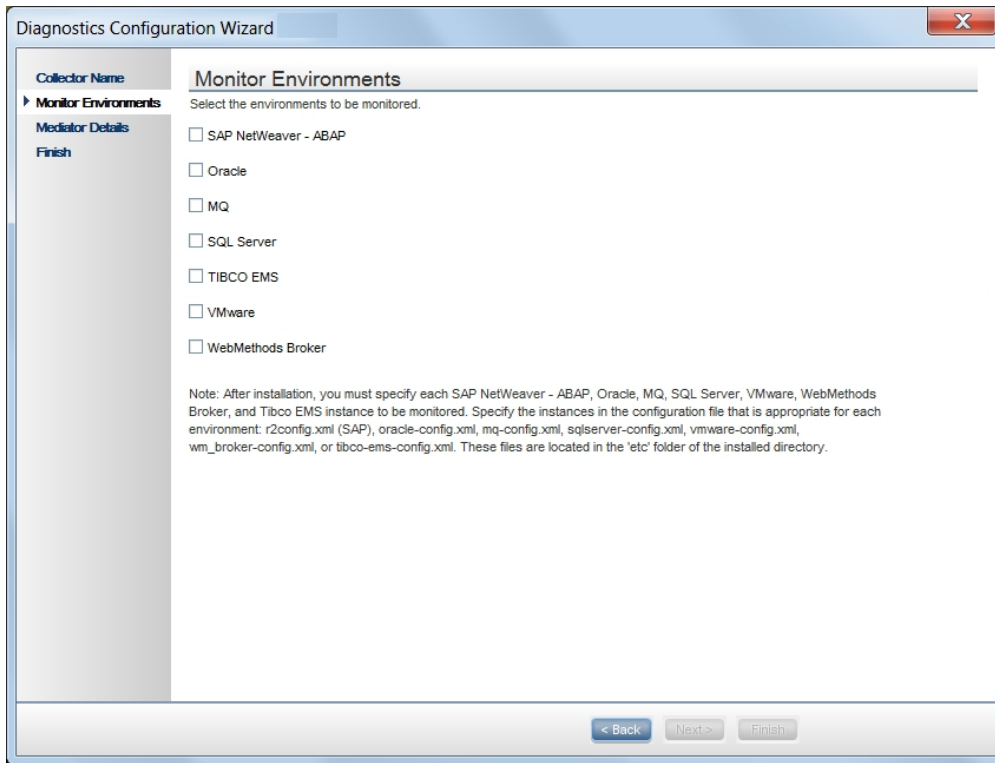
Select the options that apply to this Collector. You can select one or more options.

- **SAP NetWeaver–ABAP:** Collect data in an SAP NetWeaver–ABAP environment .

- **Oracle:** Collect data from an Oracle 10g database server.

- **MQ:** Collect data in an MQ series environment.

- **SQL Server:** Collect data from an SQL Server database.

- **VMware:** Collect data from either a VMware vCenter or a VMware ESX server.

- **TIBCO EMS:** Collect data from a TIBCO EMS environment.

- **WebMethods Broker:** Collect data from a webMethods Broker system .

> **Note:** After installation, specify each of the SAP NetWeaver–ABAP, Oracle, MQ, TIBCO EMS, SQL Server, webMethods Broker and VMware instances to be monitored. These instances are manually defined in the XML files provided with the installation. For more information, see "Configuring the Active System Property Files" on page 17.

11. If you selected SAP NetWeaver–ABAP in the previous step, copy the following files from SAP Java Connector install directory to the <collector_install_dir>\lib directory on the system where the collector is installed.

- `sapjco.jar`

- `librfc.dll` or `librfc32.dll` or `librfccm.so`

- `sapjcorfc.dll` or `libsapjcorfc.so`

If you do not know the SAP Java Connector directory name or if any of these files are missing from the directory, contact your SAP representative.

If you selected Tibco EMS in the previous step, copy the following third party jars after installation: `tibjms.jar, tibjmsadmin.jar,` and `jms-2.0.jar`. The files are typically found in your TIBCO EMS installation in the `<Tibco_EMS>/ems/<version>/lib` directory and you copy them to the `<collector_install_dir>\lib` directory on the system where the Collector is installed.

If you selected webMethods Broker in the previous step, copy the following third party jars after installation: `wm-brokerclient.jar, wm-g11nutils.jar`. The files are typically found in your Software AG installation in the `<SoftwareAG>/common/lib` directory and you copy them to the `<collector_install_dir>\lib` directory on the system where the Collector is installed.

12. Click **Next** to continue.

13. Provide information about the Diagnostics mediator server.

    Provide the details that enables communication with the Diagnostics mediator server.
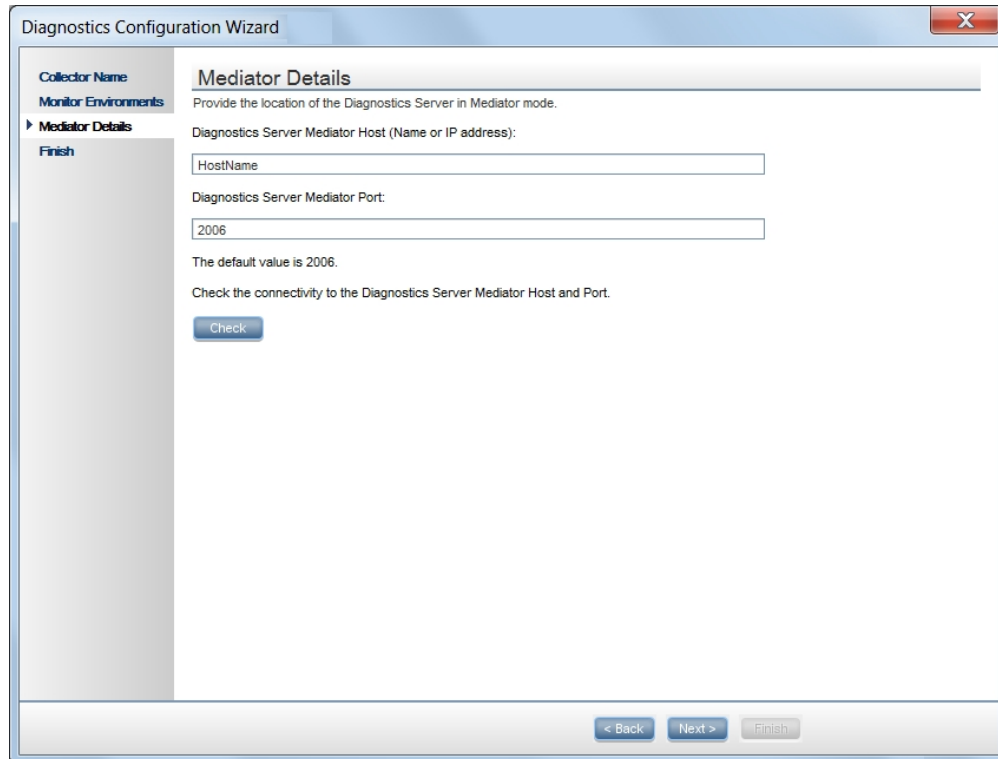
If there is only one Diagnostics Server in the Diagnostics deployment where the Collector will run, enter the host name of the Diagnostics Server and its event port information.

If there is more than one Diagnostics Server in the deployment, enter the information for the Diagnostics mediator server that is to receive the events from the Collector.

- **Diagnostics Server Mediator Host:** The host name or IP address of the host for the Diagnostics mediator server.

  > **Note:** You must specify the fully qualified host name. In a mixed OS environment, where UNIX is one of the systems, this is essential for proper network routing.

- **Diagnostics Server Mediator Port:** The port number where the Diagnostics Server is listening for Collector communication. The default port number is **2006**. If you changed the port since the Diagnostics Server was installed, specify that port number instead of the default.

  To make sure that the Diagnostics Server is running and accessible from the installation host, click **Check**.

14. Click **Next** to continue.
    The installation completes.

    When the installation completes, a message is displayed confirming that the Collector is successfully installed. Click **Done** to exit the installer.

15. Configure the XML files for your active systems.

    In step "Select the environment to monitor." on page 9 you selected the active systems to be monitored. For each of these active systems, you must configure properties that enable the Collector host and the active system host to communicate.

    For instructions on configuring the relative active system properties, see "Configuring the Active System Property Files" on page 17.

16. Verify that the Collector was installed properly and is running.

    The Collector starts running automatically when the installation is complete. You can verify the Collector installation by checking the **collector.log** file for errors. For details see, "Verifying the Diagnostics Collector Installation" on page 14.

    In the Diagnostics UI, each collector instance is represented as a probe entity of the system type: Oracle probe, SAP probe, MQ probe, EMS probe, WM probe or SQL Server probe.

Silent Installation of the Diagnostics Collector

A *silent installation* is performed automatically, without the need for user interaction. In place of user input, the silent installation takes values from the file *ovinstallparams.ini*. You can edit this file with a standard text editor.

For example, a system administrator who needs to deploy a component on multiple machines can use the *oviinstallparams.ini* file that contains all the prerequisite configuration information, and then perform a silent installation on multiple machines. This eliminates the need to provide any manual input during the installation procedure.

You can get the *oviinstallparams.ini* file from one of the following locations:

- The file is available as part of the install download along with the binaries. It is located in the **examples\silent_installation** directory.
- This document has an example file that you can copy, see Example oviinstallparams.ini File.

To perform a silent installation

1. Place the **oviinstallparams.ini**file in the same directory as the installer binary file.
2. To run the installer in silent mode , specify the **DiagServer_<release number>_<platform>_setup.bin**

or **DiagServer_<release number>_<platform>.exe** with the –i silent option at the command prompt. For example,

```
DiagServer_<release number>_<platform>.bin –i silent
```

Example oviinstallparams.ini File

Following is an example of the oviinstallparams.ini file which you can modify as required.

```
#=========================================================================================
#= Sample ovinstallparams.ini file
#= To install Diagnostics in non-interactive (silent) mode, edit this file according
#= to your needs and place it in the same folder where DiagCollector_<release number>_win64_
setup.exe file and
#= "packages" folder are.
#=
#= For silent installation, run the installer with "-i silent" flag
#= Example: DiagCollector_<release number>_win64_setup.exe -i silent (Windows)
#= DiagCollector_<release number>_linux64_setup.bin -i silent (Unix)
#=
#= Note: We do not recommend changing the installer properties parameters that follow.
#=========================================================================================
[installer.properties]
setup=DiagCollector
licenseAgreement=true
#=========================================================================================


#=========================================================================================
#= [Windows only] Installation folder. The path cannot contain spaces and must end with
#= "Collector". Note: On Unix systems, Diagnostics installation folder is set
#= to "/opt/HP/HPEDiagCollector" and cannot be changed
#=========================================================================================
prodInstallDir=C:\MercuryDiagnostics\Collector\
#=========================================================================================
#= User Input Field - id
#=========================================================================================
collectorId.id=GenericCollector
#=========================================================================================
#=User Input Field - collectors
#=========================================================================================
collectors=Oracle,MQ,SQL_Server,VMware,EMS,WM_BROKER
#=========================================================================================
#=User Input Field - host
#=========================================================================================
mediatorInfo.host=localhost
#=========================================================================================
#=User Input Field - port
#=========================================================================================
mediatorInfo.port=2006
```

How to Manually Add Another Collection Type After Installation

During the initial installation of the Collector you select the different collection types or types of active systems you want to monitor such as SAP or Oracle. After installing the Collector you can add another

collection type or active system type manually.

To manually add another type of active system:

1. Manually copy any required files to the **<collector_install_dir>\lib** directory. These files are required for SAP, Tibco EMS and webMethods Broker active systems. See the installation instructions for details on what files are required. Other types of collection such as Oracle or SQL Server do not require this step.

2. On the system where you installed the Collector, in the **<collector_install_dir>\etc\collector.properties** file edit the **active.systems** property to add the additional collection type. Valid values (case insensitive) are SAP_R3, Oracle, MQ, SQL_Server, VMWARE, EMS, WM_BROKER.

Configuring for Firewalls, HTTPS, and Proxies

The Collector requires additional configuration if it is being deployed into an Enterprise Diagnostics environment that includes firewalls, SSL-enabled communications, and proxies. This configuration is described in the Diagnostics Server Installation and Administration Guide. See the following sections:

- "Configuring Diagnostics Servers and Agents for HTTP Proxy"
- "Configuring Diagnostics to Work in a Firewall Environment"
- "Enabling HTTPS Between Components"

Password Obfuscation

Create an obfuscated password using the web application included with Diagnostics. Access the Security page (http://<host name>:2006/security) and select **Encrypt Password** at the bottom of the page. Replace <host name> with the name of the computer on which the Diagnostics server is installed.

The obfuscated password you generate can be used in the following xml files for the different collection types:

- **r3config.xml** file used to configure the SAP NetWeaver–ABAP collector
- **oracle-config.xml** file used to configure the Oracle collector
- **vmware-config.xml** file used to configure the VMware collector
- **tibco-ems-config.xml** file used to configure the TIBCO EMS collector
- **sqlserver-config.xml** file used to configure the SQL Server collector.

Enter the plaintext password, re-enter the password to confirm, and select the **Encrypt Password** button. The obfuscated password is displayed. Copy the entire obfuscated password from this page, including the OBF: at the beginning, and paste that into the appropriate property file (**r3config.xml**, **oracle-config.xml**, **vmware-config.xml, tibco-ems-config.xml** or **sqlserver-config.xml**).

> **Note:** You can continue to use the plaintext password property.

A **security.encrypted-password** property can also be used for the *mercury* user password in the following property files: **collector.properties**, **dispatcher.properties**, **server.properties**. The *mercury* user is used for authentication between the various diagnostics components. The following is a copy of the affected section of these properties files:

```
################################################################
```

```
# Remote Server Authentication Properties
#######################################################################
#
# This user name and password is used for communication between Diagnostics
# components (probes, and servers). You may want to change this password
# every so often to keep your system secure inside your enterprise. If you
# do change this password, you must first use
# http://<host name>:2006/security and select Encrypt Password to encrypt the
# password.
# Plaintext passwords can be used by replacing the security.encrypted-password
# with security.password. You must also change the encrypted password in the
# <install-dir>/etc/.htaccess file, as well as all the Diagnostics probe, and
# servers, that communicate with each other in your enterprise.
#
security.username=mercury
security.encrypted-password=OBF:1c431jg81hv41k1d1l161wu81z0d1pyl1wmt1n6h1y
m71n511wnd1pw11z0h1wu61kxw1jyl1hse1jd21c2z
```

Verifying the Diagnostics Collector Installation

The Collector starts running automatically when the installation is complete. You can verify the Collector installation by checking the **collector.log** file for errors.

Once a collector probe instance is started you can launch the Diagnostics Enterprise UI to verify that the probe is working. Go to
http://<Diagnostics_commander_server>:2006/. For now you can use the default user/password of **admin/admin** or the login you were given if a different one has been set up for you.

You can also check the System Health view to find information about the Collector deployment and the machine that hosts the collector.

To access the System Views:

1. Open the Diagnostics UI as the System customer from
   http://<Diagnostics_Commanding_Server_Name>:2006/query/.

2. In the query page locate the System customer in the list and select the link to Open Diagnostics.

3. Log in to Diagnostics and on the Applications window select **Entire Enterprise** and select any link to open the Diagnostics Views.

4. In the Views pane you see the System Views view group. Open the view group and select either the **System Health** view or **System Capacity** view.

Starting and Stopping the Diagnostics Collector

To start the Collector on a Windows machine:

Execute **Start Diagnostics Collector** from the computer's Start menu. Or enter **net start "HPE Diagnostics Collector"** at the command line.

To stop the Collector on a Windows machine:

Execute **Stop Diagnostics Collector** from the computer's Start menu. Or enter **net stop "HPE Diagnostics Collector"** at the command line.

> **Note:** The *nanny* is a process that runs as a daemon to ensure that the Collector is always running. The following two procedures start and stop the Collector using the nanny.

To start the Collector on a Linux machine (using the nanny):

1. Make sure that the **M_LROOT** environment variable is defined as the root directory of the Collector. For example, in *ksh*, you could enter the following:

   ```
   export M_LROOT=<collector_install_dir>/nanny/linux
   ```

   If the **M_LROOT** environment variable is not defined as the root directory, you will see the following error:

   ```
   Warning : MDRV: cannot find lrun root directory . Please check your M_LROOT
   Unable to format message id [-10791]
   m_agent_daemon ( is down )
   ```

2. Change directories to **$M_LROOT/bin**.

3. Run **m_daemon_setup** with the **-install** option, as in the following example:

   ```
   cd $M_LROOT/bin
   ./m_daemon_setup -install
   ```

To stop the Collector on a Linux machine (using the nanny):

1. Change directories to **$M_LROOT/bin** as set in the start procedure above.

2. Run **m_daemon_setup** with the **-remove** option, as in the following example:

   ```
   cd $M_LROOT/bin
   ./m_daemon_setup -remove
   ```

To start the Collector on a Linux machine (without using the nanny):

Run **<collector_install_dir>/bin/collector.sh**.

To stop the Collector on a Linux machine (without using the nanny):

Terminate the process using a utility such as **kill**.

Determining the Version of the Diagnostics Collector

When you request support, it is useful to know the version of the Diagnostics Collector. The version number of the Collector can be found in the **<collector_install_dir>\version.txt** file.

Uninstalling the Diagnostics Collector

To uninstall the Collector:

- On a Windows machine, execute **Uninstall Diagnostics Collector** from the computer's Start menu.

  Or you can run **uninstaller.exe**, which is located in the **<collector_install_dir>_uninst** directory.

- On a Linux or UNIX machine, run the following command:

  `/opt/HP/HPEDiagCollector/Uninstall/setup.sh`

Chapter 2: Configuring the Active System Property Files

This chapter includes:

Configuration for SAP NetWeaver-ABAP

A SAP NetWeaver–ABAP system deployment can include one or more SAP NetWeaver–ABAP application instances. These instances together form an SAP NetWeaver–ABAP system.

Depending on user permissions, access to the system or application instances on the system might be direct or might require connection through the SAP Message Server. For each SAP NetWeaver–ABAP probe entity, you must know what connection option is used.

You configure the Collector to collect data for each instance of an active SAP NetWeaver–ABAP system to be monitored. You configure SAP NetWeaver-ABAP for monitoring in the **<collector_install_ dir>\etc\r3config.xml** file. The layout, elements, and attributes of the xml file are described in **<collector_ install_dir>\etc\r3config.xsd**.

To configure SAP NetWeaver–ABAP monitoring:

1. Open **Collector\etc\r3config.xml**.

2. If you are defining an SAP NetWeaver–ABAP probe entity where access to the SAP NetWeaver–ABAP instance is through the SAP Message Server, locate the section of code preceded by the following comment:

   ```
   <!--
   Template to be used with the message server connection option.
   -->
   ```

   If you are defining an SAP NetWeaver–ABAP probe entity where access to the SAP NetWeaver–ABAP instance is direct, locate the section of code preceded by the following comment:

   ```
   <!--
   Template to be used with the direct connection option.
   -->
   ```

3. Make a copy of the comment, together with the template code below the comment, and paste it at the end of the file.

4. Comment out the original template code by typing `<!--` in an empty line above the template code and `-->` in an empty line thereafter.

5. In the copied code at the end of the file, alter the value of each property as described in the following table and save the file.

Property	Description	Value
r3system name	A logical name for the probe group under which this SAP NetWeaver–ABAP probe entity appears in the Diagnostics UI.	User-defined.
systemId	The ID of the SAP NetWeaver–ABAP system. Consists of 3 characters only.	Format: [XXX] Obtainable from the SAP system administrator.
client	The client name for the SAP NetWeaver–ABAP system.	Obtainable from the SAP system administrator.
user	The name of the user connecting to the SAP NetWeaver–ABAP system. This user needs to have at least the S_RFC Authorization Object in order to query the Dialog info. The user on the target system must have this object in their authorization profile to be able to use RFC to connect to the target system. However, for systems R/3 4.7 and earlier this is not sufficient. The workaround is to install the Collector on a machine that is time-synched with the ABAP host and then disable time-synching in the Collector by setting property timesynch.interval.secs = 0 (in Collector\etc\r3.properties).	Obtainable from the SAP system administrator.
password	The password (plaintext) of the user connecting to the SAP NetWeaver–ABAP system.	Obtainable from the SAP system administrator.
encrypted-password	The password (encrypted) of the user connecting to the SAP NetWeaver–ABAP system.	Use the EncryptPassword.jsp utility (see "Password Obfuscation" on page 13) to encrypt the password.

Property	Description	Value
messageServerHost (Message Server connection only)	The name of the SAP Message Server host machine.	Obtainable from the SAP system administrator.
r3Name (Message Server connection only)	Consists of 3 characters only.	Format: [XXX] Obtainable from the SAP system administrator.
group (Message Server connection only)	The group of the SAP application servers.	Obtainable from the SAP system administrator.
dialogInstance	Specify a list of Dialog Instances to be monitored. By default all Dialog Instances within the ABAP system (cluster) are automatically discovered and monitored. However, if the Dialog Instances are too many (and too busy) for a single Collector to handle (it may run out of memory), you can use this property to monitor only some of the Dialog Instances and monitor the rest by different Collectors.	SAP Dialog Instances

Configuration for Oracle

You configure the Collector to collect data for each instance of an active Oracle system to be monitored. You configure Oracle monitoring in the **<collector_install_dir>\etc\oracle-config.xml** file. The layout, elements, and attributes of the xml file are described in **<collector_install_dir>\etc\oracle-config.xsd.**

To configure Oracle monitoring:

1. Open **<collector_install_dir>\etc\oracle-config.xml**.
2. Copy the template code enclosed in the comment tags (<!-- and -->) and paste it at the end of the file.

   Use the **oracleInstance** element from the template to collect from Oracle 10g and 11g instances. If you want to collect from multiple instances add separate entries of the oracleInstance element.

   To collect from Oracle RAC (Real Application Clusters) specify the **oracleRac** element. The oracleRac

configurations must come after the oracleInstance configurations in the **oracle-config.xml** file.

3. In the copied code, alter the value of each property as described in the following table and save the file.

Properties	Description	Value
hostName	The name of the Oracle database server host machine. You must use the fully qualified host name. In an oracleRAC configuration, this will be the cluster alias.	Obtainable from the Oracle administrator.
portNumber	Port where the Oracle database server listens for requests.	Default value: **1521**
instanceName	Use for the oracleInstance element (does not apply to oracleRAC element). The name given to the Oracle instance during installation of the Oracle database server.	Default value: **Orcl** Obtainable from the Oracle administrator.
serviceName	Use for the oracleRac element (does not apply to oracleInstance element). serviceName along with the cluster alias hostName, isolates clients from changes in the RAC installation.	Obtainable from the Oracle administrator.
userId	The ID of the user connecting to the Oracle database server. **Note:** The user needs at least **CREATE SESSION** and **SELECT ANY DICTIONARY** to collect performance metrics.	Obtainable from the Oracle administrator.
password	The password (plaintext) of the user connecting to the Oracle database server.	Obtainable from the Oracle administrator.
encrypted-password	The password (encrypted) of the user connecting to the Oracle database server.	Use the EncryptPassword.jsp utility (see "Password Obfuscation" on page 13) to encrypt the password.

Properties	Description	Value
probeName	For an oracleInstance. The logical name to represent this Oracle instance in the Diagnostics UI. This name must be unique. In an oracleRac configuration there will be multiple probes so you don't enter a probeName.	User-defined. If this value is not defined, the same value given for **instanceName** is used. The probe name for each Oracle instance in an Oracle RAC configuration is retrieved at run-time from the INSTANCE_NAME column in the GV$INSTANCE view.
probeGroupName	The logical name of the probe group under which the probe appears in the Diagnostics UI. It can be an existing probe group, or you can define a new one. Optional for the oracleRac element, if omitted, probe group is set to serviceName.	User-defined; for example: Existing: **Default** New: **Oracle**

To enable collection of additional metrics:

1. If the Collector encounters a metric it is not configured to collect, a warning containing the unrecognized metric ID and name is logged. If the metric is a count, percent, byte, or centisecond metric, you can optionally collect the metric by adding the metric ID to **<collector_install_dir\etc\oracle.properties**.

2. Locate the property name that corresponds to the type of metric you want the Collector to collect and add the metric. The property names are:

   - oracle.metrics.count

   - oracle.metrics.percent

   - oracle.metrics.bytes

   - oracle.metrics.centiseconds (the Collector converts to milliseconds)

3. Restart the Collector.

Configuration for SQL Server

You configure the Collector to collect data for each instance of an active SQL Server system to be monitored. You configure SQL monitoring in the **<collector_install_dir>\etc\sqlserver-config.xml** file. The layout, elements, and attributes of the xml file are described in **<collector_install_dir>\etc\sqlserver-config.xsd.**

To configure SQL Server monitoring:

1. Open **<collector_install_dir>\etc\sqlserver-config.xml**.

2. Alter the value of each property as described in the following table and save the file.

Properties	Description	Value
hostName	The name of the SQL Server database host machine. You must use the fully qualified host name.	Obtainable from the SQL Server administrator.
portNumber	The number of the port where the SQL Server database listens for requests.	Default value: **1433**
instanceName	The name given to the SQL Server instance during installation of the SQL Server database. When you specify an instance name, Diagnostics**automatically discovers all SQL Server databases in the instance**. To exclude some of these databases from collection (for example, system databases), specify a comma-separated list in the **exclude.db.list** property in the **<collector_install_dir>\etc\sqlserver.properties** file.	Default value: **Default** Obtainable from the SQL Server administrator.
integratedSecurity	If set to **true**, no username/ password should be specified. The JDBC driver searches the local computer credential cache for credentials that have been provided at the computer or network logon. When the Collector is run from the service **Micro Focus Diagnostics Collector**, the Windows user credentials used to connect to SQL Server must be set as the **logon** property for the service. To do this, run the Windows Services Manager (**services.msc** from the run dialog, or **My Computer > Manage > Services and Applications > Services**). Open the Properties dialog for service **Micro Focus Diagnostics Collector**, select the Log On tab, and set **Log on as:** to the user granted access to your SQL Server instance. This must be the domain account. Restart the service. When using Windows authentication, a domain account (not a local one) needs to be used for making the connection to the SQL Server instance. If set to **false**, the username and password must be supplied. If this is not specified, its default value is false.	Default value: **false**

Properties	Description	Value
userId	The ID of the user connecting to the SQL Server database. **Note:** The user needs at least **VIEW SERVER STATE** to collect performance metrics. Create the user as follows for VIEW SERVER STATE: • CREATE LOGIN diag WITH PASSWORD = '<pwd>'; • USE master; • GRANT VIEW SERVER STATE TO diag; • GO From the SQL Server Management Studio GUI, you can right-click on the Instance name and select the properties.	Obtainable from the SQL Server administrator.
password	The password (plaintext) of the user connecting to the SQL Server database.	Obtainable from the SQL Server administrator.
encrypted-password	The password (encrypted) of the user connecting to the SQL Server database.	Use the EncryptPassword.jsp utility (see "Password Obfuscation" on page 13) to encrypt the password.
probeName	The name to be used to represent this instance as a probe in the Micro Focus Diagnostics UI. When you have **n** databases in your instance, you actually have **n+1** probes: an extra probe for the totals of the instance that includes metrics such as wait events. The extra probe is shown in the UI as probeName. The probes for each database are shown as probeName_databaseName.	User-defined. If this value is not defined, the same value given for **instanceName** is used.
probeGroupName	The logical name of the probe group under which this probe entity appears in the Diagnostics UI. This can be an existing probe group or you can define a new one.	User-defined; for example: Existing: **Default** New: **SQL Server**

Configuration for MQ

You configure the Collector to collect data for each instance of an active MQ system to be monitored. You configure MQ monitoring in the **<collector_install_dir>\etc\mq-config.xml** file. The layout, elements, and attributes of the xml file are described in **<collector_install_dir>\etc\mq-config.xsd.**

The MQ probe requires the following permissions:

```
To Display the attributes or status of the queue and Get messages from the queue.

setmqaut -m <queue_manager_name> -n ** -t queue -g <OS_group_name> +dsp +get


For Administration command queue used for remote MQSC commands and PCF commands. All
authority is equivalent to the union of the authorities alladm, allmqi, and system
appropriate to the SYSTEM.ADMIN.COMMAND.QUEUE. alladm authority is equivalent to the
union of the individual authorities chg, clr, dlt, dsp, ctrl, and ctrlx appropriate
to the SYSTEM.ADMIN.COMMAND.QUEUE. crt authority is not included in the subset
alladm. allmqi authority is equivalent to the union of the individual authorities
altusr, browse, connect, get, inq, pub, put, resume, set, and sub appropriate to the
SYSTEM.ADMIN.COMMAND.QUEUE.

setmqaut -m <queue_manager_name> -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g <OS_group_
name> +all


To Display the attributes or status of the channel.

setmqaut -m <queue_manager_name> -n ** -t channel -g <OS_group_name> +dsp


To Display the attributes or status of the queue manager, Allow the application to
set the identity and origin context fields in a message, Allow the application to set
the identity context fields in a message, and allow the queue manager to generate the
origin context, use another user's ID to open queues and put messages on queues(for
SYSTEM.ADMIN.COMMAND.QUEUE).

setmqaut -m <queue_manager_name> -t qmgr -g <OS_group_name> +connect +dsp +inq
+setall +setid +altusr
```

You can limit the types of queues from which the MQ probe collects metrics to isolate the most interesting metrics for your application. By default, the MQ probe collects metrics only from predefined (or non-dynamic) queues. You specify the queue types to collect or to ignore by setting properties in the **<collector_install_dir>\etc\mq.properties** file.

To limit the queues for which metrics are collected:

1. Open the **<collector_install_dir>\etc\mq.properties** file.
2. Locate the property name that corresponds to the MQ Queue definition type from which you do not want the Collector to collect metrics. The following table lists the property names and their corresponding MQ Queue definition types.

Properties	MQ Queue Definition Types
collect.predefined.queues	MQQDT_PREDEFINED
collect.permanent.dynamic.queues	MQQDT_PERMANENT_DYNAMIC
collect.temporary.dynamic.queues	MQQDT_TEMPORARY_DYNAMIC
collect.shared.dynamic.queues	MQQDT_SHARED_DYNAMIC

3. The **collect.predefined.queues** property is set to true by default. The other three properties are set to false by default. Specify **false** for any type for which you do not want the Collector to gather metrics and then save the **mq.properties** file.

> **Note:** These properties are supported for MQ 6.x and later versions only.

MQ jar files are included with the Diagnostics Collector but if you must overwrite these files you can. The MQ jar files provided with the Collector are located in the **<collector_install_dir>\lib** directory and can be overwritten by the MQ jar files provided in your local MQ installation. You can typically find the jar files in you local WebSphere's MQ installation's **\lib** directory containing the **com.ibm.mq.jar** file. If you have difficulty locating these files contact your WebSphere MQ administrator.

4. To exclude a specific queue's metrics from being collected, add the queue name to the **exclude.queues** parameter in the **mq.properties** file. Separate multiple queue names with commas.

To configure MQ monitoring:

1. Open **<collector_install_dir>\etc\mq-config.xml**.
2. Copy the template code and paste it at the end of the file.
3. Comment out the template code by typing `<!--` in an empty line above the template code and `-->` in an empty line thereafter.
4. In the copied code, alter the value of each property as described in the following table and save the file.

Properties	Description	Value
hostName	The hostName.	Obtainable from the MQ administrator.
portNumber	The number of the port	
queueManagerName	The MQ Manager to connect to.	Obtainable from the MQ administrator.
channelName	The channel through which to connect to the Queue Manager.	Obtainable from the MQ administrator.
securityExit	An IBM term for a pluggable security provider (a piece of code that provides a secure interface to MQ. If you are using one as a gateway to MQ, specify the complete class name as a parameter and ensure your security Exit class is available on the classpath.	

Properties	Description	Value
probeName	The name to be used to represent this instance as a probe in the Micro Focus Diagnostics UI. This name must be unique.	User-defined. If not defined, it defaults to the Queue Manager name.
probeGroupName	The logical name of the probe group under which this probe entity appears in the Diagnostics UI. This can be an existing probe group, or you can define a new one.	User-defined; for example: Existing: **Default** New: **MQ**

Configuration for TIBCO EMS

You configure the Collector to collect data for each instance of an active TIBCO Enterprise Message Service (EMS) system to be monitored.

You configure TIBCO EMS monitoring in the **<collector_install_dir>\etc\tibco-ems-config.xml** file. The layout, elements, and attributes of the xml file are described in **<collector_install_dir>\etc\tibco-ems-config.xsd.**

In addition to the configuration described below, the following TIBCO EMS jar files must be copied from your TIBCO EMS installation's **<Tibco_EMS>/ems/<version>/lib** directory to the **<collector_install_dir>\lib** directory on the system where the Collector is installed:

- tibjms.jar
- tibjmsadmin.jar

To configure TIBCO EMS monitoring:

1. Open **<collector_install_dir>\etc\tibco-ems-config.xml**.
2. Copy the template code and paste it at the end of the file.
3. Comment out the template code by typing `<!--` in an empty line above the template code and `-->` in an empty line thereafter.
4. In the copied code, alter the value of each property as described in the following table and save the file.

Properties	Description	Value
emsServerUrl	The EMS Server URL	Default is tcp://localhost:7222
username	EMS server username. The user must have the following privileges: "view-destination" and "view-server"	
password	EMS server password, plain text	

Properties	Description	Value
obfuscated-password	EMS server password obfuscated (optional). This property takes precedence over the plain test password if both are defined. If neither are defined blank is used for the password.	Use the EncryptPassword.jsp utility (see "Password Obfuscation" on page 13) to encrypt the password.
probeName	The name to be used to represent this instance as a probe in the Micro Focus Diagnostics UI. This name must be unique.	User-defined.
probeGroupName	The logical name of the probe group under which this probe entity appears in the Diagnostics UI. This can be an existing probe group, or you can define a new one.	User-defined for example: Existing: **Default** New: **TIBCO**

You can customize TIBCO data collection by setting properties in the **<collector_install_dir>\etc\tibco-ems.properties** file.

- How often to collect data
- How often to attempt to reconnect when a connection is not established
- Enable or disable server-level, queue-level and topic-level metric collection
- Include or exclude Global, Static or Temporary Queues and Topics
- Select individual metrics

Configuration for webMethods Broker

You can configure the Collector to collect data for the webMethods Broker system to be monitored.

You configure webMethods Broker monitoring in the **<collector_install_dir>\etc\wm-broker-config.xml** file. The layout, elements and attributes of the xml file are described in **<collector_install_dir>\etc\wm-broker-config.xsd**.

In addition to the configuration described below, the following webMethods Broker jar files must be copied from your webMethods Broker installation's **<SoftwareAG>/common/lib** directory to the **<collector_install_dir>\lib** directory on the system where the Collector is installed:

- wm-brokerclient.jar
- wm-g11nutils.jar

To configure webMethods Broker monitoring:

1. Open **<collector_install_dir>\etc\wm-broker-config.xml**.
2. Copy the template code and paste it at the end of the file.
3. Comment out the template code by typing `<!--` in an empty line above the template code and `-->` in an empty line thereafter.
4. In the copied code, alter the value of each property as described in the following table and save the file.

Properties	Description	Value
hostname	Broker server hostname.	Required. For example: localhost.
brokerName	The name of the broker to connect to. If omitted, connects to the default broker as defined within the broker server.	Optional
clientGroup	The name of the client group to use. If omitted, connects to the 'admin' client group.	Optional
probeGroupName	The logical name of the probe group under which this probe entity appears in the Diagnostics UI. This can be an existing probe group, or you can define a new one.	Optional, defaults to **Default**. You can enter a user defined name.

You can customize webMethods data collection by setting properties in the **<collector_install_dir>\etc\wm-broker.properties** file.

- How often to collect data
- How often to attempt to reconnect when a connection is not established
- Enable or disable server-level, queue-level metric collection
- Select individual metrics

Configuration for VMware

You configure the Collector to collect data for each VMware node to be monitored. You configure VMware monitoring in the **<collector_install_dir>\etc\vmware-config.xml** file. The layout, elements, and attributes of the xml file are described in **<collector_install_dir>\etc\vmware-config.xsd.** Changes to the **vmware-config.xml** file are picked up dynamically.

The Collector requires a patch be installed on the vCenter server: (see <http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=1024596&sliceId=1&docTypeID=DT_KB_1_1&dialogID=139216791&stateId=1 0 139218894> for more information).

You should have the latest VMware Tools installed on the VMware Guest. These tools can be installed using the vSphere Client. The latest tools are required for you to drill down from VMware Guest to Hosts in the Diagnostics UI because the VMware tools make the Guest's FQDN available to the VMware Collector via the vCenter.

The VMware Host/Guests associations are created when the Collector is started. New VMware Hosts and VMware Guests may take up to 15 minutes to show up in Diagnostics. Deleted or migrating VMware Guests may take up to five minutes to show up in Diagnostics.

To configure VMware monitoring:

1. Open **<collector_install_dir>\etc\vmware-config.xml**.
2. Copy the template code and paste it at the end of the file.

3. Comment out the template code by typing `<!--` in an empty line above the template code and `-->` in an empty line thereafter.

4. In the copied code, alter the value of each property as described in the following table and save the file.

Properties	Description	Value
serverURL	The URL used to connect to the VMware ESX or VCenter server via the VMware infrastructure vSphere Web Services API. For example: https://<myVM.myCo.com>/sdk	
userId	The VMware ESX or vCenter user id. At a minimum the user must have ReadOnly access and be placed in the Users group.	
encrypted-password	The encrypted VMware password corresponding to userId. First checks for an encrypted password and use it if it is non-blank; otherwise use the plaintext password. the plaintext password does not exist or is blank then uses blank for the password.	Optional
password	The plaintext VMware password corresponding to userId.	Optional

You can customize VMware data collection by setting properties in the **<collector_install_dir>\etc\vmware.properties** file for the following:

- You can limit the query interval and reconnection time. The query interval is just a hint to the Collector, because the sampling interval must actually be a multiple of the interval configured on the VMware Server.

- You can also filter by VMware host (ESX Server) and VMware guest (Virtual Machine). If the VMware Collector is unable to handle the load of an entire vCenter, then the host and guest filters may allow you to use the VMware Collector on the part of the vCenter that is most important to you or to partition the vCenter among multiple VMware Collectors. To use these filters, modify **vmware.properties** as described in the property file for **host.filters** and **guest.filters** properties.

Chapter 3: Upgrading the Collector

You must upgrade the Diagnostics Server before upgrading the Collectors that are connected to it because Diagnostics Servers are not forward-compatible.

To upgrade a Diagnostics Collector:

1. Stop or shut down the Diagnostics Collector that you want to upgrade.

2. Back-up the directory for the current collector installation.

   By default this is
   C:\MercuryDiagnostics\Collector on Windows
   /opt/hp/hpediagcollector on UNIX.

   Because the upgrade procedure requires you to uninstall the current Diagnostics Collector, the backup copy can be used in case you need to start over.

3. Uninstall the current Diagnostics Collector.

4. Install the new Collector into the same installation directory that was used for the old version of the Collector.

   Make sure to **use the same Collector name and Mediator host** to ensure that the persisted data for the application will match up with the metrics captured by the new collector.

   You can determine the old Collector name by viewing the backed up **<collector_install_dir>\etc\collector.properties** file.

   See "Installing Diagnostics Collectors" on page 5 for installation instructions.

5. If installing on Windows, stop the Collector.

   The Collector is started automatically when the installer finishes.

   On UNIX the Collector is not automatically started so you do not need to stop it.

6. Compare the new **etc** directory and the **backed up etc** directory to determine the differences between the two. (It might be helpful to use a diff/merge tool for this purpose.)

   Apply any differences that were caused by the customizations that you made to the **backed up etc** directory to the new **etc** directory so that they will not be lost.

Property File	Configuration Properties to Be Copied to the New Diagnostics Server
mq-config.xml	If the collector is monitoring an MQ environment.
oracle-config.xml	If the collector is monitoring an Oracle environment.
sqlserver-config.xml	If the collector is monitoring an SQL Server environment. If you are upgrading from 7.x you must remove the databaseName attribute from the sqlserver-config.xml file because in later Collector versions the databaseName is automatically discovered.
r3config.xml	If the collector is monitoring an SAP ABAP environment.

Property File	Configuration Properties to Be Copied to the New Diagnostics Server
vmware-config.xml	If the collector is monitoring a VMware environment.
tibco-ems-config.xml	If the collector is monitoring a TIBCO EMS environment.
wm-broker-config.xml	If the collector is monitoring a webMethods Broker environment.
security.properties	If the system is set up for SSL mode, set all properties and copy the certificates from the old property file to the property file.

7. Start the Diagnostics Collector.

8. You can verify the upgraded Collector by checking the version.

9. Once you are satisfied that the Diagnostic Collector has been upgraded successfully, remove the backup copy you created in Step 2.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Collector Installation Guide (Diagnostics 9.51)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docs.feedback@microfocus.com.

We appreciate your feedback!