IBM System Storage

DS Open Application Programming Interface 5.3 Installation and Reference

Version 1 Release 3

GC35-0516-02

IBM System Storage

DS Open Application Programming Interface 5.3 Installation and Reference

Version 1 Release 3

GC35-0516-02

Note:
Before using this information and the product it supports, read the information in the **Safety and environmental notices** and **Notices** sections.

This edition replaces GC35-0516-01 and all previous versions of GC35-0493.

Contents

Figures

Tables

About this guide

This publication introduces the IBM® System Storage® DS Open Application Programming Interface (API), which will be referenced to in this guide as the Common Information Model (CIM) agent. This publication also provides instructions for installing and configuring the CIM agent on the following operating systems:

- IBM Advanced Interactive Executive (AIX®) 5.3
- Linux SLES 9 and Linux RHEL 3
- Microsoft® Windows® 2003

The CIM agent can be installed on a host server.

This publication also lists the CIM components and provides descriptions of the commands that you use during the installation and configuration tasks.

After the CIM agent is installed and configured on your machine, you can implement the DS Open API. This book contains reference material that includes the following information that might assist you in writing your CIM-based applications for the DS Open API:

- DS Open API component definitions

  This section describes the elements, the namespace, and the object name for the DS Open API.
- CIM agent communication with the DS Open API

  This section describes the concepts and methods for communication between the CIM agent and the DS Open API and lists error codes that the CIM object manager (CIMOM) returns.
- DS Open API object classes

  This section provides DS Open API object classes that are used by the CIM agent to manage its model of the storage unit.

Who should use this guide

This publication is for system administrators and system and application programmers, or whoever is responsible for implementing the DS Open API and installing and configuring the CIM agent. This publication assumes that you understand the general concepts of the operating system and Internet capabilities for your enterprise.

Notices and publication information

This section contains information about safety notices that are used in this guide, environmental notices for this product, publication information, and information about sending your comments to IBM.

Safety notices

Complete this task to find information about safety notices.

To find the translated text for a danger or caution notice:

1. Look for the identification number at the end of each danger notice or each caution notice. In the following examples, the numbers **1000** and **1001** are the identification numbers.

   DANGER

   A danger notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

   1000

   CAUTION:
   A caution notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

   1001

2. Find the number that matches in the *IBM System Storage Solutions Safety Notices for IBM Versatile Storage Server and IBM System Storage Enterprise Storage Server*, GC26-7229.

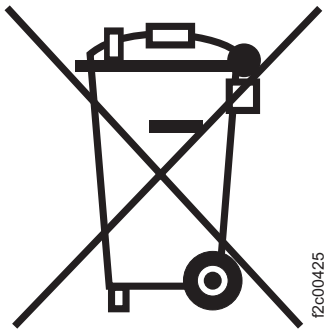
Environmental notices

This section identifies the environmental guidelines that pertain to this product.

Product recycling and disposal

This unit contains recyclable materials.

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.



Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/index.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

In the Netherlands the following applies:

For Taiwan:

Please recycle batteries.

廢電池請回收

Conventions used in this guide

The following typefaces are used to show emphasis:

boldface
Text in **boldface** represents menu items and lowercase or mixed-case command names.

italics Text in *italics* is used to emphasize a word. In command syntax, it is used for variables for which you supply actual values.

`monospace`
Text in `monospace` identifies the data or commands that you type, samples of command output, or examples of program code or messages from the system.

Ordering IBM publications

You can order copies of IBM publications using the IBM publications center.

IBM publications center

The publications center is a worldwide central repository for IBM product publications and marketing material.

The IBM publications center offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download free of charge. You can also order publications. The publications center displays prices in your local currency. You can access the IBM publications center through the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

Note: Open the Web site in a new browser window by right clicking on the link and selecting ″Open in New Window.″

Publications notification system

The IBM publications center Web site offers you a notification system for IBM publications.

If you register, you can create your own profile of publications that interest you. The publications notification system sends you a daily e-mail that contains information about new or revised publications that are based on your profile.

If you want to subscribe, you can access the publications notification system from the IBM publications center at the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

Web sites

The following Web sites provide information about the IBM System Storage DS6000 and DS8000 series and other IBM storage products.

Type of Storage Information	Web Site
CIM Agent for DS Open API Support	http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/supportresources?brandind=5000033*!ENTITY!*=5329497*!ENTITY!*=1
DS6000 Information Center	http://publib.boulder.ibm.com/infocenter/ds6000ic/index.jsp
DS8000 Information Center	http://publib.boulder.ibm.com/infocenter/ds8000ic/index.jsp
DS6000 series publications	http://www-1.ibm.com/servers/storage/support/disk/ds6800 Click **Documentation**.
DS8000 series publications	http://www-1.ibm.com/servers/storage/support/disk/ds8100 Click **Documentation**.
IBM System Storage DS6000 series	http://www-1.ibm.com/servers/storage/disk/ds6000
IBM System Storage DS8000 series	http://www-1.ibm.com/servers/storage/disk/ds8000
Host system models, operating systems, and adapters that the storage unit supports	http://www.ibm.com/servers/storage/disk/ds6000/interop.html Click **Interoperability matrix**.
Host system models, operating systems, and adapters that the storage unit supports	http://www.ibm.com/servers/storage/disk/ds8000/interop.html Click **Interoperability matrix**.
Concurrent Copy for S/390 and zSeries host systems	http://www.storage.ibm.com/software/sms/sdm/
Copy Services command-line interface (CLI)	http://www-1.ibm.com/servers/storage/support/software/cscli/
FlashCopy for S/390 and zSeries host systems	http://www.storage.ibm.com/software/sms/sdm/
IBM Disk Storage Feature Activation (DSFA)	http://www.ibm.com/storage/dsfa
IBM storage products	http://www.storage.ibm.com/
IBM version of the Java (JRE) that is often required for IBM products	http://www-106.ibm.com/developerworks/java/jdk/
Multiple Device Manager (MDM)	http://www.ibm.com/servers/storage/support/ Click **Storage Virtualization**.
Remote Mirror and Copy (formerly PPRC) for S/390 and zSeries host systems	http://www.storage.ibm.com/software/sms/sdm/
SAN fibre channel switches	http://www.ibm.com/storage/fcswitch/
Storage Area Network Gateway and Router	http://www-1.ibm.com/servers/storage/support/san/
Subsystem Device Driver (SDD)	http://www.ibm.com/systems/support/storage/software/sdd
Technical notes and product tips	http://www.ibm.com/servers/storage/support/disk/ds8100/ Click **Technical notes** on the Troubleshooting tab.

Type of Storage Information	Web Site
z/OS Global Mirror (formerly XRC) for S/390 and zSeries host systems	http://www.storage.ibm.com/software/sms/sdm/

How to send your comments

Your feedback is important to help us provide the highest quality information. If you have any comments about this information or any other DS8000™ series documentation, you can submit them in the following ways:

- e-mail

  Submit your comments electronically to the following e-mail address:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the book and, if applicable, the specific location of the text you are commenting on, such as a page number or table number.

- Mail

  Fill out the Readers' Comments form (RCF) at the back of this book. Return it by mail or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Department 61C
  9032 South Rita Road
  TUCSON AZ 85775-4401

Summary of Changes for GC35-0516-02 IBM System Storage DS Open Application Programming Interface Reference

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. This summary of changes describes new functions that have been added to this release.

New Information

- Added chapter 9, *IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service for Windows*.

Changed Information

- Updated chapter 5, *CIM agent for HMC*.

Chapter 1. Introduction to IBM System Storage DS Open API

This chapter provides the following information about the IBM System Storage™ DS Open Application Programming Interface (API), Common Information Model (CIM) standards, and CIM agent installation:

- DS Open API overview
- CIM agent overview
- CIM agent components
- CIM concepts
- CIM agent installation requirements
- CIM agent installation methods
- CIM agent security

DS Open API overview

The IBM System Storage DS Open API is a nonproprietary storage management client application that supports routine LUN management activities, such as LUN creation, mapping and masking and the creation or deletion of RAID-5 and RAID-10 ranks. It also enables Copy Services configuration and use activities, such as FlashCopy. The DS Open API supports these activities through the use of the Storage Management Initiative Specification (SMI-S), as defined by the Storage Networking Industry Association (SNIA).

The DS Open API helps integrate configuration management support into storage resource management (SRM) applications, which allow customers to benefit from existing SRM applications and infrastructures. The DS Open API also enables the automation of configuration management through customer-written applications. Either way, the DS Open API presents another option for managing storage units by complementing the use of the IBM System Storage DS Storage Manager Web-based interface and the IBM System Storage DS Command-Line interface.

You must implement the DS Open API through the IBM System Storage Common Information Model (CIM) agent, a middleware application that provides a CIM-compliant interface. The DS Open API uses the CIM technology to manage proprietary storage units as open system storage units through storage management applications. The DS Open API allows these storage management applications to communicate with your storage unit.

The DS Open API supports the IBM System Storage DS8000 and the IBM System Storage DS6000, and the IBM TotalStorage Enterprise Storage Server. It is available for the AIX, Linux, and Windows operating system environments.

For more information about these products, see the *IBM System Storage DS6000 and DS8000 Information Centers*.

CIM agent overview

A Common Information Model (CIM) agent provides a means by which a device can be managed by common building blocks rather than proprietary software. If a device is CIM-compliant, software that is also CIM-compliant can manage the device. Vendor applications can benefit from adopting the common information

model because they can manage CIM-compliant devices in a common way, rather than using device-specific programming interfaces. Using CIM, you can perform tasks in a consistent manner across devices and vendor applications.

A CIM agent consists of the components shown in Figure 1. The main components are the CIM object manager (CIMOM), the service location protocol (SLP), and the device provider. A device can be a storage server such as your IBM System Storage storage unit. The CIM agent registers itself with the SLP Service Agent (SLP SA) to enable discovery by the Client application. The SLP DA is a directory service daemon that a client application calls to locate the CIM Object Manager. The client application and the CIMOM communicate through CIM Messages. The CIMOM and device provider communicate through method calls made from the CIMOM to the provider. The device provider communicates with the device through proprietary calls.

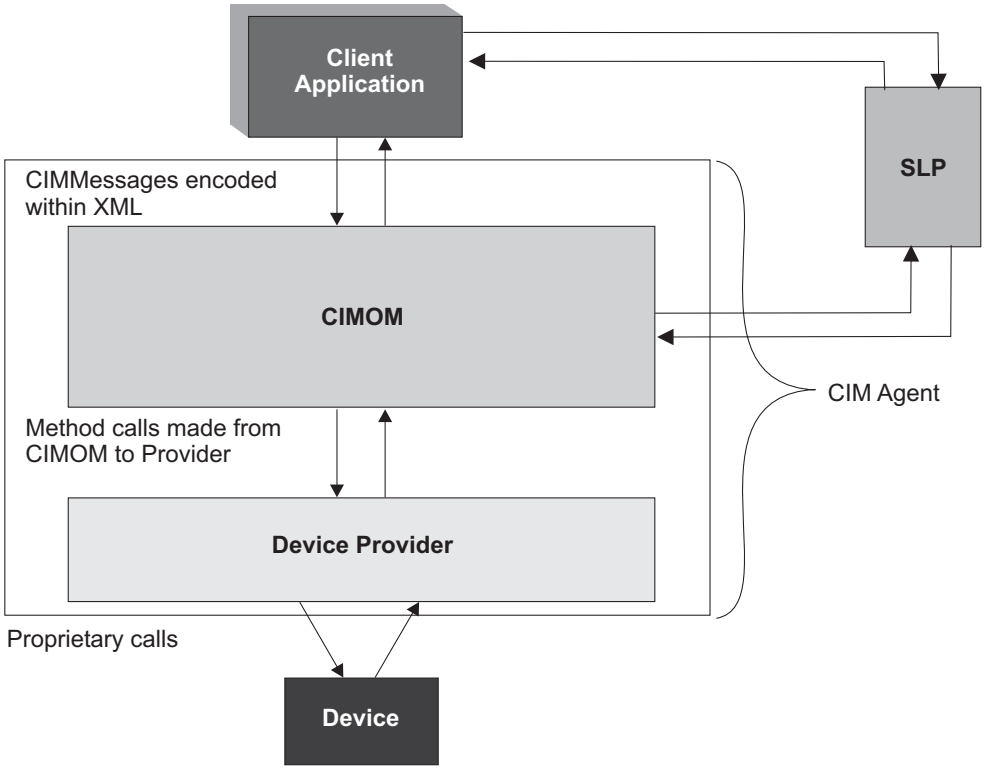


Figure 1. How a CIM agent works

The CIMOM supports the following specifications and standards:

- *Distributed Management Task Force (DMTF) Specification for CIM Operations over HTTP, Version 1.2*
- *Common Information Model (CIM) Specification, Version 2.3*
- *Storage Networking Industry Association (SNIA) Storage Management Initiative (SMI) Specification* and the *Shared Storage Model, a framework for describing storage architectures, Version 1.1*

Conformance to these specifications allows a CIM agent to act as an open-system standards interpreter, allowing other CIM-compliant storage resource management applications (IBM and non-IBM) to interoperate with each other.

When you have installed, configured, and enabled the CIM agent on a host server or an administrator's workstation within your network, that host server or

workstation can communicate with your storage unit through the CIM agent. This allows CIM-compliant applications like the DS Open API to manage the data on your storage unit.

CIM agent components

The following list describes the components of a CIM agent:

client application
A storage management API that initiates a request to a device or a data storage unit such as an IBM System Storage storage unit.

Note: A client application is not provided with the CIM agent, and it must be supplied by the customer.

CIM agent
An agent that interprets open-system data as it is transferred between the API and a device or a storage unit.

service location protocol (SLP)
SLP DA is a directory service that a client application calls to locate the CIM Object Manager. SLP SA is a service agent to allow discovery by a client application.

CIM object manager (CIMOM)
A common conceptual framework for data management. Receives, validates, and authenticates client application requests, and then directs requests to the appropriate functional component or to a device provider.

storage unit provider
A storage unit-specific handler that receives client application requests that are destined for its device or storage unit.

storage unit (also known as a storage server)
The final destination of a client application request and the processor of the request.

CIM concepts

The common information model (CIM) is an open approach to the management of systems and networks. The CIM provides a common conceptual framework applicable to all areas of management including systems, applications, databases, networks, and devices. The CIM specification provides the language and the methodology used to describe management data.

The CIM defines a set of classes with properties and associations which in turn provide a conceptual framework. The framework enables the organization of data for a specific managed environment, such as data storage. CIM Schema 2.11 for Managing a Storage Array provides information about enabling management applications to manage data in a common way.

The CIM standards and the DMTF specification provide information about Web-based enterprise management (WBEM) operations over HTTP.

When the CIMOM first starts, it registers itself to the SLP and provides information about its location (IP address and port) and the type of service it provides. A client application finds the location of the CIMOM by calling an SLP directory service. After obtaining this information, the client application opens direct communication with the CIMOM.

A client sends requests to a CIMOM in the context of a CIM model. The model is defined by the CIM schema and loaded into the repository of the CIMOM. Figure 2 shows how the schema is loaded into the data store of the CIMOM. The managed object format (MOF) compilation and creation of the data store is managed automatically during installation.

As requests arrive, the CIMOM validates and authenticates each request. Requests are either directed to the appropriate functional component of the CIMOM or directed to a device-specific handler called a provider.

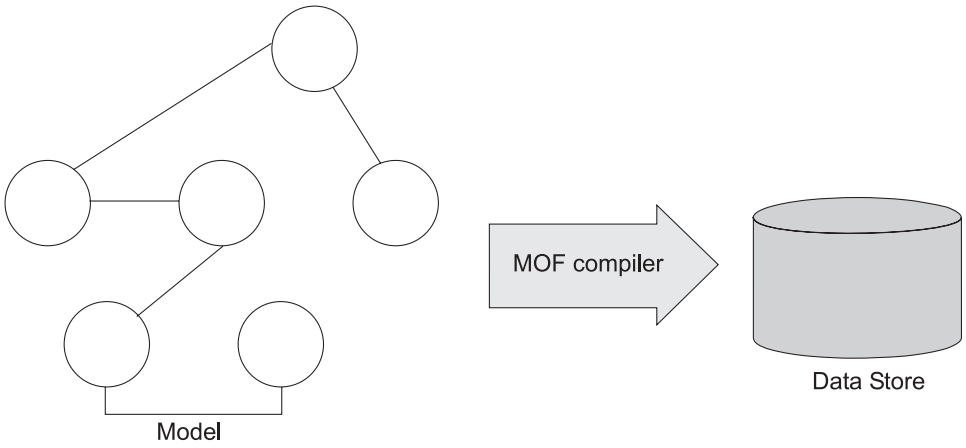


Figure 2. The MOF compiler stores the model in the CIMOM data store.

A provider makes device-unique programming interface calls on behalf of the CIMOM to satisfy a client application request. Such requests generally map a CIM request to the propriety programming interface for a device. A request to get an instance of a class or a property of an instance, for example, might be directed to a provider and a provider might make one or many requests of a device using the unique API for the device. Figure 1 on page 2 shows the communication structure between the device and the client application.

CIM agent installation requirements

Ensure that your system satisfies the following prerequisites for installing the CIM agent on a Windows 2003, AIX 5.3 with x1C Runtime 7.0 or higher, or on the Linux SLES9 or the RedHat Enterprise Linux 3 operating system before you start the installation.

Hardware

The following hardware is required:

- Personal computer, workstation, or server with Intel® Pentium® 4 or higher processor (Linux and Windows only)
- PowerPC_POWER3 processor or higher for AIX
- CD-ROM drive
- Video graphics adapter display

Workstation space

The following space on your workstation is required:

- 1 gigabyte (GB) of random-access memory (RAM) minimum depending on your system configuration

- 1 gigabyte disk space minimum
- 1 gigahertz processor speed minimum
- Up to 50 megabytes (MB) of temporary disk space for installation purposes

Note: When considering hardware requirements for your implementation, the above requirements and recommendations are just a starting point. You must also consider all applications that will share the hardware with the CIM agent and grow the hardware requirements as required.

Software

The following software is required:

- Operating systems:
  - Windows 2003
  - AIX 5.3 with Service Pack 3 (SP 3) or higher and xLC 7.0.0.0 or higher
  - SLES9 (SUSE Linux Enterprise Server)
  - RHEL3 (Red Hat Enterprise Linux)
- Common Information Model (CIM) agent. This software is on the CIM agent CD that is only available upon request. Otherwise, see the following Website for downloads: http://www-03.ibm.com/servers/storage/support/software/cimdsoapi/.
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Adobe Acrobat Reader version 4.0 or later

  You need the Adobe Acrobat Reader to read License Agreement and product information from the CIM agent for the DS Open API LaunchPad. You can download the Adobe Acrobat Reader from the following Web site:
  - http://www.adobe.com/support/downloads/main.html
- To use the CIM agent that is embedded in the DS8000 Hardware Master Console (HMC), the DS8000 must be at Release 2.4 (bundle 6.2.400.64) or later. See Chapter 5, “CIM agent for HMC,” on page 75 for details on using the CIM agent on the HMC.

CIM agent installation methods

You can choose to install the CIM agent in graphical mode or in unattended mode. In graphical mode, an installation wizard guides you through the installation. In unattended mode, also known as silent mode, you customize a response file and issue a command to run an unattended installation.

Follow the instructions in the section of the installation chapter appropriate for your operating system.

CIM agent security

The CIM agent can operate in both secure and unsecure modes.

Secure mode

All requests between the client application and the CIMOM are XML encoded requests sent over Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (SSL). The CIMOM, upon receiving a request, parses the request and processes it. Responses, when they are returned to the client application, are transformed into XML-encoded CIM status and returned in HTTP responses to the client. The default of the CIM agent is to run in secure mode using SSL.

Unsecure mode

Some vendor software might not be capable of communicating with the CIM agent in a secure mode. You can still use this vendor software by configuring the CIM agent to run with only basic user name and password security. See the configuration instructions for your operating system for the instructions for configuring the CIM agent for this less secure mode.

Chapter 2. CIM agent for AIX

This chapter includes an overview of the installation process and instructions for installing and configuring the CIM agent on an IBM AIX® operating system.

Installation overview for AIX

This section provides an overview and instructions for installing and configuring the CIM agent on the AIX operating system. Ensure that you have some knowledge of how to administer your AIX operating system before you begin to install the CIM agent. Also become familiar with the command explanations that you use to install and configure the CIM agent.

Perform the following list of installation and configuration tasks on your AIX operating system:

1. Before you install the CIM agent on an AIX operating system, verify the hardware and software requirements.
2. Install the CIM agent either in graphical mode with the help of a wizard or in unattended mode (also known as silent mode), which involves customizing a response file and issuing a command. If your system does not support the graphical mode, you cannot use the **-console** parameter for the executable file to run the installation in an interactive console mode. You must use the unattended installation mode.
3. Verify the CIM agent AIX installation.
4. Configure the CIM agent for AIX. You might want to revisit the configuration section as you add, change, or delete CIMOM authentication and storage unit information. If you add one or more DS or ESS devices, repeat this step for each device that you add.
5. Set up the user environment. After installation is complete, you must issue two export commands to allow the administrator to perform CIM agent management commands.
6. Verify the connection to your storage unit.
7. Optionally, remove the CIM agent. Perform this optional task only if you receive errors during installation verification or if the CIM agent did not set the environment variables.

Mounting the CD on AIX

This section provides instructions about how to mount a CD.

1. Log on as a user with root authority.
2. Create a mount point or choose an existing mount point.

   To create a mount point called /cdrom, type the following command:

   ```
   # mkdir /cdrom
   ```
3. Type the following command to mount the CD file system at the desired mount point:

   ```
   # mount -o ro -v cdrfs /dev/cd0 /cdrom
   ```

4. Change the current directory to the mount point for the CD drive in the AIX subdirectory. For example, if the CD was mounted at the /cdrom mount point, type the following command:

```
# cd /cdrom/AIX
```

Installing the CIM agent on AIX in graphical mode

This section includes the steps to install the CIM agent in your AIX environment using the graphical mode.

You must satisfy all prerequisites before you begin the CIM agent installation.

You can choose to install the CIM agent in graphical mode with the help of an installation wizard or in unattended (silent) mode, which involves customizing a response file and issuing a command. If you want to install the CIM agent in graphical mode, continue with this section. Before you install the CIM agent on AIX, verify that your system meets the hardware and software requirements. After the completion of either kind of installation, you must verify the installation of the CIM agent.

Follow these steps to install the CIM agent.

Note: If you do not have a graphical interface you cannot use the graphical installation mode. You must use the unattended installation mode. However, if you receive a system message that tells you to run the installer with the -console parameter, you **must** use the unattended installation mode.

1. Log on as a user with root authority.
2. Insert the CIM agent CD.
3. You can run the wizard from either the main console or from a remote X server (another UNIX machine or a PC running an X emulator). If you run it from a remote X server, perform the following steps prior to running the wizard:
   a. Set the DISPLAY variable to *hostname:displaynumber.screennumber* where:

      hostname
      The host name of the platform on which the X server runs and from which the wizard starts.

      displaynumber
      Use the number 0 if the X server controls more than one keyboard and monitor unit, for instance, a network of X terminals.

      screennumber
      This specifies which monitor to use in a multiple monitor setup.

      ```
      <hostname>:<displaynumber.screennumber>
      ```

      Note: If you logged on as a root user from the AIX main console, you do not need to perform the next two substeps because the correct settings are automatically set. However, if you did *not* log on as a root user, you must manually specify these settings under the following circumstances:

      1) If you log on as a nonroot user, switch to the root user (depending on the profile of the root user).

2) If you log on using another computer (another UNIX machine or a PC running an X emulator), referred to as an X server, you must properly set the DISPLAY environment variable. Because the X server is acting as a graphical terminal for a UNIX (in this case AIX) computer through a special protocol, the application running on the AIX operating system must know the host name (or IP address), display and screen number (normally 0) of the machine acting as the X server. You make this information available to the application setting the DISPLAY environment variable. The command for this is:

   export DISPLAY=x_server_hostname:displaynumber.screennumber

   The X server (if it is a UNIX machine) must be configured to allow clients running on remote hosts to access it, using the **xhost** command. The form, xhost +, enables any graphical application running on any machine to use the X server. Or you can use a more restrictive command, such as **xhost aix_name_or_ip**, instead.

b. Run the following command to enable any graphical application running on any host to make connections to the X server.

```
# xhost +
```

4. The CIM agent installation in graphical mode begins with a LaunchPad facility to launch the installation program wizard. The LaunchPad facility provides links for you to view various text files, such as the product overview, product readme, post installation tasks, and various Adobe Acrobat files, such as these installation instructions, product license agreement, and a browser link to the IBM storage product technical support page.

   This installation guide and license agreement are in Adobe Acrobat file format (.pdf). In order for the LaunchPad to provide links to the Adobe Acrobat files, your system *must* have Adobe Acrobat Reader installed. In order for the browser to link to the IBM storage product technical support page, you *must* have a browser installed on your system where you start the LaunchPad facility.

   If you wish to use the LaunchPad facility links to view the Adobe Acrobat files, you must have the Adobe Acrobat Reader bin location in your PATH environment variable. You can verify this by running the following command:

   ```
   echo $PATH
   ```

   Locate the Adobe Acrobat Reader bin location in the PATH, for example, usr/lpp/Acrobat5/bin. If the Adobe Acrobat Reader bin location is not in the environment path, you can set it by typing the following command:

   ```
   export PATH=$PATH:/usr/lpp/Acrobat5/bin
   ```

   where */usr/lpp/Acrobat5/bin* is the location of the Adobe Acrobat Reader bin directory.

5. Run the wizard launcher, launchpad_aix, from the AIX directory of the CD by typing the following command:

```
# ./launchpad_aix
```

This will start the CIM agent LaunchPad, a small program that launches the wizard.

6. Choose from the following options in the LaunchPad window:

   CIM Agent overview
   Offers information about the CIM agent.

   Readme file
   Offers any last minute product information that did not make it into the installation guide.

   Installation guide
   Offers instructions on how to install the CIM agent.

   License agreement
   Offers information about the license of the CIM agent.

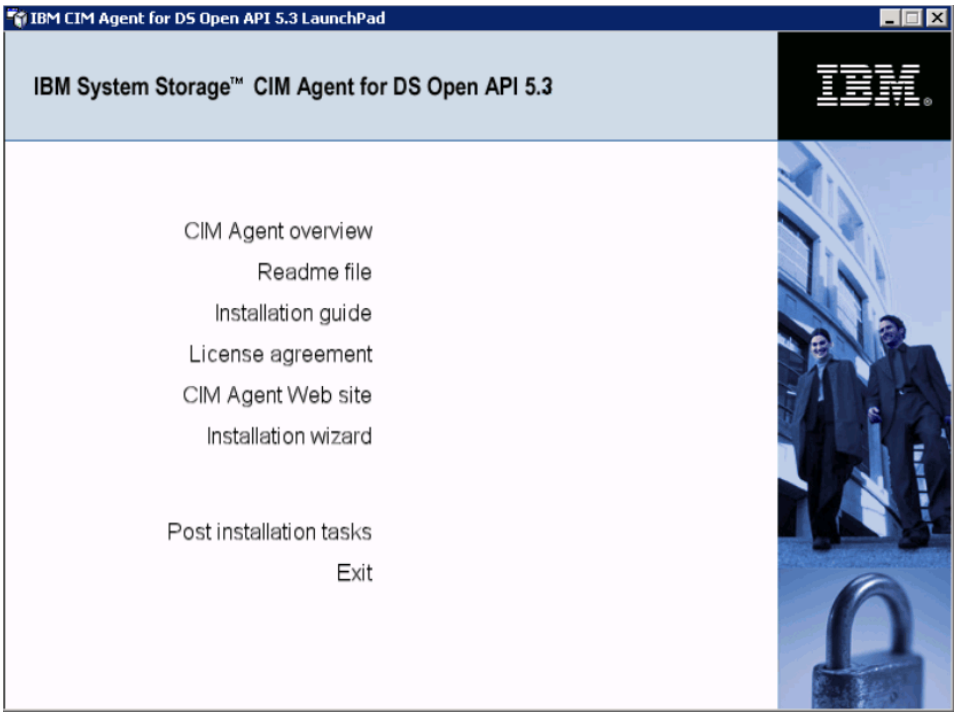
   CIM Agent Web site
   Offers information from the product Web site.

   Installation wizard
   Starts the CIM agent installation program.

   Post installation tasks
   Offers information about configuring the users and storage unit communications.

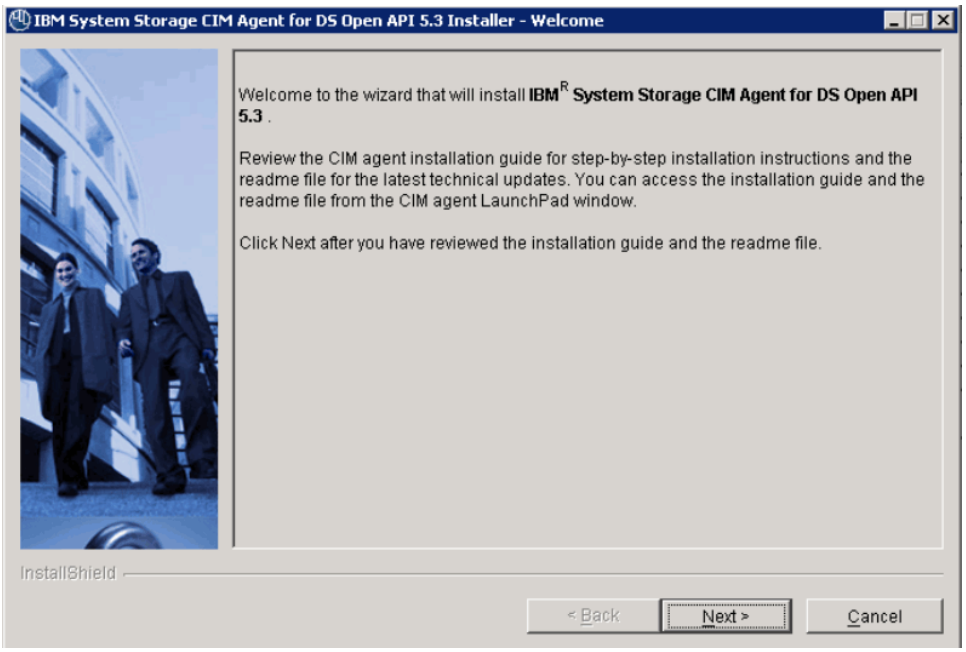
   Exit Exits the LaunchPad program.

   The LaunchPad window remains open (behind the wizard) during the installation. You can access product information after the installation has started. The LaunchPad returns to the foreground when the installation is complete. You can click **Exit** to close the LaunchPad.

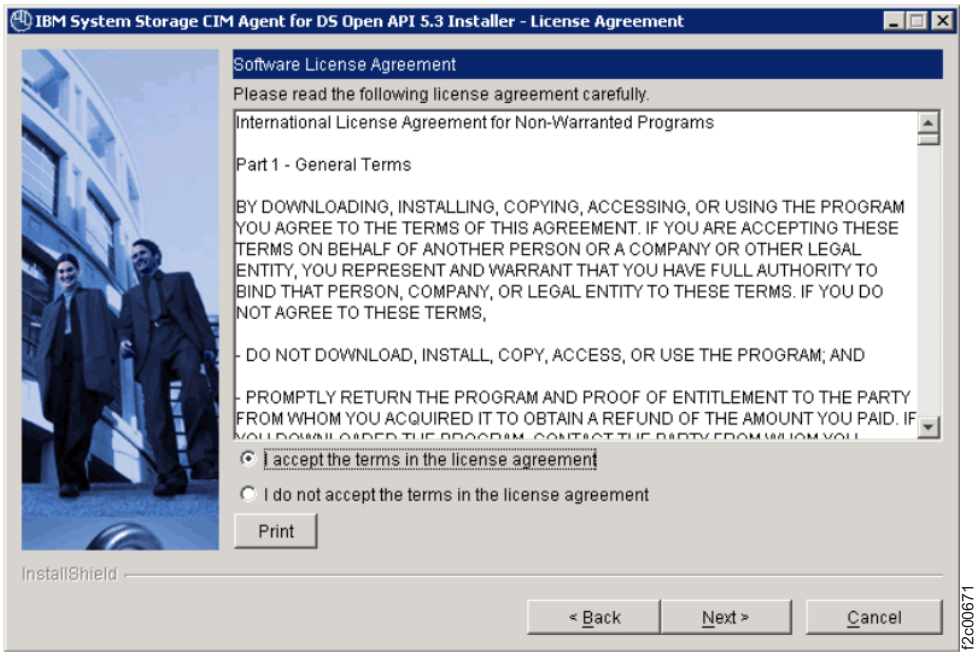


7. Check the readme file by clicking the Readme file on the LaunchPad window or by viewing the README.aix file located in the AIX directory on the CIM agent installation CD. The readme file might provide additional information that supersedes information in this guide.

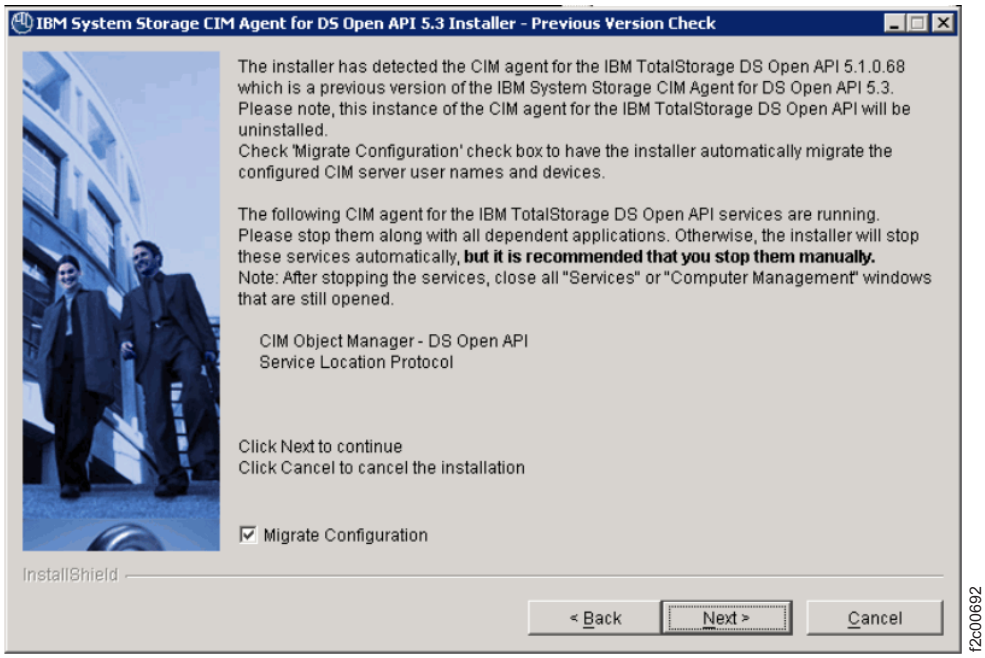
   You can also find this installation guide on the CIM agent CD under the file name installguide.pdf in the doc subdirectory.
8. Click **Installation wizard** to start the installation program.
9. The Welcome window opens and contains text suggesting which documentation to review prior to installation. Click **Next** to continue (License Agreement window opens) or **Cancel** to exit.

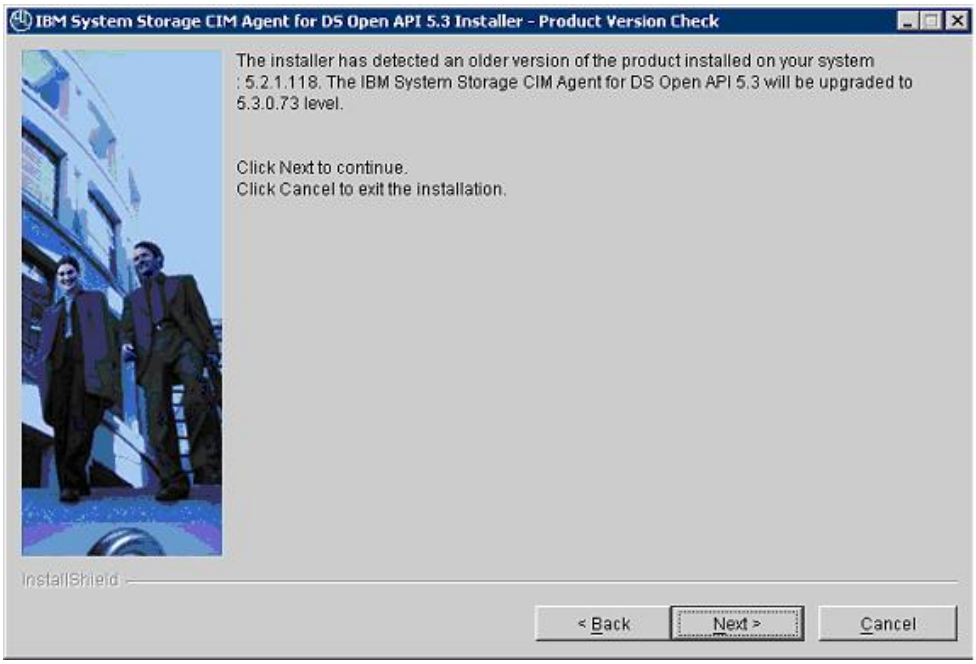


10. Read the license agreement. Click either **I accept the terms of the license agreement** and click **Next** to proceed, or click **I do not accept the terms of the license agreement** and click **Cancel** to cancel the installation.

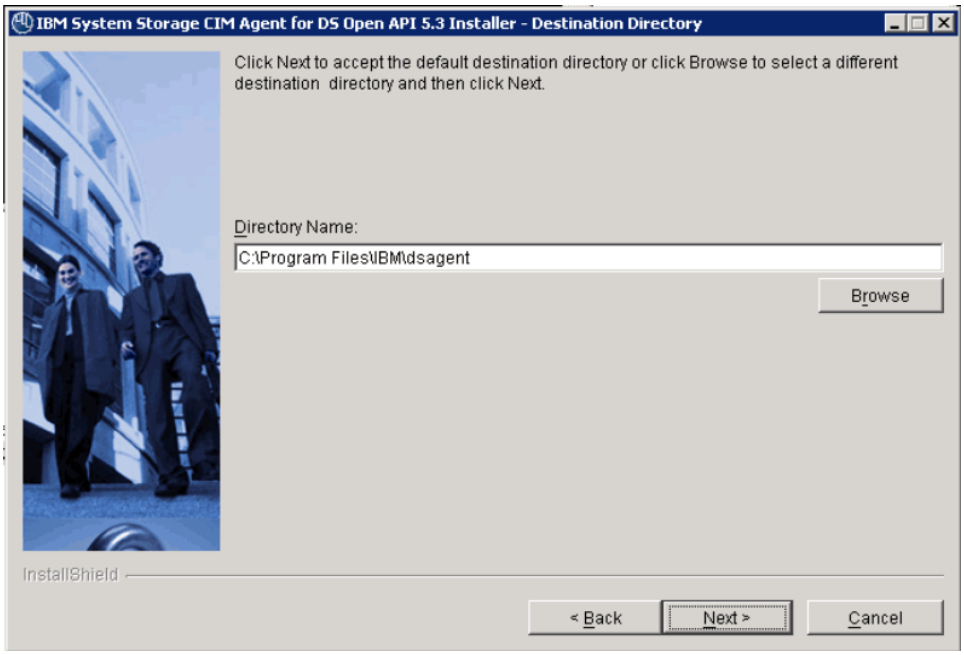


11. If the installation wizard detects a prior installation of the CIM agent, the Product Installation Check window appears. Depending on the version of the prior installation, the screen will differ. If your prior installation was a 5.1 CIM agent, check the **Migrate Configuration** check box if you want to preserve your configuration settings. Follow any specific instructions in the window. For example, the figure below shows a warning to stop running services. After you have followed all instruction, select **Next**. If your prior installation was a 5.2, 5.2.1 or 5.3 CIM agent the installation will automatically save your settings, select **Next**.





12. The Destination Directory window opens. Click **Next** to accept the default directory, or click **Browse** to select a different directory for installation and then click **Next**.



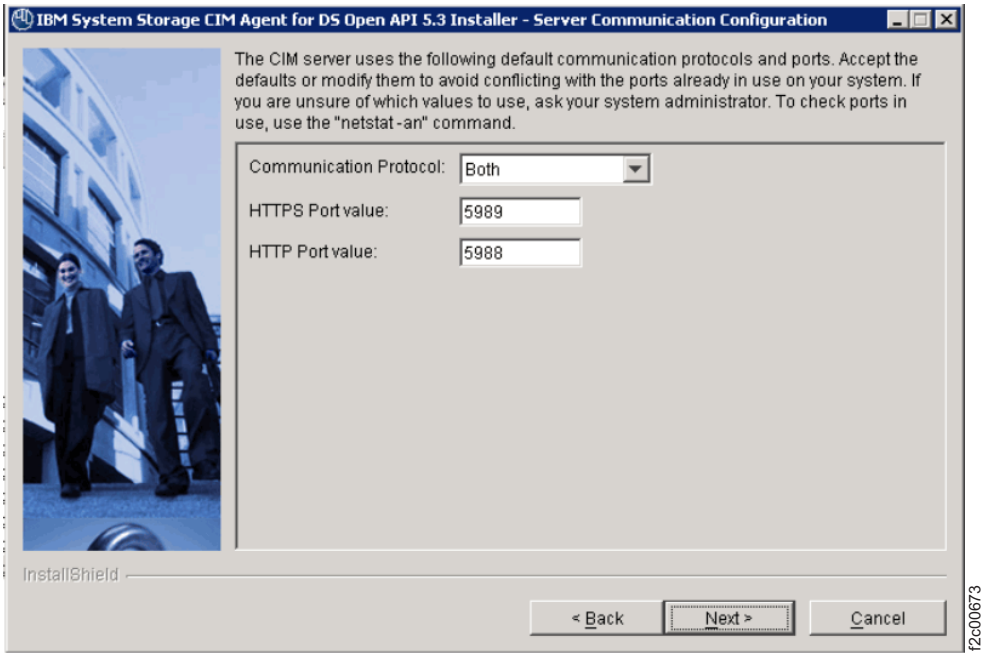
Note:

a. The Destination Directory window is displayed only if no prior installation of 5.2, 5.2.1 or 5.3 of the CIM agent was detected or if a prior installation of the 5.1 CIM agent was detected. Otherwise, the CIM agent is reinstalled or upgraded to the same install location as the prior installation.

b. If the wizard detects insufficient space for the CIM agent in the file system containing the chosen directory, you can perform one of the following steps:
   - Free some space in that directory and then click **Next**.
   - Click **Cancel** to exit the wizard, free some space in that filesystem, and then restart the wizard.
   - Click **Back** and choose another filesystem for the product.

13. When the Server Communication Configuration window opens. Click **Next** to accept the default port. If one or more of the default ports is the same as another port already in use, modify the default port and click **Next**.
    a. Use the **netstat -a** command to check which ports are in use.
    b. Accept HTTPS or HTTP as the communication protocol or select another protocol.
    c. Click **Next** to continue with the installation, or click **Cancel** to exit the wizard.

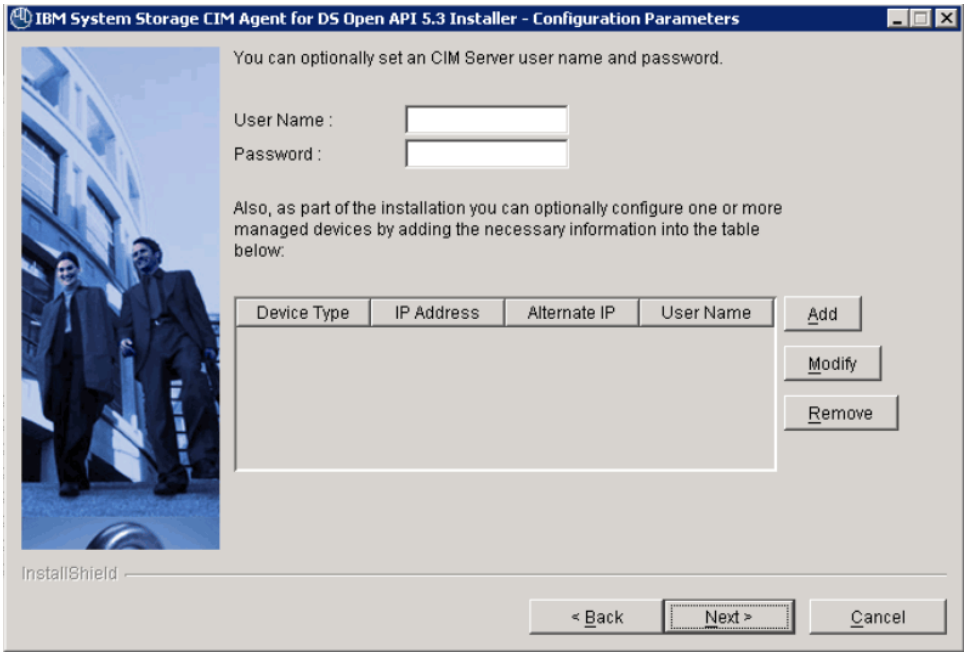
    Note: The Server Communication Configuration window is displayed only if no prior installation of 5.2, 5.2.1 or 5.3 of the CIM agent was detected or if a prior installation of the 5.1 CIM agent was detected. Otherwise, the CIM agent will use the same ports as the prior installation.



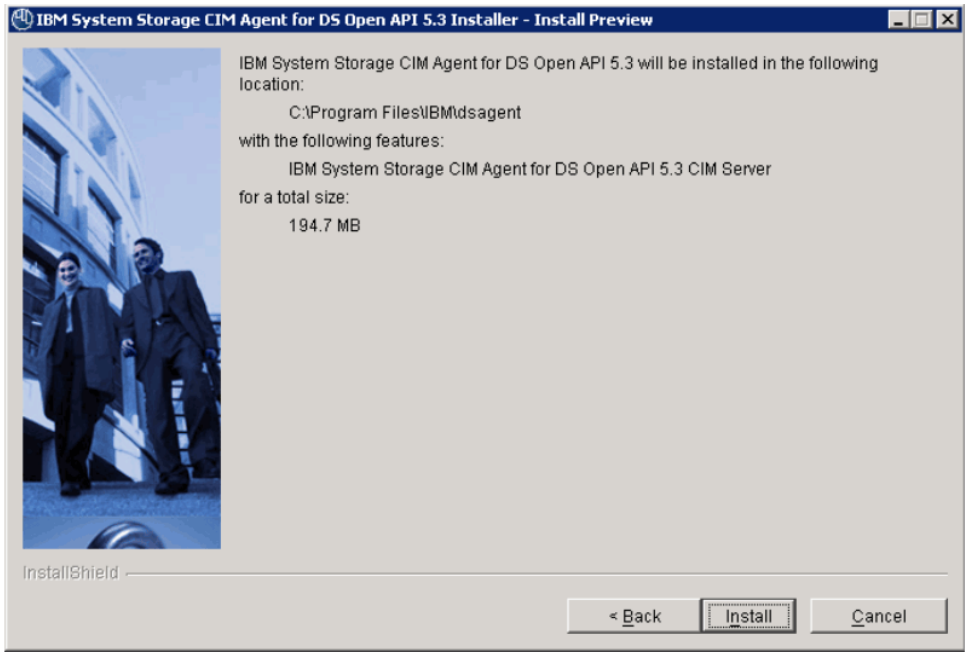
14. The Configuration Parameters window opens. Optionally enter a user name and password for the CIM server. You can click **Add** to optionally enter any information about devices that you would like to configure the agent to communicate with. When adding a device, a device type, IP address, username, and password must be specified. When adding a DS6000 or DS8000 family device, the device type should be "ds", the IP address should be of the master console, and the username and password should be the same one used to log into the DS Command Line Interface and DS Storage Manager. When adding an ESS family device for logical configuration, the device type should be "ess", the IP address should be of the primary processor complex, and the username and password should be the same as the one used to log into the

ESS Command Line Interface and ESS Specialist. Optionally, you can specify the secondary processor complex IP address in the Alternate IP field. When adding an ESS Copy Services server, the device type should be "esscs", the IP address should be of the ESS Copy Services server, and the username and password should be the one used to log into the ESS Copy Services interface. Note that an ESS Copy Services server cannot be added without also adding the associated ESS logical configuration information. However an ESS can be added for logical configuration without adding a Copy Services server. After you have finished adding the configuration information, click **Next**.

Note: The Configuration Parameters window is displayed only if no prior installation of 5.2, 5.2.1 or 5.3 of the CIM agent was detected or if a prior installation of the 5.1 CIM agent was detected and you did not select the **Migrate Configuration** check box. Otherwise, the CIM agent will preserve the devices configured in the prior installation.

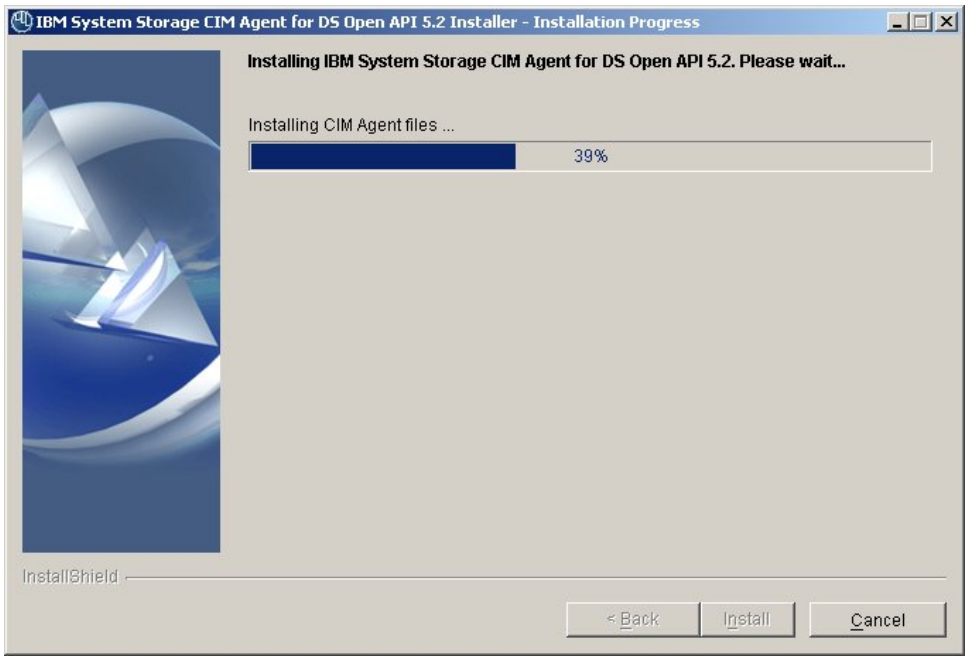


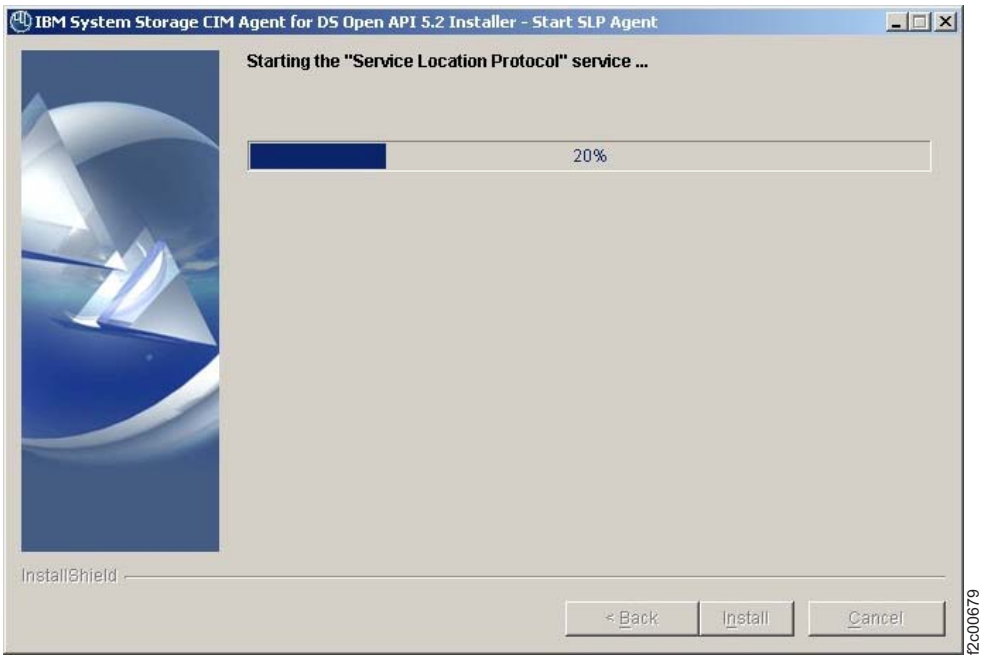
15. The Installation Preview window opens. Click **Install** to confirm the installation location and file size. You can click **Cancel** to exit the installation wizard or go back to the previous window by clicking **Back**.

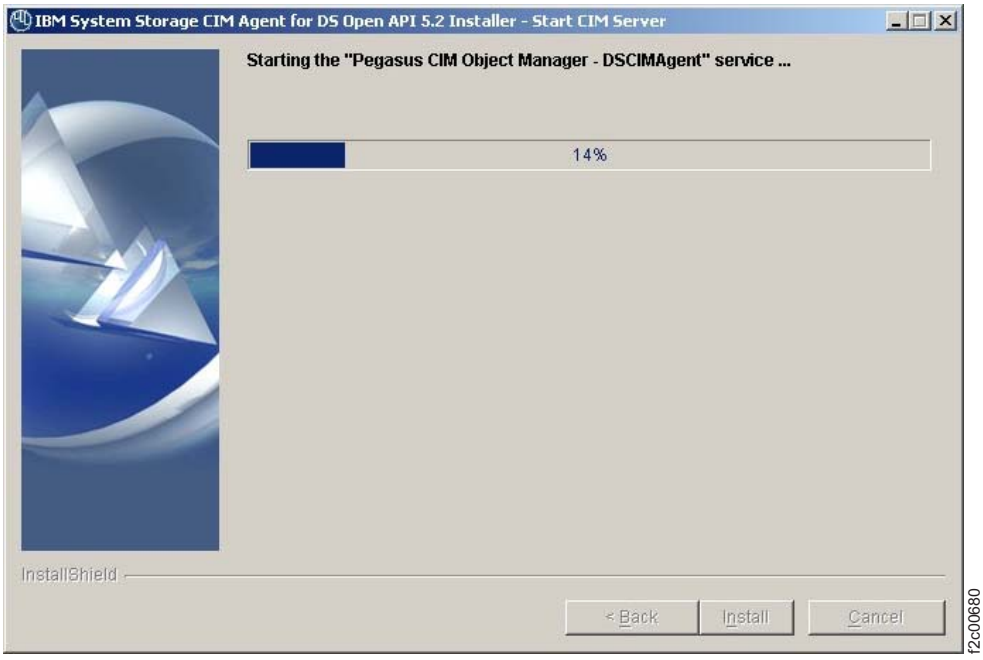


16. The Installation Progress window indicates how much of the installation has been completed. Installation usually takes 3 - 10 minutes depending on the configuration of your machine. The installation installs the CIM agent files, starts the Service Location Protocol (SLP) service, and starts the Pegasus CIM Object Manager – DSCIMAgent service. You can click **Cancel** to exit the installation wizard.

    Note: If you cancel the current operation, the information you entered or selected in previous windows is not saved. You must start the installation again from the first step.

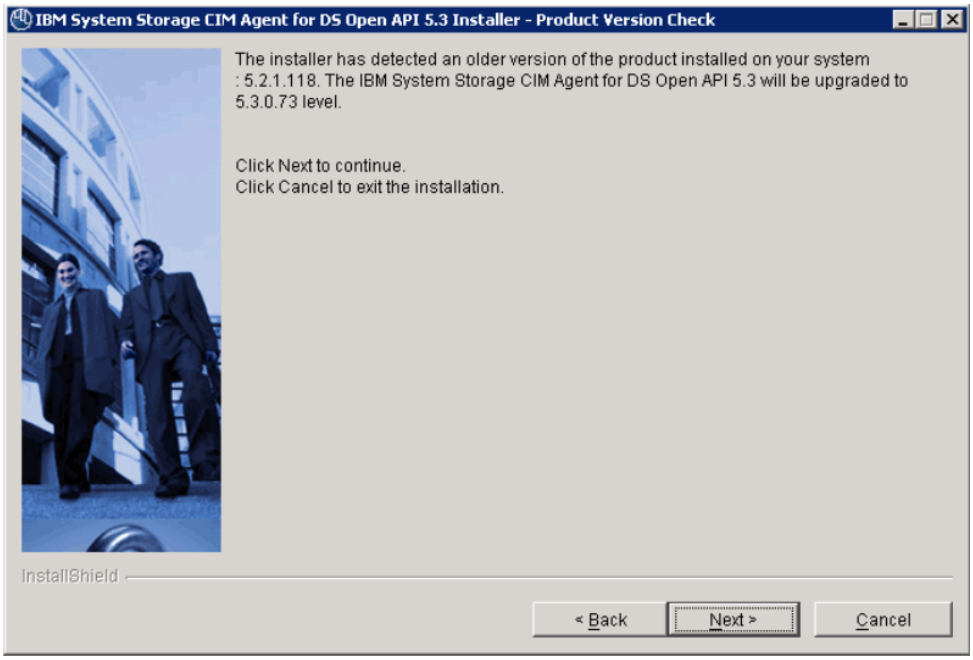






17. When the Installation Progress window closes, the **Finish** window opens. Click **Finish** to exit the installation wizard.

    Note: Before you proceed, review the log file for any possible error messages. The log file is located in *dest-path*/log/install.log, where *dest-path* is the destination directory where the CIM agent is installed. The install.log contains a trace of the installation actions.



18. Exit the LaunchPad program by clicking **Exit** on the LaunchPad window. If you have not done so already, continue with the post installation tasks for the CIM agent using the instructions in the following sections.

Installing the CIM agent on AIX in unattended (silent) mode

This section includes the steps to install the CIM agent in your AIX environment using the unattended (silent) mode.

You must satisfy all prerequisites before you begin the CIM agent installation.

You can choose to install the CIM agent in unattended (silent) mode, which involves customizing a response file and issuing a command or in graphical mode with the help of an installation wizard. If you want to install the CIM agent in unattended (silent) mode, continue with this section. After the completion of either kind of installation, you must verify the CIM agent installation.

Context:

The unattended (silent) installation capability enables you to run an installation process unattended. You can create a standard response file to ensure that the product is installed consistently on multiple systems. The responsefile file is a template located on the CIM agent CD that you must copy to disk and modify. To use the silent mode installation method, you must performing the following tasks:

1. Find the responsefile file template on the CIM agent installation compact disk.
2. Copy the responsefile template to your hard disk drive.
3. Customize the responsefile file to your specifications.
4. Save the updated responsefile file.
5. Invoke the response file using the setupaix script.

Steps:

Perform the following steps to install the CIM agent in your AIX environment using the unattended (silent) mode:

1. Log on as a user with root authority.
2. Locate the responsefile file on your CIM agent CD.
3. Retrieve and copy the responsefile file to your hard disk drive by typing the following commands:

   ```
   # mkdir  /tmp/cimagent
   # cp -p /cdrom/AIX/responsefile /tmp/cimagent
   ```

   You must also modify the responsefile with your desired CIM agent destination directory (<*dest-path*>).
4. To change the permissions on the responsefile, so you can edit and save it to disk, type the following command:

   ```
   chmod 777 /tmp/cimagent/responsefile
   ```
5. Customize the responsefile file with your parameters as follows:

   Using a text editor such as vi, modify the default options in the responsefile file with your desired values:

   - If you do not want to use the default value, remove the # character from the beginning of the line. Change the default value to the value that you want for that option. You *must* enclose all values in double quotation marks (“ ”).
   - The <*-G licenseAccepted*> option defines license agreement verification. The default value is false. Uncomment this option and set it to true only after you have read the product License Agreement. The License Agreement can be found on the installation media. For instance, the following two files should be reviewed by English-speaking users:

     ```
     <CD_ROOT>/<OS-NAME>/license/LI_en
     <CD_ROOT>/<OS-NAME>/license/LA_en
     ```

     Where <CD_ROOT> is the root of the CD image or the root of the unpackaged installation media.
   - The <*-P product.installLocation*> option defines the default directory where the product will be installed. To use another destination directory, remove the # character from the corresponding line and replace this default directory with the directory you want.
   - If an instance of the IBM System Storage CIM Agent for DS 5.1 release is already installed on the target machine, the option <*-W checkPreviousVersion.migrateConfiguration*> specifies if the configured CIM users and devices will be migrated into the newly installed configuration. The default value is true. In order not to migrate the old configuration, remove the # character from the corresponding line and set the value to false.
   - The <*-G useExistingSlp*> option specifies if you want the CIM agent to use the Service Location Protocol already installed into the system. The default value is no.
   - The <*-W serverCommunicationConfig.communicationProtocol*> option specifies the CIM agent server communication protocol. If you want to change the default value during installation, remove the # character from the corresponding line and change the default server communication protocol (″both″) to HTTP or HTTPS protocol values.
   - The <*-W serverCommunicationConfig.httpsPort*> option specifies the port number that the CIM server will use for secure HTTPS transport. This value

must not conflict with existing port assignments on the system. If you are unsure of which values to use, ask your administrator. To check ports in use, use the ″netstat -an″ command. The default value is ″5989″

- The <*-W serverCommunicationConfig.httpPort*> option specifies the port number that the CIM server will use for secure HTTP transport. This value must not conflict with existing port assignments on the system. If you are unsure of which values to use, ask your administrator. To check ports in use, use the ″netstat -an″ command. The default value is ″5988″
- With the <*-G deviceConfigurationParameters*> option you can have the installer optionally configure one or more managed devices (″ds″, ″ess″ or ″esscs″) by adding the necessary information in the following format:

  For DS device:

  ```
  -G deviceConfigurationParameters=ds;IP Address;Alternate IP;UserName;Password
  ```

  For an ESS device:

  ```
  -G deviceConfigurationParameters1=ess;IP Address;Alternate IP;UserName;Password
  ```

  For an ESSCS device:

  ```
  -G deviceConfigurationParameters2=esscs;IP Address;Alternate IP;UserName;Password
  ```

- The <*-W serverConfigParams.userName*> and <*-W serverConfigParams.password*> options define the CIM user name and password to be configured by the installer. By default, only ″superuser″ CIM user is created.

6. Save the modified responsefile file in your desired directory.
7. Type the following command to run the install file:

   ```
   # ./setupaix -options /tmp/cimagent/responsefile
   ```

   Note: <*/tmp/cimagent*> is the path of the responsefile file.
8. Wait for the wizard to complete the installation.
9. Type `echo $?` to see if the installer completed without error. If any non 0 value is returned, check for installation errors in the install.log file. This file can be found in the /log directory. Your install.log file should look similar to the following install.log file:

```
(Apr 10, 2006 5:18:08 AM), Installing CIM Agent files ...
(Apr 10, 2006 5:18:27 AM), Installing OpenSLP files ...
(Apr 10, 2006 5:18:29 AM), Installing OpenSSL files ...
(Apr 10, 2006 5:18:31 AM), Installing Java files ...
(Apr 10, 2006 5:18:38 AM), The file /opt/IBM/dsagent/config/envConf successfully updated.
(Apr 10, 2006 5:18:38 AM), The file /opt/IBM/dsagent/startup/rc.dsagent successfully updated.
(Apr 10, 2006 5:18:38 AM), The file /opt/IBM/dsagent/startup/rc.dsslpd successfully updated.
(Apr 10, 2006 5:18:38 AM), Setting CIM Server configuration ...
(Apr 10, 2006 5:18:38 AM), Command to be executed : /tmp/ismp002/790967.tmp -s
enableHttpConnection=true -p
(Apr 10, 2006 5:18:39 AM), Command to be executed : /tmp/ismp002/790967.tmp -s
enableHttpsConnection=true -p
(Apr 10, 2006 5:18:40 AM), Command to be executed : /tmp/ismp002/790967.tmp -s httpPort=5988 -p
file:///C|/CMVCDiana/api/api_ereview/Comments/release1/cmm_bk09.htm (13 of 26)4/19/2006 8:45:47 AM
CIM agent for AIX
(Apr 10, 2006 5:18:40 AM), Command to be executed : /tmp/ismp002/790967.tmp -s httpsPort=5989 -p
(Apr 10, 2006 5:18:41 AM), The CIM Server configuration successfully set.
(Apr 10, 2006 5:18:41 AM), Generating certificates ...
(Apr 10, 2006 5:18:41 AM), Command to be executed : /opt/IBM/dsagent/bin/mkcertificate certname
(Apr 10, 2006 5:18:42 AM), The certificates were successfully generated.
(Apr 10, 2006 5:18:42 AM), Enabling SSL communication ...
(Apr 10, 2006 5:18:42 AM), Command to be executed : /tmp/ismp002/4747151.tmp -s sslKeyFilePath=/opt/
IBM/dsagent/certificate/certname.key -p
(Apr 10, 2006 5:18:43 AM), Command to be executed : /tmp/ismp002/4747151.tmp -s sslCertificateFilePath=/
opt/IBM/dsagent/certificate/certname.cert -p
(Apr 10, 2006 5:18:43 AM), SSL communication enabled.
(Apr 10, 2006 5:18:44 AM), Enabling CIM server authentication ...
(Apr 10, 2006 5:18:44 AM), Command to be executed : /tmp/ismp002/3373012.tmp -s
enableAuthentication=true -p
(Apr 10, 2006 5:18:44 AM), CIM server authentication enabled.
(Apr 10, 2006 5:18:44 AM), Creating /opt/IBM/dsagent/pegasus/cimserver.passwd file ...
(Apr 10, 2006 5:18:44 AM), etcRcFileName = /etc/rc.dsagent
(Apr 10, 2006 5:18:44 AM), Copied /opt/IBM/dsagent/startup/rc.dsagent as /etc/rc.dsagent
(Apr 10, 2006 5:18:44 AM), inittabEntry = /etc/rc.dsagent >/dev/console 2>&1
(Apr 10, 2006 5:18:44 AM), Creating dsagent entry iin the /etc/inittab file ...
(Apr 10, 2006 5:18:44 AM), Installing "Service Location Protocol" service ...
(Apr 10, 2006 5:18:45 AM), The "Service Location Protocol" service successfully installed.
(Apr 10, 2006 5:18:48 AM), Setting Java Runtime Environment for the uninstaller ...
(Apr 10, 2006 5:19:26 AM), Starting the "Service Location Protocol" service ...
(Apr 10, 2006 5:19:26 AM), Command to be executed:
/etc/rc.dsslpd
(Apr 10, 2006 5:19:28 AM), Return code (rc) = 0
(Apr 10, 2006 5:19:31 AM), The "Service Location Protocol" service successfully started.
(Apr 10, 2006 5:19:32 AM), Starting the "IBM System Storage CIM Agent for DS Open API 5.3" service ...
(Apr 10, 2006 5:19:32 AM), Command to be executed:
/etc/rc.dsagent
(Apr 10, 2006 5:20:08 AM), Return code (rc) = 0
(Apr 10, 2006 5:20:38 AM), The "IBM System Storage CIM Agent for DS Open API 5.3" service successfully
started.
(Apr 10, 2006 5:20:38 AM), The "IBM System Storage CIM Agent for DS Open API 5.3" service was successfully
started.
(Apr 10, 2006 5:20:38 AM), The "Service Location Protocol" service was successfully started.
(Apr 10, 2006 5:20:38 AM), INSTSUCC: IBM System Storage CIM Agent for DS Open API 5.3 has been
successfully installed.
```

Note: If the installation fails before the target <dest-path> directory is created, you can find the temporary log in the /tmp/cimagent/install.log file.

10. Close the command prompt window by entering a command, for example **exit**. Continue with the post installation tasks for the CIM agent in the following sections. You can also continue the post installation tasks using the following option:
    a. Open the LaunchPad from the AIX directory of the CIM agent CD by typing `# ./launchpad_aix`.
    b. Click **Post installation tasks** on the LaunchPad window. Continue with the post installation tasks for the CIM agent by following the instructions in this file.

Verifying the CIM agent installation on AIX

This section provides the steps to verify that your CIM agent is installed correctly on your AIX operating system.

To verify correct CIM agent installation follow these steps:

1. Verify the installation of the service location protocol (SLP). Open a Command Prompt window and type the following command to verify that SLP is started:

   ```
   # ps -ef | grep slpd
   ```

   If the SLP daemon is started, the following output is displayed:

   ```
   root 13760 15324 0 13:20:48 pts/0 0:00 grep slpd
   daemon 18546 1 0 Apr 10 - 0:01 /opt/IBM/dsagent/slp/sbin/slpd
   ```

2. Verify the installation of the CIM agent. Check that the cimserver daemon is installed and started by typing the following command:

   ```
   # ps -ef | grep cimserv
   ```

   The following is a sample output:

   ```
   root 13758 15324 0 13:20:09 pts/0 0:00 grep cimserv
   root 14758 1 0 13:16:55 - 0:34 [cimserve]
   ```

3. You must set environment variables before you can issue any of the CIM agent management commands:

   ```
   source <dest-path>/config/envConf
   ```

   where <dest-path> is the destination directory where the CIM agent is installed.

4. Start the CIM agent, if it is not started, by typing the following command:

   #startagent

   Note: If you are currently residing in /cdrom/AIX, you must exit the /cdrom directory by typing *cd /*. You cannot unmount the CD if you are still residing in /cdrom/AIX. When you are finished with the CIM agent CD, you can release the CD with the **umount** command, for example:

   ```
   # umount /dev/cd0
   # umount /cdrom
   ```

If you are able to perform all of the verification tasks successfully, the CIM agent has been successfully installed on your AIX operating system.

Configuring the CIM agent on AIX

This section includes the steps to configure storage units and user accounts for CIM agent after it has been successfully installed.

You can change the CIM agent port value, protocol (HTTP/HTTPS), and enable or disable the debug option.

Steps:

Perform the following steps to configure ESS and DS user accounts for the CIM agent:

1. Ping each ESS and DS that the CIM agent will manage by typing the following command:
   a. Open a command prompt window.
   b. Issue a **ping** command; for example:

      ```
      # ping 9.11.111.111
      ```

      where 9.11.111.111 is an ESS processor complex or DS master console IP address
   c. Check that you can see reply statistics from the IP address. The following is example output:

      ```
      Pinging 9.11.111.111 with 32 bytes of data:

      Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
      Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
      Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
      Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
      ```

   If you see other messages that indicate that the request has timed out, see your Network Administrator for help on establishing network connectivity before you configure storage units.
2. Type the following command to configure the CIM agent for each ESS or DS server that the CIM agent can access:

   ```
   dscimcli mkdev <ip> -type <type> -user <user> -password <password>
   ```

   ip For an ESS configuration server, this is the IP address of the primary processor card.

   For an ESS copy services server, this is the IP address of the primary copy services server.

   For a DS server, this is the IP address of the primary hardware or software master console (HMC/SMC).

   type
   For an ESS configuration server, this is *ess*.

   For an ESS copy services server, this is *esscs*.

   For DS, this is *ds*.

   user/password
   For an ESS configuration server, this isthe specialist or ESSCLI user name and password.

   For an ESS copy services server, this is the specialist or ESS copy services server user name and password

   For a DS server, this is the storage manager GUI or DSCLI user name and password
3. After you have defined all of the ESS and DS servers, type the following command to verify that the devices were correctly added and have successfully connected:

   ```
   dscimcli lsdev -l
   ```

   The following is example output:

   ```
   Type   IP IP2         user name  Storage Image    Status     Code Level Min Codelevel
   ==== ===============  ========  ================ ========== =========  ============
   DS   9.11.111.111 -   admin   IBM.2107-1234567 successful 5.1.0.309  5.1.0.309
   ```

If the status is failed, there was a failure when the CIM agent attempted to connect to the storage device. If the CIM agent is unable to connect during mkdev, an error is returned immediately. If the device shows as failed in lsdev -l, it is likely that you added the device earlier (for example, during the installation wizard) and the connection is now failed. To ensure that your storage device's management interface is functioning, use the command line interface (ESSCLI or DSCLI) or graphical interface (ESS Specialist or DS Storage Manager) to attempt to log into the device from the server where the CIM agent is hosted. If you are unable to connect via the native command line interface or graphical interface, there is likely an error in the network or the storage device. If you are able to connect via the native interfaces, there is likely an error in the CIM agent. Contact your service representative for assistance.

Note: Because the CIM agent periodically collects and caches information from the defined storage units, the CIM agent might periodically take longer to respond to requests; for example, immediately after adding a new storage unit.

4. Configure the CIMOM for each user that you want to have authority to use the CIMOM by running the CIMOM configuration program.

   During the CIM agent installation, the default user name to accesses the CIM agent CIMOM is created. The default user name is "superuser" with a default password of "passw0rd". You must use the default user name and password when you use the **mkuser** command for the first time after installation. After you have added other users, you can initiate the **mkuser** command using a user name that you have defined instead of using the default.

   a. Start the CIM agent, if it is not started, by typing the following command:

      ```
      # startagent
      ```

   b. Type the following command to create the new user:

      ```
      # dscimcli mkuser cimuser -password cimpass
      ```

      The following is example output:

      ```
      User created.
      ```

      Restriction: You cannot delete or modify the current user using the **mkuser** command.

   c. You can change the default password for "superuser" by starting the **mkuser** command for a user that you added. Issue the following command to change the password:

      ```
      dscimcli chuser superuser -password passw0rd -newpassword <newpassword>
      ```

      where *newpasswd* is the new password for the superuser.

   d. You can delete the superuser by issuing the following command:

      ```
      >>>rmuser superuser
      ```

   e. Type the **exit** command to exit the CIMOM configuration program.

If you are able to perform all of the configuring tasks successfully, the CIM agent has been successfully installed on your AIX operating system.

Verifying the CIM agent connection on AIX

During this task, the CIM agent software connects to the storage unit that you identified in the configuration task.

Steps:

Perform the following steps to verify the connectivity to an ESS or DS. You also verify that the service location protocol (SLP) daemon and the CIMOM are running, because they are needed to connect to an ESS or DS using the CIM agent.

1. Before you run the command to verify the CIM agent connection, ensure the SLP daemon is started by typing the following command:

   ```
   ps -ef | grep slpd
   ```

   If the SLP daemon is not started, type the following command from a separate command prompt window.

   Note: This session remains active until you stop it. Ensure that it is running as long as the CIM agent is running.

2. Before you run the command to verify the CIM agent connection, ensure the CIMOM is started by typing the following command:

   ```
   ps -ef | grep cimserv
   ```

   If the CIMOM is not started, start it by typing the following command:

   ```
   # startagent
   ```

   Notes:

   a. The startagent command quickly returns a prompt; however, a returned prompt does not mean that the processing is complete. If there are a large number of LUNs to enumerate in the internal domain, it takes considerable time for the CIMOM to find and enumerate all those disks. Do *not* issue the **dscimcli lsdev -l** command until CIMOM processing is complete. You can view the cimom.log in the directory where you installed the CIM agent to verify the CIMOM processing status.

   b. The default is to start the secure CIMOM. It registers itself with SLP and accept requests on port 5989.

3. You can view CIMOMs registered with SLP using the **slptool findsrvs wbem** command. This command locates all WBEM services (for example, CIMOMs) in the local network. Information is displayed for the storage units to which the CIM agents can connect. In the following example, the CIM agent on host 9.11.111.111 connects to two storage units (2107.AZ123x and 2105.2223x).

   Issue the following command from a command prompt:

   ```
   # dscimcli lsdev -l
   ```

   The following is example output of a successful connection:

   ```
   Type  IP         IP2  Username  Storage Image    Status     Code Level  Min Codelevel
   ===== ============== ========= ================ ========== ==========  =============
   DS   9.11.111.111 -   admin     IBM.2107-1234567 successful 5.1.0.309   5.1.0.309
   The Status field indicates if the CIM Agent can communicate with the DS or ESS device
   ```

If you received similar output verifying a connection, the CIM agent is now running.

Removing the CIM agent from AIX in graphical mode

Perform the following steps to remove the CIM agent using graphical mode:

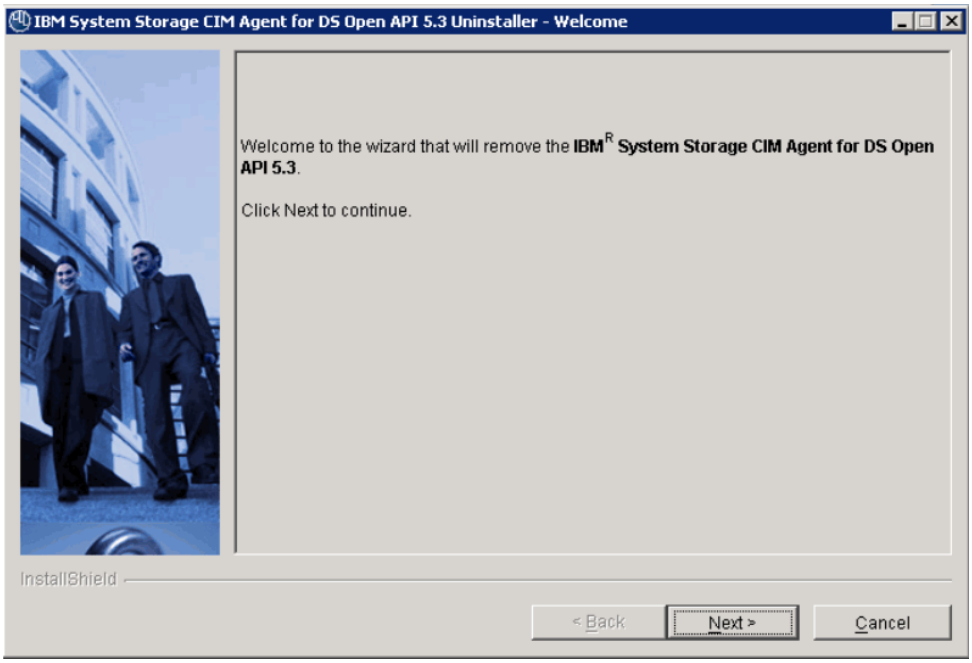
1. Type the following command to run the removal program from the _uninst subdirectory of the *<dest-path>*:

   ```
   # <dest-path>/_uninst/uninstaller
   ```

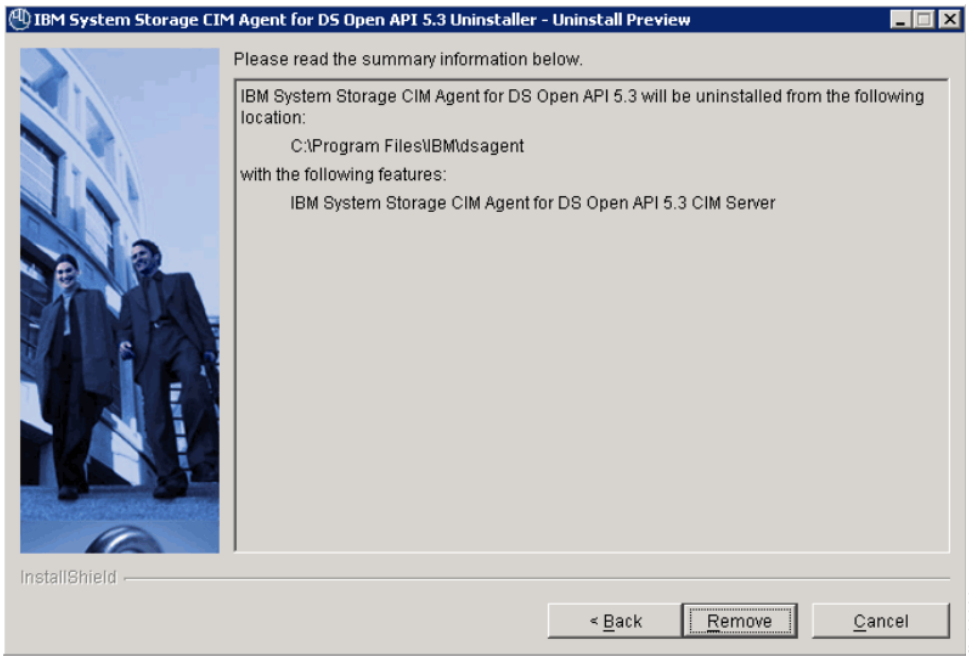
   where *<dest-path>* is the destination directory where the CIM agent is installed.
2. If the removal program was not created during the CIM agent installation, type the following command:

   ```
   # <dest-path>/java/jre/bin/java -jar <dest-path>/_uninst/
   uninstall.jar
   ```

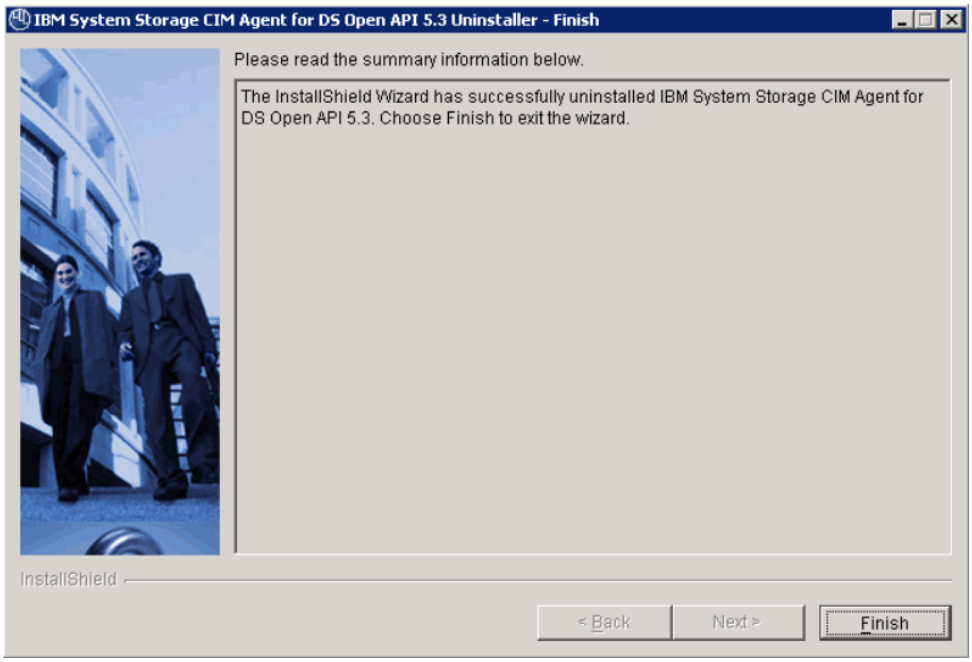
   where *<dest-path>* is the destination directory where the CIM agent is installed.
3. The Welcome window opens. Click **Next** to continue with the removal program, or click **Cancel** to exit the removal program.



4. The Uninstall Preview window displays the location of the product that will be removed. Click **Remove** to continue with the removal program, or click **Cancel** to exit.



5. The Finish window opens and displays information about the result of removal (successfully or failed).



Click **Finish** to end the removal program.

Removing the CIM agent from AIX in unattended (silent) mode

This section includes instructions to remove the CIM agent from AIX in unattended (silent) mode.

Steps:

Perform the following steps to remove the CIM agent in unattended (silent) mode:

1. Stop SLP, CIMOM, and all related processes.
2. Type the following command to run the removal program from the _uninst subdirectory:

```
<dest-path>/_uninst/uninstaller -silent
```

The CIM agent removal process *does not* remove configuration files, logs, and similar files that are created during or after the installation process. They are located in the destination path where the CIM agent has been installed. For example, the default destination path is /opt/IBM/dsagent.

Remove the directory and all of its contents (especially if you plan to reinstall the CIM agent).

Note: If you want to keep the old configuration files, save them in another location on your system before you remove them from the installation destination path, so you can restore them later.

To remove the directory, dsagent, you must type the following command, for example, from the IBM directory.

```
# rm -r /opt/IBM/dsagent
```

Note: The recursive remove is used in this example because the CIM agent has a deep directory structure. The recursive remove is very powerful and dangerous: make sure you copy any needed files to another directory before running this command. You must use the fully qualified directory name.

Chapter 3. CIM agent for Linux

This chapter includes an overview of the installation process and instructions for installing and configuring the CIM agent on a Linux operating system.

Installation overview for Linux

This section provides an overview and instructions for installing and configuring the CIM agent on the Linux (Advanced Server 3.0 and SLES 9) operating system. Ensure that you have some knowledge of how to administer the Linux operating system before you begin to install the CIM agent. Also become familiar with the command explanations that you use to install and configure the CIM agent.

Perform the following list of installation and configuration tasks on your Linux operating system:

1. Before you install the CIM agent on a Linux operating system, verify the hardware and software requirements.
2. Install the CIM agent either in graphical mode with the help of a wizard or in unattended mode (also known as silent mode), which involves customizing a response file and issuing a command. If your system does not support the graphical mode, you cannot use the **-console** parameter for the executable file to run the installation in an interactive console mode. You must use the unattended installation mode.
3. Verify the CIM agent Linux installation.
4. Configure the CIM agent for the Linux operating system. You might want to revisit the configuration section as you add, change, or delete CIMOM authentication and storage unit information. If you add one or more DS or ESS devices, repeat this step for each device you add.
5. Set up the user environment. After installation is complete, you must issue two export commands to allow the administrator to perform CIM agent management commands.
6. Verify the connection to your storage unit.
7. Optionally, remove the CIM agent. Perform this optional task only if you receive errors during installation verification or if the CIM agent did not set the environment variables.

Installing the CIM agent on Linux in graphical mode

This section includes the steps to install the CIM agent in your Linux environment using the graphical mode.

You must satisfy all hardware and software prerequisites before you begin the CIM agent installation.

You can choose to install the CIM agent in graphical mode with the help of an installation wizard or in unattended (silent) mode, which involves customizing a response file and issuing a command. If you want to install the CIM agent in graphical mode, continue with this section. After the completion of either kind of installation, you must verify the installation of the CIM agent. Before you install the CIM agent on Linux, check the hardware and software requirements.

The description of commands in this task have the convention of optional and substitution parameters between the less than ″<″ and greater than ″>″ symbols. You should become familiar with each command's explanation before entering the command. You should have some knowledge about how to administer Linux before you begin installing the CIM agent.

Note: If you do not have a graphical interface you cannot use the graphical installation mode. You must use the unattended installation mode. However, if you receive a system message that tells you to run the installer with the -console parameter, you **must** use the unattended installation mode.

Follow these steps to install the CIM agent.

1. Log on as a user with root authority.
2. Insert the CIM agent CD.
3. You can run the wizard from either the main console or from a remote X server (another UNIX machine or a PC running an X emulator). If you run it from a remote X server, perform the following steps prior to running the wizard:
   a. Set the DISPLAY variable to *hostname:displaynumber.screennumber* where:

      hostname
      The host name of the platform on which the X server runs and from which the wizard starts.

      displaynumber
      The number 0 if the X server controls more than one keyboard and monitor unit; for instance, a network of X terminals.

      screennumber
      The monitor to use in a multiple monitor setup.

      ```
      <hostname>:<displaynumber.screennumber>
      ```

      Note: If you log on as a root user from the Linux main console, you do not need to perform the next two substeps because the correct settings are automatically set. However, if you did *not* log on as a root user, you must manually specify these settings under the following circumstances:

      1) If you log on as a nonroot user, switch to the root user (depending on the profile of the root user).
      2) If you log on using another computer (another UNIX machine or a PC running an X emulator), referred to as an X server, you must properly set the DISPLAY environment variable. Because the X server is acting as a graphical terminal for a UNIX (in this case AIX) computer through a special protocol, the application that is running on the AIX operating system must know the host name (or IP address), display and screen number (normally 0) of the machine that acts as the X server. You make this information available to the application setting the DISPLAY environment variable. Issue the following command to make this information available to the application that is setting the DISPLAY environment variable:

         ```
         export DISPLAY=x_server_hostname:displaynumber.
         screennumber
         ```

The X server (if it is a UNIX machine) must be configured to allow clients that are running on remote hosts to access it, using the **xhost** command. The form, xhost +, enables any graphical application running on any machine to use the X server.

b. Run the following command to enable any graphical application running on any host to make connections to the X server.

```
# xhost +
```

4. Create a mount point or choose an existing mount point.

   Type the following command to create a mount point called /mnt/cdrom:

   ```
   # mkdir /mnt/cdrom
   ```

5. Type the following command to mount the CD-ROM file system at the desired mount point:

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```

6. Change the current directory to the mount point for the CD drive, in the LINUX directory. For example, if the CD was mounted at the /mnt/cdrom mount point, type the following command:

   ```
   # cd /mnt/cdrom/LINUX
   ```

7. Check the README.linux file that is located in the LINUX directory on the CIM agent CD. The README.linux file can provide additional information that supersedes information in this guide.

   You can also find this installation guide on the CIM agent CD under the file name installguide.pdf in the document subdirectory.

8. The CIM agent installation in graphical mode begins with a LaunchPad facility to launch the installation program wizard. The LaunchPad facility provides links for you to view various text files, such as the product overview, product readme, post installation tasks, and various Adobe Acrobat files, such as this installation guide and the product license agreement, and a browser link to the IBM storage product technical support page.

   This installation guide and license agreement are in Adobe Acrobat file format (.pdf). In order for the LaunchPad to provide links to the Adobe Acrobat files, your system *must* have Adobe Acrobat Reader installed. In order for the browser to link to the IBM storage product technical support page, you *must* have a browser installed on your system where you start the LaunchPad facility.

   If you wish to use the LaunchPad facility links to view the Adobe Acrobat files, you must have the Adobe Acrobat Reader bin location in your PATH environment variable. You can verify this by running the following command:

   ```
   echo $PATH
   ```

   Locate the Adobe Acrobat Reader bin location in the PATH, for example, /usr/opt/Acrobat5/bin. If the Adobe Acrobat Reader bin location is not in the environment path, you can set it by typing the following command:

   ```
   export PATH=$PATH:/usr/opt/Acrobat5/bin
   ```

   where */usr/opt/Acrobat5/bin* is the location of the Adobe Acrobat Reader bin directory.

9. Run the wizard launcher, launchpad_linux, from the Linux directory of the CD by typing the following command:

   ```
   # ./launchpad_linux
   ```

   This command starts the CIM agent LaunchPad, a small graphical program that launches the wizard.
10. The LaunchPad window opens. Choose from the following options:

    CIM Agent overview
    Offers information about the CIM agent.

    Readme file
    Offers any last minute product information that did not make it into this installation guide.

    Installation guide
    Offers instructions on how to install the CIM agent.

    License agreement
    Offers information about the license of the CIM agent.

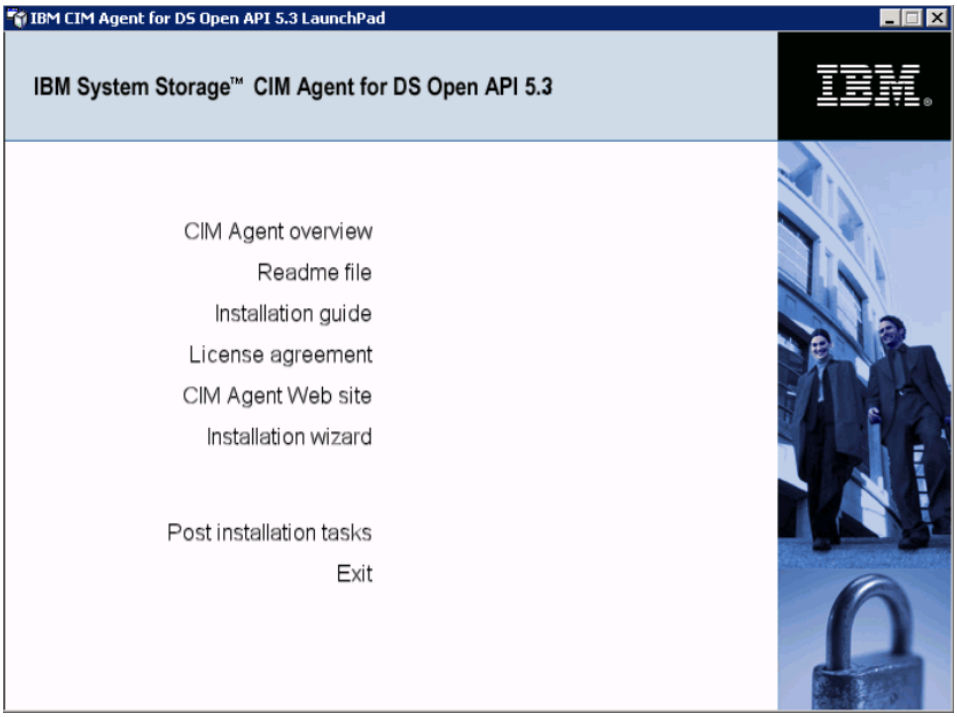
    CIM Agent Web site
    Offers information from the product Web site.

    Installation wizard
    Starts the CIM agent installation program.

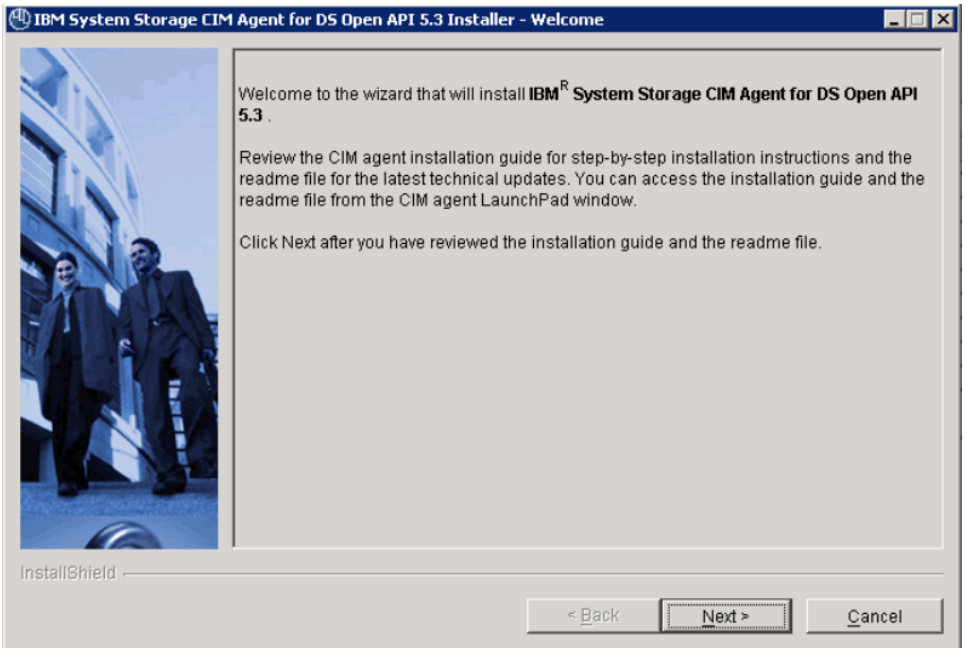
    Post installation tasks
    Offers information about configuring the users and storage unit communications.

    Exit Exits the Launchpad program.

    The LaunchPad window remains open (behind the wizard) during the installation. You can access product information after the installation has started. The LaunchPad returns to the foreground when the installation is complete. You can click **Exit** to close the LaunchPad.

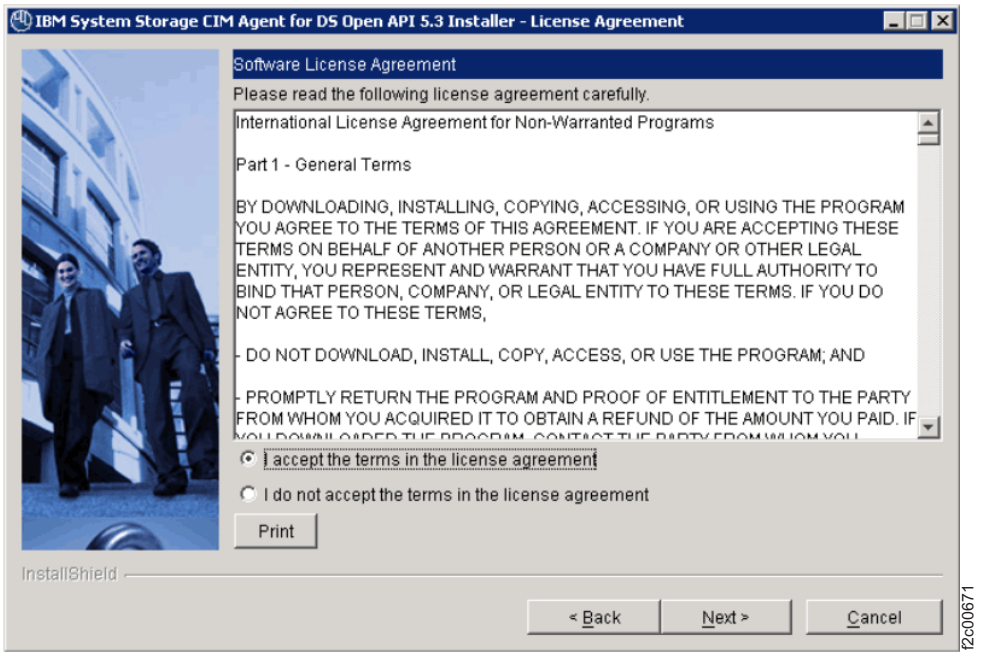


11. Click Installation wizard to begin the CIM agent installation.
12. The Welcome window opens suggesting which documentation you should review prior to installation. Click **Next** to continue. You can click **Cancel** at any time while using the wizard to exit the installation. To move back to previous screens while using the wizard, click **Back**.

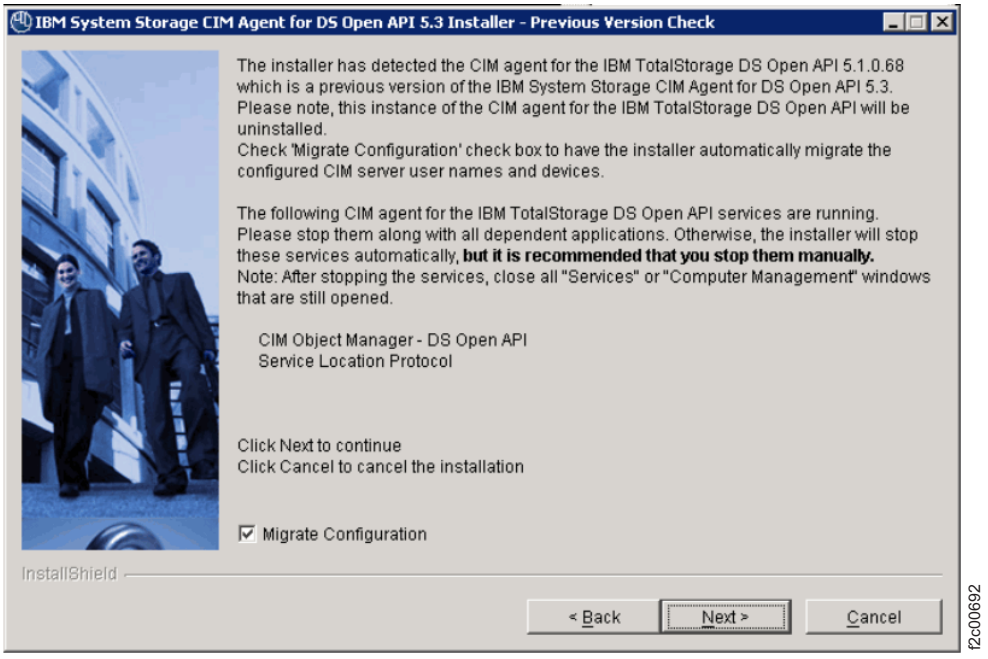


13. The License Agreement window opens. Read the license agreement information. Click **I accept the terms of the license agreement** and click **Next** to proceed, or click **I do not accept the terms of the license agreement** and

click **Cancel** to exit the installation.

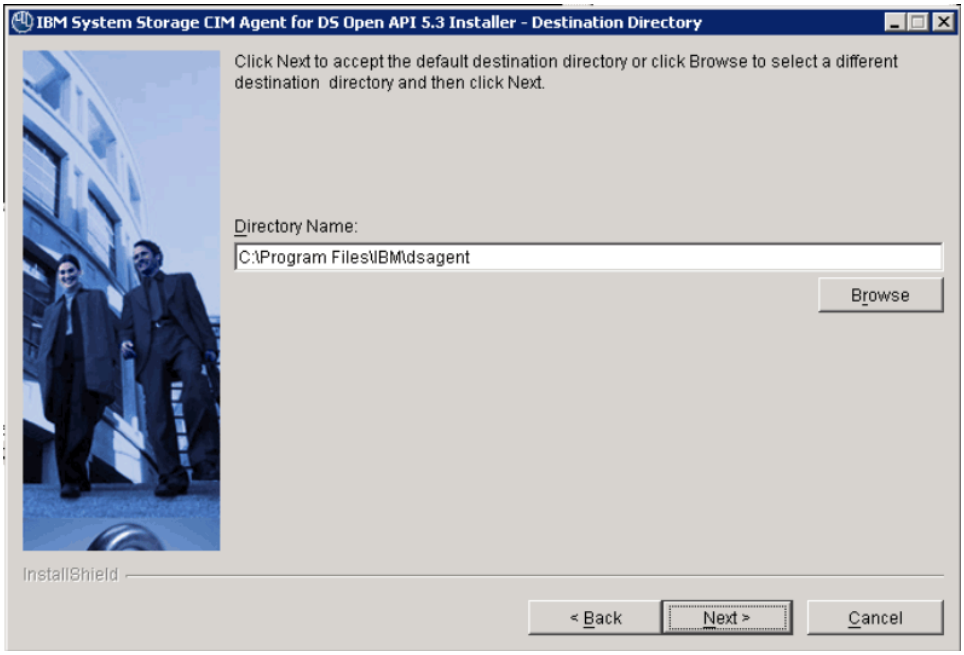


14. If the installation wizard detects a prior installation of the CIM agent, the Product Installation Check window opens. Check the **Preserve Configuration** check box if you want to preserve your configuration settings. Follow any specific instructions in the window. For example, the figure below shows a warning to stop running services. After you have followed all instruction, select **Next**.



15. The Destination Directory window opens. Click **Next** to accept the default directory where setup will install the files, or click **Browse** to select a different

directory for installation and then click **Next**.



Notes:

a. The Destination Directory window is displayed only if a version of CIM agent is not already installed. Otherwise, the CIM agent will be reinstalled or upgraded to the same install location.

b. If the program detects insufficient space for the CIM agent installation in the chosen destination, an error message is displayed. You can free some space on the destination drive and then click **Next** or you can stop the installation program by clicking **Cancel**. You can also go back by clicking **Back**, and choose another destination directory for the product.

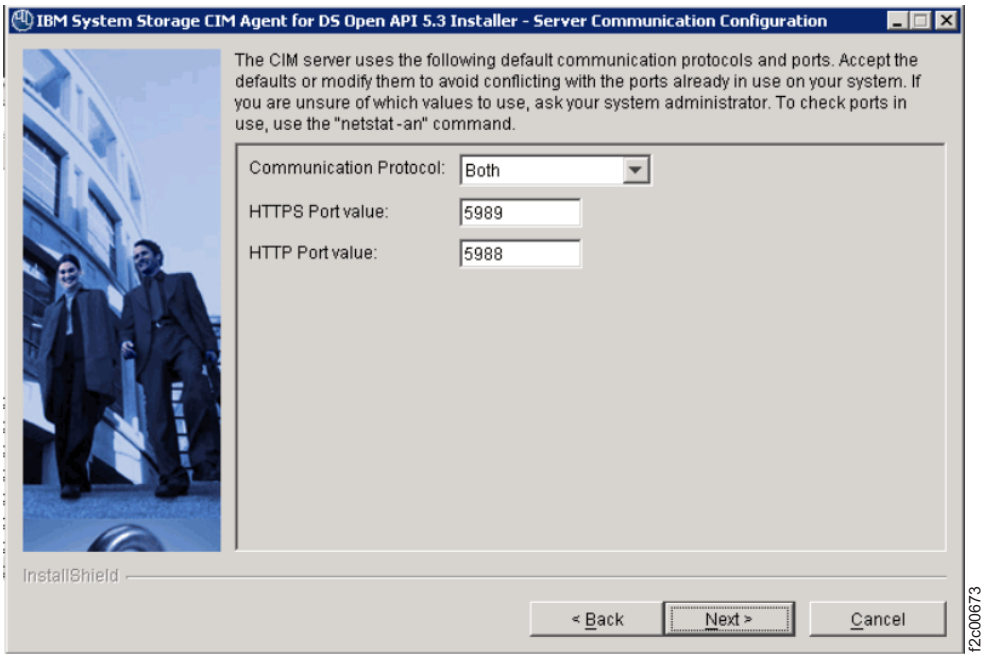
16. The Server Communication Configuration window opens. Click **Next** to accept the default port. If one or more of the default ports is the same as another port already in use, modify the default port and click **Next**.

    a. Either accept the default port or, if the default port is the same as another port already in use, modify the default port. Use the following command to check which ports are in use:

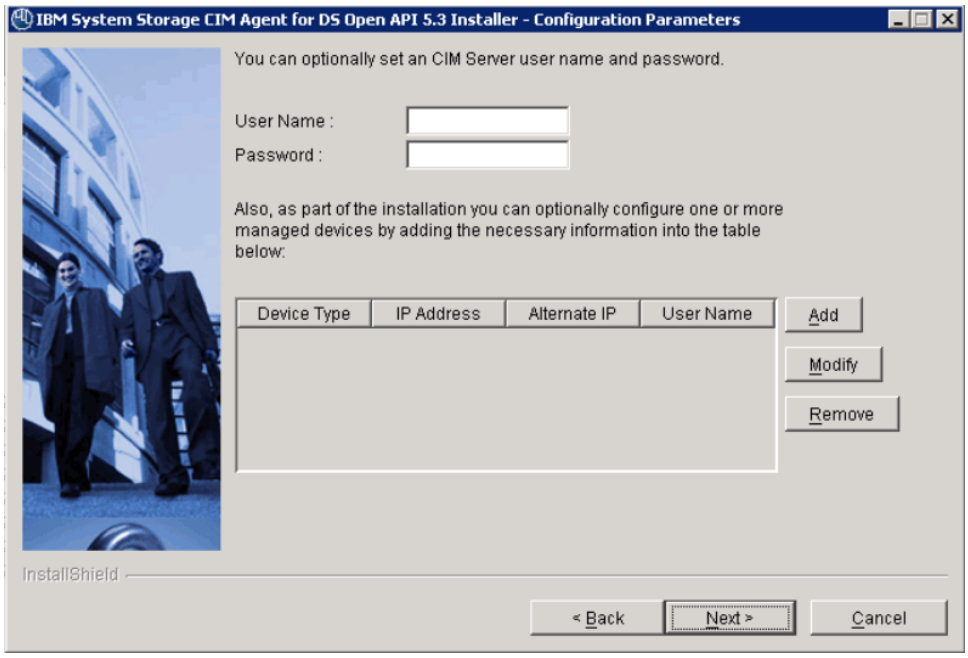
    ```
    netstat -a
    ```

    b. Either accept HTTPS as the communication protocol or select another protocol.

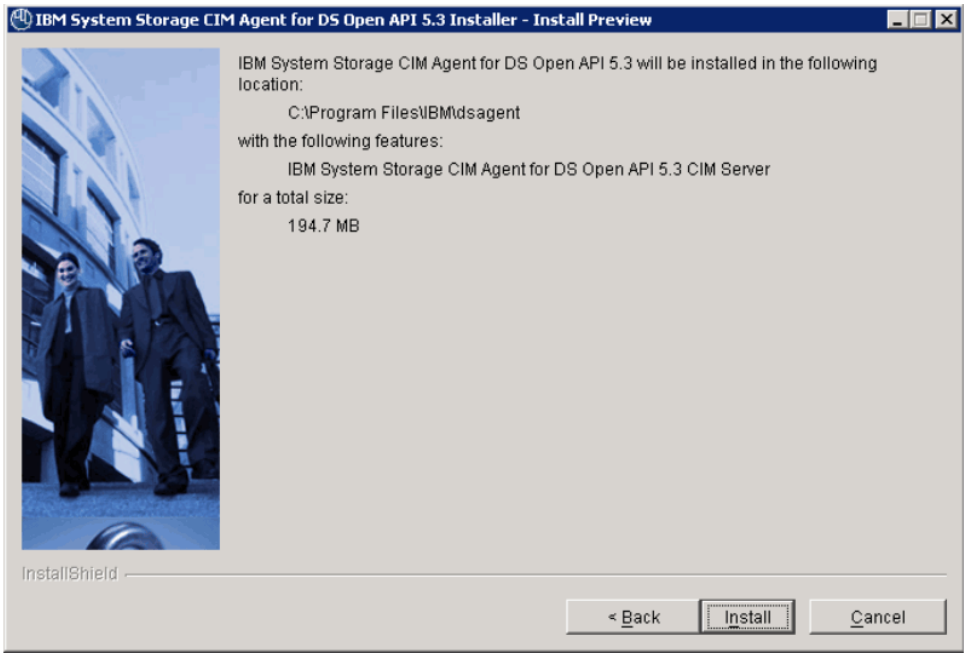
    c. Click **Next** to continue with the installation, or click **Cancel** to exit the wizard.



17. The Configuration Parameters window opens. Optionally enter a user name and password for the CIM server. You can click **Add** to optionally enter any information about devices that you would like to configure the agent to communicate with. When adding a device, a device type, IP address, username, and password must be specified. When adding a DS6000 or DS8000 family device, the device type should be "ds", the IP address should be of the master console, and the username and password should be the same one used to log into the DS Command Line Interface and DS Storage Manager. When adding an ESS family device for logical configuration, the device type should be "ess", the IP address should be of the primary processor complex, and the username and password should be the same as the one used to log into the ESS Command Line Interface and ESS Specialist. Optionally, you can specify the secondary processor complex IP address in the Alternate IP field. When adding an ESS Copy Services server, the device type should be "esscs", the IP address should be of the ESS Copy Services server, and the username and password should be the one used to log into the ESS Copy Services interface. Note that an ESS Copy Services server cannot be added without also adding the associated ESS logical configuration information. However an ESS can be added for logical configuration without adding a Copy Services server. After you have finished adding the configuration information, click **Next**.

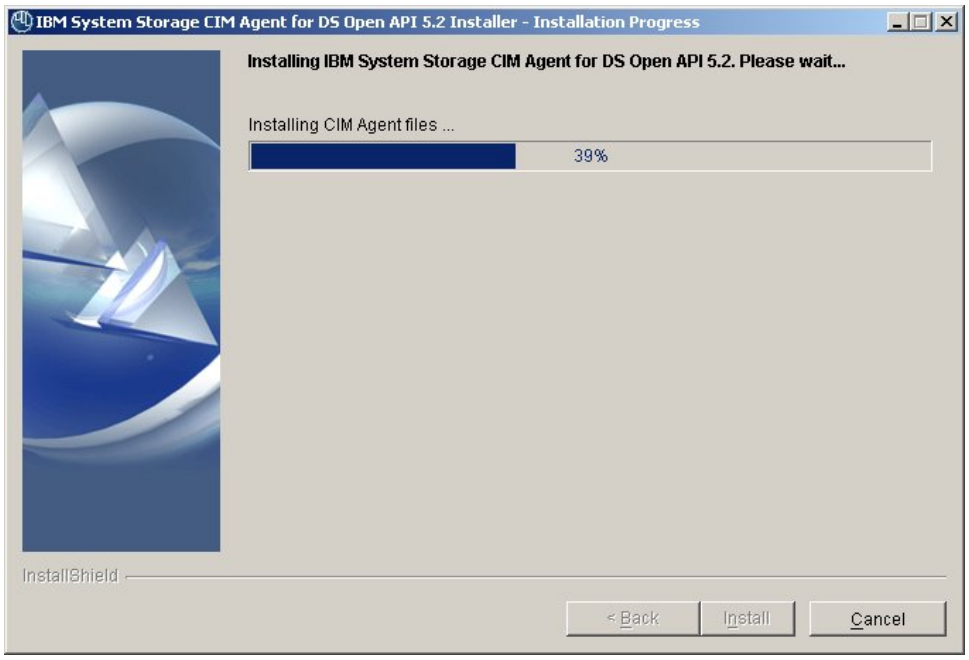


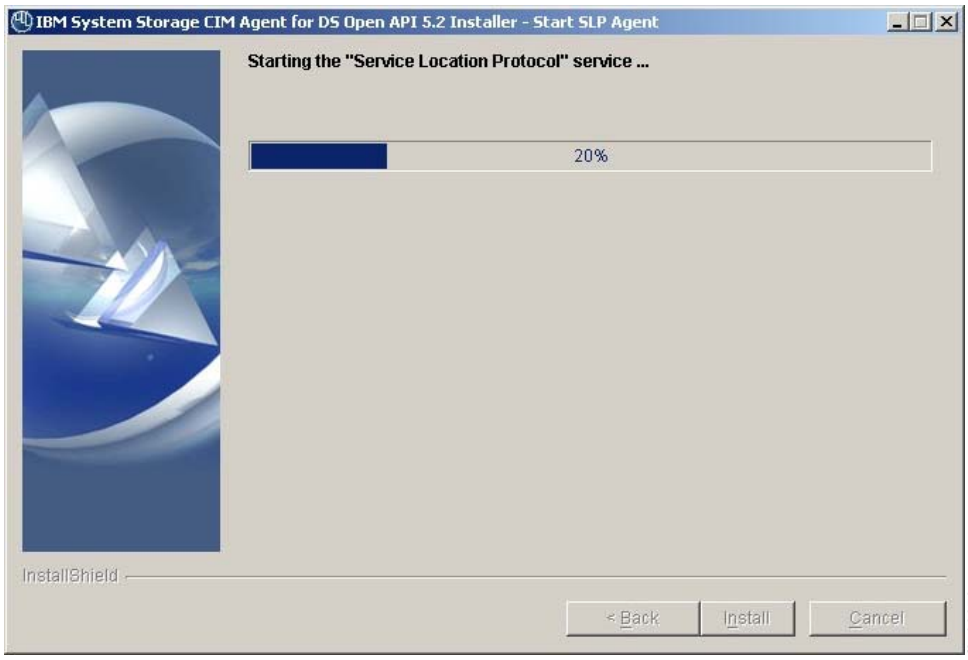
18. The Installation Preview window opens. Click **Install** to confirm the installation location and file size. You can click **Cancel** to exit the installation wizard or go back to the previous window by clicking **Back**.

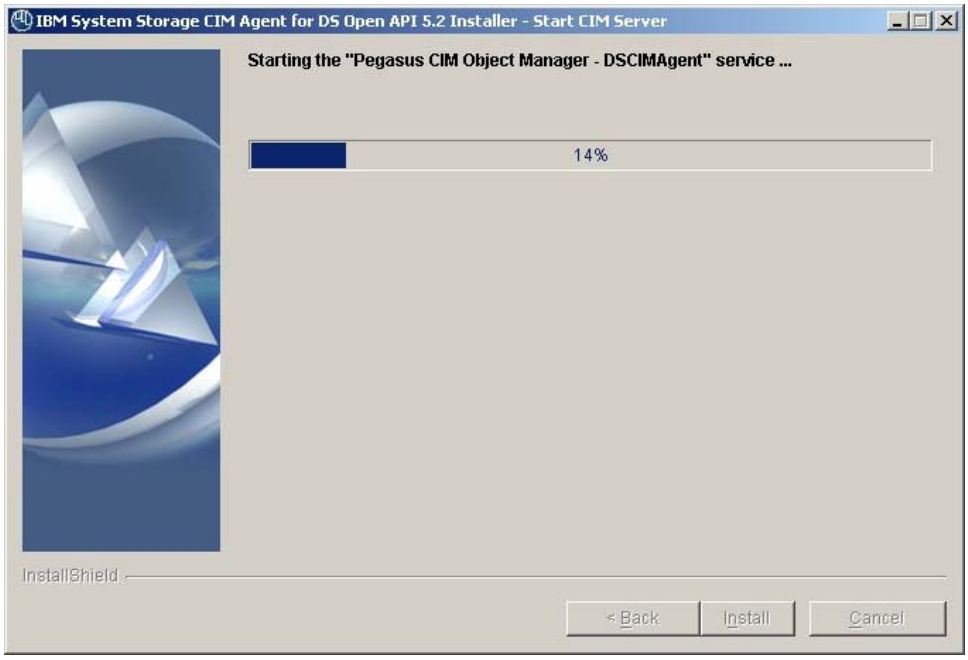


19. The Installation Progress window opens and indicates how much of the installation has been completed. Installation usually takes 3 - 10 minutes depending on the configuration of your machine. The installation installs the CIM agent files, starts the Service Location Protocol (SLP) service, and starts the Pegasus CIM Object Manager – DSCIMAgent service. You can click **Cancel** to exit the installation wizard.

Note: If you cancel the current operation, the information that you entered or selected in previous windows is not saved. You must start the installation again from the first step.

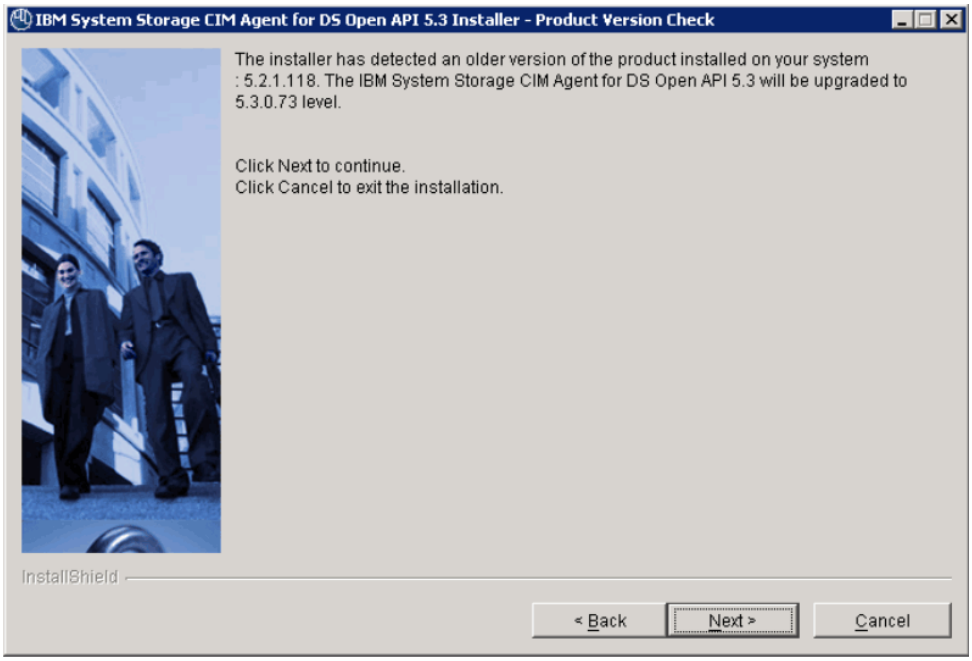






20. When the Installation Progress window closes, the **Finish** window opens. Click **Finish** to exit the installation wizard.

    Note: Before you proceed, review the log file for any possible error messages. The log file is located in *xxx*/log/install.log, where *xxx* is the destination directory where the CIM agent is installed. The install.log contains a trace of the installation actions.



21. Exit the LaunchPad program by clicking **Exit** on the LaunchPad window. If you have not done so already, continue with the post installation tasks for the CIM agent using the instructions in the following sections.

22. When you are finished with the CIM agent CD, type the following command to remove the CD:

```
# umount /mnt/cdrom
```

Installing the CIM agent on Linux in unattended (silent) mode

This section includes the steps to install the CIM agent in your Linux environment using the unattended (silent) mode.

You must satisfy all prerequisites before you begin the CIM agent installation.

You can choose to install the CIM agent in unattended (silent) mode, which involves customizing a response file and issuing a command or in graphical mode with the help of an installation wizard. If you want to install the CIM agent in unattended (silent) mode, continue with this section. After the completion of either kind of installation, you must verify the CIM agent installation.

The unattended (silent) installation capability enables you to run an installation process unattended. You can create a standard response file to ensure that the product is installed consistently on multiple systems. The responsefile file is a template located on the CIM agent CD that you must copy to disk and modify. To use the silent mode installation method, you will be performing the following tasks:

1. Find the responsefile file template on the CIM agent installation compact disk.
2. Copy the responsefile template to your hard disk drive.
3. Customize the responsefile file to your specifications.
4. Save the updated responsefile file.
5. Invoke the response file using the setuplinux script.

Steps:

Perform the following steps to install the CIM agent in your Linux environment using the unattended (silent) mode:

1. Log on as a user with root authority.
2. Type the following commands to locate the responsefile file on your CIM agent CD.

   ```
   cd /mnt/cdrom
   ```

   a. For Red Hat Advanced Server 3.0, issue the **LINIX_RHEL3** command.
   b. For SLES9, issue the **LINUX_SLES9** command.
3. Copy the responsefile file to your hard disk drive by typing the following command:

   ```
   mkdir /tmp/cimagent
   cp ./responsefile /tmp/cimagent
   ```
4. Customize the responsefile file with your parameters as follows:

   Using a text editor such as vi, modify the default options in the responsefile file with your desired values:

   - If you do not want to use the default value, remove the # character from the beginning of the line. Change the default value to the value that you want for that option. You *must* enclose all values in double quotation marks (“ ”).

- The <-G *licenseAccepted*> option defines license agreement verification. The default value is false. Uncomment this option and set it to true only after you have read the product License Agreement. The License Agreement can be found on the installation media. For instance, the following two files should be reviewed by English-speaking users:

  ```
  <CD_ROOT>/<OS-NAME>/license/LI_en
  <CD_ROOT>/<OS-NAME>/license/LA_en
  ```

  Where <CD_ROOT> is the root of the CD image or the root of the unpackaged installation media.
- The <-P *product.installLocation*> option defines the default directory where the product will be installed. To use another destination directory, remove the # character from the corresponding line and replace this default directory with the directory you want.
- If an instance of the IBM System Storage CIM Agent for DS 5.1 release is already installed on the target machine, the option <-W *checkPreviousVersion.migrateConfiguration*> specifies if the configured CIM users and devices will be migrated into the newly installed configuration. The default value is true. In order not to migrate the old configuration, remove the # character from the corresponding line and set the value to false.
- The <-G *useExistingSlp*> option specifies if you want the CIM agent to use the Service Location Protocol that is already installed into the system. The default value is no.
- The <-W *serverCommunicationConfig.communicationProtocol*> option specifies the CIM agent server communication protocol. If you want to change the default value during installation, remove the # character from the corresponding line and change the default server communication protocol (″both″) to HTTP or HTTPS protocol values.
- The <-W *serverCommunicationConfig.httpsPort*> option specifies the port number that the CIM server will use for secure HTTPS transport. This value must not conflict with existing port assignments on the system. If you are unsure of which values to use, ask your administrator. To check ports in use, use the ″netstat -an″ command. The default value is ″5989″.
- The <-W *serverCommunicationConfig.httpPort*> option specifies the port number that the CIM server will use for secure HTTP transport. This value must not conflict with existing port assignments on the system. If you are unsure of which values to use, ask your administrator. To check ports in use, use the ″netstat -an″ command. The default value is ″5988″.
- With the <-G *deviceConfigurationParameters*> option you can have the installer optionally configure one or more managed devices (″ds″, ″ess″ or ″esscs″) by adding the necessary information in the following format:

  For DS device:

  ```
  -G deviceConfigurationParameters=ds;IP Address;Alternate IP;UserName;Password
  ```

  For an ESS device:

  ```
  -G deviceConfigurationParameters1=ess;IP Address;Alternate IP;UserName;Password
  ```

  For an ESSCS device:

  ```
  -G deviceConfigurationParameters2=esscs;IP Address;Alternate IP;UserName;Password
  ```
- The <-W *serverConfigParams.userName*> and <-W *serverConfigParams.password*> options define the CIM user name and password to be configured by the installer. By default, only ″superuser″ CIM user is created.

5. Save the modified responsefile in your desired directory.

6. To launch the wizard in unattended (silent) mode with the customized responsefile, type the following command from the Linux directory on your CIM agent CD:

   ```
   # ./setuplinux -options <responsefile-path>/responsefile
   ```

   where <*responsefile-path*> is the path of the responsefile file.
7. Wait for the wizard to complete the installation.
8. Type `echo $?` to see if the installer completed without error. If any non 0 value is returned check for installation errors in the install.log file. The log file is initially created in /tmp/cimagent/install.log. At the end of the installation, you can find the log in <dest-path>/log/install.log, where <*dest-path*> is the destination directory where the CIM agent was installed. If the installation ends before the creation of <dest-path>, look in the /tmp/cimagent/install.log. Your install.log file should look similar to the following:

```
(Apr 12, 2006 3:15:13 PM), This summary log is an overview of the sequence of the installation of the IBM System
Storage CIM Agent for DS Open API 5.3.0.645
(Apr 12, 2006 3:15:13 PM), Linux system detected: SuSE Linux Enterprise Server 9
(Apr 12, 2006 3:15:27 PM), Command to be executed : find /proc -maxdepth 2 -name "exe*" -a -type l -printf "%
h/%f -> %l \n" 2>/dev/null
(Apr 12, 2006 3:15:28 PM), The following file exists : /etc/slp.conf
(Apr 12, 2006 3:15:28 PM), WARNING: The installation program has detected the "Service Location Protocol" was
previously installed into the system. You can only have one "Service Location Protocol" running on your system.If
you later uninstall it you will no longer have a "Service Location Protocol" since the IBM System Storage CIM Agent
for DS Open API 5.3 will not install another "Service Location Protocol". You will have to manually install the IBM
System Storage CIM Agent for DS Open API 5.3 - "Service Location Protocol" to reestablish a "Service Location
Protocol" service on your system.
You can either cancel the current installation, uninstall the existing "Service Location Protocol" and let the IBM
System Storage CIM Agent for DS Open API 5.3 install its own instance of "Service Location Protocol" or you can
continue the installation having the IBM System Storage CIM Agent for DS Open API 5.3 use the current instance.
(Apr 12, 2006 3:15:32 PM), IBM System Storage CIM Agent for DS Open API 5.3 will be installed in the following
location:
/opt/IBM/dsagent
- W checkPreviousVersion.migrateConfiguration = false
with the following parameters:
Communication Protocol: HTTPS and HTTP
HTTPS Port value: 5989
HTTP Port value: 5988
(Apr 12, 2006 3:15:33 PM), No configuration files to save/restore
(Apr 12, 2006 3:15:33 PM), CIM agent for the IBM Total Storage DS Open API not installed.
(Apr 12, 2006 3:15:34 PM), Installing provider libraries ...
(Apr 12, 2006 3:15:34 PM), Installing MOF files ...
(Apr 12, 2006 3:15:37 PM), Installing CIM Agent files ...
(Apr 12, 2006 3:15:40 PM), Installing OpenSLP files ...
(Apr 12, 2006 3:15:40 PM), Installing OpenSSL files ...
(Apr 12, 2006 3:15:40 PM), Installing Java files ...
(Apr 12, 2006 3:15:42 PM), The file /opt/IBM/dsagent/config/envConf successfully updated.
(Apr 12, 2006 3:15:42 PM), The file /opt/IBM/dsagent/startup/dsagent successfully updated.
(Apr 12, 2006 3:15:42 PM), The file /opt/IBM/dsagent/startup/dsslpd successfully updated.
(Apr 12, 2006 3:15:43 PM), Setting CIM Server configuration ...
(Apr 12, 2006 3:15:43 PM), Command to be executed : /tmp/ismp005/676745.tmp -s enableHttpConnection=true -
p
(Apr 12, 2006 3:15:45 PM), Command to be executed : /tmp/ismp005/676745.tmp -s enableHttpsConnection=true
-p
(Apr 12, 2006 3:15:46 PM), Command to be executed : /tmp/ismp005/676745.tmp -s httpPort=5988 -p
(Apr 12, 2006 3:15:47 PM), Command to be executed : /tmp/ismp005/676745.tmp -s httpsPort=5989 -p
(Apr 12, 2006 3:15:48 PM), The CIM Server configuration successfully set.
(Apr 12, 2006 3:15:49 PM), Generating certificates ...
(Apr 12, 2006 3:15:49 PM), Command to be executed : /opt/IBM/dsagent/bin/mkcertificate certname
(Apr 12, 2006 3:15:50 PM), The certificates were successfully generated.
(Apr 12, 2006 3:15:50 PM), Enabling SSL communication ...
(Apr 12, 2006 3:15:50 PM), Command to be executed : /tmp/ismp005/6122101.tmp -s sslKeyFilePath=/opt/IBM/
dsagent/certificate/certname.key -p
file:///C|/CMVCDiana/api/api_ereview/Comments/release1/cmm_bk10.htm (13 of 25)4/19/2006 8:45:57 AM
CIM agent for Linux
(Apr 12, 2006 3:15:50 PM), Command to be executed : /tmp/ismp005/6122101.tmp -s sslCertificateFilePath=/opt/
IBM/dsagent/certificate/certname.cert -p
(Apr 12, 2006 3:15:50 PM), SSL communication enabled.
(Apr 12, 2006 3:15:51 PM), Enabling CIM server authentication ...
(Apr 12, 2006 3:15:51 PM), Command to be executed : /tmp/ismp005/1068480.tmp -s enableAuthentication=true -
p
(Apr 12, 2006 3:15:51 PM), CIM server authentication enabled.
(Apr 12, 2006 3:15:51 PM), Creating /opt/IBM/dsagent/pegasus/cimserver.passwd file ...
(Apr 12, 2006 3:15:51 PM), Installing "IBM System Storage CIM Agent for DS Open API 5.3" service ...
(Apr 12, 2006 3:15:51 PM), The "IBM System Storage CIM Agent for DS Open API 5.3" service successfully
installed.
(Apr 12, 2006 3:15:51 PM), Skipping "Service Location Protocol" service installation ...
(Apr 12, 2006 3:15:52 PM), Setting Java Runtime Environment for the uninstaller ...
(Apr 12, 2006 3:16:22 PM), Starting the "IBM System Storage CIM Agent for DS Open API 5.3" service ...
(Apr 12, 2006 3:16:22 PM), Command to be executed:
export `echo DSAGENT_HOME=/opt/IBM/dsagent`;/etc/init.d/dsagent start
(Apr 12, 2006 3:17:41 PM), The "IBM System Storage CIM Agent for DS Open API 5.3" service successfully started.
(Apr 12, 2006 3:17:41 PM), INSTSUCC: IBM System Storage CIM Agent for DS Open API 5.3 has been successfully
installed.
```

9. Close the command prompt window by entering a command, for example **exit**. Continue with the post installation tasks for the CIM agent in the following sections. You can also continue the post installation tasks using the following option:
   a. Open the LaunchPad from the Linux directory of the CIM agent CD by typing `# ./launchpad_linux`.
   b. Click **Post installation tasks** on the LaunchPad window. Continue with the post installation tasks for the CIM agent by following the instructions in this file.

Verifying the CIM agent installation on Linux

This section provides the steps to verify that your CIM agent is installed correctly on your Linux system.

Steps

Perform the following steps to verify your CIM agent installation:

1. Verify the installation of the service location protocol (SLP).
   a. Open a Command Prompt window and type the following command to verify that SLP is installed:

      ```
      # ps -ef | grep -v grep | grep slpd
      ```

      If the SLP daemon is started, output similar to the following is displayed:

      ```
      daemon 16054     1 0 18:54 ?      00:00:00 /opt/IBM/dsagent/slp/bin/slpd
      ```

2. Verify the installation of CIM agent.
   a. Check that the CIMOM daemon is installed and started by typing the following command:

      ```
      # ps -ef | grep cimserv
      ```

      ```
      root 18151 1 0 15:16 ? 00:00:04 cimserver
      root 18237 17469 0 15:30 pts/5 00:00:00 grep cimserv
      ```

   b. If the CIMOM is not started, issue the following command to run the **startagent** file.

      ```
      startagent
      ```

      Note: Before you can issue this command, you must set the environment variables in the source <dest-path>/config/envConf.

If you are able to perform all of the verification tasks successfully, the CIM agent has been successfully installed on your Linux system.

Configuring the CIM agent on Linux

This section provides the steps to configure storage units and user accounts for CIM agent after it has been successfully installed.

You can use the modifyconfig command (described in Chapter 6) to change the configuration of some of the parameters that were configured during installation. You can change the CIM agent port value, protocol (HTTP/HTTPS), and enable or disable the debug option.

Steps:

Perform the following steps to configure storage units and user accounts for the CIM agent:

1. Ping each ESS and DS that the CIM agent manages by typing the following command:
   a. Open a command prompt window.
   b. Issue a **ping** command; for example:

```
ping 9.11.111.111
```

where 9.11.111.111 is the ESS processor complex or DS master console IP address

c. Check that you can see reply statistics from the IP address. The following is example output:

```
Pinging 9.11.111.111 with 64 bytes of data:

64 bytes from 9.186.10.119: icmp_seq=1 ttl=64 time=2.09 ms
64 bytes from 9.186.10.119: icmp_seq=2 ttl=64 time=1.02 ms
64 bytes from 9.186.10.119: icmp_seq=3 ttl=64 time=1.01 ms
64 bytes from 9.186.10.119: icmp_seq=4 ttl=64 time=1.02 ms
```

If you see other messages that indicate that the request has timed out, see your Network Administrator for help on establishing network connectivity before you configure storage units. If you have not already setup the environment variables for the CIM agent management commands, you must do so now: source <dest-path>/config/envConf

2. Type the following command to configure the CIM agent for each ESS or DS server that the CIM agent can access.

   `dscimcli mkdev <ip> -type <type> -user <user> -password <password>`

   ip For an ESS configuration server, this is the IP address of the primary processor card.

   For an ESS copy services server, this is the IP address of the primary copy services server.

   For a DS server, this is the IP address of the primary hardware or software master console (HMC/SMC).

   type

   For an ESS configuration server, this is *ess*.

   For an ESS copy services server, this is *esscs*.

   For DS, this is *ds*.

   user/password

   For an ESS configuration server, this is the specialist or ESSCLI user name and password.

   For an ESS copy services server, this is the specialist or ESS copy services server user name and password

   For a DS server, this is the storage manager GUI or DSCLI user name and password

3. After you have defined all of the ESS and DS servers, type the following command to verify that the devices were correctly added and have successfully connected:

   `dscimcli lsdev -l`

   The following is example output:

```
Type   IP IP2        user name  Storage Image    Status     Code Level Min Codelevel
==== ==============  ========  ================ ========== =========  ============
DS   9.11.111.111 -  admin     IBM.2107-1234567 successful 5.1.0.309  5.1.0.309
>>>
```

If the status is failed, there was a failure when the CIM agent attempted to connect to the storage device. If the CIM agent is unable to connect during mkdev, an error is returned immediately. If the device shows as failed in lsdev -l, it is likely that you added the device earlier (for example, during the installation wizard) and the connection is now failed. To ensure that your storage device's management interface is functioning, use the command line interface (ESSCLI or DSCLI) or graphical interface (ESS Specialist or DS Storage Manager) to attempt to log into the device from the server where the CIM agent is hosted. If you are unable to connect via the native command line interface or graphical interface, there is likely an error in the network or the storage device. If you are able to connect via the native interfaces, there is likely an error in the CIM agent. Contact your service representative for assistance.

Note: Because the CIM agent periodically collects and caches some pieces of information from the defined storage units, the CIM agent might periodically take longer to respond to requests; for example, immediately after adding a new storage unit.

4. Configure the CIMOM for each user that you want to have authority to use the CIMOM by running the CIMOM configuration program.

   During the CIM agent installation, the default user name to access the CIM agent CIMOM is created. The default user name is "superuser" with a default password of "passw0rd". You must use the default user name and password when you use the **mkuser** command for the first time after installation. After you have added other users, you can initiate the **mkuser** command using a user name that you have defined instead of using the default.

   a. Start the CIM agent, if it is not started, by typing the following command:

      ```
      # startagent
      ```

   b. Type the following command to create a new user:

      ```
      # dscimcli mkuser -user cimuser -password cimpass
      ```

      The following is example output:

      ```
      User created.
      ```

      Restriction: You cannot delete or modify the current user using the **mkuser** command.

   c. You can change the default password for ″superuser″ by starting the **mkuser** command for a user that you added. Issue the following command to change the password:

      ```
      >>>dscimcli chuser superuser -password passw0rd -newpassword <newpassword>
      ```

      where *newpasswd* is the new password for the superuser.

   d. You can delete the superuser by issuing the following command:

      ```
      >>>rmuser superuser
      ```

   e. Type the **exit** command to exit the CIMOM configuration program.

If you are able to perform all of the configuring tasks successfully, the CIM agent has been successfully installed on your Linux system.

Verifying the CIM agent connection on Linux

During this task, the CIM agent software connects to the storage unit that you identified in the configuration task.

Steps:

Perform the following steps to verify the connectivity to an ESS or DS. You also verify the service location protocol (SLP) daemon and the CIMOM are running, since they are needed to connect to a storage unit.

1. You must set environment variables before you can issue any of the CIM agent management commands:

   ```
   source <dest-path>/config/envConf
   ```

   where <*dest-path*> is the destination directory where the CIM agent is installed.
2. Before you run the command to verify the CIM agent connection, type the following command to see if the SLP daemon is started:

   ```
   ps -ef | grep slpd
   ```

   If the SLP daemon is not started, type the following command from a separate command prompt window:

   ```
   # /etc/init.d/slpd start
   ```

   Note: This session remains active until you stop it. Ensure that it is running as long as the CIM agent is running.
3. Before you run the command to verify the CIM agent connection, ensure the CIMOM is started by typing the following command:

   ```
   ps -ef | grep cimserv
   ```

   If the CIMOM is not started, start it by typing the following command:

   ```
   # startagent
   ```

   Notes:

   a. The startagent command quickly returns a prompt; however, a returned prompt does not mean that the processing is complete. If there are a large number of LUNs to enumerate in the internal domain, it takes considerable time for the CIMOM to find and enumerate all those disks. Do *not* issue the **dscimcli lsdev -l** command until CIMOM processing is complete. You can view the cimom.log in the directory where you installed the CIM agent to verify the CIMOM processing status.

   b. The default is to start the secure CIMOM. It registers itself with SLP and accept requests on port 5989.
4. You can view CIMOMs registered with SLP using the **slptool findsrvs wbem** command. This command locates all WBEM services (for example, CIMOMs) in the local network. Information is displayed for the storage units to which the CIM agents can connect. In the following example, the CIM agent on host 9.11.111.111 connects to two storage units (2107.AZ123x and 2105.2223x).

   Issue the following command from a command prompt window:

   ```
   # dscimcli lsdev -l
   ```

The following is example output of a successful connection:

```
Type  IP         IP2  Username  Storage Image    Status     Code Level  Min Codelevel
===== ========== ========= ========== ========== ========== ==========  =============
DS   9.11.111.111 -   admin     IBM.2107-1234567 successful 5.1.0.309   5.1.0.309
The Status field indicates if the CIM Agent can communicate with the DS or ESS device
```

If you received similar output verifying a connection, the CIM agent is now running.

Removing the CIM agent on Linux

This optional task provides the steps to remove the CIM agent from your Linux system.

Steps:

Perform the following steps to remove the CIM agent:

1. Log on as a user with root authority.
2. If the CIM Object Manager for DS Open API Service and the Service Location Protocol services are started, you must stop them. Type the following command to check if the CIMOM is running:

   The follow is example output if the CIMOM is running.

   ```
   # ps -ef | grep cimserv
   ```

   ```
   root 18151 1 0 15:16 ? 00:00:04 cimserver
   root 18237 17469 0 15:30 pts/5 00:00:00 grep cimserv
   ```

   If the CIMOM is running, stop it by typing the following command:

   ```
   # stopagent
   ```

The CIM agent removal process does not remove configuration files, logs, and similar files that are created during or after the installation process. They are located in the destination path where CIM agent component was installed. For example, the default target directory is **/opt/IBM/dsagent**.

Remove the directory and all of its contents (especially if you plan to reinstall CIM agent).

Note: If you want to keep the old configuration files, before removing them from the installation destination path, save them in another location on your system to restore them later.

To remove the cimagent directory you must type the following command:

```
# rm -Rf /opt/IBM/dsagent
```

Note: The recursive remove is used in the example because the CIM agent has a deep directory structure. Make sure you understand a recursive remove: it is very powerful because it removes all subdirectories without prompting you. You must use the fully qualified directory name.

Removing the CIM agent on Linux in graphical mode

Perform the following steps to remove the CIM agent in graphical mode:

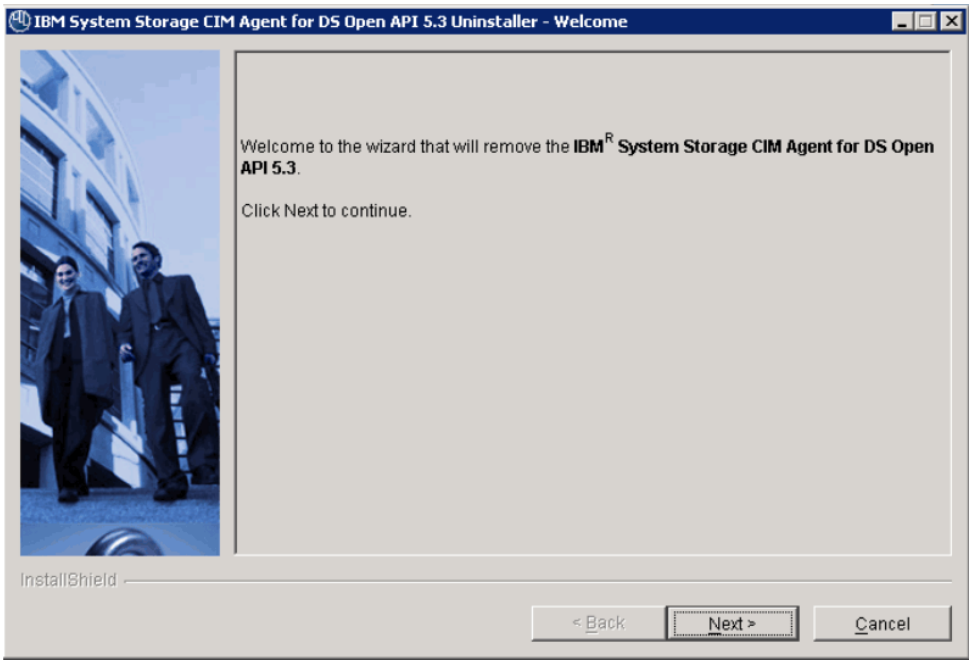
1. Type the following command to run the uninstall program from the **_uninst** subdirectory:

   ```
   # cd <dest-path>/_uninst
   # ./uninstaller
   ```

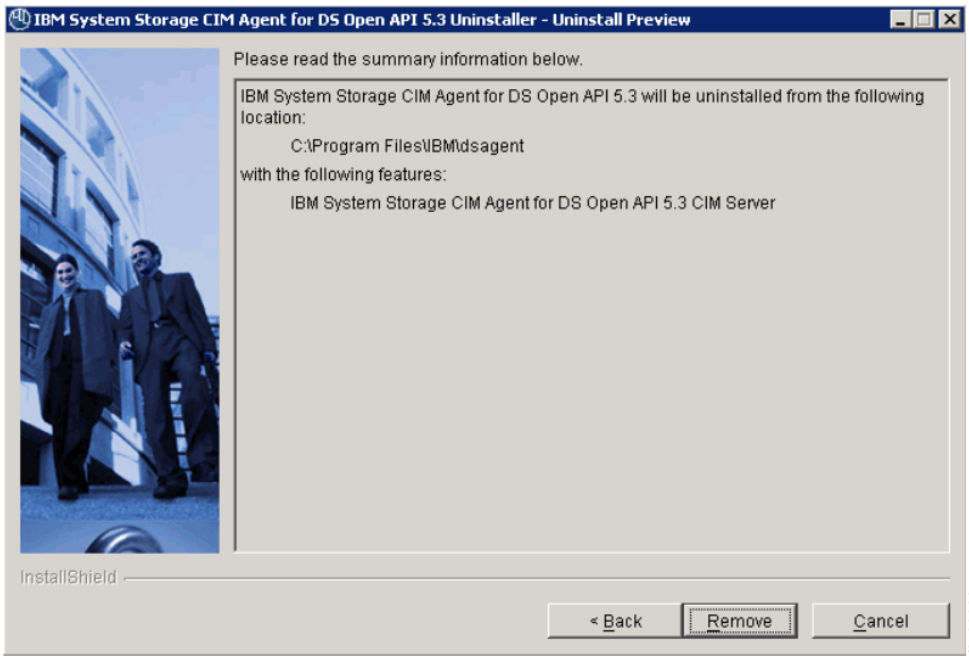
   where *<dest-path>* is the target directory where CIM agent is installed.
2. If the wizard uninstaller launcher was not created during the CIM agent installation, type the following command:

   ```
   # <dest-path>/java/jre/bin/java -jar <dest-path>/_uninst/uninstall.jar
   ```

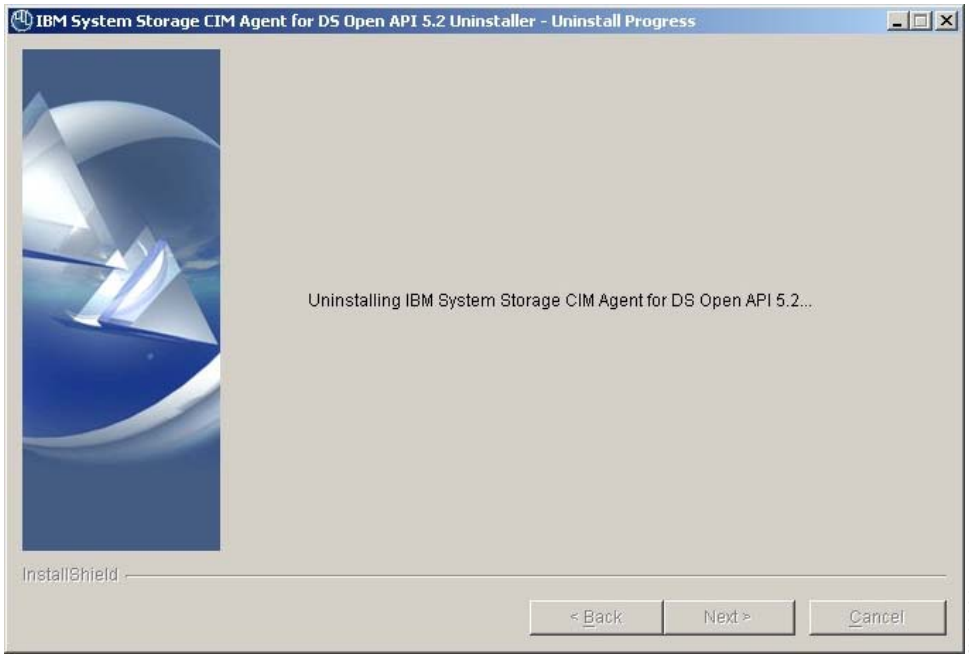
   where *<dest-path>* is the target directory where the CIM agent is installed.
3. The Welcome window opens. Click **Next** to continue with the removal program, or click **Cancel** to exit the removal program.



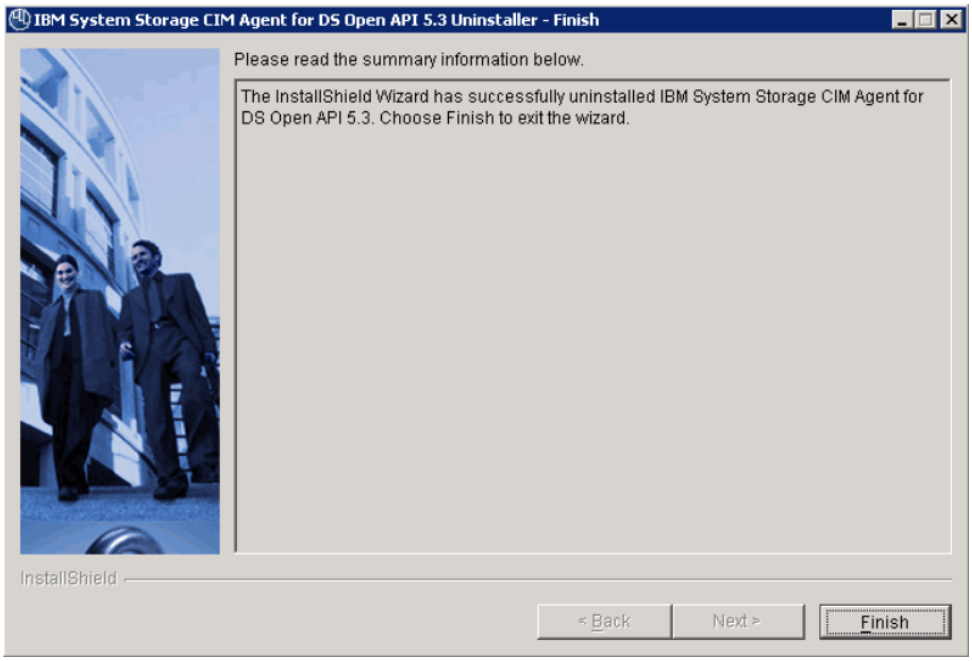
4. The Uninstall Preview window opens, and displays the location of the product that will be removed. Click **Remove** to continue with the removal program, or click **Cancel** to exit.



5. The Uninstall Progress window opens. Wait for the program to remove the CIM agent.



6. The Finish window displays information about the result of removal (successfully or failed).



Click **Finish** to end the removal program.

Removing the CIM agent on Linux in unattended (silent) mode

This section allows you to perform an unattended (silent) mode removal in Linux.

Steps:

Perform the following steps to remove the CIM agent in unattended (silent) mode:

1. Stop SLP, CIMOM, and all related processes.
2. Type the following command to run the removal program from the _uninst subdirectory:

   ```
   <dest-path>/_uninst/uninstaller -silent
   ```

3. If the program detects that the service location protocol (SLP) or the IBM CIM Object Manager (CIMOM) services are running, it displays an error message and the uninstallation fails. You can look for details in the <dest-path>/logs/uninstall.log file. However, if you want the program to automatically stop the services, you must set the stopProcessesResponse option to yes in the command line:

   ```
   <dest-path>/_uninst/uninstaller -silent -G stopProcessesResponse=yes
   ```

Chapter 4. CIM agent for Windows

This chapter includes an overview of the installation process and instructions for installing and configuring the CIM agent on a Windows 2003 operating system.

Installation overview for Windows

This section provides an overview of the installation and configuration of the CIM agent on a Windows 2003 operating system. Ensure that you know how to administer a Windows 2003 operating system before you install the CIM agent. Also be familiar with the commands that you use during installation and configuration of the CIM agent.

Perform the following list of installation and configuration tasks on your Windows operating system:

1. Before you install the CIM agent on a Windows operating system, verify the hardware and software requirements.
2. Install the CIM agent either in graphical mode with the help of a wizard or in unattended mode (also known as silent mode), which involves customizing a response file and issuing a command. If your system does not support the graphical mode, you cannot use the **-console** parameter for the executable file to run the installation in an interactive console mode. You must use the unattended installation mode.
3. Verify the CIM agent Windows installation.
4. Configure the CIM agent for Windows. You might want to revisit the configuration section as you add, change, or delete CIMOM authentication and storage unit information. If you add one or more DS or ESS devices, repeat this step for each device that you add.
5. Verify the connection to your storage unit.
6. Optionally, remove the CIM agent. Perform this optional task only if you receive errors during installation verification or if the CIM agent did not set the environment variables.

Installing the CIM agent on Windows in graphical mode

This section includes the steps to install the CIM agent in your Windows environment in graphical mode.

You must satisfy all prerequisites before you begin the CIM agent installation.

You can choose to install the CIM agent in graphical mode with the help of an installation wizard or in unattended (silent) mode, which involves customizing a response file and issuing a command. If you want to install the CIM agent in graphical mode, continue with this section. After the completion of either kind of installation, you must verify the installation of the CIM agent. Before you install the CIM agent on Windows, verify that your system meets the hardware and software requirements.

1. Log on to your system as the local administrator.
2. Insert the CIM agent CD into the CD-ROM drive.

The CIM agent program should start within 15 - 30 seconds if you have autorun mode set on your system. If the LaunchPad window does not open, perform the following steps:

a. Use a Command Prompt or Windows Explorer to change to the Windows directory on the CD.
b. If you are using a Command Prompt type:

```
LaunchPad
```

c. If you are using Windows Explorer, double-click on the **LaunchPad.bat** file.

Note: If you are viewing the folder with Windows Explorer with the option selected to hide file extensions for known file types, find the LaunchPad file with the file type of MS-DOS Batch File.

3. The following options are displayed when the LaunchPad window opens:

CIM Agent overview
Offers information about the CIM agent

Readme file
Offers any last minute product information that did not make it into this installation guide

Installation guide
Offers instructions on how to install the CIM agent (a softcopy of this document)

License agreement
Offers information about the license for the CIM agent

CIM Agent Web site
Offers information from the product Web site

Installation wizard
Starts the CIM agent installation program

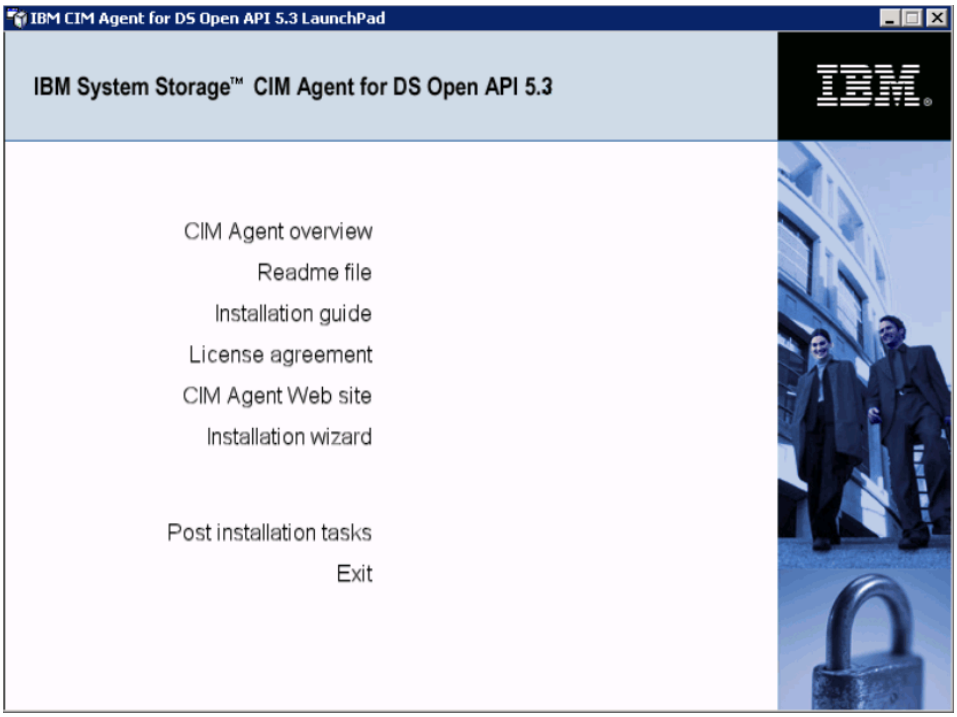
Post installation tasks
Offers information about configuring users and storage unit communication

Exit Exits the CIM agent LaunchPad program

4. Click the **Readme file** from the LaunchPad window or from the **README.txt** file located in the doc or Windows directory on the CIM agent CD to check for information that might supersede the information in this guide.
5. Click **Installation wizard** from the LaunchPad window to start the installation.

Note: The LaunchPad window remains open behind the installation wizard so that you can access product information during the installation process. Click **Exit** if you want to close the LaunchPad.

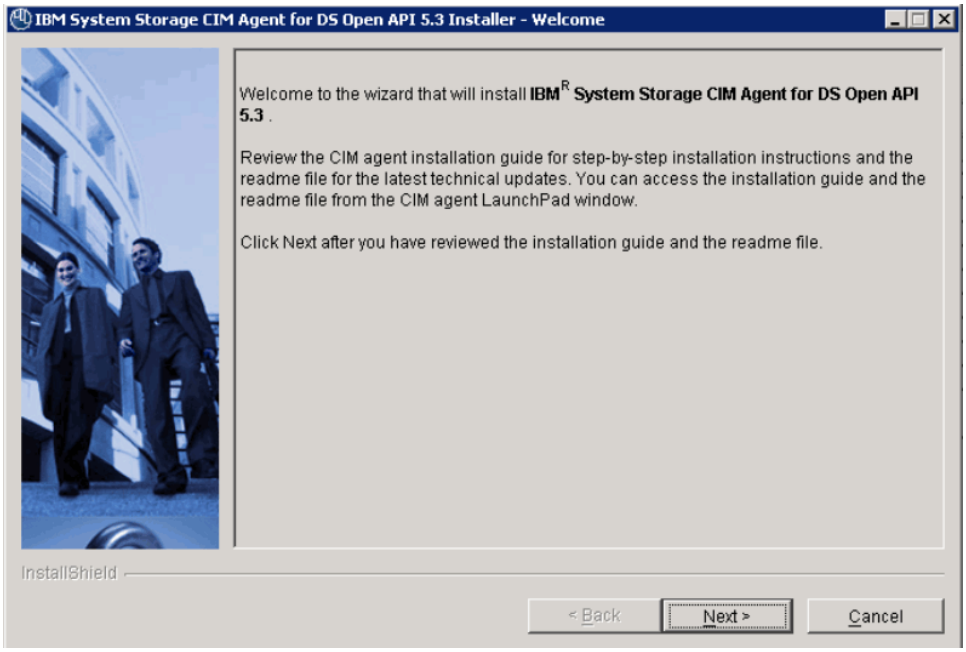
The LaunchPad window remains open (behind the wizard) during the installation. You can access product information after the installation has started. The LaunchPad returns to the foreground when the installation is complete. You can click **Exit** to close the LaunchPad.



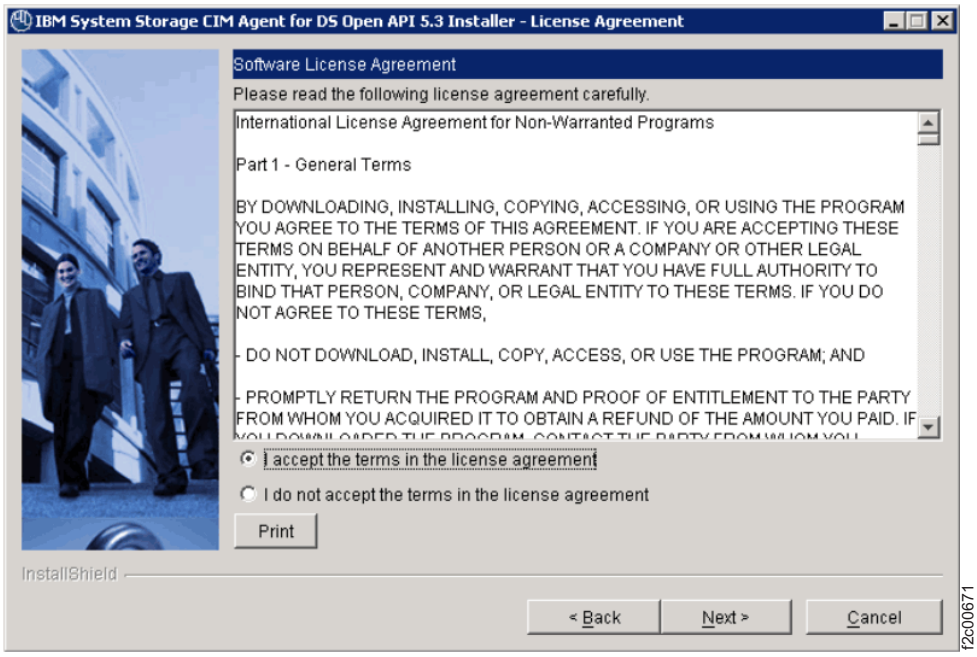
6. There might be a slight delay while the software loads on your system. After the software loads a DOS prompt window opens to display the following message:

```
Initializing InstallShield Wizard...
Preparing Java (tm) Virtual Machine ..... .
.................................................
```

7. The Welcome window opens suggesting what documentation you should review prior to installation. Click **Next** to continue, or click **Cancel** to exit the installation.

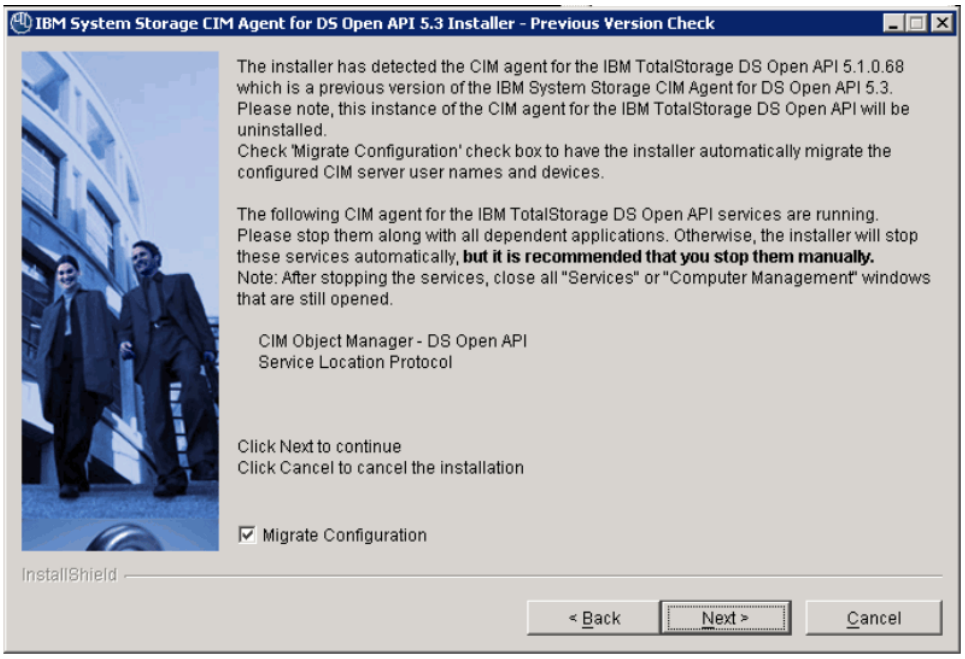


8. The License Agreement window opens. Read the license agreement information. Select **I accept the terms of the license agreement**, then click **Next** to accept the license agreement. Otherwise, keep the selection **I do not accept the terms of the license agreement** (it is the default) and click **Cancel** to exit the installation.

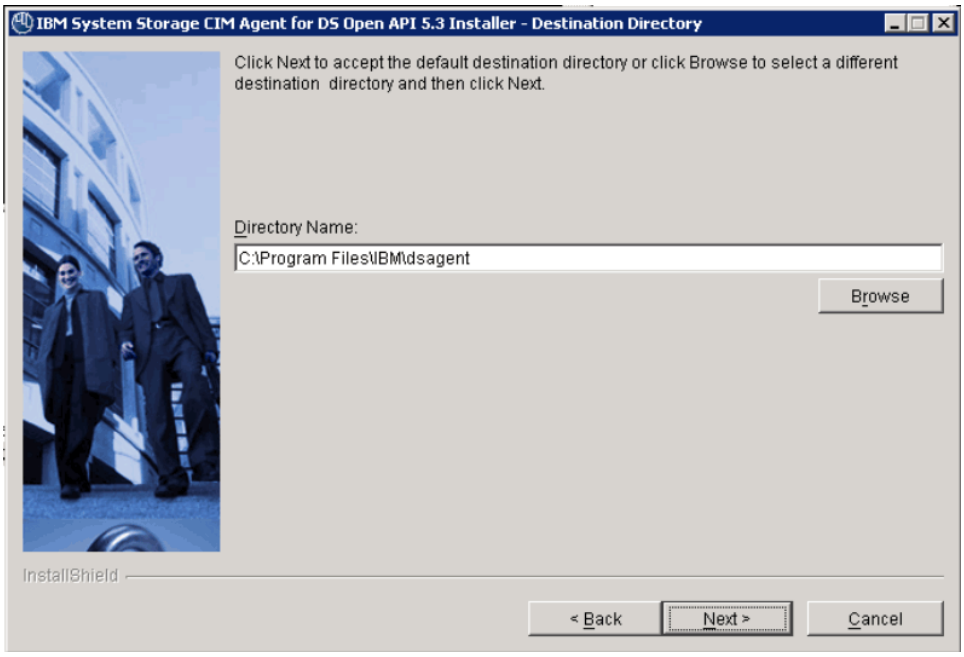


9. If the installation wizard detects a prior installation of the CIM agent, the Product Installation Check window opens. Check the **Preserve Configuration** check box if you want to preserve your configuration settings. Follow any specific instructions in the window. For example, the figure below shows a warning to stop running services. After you have followed all instructions,

select **Next**.



10. The Destination Directory window opens. Click **Next** to accept the default directory where setup will install the files, or click **Browse** to select a different directory for installation and then click **Next**.



Note:

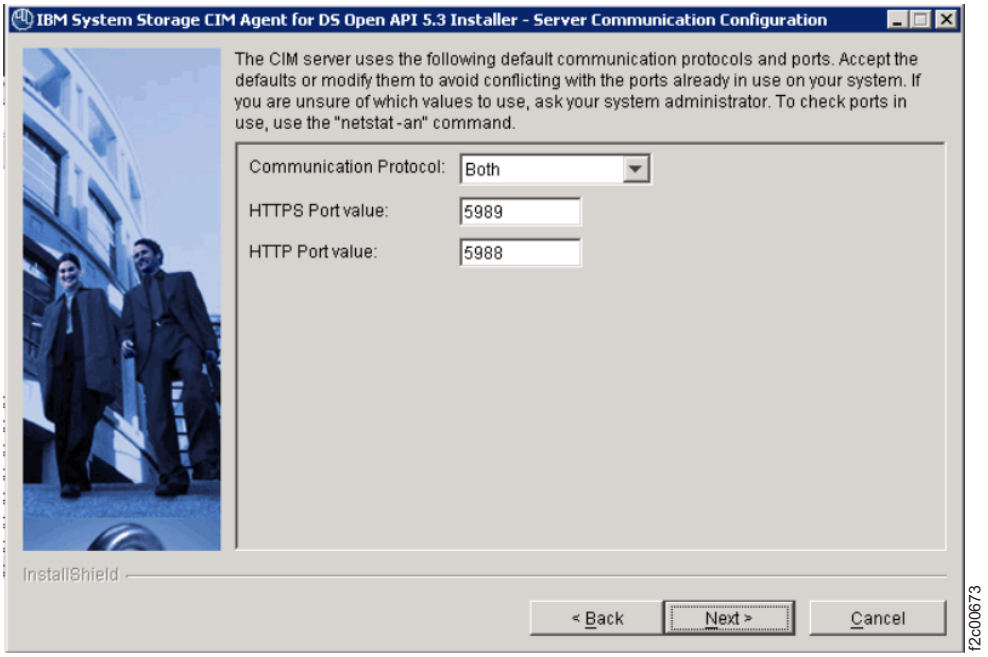
a. The Destination Directory window is displayed only if a version of CIM agent is not already installed. Otherwise, the CIM agent is reinstalled or upgraded to the same install location.

b. If the program detects insufficient space for the CIM agent installation in the chosen destination, an error message is displayed. You can free some space on the destination drive and then click **Next** or you can stop the installation program by clicking **Cancel**. You can also go back by clicking **Back**, and choose another destination directory for the product.

11. The Server Communication Configuration window opens. Click **Next** to accept the default communication protocol and ports. If one or more of the default ports is the same as another port already in use, modify the default port and click **Next**. Use the following command to check which ports are in use.
    a. Either accept the default port or, if the default port is the same as another port already in use, modify the default port. Use the following command to check which ports are in use:

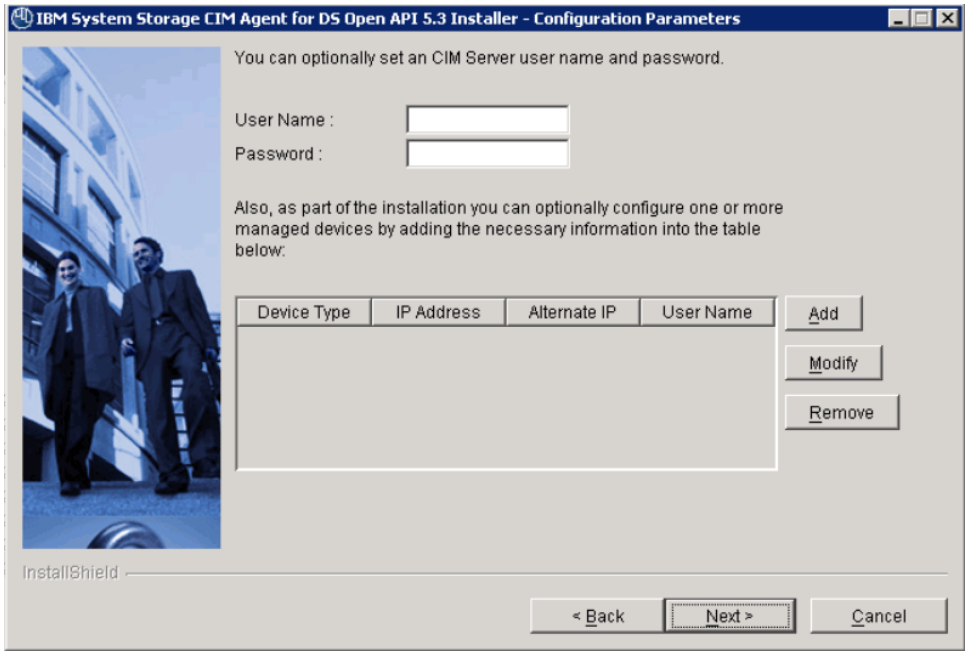
       ```
       netstat -a
       ```

    b. Either accept HTTPS as the communication protocol or select another protocol.
    c. Click **Next** to continue with installation, or click **Cancel** to exit the wizard.

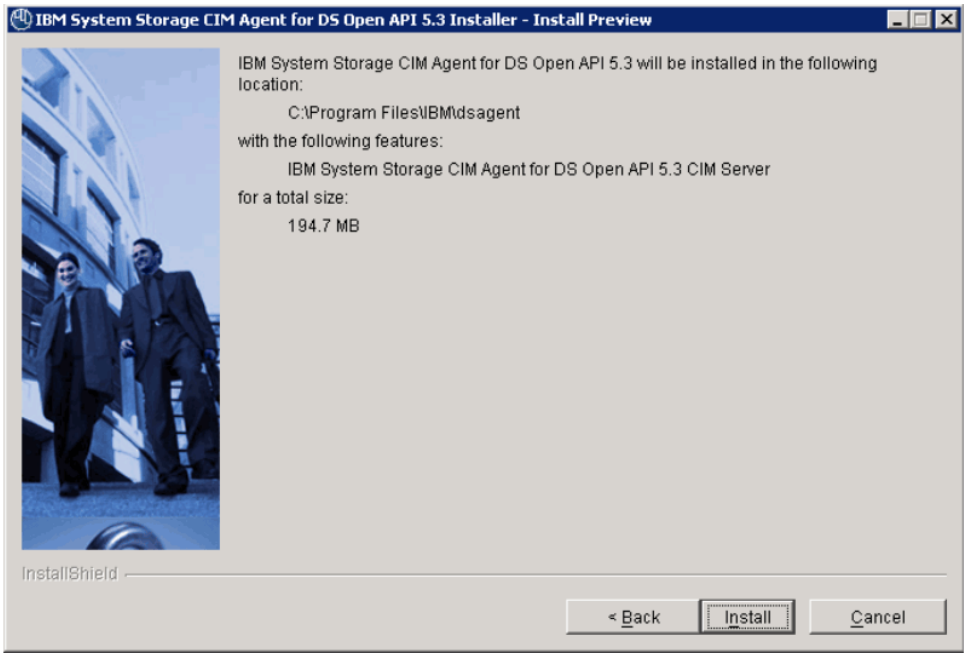


12. The Configuration Parameters window opens. Optionally enter a user name and password for the CIM server. You can click **Add** to optionally enter any information about devices that you would like to configure the agent to communicate with. When adding a device, a device type, IP address, username, and password must be specified. When adding a DS6000 or DS8000 family device, the device type should be "ds", the IP address should be of the master console, and the username and password should be the same one used to log into the DS Command Line Interface and DS Storage Manager. When adding an ESS family device for logical configuration, the device type should be "ess", the IP address should be of the primary processor complex, and the username and password should be the same as the one used to log into the ESS Command Line Interface and ESS Specialist. Optionally, you can specify the secondary processor complex IP address in the Alternate IP field. When

adding an ESS Copy Services server, the device type should be "esscs", the IP address should be of the ESS Copy Services server, and the username and password should be the one used to log into the ESS Copy Services interface. Note that an ESS Copy Services server cannot be added without also adding the associated ESS logical configuration information. However an ESS can be added for logical configuration without adding a Copy Services server. After you have finished adding the configuration information, click **Next**.

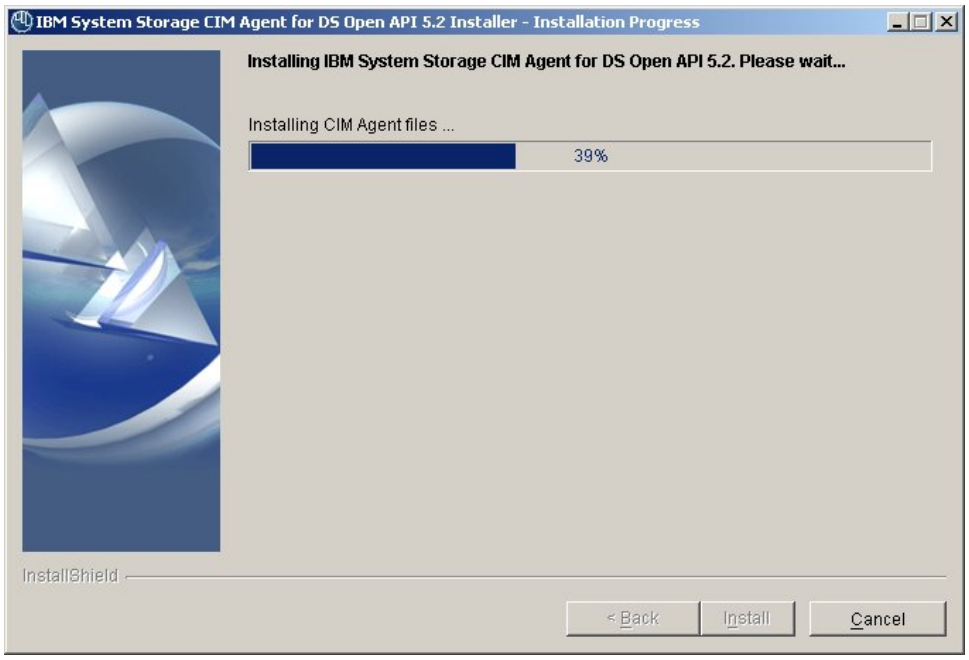


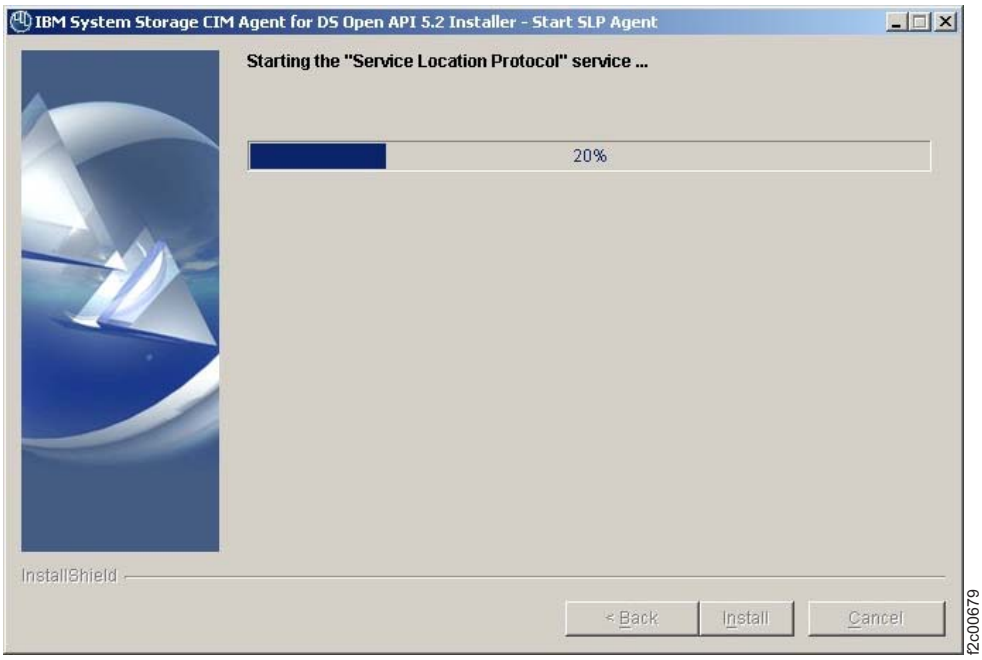
13. The Installation Preview window opens. Click **Install** to confirm the installation location and file size. You can click **Cancel** to exit the installation wizard or go back to the previous window by clicking **Back**.

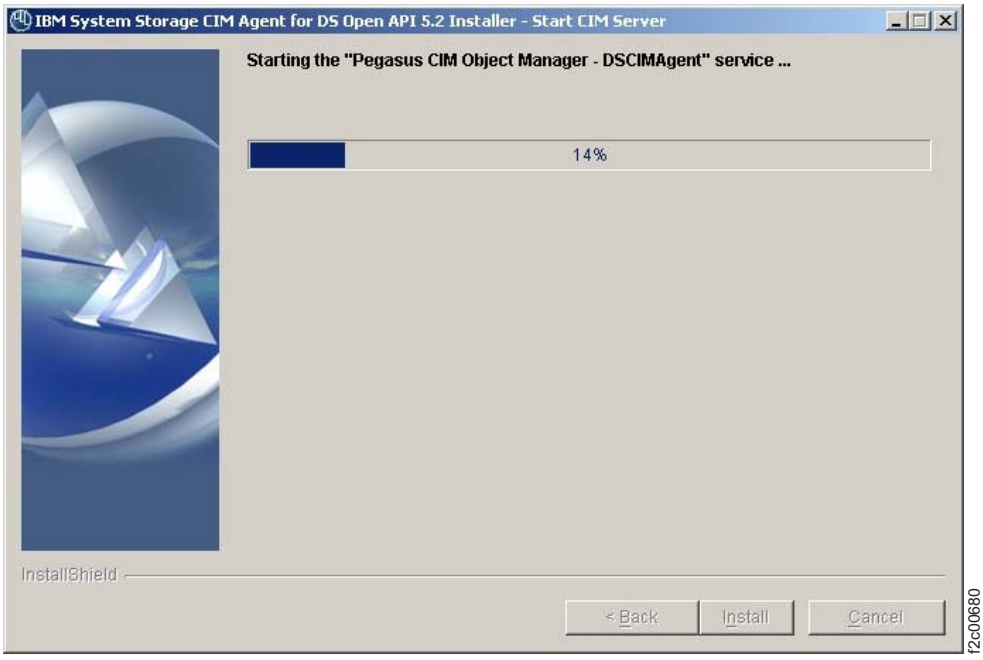


14. The Installation Progress window indicates how much of the installation has been completed. Installation usually takes 3 - 10 minutes depending on the configuration of your machine. The installation installs the CIM agent files, starts the Service Location Protocol (SLP) service, and starts the Pegasus CIM Object Manager – DSCIMAgent service. You can click **Cancel** to exit the installation wizard.

    Note: If you click **Cancel**, a pop-up window opens asking you to confirm the cancellation of the installation wizard: "Cancel the current operation? **Yes** **No**". Be aware that if you confirm the cancellation by clicking Yes, the information you entered or selected in previous windows is not saved. You must start the installation again from the first step.

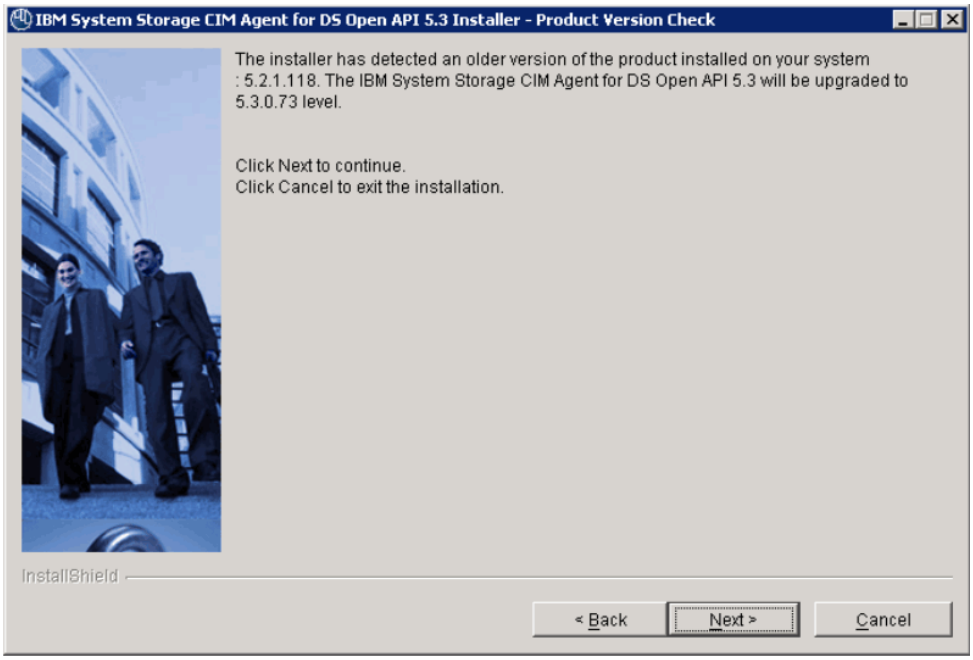






15. When the Installation Progress window closes, the **Finish** window opens. Click **Finish** to exit the installation wizard.

    Note: Before proceeding, you might want to review the log file for any possible error messages. The log file is located in <*dest-path*> \log\install.log, where <*dest-path*> is the destination directory where the CIM agent for Windows is installed. The default path is c:\Program Files\IBM\dsagent. The install.log contains a trace of the installation actions.



16. Exit the LaunchPad program by clicking **Exit** on the LaunchPad window. If you have not done so already, continue with the post installation tasks for the CIM agent using the instructions in the following sections.

    Note: Ordinarily, you do not need to restart your system during or after the installation of the CIM agent. However, the installation wizard might determine that a restart is necessary. Restart your system if required. After you restart the system, the installation wizard continues with the installation.

Installing the CIM agent on Windows in unattended (silent) mode

This section includes the steps to install the CIM agent in your Windows environment using the unattended (silent) mode.

You must satisfy all prerequisites before you begin the CIM agent installation.

The unattended (silent) install option allows you to run installation unattended. Use this method of installation to customize a response file and issue a command from a command prompt window. The response file is a template on the CIM agent CD. You can also create a standard response file to ensure that the product is installed consistently on multiple systems. After the completion of the installation, you must verify the CIM agent installation.

1. Log on as local administrator user.
2. Insert the CIM agent CD.
3. Locate the response file (named *responsefile_template.txt*) on your CIM agent CD.
4. Using Windows Explorer or a command prompt, copy the response file to your hard drive.
5. Customize the responsefile file with your parameters as follows:

- If you do not want to use the default value, remove the # character from the beginning of the line. Change the default value to the value that you want for that option. You *must* enclose all values in double quotation marks (" ").
- The <*-G licenseAccepted*> option defines license agreement verification. The default value is false. Uncomment this option and set it to true only after you have read the product License Agreement. The License Agreement can be found on the installation media. For instance, the following two files should be reviewed by English-speaking users:

  ```
  <CD_ROOT>/<OS-NAME>/license/LI_en
  <CD_ROOT>/<OS-NAME>/license/LA_en
  ```

  Where <CD_ROOT> is the root of the CD image or the root of the unpackaged installation media.
- The <*-P product.installLocation*> option defines the default directory where the product will be installed. To use another destination directory, remove the # character from the corresponding line and replace this default directory with the directory you want.
- If an instance of the IBM System Storage CIM Agent for DS 5.1 release is already installed on the target machine, the option <*-W checkPreviousVersion.migrateConfiguration*> specifies if the configured CIM users and devices will be migrated into the newly installed configuration. The default value is true. In order not to migrate the old configuration, remove the # character from the corresponding line and set the value to false.
- The <*-G useExistingSlp*> option specifies if you want the CIM agent to use the Service Location Protocol that is already installed into the system. The default value is no.
- The <*-W serverCommunicationConfig.communicationProtocol*> option specifies the CIM agent server communication protocol. If you want to change the default value during installation, remove the # character from the corresponding line and change the default server communication protocol ("both") to HTTP or HTTPS protocol values.
- The <*-W serverCommunicationConfig.httpsPort*> option specifies the port number that the CIM server will use for secure HTTPS transport. This value must not conflict with existing port assignments on the system. If you are unsure of which values to use, ask your administrator. To check ports in use, use the "netstat -an" command. The default value is "5989"
- The <*-W serverCommunicationConfig.httpPort*> option specifies the port number that the CIM server will use for secure HTTP transport. This value must not conflict with existing port assignments on the system. If you are unsure of which values to use, ask your administrator. To check ports in use, use the "netstat -an" command. The default value is "5988".
- With the <*-G deviceConfigurationParameters*> option you can have the installer optionally configure one or more managed devices ("ds", "ess" or "esscs") by adding the necessary information in the following format:

  For DS device:

  ```
  -G deviceConfigurationParameters=ds;IP Address;Alternate IP;UserName;Password
  ```

  For an ESS device:

  ```
  -G deviceConfigurationParameters1=ess;IP Address;Alternate IP;UserName;Password
  ```

  For an ESSCS device:

  ```
  -G deviceConfigurationParameters2=esscs;IP Address;Alternate IP;UserName;Password
  ```

- The <-W *serverConfigParams.userName*> and <-W *serverConfigParams.password*> options define the CIM user name and password to be configured by the installer. By default, only ″superuser″ CIM user is created.

6. Save the modifications to the **responsefile** file. Save the file *without* a file extension such as .txt.
7. From a command prompt, type the following command:

   ```
   <CD drive path>\W2003\install -options <response file path>\responsefile
   ```

   where <*CD drive path*> is the path of your CD-ROM drive. <*response file path*> is the path of the responsefile file that you copied in step 4 on page 62 and customized in step 5 on page 62.
8. During the installation you will see dotted lines scrolling across the screen. When the installation program ends, you see the cursor.
9. Check for installation errors in the install.log file. After all the prerequisite checks have been performed, the log file is copied to the <dest-path>\log directory. This file can be found in the <dest-path >\log\ directory. This file is initially created in the system temporary file under the subdirectory **cimagent**. The following is an example of an install.log file:

```
(Apr 12, 2006 3:55:11 PM), Found "Service Location Protocol" active installed by the IBM System Storage CIM Agent
for DS Open API 5.3
(Apr 12, 2006 3:55:16 PM), IBM System Storage CIM Agent for DS Open API 5.3 will be installed in the following
location:
C:\Program Files\IBM\dsagent
- W checkPreviousVersion.migrateConfiguration = false
with the following parameters:
Communication Protocol: HTTPS and HTTP
HTTPS Port value: 5989
HTTP Port value: 5988
(Apr 12, 2006 3:55:16 PM), Verifying locked files. Please wait...
(Apr 12, 2006 3:55:16 PM), No locked files were detected.
(Apr 12, 2006 3:55:16 PM), No configuration files to save/restore
(Apr 12, 2006 3:55:17 PM), CIM agent for the IBM Total Storage DS Open API not installed.
(Apr 12, 2006 3:55:28 PM), Installing provider libraries ...
(Apr 12, 2006 3:55:29 PM), Installing MOF files ...
(Apr 12, 2006 3:55:57 PM), Installing CIM Agent files ...
(Apr 12, 2006 3:56:15 PM), Installing OpenSLP files ...
(Apr 12, 2006 3:56:15 PM), Installing OpenSSL files ...
(Apr 12, 2006 3:56:17 PM), Installing Java files ...
(Apr 12, 2006 3:56:27 PM), The file C:\Program Files\IBM\dsagent\config\envConf.bat successfully updated.
(Apr 12, 2006 3:56:33 PM), Setting CIM Server configuration ...
(Apr 12, 2006 3:56:33 PM), Command to be executed : C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ismp012
\cimconfig.bat -s enableHttpConnection=true -p
(Apr 12, 2006 3:56:36 PM), Command to be executed : C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ismp012
\cimconfig.bat -s enableHttpsConnection=true -p
(Apr 12, 2006 3:56:39 PM), Command to be executed : C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ismp012
\cimconfig.bat -s httpPort=5988 -p
(Apr 12, 2006 3:56:41 PM), Command to be executed : C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ismp012
\cimconfig.bat -s httpsPort=5989 -p
(Apr 12, 2006 3:56:43 PM), The CIM Server configuration successfully set.
(Apr 12, 2006 3:56:43 PM), Generating certificates ...
(Apr 12, 2006 3:56:43 PM), Command to be executed : "C:\Program Files\IBM\dsagent\bin\mkcertificate.bat" certname
(Apr 12, 2006 3:56:44 PM), The certificates were successfully generated.
(Apr 12, 2006 3:56:44 PM), Enabling SSL communication ...
(Apr 12, 2006 3:56:44 PM), Command to be executed : C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ismp012
\cimconfig.bat -s sslKeyFilePath=C:\Program Files\IBM\dsagent\certificate\certname.key -p
(Apr 12, 2006 3:56:46 PM), Command to be executed : C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ismp012
\cimconfig.bat -s sslCertificateFilePath=C:\Program Files\IBM\dsagent\certificate\certname.cert -p
(Apr 12, 2006 3:56:49 PM), SSL communication enabled.
(Apr 12, 2006 3:56:49 PM), Installing "Service Location Protocol" service ...
(Apr 12, 2006 3:56:49 PM), Command to be executed:
"C:\Program Files\IBM\dsagent\slp/bin/slpd" -install
(Apr 12, 2006 3:56:52 PM), The "Service Location Protocol" service successfully installed.
(Apr 12, 2006 3:56:52 PM), Installing "IBM System Storage CIM Agent for DS Open API 5.3 Pegasus Server" service ...
file:///C|/CMVCDiana/api/api_ereview/Comments/release1/cmm_bk11.htm (11 of 24)4/19/2006 8:46:03 AM
CIM agent for Windows
(Apr 12, 2006 3:56:52 PM), Command to be executed:
"C:\Program Files\IBM\dsagent\pegasus\bin\cimserver.exe" -install DSCIMAgent
(Apr 12, 2006 3:56:56 PM), The "IBM System Storage CIM Agent for DS Open API 5.3 Pegasus Server" service
successfully installed.
(Apr 12, 2006 3:56:57 PM), Setting Java Runtime Environment for the uninstaller ...
(Apr 12, 2006 3:57:07 PM), Creating Windows registry entries ...
(Apr 12, 2006 3:57:07 PM), Windows registry entries successfully created.
(Apr 12, 2006 3:57:07 PM), Starting the "Service Location Protocol" service ...
(Apr 12, 2006 3:57:07 PM), Command to be executed:
net start "slpd"
(Apr 12, 2006 3:57:10 PM), Return code (rc) = 0
(Apr 12, 2006 3:57:13 PM), The "Service Location Protocol" service successfully started.
(Apr 12, 2006 3:57:13 PM), Starting the "IBM System Storage CIM Agent for DS Open API 5.3 Pegasus Server"
service ...
(Apr 12, 2006 3:57:13 PM), Command to be executed:
net start "DSCIMAgent"
(Apr 12, 2006 3:57:17 PM), Return code (rc) = 0
(Apr 12, 2006 3:57:47 PM), The "IBM System Storage CIM Agent for DS Open API 5.3 Pegasus Server" service
successfully started.
(Apr 12, 2006 3:57:48 PM), INSTSUCC: IBM System Storage CIM Agent for DS Open API 5.3 has been successfully
installed.
```

10. Close the command prompt window by entering a command, for example **exit**. Continue with the post-installation tasks for the CIM agent using the instructions in the following sections. You can also continue the post installation tasks using the following option:
    a. Open the LaunchPad from the command prompt window by typing `LaunchPad`.
    b. Click **Post installation tasks** on the LaunchPad window. Continue with the post installation tasks for the CIM agent by following the instructions in this file.

Verifying the CIM agent installation on Windows

This task verifies that your CIM agent is installed correctly on your Windows operating system.

Steps:

Perform the following steps to verify your CIM agent installation on your Windows operating system:

1. Verify the installation of the Service Location Protocol (SLP).
   a. Verify that SLP is started. Right-click **My Computer -> Manage -> Services and Applications -> Services**.
   b. Find **Service Location Protocol** in the Services window list. For this component, the Status column is marked **Started** and the Startup Type column is marked **Manual**. If those conditions are not met, right-click on the SLP and select **Start** from the pop-up menu. Wait for the Status column to be changed to **Started**.
   c. Do not close the Services window because you will also use it to verify the CIM object manager (CIMOM) service.
2. Verify the installation of the CIM agent.
   a. Verify that the CIMOM service is started. If you closed the Services window, right-click **My Computer -> Manage -> Services and Applications -> Services**.
   b. Find **IBM System Storage CIM Agent for DS Open API 5.3 Pegasus Server** in the Services window list. For this component, the Status column is marked **Started** and the Startup Type column is marked **Automatic**. If those two conditions are not met, right-click the **IBM System Storage CIM Agent for DS Open API 5.3 Pegasus Server** and select **Start** from the pop-up menu. Wait for the Status column to change to **Started**.
   c. Close the Services window.
   d. Close the Administrative Tools window.

If you are able to perform all of the verification tasks successfully, the DS CIM agent has been successfully installed on your Windows system. Next, perform the required configuration tasks.

Configuring the CIM agent for Windows

This task configures the CIM agent after it has been successfully installed. This section repeats the instructions in the Post Installation Tasks option that you open from the LaunchPad window.

Perform the following steps to configure the CIM agent:

1. Ping each ESS and DS that the CIM agent will manage by typing the following command:
   a. Open a command prompt window and issue a **ping** command; for example:
      `ping 9.11.111.111`

      where 9.11.111.111 is and ESS processor complex or DS master console IP address
   b. Check that you can see reply statistics from the IP address. The following is example output:

```
Pinging 9.11.111.111 with 64 bytes of data:

64 bytes from 9.186.10.119: icmp_seq=1 ttl=64 time=2.09 ms
64 bytes from 9.186.10.119: icmp_seq=2 ttl=64 time=1.02 ms
64 bytes from 9.186.10.119: icmp_seq=3 ttl=64 time=1.01 ms
64 bytes from 9.186.10.119: icmp_seq=4 ttl=64 time=1.02 ms
```

If you see other messages that indicate that the request has timed out, see your Network Administrator for help on establishing network connectivity before you configure storage units.

2. Type the following command to configure the CIM agent for each ESS or DS server that the CIM agent can access.

   `dscimcli mkdev <ip> -type <type> -user <user> -password <password>`

   ip For an ESS configuration server, this is the IP address of the primary processor card.

   For an ESS copy services server, this is the IP address of the primary copy services server.

   For a DS server, this is the IP address of the primary hardware or software master console (HMC/SMC).

   type
   For an ESS configuration server, this is *ess*.

   For an ESS copy services server, this is *esscs*.

   For DS, this is *ds*.

   user/password
   For an ESS configuration server, this is the specialist or ESSCLI user name and password.

   For an ESS copy services server, this is the specialist or ESS copy services server user name and password

   For a DS server, this is the storage manager GUI or DSCLI user name and password

3. After you have defined all of the ESS and DS servers, type the following command to verify that the devices were correctly added and have connected successfully:

   `dscimcli lsdev -l`

   The following is example output:

```
Type   IP IP2          user name  Storage Image    Status     Code Level  Min Codelevel
=====  =============== ========= ==============   =======    =========== =============
DS     9.11.111.111 -  admin     IBM.2107-1234567 successful 5.1.0.309   5.1.0.309
```

   Note: Because the CIM agent periodically collects and caches some pieces of information from the defined storage units, the CIM agent might periodically take longer to respond to requests, including immediately after adding a new storage unit.

4. Configure the CIMOM for each user that you want to have authority to use the CIMOM by running the CIMOM configuration program.

   During the CIM agent installation, the default user name to access the CIM agent CIMOM is created. The default user name is “superuser” with a default password of “passw0rd”. You must use the default user name and password when you use the **mkuser** command for the first time after installation. After

you have added other users, you can initiate the **mkuser** command using a user name that you defined instead of using the default.

a. Start the CIM agent, if it is not started, by typing the following command:

```
# startagent
```

b. Type the following command:

```
# dscimcli mkuser -user cimuser -password cimpass
```

The following is example output:

```
User created.
```

Restriction: You cannot delete or modify the current user using the **mkuser** command.

c. You can change the default password for "superuser" by starting the **mkuser** command for a user that you added. Issue the following command to change the password:

```
>>> dscimcli chuser superuser -password passw0rd -newpassword <newpassword>
```

where *newpassword* is the new password for the superuser.

d. You can delete the superuser by issuing the following command:

```
>>>rmuser superuser
```

e. Type the **exit** command to exit the CIMOM configuration program.

If you were able to perform all of the configuring tasks successfully, the CIM agent has been successfully installed and configured on your Windows system.

Verifying the CIM agent connection on Windows

During this task, the CIM agent software connects to the storage unit that you identified in the configuration task.

1. Verify that you have network connectivity to the ESS or DS from the system where the CIM agent is installed. To do this, perform the following steps:
   a. Open a command prompt window.
   b. Issue a **ping** command to the ESS; for example:

```
ping 9.11.111.111
```

   where 9.11.111.111 is the ESS processor complex or DS master console IP address

   c. Check that you can see reply statistics from the ESS IP address. The following is example output:

```
Pinging 9.11.111.111 with 32 bytes of data:

Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
Reply from 9.11.111.111: bytes=32 time<10ms TTL=255
```

If you see other messages that indicate that the request has timed out, see your Network Administrator for help on establishing network connectivity from the system where the CIM agent is installed.

2. Verify that the ESS CLI is operational and can connect to the storage unit. To do this, perform the following steps:
   a. Open a command prompt window.
   b. Issue the following command:

      ```
      dscimcli lsdev -l
      ```

      The following is an example of a successful response:

      ```
      Thu Oct 09 11:22:28 PDT 2003 IBM ESSCLI 2.4.0.236
      Server Mode Mfg WWN CodeEC Cache NVS Racks
      ---------- ----- --- ---------------- --------- ----- ----- -----
      2105.22232 800 013 5005076300C09470 2.4.0.236 8GB 2GB
      ```

   Note: In some cases the ESS CLI does not work correctly unless the system has been restarted following the new installation of the ESS CLI.
3. Using the Windows Services Facility, verify that the SLP is active by right-clicking **My Computer -> Manage -> Services and Applications -> Services**.
   a. Find the Service Location Protocol (SLP) in the Name column.

      For this component, the Status column is marked **Started** and the Startup Type column is marked **Manual**. If either of those conditions are not met, right click on **Service Location Protocol** and click **Start** from the pop-up menu. Wait for the Status to change to **Started**
   b. Do not close the Services window, because you use it in the next step to verify that the CIMOM is started.
4. Verify that the CIMOM is active by finding **CIM Object Manager - DS Open API** in the Name column of the Services window.

   For this component, if the Status column is not marked **Started**, right click on **CIM Object Manager - DS Open API** and click **Start** from the pop-up menu. Wait for the Status to change to **Started**.
5. Verify CIMOM registration with SLP by selecting **Start-> Programs-> CIM agent for IBM System Storage DS Open API-> Check CIMOM Registration**. The window closes when you press any key, as instructed in the output:

   ```
   service: wbem:http://tpc035/ 5988, 65535
   press any key to continue...
   ```

   Note: If the verification of the CIMOM registration is not successful, stop and restart the SLP and CIMOM services.

This completes the verification of the connection to the ESS.

Removing the CIM agent from Windows

This optional task provides instructions for removing the CIM agent from your Windows operating system.

Steps:

Perform the following steps to remove the CIM agent from your Windows operating system:

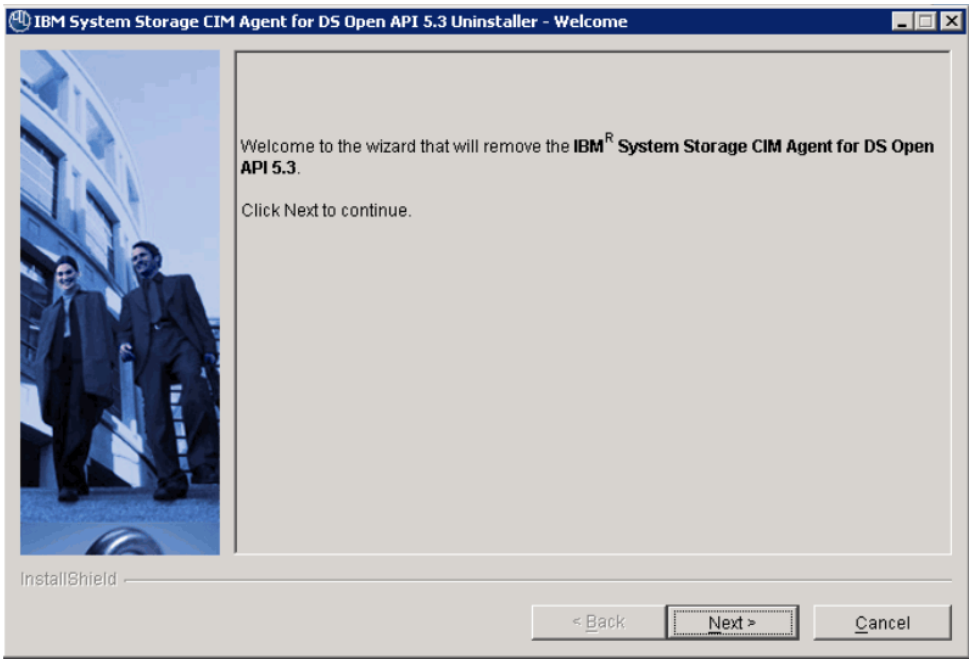
1. Log on to the system where the CIM agent is installed. Log on with a user name that is a local system administrator.

2. Stop the CIMOM and the SLP services if they are started.
   a. Click **Start -> Settings -> Control Panel**. In the Control Panel window, double-click on the **Administrative Tools** icon and then double-click the **Services** icon. The Services window opens.
   b. Stop the SLP service if it has already been installed by the CIM agent installer:
      1) In the Services window, scroll to **IBM System Storage CIM Agent for DS Open API 5.3**. Click on the service to select it.
      2) If the Status column shows Started, right-click the service, and then click **Stop** on the menu.
   c. Stop the SLP service:

      Note: You must be careful if you have other applications that use SLP service. In this case, you must stop these applications before you stop SLP service, because the SLP service is deleted during the removal process. You must also stop the configuration utilities for the CIM agent, if they are running.

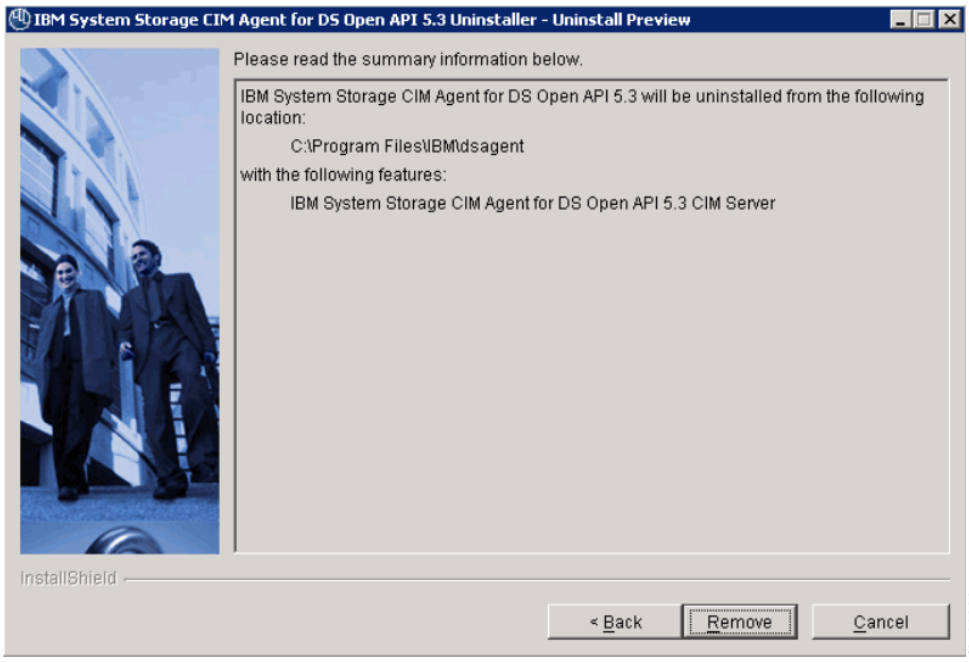
      1) In the Services window, scroll to **Service Location Protocol**. Click on this service to select it.
      2) If it is running (the Status column shows Started), right-click the service, and then click **Stop** on the menu.

         (If you did not stop the CIM Object Manager service, the system now asks if you want to stop the CIM Object Manager service. Because CIM Object Manager service is dependent on the Service Location Protocol service which you just stopped, you must click **Yes** to stop the CIM Object Manager service.)
      3) Wait for the services to stop.
      4) Close the Services window.
      5) Close the Administrative Tools window.
3. Use the Windows Add/Remove Programs facility to remove the CIM agent and the Service Location Protocol components.
   a. From the Windows menu bar, click **Start -> Settings -> Control Panel**. Double-click **Add/Remove Programs**.
   b. Click **IBM System Storage CIM Agent for DS Open API 5.3** from the list of currently installed programs and click **Remove** to remove the product.
4. The Welcome window for the Uninstaller opens. Click **Next** to continue or click **Cancel** to stop the removal of the CIM agent.



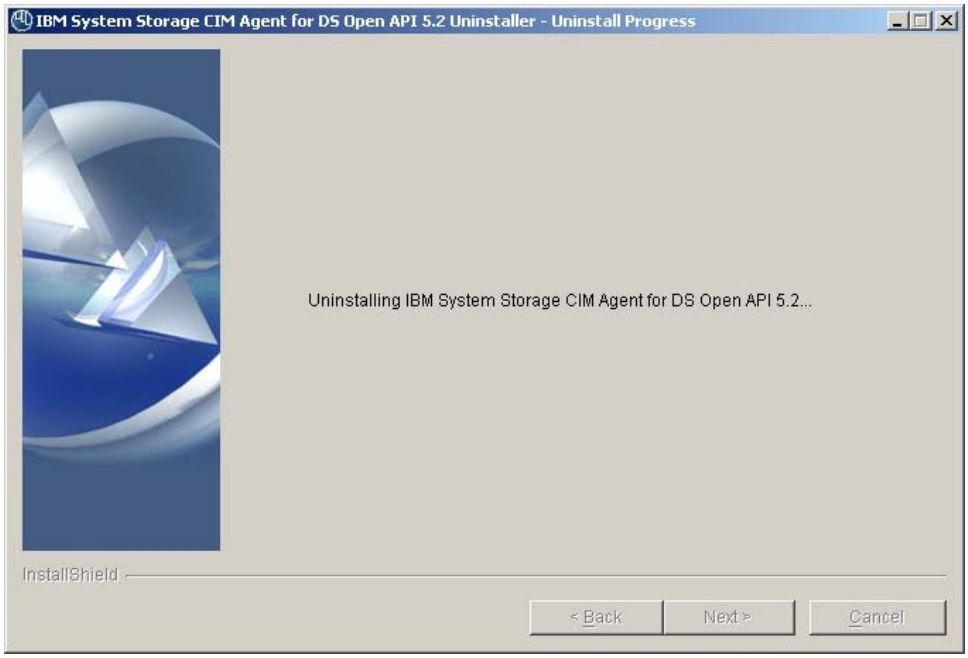
f2c00682

5. The Uninstall Preview window opens. Click **Remove** to confirm the location that the program will be removed from and the features to be removed. You can click **Cancel** to exit the wizard and stop the removal of the CIM agent or go back to the previous window by clicking **Back**.

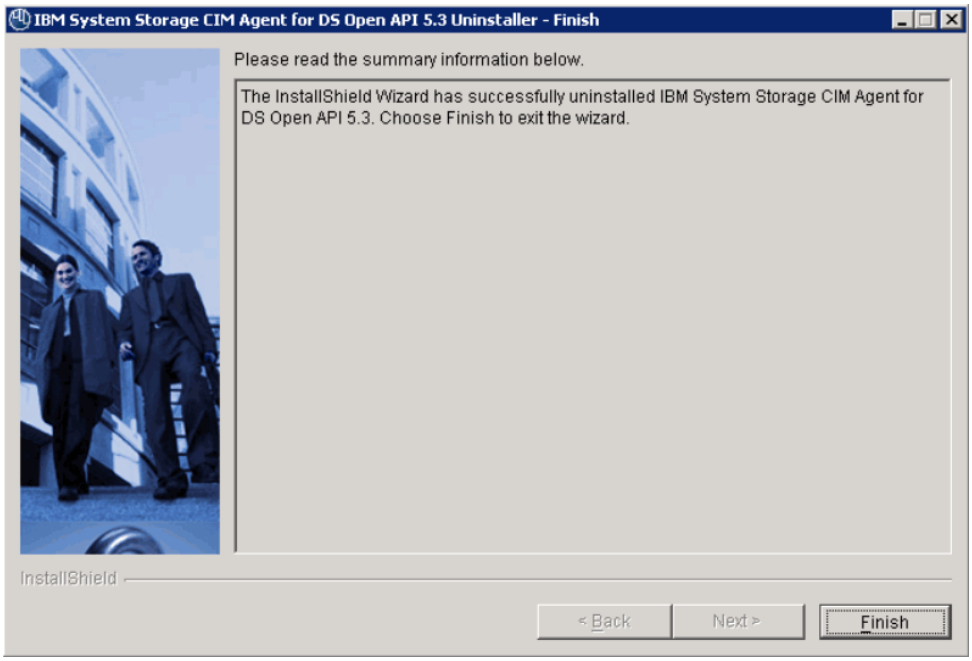


f2c00683

6. The Uninstallation Progress window opens. Wait for the program to remove the CIM agent product.



7. The Finish window for the Uninstaller opens. This window indicates the result of the removal process (successful or failed). Click **Finish** to complete the removal process and exit the wizard.



   If the program could not remove some information from the system, the Restart window opens. You will need to restart your system. At the restart, the previously locked files are released and automatically deleted.
8. Close the Add/Remove Programs window.
9. Restart the system (now or later) to complete the removal process.

Perform the following steps to complete the removal process:

1. If the system has not been restarted since CIM agent was removed, do so now.
2. Log on as a local administrator.
3. Remove other files and folders for CIM agent, as the removal process does not delete configuration files, logs, and similar files that were created during or after the installation process. The files are located in the destination path where you installed the CIM agent. An example of the default destination path is: `C:\Program Files\IBM\cimagent`. Remove the cimagent folder and all of its contents (especially if you plan to reinstall CIM agent).

   Note: If you want to keep the old configuration files, save them in another location on your system to restore them later before removing them from the installation destination path.
4. Perform other cleanup tasks:
   a. Close both the Services and the Add/Remove Program windows if you have not already done so.
   b. Empty your Windows Recycle Bin to reclaim the disk space that was made available during the removal process.

Chapter 5. CIM agent for HMC

Beginning with DS8000 Release 2.4, the CIM Agent is pre-installed on the hardware management console (HMC). This chapter includes an overview of the setup process and instructions for enabling and configuring the CIM agent on the DS8000 HMC.

The DS8000 can be managed either by the CIM agent that is bundled with the HMC or with a separately installed CIM agent. The HMC CIM agent has the following limitations:

- The CIM agent is initially disabled on the HMC and must be enabled through the WebSM management console before it can be used.
- The HMC CIM agent can only support DS8000 devices that are managed by that HMC. This CIM agent is not able to manage any ESS 800 or DS6000 devices, or any DS8000 devices that are managed by a different HMC.
- The HMC CIM agent must use secure connections over port 6989.
- The configuration is performed remotely. Therefore, you must download and install the dscimcli utility on an additional machine.

Installation overview for HMC

This section provides an overview of the installation and configuration of the CIM agent on the HMC.

Perform the following list of installation and configuration tasks:

1. Before you enable the CIM agent on the HMC, verify the hardware and software requirements.
2. Download and install the dscimcli utility.
3. Enable the CIM agent using the HMC graphical user interface.
4. Configure the CIM agent for HMC. If you add more than one DS device, repeat this step for each device.
5. Set up the user environment. After installation is complete, you must issue two export commands to allow the administrator to perform CIM agent management commands.
6. Verify the connection to your storage unit.

Installing and configuring the dscimcli utility

This section includes the steps to install and configure the dscimcli utility.

The dscimcli utility, which configures the CIM agent, is available from the DS CIM agent Web site as part of the DS CIM agent installation bundle, and also as a separate installation bundle. In order to configure and manage a CIM agent that is running on a DS8000 HMC, you must download and install the dscimcli utility on a separate server, for example the server that is running your client application like TPC or your laptop. dscimcli is a small utility that runs on the same platforms that the proxy CIM agent runs on, but does not consume nearly as much memory or CPU as the full CIM agent installation. So the separate dscimcli installation bundle should be able to run on any reasonable server or laptop. To install from the separate bundle, perform these steps:

1. Download and extract the dscimcli .zip file onto your hard drive.
2. The top-level directories of the extracted contents represent the different operating systems. Set your DSAGENT_HOME environment variable to one of those directories depending on your platform (AIX, LINUX_RHEL3, LINUX_SLES9, or W2003). For example, in Linux you might set:

   ```
   export DSAGENT_HOME=/work/dscimcli/LINUX_SLES9
   ```

   On Windows, the syntax is set:

   ```
   Set DSAGENT_HOME=C:\Documents and Settings\Administrator\Desktop\dscimcli\W2003
   ```
3. Add the bin directory of the DSAGENT_HOME to your path. For example, on a Linux system, you can set the following path:

   ```
   Set PATH=%PATH%;%DSAGENT_HOME%\bin
   ```

   On Windows, the syntax is set:

   ```
   PATH=%PATH%;%DSAGENT_HOME%\bin
   ```

Regardless of which means that you use to obtain the utility, you must specify the server location of the HMC when executing dscimcli commands using one of two mechanisms:

command line option
The server location can be placed onto the command line for each invocation of dscimcli with the `-s` option. For example:

```
dscimcli -s https://<hmc ip>:6989 lsconfig
```

where `<hmc ip>` is the HMC IP address.

environment variable
Instead of supplying the server location each time on the command line, you can set the DSCIM_SERVER environment variable. For example:

```
export DSCIM_SERVER=https://<hmc ip>:6989 dscimcli lsconfig
```

where `<hmc ip>` is the HMC IP address.

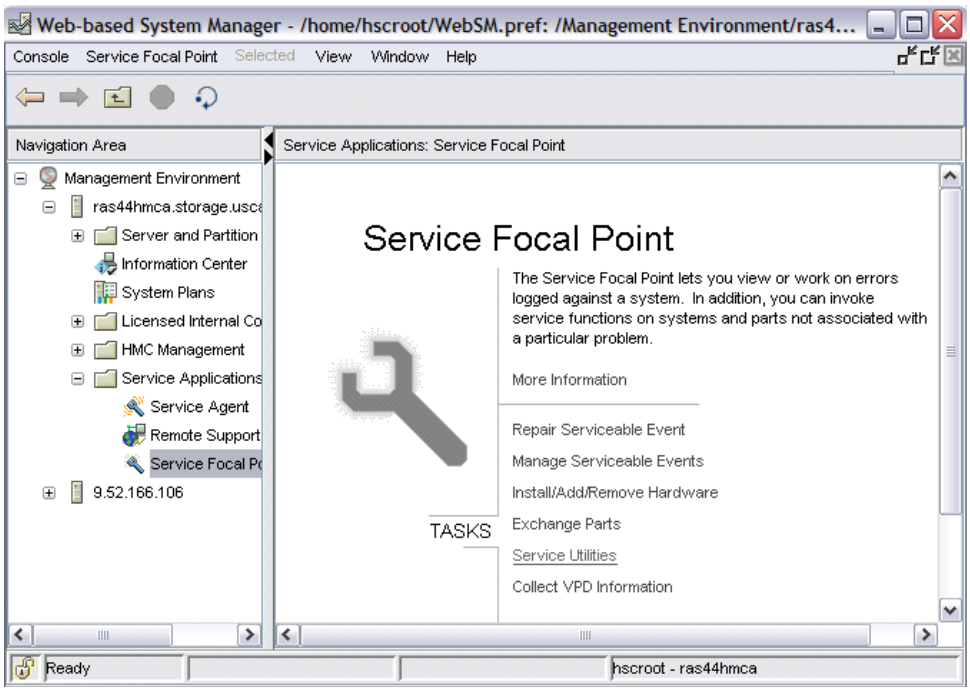
Enabling the CIM agent on the HMC

This section includes the steps to enable the CIM agent on the HMC.

Perform the following steps to enable the HMC CIM agent:

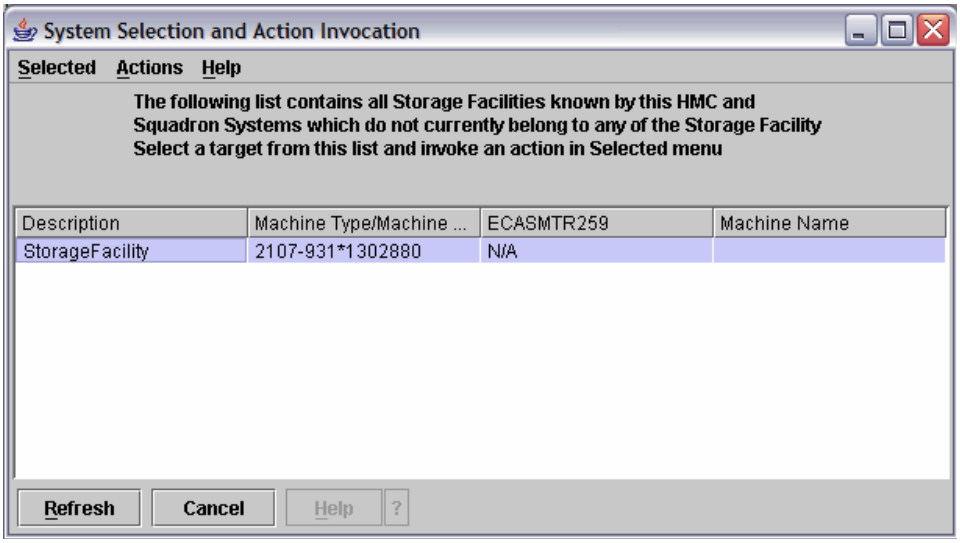
1. Use the WebSM management console to navigate to **Service Applications**, and then select **Service Focal Point**.

   You will see the following screen:

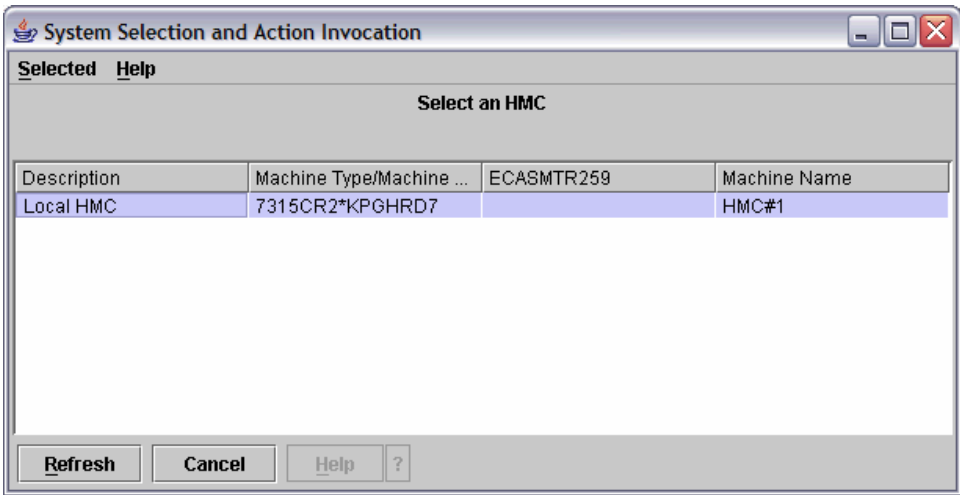


In the Service Focal Point window, select Service Utilities.

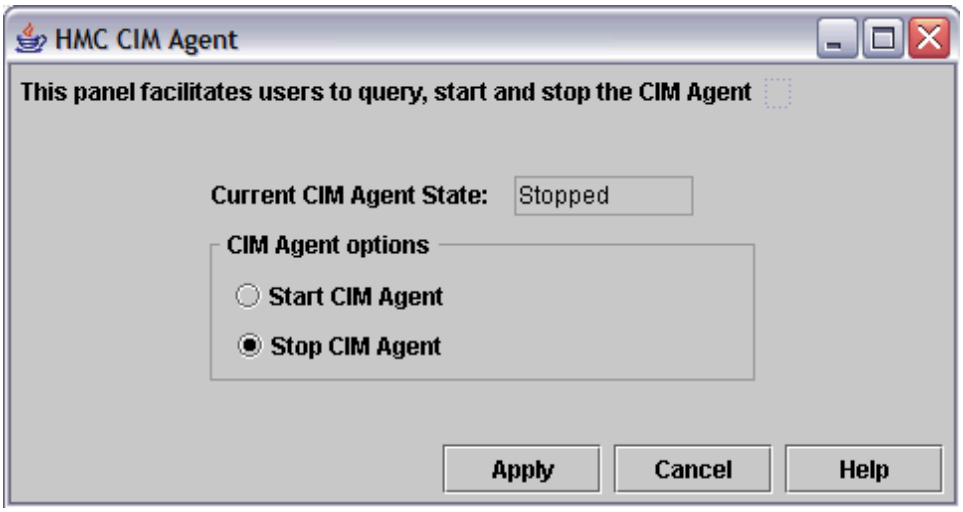
2. Highlight the storage facility. On the Selected menu, select **Get HMCs**.



3. Highlight the HMC. On the Selected menu, select **Start/Stop CIM**.



4. The HMC CIM agent panel shows the current state of the CIM agent. You can change the status by selecting the **Start CIM Agent** option and clicking **Apply**.



Configuring the CIM agent for HMC

This section provides the steps to configure storage units and user accounts for the CIM agent after it has been successfully enabled.

Perform the following steps to configure the storage unit and user accounts for the CIM agent:

1. Verify that the HMC is managing the DS8000 that you want to add to the CIM agent.
2. Type the following command (all on one line) to configure th CIM agent for the DS8000 server that the CIM agent can access:

   ```
   dscimcli -s https://<hmc ip>:6989 mkdev <hmc ip> -type ds [ -ip2 <hmc2 ip> ]
   -user <user> -password <password>
   ```

   where:

   <hmc ip>
   is the IP address of the HMC.

<hmc2 ip>
is the IP address of the secondary HMC (optional).

<user> is the user name that is used to log into the storage manager on the HMC.

<password>
is the password that is used to log into the storage manager on the HMC.

Verifying the CIM agent connection

This section provides the steps to verify that the CIM agent software connects to the storage unit that you identified in the configuration task.

Perform the following steps to verify storage unit and CIM connectivity:

1. Verify the CIM agent configuration and connectivity by issuing the following command:

   ```
   dscimcli -s https://<hmc>:6989 lsdev -l
   ```

   The following is an example of the output:

   ```
   Type IP IP2 user name Storage Image Status Code Level Min Codelevel
   ===== ============== ========= ============== ======= =========== =============
   DS  9.1.11.11  admin  IBM.2107-123456  successful  5.1.0.309  5.1.0.309
   ```

   If the status is failed, there was a failure when the CIM agent attempted to communicate with the storage device. If the CIM agent was unable to communicate during mkdev, an error is returned immediately. If the device shows as failed in lsdev -l, it is likely that you added the device earlier and the communication is now failed. To ensure that your storage device's management interface is functioning, use DSCLI or DS Storage Manager to attempt to log into the device. If you are unable to connect via DSCLI or DS Storage Manager, there is likely an error in the storage device. If you are able to connect via the native interfaces, there is likely an error in the CIM agent. Contact your service representative for assistance.

2. Verify that the CIM agent has registered into SLP by issuing the following command:

   ```
   slptool findsrvs service:wbem
   ```

   The output is a list of CIM agent services in the following form:

   ```
   service:wbem:https://<HMC IP>:6989,<Timeout>
   ```

   where:

   <HMC IP>
   represents the IP address of the HMC.

   <Timeout>
   is the number of seconds that remain before the entry times out of SLP.

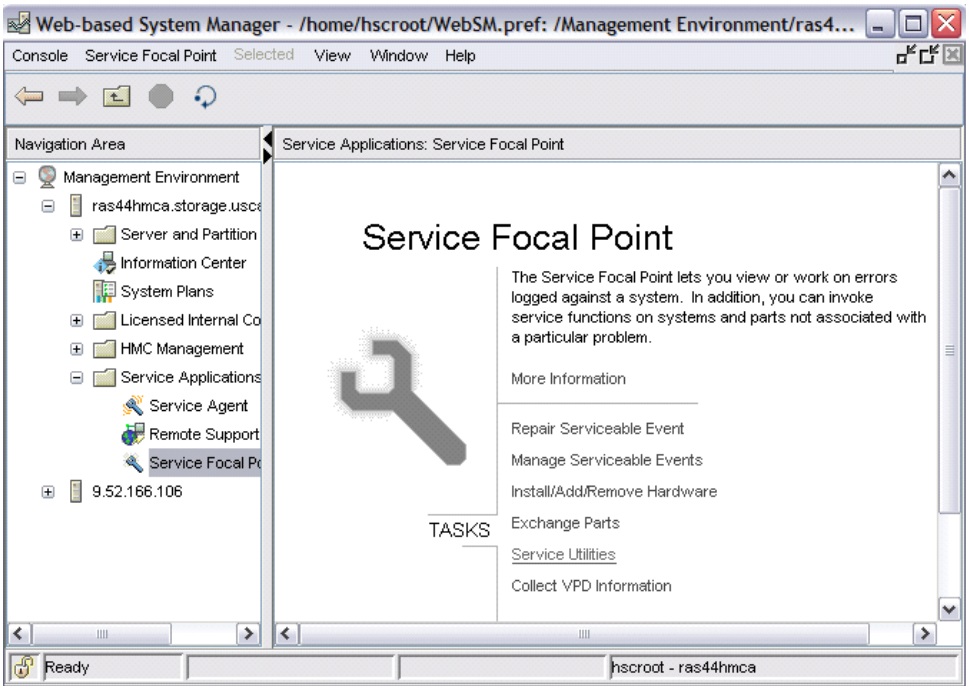
Disabling the CIM agent on the HMC

This section includes the steps to disable the CIM agent on the HMC.

Perform the following steps to disable the HMC CIM agent:

1. Use the WebSM management console to navigate to **Service Applications**, and then select **Service Focal Point**.

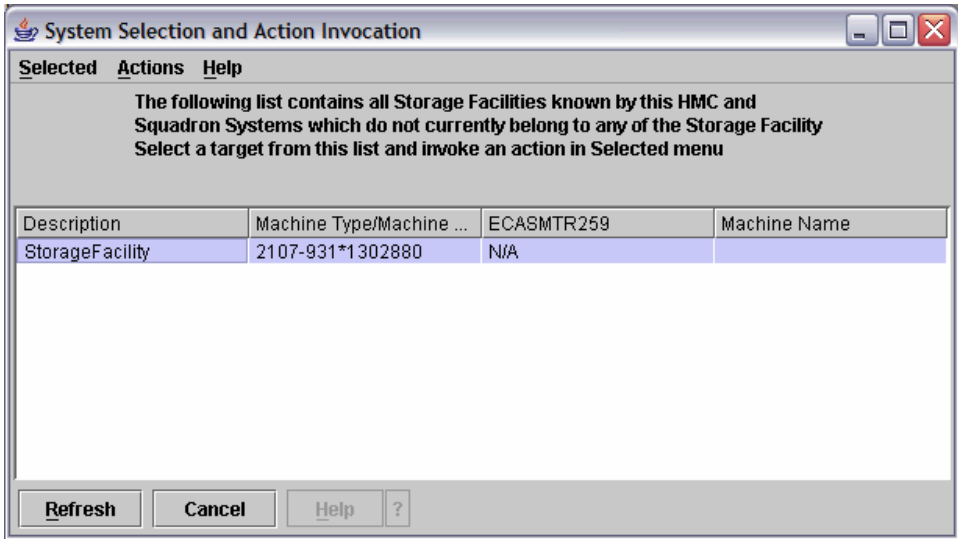
   You will see the following screen:



f2d00144

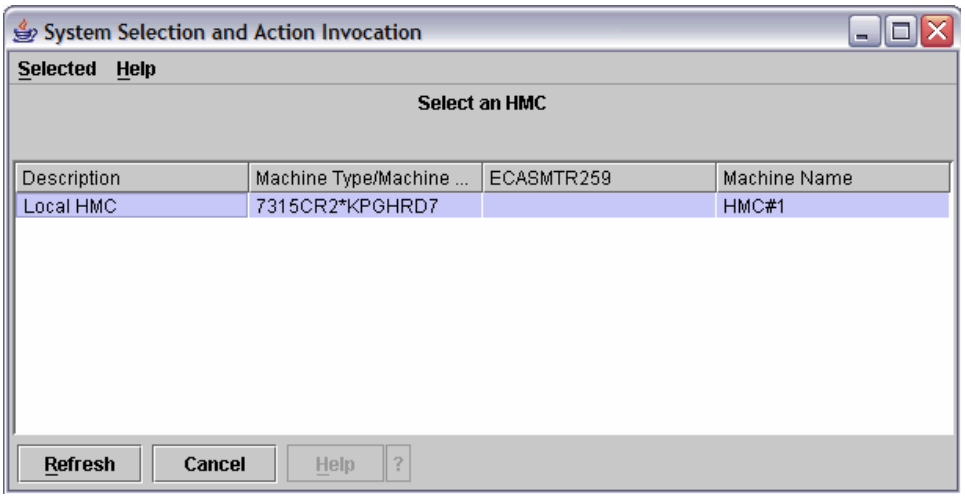
   In the Service Focal Point window, select **Service Utilities**.

2. Highlight the storage facility. On the Selected menu, select **Get HMCs**.

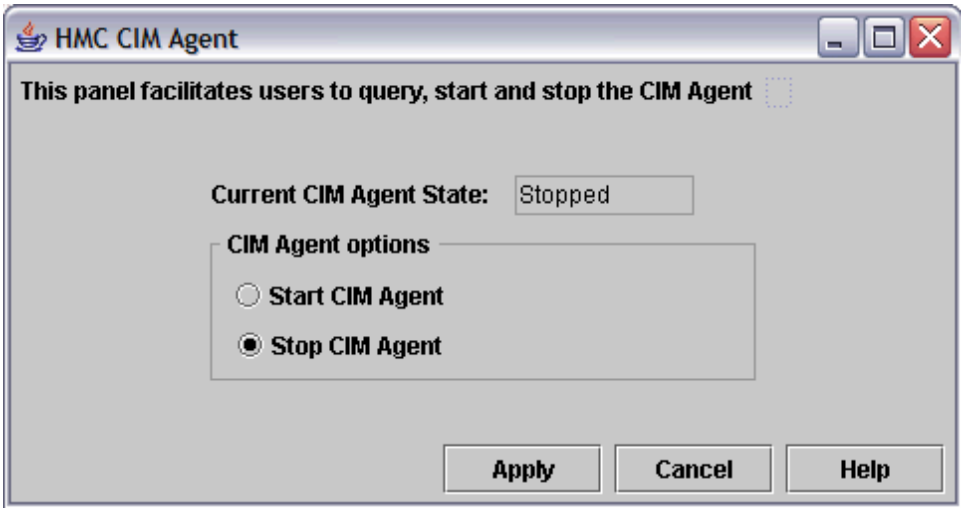


f2d00145

3. Highlight the HMC. On the Selected menu, select **Start/Stop CIM**.



4. The HMC CIM agent panel shows the current state of the CIM agent. You can change the status by selecting the **Stop CIM Agent** option and clicking **Apply**.



Chapter 6. CIM agent management commands

This chapter includes information about the commands that you use when you install and configure the CIM agent on a server or workstation running a Linux, AIX, or Windows 2003 operating system. This chapter also presents a complete character syntax of the programs, commands, flags, and values that you can use for each command. There is also a section that shows examples of commands and the output that results from issuing the command.

Overview of the CIM agent management commands

This section briefly introduces the CIM agent management commands and provides general guidelines for using the commands.

Before you use the commands, refer to the appropriate installation and configuration chapters for your operating system for information about how to install or configure and enable the CIM agent.

Invoking the CIM agent

You can invoke the CIM agent using single command-line invocation. You can invoke a command by including all of the relevant subcommands, parameters, and values on one command line.

Conventions used in this chapter

This section describes the notational conventions that are used in this chapter for the syntax diagrams.

Syntax diagrams

A syntax diagram uses symbols to represent the elements of a command and to specify the rules for using these elements. This section shows you how to read the syntax diagrams that represent the CIM agent commands. In doing so, it defines the symbols that represent the CIM agent command elements.

Main path line

Begins on the left with double arrowheads (>>) and ends on the right with two arrowheads facing each other (><). If a diagram is longer than one line, each line to be continued ends with a single arrowhead (>) and the next line begins with a single arrowhead. Read the diagrams from left-to-right, and top-to-bottom, along the main path line.

Keyword

Represents the name of a command, flag, parameter, or argument. A keyword is not in italics. Spell a keyword exactly as it is shown in the syntax diagram.

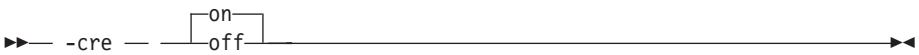
Required keywords

Indicates the parameters or arguments that you must specify for the command. Required keywords display on the main path line. Required keywords that cannot be used together are stacked vertically.

Optional keywords

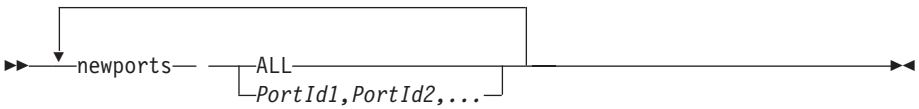
Indicates the parameters or arguments that you can choose to specify for the command. Optional keywords appear below the main path line. Optional keywords that cannot be used together are stacked vertically.

Default value



Appears above the main path line.

Repeatable keyword or value

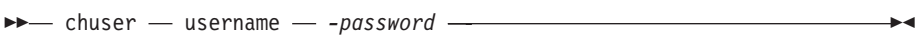


Represents a parameter or argument that you can specify more than once. A repeatable keyword or value is represented by an arrow that returns to the left above the keyword or value.

parameter values

Represents the value you must supply for a parameter or argument, such as a file name, user name, or password. Variables are in italics.

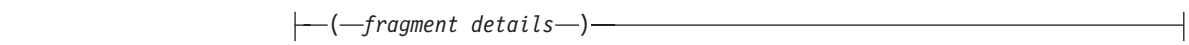
Space separator



Adds a blank space on the main path line to separate keywords, parameters, arguments, or variables from each other.

Syntax fragment

Fragment name:



Breaks up syntax diagrams that are too long, too complex, or repetitious. The fragment name is inserted in the main diagram, and the actual fragment is shown below the main diagram.

Special characters

The following special characters are used in the command examples:

- (minus) or / (slash) sign
Flags are prefixed with a minus- or slash/ sign. Flags define the action of a command or modify the operation of a command. You can use multiple flags, followed by parameters, when you issue a command.

[] square brackets
Optional values are enclosed in square brackets.

{ } braces
Required or expected values are enclosed in braces.

| vertical bar
A vertical bar signifies that you can choose only one value.

For example, `[ a | b ]` indicates that you can choose a, b, or nothing. Similarly, `{ a | b }` indicates that you must choose either a or b.

... ellipsis
An ellipsis signifies the values that can be repeated on the command line.

Emphasis

The following typefaces are used to show emphasis:

boldface
Text in **boldface** represents menu items and command names.

italics
Text in *italics* is used to emphasize a word. In command syntax, it is used for variables for which you supply actual values.

`monospace`
Text in `monospace` identifies the data or command instances that you type, samples of command output, examples of program code or messages from the system, or names of command flags, parameters, arguments, and name-value pairs.

Anatomy of a command line

This section describes the parts of a command line string and also shows an example of a command line string

The command-line string, as discussed in this document, consists of the following parts:

Command name
Name of the command that the user issues, such as **mkuser**.

Command options
Options that modify the behavior of the command. Command options can be required or optional.

Flags Command options marked with dash before the name, such as -create. Sometimes flags require extra parameters and sometimes they do not.

Values
Command options that set the value of a flag.

Arguments
Required target (object) of the command and are always the last items, not associated with an option, on the command line.

This is an example of a command line string.

```
dscimcli mkuser jsmith -password mypassword
```

Description of commands

This section describes the CIM agent commands you can use to manage the CIM agent. Some of these commands are stand-alone and do not need to be used in conjunction with the dscimcli command, and others must only be used with the dscimcli command.

Note: Before using the dscimcli commands, you must set the **DSAGENT_HOME** environment variable to the directory where the CIM agent was installed. You must also include **DSAGENT_HOME/bin** in your PATH environment variable.

The following operational commands are not used with the dscimcli command, and are stand-alone commands:

startagent
Starts the CIM agent.

stopagent
Stops the CIM agent

mkrepository
Deletes the current repository, recompiles the mof files, and creates a new repository.

dscimcli
Views and modifies the configuration of the CIM agent.

collectlogs
Collects DS 5.3 CIM agent logs after a failure has occurred.

Operational commands

This section describes the following CIM agent operational commands:

- **startagent**
- **stopagent**
- **mkrepository**
- **collectlogs**

startagent

Use the **startagent** command to start the CIM agent.

Syntax

Parameters

There are no options for the **startagent** command.

Description

Use the **startagent** command to run the CIM agent code. When you use the **startagent** command, it registers itself with SLP and accepts requests on the port that is specified in the cimom.properties file (by default 5989).

This command starts the CIM agent when the CIM agent is installed. Generally it is installed as a service or part of the system **inittab**. In most cases, there is no reason to start the CIM agent manually; however, this command starts the CIM agent, if needed.

The certificate used by the CIM agent must also be made available to each client software product that intends to communicate with the CIM agent.

stopagent

Use the **stopagent** command to stop the CIM agent.

Syntax

Parameters

There are no options for the **stopagent** command.

Description

Use the **stopagent** command to stop the CIM agent.

mkrepository

Use the **mkrepository** command to delete the current repository, recompile the mof files, and create a new repository.

Syntax

Parameters

There are no options for the **mkrepository** command.

Description

Use the **mkrepository** command only if there is a problem with the repository directory.

collectlogs

Use the **collectlogs** command to collect DS CIM agent logs after a failure has occured.

Syntax

Parameters

There are no options for the **collectlogs** command.

Description

Use the **collectlogs** command to collect DS CIM agent logs after a failure has occurred. The collected files will be placed into a zip file in the $DSAGENT_HOME/log directory.

dscimcli commands

The following sections describe the dscimcli commands that you can invoke in single-shot mode to manage the CIM Agent.

Table 1 describes the subcommands that you can use with the dscimcli command.

Table 1. Summary of dscimcli agent subcommands

Command Category	Command Description
Help	**-h | -help** Lists all available commands and options. **dscimcli** Displays a brief summary of commands and options.
SSL Certificate management	**lscert** List the current SSL certificate. **mkcert** Creates a new SSL certificate. **rmcert** Removes the current SSL certificate. **getcert** Obtains the current SSL certificate from the CIM agent in ASCII form.
Device management	**lsdev** Lists the current ESS/DS devices currently managed by the CIM agent. **mkdev** Adds a device to be managed by the CIM agent. **rmdev** Removes a device from being managed by the CIM agent.

Table 1. Summary of dscimcli agent subcommands (continued)

Command Category	Command Description
Configuration management	**lsconfig** List the current configuration properties of the CIM agent. **chconfig** Modifies the specified configuration properties of the CIM agent.
User management	**mkuser** Adds a user entry to the password file. A user with administrative authority uses this command to create a user account with a password and group authority. **chuser** Changes the user entry in the password file. This command modifies and locks or unlocks a user account, and creates new passwords. **lsuser** Lists the current users that exist in the password file, and access authority levels. **rmuser** Removes the user from the password file. A user with administrative authority uses this command to remove a user account.
CIM agent management	**restartagent** Restarts the CIM agent. This function is only supported for the CIM agent running on the HMC. If it is executed for a CIM agent running on a proxy server, it will simply shut the agent down.

help

Use the **help** command to display information about commands.

Syntax

```
►►— dscimcli — -help ————————————————————————————————►◄
```

Parameters

This section describes the syntax for the options and values that you can use with the **help** command.

[-h | -help]
Displays a help message.

Example

```
>>>dscimcli -help
```

The resulting output:

```
Usage: /snapshots/da2/local/ship/pegasus/bin/dscimcli command arg1 ... argN [options]
Options:
    Server location($DSCIM_SERVER):[ -s [[protocol://]ip[:port][/namespace]].Default(https://1.2.3.4:5989/root/ibm)
    Authentication info ($DSCIM_USER):[-u username:password ]. Default(superuser:passw0rd)
    Timeout ($DSCIM_TIMEOUT): [-t timeout]. Default(60)
    Verbose: [-v]. Default(false)
    Help: [-help].
Command list:
 Device management:
    lsdev [-l]
    mkdev ip[-type ds|ess|esscs][-ip2 ip][-user username][-password password]
             (default: user=admin , password=admin)
    rmdev ip -type ds|ess|esscs
 User management:
    lsuser
    mkuser username -password password
    chuser username -password password -newpassword newpassword
    rmuser username
 Configuration management:
    lsconfig
    chconfig [-insecureport port*] [-secureport port*]
             [-enableinsecure yes|no*] [-enablesecure yes|no*]
             [-certificate certname*] [-loglevel fatal|error|warn|info]
             [-tracecomponent comma_separated_list](possible values: all, none, cpa, sea, jni, servicemanager)
             [-tracemask comma_separated_list](possible values: all, none, entryexit, fine, debug, perf)
             [-jvmarg args] [-essdutycycle time]
             *: requires a restart of the CIM Agent
 SSL Certificate management:
    lscert
    mkcert certname
    rmcert certname
    getcert certname
```

SSL Certificate commands

The following sections describe the following CIM agent SSL certificate commands:

- **lscert**
- **getcert**
- **rmcert**
- **mkcert**

lscert

Use the **lscert** command to list the current SSL certificates.

Syntax

Parameters

There are no options and values that you can use with the **lscert** command.

Example

```
>>>dscimcli lscert
```

The resulting output:

```
Certificate
==============
ssl
test
alex
```

getcert

Use the **getcert** command to obtain the current SSL certificate.

Syntax

Parameters

This section describes the syntax for the options and values that you can use with the **getcert** command.

certname
Specifies the name of the certificate.

Example

```
>>>dscimcli getcert certname
```

The resulting output:

```
 -----BEGIN CERTIFICATE-----
MIICczCCAdwCCQCH2mGnKwgJyzANBgkqhkiG9w0BAQQFADB+MQswCQYDVQQGEwJV
UzELMAkGA1UECBMCTlkxDzANBgNVBAcTBkFybW9uazEMMAoGA1UEChMDSUJNMRIw
EAYDVQQLEwlDSU0gQWdlbnQxDjAMBgNVBAMTBW93bmVyMR8wHQYJKoZIhvcNAQkB
FhBvd25lckB1cy5pYm0uY29tMB4XDTA2MDMyOTExMDMzOVoXDTA3MDMyOTExMDMz
OVowfjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk5ZMQ8wDQYDVQQHEwZBcm1vbmsx
DDAKBgNVBAoTA0lCTTESMBAGA1UECxMJQ0lNIEFnZW50MQ4wDAYDVQQDEwVvd25l
cjEfMB0GCSqGSIb3DQEJARYQb3duZXJAdXMuaWJtLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEAzG5Qsm5pG8ZrGO94MHED9H1lZwp+qnaXzkIUTLW7IzbC
izEyTyydZ/rnjbtcKlJrCyT3RavRR1ed4thIlKPr91qagqQoDngIvU0T6DD+sekG
Kt7W8aEaSOBD2Z0/iVuJhPn+krPJsSX92F28uHmen5hSR2UQFHT6iGnCOjR6kBcC
AwEAATANBgkqhkiG9w0BAQQFAAOBgQAD8s4RubCyBzQ8XmrMQmLAc2fGBJBbjNd7
9DFrb6N8RXPaOHJgMVJbdRCUM3Rn8vMSIk0O+nWr/R7LK72CEu+4yDG4wyEjATau
PRbVBUfuWdIlmxbAlfup3rFWGQVXlf7bSoQaHx8gzRAOIhzfs0p30TZReTo7jHSQ
rcLHrLkEdQ==
-----END CERTIFICATE-----
```

rmcert

Use the **rmcert** command to remove the current SSL certificate.

Syntax

Parameters

This section describes the syntax for the options and values that you can use with the **rmcert** command.

certname
Specifies the name of the SSL certificate that you are attempting to remove.

Example

```
>>>dscimcli rmcert certname
```

The resulting output:

```
Certificate removed
```

mkcert

Use the **mkcert** command to check the level of security on your host.

Syntax

Description

The **mkcert** command runs at installation and can be rerun whenever the user feels that security might be compromised. The **mkcert** command creates an X.509 certificate and places it in a certificate store called truststore. This certificate might be required by client code that communicates with the CIM agent using SSL secure communication. If you have installed a product that uses this type of communication with the CIM agent, be sure that the certificate that is created with the **mkcert** command is available to all clients and software products that communicate with the CIM agent.

Parameters

This section describes the syntax for the options and values you can use with the **mkcert** command.

certname
Requires a restart of the CIM agent.

Example

```
>>>dscimcli mkcert certname
```

The resulting output:

```
Certificate created
```

Device management commands

This section describes the following CIM agent device management commands:

- **lsdev**
- **mkdev**
- **rmdev**

lsdev

Use the **lsdev** command to display a report of the current ESS and DS devices currently managed by the CIM agent.

Syntax

Parameters

This section describes the syntax for the options and values that you can use with the **lsdev** command.

[-l | -long]
Displays an extended report listing.

Example

```
>>>dscimcli lsdev -l
```

The resulting output:

```
Type IP            IP2   Username Storage Image    Status     Code Level  Min Codelevel
==== ============  ===== ======== ================ ========== ==========  =============
DS   9.11.111.111  -     admin    IBM.2107-1234567 successful 5.1.0.309   5.1.0.309
```

```
>>>dscimcli lsdev
```

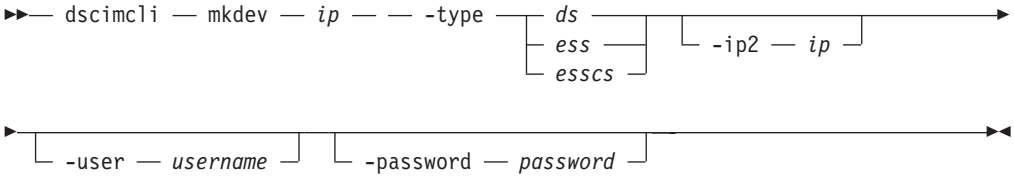
The resulting output:

```
Type  IP             IP2      Username
===== =========      ======== =========
DS    9.11.111.111    -       admin
```

mkdev

Use the **mkdev** command to add a device to be managed by the CIM agent

Syntax



Parameters

This section describes the syntax for the options and values that you can use with the **mkdev** command.

ip Specifies the dotted decimal IP address of the device you are creating. When adding a DS6000 or DS8000 family device, the device type is ″ds″, the IP address is the master console. When adding an ESS family device for logical configuration, the IP address is the primary processor complex. When adding an ESS Copy Services server, the IP address is the ESS Copy Services server. Note that an ESS Copy Services server cannot be added without also adding the associated ESS logical configuration information. However, an ESS can be added for logical configuration without adding a Copy Services server.

-type *ds | ess | esscs*
Specifies the type of device that you are creating. When adding a DS6000 or DS8000 family device, the device type is ″ds″. When adding an ESS family device for logical configuration, the device type is ″ess″. When adding an ESS Copy Services Server, the device type is ″esscs″.

[ip2]
Specifies the dotted decimal secondary IP address of the device that you are creating.

[-user] *[-username]*
Specifies the user name that the CIM agent will use when communicating with the device. When adding a DS6000 or DS8000 family device, the username and password are the same as used to log into the DS Command Line Interface and DS Storage Manager. When adding an ESS family device for logical

configuration, the username and password are the same as used to log into the ESS Command Line Interface and ESS Specialist. When adding an ESS Copy Services server, the username and password are those used to log into the ESS Copy Services interface. The default user is **admin**.

[-password] *[password]*
Specifies the password that the CIM agent will use when communicating with the device. The default password is **admin**.

Example

```
>>>dscimcli mkdev 9.11.111.111 -type ds -user notshown -password notshown
```

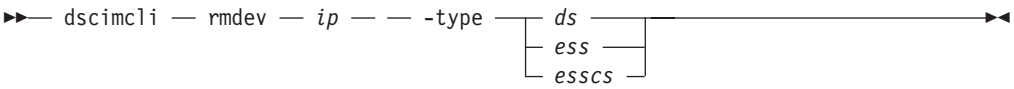
The resulting output:

```
Device successfully added
```

rmdev

Use the **rmdev** command to remove a device from being managed by the CIM agent.

Syntax



Parameters

This section describes the syntax for the options and values that you can use with the **rmdev** command.

ip Specifies the dotted decimal IP address of the device that you are creating.

-type *ds | ess | esscs*
Specifies the type of device that you are creating.

Example

```
>>>dscimcli rmdev 1.2.3.4 -type ds
```

The resulting output:

```
Device successfully removed
```

Configuration management commands

This section describes the following CIM agent configuration management commands:

- **lsconfig**
- **chconfig**

lsconfig

Use the **lsconfig** command to list the current configuration properties of the CIM agent.

Syntax

Parameters

There are no options or values that you can use with the **lsconfig** command.

Example

```
>>>dscimcli lsconfig
```

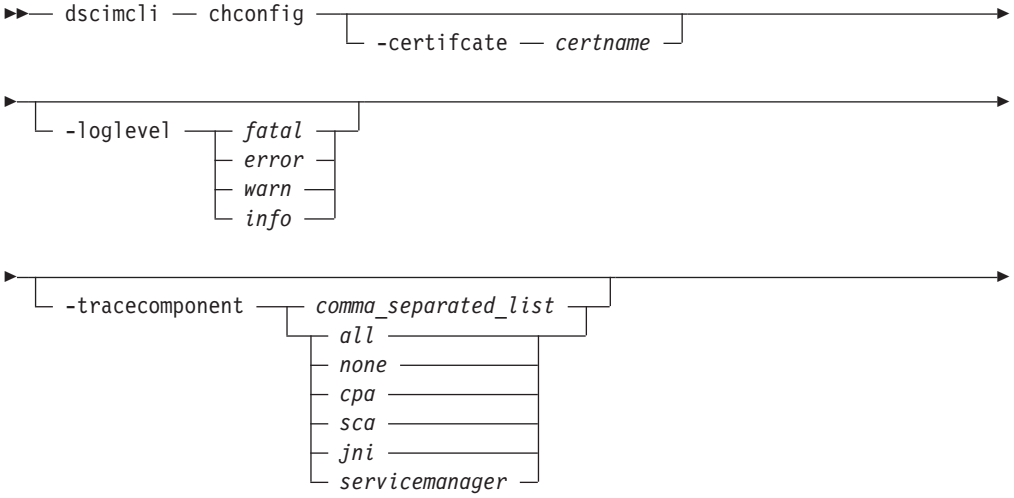
The resulting output:

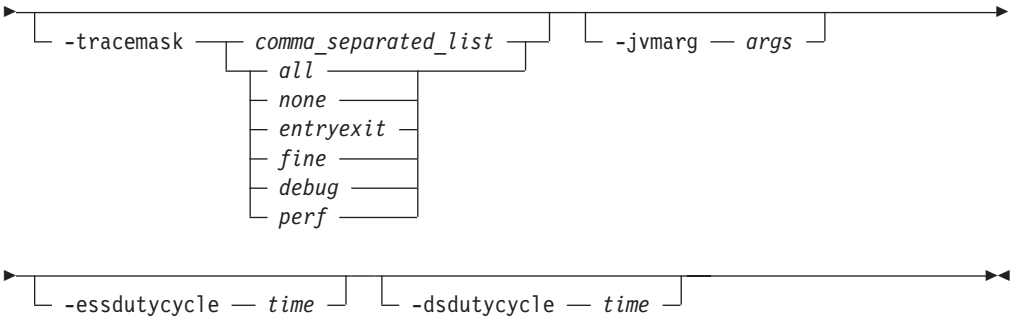
```
Property       Current Value                 After Restart
============== ============================= ==============================
insecureport   5988                          5988
secureport     5989                          5989
certificate    alex                          alex
enablesecure   true                          true
enableinsecure true                          true
loglevel       warn                          warn
tracemask      none                          none
tracecomponent none                          none
jvmarg         -Xms128m -Xmx512m             -Xms128m -Xmx512m
essdutycycle   20                            20
```

chconfig

Use the **chconfig** command to modify the specified configuration properties of the CIM agent.

Syntax





Parameters

This section describes the syntax for the options and values that you can use with the **chconfig** command.

-insecureport *port*
Requires a restart of the CIM agent.

-secureport *port*
Requires a restart of the CIM agent.

-enableinsecure
[yes | no] Requires a restart of the CIM agent.

-enablesecure
[yes | no] Requires a restart of the CIM agent.

-certificate *certname*
Requires a restart of the CIM agent.

-loglevel
[fatal | error | warn | info]

–tracecomponent *comma_separated_list*
Possible values: all, none, cpa, sea, jni, servicemanager

-tracemask *comma_separated_list*
Possible values: all, non, entryexit, fine, debug, perf

-jvmarg args
Specifies a freeform string that is passed in as an argument to the JVM. One use for this parameter is setting the memory parameters. For example, if jvmargs is set to -Xms128m -Xmx 512m, , there is a maximum of 512 megabytes allocated to the JVM heap. For larger configurations, if the JVM is running out of memory, this can be increased, for example, to -Xms128m -Xmx1024m.

-essdutycycle time
Specifies the percentage of time that is spent updating the cache for ESS objects

-dsdutycycle time
Specifies the percentage of time that is spent updating the cache for DS objects

Example

```
>>>dscimcli chconfig -loglevel info -tracecomponent all -tracemask all
```

The resulting output:

```
LogLevel changed
TraceComponent changed
TraceMask changed
```

User management commands

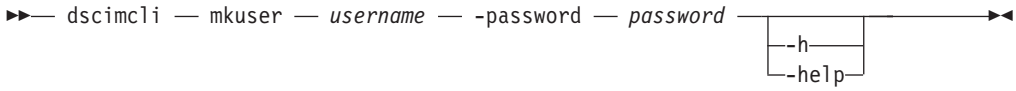
This section describes the following CIM agent user management commands:

- **mkuser**
- **chuser**
- **lsuser**
- **rmuser**

mkuser

Use the **mkuser** command to add a user entry to the password file. A user with administrative authority uses this command to create a user account with a password and user group authority.

Syntax



Parameters

This section describes the syntax for the options and values that you can use with the **mkuser** command.

-password
Specifies that a new password be assigned to the user.

[-h | -help]
Displays a help message.

Example

```
>>>dscimcli mkuser jsmith -password notshown
```

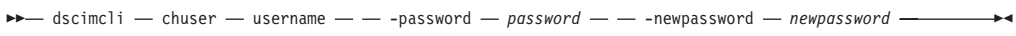
The resulting output:

```
user created
```

chuser

Use the **chuser** command to modify the user password entry in the password file. A user with administrative authority uses this command to update a user account password, modify user group authority, or lock and unlock a password. Users without administrative authority use this command to change an expired password or create a new password.

Syntax



Parameters

This section describes the syntax for the options and values that you can use with the **chuser** command.

username
Specifies the user ID for which you are attempting to modify the password.

-password *password*
Specifies the current password for the user ID that you want to modify.

-newpassword *newpassword*
Specifies that a new password be assigned to the user.

Example

```
>>>dscimcli chuser <jsmith> -password <abcdeg123> -newpassword <notshown>
```

The resulting output:

```
Password successfully changed
```

lsuser

Use the **lsuser** command to list the users that currently exist in the password file, and the authority levels.

Syntax

Parameters

This section describes the syntax for the options and values that you can use with the **lsuser** command.

Example

```
>>>dscimcli lsuser
```

The resulting output:

```
USERNAME
=========
jsmith
ljohnson
bcollins
```

rmuser

Use the **rmuser** command to remove a user account from the password file.

Syntax

Parameters

This section describes the syntax for the options and values that you can use with the **rmuser** command.

username
Specifies the user ID that you are attempting to remove.

Example

```
>>>dscimcli rmuser jsmith
```

The resulting output:

```
User removed
```

Chapter 7. DS Open API component definitions

This section describes the elements, the namespace, and the object name for the DS Open API.

Elements

The DS Open API consists of the following elements: schemas, classes, properties, methods, indications, associations, references and qualifiers. The following list describes each type of element:

Schema
A group of classes defined to a single namespace. Within the CIM agent, the schemas that are supported are the ones loaded through the managed object format (MOF) compiler.

Class The definition of an object within some hierarchy. Classes can have methods and properties and be the target of an association.

Property
A value used to characterize instances of a class.

Method
An implementation of a function on a class.

Indication
An object representation of an event.

Association
A class that contains two references which define a relationship between two objects.

Reference
A unique identifier of an object that is based on its key properties.

Qualifier
Additional information about other elements, classes, associations, indications, methods, method parameters, instances, properties, or references.

Namespace

DS Open API operations always execute within the context of a namespace. A namespace defines the scope over which a DS Open API schema applies. The only namespace supported by the CIM agent is **root/ibm**. A DS Open API schema or version is loaded into a namespace when that schema is compiled by the MOF compiler. The namespace must be specified within the message that the client sends to the CIM agent.

Clients cannot create new namespaces. Attempts to do so result in errors.

Object name

An object name consists of a namespace path and a model path. The namespace path provides access to the DS Open API implementation managed by the CIM agent. The model path provides navigation within the implementation. An example of an object name is:

```
http://cimom.host.com/root/ibm:CIM_Class.key1=value1,key2=value2
```

where *http://cimom.host.com/root/ibm* is the namespace path and the rest is the model path.

Chapter 8. CIM agent communication with the DS Open API

This section describes communication between the CIM agent and the DS Open API. It includes the following information:

- CIM agent communication concepts
- CIM agent communication methods
- CIM agent functional groups
- CIM agent return codes
- Error codes that are returned by the CIMOM

CIM agent communication concepts

This section describes the concepts involved in communication between the CIM agent and the client application.

Client communication

A client application communicates with the CIM agent through operation request messages encoded within XML. The CIM agent returns responses with operation response messages. Requests and responses are subelements of the CIM <MESSAGE> element.

A <MESSAGE> sent to the CIM agent must contain an ID attribute. A response from the CIM agent returns this value and thereby enables the client to track requests and their responses.

The CIM agent supports simple requests and simple responses. Simple requests are operation request messages that contain the <SIMPLEREQ> XML tag. Simple responses are operation response messages that contain the <SIMPLERSP> tag. A client application determines that the CIM Agent only supports simple operation requests and responses by examining the results of running the OPTIONS method.

Intrinsic and Extrinsic Methods

All operations on the CIM agent are performed by running one or more methods. A method is either an intrinsic method or an extrinsic method. Intrinsic methods are supported by the CIM agent itself. These methods are included within XML <IMETHODCALL> tags sent in messages to the CIM agent. Extrinsic methods are defined by the schema supported by the CIM agent. These methods are included within XML <METHODCALL> tags sent in messages to the CIM agent.

Client applications can call on the CIM agent using the methods. These methods fall within certain functional groups that might or might not actually be supported by the CIM agent.

CIM agent communication methods

The following sections and tables list the CIM intrinsic and extrinsic communication methods along with their parameters.

Client application calls to these intrinsic methods result in CIM agent calls to the device provider, if the device provider surfaces the classes or instances that are referenced in those calls.

The CIM agent returns <IMETHODRESPONSE> or <METHODRESPONSE> elements to the client application when the intrinsic or extrinsic methods are used. These elements are contained within a <MESSAGERESPONSE> tag.

GetClass

The GetClass method returns a single class from the target namespace. Table 2 describes the parameters of the GetClass method.

Table 2. GetClass method parameters

Parameter	Type	Description
ClassName	String	Defines the name of the class to retrieve.
LocalOnly	Boolean	TRUE returns all properties, methods, and qualifiers overridden within the definition of the class.
IncludeQualifiers	Boolean	TRUE returns all qualifiers for the class, its properties, methods, or method parameters. FALSE returns no qualifiers.
IncludeClassOrigin	Boolean	TRUE returns the CLASSORIGIN attribute of the class.

Return values: Either a single class or one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_FAILED

GetInstance

The GetInstance method returns a single instance from the target namespace. Table 3 describes the parameters of the GetInstance method.

Table 3. GetInstance method parameters

Parameter	Type	Description
InstanceName	String	Defines the name of the instance to retrieve.
IncludeClassOrigin	Boolean	TRUE returns the CLASSORIGIN attribute of the class.

Return values: Either a single class or one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_NOT_FOUND
- CIM_ERR_FAILED

DeleteClass

The DeleteClass method deletes a single class from the target namespace.

Note: This operation is not supported. The CIM_ERR_NOT_SUPPORTED error code is returned to the client application if a request to process this operation is received.

DeleteInstance

The DeleteInstance method deletes a single instance from the target namespace. Table 4 describes the parameters of the DeleteInstance method.

Table 4. DeleteInstance method parameters

Parameter	Type	Description
InstanceName	String	Defines the name of the instance to delete.

Return values: The named instance is deleted or one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_NOT_FOUND
- CIM_ERR_FAILED

Note: These are CIM standard methods, but the DS CIM Agent version 5.3 does not have any features that use this method.

CreateClass

The CreateClass method creates a new class from the target namespace.

Note: This operation is not supported. The CIM_ERR_NOT_SUPPORTED error code is returned to the client application if a request to process this operation is received.

CreateInstance

The CreateInstance method creates an instance in the target namespace. The instance must not already exist. Table 5 describes the parameters of the CreateInstance method.

Table 5. CreateInstance method parameters

Parameter	Type	Description
Instance	Object	The instance to be created. The instance must be based on a class already defined in the target namespace.

Return values: If successful, the specified instance is created. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_ALREADY_EXISTS

- CIM_ERR_FAILED

Note: These are CIM standard methods, but the DS CIM Agent version 5.3 does not have any features that use this method.

ModifyClass

The ModifyClass method modifies an existing class.

Note: This operation is not supported. The CIM_ERR_NOT_SUPPORTED error code is returned to the client application if a request to process this operation is received.

ModifyInstance

The ModifyInstance method modifies an existing instance in the target namespace. The instance must already exist. Table 6 describes the parameters of the ModifyInstance method.

Table 6. ModifyInstance method parameters

Parameter	Type	Description
Instance	Object	Defines the modified instance.

Return values: If successful, the specified instance is updated. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_NOT_FOUND
- CIM_ERR_FAILED

Note: These are CIM standard methods, but the DS CIM Agent version 5.3 does not have any features that use this method.

EnumerateClasses

The EnumerateClasses method returns a single class from the target namespace. Table 7 describes the parameters of the EnumerateClasses method.

Table 7. EnumerateClasses method parameters

Parameter	Type	Description
ClassName	String	Defines the name of the class for which subclasses are to be returned. If this field is NULL, all base classes within the target namespace are returned.
DeepInheritance	Boolean	TRUE returns all subclasses of the specified class. FALSE returns only immediate child subclasses.
LocalOnly	Boolean	TRUE returns all properties, methods, and qualifiers, that are overridden within the definition of the class.
IncludeQualifiers	Boolean	TRUE returns all qualifiers for the class, its properties, methods, or method parameters. FALSE returns no qualifiers.

Table 7. EnumerateClasses method parameters (continued)

Parameter	Type	Description
IncludeClassOrigin	Boolean	TRUE returns the CLASSORIGIN of the class.

Return values: If successful, zero or more classes (CIMClass) are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_FAILED

EnumerateClassNames

The EnumerateClassNames method enumerates the names of subclasses of a class defined within the target namespace. Table 8 describes the parameters of the EnumerateClassNames method.

Table 8. EnumerateClassNames method parameters

Parameter	Type	Description
ClassName	String	Defines the name of the class for which subclass names are to be returned. If this field is NULL, all base class names within the target namespace are returned.
DeepInheritance	Boolean	TRUE returns all subclass names of the specified class. FALSE returns only immediate child subclass names.

Return values: If successful, zero or more class names are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_FAILED

EnumerateInstances

The EnumerateInstances method enumerates instances of a defined class in the target namespace. Table 9 describes the parameters of the EnumerateInstances method.

Table 9. EnumerateInstances method parameters

Parameter	Type	Description
ClassName	String	Defines the name of the class for which instances are to be returned.
DeepInheritance	Boolean	TRUE returns all instances and all properties of the instance, including those added by subclassing. FALSE returns only properties that are defined for the specified class.
IncludeClassOrigin	Boolean	TRUE returns the CLASSORIGIN attribute of the class within the instance.

Return values: If successful, zero or more instances (Objects) are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_FAILED

EnumerateInstanceNames

The EnumerateInstanceNames method enumerates the names of the instances of a class within a target namespace. Table 10 describes the parameter of the EnumerateInstanceNames method.

Table 10. EnumerateInstanceNames method parameters

Parameter	Type	Description
ClassName	String	Defines the name of the class for which instance names are returned.

Return values: If successful, zero or more names of instances are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_FAILED

ExecuteQuery

The ExecuteQuery method processes a query against the target namespace. Table 11 describes the parameters of the ExecuteQuery method.

Table 11. ExecuteQuery method parameters

Parameter	Type	Description
QueryLanguage	String	Defines the query language in which the query parameter is expressed.
Query	String	Defines the query to be executed.

Return values: If successful, the method returns a table definition, followed by zero or more rows that correspond to the results of the query. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_NOT_SUPPORTED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_QUERY_LANGUAGE_NOT_SUPPORTED
- CIM_ERR_QUERY_FEATURE_NOT_SUPPORTED

- CIM_ERR_INVALID_QUERY
- CIM_ERR_FAILED

Associators

The Associators method enumerates classes or instances that are associated with a particular CIM Object. Table 12 describes the parameters of the Associators method.

Table 12. Associators method parameters

Parameter	Type	Description
ObjectName	String	Defines the class name or instance name that is the source of the association.
AssocClass	String	If not NULL, indicates that all objects must be associated with the source object through an instance of this class or one of its subclasses.
ResultClass	String	If not NULL, indicates that all returned objects must be instances of this class or one of its subclasses or be this class.
Role	String	If not NULL, indicates that each return object must be associated with the source object through an association in which the source object plays the specified role. The name of the property in the association class that refers to the source object must match the value of this parameter.
ResultRole	String	If not NULL, indicates that each returned object must be associated with the source object through an association in which the return object plays the specified role. That is, the name of the property in the association class that refers to the returned object must match the value of this parameter.
IncludeClassOrigin	Boolean	TRUE returns the CLASSORIGIN attribute of the class.

Return values: If successful, zero or more classes (CIMClass) or instances (Objects) are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_FAILED

AssociatorNames

The AssociatorNames method enumerates the names of the classes or instances that are associated with a particular CIM object. Table 13 describes the parameters of the AssociatorNames method.

Table 13. AssociatorNames method parameters

Parameter	Type	Description
ObjectName	String	Defines the class name or instances name that is the source of the association.

Table 13. AssociatorNames method parameters (continued)

Parameter	Type	Description
AssocClass	String	If not NULL, indicates that all returned object paths returned identify an object that is associated with the source object through an instance of this class or one of its subclasses.
ResultClass	String	If not NULL, indicates that all returned object paths must identify instances of this class or one of its subclasses or must be this class.
Role	String	If not NULL, the name of the property in the association class that refers to the source object must match the value of this parameter.
ResultRole	String	If not NULL, the name of the property in the association class that refers to the return object must match the value of this parameter.

Return values: If successful, zero or more class paths (CIMObjectPath) are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_FAILED

References

The References method enumerates the association objects that refer to a particular target class or instance. Table 14 describes the parameters of the References method.

Table 14. References method parameters

Parameter	Type	Description
ObjectName	String	Defines the class name or instance name whose referring objects are to be returned.
ResultClass	String	If not NULL, indicates that all returned objects must be instances of this class or one of its subclasses or must be this class.
Role	String	If not NULL, must be a valid property name. Each returned object must refer to the target object through a property whose name matches the value of this parameter.
IncludeClassOrigin	Boolean	TRUE returns the CLASSORIGIN attribute of the class.

Return values: If successful, zero or more classes (CIMClass) or instances (Objects) are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_FAILED

ReferenceNames

The ReferenceNames method enumerates the association objects that refer to a particular target class or instance. Table 15 describes the parameters of the ReferenceNames method.

Table 15. ReferenceNames method parameters

Parameter	Type	Description
ObjectName	String	Defines the class name or instance name whose referring objects are to be returned.
ResultClass	String	If not NULL, indicates that all returned object paths must be object paths of instances of this class or one of its subclasses, or must be this class.
Role	String	If not NULL, must be a valid property name. Each returned object must refer to the target object through a property whose name matches the value of this parameter.

Return values: If successful, the return value specifies the value of the requested property. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_NOT_FOUND
- CIM_ERR_NO_SUCH_PROPERTY
- CIM_ERR_FAILED

GetProperty

The GetProperty method retrieves a single property value from an instance in the target namespace. Table 16 describes the parameters of the GetProperty method.

Table 16. GetProperty method parameters

Parameter	Type	Description
InstanceName	String	Defines the name of the instance.
Property	String	The name of the property whose value is to be returned from the instance.

Return values: If successful, the return value specifies the value of the requested property. Otherwise, one of the following return codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_NOT_FOUND
- CIM_ERR_NO_SUCH_PROPERTY
- CIM_ERR_FAILED

SetProperty

The SetProperty method sets a single property value within an instance in the target namespace. Table 17 describes the parameters of the SetProperty method.

Table 17. SetProperty method parameters

Parameter	Type	Description
InstanceName	String	Defines the name of the instance.
PropertyName	String	The name of the property whose value is to be updated.

Return values: If successful, the instance is updated. Otherwise, one of the following return codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_INVALID_CLASS
- CIM_ERR_NOT_FOUND
- CIM_ERR_NO_SUCH_PROPERTY
- CIM_ERR_TYPE_MISMATCH
- CIM_ERR_FAILED

GetQualifier

The GetQualifier method retrieves a single qualifier declaration from the target namespace. Table 18 describes the parameters of the GetQualifier method.

Table 18. GetQualifier method parameters

Parameter	Type	Description
QualifierName	String	Defines the qualifier whose declaration is to be returned.

Return values: If successful, the value of the qualifier is returned. Otherwise, one of the following return codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_NOT_FOUND
- CIM_ERR_FAILED

SetQualifier

The SetQualifier method creates or updates a qualifier declaration in the target namespace. Table 19 describes the parameters of the SetQualifier method.

Table 19. SetQualifier method parameters

Parameter	Type	Description
QualifierDeclaration	Void	Defines the qualifier declaration to be added to the target namespace.

Return values: If successful, the qualifier is updated in the target namespace. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_NOT_FOUND
- CIM_ERR_FAILED

DeleteQualifier

The DeleteQualifier method deletes a single class from the target namespace.

Note: This operation is not supported. The CIM_ERR_NOT_SUPPORTED error message is returned to the client application if a request to execute this operation is received.

EnumerateQualifiers

The EnumerateQualifiers method enumerates qualifier declarations from the target namespace.

There are no parameters for this method.

Return values: If successful, zero or more qualifier declarations are returned. Otherwise, one of the following error codes is returned:

- CIM_ERR_ACCESS_DENIED
- CIM_ERR_INVALID_NAMESPACE
- CIM_ERR_INVALID_PARAMETER
- CIM_ERR_FAILED

CIM agent functional groups

Table 20 describes the functional groups supported by the CIM agent. This information is also returned to a client which makes an OPTIONS request of the CIM agent.

Table 20. Functional groups for the CIM agent

Functional group	Parameters	Supported or Not Supported
Basic read	• GetClass • EnumerateClasses • EnumerateClassNames • GetInstance • EnumerateInstances • EnumerateInstanceNames • GetProperty	Supported
Basic write	• SetProperty	Not Supported
Schema manipulation	• CreateClass • ModifyClass • DeleteClass	Not Supported

Table 20. Functional groups for the CIM agent (continued)

Functional group	Parameters	Supported or Not Supported
Instance manipulation	• CreateInstance • ModifyInstance • DeleteInstance	Supported
Association traversal	• Associators • AssociatorNames • References • ReferenceNames	Supported
Qualifier declaration	• GetQualifier • SetQualifier • DeleteQualifier • EnumerateQualifiers	Supported
Query execution	• ExecQuery	Supported

Error codes returned by the CIMOM

This section identifies the possible error codes returned by CIMOM communication methods.

Return Error Codes

The CIMOM might return status to the client application in one of two ways:

- Through HTTP status messages or
- Through error codes contained within <METHODRESPONSE> or <IMETHODRESPONSE> XML tags

Table 21 describes the vendor-specific status codes that the CIMOM might return. For CIM standard return codes, see the CIM schema.

Table 21. Return error codes for the CIMOM

Symbolic Name	Code	Definition
CIM_ERR_FAILED	1	A general error occurred that is not covered by a more specific error code.
CIM_ERR_ACCESS_DENIED	2	Access to a CIM resource was not available to the client.
CIM_ERR_INVALID_NAMESPACE	3	The target namespace does not exist.
CIM_ERR_INVALID_PARAMETER	4	One or more parameter values passed to the method were invalid.
CIM_ERR_INVALID_CLASS	5	The specified class does not exist.
CIM_ERR_NOT_FOUND	6	The requested object could not be found.
CIM_ERR_NOT_SUPPORTED	7	The requested operation is not supported.
CIM_ERR_CLASS_HAS_CHILDREN	8	The operation cannot be carried out on this class because it has instances.
CIM_ERR_CLASS_HAS_INSTANCES	9	The operation cannot be carried out on this class because it has instances.

Table 21. Return error codes for the CIMOM (continued)

Symbolic Name	Code	Definition
CIM_ERR_INVALID_SUPERCLASS	10	The operation cannot be carried out since the specified superclass does not exist.
CIM_ERR_ALREADY_EXISTS	11	The operation cannot be carried out because an object already exists.
CIM_ERR_NO_SUCH_PROPERTY	12	The specified property does not exist.
CIM_ERR_TYPE_MISMATCH	13	The value supplied is incompatible with the type.
CIM_ERR_QUERY_LANGUAGE_NOT_SUPPORTED	14	The query language is not recognized or supported.
CIM_ERR_INVALID_QUERY	15	The query is not valid for the specified query language.
CIM_ERR_METHOD_NOT_AVAILABLE	16	The extrinsic method could not be executed.
CIM_ERR_METHOD_NOT_FOUND	17	The specified extrinsic method does not exist.
CIM_ERR_LOW_ON_MEMORY	20	There is not enough memory.
XMLERROR	21	An XML error has occurred.
CIM_ERR_LISTNER_ALREADY_DEFINED	22	The listener is already defined.
CIM_ERR_INDICATION_NOT_COLLECTED	23	The indications are not collected.
CIM_ERR_NO_METHOD_NAME	24	The method name is null.
CIM_ERR_INVALID_QUALIFIER_DATATYPE	25	The datatype qualifier is invalid.
CIM_ERR_NAMESPACE_NOT_IN_MANAGER	26	The namespace value is not found.
CIM_ERR_INSTANTIATE_FAILED	27	The instantiation failed.
CIM_ERR_FAILED_TO_LOCATE_INDICATION_ HANDLER	28	The indication handler is not found.
CIM_ERR_IO_EXCEPTION	29	An IO exception has occurred.
CIM_ERR_COULD_NOT_DELETE_FILE	30	The file could not be deleted.
INVALID_QUALIFIER_NAME	31	The qualifier name is null.
NO_QUALIFIER_VALUE	32	The qualifier value is null.
NO_SUCH_QUALIFIER1	33	There is no such qualifier.
NO_SUCH_QUALIFIER2	34	There is no such qualifier.
QUALIFIER_UNOVERRIDABLE	35	The qualifier is unoverridable.
SCOPE_ERROR	36	A scope error has occurred.
TYPE_ERROR	37	A type error has occurred.
CIM_ERR_MISSING_KEY	38	The key is missing.
CIM_ERR_KEY_CANNOT_MODIFY	39	The key cannot be modified.
CIM_ERR_NO_KEYS	40	There are no keys found.
CIM_ERR_KEYS_NOT_UNIQUE	41	The keys are not unique.
CIM_ERR_SET_CLASS_NOT_SUPPORTED	100	The set class operation is not supported.
CIM_ERR_SET_INSTANCE_NOT_SUPPORTED	101	The set instance operation is not supported.
CIM_ERR_QUALIFIER_NOT_FOUND	102	The qualifier value is not found.
CIM_ERR_QUALIFIERTYPE_NOT_FOUND	103	The qualifier type is not found.

Table 21. Return error codes for the CIMOM (continued)

Symbolic Name	Code	Definition
CIM_ERR_CONNECTION_FAILURE	104	The connection failed.
CIM_ERR_FAIL_TO_WRITE_TO_SERVER	105	There is a fail to write to the server.
CIM_ERR_SERVER_NOT_SPECIFIED	106	The server not specified.
CIM_ERR_INDICATION_ERROR	107	There is an indication processing error.
CIM_ERR_FAIL_TO_WRITE_TO_CIMOM	108	There is a fail to write to the CIMOM.
CIM_ERR_SUBSCRIPTION_EXISTS	109	A subscription already exists.
CIM_ERR_INVALID_SUBSCRIPTION_DEST	110	The subscription destination is invalid.
CIM_ERR_INVALID_FILTER_PATH	111	The filter path is invalid.
CIM_ERR_INVALID_HANDLER_PATH	112	The handler path is invalid.
CIM_ERR_NO_FILTER_INSTANCE	113	The filter instance is not found.
CIM_ERR_NO_HANDLER_INSTANCE	114	The handler instance is not found.
CIM_ERR_UNSUPPPORTED_FILTER	115	There is an unsupported filter referenced in the subscription.
CIM_ERR_INVALID_TRUSTSTORE	116	The CIMOM cannot be connected to because there is a bad or missing truststore or an incorrect truststore password.
CIM_ERR_ALREADY_CONNECTED	117	The CIMOM cannot be connected to because it is already connected.
CIM_ERR_UNKNOWN_SERVER	118	The server is unknown. The CIMOM cannot be connected to.
CIM_ERR_INVALID_CERTIFICATE	119	The correct certificate cannot be found in truststore. The CIMOM cannot be connected to.

Chapter 9. IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service for Windows

If you require IBM System Storage support for Microsoft Volume Shadow Copy or Microsoft Virtual Disk Services, continue to use DS CIM agent version 5.3 or later (5.1 or earlier is also supported, but requires some additional steps).

IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service overview

The following information provides an overview of Microsoft Volume Shadow Copy Service and Virtual Disk Service.

Microsoft Volume Shadow Copy Service

IBM System Storage Support for Microsoft Volume Shadow Copy and Virtual Disk Services control storage units using a CIM client query.

You must install the CIM agent, a middleware application that provides a CIM-compliant interface, before installing Microsoft Volume Shadow Copy and Virtual Disk Services. The Microsoft Volume Shadow Copy and Virtual Disk Services uses the CIM technology to manage proprietary devices as open system devices through storage management applications.

IBM System Storage support for Microsoft Volume Shadow Copy Service enables users to quickly back up and restore large amounts of data on Windows Server 2003. Microsoft Volume Shadow Copy Service coordinates with a provider and the storage unit to create a consistent shadow copy of a volume or group of volumes at a point-in-time. Point-in-time shadow copies ensure consistency for Microsoft Volume Shadow Copy Service-aware writers, and also works with applications that do not support Microsoft Volume Shadow Copy Service technology. The shadow copy can be created while the volume is mounted and files are in use.

In order to accomplish this fast backup, a backup application initiates a shadow copy backup. Microsoft Volume Shadow Copy Service then coordinates with the Microsoft Volume Shadow Copy Service writers to briefly hold writes on the databases, applications, or both. Next, Microsoft Volume Shadow Copy Service flushes the file system buffers and asks a provider to initiate a FlashCopy of the data. Once the FlashCopy is logically complete, Microsoft Volume Shadow Copy Service allows writes to resume and notifies the requestor that the backup has completed successfully.

The volumes are then mounted hidden and read-only, to be used when rapid restore is necessary. Alternatively, the volumes can be mounted on a different host and used for application testing or backup to tape. Furthermore, the shadow copies are transportable shadow copies that can be mounted on a different host and used for application testing or backup to tape.

Microsoft Virtual Disk Service

IBM System Storage Support for Microsoft Virtual Disk Service provides a single vendor and technology neutral interface for managing block storage virtualization,

whether done by OS software, RAID storage hardware, or other storage virtualization engines. Microsoft Virtual Disk Service enables the management of heterogeneous storage systems, by using both client and provider APIs. The service allows you to perform the following functions:

- List information about:
  - Providers
  - Subsystems
  - Controllers
  - Luns
  - Drives
- Create or delete LUNs
- Configure LUNs automatically, which facilitates dynamic reconfiguration by hardware in response to load or fault handling.

IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service installation overview

This section provides an overview of the installation and configuration of Microsoft Volume Shadow Copy and Virtual Disk Services on a Windows Server 2003 operating system. You should have some knowledge of how to administer a Windows Server 2003 operating system before you install Microsoft Volume Shadow Copy Service or Volume Shadow Copy Service. You should also become familiar with the installation tasks and gather all of the information you will need for installation ahead of time.

The following installation tasks are presented in the order in that they must be performed:

1. Before you install Microsoft Volume Shadow Copy or Virtual Disk Services, check the hardware and software requirements.
2. Install the prerequisite CIM agent software.
3. Run the InstallShield Wizard for Microsoft Volume Shadow Copy and Virtual Disk Services to install the IBM VSS and VDS Hardware Providers.
4. Create free and reserved volume pools.
5. Verify the installation.
6. Reconfigure the services. Perform this optional task if you would like to change the configuration that you established during installation.

IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service installation requirements

Ensure that your system satisfies the following prerequisite for installing Microsoft Volume Shadow Copy and Virtual Disk Services on a Windows Server 2003 operating system before you start the installation.

You must install the CIM agent *before* you install Microsoft Volume Shadow Copy and Virtual Disk Services. You can locate the CIM agent on the same machine as Microsoft Volume Shadow Copy and Virtual Disk Services or on a different machine.

Hardware

The following minimum hardware is required:

- For Volume Shadow Copy Services: a DS8000, DS6000, or ESS storage unit (with FlashCopy Version 1 or 2)
- For Virtual Disk Services: a DS8000 storage unit

  Note: If you are using ESS F*xx* models, at least one ESS in the environment must be a model 800.
- A system capable of running Windows Server 2003
- 133 - 733 megahertz CPU
- 128 - 256 megabytes of random access memory
- 1.5 gigabyte disk space
- Supported QLogic or Emulex fibre-channel host bus adapter (HBA)

Software

The following software is required:

- Windows Server 2003 operating system. The following editions of Windows Server 2003 are supported:
  - Standard Edition, 32-bit version
  - Enterprise Edition, 32-bit version
  - Standard Edition, *x*64 version
  - Enterprise Edition, *x*64 version
  - Standard Edition R2
  - Enterprise Edition R2
- Common Information Model (CIM) agent. The CIM agent can be located on the same machine as Microsoft Volume Shadow Copy Service or on a different machine. You can find this software on the *CIM agent for IBM System Storage DS Open Application Programming Interface* CD. For VDS, use DS CIM Agent 5.1 or earlier. For VSS, IBM recommends using DS CIM Agent 5.3, but 5.1 is also supported.
- Microsoft Volume Shadow Copy Service compliant backup software

The following software is recommended:

- Windows Server 2003 Service Pack 2 which contains important VSS fixes from Microsoft, including KB911062 and KB913648
- SDDDSM multipathing software

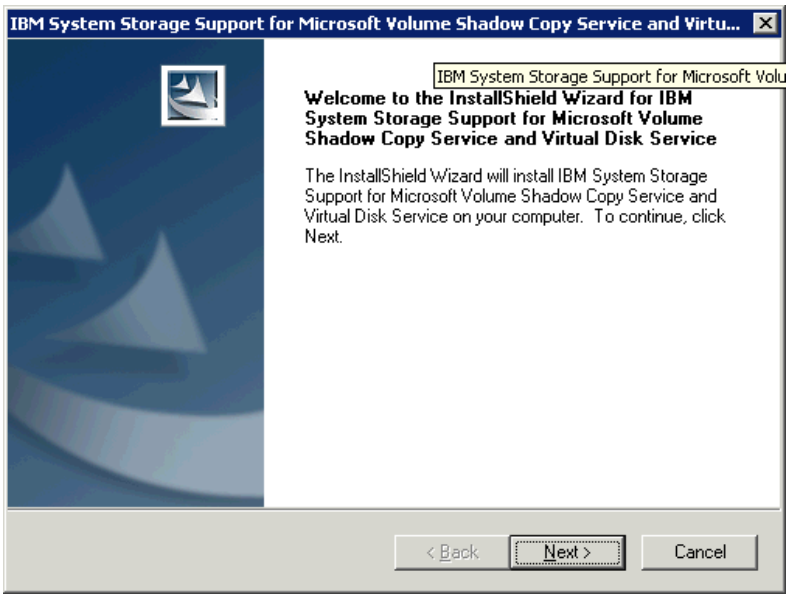
Installing the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service on Windows

This section includes the steps to install the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service on your Windows system.

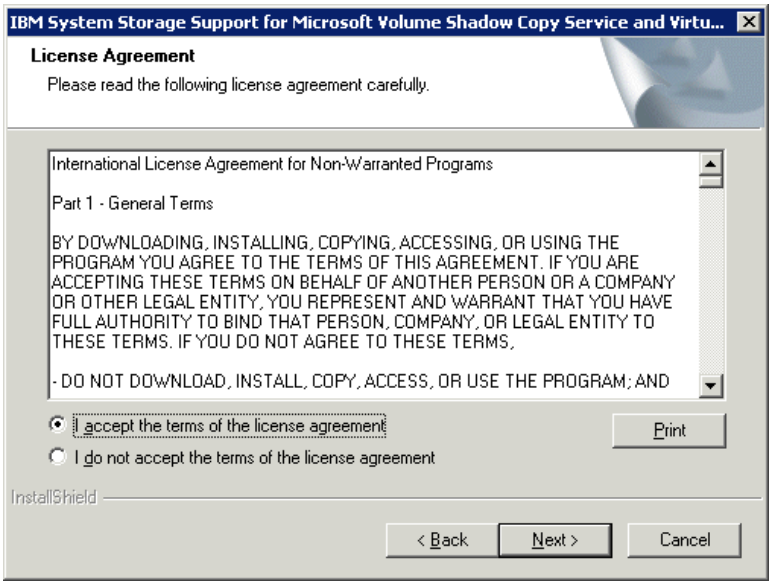
You must satisfy all prerequisites that are listed in the installation requirements section before you start the installation.

1. Log on to your system as the local administrator.
2. Run the InstallShield Wizard by inserting the *IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service* CD into the CD-ROM drive.
3. The Welcome window opens. Click **Next** to continue with the InstallShield Wizard. You can click **Cancel** at any time while using the wizard to exit the

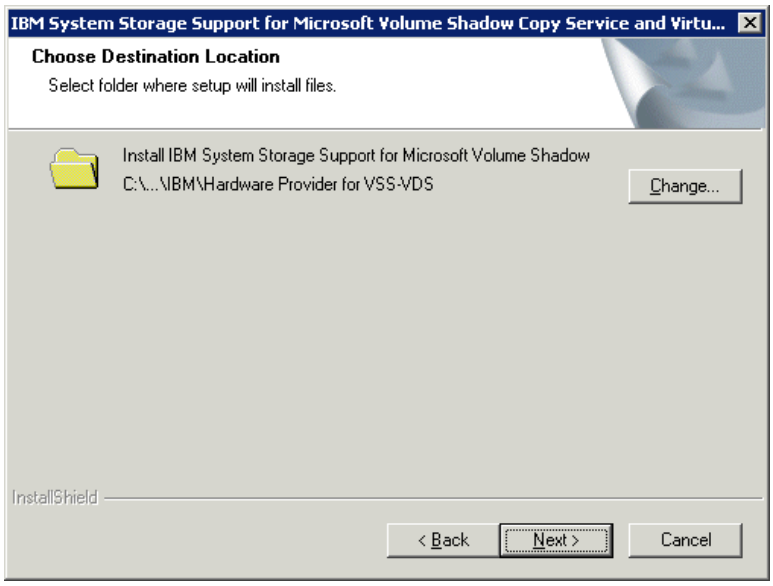
installation. To move back to previous screens while using the wizard, click **Back**.



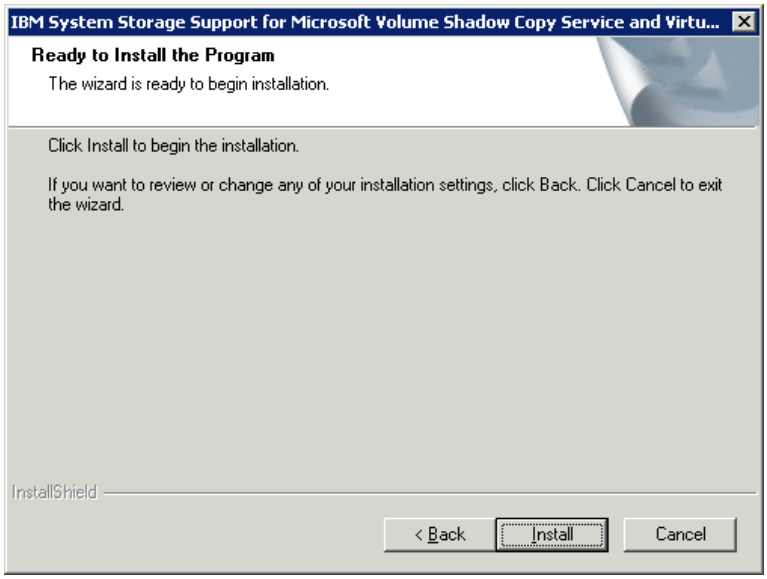
4. The License Agreement window opens. Read the license agreement information. Select whether you accept the terms of the license agreement and click **Next**. If you do not accept, you cannot continue with the installation.



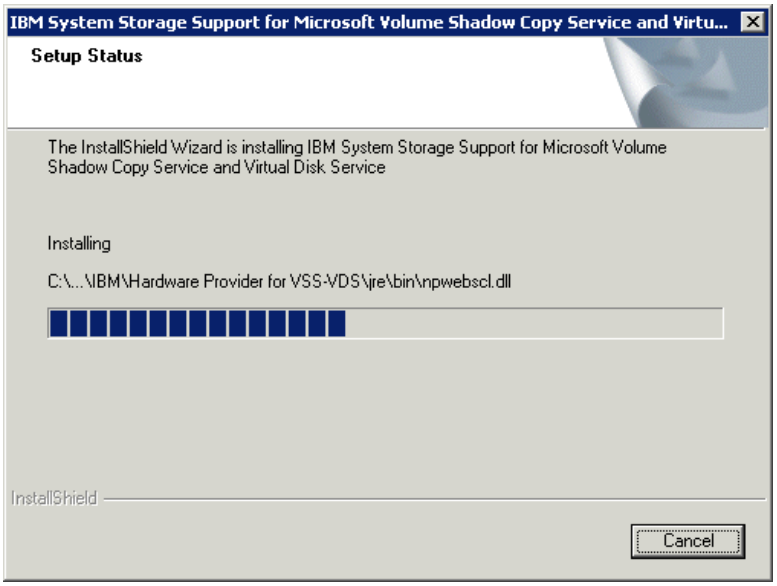
5. The Choose Destination Location Window opens. Click **Next** to accept the default directory where the setup will install the files, or click **Change** to select a different directory and then click **Next**.



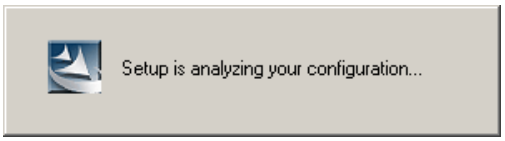
6. The Ready to Install the Program window opens. Click **Install** to begin the installation. To exit the wizard and end the installation, click **Cancel**.



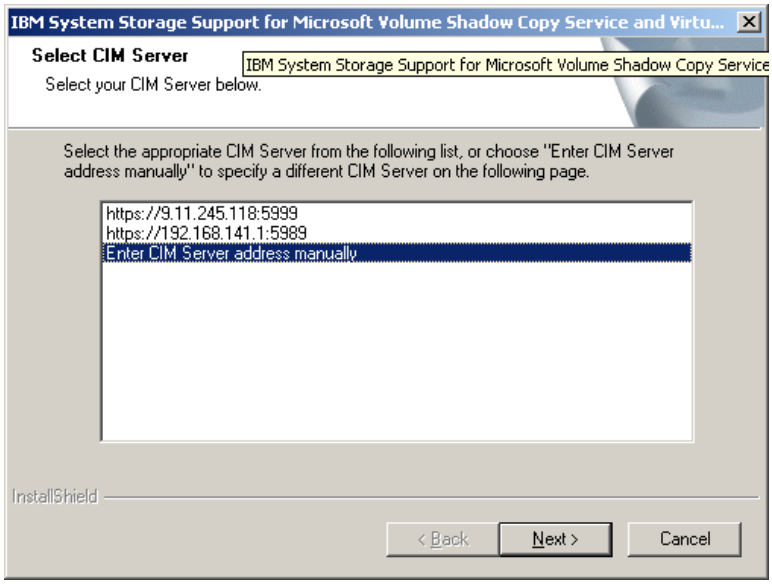
7. The Setup Status window opens. Wait for the setup to complete, or click **Cancel** if you want to stop the setup.



The program setup verifies your configuration.



8. The Select CIM Server window opens. In order to connect to the CIM agent, Microsoft Volume Shadow Copy and Disk Services must obtain some information about the server that the CIM agent is installed on. Select the required CIM server, or select Enter the CIM Server address manually, and click **Next**.

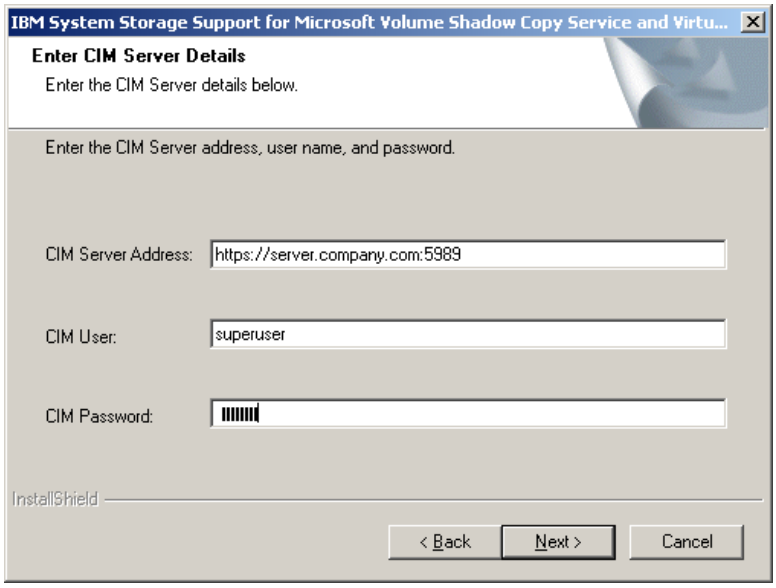


9. The Enter CIM Server Details window opens. Enter your CIM user name and CIM password, and then click **Next**.

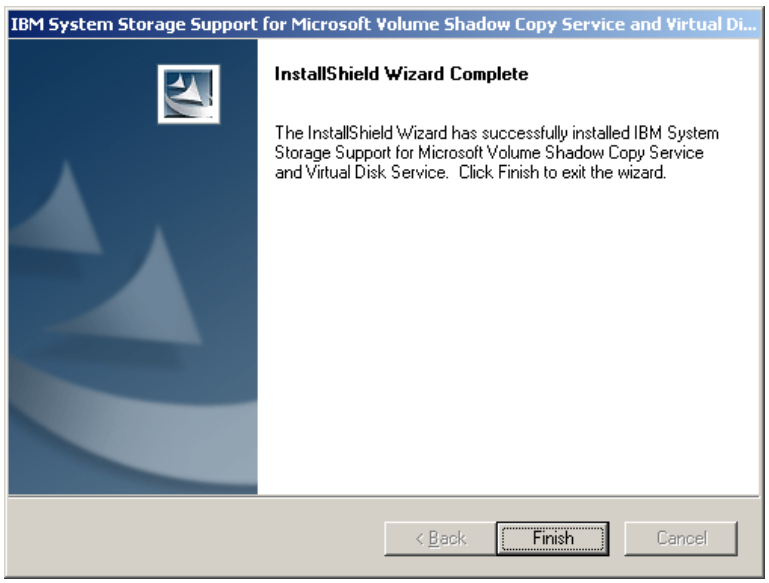
Note:

a. If these settings change after installation, you can use the *ibmvcfg.exe* tool to update Microsoft Volume Shadow Copy and Virtual Disk Services with the new settings.

b. If you do not have the CIM agent port, host, or user information, contact your CIM agent administrator.



10. The InstallShield Wizard Complete window opens. The installation is complete. Click **Finish** to exit the wizard.



11. The installation program might prompt you to reboot your system.
12. If you are connecting to a CIM Agent 5.1 or earlier, you must perform the additional configuration steps:
    a. Copy the truststore file from the CIM Agent server to any location on the VSS/VDS system.

b. Open a command prompt and change directory to the installed directory.
c. Run the command:
```
ibmvcfg set truststore truestore file name
```
d. Run the command:
```
ibmvcfg set trustpassword ibmstore
```
e. Restart the IBM VSS service either with the services panel, or by running the commands:
```
net stop IBMVSS
net start IBMVSS
```

If you are able to perform all of the installation tasks successfully, Microsoft Volume Shadow Copy Service has been successfully installed on your Windows system.

Creating the VSS_FREE and VSS_RESERVED pools for Microsoft Volume Shadow Copy Service

This task allows you to create the VSS_FREE and VSS_RESERVED pools.

Before using the IBM System Storage support for Microsoft Volume Shadow Copy for the first time, you must designate which volumes that the services can use as FlashCopy target volumes. This designation is done by creating a VSS_FREE pool and a VSS_RESERVED pool, represented by virtual hosts that are created on the storage unit. Once the virtual hosts are created, volumes can be added to the free pool by simply assigning a volume to the virtual host.

Perform the following steps using the IBM System Storage DS Storage Manager or DS CLI to create the VSS_FREE and VSS_RESERVED pools:

Note: If you are using the DS CLI you must perform these steps in order.

1. Create a volume group with the name ″VSS_FREE″ or another name, of the same type as your Windows Server 2003 host, for example: SCSI Map 256.
2. Create a virtual hostconnect on the storage unit named ″VSS_FREE″ or another name, with the following parameters:
   a. -profile ″Intel - Windows 2003″
   b. -addrdiscovery LUNPolling
   c. *-volgrp* Where *volgrp* is volume group created in step 1.
   d. -wwname 5000000000000001
3. Create a volume group with the name ″VSS_RESERVED″ or another name, of the same type as your Windows Server 2003 host, e.g. SCSI Map 256.
4. Create a virtual hostconnect on the storage unit named ″VSS_RESERVED″ or another name, with the following parameters:
   a. -profile ″Intel - Windows 2003″
   b. -addrdiscovery LUNPolling
   c. *-volgrp* Where *volgrp* is volume group created in step 3.
   d. -wwname 5000000000000000
5. Create and assign free volumes to the VSS_FREE volume group.

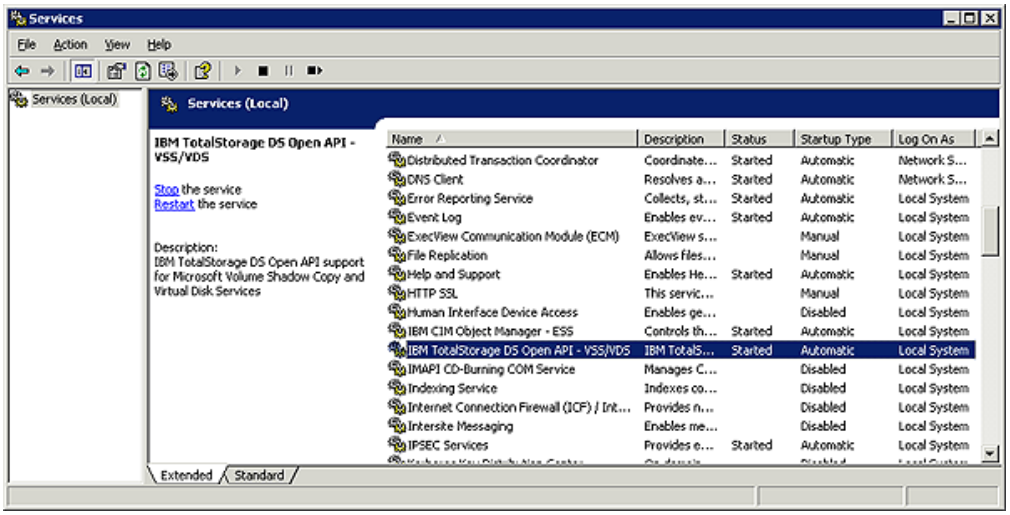
   Note: If you already have volumes that are created for the VSS_FREE virtual host, you must assign those volumes to VSS_FREE.

Verifying the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service Windows installation

This task verifies that the services that you selected to install are correctly installed on your system. During installation, you had the option to install Microsoft Volume Shadow Copy Service, Microsoft Virtual Disk Services, or both.

Perform the following steps to verify the installation of the services that you selected to install:

1. If verifying Microsoft Volume Shadow Copy Service installation, select **Start** -> **All Programs** -> **Administrative Tools** -> **Services**
2. Ensure that there is a service named IBM System Storage Support for Microsoft Volume Shadow Copy that is listed, and that the Status is Started and the Startup Type is Automatic.



3. Open a command prompt window and type the following command to verify that DS Open API Support for Microsoft Volume Shadow Copy and Virtual Disk Services is installed:

   ```
   vssadmin list providers
   ```

   Ensure each service that you installed is listed as a provider.

If you are able to perform all of these verification tasks successfully, either Microsoft Volume Shadow Copy, Virtual Disk Services, or both, have been successfully installed on your Windows system.

Verifying IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service Windows configuration

This task verifies that Microsoft Volume Shadow Copy and Virtual Disk Services are configured correctly on your Windows system.

After you have created the VSS_FREE and VSS_RESERVED pools for Microsoft Volume Shadow Copy Service, perform the following steps to verify your configuration:

1. Issue the following command:

   ```
   ibmvcfg listvols
   ```

   All of the volumes on your storage unit are listed with the WWPNs that they are assigned to.
2. If the volumes are not listed, check the connectivity of your CIM agent. Then, check your IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service configuration. You can reconfigure using the commands that are listed in the next section. The IBMVSS.log provides more detailed information on which of the settings is incorrect. IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service do not work if this command does not complete successfully.

Result:

If you are able to perform all of the verification tasks successfully, Microsoft Volume Shadow Copy and Virtual Disk Services has been successfully configured on your Windows system.

IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service reconfiguration commands

After installation, you can use several commands on the ibmvcfg.exe tool to change or correct parameters that you used to install the Microsoft Volume Shadow Copy and Virtual Disk Services. To do this, you must use the utility ibmvcfg.exe. You do not have to set many of the settings because there are defaults that are provided for them in Microsoft Volume Shadow Copy and Virtual Disk Services. Table 22 shows the commands that you can use for reconfiguration.

Note: If you do not know which settings to provide (for example, passwords or user names) for the following commands, contact your system administrator.

Table 22. Microsoft Volume Shadow Copy and Virtual Disk Services reconfiguration commands

Command	Description	Example
ibmvcfg showcfg	Provides the current settings.	
CIMOM settings		
ibmvcfg set username <CIMOM username>	Sets the CIMOM user name.	`ibmvcfg set username johnny`
ibmvcfg set password <CIMOM password>	Sets the CIMOM user password.	`ibmvcfg set password mypassword`
ibmvcfg set usingSSL	Specifies whether to use Secure Socket Layers to connect to the CIMOM.	`ibmvcfg set usingSSL yes`
ibmvcfg set cimomPort <portnum>	Specifies the CIMOM port number. The default value is 5989.	`ibmvcfg set cimomPort 5989`
ibmvcfg set cimomHost <server name>	Sets the name of the CIMOM server.	`ibmvcfg set cimomHost cimomserver`

Table 22. Microsoft Volume Shadow Copy and Virtual Disk Services reconfiguration commands (continued)

Command	Description	Example
ibmvcfg set namespace <namespace>	Specifies the namespace value that CIMOM is using. The default value is `\root\ibm`.	`ibmvcfg set namespace \root\ibm`
Volume Shadow Copy Service settings		

ibmvcfg listvols	Lists the volumes that are currently in the freepool, unassigned, or all volumes. By default, without any additional parameters, this command lists all of the volumes.	`ibmvcfg listvols`
		`ibmvcfg listvols free`
		`ibmvcfg listvols unassigned`
		`ibmvcfg listvols all`

ibmvcfg listvols free	Lists the volumes that are currently in the freepool, unassigned, or both.	`ibmvcfg listvols free`
ibmvcfg listvols unassigned	Lists the volumes that are currently in the freepool, unassigned, or both.	`ibmvcfg listvols unassigned`
ibmvcfg add	Adds a volume or volumes to the freepool.	`ibmvcfg add 12312345 32112345`
ibmvcfg rem	Removes a volume or volumes from the freepool.	`ibmvcfg rem 512` `ibmvcfg rem 51212345`
ibmvcfg set vssFreeInitiator <WWPN>	Specifies the WWPN that designates the freepool. The default value is `5000000000000000`. Modify this value only if there is a host already in your environment with a WWPN of 5000000000000000.	`ibmvcfg set vssFreeInitiator 5000000000000000`
ibmvcfg set vssReservedInitiator <WWPN>	Specifies the WWPN that designates the reservedpool. The default value is `5000000000000001`. Modify this value only if there is a host already in your environment with a WWPN of 5000000000000001.	`ibmvcfg set vssFreeInitiator 5000000000000001`

Table 22. Microsoft Volume Shadow Copy and Virtual Disk Services reconfiguration commands (continued)

Command	Description	Example
ibmvcfg set FlashCopyVer <1 | 2>	Sets the FlaschCopy version that is available on the storage unit. The default value is 1.	`ibmvcfg set FlashCopyVer 1`
Virtual Disk Service settings		
None		

Error codes returned by Microsoft Volume Shadow Copy and Virtual Disk Services

Return Error Codes

Table 23 lists Microsoft Volume Shadow Copy and Virtual Disk Services error codes.

Note: These errors are logged in the Windows Event Monitor and in the Microsoft Volume Shadow Copy and Virtual Disk Services log file that located in the directory chosen during installatin.

Table 23. Return error codes for Microsoft Volume Shadow Copy and Virtual Disk Services

Symbolic Name	Code	Definition
ERR_JVM	1000	JVM Creation failed.
ERR_CLASS_NOT_FOUND	1001	Class not found: %1.
ERR_MISSING_PARAMS	1002	Some required parameters are missing.
ERR_METHOD_NOT_FOUND	1003	Method not found: %1.
ERR_REQUIRED_PARAM	1004	A missing parameter is required. Use the configuration utility to set this parameter: %1.
ERR_RECOVERY_FILE_CREATION_FAILED	1600	The recovery file was not created.
ERR_ARELUNSSUPPORTED_IBMGETLUNINFO	1700	ibmGetLunInfo failed in AreLunsSupported.
ERR_FILLLUNINFO_IBMGETLUNINFO	1800	ibmGetLunInfo failed in FillLunInfo.
ERR_GET_TGT_CLEANUP	1900	Failed to delete the following temp files: %1
ERR_LOG_SETUP	2500	Error initializing log.
ERR_CLEANUP_LOCATE	2501	Unable to search for incomplete Shadow Copies. Windows Error: %1.

Table 23. Return error codes for Microsoft Volume Shadow Copy and Virtual Disk Services (continued)

Symbolic Name	Code	Definition
ERR_CLEANUP_READ	2502	Unable to read incomplete Shadow Copy Set information from file: %1.
ERR_CLEANUP_SNAPSHOT	2503	Unable to cleanup snapshot stored in file: %1.
ERR_CLEANUP_FAILED	2504	Cleanup call failed with error: %1.
ERR_CLEANUP_OPEN	2505	Unable to open file: %1.
ERR_CLEANUP_CREATE	2506	Unable to create file: %1.
ERR_HBAAPI_LOAD	2507	HBA: Error loading hba library: %1.
ERR_ESSSERVICE_EXCEPTION	3000	ESSService: An exception occurred. Check the ESSService log.
ERR_ESSSERVICE_LOGGING	3001	ESSService: Unable to initialize logging.
ERR_ESSSERVICE_CONNECT	3002	ESSService: Unable to connect to the CIM agent. Check your configuration.
ERR_ESSSERVICE_SCS	3003	ESSService: Unable to get the Storage Configuration Service. Check your configuration.
ERR_ESSSERVICE_INTERNAL	3004	ESSService: An internal error occurred with the following information: %1.
ERR_ESSSERVICE_FREE_CONTROLLER	3005	ESSService: Unable to find the VSS_FREE controller.
ERR_ESSSERVICE_RESERVED_CONTROLLER	3006	ESSService: Unable to find the VSS_RESERVED controller. Check your configuration.
ERR_ESSSERVICE_INSUFFICIENT_TARGETS	3007	Unable to find suitable targets for all volumes.
ERR_ESSSERVICE_ASSIGN_FAILED	3008	ESSService: The assign operation failed. Check the CIM agent log for details.
ERR_ESSSERVICE_WITHDRAW_FAILED	3009	ESSService: The withdraw FlashCopy operation failed. Check the CIM agent log for details.

Uninstalling the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service on Windows

Use the steps below to uninstall VSS or VDS services.

1. Log on to your system as the local administrator.
2. Click **Start -> Control Panel**.
3. The Control Panel window opens. Double-click on **Add or Remove Programs** and then select **IBM IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service**. Click **Remove** to remove the program.
4. Select **Yes** when you are asked if you want to completely remove the selected application and all of it components, or click **No** to go back to the Add or Remove Programs window.
5. The progress window quickly opens and closes.
6. The Finish window opens. Click **Finish**. The removal is now complete.

If you are able to perform all of the uninstallation tasks successfully, Microsoft Volume Shadow Copy and Virtual Disk Services have been successfully uninstalled on your Windows system.

Accessibility

Accessibility features provide users who have disabilities with the ability to successfully access information and use technology.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

Features

These are the major accessibility features in the IBM System Storage DS8000 information:

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. IBM Home Page Reader version 3.0 has been tested.
- You can operate features using the keyboard instead of the mouse.

Navigating by keyboard

You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the IBM System Storage DS8000 information from the keyboard by using the shortcut keys for your browser or Home Page Reader. See your browser Help for a list of shortcut keys that it supports. See the following Web site for a list of shortcut keys supported by Home Page Reader: http://www-306.ibm.com/able/solution_offerings/keyshort.html

Accessing the publications

You can find HTML versions of the IBM System Storage DS8000 information at the following Web site: http://www.ehone.ibm.com/public/applications/publications/cgibin/pbi.cgi

You can access the information using IBM Home Page Reader 3.0.

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 give 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.

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 PUBLICATIONS "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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been

estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these Publications for your personal, non commercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these Publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these Publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these Publications, or reproduce, distribute or display these Publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the Publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- AIX
- DB2
- DFSMS/MVS
- DFSMS/VM
- DS4000
- DS6000
- DS8000
- e (logo)
- Enterprise Storage Server
- ES/9000
- ESCON
- FICON
- FlashCopy
- Graphically Dispersed Parallel Sysplex
- HACMP
- i5/OS
- IBM
- IntelliStation
- MVS/ESA
- Netfinity
- NetVista
- Operating System/400
- OS/400
- RS/6000
- S/390
- Seascape
- SNAP/SHOT
- SP
- System/390
- System p5
- System Storage
- Versatile Storage Server
- Virtualization Engine
- VSE/ESA
- z/Architecture
- z/OS
- z/VM
- zSeries

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This equipment has been tested and complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the users authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European community contact:

IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
E-mail: tjahn@de.ibm.com

Germany compliance statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit.

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japanese Voluntary Control Council for Interference (VCCI) class A statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Ministry of Information and Communication (MIC) statement

Please note that this device has been certified for business use with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for one of residential use.

Taiwan class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。 VS07171L

Taiwan Contact Information

This topic contains the product service contact information for Taiwan.

```
IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888
```

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Java Compatibility logo

The Java Compatibility logo identifies products that incorporate a Java application environment (JDK or JRE). These products pass the applicable, JavaSoft defined, Java Compatibility test suite in order to enable execution of Java or Personal Java (pJava) applications.

Glossary

This glossary includes terms for the IBM System Storage and other Resiliency Family products.

This glossary includes selected terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172–1990, copyright 1990 by the American National Standards Institute (ANSI), 11 West 42nd Street, New York, New York 10036. Definitions derived from this book have the symbol (A) after the definition.
- *IBM Terminology*, which is available online at the following Web site: http://w3-03.ibm.com/globalization/page/1728. Definitions derived from this source have the symbol (GC) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions derived from this book have the symbol (I) after the definition. Definitions taken from draft international standards, committee drafts, and working papers that the ISO/IEC JTC1/SC1 is developing have the symbol (T) after the definition, indicating that final agreement has not been reached among the participating National Bodies of SC1.

This glossary uses the following cross-reference forms:

See Refers the reader to one of two kinds of related information:

- A term that is the expanded form of an abbreviation or acronym. This expanded form of the term contains the full definition.
- A synonym or more preferred term

See also
Refers the reader to one or more related terms.

Contrast with
Refers the reader to a term that has an opposite or substantively different meaning.

Numerics

750 A model of the Enterprise Storage Server featuring a 2-way processor with limited physical storage capacity. This model can be updated to the model 800.

800 A model of the Enterprise Storage Server featuring a standard processor or an optional Turbo processor. The Model 800 supports RAID 5, RAID 10, and 15000 rpm drives. Model 800 supersedes Model F20.

1750 The machine type for the IBM System Storage DS6000 series. Models for the DS6000 include the 511 and EX1.

2105 The machine number for the IBM TotalStorage Enterprise Storage Server. Models of the Enterprise Storage Server are expressed as the number 2105 followed by "Model <*xxx*>", such as 2105 Model 800. The 2105 Model 100 is an Enterprise Storage Server expansion enclosure that is typically referred to simply as the Model 100.

2107 A hardware machine type for the IBM System Storage DS8000 series. Hardware models for the 2107 include base units 921, 922, 931, 932, 9A2, 9B2 and expansion units 92E and 9AE.

2244 A function authorization machine type for the IBM System Storage DS8000 series. The 2244 function authorization machine type corresponds with the 2107 hardware machine type and is used only for purposes of billing and authorizing the licensed functions on the 2107. Function authorization models for the 2244 are related to the type of licensed functions that you order. For example, Model RMC is for the remote mirror and copy function on a 2107 storage unit.

239x Function authorization machine types for the IBM System Storage DS8000 series. These machine types indicate the

warranty period for the licensed functions and they include the following machine types: 2396 (one-year warranty), 2397 (two-year warranty), 2398 (3-year warranty), and 2399 (four-year warranty). Each 239x function authorization machine type corresponds to the 242x hardware machine type that represents the same warranty period. For example, you order a 2398 (3-year warranty) function authorization machine type for a 2423 (3-year warranty) hardware machine. The 239x machine types are used only for purposes of billing and authorizing the licensed functions on the 242x machines. The 239x machine types have one model (Model LFA) with several types of available licenses for that model. For example, Model LFA, RMC license is for the remote mirror and copy function on a 242x storage unit.

242x Hardware machine types for the IBM System Storage DS8000 series. The 242x hardware machine types include machine types 2421 (one-year warranty), 2422 (two-year warranty), 2423 (3-year warranty), and 2424 (four-year warranty). Hardware models for the 242x machine types include base units 931, 932, 9B2 and expansion units 92E and 9AE.

3390 The machine number of an IBM disk storage system. The Enterprise Storage Server, when interfaced to IBM zSeries hosts, is set up to appear as one or more 3390 devices, with a choice of 3390-2, 3390-3, or 3390-9 track formats.

3990 The machine number of an IBM control unit.

7133 The machine number of an IBM disk storage system. The Model D40 and 020 drawers of the 7133 can be installed in the 2105-100 expansion enclosure of the ESS.

A

access 1) To obtain computing services or data.

2) In computer security, a specific type of interaction between a subject and an object that results in flow of information from one to the other.

access-any mode
One of the two access modes that can be set for the storage unit during initial configuration. It enables all fibre-channel-attached host systems with no defined access profile to access all logical volumes on the storage unit. With a profile defined in DS Storage Manager for a particular host, that host has access only to volumes that are assigned to the WWPN for that host. See also *pseudo host* and *worldwide port name*.

ACK See *request for acknowledgment and acknowledgment*.

agent A program that automatically performs some service without user intervention or on a regular schedule. See also *subagent*.

alert A message or log that a storage unit generates as the result of error event collection and analysis. An alert indicates that a service action is required.

allegiance
For zSeries, a relationship that is created between a device and one or more channel paths during the processing of certain conditions. See also *implicit allegiance*, *contingent allegiance*, and *reserved allegiance*.

allocated storage
The space that is allocated to volumes but not yet assigned. Contrast with *assigned storage*.

American National Standards Institute (ANSI)
An organization of producers, consumers, and general interest groups that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

anonymous
In the DS Storage Manager, the label on an icon that represents all connections that are using fibre-channel adapters between the storage unit and hosts but are not completely defined to the storage unit. See also *anonymous host*, *pseudo host*, and *access-any mode*.

anonymous host
Synonym for *pseudo host*. Contrast with *anonymous* and *pseudo host*.

ANSI See *American National Standards Institute*.

APAR See *authorized program analysis report*. (GC)

API See *application programming interface*.

application programming interface
An interface that allows an application program that is written in a high-level language to use specific data or functions of the operating system or another program.

arbitrated loop
A fibre-channel topology that enables the interconnection of a set of nodes. See also *point-to-point connection* and *switched fabric*.

array An ordered collection, or group, of physical devices (disk drive modules) that is used to define logical volumes or devices. In the storage unit, an array is a group of disks that the user designates to be managed by the RAID technique. See also *redundant array of independent disks*.

ASCII (American National Standard Code for Information Interchange) The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A) Some organizations, including IBM, have used the parity bit to expand the basic code set.

assigned storage
The space that is allocated to a volume and that is assigned to a port.

authorized program analysis report (APAR)
A request for correction of a defect in a current release of an IBM-supplied program. (GC)

availability
The degree to which a system or resource is capable of performing its normal function. See *data availability*.

B

bay The physical space that is used for installing SCSI, ESCON, and fibre-channel host adapter cards. The DS8000 storage unit has four bays, two in each cluster. See also *service boundary*.

bit The smallest unit of computer information, which has two possible states that are represented by the binary digits 0 or 1. See also *byte*.

block A string of data elements recorded or transmitted as a unit. The elements may be characters, words, or physical records. (GC)

A group of consecutive bytes used as the basic storage unit in fixed-block architecture (FBA). All blocks on the storage device are the same size (fixed size). See also *fixed-block architecture* and *data record*.

byte A string that represents a character and usually consists of eight binary digits that are treated as a unit. A byte is the smallest unit of storage that can be addressed directly. (GC) See also *bit*.

C

cache A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (GC)

cache fast write
A form of the fast-write operation in which the storage server writes the data directly to cache, where it is available for later destaging.

cache hit
An event that occurs when a read operation is sent to the cluster, and the requested data is found in cache. Contrast with *cache miss*.

cache memory
Memory, typically volatile memory, that a storage server uses to improve access times to instructions or data. The cache memory is typically smaller and faster than the primary memory or storage medium. In addition to residing in cache memory, the same data also resides on the storage devices in the storage unit.

cache miss
An event that occurs when a read operation is sent to the cluster, but the data is not found in cache. Contrast with *cache hit*.

call home
A communication link established between the storage product and a service provider. The storage product can use this link to place a call to IBM or to another service provider when it requires service.

With access to the machine, service personnel can perform service tasks, such as viewing error logs and problem logs or initiating trace and dump retrievals. (GC) See also *heartbeat* and *remote technical assistance information network*.

cascading
1) Connecting network controllers to each other in a succession of levels to concentrate many more lines than a single level permits.

2) In high-availability cluster multiprocessing (HACMP), pertaining to a cluster configuration in which the cluster node with the highest priority for a particular resource acquires the resource if the primary node fails. The cluster node relinquishes the resource to the primary node upon reintegration of the primary node into the cluster.

catcher
A server that service personnel use to collect and retain status data that an DS8000 sends to it.

CCR See *channel command retry*.

CCW See *channel command word*.

CD See *compact disc*.

central electronics complex
The set of hardware facilities that are associated with a host computer.

channel
The part of a channel subsystem that manages a single I/O interface between a channel subsystem and a set of control units.

channel command retry (CCR)
The protocol used between a channel and a control unit that enables the control unit to request that the channel reissue the current command.

channel command word (CCW)
A data structure that specifies an I/O operation to the channel subsystem.

channel path
The interconnection between a channel and its associated control units.

channel subsystem
The part of a host computer that manages I/O communication between the program and any attached control units.

channel-subsystem image
In mainframe computing, the logical functions that a system requires to perform the function of a channel subsystem. With ESCON multiple image facility (EMIF), one channel subsystem image exists in the channel subsystem for each logical partition (LPAR). Each image appears to be an independent channel subsystem program, but all images share a common set of hardware facilities. (GC)

CKD See *count key data*.

CLI See *command-line interface*. See also *IBM System Storage DS CLI.*

cluster
1) A partition capable of performing all DS8000 series functions. With two clusters in the DS8000 storage unit, any operational cluster can take over the processing of a failing cluster.

cluster processor complex
The unit within a cluster that provides the management function for the DS8000 series. It consists of cluster processors, cluster memory, and related logic.

command-line interface (CLI)
An interface that defines a set of commands and enables a user (or a script-like language) to issue these commands by typing text in response to the command prompt (for example, DOS commands or UNIX shell commands). See also *IBM System Storage DS CLI*.

compact disc
An optically read disc, typically storing approximately 660 MB. CD-ROM (compact disc read-only memory) refers to the read-only format used to distribute DS8000 series code and documentation.

compression
1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks.

2) Any encoding that reduces the number of bits used to represent a given message or record. (GC)

concurrent copy
A facility on a storage server that enables a program to make a backup of a data set while the logical volume remains

available for subsequent processing. The data in the backup copy is frozen at the point in time that the server responds to the request.

concurrent installation of licensed internal code
Process of installing licensed internal code on a DS8000 series while applications continue to run.

concurrent maintenance
Service that is performed on a unit while it is operational.

concurrent media maintenance
Service performed on a disk drive module (DDM) without losing access to the data.

configure
In storage, to define the logical and physical devices, optional features, and program products of the input/output subsystem through the user interface that the storage unit provides for this function.

consistency group
A group of volumes participating in FlashCopy relationships in a logical subsystem, across logical subsystems, or across multiple storage units that must be kept in a consistent state to ensure data integrity.

consistency group interval time
The value in seconds that indicates the length of time between the formation of consistency groups.

consistent copy
A copy of a data entity (a logical volume, for example) that contains the contents of the entire data entity at a single instant in time.

console
A user interface to a server, for example, the interface provided on a personal computer. See also *IBM System Storage Management Console*.

contingent allegiance
In mainframe computing, a relationship that is created in a control unit between a device and a channel when the channel accepts unit-check status. The allegiance causes the control unit to guarantee access; the control unit does not present the busy status to the device. The allegiance enables the channel to retrieve sense data that is associated with the unit-check status on the channel path associated with the allegiance. (GC)

control path
The route that is established from the master storage unit to the subordinate storage unit when more than one storage unit participates in a Global Mirror session. If there is only one storage unit (the master) in the Global Mirror session, no control path is required.

control unit (CU)
1) A device that coordinates and controls the operation of one or more input/output devices, and synchronizes the operation of such devices with the operation of the system as a whole.

2) For zSeries, a storage server with ESCON or OEMI interfaces. The control unit adapts a native device interface to an I/O interface that a zSeries host system supports.

3) The portion of the storage unit that supports the attachment of emulated count key data devices over ESCON, FICON, or OEMI interfaces. See also *cluster*.

control-unit image
In mainframe computing, a logical subsystem that is accessed through an ESCON I/O interface. One or more control-unit images exist in each control unit. Each image appears as an independent control unit, but all control-unit images share a common set of hardware facilities. The DS8000 series can emulate 3990-3, TPF, 3990-6, or 2105 control units.

control-unit-initiated reconfiguration (CUIR)
A software mechanism that the DS8000 series uses to request that an operating system of a zSeries host verify that one or more subsystem resources can be taken offline for service. The DS8000 series can use this process to automatically vary channel paths offline and online to facilitate bay service or concurrent code installation. Depending on the operating system, support for this process might be model dependent, might depend on the IBM TotalStorage Enterprise Storage Server Subsystem Device Driver, or might not exist.

Coordinated Universal Time (UTC)
The international standard of time that is kept by atomic clocks around the world.

Copy Services
A collection of optional software features, with a Web-browser interface, that is used for configuring, managing, and monitoring data-copy functions.

count field
The first field of a count key data (CKD) record. This eight-byte field contains a four-byte track address (CCHH). It defines the cylinder and head that are associated with the track, and a one-byte record number (R) that identifies the record on the track. It defines a one-byte key length that specifies the length of the record's key field (0 means no key field). It defines a two-byte data length that specifies the length of the record's data field (0 means no data field). Only the end-of-file record has a data length of zero.

count key data (CKD)
In mainframe computing, a data-record format employing self-defining record formats in which each record is represented by up to three fields: a *count* field that identifies the record and specifies its format, an optional *key* field that identifies the data area contents, and an optional *data* field that typically contains the user data. For CKD records on the storage unit, the logical volume size is defined in terms of the device emulation mode (3390 or 3380 track format). The count field is always 8 bytes long and contains the lengths of the key and data fields, the key field has a length of 0 to 255 bytes, and the data field has a length of 0 to 65 535 or the maximum that will fit on the track. See also *data record*.

CPC See *cluster processor complex*.

CRC See *cyclic redundancy check*.

CU See *control unit*.

CUIR See *control-unit initiated reconfiguration*.

custom volume
A volume in count-key-data (CKD) format that is not a standard volume, which means that it does not necessarily present the same number of cylinders and capacity to its assigned logical control unit as provided by one of the following standard zSeries volume types: 3390-2, 3390-3, 3390-9, 3390-2 (3380-track mode), or 3390-3 (3380-track mode). See also *count-key-data*, *interleave*, *standard volume*, and *volume*.

CUT See *Coordinated Universal Time*.

cyclic redundancy check (CRC)
A redundancy check in which the check key is generated by a cyclic algorithm. (T)

cylinder
A unit of storage on a CKD device with a fixed number of tracks.

D

DA See *device adapter*.

daisy chain
See *serial connection*.

DASD
See *direct access storage device*.

DASD fast write (DFW)
A function of a storage server in which active write data is stored in nonvolatile cache, thus avoiding exposure to data loss.

data availability
The degree to which data is available when needed, typically measured as a percentage of time that the system would be capable of responding to any data request (for example, 99.999% available).

data compression
A technique or algorithm used to encode data such that the encoded result can be stored in less space than the original data. The original data can be recovered from the encoded result through a reverse technique or reverse algorithm. See also *compression*.

Data Facility Storage Management Subsystem (DFSMS)
An operating environment that helps automate and centralize the management of storage. To manage storage, DFSMS provides the storage administrator with control over data class, storage class, management class, storage group, and automatic class selection routine definitions.

data field
The optional third field of a count key data (CKD) record. The count field specifies the length of the data field. The data field contains data that the program writes.

data record
The basic unit of zSeries storage on a DS8000, also known as a count-key-data (CKD) record. Data records are stored on a track. The records are sequentially numbered starting with 0. The first record, R0, is typically called the track descriptor record and contains data that the operating system normally uses to manage the track. See also *count-key-data* and *fixed-block architecture*.

data set FlashCopy
For zSeries hosts, a feature of FlashCopy that indicates how many partial volume FlashCopy relationships are active on a volume.

data sharing
The ability of multiple host systems to concurrently utilize data that they store on one or more storage devices. The storage unit enables configured storage to be accessible to any, or all, attached host systems. To use this capability, the host program must be designed to support data that it is sharing.

DDM See *disk drive module*.

DDM group
See *disk pack*.

dedicated storage
Storage within a storage unit that is configured such that a single host system has exclusive access to the storage.

demote
To remove a logical data unit from cache memory. A storage server demotes a data unit to make room for other logical data units in the cache or because the logical data unit is not valid. The storage unit must destage logical data units with active write units before they can be demoted. See also *destage*.

destage
To move data from an online or higher priority to an offline or lower priority device. The storage unit stages incoming data into cache and then destages it to disk.

device For zSeries, a disk drive.

device adapter (DA)
A physical component of the DS8000 that provides communication between the clusters and the storage devices. The DS8000 has eight device adapters that it deploys in pairs, one from each cluster. Device adapter pairing enables the DS8000 to access any disk drive from either of two paths, providing fault tolerance and enhanced availability.

device address
For zSeries, the field of an ESCON device-level frame that selects a specific device on a control-unit image.

device ID
The unique two-digit hexadecimal number that identifies the logical device.

device interface card
A physical subunit of a storage cluster that provides the communication with the attached device drive modules.

device number
For zSeries, a four-hexadecimal-character identifier, for example 13A0, that the systems administrator associates with a device to facilitate communication between the program and the host operator. The device number is associated with a subchannel.

device sparing
A subsystem function that automatically copies data from a failing device drive module to a spare device drive module. The subsystem maintains data access during the process.

DFS See *distributed file service*.

DFSMS
See *Data Facility Storage Management Subsystem*.

direct access storage device (DASD)
1) A mass storage medium on which a computer stores data.

2) A disk device.

disk cage
A container for disk drives. Each disk cage supports eight disk packs (64 disks).

disk drive
Standard term for a disk-based nonvolatile storage medium. The DS8000 series use hard disk drives as the primary nonvolatile storage media to store host data.

disk drive module (DDM)
A field replaceable unit that consists of a single disk drive and its associated packaging.

disk drive module group
See *disk pack*.

disk drive set
A specific number of identical disk drives that have the same physical capacity and rpm.

disk pack
A group of disk drive modules (DDMs) installed as a unit in a DDM bay.

disk group
A collection of 4 disk drives that are connected to the same pair of IBM Serial Storage adapters and can be used to create a RAID array. A disk group can be formatted as count key data or fixed block, and as RAID or non-RAID, or it can be left unformatted. A disk group is a logical assemblage of disk drives. Contrast with *disk pack*.

distributed file service (DFS)
A service that provides data access over IP networks.

DNS See *domain name system*.

domain
1) That part of a computer network in which the data processing resources are under common control.

2) In TCP/IP, the naming system used in hierarchical networks.

domain name system (DNS)
In TCP/IP, the server program that supplies name-to-address translation by mapping domain names to internet addresses. The address of a DNS server is the internet address of the server that hosts the DNS software for the network.

dotted decimal notation
A convention used to identify IP addresses. The notation consists of four 8-bit numbers written in base 10. For example, `9.113.76.250` is an IP address that contains the octets 9, 113, 76, and 250.

drawer
A unit that contains multiple device drive modules and provides power, cooling, and related interconnection logic to make the device drive modules accessible to attached host systems.

drive 1) A peripheral device, especially one that has addressed storage media. See also *disk drive module*.

2) The mechanism used to seek, read, and write information on a storage medium.

DS8000 series
See *IBM System Storage DS8000*.

DS8000 Batch Configuration tool
A program that automatically configures a DS8000 storage unit. The configuration is based on data that IBM service personnel enter into the program.

DS Storage Manager
See *IBM System Storage DS Storage Manager*.

duplex
1) Regarding Copy Services, the state of a volume pair after Remote Mirror and Copy has completed the copy operation and the volume pair is synchronized.

2) In general, pertaining to a communication mode in which data can be sent and received at the same time.

dynamic sparing
The ability of a storage server to move data from a failing disk drive module (DDM) to a spare DDM while maintaining storage functions.

E

E10 The predecessor of the F10 model of the Enterprise Storage Server. See also *F10*.

E20 The predecessor of the F20 model of the Enterprise Storage Server. See also *F20*.

EC See *engineering change*.

ECKD See *extended count key data*.

eight pack
See *disk pack*.

electrostatic discharge (ESD)
An undesirable discharge of static

electricity that can damage equipment and degrade electrical circuitry.

emergency power off (EPO)
A means of turning off power during an emergency, usually a switch.

EMIF See *ESCON multiple image facility*.

enclosure
A unit that houses the components of a storage subsystem, such as a control unit, disk drives, and power source.

end of file
A coded character recorded on a data medium to indicate the end of the medium. On a count-key-data direct access storage device, the subsystem indicates the end of a file by including a record with a data length of zero.

engineering change (EC)
An update to a machine, part, or program.

Enterprise Systems Architecture/390 (ESA/390)
An IBM architecture for mainframe computers and peripherals. Processor systems that follow the ESA/390 architecture include the ES/9000® family. See also *z/Architecture*.

Enterprise Systems Connection (ESCON)
1) A zSeries computer peripheral interface. The I/O interface uses zSeries logical protocols over a serial interface that configures attached units to a communication fabric.

2) A set of IBM products and services that provide a dynamically connected environment within an enterprise.

EPO See *emergency power off*.

ERDS See *error-recording data set*.

error-recording data set (ERDS)
On zSeries hosts, a data set that records data-storage and data-retrieval errors. A service information message (SIM) provides the error information for the ERDS.

error recovery procedure
Procedures designed to help isolate and, where possible, to recover from errors in equipment. The procedures are often used in conjunction with programs that record information on machine malfunctions.

ESA/390
See *Enterprise Systems Architecture/390*.

ESCD See *ESCON director*.

ESCON
See *Enterprise System Connection*.

ESCON channel
A zSeries channel that supports ESCON protocols.

ESCON director (ESCD)
An I/O interface switch that allows the interconnection of multiple ESCON interfaces in a distributed-star topology.

ESCON host systems
zSeries hosts that attach to the DS8000 series with an ESCON adapter. Such host systems run on operating systems that include MVS, VSE, TPF, or versions of VM.

ESCON multiple image facility (EMIF)
For zSeries, a function that enables LPARs to share an ESCON channel path by providing each LPAR with its own channel-subsystem image.

EsconNet
In the DS Storage Manager, the label on a pseudo host icon that represents a host connection that uses the ESCON protocol and that is not completely defined on the DS8000. See also *pseudo host* and *access-any mode*.

ESD See *electrostatic discharge*.

eServer
See *IBM eServer*.

ESSNet
See *IBM TotalStorage Enterprise Storage Server Network*.

extended count key data (ECKD)
An extension of the count key data (CKD) architecture.

extent A continuous space on a disk that is occupied by or reserved for a particular data set, data space, or file. The unit of increment is a track. See also *multiple allegiance* and *parallel access volumes*.

extent pool
A groups of extents. See also *extent*.

F

fabric In fibre channel technology, a routing

structure, such as a switch, receives addressed information and routes to the appropriate destination. A fabric can consist of more than one switch. When multiple fibre-channel switches are interconnected, they are said to be *cascaded*.

failback
Pertaining to a cluster recovery from failover following repair. See also *failover*.

failover
Pertaining to the process of transferring all control to a single cluster when the other cluster in the storage unit fails. See also *cluster* and *failback*.

fast write
A write operation at cache speed that does not require immediate transfer of data to a disk drive. The subsystem writes the data directly to cache, to nonvolatile storage, or to both. The data is then available for destaging. A fast-write operation reduces the time an application must wait for the I/O operation to complete.

FATA See *fibre-channel ATA*.

FBA See *fixed-block architecture*.

FC See *feature code*. **Note**: *FC* is a common abbreviation for fibre channel in the industry, but the DS8000 customer documentation library reserves *FC* for feature code.

FC-AL See *Fibre Channel ATA*.

FCP See *Fibre Channel Protocol*.

FCS See *Fibre Channel standard*.

feature code (FC)
A code that identifies a particular orderable option and that is used by service personnel to process hardware and software orders. Individual optional features are each identified by a unique feature code.

fibre channel
A data-transmission architecture based on the ANSI Fibre Channel standard, which supports full-duplex communication. The DS8000 supports data transmission over fiber-optic cable through its fibre-channel adapters. See also *Fibre Channel Protocol* and *Fibre Channel standard*.

fibre-channel ATA (FATA)
A hard drive that combines a fibre channel interface with an ATA drive. FATAs, which provide the high performance and capacity of an ATA drive, can be used wherever fibre channel drives can connect.

Fibre Channel Arbitrated Loop (FC-AL)
An implementation of the Fibre Channel Standard that uses a ring topology for the communication fabric. Refer to American National Standards Institute (ANSI) X3T11/93-275. In this topology, two or more fibre-channel end points are interconnected through a looped interface. This topology directly connects the storage unit to an open systems host without going through a fabric switch.

Fibre Channel Connection (FICON)
A fibre-channel communications protocol that is designed for IBM mainframe computers and peripherals. It connects the storage unit to one or more S/390 hosts using a FICON S/390 channel either directly or through a FICON switch.

Fibre Channel Protocol (FCP)
A protocol used in fibre-channel communications with five layers that define how fibre-channel ports interact through their physical links to communicate with other ports.

Fibre Channel standard (FCS)
An ANSI standard for a computer peripheral interface. The I/O interface defines a protocol for communication over a serial interface that configures attached units to a communication fabric. The protocol has two layers. The IP layer defines basic interconnection protocols. The upper layer supports one or more logical protocols (for example, FCP for SCSI command protocols and SBCON for zSeries command protocols). Refer to American National Standards Institute (ANSI) X3.230-199x. See also *Fibre Channel Protocol*.

fibre-channel topology
An interconnection topology supported on fibre-channel adapters. See also *point-to-point connection*, *switched fabric*, and *arbitrated loop*.

Fibre Channel Switched Fabric (FC-SF)
An implementation of the Fibre Channel

Standard that connects the storage unit to one or more open systems hosts through a fabric switch or connects one or more S/390 hosts that run LINUX on an Fibre Channel Protocol S/390 channel.

FICON
See *fibre-channel connection*.

FiconNet
In the DS Storage Manager, the label on a pseudo host icon that represents a host connection that uses the FICON protocol and that is not completely defined on the DS8000 series. See also *pseudo host* and *access-any mode*.

field replaceable unit (FRU)
An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit might contain other field replaceable units. (GC)

FIFO See *first-in-first-out*.

File Transfer Protocol (FTP)
In TCP/IP, an application protocol used to transfer files to and from host computers. See also *Transmission Control Protocol/Internet Protocol*.

firewall
A protection against unauthorized connection to a computer or a data storage system. The protection is usually in the form of software on a gateway server that grants access to users who meet authorization criteria.

first-in-first-out (FIFO)
A queuing technique in which the next item to be retrieved is the item that has been in the queue for the longest time. (A)

fixed-block architecture (FBA)
An architecture for logical devices that specifies the format of and access mechanisms for the logical data units on the device. The logical data unit is a block. All blocks on the device are the same size (fixed size). The subsystem can access them independently.

fixed-block device
An architecture for logical devices that specifies the format of the logical data units on the device. The logical data unit is a block. All blocks on the device are the same size (fixed size); the subsystem can access them independently. This is the required format of the logical data units for host systems that attach with a SCSI or fibre-channel interface. See also *fibre channel* and *small computer systems interface*.

FlashCopy
An optional feature of the DS8000 series that can make an instant copy of data; that is, a point-in-time copy of a volume.

FlashCopy relationship
A mapping of a FlashCopy source volume and a FlashCopy target volume that allows a point-in-time copy of the source volume to be copied to the target volume. FlashCopy relationships exist from the time that you initiate a FlashCopy operation until the storage unit copies all data from the source volume to the target volume or until you delete the FlashCopy relationship, if it is persistent.

FRU See *field replaceable unit*.

FTP See *File Transfer Protocol*.

full duplex
See *duplex*.

fuzzy copy
A function of the Global Copy feature wherein modifications to the primary logical volume are performed on the secondary logical volume at a later time. The original order of update is not strictly maintained. See also *Global Copy*.

G

GB See *gigabyte*.

GDPS See *Geographically Dispersed Parallel Sysplex*.

Geographically Dispersed Parallel Sysplex (GDPS)
A zSeries multisite application-availability solution.

gigabyte (GB)
A gigabyte of storage is 10^9 bytes. A gigabyte of memory is 2^{30} bytes.

Global Copy
An optional capability of the DS8000 remote mirror and copy feature that maintains a fuzzy copy of a logical volume on the same DS8000 storage unit

or on another DS8000 storage unit. In other words, all modifications that any attached host performs on the primary logical volume are also performed on the secondary logical volume at a later point in time. The original order of update is not strictly maintained. See also *Remote Mirror and Copy* and *Metro Mirror*.

Global Mirror
An optional capability of the remote mirror and copy feature that provides a 2-site extended distance remote copy. Data that is written by the host to the storage unit at the local site is automatically maintained at the remote site. See also *Metro Mirror* and *Remote Mirror and Copy*.

group In DS8000 documentation, a nickname for two different kinds of groups, depending on the context. See *disk pack* or *Copy Services server group*.

H

HA See *host adapter*.

HACMP
See *high availability cluster multiprocessing*.

hard disk drive (HDD)
1) A storage medium within a storage server used to maintain information that the storage server requires.

2) A mass storage medium for computers that is typically available as a fixed disk (such as the disks used in system units of personal computers or in drives that are external to a personal computer) or a removable cartridge.

hardware service manager
An option on an AS/400 or iSeries host that enables the user to display and work with system hardware resources and to debug input-output processors (IOP), input-output adapters (IOA), and devices.

HCD See *Hardware Configuration Data*.

HDA See *head disk assembly*.

HDD See *hard disk drive*.

hdisk An AIX term for storage space.

head disk assembly (HDA)
The portion of an HDD associated with the medium and the read/write head.

heartbeat
A status report sent at regular intervals from the DS8000 storage unit. The service provider uses this report to monitor the health of the call home process. See also *call home*, *heartbeat call home record*, and *remote technical assistance information network*.

heartbeat call home record
Machine operating and service information sent to a service machine. These records might include such information as feature code information and product logical configuration information.

hierarchical storage management
1) A function in storage management software, such as Tivoli Storage Management or Data Facility Storage Management Subsystem/MVS (DFSMS/MVS), that automatically manages free space based on the policy that the storage administrator sets.

2) In AS/400 storage management, an automatic method to manage and distribute data between the different storage layers, such as disk units and tape library devices.

high availability cluster multiprocessing (HACMP)
Software that provides host clustering, so that a failure of one host is recovered by moving jobs to other hosts within the cluster.

high-speed loop (HSL)
A hardware connectivity architecture that links system processors to system input/output buses and other system units.

home address
A nine-byte field at the beginning of a track that contains information that identifies the physical track and its association with a cylinder.

hop Interswitch connection. A hop count is the number of connections that a particular block of data traverses between source and destination. For example, data traveling from one hub over a wire to another hub traverses one hop.

host See *host system*.

host adapter
A physical subunit of a storage server that provides the ability to attach to one or more host I/O interfaces.

host name
The Internet address of a machine in the network. The host name can be entered in the host definition as the fully qualified domain name of the attached host system, such as `mycomputer.city.company.com`, or as the subname of the fully qualified domain name, for example, `mycomputer`. See also *host system*.

host processor
A processor that controls all or part of a user application network. In a network, the processing unit in which the data communication access method resides. See also *host system*.

host system
A computer, either of the mainframe (for example, zSeries) or of the open-systems type, that is connected to the DS8000 series. Hosts are connected through ESCON, FICON, or fibre-channel interfaces.

hot plug
Pertaining to the ability to add or remove a hardware facility or resource to a unit while power is on.

HSL See *high-speed loop*.

HyperPAV (IBM HyperPAV)
An optional licensed function that you can use in conjunction with the parallel access volumes (PAV) function. IBM HyperPAV associates the volumes with either an alias address or a specified base logical volume number. When a host system requests IBM HyperPAV processing and the processing is enabled, aliases on the logical subsystem are placed in an IBM HyperPAV alias access state on all logical paths with a given path group ID. IBM HyperPAV is only supported on FICON channel paths.

i5/OS The IBM operating system that runs the IBM i5/OS and eServer i5 server families of servers.

IBM eServer
The IBM brand name for a series of server products that are optimized for e-commerce. The products include the iSeries, pSeries, xSeries, and zSeries.

IBM product engineering (PE)
The third-level of IBM service support. Product engineering is composed of IBM engineers who have experience in supporting a product or who are knowledgeable about the product.

IBM Serial Storage adapter
A physical adapter based on the IBM Serial Storage architecture. IBM Serial Storage adapters connect disk drive modules to DS8000 clusters.

IBM System Storage
The brand name used to identify storage products from IBM, including the IBM System Storage DS8000 series. See also *IBM System Storage DS8000* and *IBM System Storage DS Storage Manager*.

IBM System Storage DS8000
A member of the IBM System Storage Resiliency Family of storage servers and attached storage devices (disk drive modules). The DS8000 series storage product delivers high-performance, fault-tolerant storage and management of enterprise data, affording access through multiple concurrent operating systems and communication protocols. High performance is provided by multiple symmetrical multiprocessors, integrated caching, RAID support for the disk drive modules, and disk access through a high-speed serial storage architecture interface.

IBM System Storage DS CLI
The command-line interface (CLI) that works with DS8000, DS6000, and 2105 models.

IBM System Storage DS Storage Manager (DS Storage Manager)
Software with a Web-browser interface for configuring the DS8000 series.

IBM HyperPAV
See *HyperPAV*.

IBM TotalStorage Enterprise Storage Server Network (ESSNet)
A private network providing Web browser access to the Enterprise Storage Server. IBM installs the ESSNet software on an IBM workstation called the IBM

TotalStorage ESS Master Console, supplied with the first ESS delivery.

IBM System Storage Management Console (MC)
An IBM workstation that acts as the focal point for configuration, Copy Services management, and maintenance for the DS8000 series. It includes a Web browser that provides links to the user interface, including the DS Storage Manager and the DS8000 Copy Services.

IBM System Storage Multipath Subsystem Device Driver (SDD)
IBM software that provides multipath configuration support for a host system that is attached to storage devices. SDD provides enhanced data availability, dynamic input/output load balancing across multiple paths, and automatic path failover protection.

IBM System Storage Resiliency Family
A set of hardware and software features and products, as well as integrated software and services that are available on the IBM System Storage DS8000 series and the IBM TotalStorage Enterprise Storage Server, Models 750 and 800.

image See *storage image*.

IML See *initial microcode load*.

implicit allegiance
In Enterprise Systems Architecture/390, a relationship that a control unit creates between a device and a channel path when the device accepts a read or write operation. The control unit guarantees access to the channel program over the set of channel paths that it associates with the allegiance.

initial microcode load (IML)
The action of loading microcode for a computer into that computer's storage.

initial program load (IPL)
The action of loading software into a computer, typically an operating system that controls the computer.

initiator
A SCSI device that communicates with and controls one or more targets. Contrast with *target*.

i-node The internal structure in an AIX operating system that describes the individual files in the operating system. It contains the code, type, location, and owner of a file.

input/output (I/O)
Pertaining to (a) input, output, or both or (b) a device, process, or channel involved in data input, data output, or both.

input/output configuration data set
A configuration definition built by the I/O configuration program (IOCP) and stored on disk files associated with the processor controller.

interleave
To automatically create two striped partitions across the drives in a RAID-5 array, both of which use the count-key-data (CKD) record format.

Internet Protocol (IP)
In the Internet suite of protocols, a protocol without connections that routes data through a network or interconnecting networks and acts as an intermediary between the higher protocol layers and the physical network. The upper layer supports one or more logical protocols (for example, a SCSI-command protocol and a zSeries command protocol). Refer to ANSI X3.230-199*x*. The IP acronym is the IP in TCP/IP. See also *Transmission Control Protocol/Internet Protocol*.

invalidate
To remove a logical data unit from cache memory because it cannot support continued access to the logical data unit on the device. This removal might be the result of a failure within the storage server or a storage device that is associated with the device.

I/O See *input/output*.

I/O adapter (IOA)
An input-output adapter on the PCI bus.

IOCDS
See *input/output configuration data set*.

IOCP See *I/O Configuration Program*.

I/O Configuration Program (IOCP)
A program that defines to a system all the available I/O devices and channel paths.

I/O device
An addressable read and write unit, such as a disk drive device, magnetic tape device, or printer.

I/O interface
An interface that enables a host to perform read and write operations with its associated peripheral devices.

I/O Priority Queueing
A facility in the Workload Manager of zSeries that enables the system administrator to set priorities for queueing I/Os from different system images. See also *multiple allegiance* and *parallel access volumes*.

I/O processor (IOP)
Controls input-output adapters and other devices.

I/O sequential response time
The time an I/O request is queued in processor memory waiting for previous I/Os to the same volume to complete.

IP See *Internet Protocol*.

IPL See *initial program load*.

iSeries
An IBM eServer product that emphasizes integration. It is the successor to the AS/400 family of servers.

J

Java Virtual Machine (JVM)
A software implementation of a central processing unit (CPU) that runs compiled Java code (applets and applications). (GC)

JVM See *Java Virtual Machine*.

K

KB See *kilobyte*.

key field
The second (optional) field of a count key data record. The key length is specified in the count field. The key length determines the field length. The program writes the data in the key field and uses the key field to identify or locate a given record. The subsystem does not use the key field.

kilobyte (KB)
1) For processor storage, real, and virtual storage, and channel volume, 2^{10} or 1024 bytes.

2) For disk storage capacity and communications volume, 1000 bytes.

Korn shell
Interactive command interpreter and a command programming language.

KPOH
See *thousands of power-on hours*.

L

LAN See *local area network*.

last-in first-out (LIFO)
A queuing technique in which the next item to be retrieved is the item most recently placed in the queue. (A)

LBA See *logical block address*.

LCU See *logical control unit*.

least recently used (LRU)
1) The algorithm used to identify and make available the cache space that contains the least-recently used data.

2) A policy for a caching algorithm that chooses to remove from cache the item that has the longest elapsed time since its last access.

LED See *light-emitting diode*.

licensed machine code
Microcode that IBM does not sell as part of a machine, but licenses to the customer. LMC is implemented in a part of storage that is not addressable by user programs. Some IBM products use it to implement functions as an alternate to hard-wired circuitry.

LIFO See *last-in first-out*.

light-emitting diode (LED)
A semiconductor chip that gives off visible or infrared light when activated.

link address
On an ESCON interface, the portion of a source or destination address in a frame that ESCON uses to route a frame through an ESCON director. ESCON associates the link address with a specific switch port that is on the ESCON director. Equivalently, it associates the link address with the channel subsystem or control unit link-level functions that are attached to the switch port.

link-level facility
The ESCON hardware and logical functions of a control unit or channel subsystem that allow communication over an ESCON write interface and an ESCON read interface.

local area network (LAN)
A computer network located on a user's premises within a limited geographic area.

local e-mail
An e-mail configuration option for storage servers that are connected to a host-system network that does not have a domain name system (DNS) server.

logical address
On an ESCON interface, the portion of a source or destination address in a frame used to select a specific channel-subsystem or control-unit image.

logical block address (LBA)
The address assigned by the DS8000 to a sector of a disk.

logical control unit (LCU)
See *control-unit image*.

logical data unit
A unit of storage that is accessible on a given device.

logical device
The facilities of a storage server (such as the DS8000 series) associated with the processing of I/O operations directed to a single host-accessible emulated I/O device. The associated storage is referred to as a logical volume. The logical device is mapped to one or more host-addressable units, such as a device on a zSeries I/O interface or a logical unit on a SCSI I/O interface, such that the host initiating I/O operations to the I/O-addressable unit interacts with the storage on the associated logical device.

logical partition (LPAR)
For zSeries, a set of functions that create the programming environment in which more than one logical partition (LPAR) is established on a processor. An LPAR is conceptually similar to a virtual machine environment except that the LPAR is a function of the processor. Also, the LPAR does not depend on an operating system to create the virtual machine environment. (DS8000 series only)

logical path
1) The relationship between a channel image and a control-unit image that designates the physical path to be used for device-level communications between these images. The logical path is established as part of the channel and control-unit initialization procedures by the exchange of link-level frames.

2) With the Remote Mirror and Copy feature, the relationship between a source logical subsystem (LSS) and a target LSS that is created over a physical path through the interconnection fabric that is used for Remote Mirror and Copy functions. An LSS is a primary control unit, which performs the functions of a channel image.

logical subsystem (LSS)
A topological construct that consists of a group of up to 256 logical devices. A DS8000 storage unit can have (if CDK only) up to 32 CKD-formatted logical subsystems (8192 CKD logical devices) or (if FBA only) up to 32 fixed-block logical subsystems (8192 fixed-block logical devices). If mixed CKD and FBA, a DS8000 can have up to 16 CKD-formatted logical subsystems (4096 CKD logical devices) and up to 16 fixed-block logical subsystems (4096 fixed-block logical devices). The logical subsystem facilitates configuration of the DS8000 and might have other implications relative to the operation of certain functions. There is a one-to-one mapping between a CKD logical subsystem and a zSeries control-unit image.

For zSeries hosts, a logical subsystem represents a logical control unit (LCU). Each control-unit image is associated with only one logical subsystem. See also *control-unit image*.

logical unit
In open systems, a logical disk drive.

logical unit number (LUN)
In the SCSI protocol, a unique number that is used on a SCSI bus to enable it to differentiate between separate devices, each of which is a logical unit.

logical volume
The storage medium that is associated with a logical disk drive. A logical volume typically resides on one or more storage devices. The DS8000 administrator defines this unit of storage. The logical volume, when residing on a RAID-formatted array, is spread over the drives in the array.

logical volume manager (LVM)
A set of system commands, library routines, and other tools that allow the user to establish and control logical volume storage. The LVM maps data between the logical view of storage space and the physical disk drive module.

longitudinal redundancy check (LRC)
1) A method of error checking during data transfer that involves checking parity on a row of binary digits that are members of a set that forms a matrix. Longitudinal redundancy check is also called a longitudinal parity check.

2) A mechanism that the DS8000 uses for locating errors. The LRC checks the data as it progresses from the host, through theDS8000 controller, into the device adapter, and to the array.

longwave laser adapter
A connector that is used between a host and the DS8000 to support longwave fibre-channel communication.

loop The physical connection between a pair of device adapters in the DS8000 storage unit. See also *device adapter*.

LPAR See *logical partition*.

LRC See *longitudinal redundancy check*.

LRU See *least recently used*.

LSS See *logical subsystem*.

LUN See *logical unit number*.

LVM See *logical volume manager*.

M

machine level control (MLC)
A database that contains the EC level and configuration of products in the field.

machine reported product data (MRPD)
Product data gathered by a machine and sent to a destination such as an IBM support server or RETAIN. These records might include such information as feature code information and product logical configuration information.

mainframe
A computer, usually in a computer center, with extensive capabilities and resources to which other computers may be connected so that they can share facilities. (T)

maintenance analysis procedure (MAP)
A hardware maintenance document that gives an IBM service representative a step-by-step procedure for tracing a symptom to the cause of a failure.

management console
See *IBM System Storage Management Console*.

management information base (MIB)
1) A collection of objects that can be accessed by means of a network management protocol. (GC)

2) The MIB record conforms to the Open Systems Interconnection (OSI) standard defined by the International Organization for Standardization (ISO) for the exchange of information. See also *simple network management protocol*.

MAP See *maintenance analysis procedure*.

master storage unit
The physical unit that controls the creation of consistency groups in a Global Mirror session. The master storage unit sends commands to subordinate storage units. A storage unit can be a master for only one Global Mirror session. Contrast with *subordinate storage unit*.

maximum consistency group drain time
The value in seconds that indicates the maximum time that writes from the local site are delayed to the remote site while the current consistency group is being formed at the remote site. When this time is exceeded, the current attempt to form a consistency group is ended and another attempt is started. If this time is exceeded five times, this maximum time is ignored on the next attempt to form a consistency group. The default value is the larger of four minutes or two times the consistency group interval time if this value is set to zero.

maximum coordination time
The value in milliseconds that indicates the maximum time that is allowed for host I/O to be delayed during the coordination of the primary volumes of an Global Mirror session. The default is 50 milliseconds if this value is set to zero.

MB See *megabyte*.

MC See *IBM System Storage Management Console*.

MCA See *Micro Channel architecture*.

MDM See *Multiple Device Manager*.

mean time between failures (MTBF)
1) A projection of the time that an individual unit remains functional. The time is based on averaging the performance, or projected performance, of a population of statistically independent units. The units operate under a set of conditions or assumptions.

2) For a stated period in the life of a functional unit, the mean value of the lengths of time between consecutive failures under stated conditions. (I) (A)

medium
For a storage unit, the disk surface on which data is stored.

megabyte (MB)
1) For processor storage, real and virtual storage, and channel volume, 2^{20} or 1 048 576 bytes.

2) For disk storage capacity and communications volume, 1 000 000 bytes.

Metro Mirror
A function of a storage server that maintains a consistent copy of a logical volume on the same storage server or on another storage server. All modifications that any attached host performs on the primary logical volume are also performed on the secondary logical volume. See also *Remote Mirror and Copy* and *Global Copy*.

MES See *miscellaneous equipment specification*.

MIB See *management information base*.

Micro Channel architecture (MCA)
The rules that define how subsystems and adapters use the Micro Channel bus in a computer. The architecture defines the services that each subsystem can or must provide.

Microsoft Internet Explorer
Web browser software manufactured by Microsoft.

migration
The replacement of a system or subsystem with a different type of system or subsystem, such as replacing a SCSI host adapter with a fibre-channel host adapter. In the context of data migration regarding the DS8000, the transfer of data from one storage unit to another, such as from a 3390 to the DS8000.

MIH See *missing-interrupt handler*.

mirrored pair
Two units that contain the same data. The system refers to them as one entity.

mirroring
In host systems, the process of writing the same data to two disk units within the same auxiliary storage pool at the same time.

miscellaneous equipment specification (MES)
IBM field-installed change to a machine.

missing-interrupt handler (MIH)
An MVS and MVS/XA facility that tracks I/O interrupts. MIH informs the operator and creates a record whenever an expected interrupt fails to occur before a specified elapsed time is exceeded.

MLC See *machine level control*.

mobile solutions terminal (MoST)
The mobile terminal used by service personnel.

mode conditioning patch cable
A cable that converts a single-mode signal from a longwave adapter into a light signal that is appropriate for multimode fibre. Another mode conditioning patch cable is required at the terminating end of the multimode fibre to convert the signal back to a single-mode signal for a longwave adapter.

Model 100
A 2105 Model 100, often simply referred to as a Mod 100, is an expansion enclosure for the Enterprise Storage Server. See also *2105*.

MoST See *mobile solutions terminal*.

MRPD
See *machine reported product data*.

MSA See *multiport serial adapter*.

MTBF See *mean time between failures*.

Multipath Subsystem Device Driver
See *IBM System Storage DS8000 Multipath Subsystem Device Driver*.

multiple allegiance
A DS8000 hardware function that is independent of software support. This function enables multiple system images to concurrently access the same logical volume on the DS8000 as long as the system images are accessing different extents. See also *extent* and *parallel access volumes*.

Multiple Device Manager (MDM)
A component of the IBM TotalStorage Productivity Center that allows administrators to configure, manage, and monitor the performance of SAN storage devices from a single console.

multiple relationship FlashCopy
An option of the DS8000 that creates backup copies from one source to multiple targets by simultaneously establishing multiple FlashCopy relationships.

multiple virtual storage (MVS)
Implies MVS/390, MVS/XA, MVS/ESA, and the MVS element of the zSeries operating system.

multiplex
The action of transmitting simultaneously.

multiport serial adapter (MSA)
An adapter on the IBM System Storage Management Console that has multiple ports to which aDS8000 can be attached.

multiprocessor
A computer that includes two or more processors that have common access to a main storage. For the DS8000, the multiprocessors operate in parallel.

MVS See *multiple virtual storage*.

N

name server
A server that stores names of the participating DS8000 clusters.

near-line
A type of intermediate storage between online storage (which provides constant, rapid access to data) and offline storage (which provides infrequent data access for backup purposes or long-term storage).

Netfinity
IBM Intel-processor-based server; predecessor to the IBM xSeries server.

Netscape Navigator
Web browser software manufactured by Netscape.

network manager
A program or group of programs that is used to monitor, manage, and diagnose the problems of a network. (GC)

node The unit that is connected in a fibre-channel network. A DS8000 is a node in a fibre-channel network.

non-RAID
A disk drive set up independently of other disk drives and not set up as part of a disk pack to store data using the redundant array of disks (RAID) data-striping methodology.

nonremovable medium
A recording medium that cannot be added to or removed from a storage device.

nonvolatile storage (NVS)
Memory that stores active write data to avoid data loss in the event of a power loss.

NVS See *nonvolatile storage*.

O

octet In Internet Protocol addressing, one of the four parts of a 32-bit integer presented in dotted decimal notation. See also *dotted decimal notation*.

OEMI See *original equipment manufacturer's information*.

open system
A system whose characteristics comply with standards made available

throughout the industry and that therefore can be connected to other systems complying with the same standards. Applied to the DS8000, such systems are those hosts that connect to the DS8000 through SCSI or FCP protocols. See also *small computer system interface* and *Fibre Channel Protocol*.

organizationally unique identifier (OUI)
An IEEE-standards number that identifies an organization with a 24-bit globally unique assigned number referenced by various standards. OUI is used in the family of 802 LAN standards, such as Ethernet and Token Ring.

original equipment manufacturer's information (OEMI)
A reference to an IBM guideline for a computer peripheral interface. The interface uses ESA/390 logical protocols over an I/O interface that configures attached units in a multidrop bus topology.

OS/390
The IBM operating system that includes and integrates functions that many IBM software products (including the MVS operating system) previously provided for the IBM S/390 family of enterprise servers.

OUI See *organizationally unique identifier*.

P

panel The formatted display of information that appears on a display screen.

parallel access volumes (PAV)
A licensed function of the DS8000 that enables OS/390 and z/OS systems to issue concurrent I/O requests against a count key data logical volume by associating multiple devices of a single control-unit image with a single logical device. Up to eight device addresses can be assigned to a PAV. The PAV function enables two or more concurrent write operations to the same logical volume, as long as the write operations are not to the same extents. See also *extent*, *I/O Priority Queueing*, and *multiple allegiance*.

parity A data checking scheme used in a computer system to ensure the integrity of the data. The RAID implementation uses parity to re-create data if a disk drive fails.

path group
In zSeries architecture, a set of channel paths that are defined to a control unit as being associated with a single logical partition (LPAR). The channel paths are in a group state and are online to the host. See also *logical partition*.

path group identifier
In zSeries architecture, the identifier that uniquely identifies a given logical partition (LPAR). The path group identifier is used in communication between the LPAR program and a device. The identifier associates the path group with one or more channel paths, thereby defining these paths to the control unit as being associated with the same LPAR. See also *logical partition*.

PAV See *parallel access volumes*.

PCI See *peripheral component interconnect*.

PDU See *protocol data unit*.

PE See *IBM product engineering*.

peripheral component interconnect (PCI)
An architecture for a system bus and associated protocols that supports attachments of adapter cards to a system backplane.

persistent FlashCopy
A state where a FlashCopy relationship remains indefinitely until the user deletes it. The relationship between the source and target volumes is maintained after a background copy completes.

physical path
A single path through the I/O interconnection fabric that attaches two units. For Copy Services, this is the path from a host adapter on one DS8000 (through cabling and switches) to a host adapter on anotherDS8000.

pinned data
Data that is held in cache until either an error condition is corrected and it can be moved to disk storage or until the data is discarded by a host command. Pinned data conditions can only occur on an ESS Model 800 during fast-write or dual-copy functions.

planar The main printed circuit board (PCB) that other PCBs or assemblies plug into. The planar distributes both power and signals and therefore creates a common communications path to whichever device that plugs into it.

point-in-time copy
A FlashCopy option that creates an instantaneous view of original source data at a specific moment in time.

point-to-point connection
A fibre-channel topology that enables the direct interconnection of ports. See also *arbitrated loop* and *switched fabric*.

port A physical connection on a host adapter to the cable that connects the DS8000 to hosts, switches, or another DS8000. The DS8000 uses SCSI and ESCON host adapters that have two ports per adapter, and fibre-channel host adapters that have one port. See also *ESCON*, *fibre-channel*, *host adapter*, and *small computer system interface*.

POST See *power-on self test*.

power-on self test (POST)
A diagnostic test that servers or computers run when they are turned on.

predictable write
A write operation that can cache without knowledge of the existing format on the medium. All write operations on FBA DASD devices are predictable. On CKD DASD devices, a write operation is predictable if it does a format write operation for the first data record on the track.

primary control unit
The DS8000 to which a Remote Mirror and Copy primary device is physically attached.

processor complex
A partition of a storage server that is capable of performing all defined functions of the storage server. Multiple processor complexes provide redundancy.

product engineering
See *IBM product engineering*.

program
On a computer, a generic term for software that controls the operation of the computer. Typically, the program is a logical assemblage of software modules that perform multiple related tasks.

program-controlled interruption
An interruption that occurs when an I/O channel fetches a channel command word with the program-controlled interruption flag on.

program temporary fix (PTF)
A temporary solution to, or bypass of, a problem diagnosed by IBM as the result of a defect in a current unaltered release of a licensed program. (GC)

promote
To add a logical data unit to cache memory.

protected volume
In AS/400, a disk storage device that is protected from data loss by RAID techniques. An AS/400 host does not mirror a volume configured as a protected volume, while it does mirror all volumes configured as unprotected volumes. The DS8000, however, can be configured to indicate that an AS/400 volume is protected or unprotected and give it RAID protection in either case.

protocol data unit (PDU)
A unit of data specified in the protocol of a given layer and consisting of protocol control information for the layer and, possibly, user data for the layer.

pSeries
The product name of an IBM eServer product that emphasizes performance. It is the successor to the RS/6000 family of servers.

pseudo host
A host connection that is not explicitly defined to the DS8000 and that has access to at least one volume that is configured on the DS8000. The FiconNet pseudo host icon represents the FICON protocol. The EsconNet pseudo host icon represents the ESCON protocol. The pseudo host icon labelled `Anonymous` represents hosts connected through the FCP protocol. *Anonymous host* is a commonly used synonym for *pseudo host*. The DS8000 adds a pseudo host icon only when it is set to access-any mode. See also *access-any mode*.

PTF See *program temporary fix*.

PV Links
Short for Physical Volume Links, an alternate pathing solution from Hewlett-Packard that provides for multiple paths to a volume, as well as static load balancing.

R

R0 See *track-descriptor record*.

rack See *enclosure*.

RAID See *redundant array of independent disks*. RAID is also commonly expanded to redundant array of *inexpensive* disks. See also *array*.

RAID 5
A type of RAID that optimizes cost-effective performance while emphasizing use of available capacity through data striping. RAID 5 provides fault tolerance for up to two failed disk drives by distributing parity across all the drives in the array plus one parity disk drive. The DS8000 automatically reserves spare disk drives when it assigns arrays to a device adapter pair (DA pair). See also *device adapter*, *RAID 10*, and *redundant array of independent disks*.

RAID 10
A type of RAID that optimizes high performance while maintaining fault tolerance for up to two failed disk drives by striping volume data across several disk drives and mirroring the first set of disk drives on an identical set. The DS8000 automatically reserves spare disk drives when it assigns arrays to a device adapter pair (DA pair). See also *device adapter*, *RAID 5*, and *redundant array of independent disks*.

random access
A mode of accessing data on a medium in a manner that requires the storage device to access nonconsecutive storage locations on the medium.

rank One or more arrays that are combined to create a logically contiguous storage space.

redundant array of independent disks (RAID)
A methodology of grouping disk drives for managing disk storage to insulate data from a failing disk drive.

refresh FlashCopy target volume
An option (previously called *incremental FlashCopy*) of the DS8000 that creates a point-in-time data copy without copying an entire volume for each point-in-time copy.

Remote Mirror and Copy
A feature of a storage server that constantly updates a secondary copy of a logical volume to match changes made to a primary logical volume. The primary and secondary volumes can be on the same storage server or on separate storage servers. See also *Global Mirror*, *Metro Mirror* and *Global Copy*.

remote technical assistance information network (RETAIN)
The initial service tracking system for IBM service support, which captures heartbeat and call-home records. See also *support catcher* and *support catcher telephone number*.

REQ/ACK
See *request for acknowledgment and acknowledgment*.

request for acknowledgment and acknowledgment (REQ/ACK)
A cycle of communication between two data transport devices for the purpose of verifying the connection, which starts with a request for acknowledgment from one of the devices and ends with an acknowledgment from the second device. The REQ and ACK signals help to provide uniform timing to support synchronous data transfer between an initiator and a target. The objective of a synchronous data transfer method is to minimize the effect of device and cable delays.

reserved allegiance
For zSeries, a relationship that is created in a control unit between a device and a channel path, or path group, when the device completes a Sense Reserve command. The allegiance causes the control unit to guarantee access (that is, busy status is not presented) to the device. Access is over the set of channel paths that are associated with the allegiance; access is for one or more channel programs until the allegiance ends.

RETAIN
See *remote technical assistance information network*.

S

S/390 IBM enterprise servers based on Enterprise Systems Architecture/390 (ESA/390). *S/390* is the currently accepted shortened form of the original name *System/390*.

S/390 storage
Storage arrays and logical volumes that are defined as connected to S/390 servers. This term is synonymous with count-key-data storage.

SAID See *system adapter identification number*.

SAM See *sequential access method*.

SAN See *storage area network*.

SBCON
See *Single-Byte Command Code Sets Connection*.

screen The physical surface of a display device upon which information is shown to users.

SCSI See *small computer system interface*.

SCSI device
A disk drive connected to a host through an I/O interface using the SCSI protocol. A SCSI device is either an initiator or a target. See also *initiator* and *small computer system interface*.

SCSI-FCP
Synonym for Fibre Channel Protocol, a protocol used to transport data between an open-systems host and a fibre-channel adapter on an DS8000. See also *Fibre Channel Protocol* and *small computer system interface*.

SCSI host systems
Host systems that are attached to the DS8000 with a SCSI interface. Such host systems run on UNIX, i5/OS, Windows NT, Windows 2000, or Novell NetWare operating systems.

SCSI ID
A unique identifier assigned to a SCSI device that is used in protocols on the SCSI interface to identify or select the device. The number of data bits on the SCSI bus determines the number of available SCSI IDs. A wide interface has 16 bits, with 16 possible IDs.

SDD See *IBM Subsystem Multipathing Device Driver*.

secondary control unit
The DS8000 to which a Remote Mirror and Copy secondary device is physically attached.

self-timed interface (STI)
An interface that has one or more conductors that transmit information serially between two interconnected units without requiring any clock signals to recover the data. The interface performs clock recovery independently on each serial data stream and uses information in the data stream to determine character boundaries and inter-conductor synchronization.

sequential access
A mode of accessing data on a medium in a manner that requires the storage device to access consecutive storage locations on the medium.

sequential access method (SAM)
An access method for storing, deleting, or retrieving data in a continuous sequence based on the logical order of the records in the file.

serial connection
A method of device interconnection for determining interrupt priority by connecting the interrupt sources serially.

server A host that provides certain services to other hosts that are referred to as clients.

A functional unit that provides services to one or more clients over a network. (GC)

service boundary
A category that identifies a group of components that are unavailable for use when one of the components of the group is being serviced. Service boundaries are provided on the DS8000, for example, in each host bay and in each cluster.

service clearance
The area that is required to open the service covers and to pull out components for servicing.

service information message (SIM)
A message sent by a storage server to service personnel through an zSeries operating system.

service personnel
A generalization referring to individuals or companies authorized to service the DS8000. The terms *service provider*, *service representative*, and *IBM service support representative (SSR)* refer to types of service personnel. See also *service support representative*.

service processor
A dedicated processing unit that is used to service a storage unit.

service support representative (SSR)
Individuals or a company authorized to service the DS8000. This term also refers to a service provider, a service representative, or an IBM service support representative (SSR). An IBM SSR installs the DS8000.

SES SCSI Enclosure Services.

session
A collection of volumes within a logical subsystem that are managed together during the creation of consistent copies of data. All volumes in a session must transfer their data successfully to the remote site before the increment can be called complete.

SFP Small form factor pluggables.

shared storage
Storage that is configured so that multiple hosts can concurrently access the storage. The storage has a uniform appearance to all hosts. The host programs that access the storage must have a common model for the information on a storage device. The programs must be designed to handle the effects of concurrent access.

shortwave laser adapter
A connector that is used between host and DS8000 to support shortwave fibre-channel communication.

SIM See *service information message*.

Simple Network Management Protocol (SNMP)
In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB). (GC) See also *management information base*.

simplex volume
A volume that is not part of a FlashCopy, XRC, or PPRC volume pair.

Single-Byte Command Code Sets Connection (SBCON)
The ANSI standard for the ESCON I/O interface.

small computer system interface (SCSI)
A standard hardware interface that enables a variety of peripheral devices to communicate with one another. (GC)

smart relay host
A mail relay or mail gateway that has the capability to correct e-mail addressing problems.

SMIT See *System Management Interface Tool*.

SMP See *symmetrical multiprocessor*.

SNMP
See *Simple Network Management Protocol*.

SNMP agent
A server process that resides on a network node and is responsible for communicating with managers regarding that node. The node is represented as a managed object, which has various fields or variables that are defined in the appropriate MIB.

SNMP manager
A managing system that runs a managing application or suite of applications. These applications depend on Management Information Base (MIB) objects for information that resides on the managed system. Managers generate requests for this MIB information, and an SNMP agent on the managed system responds to these requests. A request can either be the retrieval or modification of MIB information.

software transparency
Criteria applied to a processing environment that states that changes do not require modifications to the host software in order to continue to provide an existing function.

source device
One of the devices in a dual-copy or remote-copy volume pair. All channel commands to the logical volume are directed to the source device. The data on the source device is duplicated on the target device. See also *target device.*

spare A disk drive on the DS8000 that can replace a failed disk drive. A spare can be predesignated to allow automatic dynamic sparing. Any data preexisting on a disk drive that is invoked as a spare is destroyed by the dynamic sparing copy process.

spatial reuse
A feature of serial storage architecture that enables a device adapter loop to support many simultaneous read/write operations. See also *serial storage architecture*.

SSID See *subsystem identifier*.

SSR See *service support representative*.

stacked status
For zSeries, the condition when the control unit is in a holding status for the channel, and the last time the control unit attempted to present the status, the channel responded with the stack-status control.

stage operation
The operation of reading data from the physical disk drive into the cache.

staging
To move data from an offline or low-priority device back to an online or higher priority device, usually on demand of the system or on request of the user.

standard volume
A volume that emulates one of several zSeries volume types, including 3390-2, 3390-3, 3390-9, 3390-2 (3380-track mode), or 3390-3 (3380-track mode), by presenting the same number of cylinders and capacity to the host as provided by the native zSeries volume type of the same name.

STI See *self-timed interface*.

storage area network
A network that connects a company's heterogeneous storage resources.

storage capacity
The amount of data that a storage medium can hold; usually expressed in kilobytes, megabytes, or gigabytes.

storage complex
A configuration of one or more storage units that is managed by a management console.

storage device
A physical unit that provides a mechanism to store data on a given medium such that it can be subsequently retrieved. See also *disk drive module*.

storage extent
The minimum contiguous range of storage on a physical storage device, array, or rank that can be allocated to a local volume

storage image
A partitioning of a storage unit that provides emulation of a storage server with one or more storage devices that provides storage capability to a host computer. You can configure more than one storage image on a storage unit. (DS8000 series only)

storage server
A physical unit that manages attached storage devices and provides an interface between them and a host computer by providing the function of one or more logical subsystems. The storage server can provide functions that the storage device does not provide. The storage server has one or more clusters.

storage unit
A physical unit that consists of a storage server that is integrated with one or more storage devices that provide storage capability to a host computer.

storage unit identifier
A unique identifier for a storage unit that consists of a manufacturer, a model number, a type number, a plant of manufacture, and a sequence number.

striping
A technique that distributes data in bit, byte, multibyte, record, or block increments across multiple disk drives.

subagent
An extension to an SNMP agent that

permits a user to dynamically add, or in some cases replace, additional management variables in the local MIB, thereby providing a means of extending the range of information that network managers can access. See also *agent*.

subchannel
A logical function of a channel subsystem associated with the management of a single device.

subordinate storage unit
The physical unit that receives commands from the master storage unit and is specified when a Global Mirror session is started. The subordinate storage unit forms consistency groups and performs other Global Mirror processing. A subordinate storage unit can be controlled by only one master storage unit. Contrast with *master storage unit*.

subsystem identifier (SSID)
A number that uniquely identifies a logical subsystem within a computer installation.

support catcher
See *catcher*.

support catcher telephone number
The telephone number that connects the support catcher server to the DS8000 to receive a trace or dump package. See also *support catcher* and *remote technical assistance information network*.

switched fabric
A fibre-channel topology in which ports are interconnected through a switch. Fabric switches can also be interconnected to support numerous ports on a single network. See also *arbitrated loop* and *point-to-point connection*.

symmetrical multiprocessor (SMP)
An implementation of a multiprocessor computer consisting of several identical processors configured in a way that any subset of the set of processors is capable of continuing the operation of the computer. TheDS8000 contains four processors set up in SMP mode.

synchronous write
A write operation whose completion is indicated after the data has been stored on a storage device.

System/390
See *S/390*.

system adapter identification number (SAID)
The unique identification number that is automatically assigned to each DS8000 host adapter for use by Copy Services.

System Management Interface Tool (SMIT)
An interface tool of the AIX operating system for installing, maintaining, configuring, and diagnosing tasks.

System Modification Program
A program used to install software and software changes on MVS systems.

T

target A SCSI device that acts as a subordinate to an initiator and consists of a set of one or more logical units, each with an assigned logical unit number (LUN). The logical units on the target are typically I/O devices. A SCSI target is analogous to a zSeries control unit. See also *small computer system interface*.

target device
One of the devices in a dual-copy or remote-copy volume pair that contains a duplicate of the data that is on the source device. Unlike the source device, the target device might only accept a limited subset of data. See also *source device.*

TB See *terabyte*.

TCP/IP
See *Transmission Control Protocol/Internet Protocol*.

terabyte (TB)
1) Nominally, 1 000 000 000 000 bytes, which is accurate when speaking of bandwidth and disk storage capacity.

2) For DS8000 cache memory, processor storage, real and virtual storage, a terabyte refers to 2^{40} or 1 099 511 627 776 bytes.

terminal emulator
A function of the management console that allows it to emulate a terminal.

thousands of power-on hours (KPOH)
A unit of time used to measure the mean time between failures (MTBF).

time sharing option (TSO)
An operating system option that provides interactive time sharing from remote terminals.

System Storage
See *IBM System Storage*.

TPF See *transaction processing facility*.

track A unit of storage on a CKD device that can be formatted to contain a number of data records. See also *home address*, *track-descriptor record*, and *data record*.

track-descriptor record (R0)
A special record on a track that follows the home address. The control program uses it to maintain certain information about the track. The record has a count field with a key length of zero, a data length of 8, and a record number of 0. This record is sometimes referred to as R0.

transaction processing facility (TPF)
A high-availability, high-performance IBM operating system, designed to support real-time, transaction-driven applications. The specialized architecture of TPF is intended to optimize system efficiency, reliability, and responsiveness for data communication and database processing. TPF provides real-time inquiry and updates to a large, centralized database, where message length is relatively short in both directions, and response time is generally less than three seconds. Formerly known as the Airline Control Program/Transaction Processing Facility (ACP/TPF).

Transmission Control Protocol (TCP)
A communications protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP)
1) A combination of data-transmission protocols that provide end-to-end connections between applications over interconnected networks of different types.

2) A suite of transport and application protocols that run over the Internet Protocol. (GC) See also *Internet Protocol* and *Transmission Control Protocol*.

transparency
See *software transparency*.

TSO See *time sharing option*.

turbo processor
A faster multiprocessor that has six processors with common access to the main storage.

U

UFS UNIX filing system.

Ultra-SCSI
An enhanced small computer system interface.

unconfigure
To delete the configuration.

unit address
For zSeries, the address associated with a device on a given control unit. On ESCON interfaces, the unit address is the same as the device address. On OEMI interfaces, the unit address specifies a control unit and device pair on the interface.

unprotected volume
An AS/400 term that indicates that the AS/400 host recognizes the volume as an unprotected device, even though the storage resides on a RAID-formatted array and is, therefore, fault tolerant by definition. The data in an unprotected volume can be mirrored. Also referred to as an *unprotected device*.

upper-layer protocol
The layer of the Internet Protocol (IP) that supports one or more logical protocols (for example, a SCSI-command protocol and an ESA/390 command protocol). Refer to ANSI X3.230-199*x*.

UTC See *Coordinated Universal Time*.

V

virtual machine facility
A virtual data processing machine that

appears to the user to be for the exclusive use of that user, but whose functions are accomplished by sharing the resources of a shared data processing system. An alternate name for the VM/370 IBM operating system.

vital product data (VPD)
Information that uniquely defines the system, hardware, software, and microcode elements of a processing system.

VM The root name of several IBM operating systems, such as VM/XA, VM/ESA, VM/CMS, and z/VM. See also *virtual machine facility*.

volume
For zSeries, the information recorded on a single unit of recording medium. Indirectly, it can refer to the unit of recording medium itself. On a nonremovable-medium storage device, the term can also indirectly refer to the storage device associated with the volume. When multiple volumes are stored on a single storage medium transparently to the program, the volumes can be referred to as logical volumes.

volume group
A collection of either physical or logical volumes.

volume label
A unique identifier that a user assigns to a logical volume.

VPD See *vital product data*.

VSE/ESA
An IBM operating system, the letters of which represent virtual storage extended/enterprise systems architecture.

W

weight distribution area
The area that is required to distribute the weight of the storage unit.

worldwide node name (WWNN)
A unique 64-bit identifier for a host that contains a fibre-channel port. See also *worldwide port name*.

worldwide port name (WWPN)
A unique 64-bit identifier associated with a fibre-channel adapter port. It is assigned in an implementation- and protocol-independent manner. See also *worldwide node name*

write hit
A write operation in which the requested data is in the cache.

write penalty
The performance impact of a classical RAID-5 write operation.

WWNN
See *worldwide node name*.

WWPN
See *worldwide port name*.

X

xSeries
The product name of an IBM eServer product that emphasizes industry-standard server scalability and self-managing server technologies. It is the successor to the Netfinity family of servers.

Z

z/Architecture
An IBM architecture for mainframe computers and peripherals. The IBM eServer zSeries family of servers uses the z/Architecture architecture. It is the successor to the S/390 and 9672 family of servers. See also *iSeries*.

zoning
In fibre-channel environments, the grouping of multiple ports to form a virtual, private, storage network. Ports that are members of a zone can communicate with each other, but are isolated from ports in other zones.

z/OS An operating system for the IBM eServer product line that supports 64-bit real storage.

zSeries Global Mirror
A function of a storage server that assists a control program to maintain a consistent copy of a logical volume on another storage unit. All modifications of the primary logical volume by any attached host are presented in order to a single host. The host then makes these modifications on the secondary logical

volume. This function was formerly called *extended remote copy* or *XRC*.

zSeries
An IBM eServer family of servers that emphasizes near-zero downtime.

IBM enterprise servers based on z/Architecture.

zSeries storage
Storage arrays and logical volumes that are defined in the DS8000 as connected to zSeries servers.

Index

Readers' Comments — We'd Like to Hear from You

IBM System Storage
DS Open Application Programming Interface 5.3
Installation and Reference
Version 1 Release 3

Publication No. GC35-0516-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.

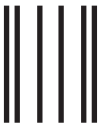
If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	E-mail address

Readers' Comments — We'd Like to Hear from You
GC35-0516-02

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department 61C
9032 South Rita Road
Tucson, AZ 85775-4401

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in USA

GC35-0516-02

Spine information:

IBM System Storage

DS Open API Reference

Version 1
Release 3