IBM System Storage DS
Version 6 Release 2

Open Application Programming Interface Installation and Reference

GC35-0516-10

Note
Before using this information and the product it supports, read the information in the Notices section.

This edition applies to Version 6, Release 2, of the IBM Storage System DS8000 Open Application Programming Interface and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures v

Tables vii

About this guide ix
Who should use this guide ix
Conventions used in this guide ix
DS8000 library and related publications ix
How to order IBM publications xii
How to send your comments xii

Summary of changes xv

Chapter 1. Introduction to IBM System Storage DS open application programming interface 1
DS open application programming interface 1
CIM agent overview 1
CIM agent components 3
CIM concepts 3
CIM agent security 4

Chapter 2. CIM agent for HMC 5
Installation overview for HMC 6
Installing and configuring the DSCIMCLI utility . . 6
Enabling the CIM agent on the HMC 7
Configuring the CIM agent for HMC 7
Verifying the CIM agent connection. 8
Disabling the CIM agent on the HMC 9

Chapter 3. CIM agent management commands 11
Overview of the CIM agent management commands 11
Invoking the CIM agent 11
Conventions used in this chapter 11
Syntax diagrams 11
Special characters 13
Emphasis 13
Anatomy of DSCIMCLI commands 13
Description of commands. 14
DSCIMCLI commands 14
help 15
SSL Certificate commands 16
Configuration management commands 18
Log collection commands 21

Chapter 4. DS Open API component definitions 23

Chapter 5. CIM agent communication with the DS Open API 25
CIM agent communication concepts 25
CIM agent communication methods 25
CIM agent functional groups 36
Error codes returned by the CIMOM 36

Chapter 6. IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service for Windows 39
IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service overview 39
IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software installation requirements 40
Hardware 40
Software 40
Installing the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software 41
Creating the VSS_FREE and VSS_RESERVED pools 42
Verifying the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software installation 43
Verifying IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software configuration 44
IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software configuration commands 45
IBM System Storage support for Microsoft Volume Shadow Copy and Virtual Disk Services software error codes 47
Uninstalling the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software 48

Chapter 7. IBM VSS Hardware Provider 4.2.1 support for VMware 51
Prerequisites 51
Setting Hardware Provider parameters for VMware 52
Generate Java key store 53
Configuring NPIV support 54
Prerequisites 54
Setting up NPIV 54
Verify that VM is functioning correctly 55
Taking snapshots with NPIV 55
Taking snapshots with various protocols. 56
Storage protocol priority 56
Special cases and exceptions 57

Chapter 8. IBM VSS Hardware Provider 4.2.1 support for Hyper-V 59
Primary configuration of Hyper-V 59
Prerequisites 59

Configuring the Hyper-V (host) server 59
Configuring the IBM VSS Hardware Provider . . 60
Configuring source volumes 60
Taking snapshots 61
Advanced configuration of Hyper-V 61
Creating virtual ports 61
Creating zoning 62
Creating storage 62
Configuring the host disk 62
Deploying guests 62
Configuring source volumes 63
Verifying NPIV configuration 63
Taking a snapshot 63
Troubleshooting the Hyper-V configuration 63
The provider cannot find any Fibre Channel initiator. 64
The volume is not supported by provider . . . 64
Importing shadow copy failed or locating LUN failed while taking shadow copy 64
Target LUNs are not attached to host through a virtual port 64

Notices 65
Trademarks 66
Electronic emission notices 67
Federal Communications Commission statement 67
Industry Canada compliance statement 67
European Union Electromagnetic Compatibility Directive 67
Japanese Voluntary Control Council for Interference (VCCI) class A statement. 69
Japanese Electronics and Information Technology Industries Association (JEITA) statement. . . . 69
Korea Communications Commission (KCC) Electromagnetic Interference (EMI) Statement . . 69
Russia Electromagnetic Interference (EMI) Class A Statement 70
Taiwan Class A compliance statement 70
Taiwan contact information 70

Index 71

Figures

1. How a CIM agent works 2
2. The MOF compiler stores the model in the CIMOM data store. 4

Tables

1. DS8000 library x
2. Other IBM publications x
3. IBM documentation and related websites xi
4. Summary of DSCIMCLI agent subcommands 14
5. GetClass method parameters 26
6. GetInstance method parameters 26
7. DeleteInstance method parameters 27
8. CreateInstance method parameters 27
9. ModifyInstance method parameters 28
10. EnumerateClasses method parameters . . . 28
11. EnumerateClassNames method parameters 29
12. EnumerateInstances method parameters 29
13. EnumerateInstanceNames method parameters 30
14. ExecuteQuery method parameters 30
15. Associators method parameters 31
16. AssociatorNames method parameters 32
17. References method parameters 32
18. ReferenceNames method parameters 33
19. GetProperty method parameters 33
20. SetProperty method parameters 34
21. GetQualifier method parameters 34
22. SetQualifier method parameters 35
23. Functional groups for the CIM agent 36
24. Return error codes for the CIMOM. 37
25. Microsoft Volume Shadow Copy and Virtual Disk Services software configuration commands 45
26. IBM System Storage support for Microsoft Volume Shadow Copy and Virtual Disk Services software error codes. 47
27. Role settings in vCenter 52
28. Server certificate filenames and locations 53

About this guide

This publication introduces the IBM® System Storage DS® Open Application Programming Interface (API), which is referenced in this guide as the Common Information Model (CIM) agent. This publication supports the DS8000 series release 6.1.

This publication also lists the CIM components and provides descriptions of the commands that you use during the installation and configuration tasks. The following information can 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 configuring the CIM agent.

This publication assumes that you understand the general concepts of the operating system and Internet capabilities for your enterprise.

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.

DS8000 library and related publications

Product manuals, other IBM publications, and websites contain information that relates to DS8000®.

DS8000 Information Center

The IBM System Storage® DS8000 Information Center contains all of the information that is required to install, configure, and manage the DS8000. The

information center is updated between DS8000 product releases to provide the most current documentation. The information center is available at the following website: DS8000 Information Center

DS8000 library

Table 1 lists and describes the publications that make up the DS8000 library. Unless otherwise noted, these publications are available in Adobe portable document format (PDF). Go to the DS8000 Library to obtain a publication.

Table 1. DS8000 library

Title	Description	Order Number
IBM System Storage DS: Command-Line Interface User's Guide	This guide describes the commands that you can use from the command-line interface (CLI) for managing your DS8000 configuration and Copy Services relationships. The CLI provides a set of commands that you can use to write customized scripts for a host system.	GC53-1127
IBM System Storage DS8000: Host Systems Attachment Guide	This guide provides information about attaching hosts to the DS8000 storage unit. The DS8000 provides a variety of host attachments so that you can consolidate storage capacity and workloads for open-systems hosts and System z® or S/390® hosts.	GC27-2298
IBM System Storage DS8000: Introduction and Planning Guide	This guide introduces the DS8000 product and lists the features you can order. It also provides guidelines for planning the installation and configuration of the storage unit.	GC27-2297
IBM System Storage Multipath Subsystem Device Driver User's Guide	This publication describes how to use the IBM Subsystem Device Driver (SDD) on open-systems hosts to enhance performance and availability on the DS8000. SDD creates single devices that consolidate redundant paths for logical unit numbers. SDD permits applications to run without interruption when path errors occur. It balances the workload across paths, and it transparently integrates with applications.	GC27-2122
IBM System Storage DS Application Programming Interface Reference	This publication provides reference information for the IBM System Storage DS application programming interface (API) and provides instructions for installing the Common Information Model Agent, which implements the API.	GC35-0516

Other IBM publications

Other IBM publications contain additional information that is related to the DS8000 product library. Table 2 is divided into categories to help you find publications that are related to specific topics.

Table 2. Other IBM publications

Title	Description	Order number
System Storage Productivity Center		
IBM System Storage Productivity Center Introduction and Planning Guide	This publication introduces the IBM System Storage Productivity Center hardware and software.	SC23-8824

Table 2. Other IBM publications (continued)

Title	Description	Order number
Read This First: Installing the IBM System Storage Productivity Center	This publication provides quick instructions for installing the IBM System Storage Productivity Center hardware.	GI11-8938
IBM System Storage Productivity Center Software Installation and User's Guide	This publication describes how to install and use the IBM System Storage Productivity Center software.	SC23-8823
IBM System Storage Productivity Center User's Guide	This publication describes how to use the IBM System Storage Productivity Center to manage the DS8000, IBM System Storage SAN Volume Controller clusters, and other components of your data storage infrastructure from a single interface.	SC27–2336
IBM Tivoli® Key Lifecycle Manager		
IBM Tivoli Key Lifecycle Manager Installation and Configuration Manager	This publication describes how to install and configure the Tivoli encryption key manager. The key server can be used to manage the encryption keys assigned to the IBM Full Disk Encryption disk drives in the DS8000.	SC23-9977
IBM System Management Pack for Microsoft		
IBM System Management Pack for Microsoft System Center Operations Manager User Guide	This publication describes how to install, configure, and use the IBM Storage Management Pack for Microsoft System Center Operations Manager (SCOM).	GC27-3909

IBM documentation and related websites

The following websites provide information about the DS8000 or related products or technologies:

Table 3. IBM documentation and related websites

Website	Link
IBM System Storage DS8000 series	IBM Storage Disk DS8000
Support for DS8000, IBM System Storage, and IBM TotalStorage® products	IBM TotalStorage Products Support
Concurrent Copy for IBM System z and S/390 host systems	IBM Storage Software System z and S/390 host systems
DS8000 command-line interface (DS CLI)	DS8000 Information Center The information center has a complete command reference for the DS CLI.
Information about code bundles for DS8700 and DS8800.	IBM Support - DS8700 code bundles See **Section 3** for cross-reference links to SDD. IBM Support - DS8800 code bundles
IBM FlashCopy® for System z and S/390 host systems	IBM Storage Software System z and S/390 host systems

Table 3. IBM documentation and related websites (continued)

Website	Link
Host system models, operating systems, adapters, and switches that the DS8000 series supports	Host system models, OS, adapters and switches Click **Interoperability matrix**. IBM Storage SSIC Click **New search**.
IBM Disk Storage Feature Activation (DSFA)	IBM Storage DSFA
IBM version of the Java SE Runtime Environment (JRE) that is often required for IBM products	IBM Java SE Runtime Environment (JRE)
Information about IBM Storage Easy Tier™	• IBM Storage Easy Tier Deployment Considerations Guide • IBM Storage Easy Tier performance on DS8700
Remote Mirror and Copy (formerly Peer-to-Peer Remote Copy [PPRC]) for System z and S/390 host systems	IBM Storage Software System z and S/390 host systems
SAN Fibre Channel switches	IBM Storage SAN switches
Subsystem Device Driver (SDD)	IBM Storage Software SDD
IBM Publications Center	IBM Publications Center
IBM Redbooks® publications	IBM Redbooks Publications

Related accessibility information

To view a PDF file, you need Adobe Acrobat Reader, which can be downloaded for free from the Adobe website at: Adobe Downloads

How to order IBM publications

The IBM 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 at no charge. You can also order publications. You can access the IBM Publications Center at:

http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss.

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

To submit any comments about this book or any other DS8000 documentation:

- Go to the DS8000 information center website at DS8000 Feedback. There you will find the feedback page where you can enter and submit comments.

- Send your comments by email to starpubs@us.ibm.com. Be sure to include the following information:
  - In the subject line of the email:
    - Exact publication title and version
    - Publication form number (for example, GC26-1234-02)
  - Page, table, or illustration numbers that you are commenting on
  - A detailed description of any information that should be changed

Summary of changes

This document contains terminology, maintenance, and editorial changes for version GC35-0516-10 of the IBM System Storage DS Open Application Programming Interface Installation and Reference. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

New information

- Added IBM VSS Hardware Provider 4.2.1 for VMware information. For information, see Chapter 7, "IBM VSS Hardware Provider 4.2.1 support for VMware," on page 51.
- Added Hyper-V guest OS with IBM VSS Hardware Provider for DS8000 information. For information, see Chapter 8, "IBM VSS Hardware Provider 4.2.1 support for Hyper-V," on page 59.

Chapter 1. Introduction to IBM System Storage DS open application programming interface

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 application programming interface
- CIM agent overview
- CIM agent components
- CIM concepts
- CIM agent installation requirements
- CIM agent installation methods
- CIM agent security

DS open application programming interface

The IBM System Storage DS 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, RAID 6, and RAID 10 volume spaces. 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 help you to use existing SRM applications and infrastructures. The DS Open API can also be used to automate 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 DS command-line interface.

Note: The DS Open API supports the IBM System Storage DS8000 series and is an embedded component.

You can implement the DS Open API without using a separate middleware application, like the IBM System Storage Common Information Model (CIM) agent, which provides a CIM-compliant interface. The DS Open API uses the CIM technology to manage proprietary devices as open system devices through storage management applications. The DS Open API is used by storage management applications to communicate with a storage unit.

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.

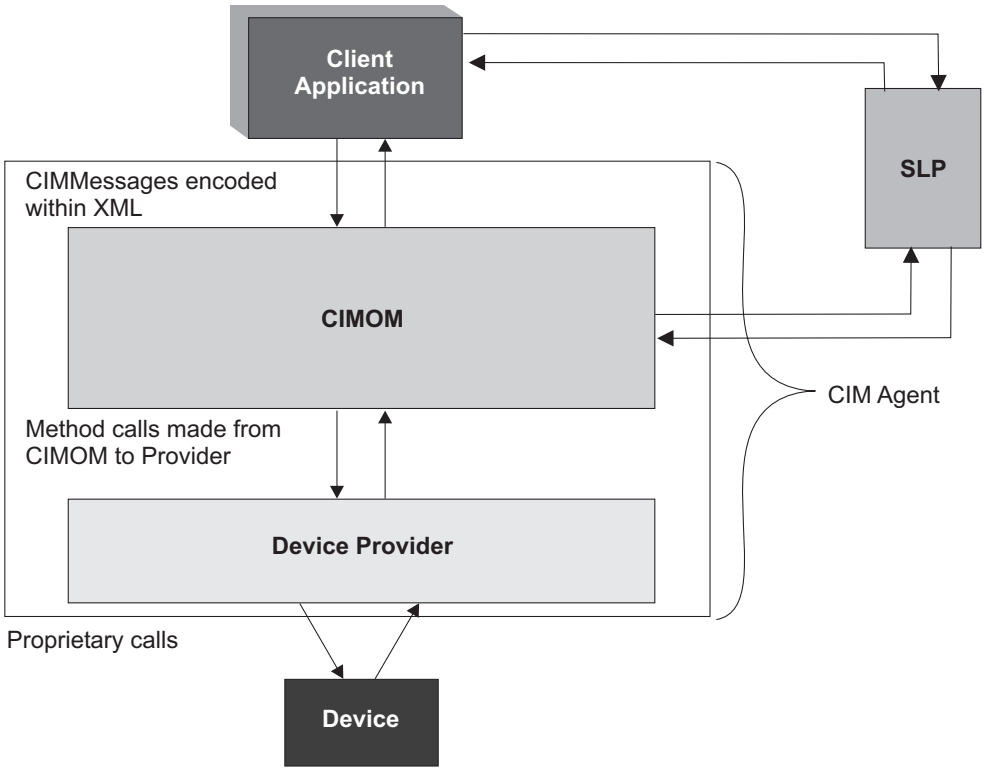


Figure 1. How a CIM agent works

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 1.2*
- *The Common Information Model (CIM) agent release 5.4.3 and later complies with Storage Management Initiative Specification (see IBM's certification status in SNIA website: http://www.snia.org/forums/smi/tech_programs/ctp/conformingproviders/)*

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 that 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.

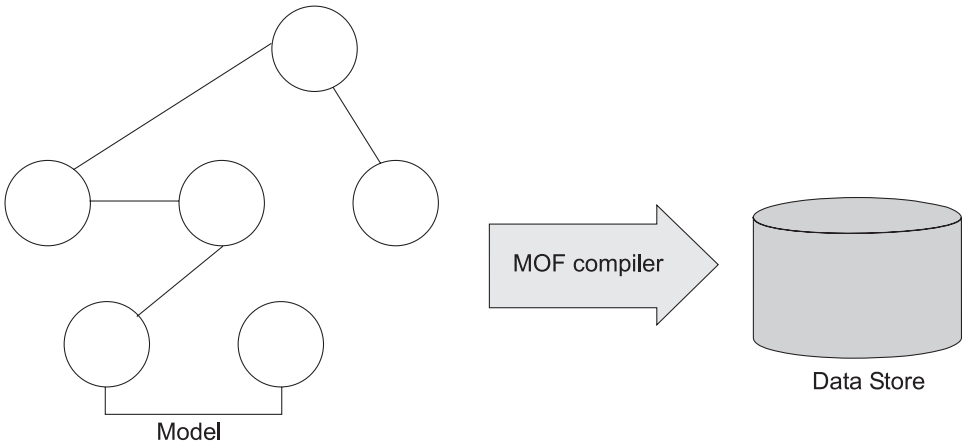


Figure 2. The MOF compiler stores the model in the CIMOM data store.

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 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 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 HMC

Beginning with DS8000 release 4.1, the CIM agent is preinstalled on the hardware management console (HMC). The embedded CIM agent in DS8000 release 6.1 is auto enabled and preconfigured. This chapter includes an overview of the setup process to manage the embedded CIM agent in DS8000 release 6.1.

You can manage the DS8000 from the CIM agent that is bundled with the HMC or from a CIM agent that is installed on a separate system. The CIM agent that is embedded on the HMC has the following limitations:

- The HMC CIM agent can only support DS8000 devices that are managed by the HMC. The CIM agent is not able to manage any ESS 800 or DS6000 devices, or any DS8000 devices that are managed by a different HMC. Therefore, some of the device management options such as using the DSCIMCLI to add or remove devices are not supported.
- The HMC CIM agent must use secure connections over port 6989.
- You perform some of the management and configuration activities of the embedded CIM agent from a remote server. Therefore, you must download and install the DSCIMCLI utility on a remote server.

  To download the DSCIMCLI:

  1. Visit the IBM support page at http://www.ibm.com/support/us/en/.
  2. From the IBM Support Portal, under **Choose your products**, select **Browse for a product** and **System Storage**.
  3. Select the product family **Storage software** > **Other software products**.
  4. Select the software product **CIM Agent for DS Open (API)** and under **Choose your page**, select **Downloads** and click **Continue**.
  5. Click the link under **Tool/Utility**.
  6. Select the DSCIMCLI version corresponding to your release.
- Because the DS agent uses the device user account to perform authentication, user account management is not supported from the DSCIMCLI. For example, you cannot use the DSCIMCLI to create, delete, modify or list accounts. To manage accounts, you must use the DS Command-line Interface (CLI) or the DS Storage Manager (GUI).

Beginning with release 6.1, the embedded CIM agent reduces resource consumption on the HMC by:

- Disabling the device configuration object caches and indications by default
- Enabling all the object caches and indications whenever instances of one of the following CIM classes are enumerated. (For more information on enumerating instances with the EnumerateInstances method, see "CIM agent communication methods" on page 25.)
  - IBMTSDS_StorageSystem
  - IBMTSDS_StorageLPARSystem
  - IBMTSDS_Volume
  - IBMTSDS_ExtentPool
  - IBMTSDS_DiskDrive
  - IBMTSDS_ArraySitePool
  - IBMTSDS_RankPool

– IBMTSDS_VolumeGroup
– IBMTSDS_FCPort
– IBMTSDS_StorageHardwareID
– IBMTSDS_SCSIProtocolController
– IBMTSDS_VolumeDistribution
– IBMTSDS_VirtualPool
– IBMTSDS_SEVolume
– IBMTSDS_ArrayPool

Installation overview for HMC

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

Perform the following list of installation and configuration tasks:

1. Download and install the DSCIMCLI utility.
2. Enable the CIM agent using the HMC graphical user interface.

   Note: You can skip step 2 for DS8000 6.1 because the CIM agent is all ready enabled.
3. Verify the connection to your storage unit.

Installing and configuring the DSCIMCLI utility

The DSCIMCLI utility is used to configure the CIM agent and is available from the DS CIM agent Web site.

About this task

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. The DSCIMCLI can run on the same platforms that the proxy CIM agent runs on, but does not consume nearly as much memory as the full CIM agent installation.

The DSCIMCLI can be installed on the following operating systems:

- The supported platforms for 5.4.1 and later versions of the DSCIMCLI utility include Win2008, Win2003, and SLES 10.
- The supported platforms for 5.2, 5.3, and 5.4 versions of the CIM agent include Win2003, RedHat Advanced Server 3.0, SLES 9, and AIX 5.3.
- The supported platforms for the 5.1.0 version of the CIM agent include Win2000, Win2003, RedHat Advanced Server 3.0, AIX 5.1, AIX 5.2, and AIX 5.3.
- RHEL3 (Red Hat Enterprise Linux) (For DS8000 release 4.0 or earlier only)

Perform the following steps to install and configure the DSCIMCLI utility:

Procedure

1. Download one of the following available files:
   - IBM-DSCIMCLI-5.5.1.xxx.zip
   - IBM-DSCIMCLI-5.5.1.xxx.tar.Z

   These files have identical content.
2. For Linux operating systems, perform the following steps:

a. Create a working directory and copy the DSCIMCLI distribution archive into the directory.
b. From the working directory, issue one of the following commands to uncompress and extract the DSCIMCLI distribution archive:

```
tar -xzvf archive.tar.Z
unzip archive.tar.Z
```

where *archive.tar.Z* is the name of the DSCIMCLI archive file.

3. For Windows operating systems, perform the following steps:
   a. Create a working directory and copy the DSCIMCLI distribution archive into the directory.
   b. From the working directory, use the windows native Archive Extraction Wizard to extract the files.
4. The top-level directories of the extracted content represent the different operating systems. Set your DSAGENT_HOME environment variable to one of those directories depending on your operating system. On Linux, the following syntax can be used:

```
export PATH=$PATH:$DSAGENT_HOME/bin
```

On Windows, the following syntax can be used:

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

Enabling the CIM agent on the HMC

For releases prior to DS8000 release 4.1, the CIM agent is not automatically enabled. You must enable the CIM agent on the HMC before you can use it. For DS8000 release 4.1 and later, the CIM agent is enabled by default. You do not have to enable the CIM agent unless it has been disabled.

About this task

Perform the following steps to enable the HMC CIM agent:

Procedure

1. From the HMC Welcome page, click **HMC Management**. The HMC Management window is displayed.
2. Click **Start/Stop CIM Agent**. The HMC CIM Agent window is displayed with the current state of the CIM agent.
3. Select **Start CIM Agent** and click **Apply**. The CIM agent is started and the state is updated.

Configuring the CIM agent for HMC

This section provides information on configuring the CIM agent for HMC.

About this task

For DS8000 release 4.0 and earlier, the CIM agent administrator and storage administrator are required to create and maintain user passwords for both the CIM agent and the DS8000 management applications.

However, for DS8000 release 4.1 and later, the embedded CIM agent does not require configuration changes to manage DS8000 devices. Instead, the DS8000

device user names and passwords are used to authenticate CIM client requests. The DS8000 administrator must create user names and passwords that CIM clients can use to attach to the CIM agent. Each user that is created can be in any group. But users that are created in any group other than the administrator group cannot perform manipulation functions except queries with DS8000 release 6.1 CIM agents. The DS8000 administrator can use the DSCLI or the HMC console GUI to create user names and passwords.

Beginning with release 6.1, for each request to the embedded CIM agent, the CIM agent first checks the role of the requesting user. If the user is not in one of the following valid roles, the request is rejected:

- Administrator
- Copy Services operator
- Logical operator
- Physical operator
- Service
- Monitor

Verifying the CIM agent connection

You must verify that the CIM agent software connects to the storage unit that you identified during configuration.

About this task

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

Procedure

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

   ```
   dscimcli -s https://hmc_ip:6989 -u DS8000user
   -p DS8000password lsdev -l
   ```

   where *hmc ip* is the IP address of the HMC, *DS8000user* is the user name that is used to log into the DS8000 Storage Manager, and *DS8000password* is the password that is used to log into the DS8000 Storage Manager.

   The following is an example of the output that is displayed:

   ```
   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, the CIM agent cannot communicate with the storage device. If the CIM agent was unable to communicate during mkdev, an error is immediately returned. To ensure that your storage device's management interface is functioning, use the DSCLI or DS Storage Manager to attempt to log into the device. If you cannot connect through the DSCLI or DS Storage Manager, there is likely an error in the storage device. If you are able to connect through 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 and *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.

About this task

Perform the following steps to disable the HMC CIM agent:

Procedure

1. From the HMC Welcome page, click **HMC Management**. The HMC Management window is displayed.
2. Click **Start/Stop CIM Agent**. The HMC CIM Agent window is displayed with the current state of the CIM agent.
3. Select **Stop CIM Agent** and click **Apply**. The CIM agent is stopped and the state is updated.

Chapter 3. 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, Windows 2003, or W2K8 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.

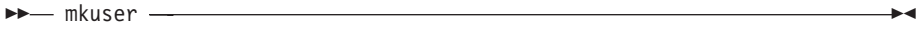
Syntax diagrams

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.

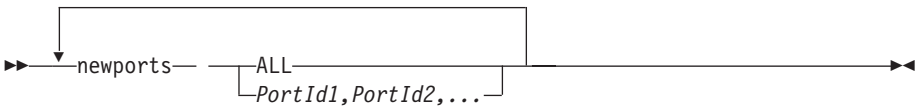
Optional keywords

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

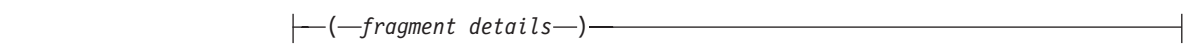
Represents the value you must supply for a parameter or argument, such as a file name, user name, or password. Variables are in italics.

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 DSCIMCLI commands

To issue a command, you must include the command name and any options, flags, values, or arguments.

The following list defines the anatomy of commands:

Command name
The name of the command that you can issue. For example, **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. Some flags require extra parameters.

Values
Command options that set the value of a flag.

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

The following is an example of a command that you can enter in the DSCIMCLI:

```
dscimcli -s https://hmc_ip:6989 -u DS8000user -p DS8000password lsdev -l
```

Description of commands

This section describes the CIM agent commands that you can use to manage the CIM agent.

Important: Before you use the **dscimcli** command, you must set the **DSAGENT_HOME** environment variable to the directory where the CIM agent is installed. You must also include DSAGENT_HOME/bin in the **PATH** environment variable.

DSCIMCLI commands

You can use DSCIMCLI commands in single-shot mode to manage the CIM agent.

Table 4 describes the subcommands that you can use with the DSCIMCLI.

Note: Because the CIM agent in DS8000 release 4.1 and later is embedded and has a pre-configured and integrated device management application, some of the DSCIMCLI commands are not supported. These commands include **mkdev**, **rmdev**, **lsuser**, **mkuser**, **rmuser**, and **chuser**.

Table 4. 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.
Configuration management	**lsconfig** List the current configuration properties of the CIM agent. **chconfig** Modifies the specified configuration properties of the CIM agent.

Table 4. Summary of DSCIMCLI agent subcommands (continued)

Command Category	Command Description
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.
Log collection	**collectlog** Collects the CIM agent log files. **Note:** For information about accessing log files, see http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp?topic=/com.ibm.itpc.doc/tpcpdg3179.htm.

help

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

Syntax

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: /opt/IBM/dsagent/pegasus/bin/dscimcli
command arg1 ... argN [options]
Options:
    Server location ($DSCIM_SERVER): [ -s [[protocol://]ip[:port][/namespace] ].
Default(https://127.0.0.1:5989/root/ibm)
    Authentication info ($DSCIM_USER): [ -u username -p password ].
    Timeout ($DSCIM_TIMEOUT): [-t timeout]. Default(120)
    Verbose: [-v]. Default(false)
    Help: [-help].
Command list:
 Device management (mkdev and rmdev will not be supported since 5.4.1 DS Agent):
    lsdev [-l]
    mkdev ip [-type ds|ess|esscs] [-ip2 ip] [-user username] [-password password]
             (default: type=ds , user=admin , password=admin)
    rmdev ip -type ds|ess|esscs
 User management (User management will not be supported since 5.4.1 DS Agent):
    lsuser
    mkuser username -password password
    chuser username -password password -newpassword newpassword
    rmuser username
 Configuration management:
    lsconfig
    chconfig
             [-certificate certname*] [-loglevel fatal|error|warn|info]
             [-tracecomponent comma_separated_list] (possible values: all, none, cpa,
               cim, sea, jni,
               servicemanager, slp)
             [-tracemask comma_separated_list] (possible values: all, none, entryexit,
               fine, debug, perf)
             [-jvmarg args] [-essdutycycle time] [-dsdutycycle time]
             [-slpregips comma_separated_list] (possible value: list of comma
               separated IPs, none)
             [-essperfstatsip IP, none]
             *: requires a restart of the CIM Agent
 SSL Certificate management:
    lscert
    mkcert certname
    rmcert certname
    getcert certname
 Server management:
    restartagent
 Collect Logs: (Used for DS Agent 5.4.1 or later only)
    collectlog [-d directoryname] (default: DSAGENT_HOME)
 Clear Subscriptions:
    clearsubscriptions
```

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
```

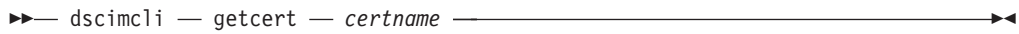
The resulting output:

```
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
```

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
```

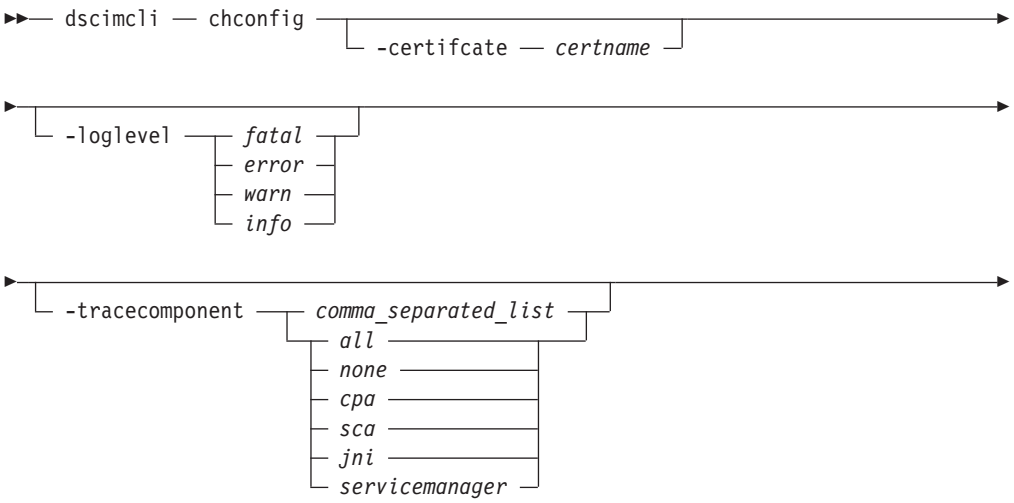
The resulting output:

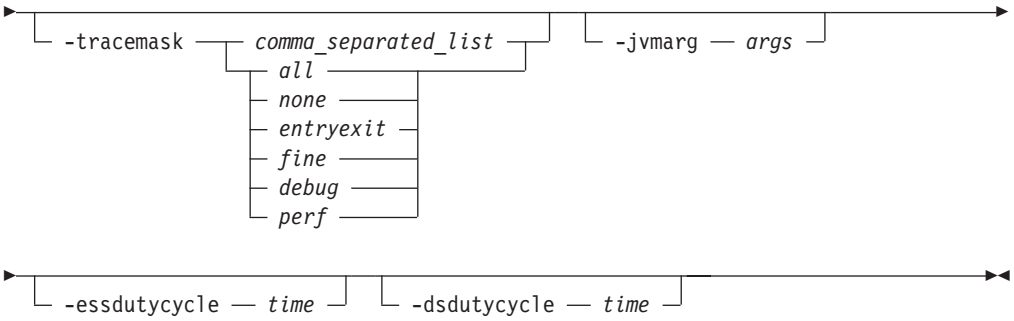
```
Property       Current Value                  After Restart
============== ============================== ==============================
insecureport   5988                           5988
secureport     5989                           5989
certificate    alex                           alex
enablesecure   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
```

Log collection commands

This section describes the CIM agent log collection command.

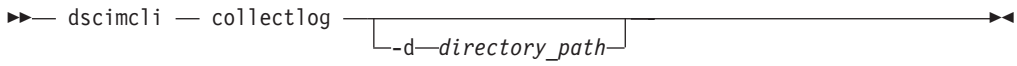
The following command is available:

collectlog

collectlog

Use the collectlog command to remotely collect the CIM agent log files.

Syntax



Parameters

-d *directory_path*
The directory for which you want to write the CIM agent logs. The default directory is DSAGENT_HOME.

```
dscimcli collectlog
```

The resulting output:

```
Old remote log files were listed.
No old log file on the DS Agent side.
New remote log file was successfully created.
getting log file dscim-logs-2009.1.19-18.30.6.zip from DS Agent: complete 100%.
Local log file was successfully created and saved as dscim-logs-2009.1.19-18.30.6.zip.
The new created log file dscim-logs-2009.1.19-18.30.6.zip was successfully got
 from DS Agent side.
The new created log file dscim-logs-2009.1.19-18.30.6.zip was successfully
 deleted on DS Agent side.
```

Chapter 4. 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 run within the context of a namespace. A namespace defines the scope over which a DS Open API schema applies. 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 5. CIM agent communication with the DS Open API

This section describes the communication between the CIM agent and the DS Open API.

The following information is included in this section:

- CIM agent communication concepts
- CIM agent communication methods
- CIM agent functional groups
- 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 most current information for the communication methods is found in the Managed Object Format (MOF) documentation, which is available in the DSCIMCLI package. Extract the package and use a browser to open index.html in the doc directory.

The following sections and tables list the CIM agent intrinsic and extrinsic communication methods and parameters.

Client application calls to intrinsic methods result in CIM agent calls to the device provider if the device provider surfaces the classes or instances that are referenced in the 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 5 describes the parameters of the GetClass method.

Table 5. 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 6 describes the parameters of the GetInstance method.

Table 6. 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 7 describes the parameters of the DeleteInstance method.

Table 7. 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 5.4 or later 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 8 describes the parameters of the CreateInstance method.

Table 8. CreateInstance method parameters

Parameter	Type	Description
Instance	Object	The instance to be created. The instance must be based on a class that is 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 5.4 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 9 describes the parameters of the ModifyInstance method.

Table 9. 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 5.4 does not have any features that use this method.

EnumerateClasses

The EnumerateClasses method returns a single class from the target namespace. Table 10 describes the parameters of the EnumerateClasses method.

Table 10. 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.

Table 10. EnumerateClasses method parameters (continued)

Parameter	Type	Description
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 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 11 describes the parameters of the EnumerateClassNames method.

Table 11. 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 12 describes the parameters of the EnumerateInstances method.

Table 12. EnumerateInstances method parameters

Parameter	Type	Description
ClassName	String	Defines the name of the class for which instances are to be returned.

Table 12. EnumerateInstances method parameters (continued)

Parameter	Type	Description
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 13 describes the parameter of the EnumerateInstanceNames method.

Table 13. 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 14 describes the parameters of the ExecuteQuery method.

Table 14. 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 15 describes the parameters of the Associators method.

Table 15. 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 16 describes the parameters of the AssociatorNames method.

Table 16. AssociatorNames method parameters

Parameter	Type	Description
ObjectName	String	Defines the class name or instances name that is the source of the association.
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 17 describes the parameters of the References method.

Table 17. 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 18 describes the parameters of the ReferenceNames method.

Table 18. 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 19 describes the parameters of the GetProperty method.

Table 19. 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 20 describes the parameters of the SetProperty method.

Table 20. 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 21 describes the parameters of the GetQualifier method.

Table 21. 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 22 on page 35 describes the parameters of the SetQualifier method.

Table 22. 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 23 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 23. 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
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 that are returned by CIMOM communication methods.

Return Error Codes

The CIMOM might return status to the client application in one of the following ways:

- Through HTTP status messages
- Through error codes contained within <METHODRESPONSE> or <IMETHODRESPONSE> XML tags

Table 24 describes the vendor-specific status codes that the CIMOM might return. For CIM standard return codes, see the CIM schema.

Table 24. 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 not valid.
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.
CIM_ERR_INVALID_SUPERCLASS	10	The operation cannot be carried out because 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 not compatible with the type that is specified.
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 not valid.
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.

Table 24. Return error codes for the CIMOM (continued)

Symbolic Name	Code	Definition
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 cannot be overwritten.
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.
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 is not specified.
CIM_ERR_INDICATION_ERROR	107	There is an indication processing error.
CIM_ERR_FAIL_TO_WRITE_TO_CIMOM	108	A write to the CIMOM has failed.
CIM_ERR_SUBSCRIPTION_EXISTS	109	A subscription already exists.
CIM_ERR_INVALID_SUBSCRIPTION_DEST	110	The subscription destination is not valid.
CIM_ERR_INVALID_FILTER_PATH	111	The filter path is not valid.
CIM_ERR_INVALID_HANDLER_PATH	112	The handler path is not valid.
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 a filter that is not supported 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 accept connections.
CIM_ERR_INVALID_CERTIFICATE	119	The correct certificate cannot be found in truststore. The CIMOM cannot accept connections.

Chapter 6. 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 IBM System Storage Support for Microsoft Volume Shadow Copy and Virtual Disk Services software uses a CIM client query to control storage units. The Microsoft Volume Shadow Copy and Virtual Disk Services software uses the CIM technology to manage proprietary devices as open system devices through storage management applications.

Microsoft Volume Shadow Copy Service

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 and Windows Server 2008 operating systems. Microsoft Volume Shadow Copy Service coordinates with a provider and the storage unit to create a consistent shadow copy of a volume or a 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 work with applications that do not support Microsoft Volume Shadow Copy Service technology. The shadow copy can be created while the volume is mounted and the files are in use.

To perform a quick 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. After the FlashCopy operation 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 to be used when rapid restore is necessary. The volumes and shadow copies can also be mounted on a different host and used for application testing or backed up 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 the operating system 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 software installation requirements

Ensure that your system satisfies the hardware and software prerequisites for installing IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software on a Windows Server 2003 or Windows Server 2008 operating system before you start the installation.

You must install the CIM agent *before* you install Microsoft Volume Shadow Copy and Virtual Disk Services. The IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software can be installed on the same system as the CIM agent.

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 or Windows Server 2008
- 133 - 733 megahertz CPU
- 128 - 256 megabytes of random access memory
- 1.5 gigabytes of disk space
- A supported QLogic or Emulex Fibre Channel host bus adapter (HBA)

Software

The following software is required:

- Windows Server 2003 or Windows Server 2008 operating system. The following editions are supported:
  - Standard Server Edition 32-bit version
  - Enterprise Edition, 32-bit version
  - Standard Server Edition, 64-bit version
  - Enterprise Edition, 64-bit version
  - Standard Edition R2 with SP2, 32-bit version
  - Enterprise Edition R2 with SP2, 64-bit version
- Common Information Model (CIM) agent. The CIM agent can be located on the same system 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, use DS CIM Agent 5.3; however, 5.1 is also supported.

- Microsoft Volume Shadow Copy Service compliant backup software

The following software is recommended:

- Windows Server 2003 R2 Service Pack 2. This software contains important VSS fixes from Microsoft, including KB972623, KB957778, KB949391, KB940349, and KB932532
- Windows Server 2008 Service Pack 2
- Windows Server 2008 R2
- SDDDSM multipathing software

Installing the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software

This task installs the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service on a Windows system.

Before you begin

You must satisfy all prerequisites that are listed in the installation requirements section before you start the installation.

Procedure

1. Log on to Windows as an 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. The Welcome panel is displayed.
3. Click **Next** to continue. The License Agreement panel is displayed. You can click **Cancel** at any time to exit the installation. To move back to previous screens while using the wizard, click **Back**.
4. 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. The Choose Destination Location panel is displayed.
5. Click **Next** to accept the default directory where the setup program will install the files, or click **Change** to select a different directory. Click **Next**. The Ready to Install the Program panel is displayed.
6. Click **Install** to begin the installation. To exit the wizard and end the installation, click **Cancel**. The Setup Status panel is displayed.

   The program setup verifies your configuration. After your configuration is verified, the Select CIM Server panel is displayed.
7. Select the required CIM server, or select **Enter the CIM Server address manually**, and click **Next**. The Enter CIM Server Details panel is displayed.
8. Enter the following information in the fields:
   - In the **CIM Server Address** field, type the name of the server where the CIM agent is installed.
   - In the **CIM User** field, type the user name that the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software will use to gain access to the server where the CIM agent is installed. For example, enter the name Administrator.

- In the **CIM Password** field, type the password for the user name that the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software will use to gain access to the CIM agent and click **Next**.

Notes:

a. If these settings change after installation, you can use the ibmvcfg.exe utility to update the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software with the new settings.
b. If you do not have the CIM agent server, port, or user information, contact your CIM agent administrator.

The InstallShield Wizard Complete panel is displayed.

9. Click **Finish**. If necessary, the InstallShield Wizard prompts you to restart the system.

What to do next

If you are connecting to a DS 5.1 or earlier CIM agent, you must perform the following additional configuration steps:

1. Copy the truststore file from the CIM agent server to any location that is on the system where the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service is installed.
2. Open a command prompt and change to the directory where the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service is installed.
3. Issue the following command:

   ```
   ibmcfg set truststore file_name
   ```
   where *file_name* is the name of the truststore file.
4. Issue the following command:

   ```
   ibmcfg set trustpassword ibmstore
   ```
5. Stop and then restart the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service.

Creating the VSS_FREE and VSS_RESERVED pools

This task creates the free volume pool (VSS_FREE) and the reserved volume pool (VSS_RESERVED) that are used to assign volumes to the virtual host.

About this task

Before you can use the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software, you must specify the volumes that can be used as FlashCopy target volumes. You specify the volumes after you create a VSS_FREE pool and a VSS_RESERVED pool. These pools are represented by virtual hosts that are created on the storage unit. After the virtual hosts are created, you can add volumes to the free pool by 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:

Important: If you are using the DS CLI, you must perform these steps in order.

Procedure

1. Create a volume group with the name VSS_FREE or a name that is the same type as the Windows Server 2003 or Windows Server 2008 host. For example, SCSI Map 256.
2. Use the following parameters to create a virtual hostconnect on the storage unit that is named VSS_FREE or another name:

   -profile *Intel - Windows 2003*
   where *Intel - Windows 2003* is the profile to use for the connection.

   -addrdiscovery *LUNPolling*

   -*volgrp*
   where *volgrp* is the name of the volume group you created in step 1.

   -wwname *5000000000000001*
3. Create a volume group with the name VSS_RESERVED or a name that is the same type as the Windows Server 2003 or Windows Server 2008 host. For example, SCSI Map 256.
4. Use the following parameters to create a virtual hostconnect on the storage unit that is named VSS_RESERVED or another name:

   -profile *Intel - Windows 2003*
   where *Intel - Windows 2003* is the profile to use for the connection.

   -addrdiscovery *LUNPolling*

   -*volgrp*
   where *volgrp* is the name of the volume group you created in step 3.

   -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 software installation

This task verifies that the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software is correctly installed on the server.

About this task

Perform the following steps to verify the installation:

Procedure

1. Click **Start** > **All Programs** > **Administrative Tools** > **Services** from Windows server task bar. The Services window opens.
2. Ensure that there is a service named IBM System Storage Support for Microsoft Volume Shadow Copy that is listed, and that **Status** is started and **Startup Type** is Automatic.
3. Open a command prompt window and type the following command:

   ```
   vssadmin list providers
   ```

4. Ensure that the IBM System Storage Support for Microsoft Volume Shadow Copy Service is listed as a provider.

Results

If you are able to perform all of these verification tasks successfully, the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software was successfully installed on the server.

Verifying IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software configuration

This task verifies that the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software is correctly configured on the server.

Before you begin

This task assumes that you have already created the VSS_FREE and VSS_RESERVED pools.

About this task

Perform the following steps to verify the configuration:

Procedure

1. Issue the following command to list all of the volumes for the storage unit:

   ```
   ibmvcfg list all
   ```

2. If the volumes are not listed, perform the following steps:
   a. Check the connectivity of the CIM agent.
   b. Check the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software configuration.
   c. Check the IBMVSS.log file to view detailed information for the settings that are not correct. The IBMVSS.log file is located in the directory where the IBM System Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software is installed.
   d. Use the commands that are provided by the ibmvcg.exe utility to fix any settings that are not correct. See *"IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software configuration commands" on page 45*.

Results

If you are able to perform all of these verification tasks successfully, the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software was successfully configured on the server.

IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software configuration commands

You can change the parameters that you defined when you installed the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software. You must use the ibmvcfg.exe utility to change the parameters.

Table 25 describes the configuration commands that are provided by the ibmvcfg.exe utility.

Notes:

1. If you do not know which settings to provide (for example, passwords or user names) for these commands, contact your system administrator.
2. If you are deleting a FlashCopy relationship, the relationship is not deleted if incremental FlashCopy is activated in the IBM hardware provider. To delete an incremental FlashCopy relationship, use the ibmvcfg.exe utility.

Table 25. Microsoft Volume Shadow Copy and Virtual Disk Services software configuration commands

Command	Description	Example
ibmvcfg *showcfg*	Provides the current settings.	`ibmvcfg showcfg`
Ibmvcfg */h, /help, -?, /?*	Provides help	`ibmvcfg ?`
CIMOM settings		
ibmvcfg set cimomHost *IP or host_name*	Sets the CIMOM host either host IP or host name can be used.	`ibmvcfg set cimomHost 10.1.1.88`
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 cimomPort portnumber*	Specifies the CIMOM port number. The default value is `5989`. For embedded CIMOM secured port number, by default is `6989`.	`ibmvcfg set cimomPort 5989`
ibmvcfg set usingssl *yes/no*	Specifies CIMOM SSL connection. The default value is true.	`ibmvcfg set usingssl yes`
Ibmvcfg timeout *value*	Sets the CIM enumeration time out value in second. The default value is 0. Zero means infinite timeout.	`ibmvcfg set timeout 80`
Volume Shadow Copy Service settings		
ibmvcfg *set vssFreeInitiator WWPN*	Sets the defined free pool on the DS storage. The default value is `5000000000000000`.	`ibmvcfg set vssFreeInitiator 80000000000000AA`
ibmvcfg *set vssReservedInitiator WWPN*	Sets the defined reserved pool on the DS storage. The default value is `5000000000000001`.	`ibmvcfg set vssReservedInitiator 80000000000000AB`

Table 25. Microsoft Volume Shadow Copy and Virtual Disk Services software configuration commands (continued)

Command	Description	Example
Ibmvcfg *set backgroundCopy 0-100*	Specifies copy rate from 0 to 100. The default value is `50`, and 0 zero is no copy.	`ibmvcfg set backgroundCopy 0`
Ibmvcfg *set incrementalFC yes/no*	Enable or disable incremental flashCopy. By default is `false`.	`ibmvcfg set incrementalFC yes`
ibmvcfg *list all -l*	Lists all VDisks, including information about volume ID, UUID, volume name, size, operational state, health status, type of volume, and VDisks to host mappings and host name. Use the –l parameter to output in verbose list column format.	`ibmvcfg list all` `ibmvcfg list all -l`
ibmvcfg *list free -l*	Lists the volumes that are currently in the free pool. Use the –l parameter to output in verbose list column format.	`ibmvcfg list free` `ibmvcfg list free -l`
ibmvcfg *list reserved -l*	Lists the volumes that are currently in the reserved pool. Use the –l parameter to output in verbose list column format.	`ibmvcfg list reserved` `ibmvcfg list reserved -l`
ibmvcfg *list assigned -l*	Lists the volumes that are currently in the assigned pool/host. Use the –l parameter to output in verbose list column format.	`ibmvcfg list assigned` `ibmvcfg list assigned -l`
ibmvcfg *list unassigned-l*	Lists the volumes that are currently in the unassigned pool/host. Use the –l parameter to output in verbose list column format.	`ibmvcfg list unassigned` `ibmvcfg list unassigned -l`
ibmvcfg *list infc -l*	Lists all the FlashCopy relationships on the SAN Volume Controller. This command lists both incremental and non-incremental FlashCopy relationships.	`ibmvcfg list infc` `ibmvcfg list infc -l`
ibmvcfg *add unassigned_volumes*	Adds one or more volumes to the free pool of volumes.	`ibmvcfg add 13036511188` `ibmvcfg add LUN18`
ibmvcfg *rem free_volumes*	Removes one or more volumes from the free pool of volumes.	`ibmvcfg rem 13036511188` `ibmvcfg rem LUN18`
ibmvcfg *del target_volumes*	Deletes one or more FlashCopy relationships. Use the serial number of the FlashCopy target to delete the relationship.	`ibmvcfg del 13036511188` `ibmvcfg del LUN18`
Virtual Disk Service settings		

Table 25. Microsoft Volume Shadow Copy and Virtual Disk Services software configuration commands (continued)

Command	Description	Example
Ibmvcfg *set trace value*	Sets the trace log debugging information from value 1 to 7. The default value is 3.	`ibmvcfg set trace 7`

IBM System Storage support for Microsoft Volume Shadow Copy and Virtual Disk Services software error codes

Error codes provide information on the status of operations. Error codes are logged in the Windows Event Monitor and in the Microsoft Volume Shadow Copy and Virtual Disk Services software log file that is located in the installation directory.

Table 26 lists the return error codes and their symbolic names and definitions.

Table 26. IBM System Storage support for Microsoft Volume Shadow Copy and Virtual Disk Services software error codes

Code	Symbolic Name	Definition
1000	ERR_JVM	JVM Creation failed.
1001	ERR_CLASS_NOT_FOUND	Class not found: %1.
1002	ERR_MISSING_PARAMS	Some required parameters are missing.
1003	ERR_METHOD_NOT_FOUND	Method not found: %1.
1004	ERR_REQUIRED_PARAM	A missing parameter is required. Use the configuration utility to set this parameter: %1.
1600	ERR_RECOVERY_FILE_CREATION_FAILED	The recovery file was not created.
1700	ERR_ARELUNSSUPPORTED_IBMGETLUNINFO	ibmGetLunInfo failed in AreLunsSupported.
1800	ERR_FILLLUNINFO_IBMGETLUNINFO	ibmGetLunInfo failed in FillLunInfo.
1900	ERR_GET_TGT_CLEANUP	Failed to delete the following temp files: %1.
2500	ERR_LOG_SETUP	Error initializing log.
2501	ERR_CLEANUP_LOCATE	Unable to search for incomplete Shadow Copies. Windows Error: %1.
2502	ERR_CLEANUP_READ	Unable to read incomplete Shadow Copy Set information from file: %1.
2503	ERR_CLEANUP_SNAPSHOT	Unable to cleanup snapshot stored in file: %1.
2504	ERR_CLEANUP_FAILED	Cleanup call failed with error: %1.

Table 26. IBM System Storage support for Microsoft Volume Shadow Copy and Virtual Disk Services software error codes (continued)

Code	Symbolic Name	Definition
2505	ERR_CLEANUP_OPEN	Unable to open file: %1.
2506	ERR_CLEANUP_CREATE	Unable to create file: %1.
2507	ERR_HBAAPI_LOAD	HBA: Error loading hba library: %1.
3000	ERR_ESSSERVICE_EXCEPTION	ESSService: An exception occurred. Check the ESSService log.
3001	ERR_ESSSERVICE_LOGGING	ESSService: Unable to initialize logging.
3002	ERR_ESSSERVICE_CONNECT	ESSService: Unable to connect to the CIM agent. Check your configuration.
3003	ERR_ESSSERVICE_SCS	ESSService: Unable to get the Storage Configuration Service. Check your configuration.
3004	ERR_ESSSERVICE_INTERNAL	ESSService: An internal error occurred with the following information: %1.
3005	ERR_ESSSERVICE_FREE_CONTROLLER	ESSService: Unable to find the VSS_FREE controller.
3006	ERR_ESSSERVICE_RESERVED_CONTROLLER	ESSService: Unable to find the VSS_RESERVED controller. Check your configuration.
3007	ERR_ESSSERVICE_INSUFFICIENT_TARGETS	Unable to find suitable targets for all volumes.
3008	ERR_ESSSERVICE_ASSIGN_FAILED	ESSService: The assign operation failed. Check the CIM agent log for details.
3009	ERR_ESSSERVICE_WITHDRAW_FAILED	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 software

You can use the Add or Remove Programs tool that is provided with Windows operating system to uninstall the IBM System Storage support Microsoft Volume Shadow Copy Service and Virtual Disk Service software.

About this task

Perform the following steps to uninstall the IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software:

Procedure

1. Log on to your system as the local administrator.
2. Click **Start** > **Control Panel**. The Control Panel window opens.
3. Double-click **Add or Remove Programs**. The Add or Remove Programs window opens.
4. Select **IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service** and click **Remove**.
5. Click **Yes** when you are asked if you want to completely remove the selected application and all of it components. The progress window quickly opens and closes.
6. When the Finish window opens, click **Finish**. The removal is now complete.

Results

The IBM System Storage support for Microsoft Volume Shadow Copy Service and Virtual Disk Service software is no longer installed on the Windows system.

Chapter 7. IBM VSS Hardware Provider 4.2.1 support for VMware

This section provides the steps to configure IBM VSS Hardware Provider 4.2.1 support for VMware.

IBM VSS Hardware Provider for DS8000 provides support for Windows Server in VMware ESX Server. This feature is necessary for the Windows Server to issue snapshots in the VMware virtual platform.

Because the copy service is actually a volume-level copy, the Hardware Provider uses the raw device mapping feature of ESX Server, by which an entire volume would be physically attached to the virtual machine. For more information about the raw disk mapping feature in ESX Server, refer to the VMware site.

For the Hardware Provider to manipulate raw disk mapping disks, it needs to interact with the ESX Server during the snapshot. This is done through the VMware Web Service on the ESX Server which holds the virtual machine. This section describes how to set up the Hardware Provider and how the VSS Hardware Provider works in a VMware virtual platform.

Prerequisites

The following requirements must be met before configuring IBM VSS Hardware Provider 4.2.1 support for VMware.

Platforms Supported

The VSSVDS provider supports the following ESX Server platforms:

- vSphere ESX Server 4.x
- vSphere ESXi Server 4.x

VMware Tools

Install VMware Tools to provide communication between the ESX Server web services and VM. VMware Tools collects the guest-related information (such as the IP address, hostname, and so on).

To install the VMware Tools, power-on the guest OS, and select the **Install/Upgrade VMWare Tools** on the VIClient menu for the specific guest. Then login to the Windows Server guest and install the package.

vSphere Web Services

The vSphere Web Services should be up and running for the Hardware Provider to work in the guest Windows Server. The Web Services is on by default as ESX/ESXi OS loaded.

To check whether the Web Services is online, use a web browser to access the URL, for example, https:// *189.0.0.222* /mob . It should prompt for a user credential to log in to the hosted web services. (The IP address, *189.0.0.222* is an example ESX server IP.)

If the vSphere Web Services fails to run, refer to the *ESXi Configuration Guide*, section "Modifying ESXi Web Proxy Settings," to configure the proxy.xml, and then restart the service.

User privileges

The following privileges need to be assigned to the user:

Host->Configuration->Storage partition configuration

Virtual machine->Configuration->Raw device

Virtual machine->Configuration->Change resource

Virtual machine->Configuration->Add or remove device

If the Hardware Provider communicates with vCenter, the Read-only role needs to be assigned to the data center to which the ESX Server belongs. A role with the privileges described above should be created. The role settings in vCenter are shown in Table 27.

Table 27. Role settings in vCenter

User/Group	Role
vCenter	No access
Data center	Read-only
ESX Server	vssrole
Virtual machine	

Setting Hardware Provider parameters for VMware

This section provides the steps to set the Hardware Provider parameters for VMware.

About this task

There are several Hardware Provider parameters for the VMware guest support feature, and they are mainly for the Hardware Provider to communicate with the ESX Server Web Services to manipulate the raw device mapping disks during a snapshot.

There are two cases which require the setting up of parameters for VMware:

- The snapshot disk is discovered by ESX server through Fibre Channel, and mapped to a virtual machine as a raw device mapping disk.
- The snapshot disk is discovered by ESX server through ESX software iSCSI, and mapped to a virtual machine as a raw device mapping disk.

There are four provider parameters which are available only on the VMware virtual platform:

vmhost
The VMware Web Service located on the ESX Server, such as https://ESX_Server_IP/sdk.

vmuser
The user who has access to the ESX Server with authority to perform raw device mapping disk operations.

vmpassword
The password for the vmuser to log in.

vmcredential
The session credential store path for the ESX Server used by Java.

The vmcredential path is the full path name of the Java key file. “Generate Java key store” shows the procedure to generate the Java key store.

You can set the parameters with the IBM VSS configuration tool ibmvcfg, for example:

```
C:\Program Files\IBM\Hardware Provider for VSS-VDS>ibmvcfg set vmhost https://9.11.110.115/sdk
```

Generate Java key store

There are two steps to generate the Java credential key store.

Procedure

1. Obtain the ESX Server certificates. You can obtain the server certificate in two ways:
   - To obtain server certificates using vSphere Client:
     a. Create a directory named VMware-Certs (at the root level) for the certificates: C:\VMware-Certs .
     b. Install the vSphere Client on the development workstation, if necessary.
     c. Launch the vSphere Client and then navigate to the ESX, ESXi, or vCenter Server web server. A security warning message box displays regarding the certifying authority for the certificate.
     d. Click **View Certificate** to display the Certificate properties page.
     e. Click the **Details** tab.
     f. Click **Copy to File...** to launch the Certificate Export wizard.
     g. Select **DER encoded binary X.509** (the default), and click **Next**.
     h. Click **Browse...** and navigate to the C:\VMware-Certs subdirectory.
     i. Enter a name for the certificate that identifies the server to which it belongs: C:\VMware-Certs\<*server_name*>.cer .
   - To obtain server certificates using the secure shell client application:
     a. Connect to the ESX system using an SSL client from the development workstation. Remote connections to the ESX service console as root are effectively disabled, so you must connect as another user with privileges on the server to obtain the certificate.

        The server certificate filenames and locations of ESX and vCenter Server are listed in Table 28.

Table 28. Server certificate filenames and locations

Server	Directory location for certificate	Certificate
ESX 4.0	/etc/vmware/ssl/	rui.crt
vCenter Server 4.0	C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\	

     b. Copy the certificates from the server to the certificate subdirectory of the development workstation, using a unique filename for the certificate (assuming you are copying multiple default certificates from multiple ESX systems, for example).
2. Create a directory for the Java key store, for example C:\VMware .
3. Use the Java keytool utility to import a certificate, using the following syntax:

```
keytool -import -file <certificate_filename> -alias <server_name> -keystore vmware.keystore
```

   For example:

```
C:\Program Files\IBM\Hardware Provider for VSS-VDS\jre\bin>
keytool.exe -import -file C:\tools\rui.crt -keystore C:\VMware\vmware.keystore
```

A prompt requesting a password for the keystore appears: *Enter keystore password:*

4. Create a password for the keystore by entering it at the prompt. The keystore utility displays the certificate information at the console.
5. At the end of the certificate information, a prompt displays a request for confirmation that the certificate is trusted. Type **yes** and press **Enter** to import the certificate into the vmware.keystore keystore.

   The console displays this message:

   ```
   Certificate was added to keystore.
   ```

6. Set the vmcredential to be the vmware.keystore path, as follows:

   ```
   > ibmvcfg set vmcredential C:\VMware\vmware.keystore
   ```

7. Use **ibmvcfg showcfg** to display that the configuration is correctly saved.

Configuring NPIV support

This section provides the steps to configure NPIV support for VMware.

About this task

NPIV is an extension to the Fibre Channel industry standard. In a server virtualization environment, NPIV allows each VM to have a unique Fibre Channel World Wide Name (WWN), enabling multiple virtual machines to share a single physical HBA and switch port.

Prerequisites

About this task

The following software and hardware requirements must be met to enable NPIV:

- NPIV needs to be supported on the switch connected to the HBA.
- HBAs must support NPIV. The following vendors and models of HBAs are supported:
  - Brocade: any 4 Gbit/sec or 8 Gbit/sec HBA
  - Emulex: 4Gbit/sec HBA running firmware level 2.70a5 or later; all Emulex 8 Gbit/sec HBAs running firmware 1.00a9 or later
  - QLogic: any 4 Gbit/sec or 8 Gbit/sec HBA
- NPIV is completely transparent to storage arrays, so no specific support is required.
- NPIV can be used only with raw device mapping (RDM) disks. VMFS disks do not support NPIV. To implement NPIV, the physical HBAs port WWN on an ESX Server host must have access to all LUNs that are to be accessed by VMs.
- If you deploy a VM from a template or a clone, the new VM does not retain the WWN.

Setting up NPIV

About this task

This section provides the procedure for setting up NPIV. For more detailed information, refer to the VMware site.

Server administrator tasks

1. Do not power on your VM for this procedure; your virtual machine needs to be powered off.
2. Add a raw device mapping disk to the virtual machine.
3. Enable NPIV with VI Client by assigning virtual WWPNs.
4. Record the node WWN and the port WWNs. Give this information to the storage administrator to zone and LUN-mask the back-end storage. (Follow the Storage Administrator steps below to zone and LUN-mask.)
5. After the storage administrator completes zoning and configuration of the storage, you can power on the VM.

Storage administrator tasks

1. Login to the switch and create separate zones for virtual port WWNs and physical HBA port WWNs. There is not a fixed way on how to zone, but it is best practice to zone all the physical HBA port WWNs in a single zone with storage initiator, and then individually zone each VM's virtual HBA port WWNs to a storage array port WWN.
2. On the storage subsystem, create separate hosts (SVC) or hostconnections (DS8000) with separate volume groups for physical HBA ports and virtual HBA ports. For example, in SVC 5.1, create a host with physical HBA WWPNs, and create another host for VM with virtual HBA WWPNs.
3. There are now two hosts, one for physical HBA port WWPNs and one for virtual port WWPNs. For a LUN to work through NPIV, it needs to be mapped to both hosts.

Verify that VM is functioning correctly

About this task

After the setup procedures are completed, the NPIV is functioning after VM is powered on. To verify that I/O traffic is going through the virtual port (depending on the host HBA), SSH into the physical ESX Server and issue the following command, as applicable to your configuration (replace number "1" at the end of the cat command with the number of your HBA):

- Brocade HBA: **cat /proc/bfa/1**
- QLogic HBA: **cat /proc/scsi/qla2300/1**
- Emulex HBA: **cat /proc/scsi/lpfc/1**

Everything is working if you see the virtual WWNs (also known as vPorts) listed in the resulting display.

Note: You can enable NPIV only after at least one raw device mapping disk has been attached to the VM.

Taking snapshots with NPIV

About this task

The IBM VSS provider automatically detects whether the NPIV is enabled. If the NPIV is enabled and correctly functioning, the provider takes proper actions during the various snapshot stages.

Create snapshot

When you create a snapshot, the provider maps the snapshot target LUN

to both the physical HBA WWPNs and virtual WWPNs. Then the LUN is assigned to the virtual machine from the ESX Server as a raw device mapping disk.

Delete snapshot
When you delete a snapshot, the VSS provider first unassigns the raw device mapping disk from the virtual machine. Then the LUN is masked from both physical HBA WWPNs and virtual WWPNs.

Import snapshot
The import operation uses NPIV when it is enabled and functioning. The process is similar to creating a snapshot. The VSS provider first maps the snapshot target LUN to both the physical HBA WWPNs and virtual WWPNs of the destination server. Then the LUN is assigned to the virtual machine from the ESX Server as a raw device mapping disk.

Mask snapshot
The mask operation causes the raw device mapping disk to be removed from virtual machine (as in deleting a snapshot). Then the LUN is masked from both physical HBA WWPNs and virtual WWPNs.

Taking snapshots with various protocols

This section provides the steps to take snapshots with various protocols.

About this task

The VSS configuration tool provides the user a choice of what protocol to use when more than one storage protocol is available. The choices are:

- Auto
- Fibre Channel (FC)
- iSCSI

You can set the storage protocol with the command. For example:

```
>ibmvcfg set storageProtocol FC
```

The choice, **auto** means that the VSS provider decides which protocol to use. “Storage protocol priority” provides more information about the storage protocol priority.

Storage protocol priority

About this task

When several protocols coexist, there should be a priority defined for what protocol to use during the snapshot. For example, this is a case that requires a decision on what protocol to use: an ESX Server has Fibre Channel HBA and also has ESX Server software iSCSI enabled.

As for which protocol to use, it depends on the **storageProtocol** parameter of the provider configuration, as well as what protocols are available.

Among the various protocols, ESX Server Fibre Channel has the highest priority. This means that when storageProtcol is set to **auto**, the provider first checks whether ESX Server Fibre Channel is available. The provider tries other protocols only when the Fibre Channel protocol is not available.

Special cases and exceptions

About this task

The VSS Hardware Provider offers the user a choice of storage protocol, so it is the user's responsibility to ensure that a change of storage protocol and provider settings for VMware does not impact the previously created snapshots. For example, the following case illustrates a problem caused by a change in settings:

1. Create snapshot with Fibre Channel protocol
2. Incorrectly modify or clear the VMware settings
3. Delete the previous created snapshot

In this case, the flashcopy map is removed from the storage and the target LUN is unmapped from the hosts. However, the raw device mapping file remains on the ESX Server because the VMware settings (vmhost, vmuser, vmpassword, or vmcredential) have been incorrectly set, leaving the provider unable to communicate with the ESX Server.

In the above case, a warning message is displayed whenever the user tries to change the VMware settings via ibmvcfg. There is no need to set up the provider parameters for VMware (such as vmhost, vmuser, and so on).

Note: When the VMware settings are correct, a deletion (which would be step 4 in the above procedure) can still be successful with the removal of the raw device mapping file.

Chapter 8. IBM VSS Hardware Provider 4.2.1 support for Hyper-V

This section provides the steps to take shadow copies in a Hyper-V guest OS with IBM VSS Hardware Provider for DS8000.

There is no Fibre Channel HBA on a guest OS. IBM VSS Hardware Provider serves as a bridge to associate the Fibre Channel HBA on a host with the guest OS during the creation and deletion of a shadow copy. Privileges to access the host WMI are required to support this feature.

The Hardware Provider supports shadow copy on passthrough disks in the guest OS, because it cannot support the hardware information of a virtual hard disk. The volume shadow copy's target LUN is automatically attached to a guest OS as a passthrough disk by the Hardware Provider.

Primary configuration of Hyper-V

This section provides the steps to create shadow copies in a Hyper-V guest OS.

Prerequisites

Before you begin

The following requirements must be met before configuring Hyper-V:

- IBM VSS Hardware Provider 4.2.1
- Server Hardware. Microsoft recommends server configuration for Microsoft Windows Server 2008 Hyper-V.
- Microsoft Windows Server 2008 Hyper-V
- Multi-pathing I/O (MPIO) software. (Available from your storage array vendor.)

Configuring the Hyper-V (host) server

This section provides the steps to configure the Hyper-V (host) server.

Procedure

1. Install Microsoft Windows Server 2008 x64.
2. Install the Hyper-V role on the Windows Server via Server Manager (reboot needed).
3. Disable automount by turning off automount for the disks on host with the following commands:
   a. C:\>diskpart
   b. C:\>automount disable
4. Allow for remote administration on physical host. Use the following command to enable the Windows Firewall:

   ```
   netsh firewall set service RemoteAdmin enable
   ```
5. Install the MPIO driver that is included with Windows 2008.
6. Install the MPIO driver that is supplied by your storage vendor.
7. Install and configure Hyper-V guest OS via Hyper-V Manager. The guest OS should be windows 2003 R2 or above.

Configuring the IBM VSS Hardware Provider

This section provides the steps to configure the IBM VSS Hardware Provider.

Procedure

1. Logon to the Hyper-V guest OS and install IBM VSS Hardware Provider.x
2. Set the following parameters to access the host server:
   - Host server IP address
   - Domain
   - User name

   a. A. The user should have the following privileges:
      - Access to WMI on the host server
      - Query of WMI objects in the following name spaces:
        - root/cimv2
        - root/wmi, root/default
        - root/virtualization
      - Management of resources in the name space root/virtualization

   b. Domain should be set as host name if the user does not belong to a Windows domain.

   c. Use the following commands to set the parameters:
      - Set IP address of the host server:

        ibmvcfg set vmhost <*hyper-V host IP address*>
      - Set user name:

        ibmvcfg set vmusername <*hyper-V host user name which can manage hyper-V*>
      - Set password:

        ibmvcfg set vmpassword <*hyper-V host user password*>
      - Set domain:

        ibmvcfg set vmdomain <*hyper-V host user domain*>

   d. To display and review the settings, issue the command, **ibmvcfg showcfg**.

Configuring source volumes

This section provides the steps to configure source volumes.

About this task

Because the Hardware Provider supports taking shadow copies only for volumes that are based on disks from DS8000, the disks need to be assigned to the guest OS by passthrough mode.

Procedure

1. Shutdown the guest OS.
2. Add SCSI controller to the guest OS.
3. Add the passthrough disk drive to the guest OS (the guest OS can be running). The disks should be in the offline state on the host, otherwise they cannot appear in the physical hard disk combination box.
4. Logon to the guest OS, create a volume on the newly added hard disk, and assign a drive letter or mount point to the volume.

Note: Volumes on several dynamic disks are not supported.

Taking snapshots

This section provides the steps to configure source volumes

About this task

You need to configure LUNs as the snapshot target in the free pool on storage. The target LUNs must be the same size as source LUNs. Before taking a snapshot for the volume on the guest OS, you can run the following command to check whether the configuration is correct (*X* is the driver letter or mount point to take the snapshot; one or more drive letters or mount points are supported by this command):

```
ibmvcfg testsnapshot X:
```

The procedures for taking, deleting, masking, re-synchronizing, and importing snapshots are the same as for the physical host. Hardware Provider attaches the target LUNs to the physical host, then assigns it to guest OS as a passthrough disk when taking or importing snapshots. The Hardware Provider removes the target LUN from guest OS before detaching it from physical host when deleting or masking a snapshot.

Advanced configuration of Hyper-V

This section describes N_Port Virtualization (NPIV) and storage protocol priority supports in the Hardware Provider.

Before you begin

The following requirements must be in place before configuring NPIV:

- NPIV-enabled Fibre Channel adapter
- NPIV-enabled Fibre Channel switch
- Fibre Channel HBA Manager and Agent with V-Port creation feature
- NPIV WMI provider installed on host (most of the Fibre Channel drivers implement it.)

About this task

NPIV uses HBA technology to create virtual HBA ports on hosts by abstracting the underlying physical port. This support enables a single physical Fibre Channel HBA port to function as multiple logical ports, each with its own identity. Each virtual machine can then attach to its own virtual HBA port and be independently zoned to a distinct and dedicated World Wide Port Name (WWPN).

For more information about NPIV and HBA technology, refer to your HBA vendor documentation.

Creating virtual ports

This section provides the steps to create virtual ports.

Procedure

1. Open the Fibre Channel HBA Manager GUI.
2. Select a physical port.

3. Create a virtual port on the physical port.

Creating zoning

This section provides the steps to create zoning.

Procedure

1. Create an alias and zone with a previously created virtual port and storage, but do not add the host WWN to the zone. The only two things in that zone are the new NPIV port and the storage.
2. You do not need to reboot the host to make the NPIV port available.

Creating storage

This section provides the steps to create storage.

About this task

To create storage, add the virtual port to the LUN that contains the guest. You do not need to add the physical port to the LUN.

Configuring the host disk

This section provides the steps to configure the host disk.

Procedure

1. For virtual disks:
   a. Bring the new LUN online and initialize it.
   b. Assign drive letters to the volume that contains the guest OS configuration files and VHDs.

      Note: A volume with a mount point does not support NPIV.
2. For pass through disks:
   a. You need two LUNs per guest: one for the configuration files; and the other to install the OS on.
   b. Assign a drive letter to the volume containing configuration files.
   c. Ensure that the disk is offline to install the OS.

Deploying guests

This section provides the steps to deploy guests.

Deploying with Hyper-V Manager

Procedure

1. Open Hyper-V Manager.
2. In the Actions panel, click **New** > **Virtual Machine ...**.
3. When you are prompted for a location for the virtual machine, choose the volume that is on the LUN that you created earlier.
4. After Memory and Networking configurations, specify the hard disk on which to install the guest OS.
   - For a virtual hard disk, locate it on a volume that is on the LUN through the virtual port.
   - For a passthrough disk, it should be from the virtual port, be marked offline, and be configured as an MBR disk type. GPT and dynamic do not work with

a passthrough disk. If the disk is previously configured as GPT or dynamic, you must bring the disk online and convert it, which means that you need to shut down the guest.

Deploying with SVCMM

Procedure

1. If the host is managed by Microsoft System Center Virtual Machine Manager (SCVMM), you can create a virtual machine through it.
2. When you get to the screen prompting for the host on which to place the guest, select the one that has the virtual port active.
3. When you are prompted for a location for the files, click **Browse** and select the LUN created earlier. If you do not see it, you might need to refresh the disks or check the host to make sure the disk is online and formatted.
4. The configuration of the disk on which to install the guest OS is the same as for Hyper-V Manager.

Configuring source volumes

This section provides information for configuring source volumes.

About this task

The steps are the same as for primary configuration, except the LUN is through virtual port.

Verifying NPIV configuration

This section provides the steps to verify NPIV configuration.

About this task

To ensure that a LUN is from a virtual port, you can open the Fibre Channel HBA Manager and see whether the LUN is under the virtual port (some of the Fibre Channel HBA Managers do not support this feature).

Taking a snapshot

This section provides the steps to take a snapshot.

About this task

The procedure for taking a snapshot is the same as for primary configurations, except the Hardware Provider attaches the LUN to the host through a virtual port automatically.

Troubleshooting the Hyper-V configuration

This section provides troubleshooting information for Hyper-V.

Before you begin

The provider cannot find any Fibre Channel initiator

About this task

Procedure

1. Verify the Fibre Channel configurations on host, SAN, and storage. Ensure that there is at least one initiator installed on host or guest OS.
2. Verify the settings for Hyper-V. Ensure that the IP address, user name, password, and domain are set correctly, the user is authorized to access WMI on host, and domain is set as host's computer name if it is not domain user.
3. Ensure that the storage protocol setting and existing initiator configuration are not conflicting.

The volume is not supported by provider

Procedure

1. Verify that the volume on the disk is supported by the Hardware Provider. The disk needs to be from DS8000, and be added to the guest OS as a passthrough disk.
2. Virtual hard disks are not supported by the Hardware Provider, though they can be on the LUN from DS8000.

Importing shadow copy failed or locating LUN failed while taking shadow copy

Procedure

1. A volume on several dynamic disks is not supported by Hyper-V. Though the Hardware Provider can support dynamic disks, Hyper-V cannot add the dynamic disks to the guest OS. Ensure that the source volume is on a basic disk. Because MS VSS and the Hardware Provider cannot check this situation during the taking of a snapshot, the best way to avoid this case is to run the **ibmvcfg testsnapshot ...** command to check whether the current configuration supports snapshots for the volumes.
2. There is no SCSI controller or sufficient address space on the SCSI controller on the guest OS. Shutdown guest OS and add a SCSI controller to it.

Target LUNs are not attached to host through a virtual port

About this task

Procedure

1. Verify virtual port configuration on the host, SAN, and storage.
2. Verify that guest OS configuration files are on the LUN through a virtual port. The volume on the LUN must be assigned a drive letter; mount point is not supported.

Notices

The information provided by this media supports the products and services described with consideration for the conditions described herein.

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 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 PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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.

Trademarks

This topic lists trademarks that appear in this information.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web by going to the Copyright and trademark information website.

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 and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds 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.

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 statement

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply 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 in order 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 user's 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 Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (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 non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Tel: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG 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 Mabnahmen 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

```
International Business Machines Corp.
New Orchard Road
Armonk,New York 10504
Tel: 914-499-1900
```

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland
Technical Regulations, Department M456

IBM-Allee 1, 71137 Ehningen, Germany
Tel: +49 7032 15-2937
e-mail: tjahn@de.ibm.com

Generelle Informationen:

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、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。 VCCI-A

Translation:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

Japanese Electronics and Information Technology Industries Association (JEITA) statement

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)

高調波ガイドライン適合品

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)

高調波ガイドライン準用品

Korea Communications Commission (KCC) Electromagnetic Interference (EMI) Statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

f2c01252

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

rusemi

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。

taiemi

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

Index

A

about this document
  sending comments xii
about this guide
  notational conventions 11
anatomy of a command line 13
association, DS Open API 23
AssociatorNames method parameters 32
Associators method parameters 31

C

certificate commands 16
chconfig command 19
CIM agent
  commands 14
  communication concepts 25
  components 3
  concepts 3
  configuration programs 14
  configuring for HMC 7
  disabling on the HMC 9
  enabling on the HMC 7
  functional groups 36
  installation overview for HMC 6
  installing the dscimcli utility 6
  intrinsic and extrinsic communication methods 25
  invoking 11
  overview 1
  security 4
  verifying connection to storage unit 8
CIM Agent
  communication with the DS Open API 25
CIM agent communication methods 26
CIM API communication methods
  AssociatorNames 32
  Associators 31
  CreateInstance 27
  DeleteInstance 27
  DeleteQualifier 35
  Enumerate 28
  EnumerateClass 29
  EnumerateInstanceNames 30
  EnumerateInstances 29
  EnumerateQualifiers 35
  error codes 36
  ExecQuery 30
  GetClass 26
  GetInstance 26
  GetProperty 33
  GetQualifierGet 34
  ModifyInstance 28
  ReferenceNames 33
  References 32
  SetProperty 34
  SetQualifier 34
CIM component definitions
  namespace 23
  object name 23
CIM component definitions core classes 23
CIMOM operations
  client communication 25
  intrinsic and extrinsic methods 25
class, DS Open API 23
CLI
  example commands 13
command line string 13
commands
  certificate 16
  chconfig 19
  configuration management 18
  example of a typical command line string 13
  getcert 17
  help 15
  interactive mode 11
  lscert 16
  lsconfig 19
  mkcert 18
  operational 14
  rmcert 17
  shell mode 11
comments, sending xii
configuration management commands 18
configuration verification
  Microsoft Virtual Disk Service 44
  Microsoft Volume Shadow Copy Service 44
  Virtual Disk Service 44
  Volume Shadow Copy Service 44
core classes, CIM 23
CreateInstance method parameters 27

D

DeleteInstance method parameters 27
documentation
  improvement xii
DS Open API component definitions
  elements 23

E

elements, DS Open API 23
emphasis 13
EnumerateClasses method parameters 28
EnumerateInstanceNames method parameters 30
EnumerateInstances method parameters 29
EnumerateQualifiers method 35
error codes
  Microsoft Virtual Disk Service 47
error codes *(continued)*
  Microsoft Volume Shadow Copy Service 47
  Virtual Disk Service 47
  Volume Shadow Copy Service 47
error codes returned by the CIMOM 36
ExecQuery method parameters 30

F

functional groups 36

G

getcert command 17
GetClassGetClass method parameters 26
GetInstance method parameters 26
GetProperty method parameters 33
guidelines for invoking the CIM agent 11

H

hardware
  required for Microsoft Virtual Disk Service 40
  required for Microsoft Volume Shadow Copy Service 40
  required for Virtual Disk Service 40
  required for Volume Shadow Copy Service 40
hardware management console
  CIM agent limitations 5
  configuring the CIM agent 7
  enabling the CIM agent 7
  installation overview 6
help command 15
HMC
  disabling the CIM agent 9
Hyper-V 59
  configuration, advanced
    guests, deploying 62
    host disk, configuring 62
    N_Port Virtualization (NPIV) 61
    NPIV configuration, verifying 63
    snapshots, taking 63
    source volumes, configuring 63
    storage protocol priority supports 61
    storage, creating 62
    virtual ports, creating 61
    zoning, creating 62
  configuration, primary 59
    Hyper-V (host) server, configuring 59
    IBM VSS Hardware Provider, configuring 60
    snapshots, taking 61
    source volumes, configuring 60
  configuration, troubleshooting 64

I

IBM VSS Hardware Provider 4.2.1
  support for Hyper-V 59
    configuration, advanced
      guests, deploying 62
      host disk, configuring 62
      N_Port Virtualization (NPIV) 61
      NPIV configuration, verifying 63
      snapshots, taking 63
      source volumes, configuring 63
      storage protocol priority supports 61
      storage, creating 62
      virtual ports, creating 61
      zoning, creating 62
    configuration, primary 59
      Hyper-V (host) server, configuring 59
      IBM VSS Hardware Provider, configuring 60
      snapshots, taking 61
    configuration, troubleshooting 64
    source volumes, configuring 60
IBM VSS Hardware Provider 4.2.1
  support for VMware
    configuring 51
    Hardware Provider parameters for VMware, setting 52
    NPIV support, configuring 54
    prerequisites 51
    snapshots, taking with various protocols 56
ibmvcfg commands 45
indication, DS Open API 23
installation
    dscimcli utility 6
    overview for HMC 6
installation verification
    Microsoft Virtual Disk Service 43
    Microsoft Volume Shadow Copy Service 43
    Virtual Disk Service 43
    Volume Shadow Copy Service 43
installing
    Microsoft Virtual Disk Service 41
    Microsoft Volume Shadow Copy Service 41
    Virtual Disk Service 41
    Volume Shadow Copy Service 41
invoking the CIM agent 11

L

limitations
    CIM agent 5
lscert command 16
lsconfig command 19

M

method, DS Open API 23
Microsoft Virtual Disk Service
    checking configuration 44
    checking installation 43
    error codes 47
    installing 41
    required hardware 40
    required software 40
    uninstalling 49
    VSS_FREE 42
    VSS_RESERVED 42
Microsoft Virtual Disk Service *(continued)*
    required hardware 40
    required software 40
    uninstalling 49
    VSS_FREE 42
    VSS_RESERVED 42
Microsoft Volume Shadow Copy Service
    checking configuration 44
    checking installation 43
    error codes 47
    installing 41
    required hardware 40
    required software 40
    uninstalling 49
    VSS_FREE 42
    VSS_RESERVED 42
mkcert command 18
ModifyInstance method parameters 28

N

NamesEnumerateClassNames method parameters 29
namespace, CIM 23
notational conventions
    emphasis 13
    special characters 13

O

object name, CIM 23
operational commands 14

P

parameters
    changing using ibmvcfg.exe utility 45
pool
    VSS_FREE 42
    VSS_RESERVED 42
property, DS Open API 23

Q

Qualifier method parameters 34
qualifier, DS Open API 23

R

raw device mapping 51
reader feedback, sending xii
reference, DS Open API 23
ReferenceNames method parameters 33
References method parameters 32
rmcert command 17

S

schema, DS Open API 23
sending
    comments xii
SetProperty method parameters 34
SetQualifier method parameters 34
software
    required for Microsoft Virtual Disk Service 40
    required for Microsoft Volume Shadow Copy Service 40
    required for Virtual Disk Service 40
    required for Volume Shadow Copy Service 40
special characters 13
storage unit
    verifying connection to CIM agent 8

T

Trademarks 66

U

uninstalling
    Microsoft Virtual Disk Service 49
    Microsoft Volume Shadow Copy Service 49
    Virtual Disk Service 49
    Volume Shadow Copy Service 49

V

Virtual Disk Service
    checking configuration 44
    checking installation 43
    error codes 47
    installing 41
    required hardware 40
    required software 40
    uninstalling 49
    VSS_FREE 42
    VSS_RESERVED 42
VMware
    configuration
      Hardware Provider parameters, setting 52
    configuring 51
    IBM VSS Hardware Provider 4.2.1, support for 51
    prerequisites 51
Volume Shadow Copy Service
    checking configuration 44
    checking installation 43
    error codes 47
    installing 41
    required hardware 40
    required software 40
    uninstalling 49
    VSS_FREE 42
    VSS_RESERVED 42
VSS VMware
    configuration
      NPIV support 54
    snapshots, taking with various protocols 56
VSS_FREE 42
VSS_RESERVED 42

W

Windows
installing the dscimcli utility 6

Printed in USA

GC35-0516-10