

IBM Spectrum Control
Version 5.3.5

Administrator's Guide



Note:

Before using this information and the product it supports, read the information in [“Legal notices” on page 151](#).

This edition applies to version 5, release 3, modification 5 of IBM Spectrum Control (product numbers 5725-F93, 5725-G33, 5725-Y23, and 5725-Y24) and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces SC27-8768-04.

© **Copyright International Business Machines Corporation 2014, 2019.**

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

Contents

About this guide.....	vii
Who should read this guide.....	vii
Publications.....	vii
Accessing publications online.....	vii
IBM Redbooks.....	vii
Translation.....	viii
Providing feedback about publications.....	viii
IBM Spectrum Control technical community.....	viii
Contacting IBM Software Support	viii
Reporting a problem.....	ix
Conventions used in this guide.....	ix
 Chapter 1. Configuring	1
Starting IBM Spectrum Control.....	1
Overview of required user names for initial logon.....	1
Configuring history and data retention.....	2
Configuring user authentication.....	3
Authorizing users.....	5
Managing authentication	11
Adding customized text to the logon page.....	21
Configuring switches.....	21
Managing a SAN without agents.....	22
Setting timeout values for the Device server.....	23
Configuring Service Location Protocol.....	24
Router configuration.....	24
SLP directory agent configuration.....	25
Environment configuration.....	25
SLP registration and slptool	25
SLP discovery.....	26
Configuring IP addressing.....	26
Configuring IBM Spectrum Control with multiple IP addresses.....	26
Changing the HOSTS file.....	27
Deploying Storage Resource agents.....	28
Deployment guidelines and limitations for Storage Resource agents.....	28
Creating a certificate for SSH protocol	33
Replacing default SSL certificates with custom certificates.....	38
Configuration guidelines for 500 or more agents.....	42
Including a Storage Resource agent with a server master image.....	43
Configuring LUN provisioning for Oracle Solaris.....	43
Assigning TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUNs to Oracle Solaris HBAs.....	44
Modifying the HBA configuration file.....	44
Setting Persistent Name Binding for QLogic HBAs by using the appropriate software.....	44
Modifying the SCSI disk configuration file.....	45
Checking for TotalStorage Enterprise Storage Server, DS6000, or DS8000 multipaths in VxDMP...46	
Checking for a fully qualified host name	47
Checking for a fully qualified host name for AIX systems.....	47
Checking for a fully qualified host name for Linux systems.....	47
Checking for a fully qualified host name for Oracle Solaris.....	48
Checking for a fully qualified host name for Windows systems.....	48

Importing authentication information for a Storage Resource agent.....	49
Installing and configuring the IBM Spectrum Control server with multiple NIC cards.....	50
Creating an SSH certificate for the root user ID.....	51
Replacing the default SSL certificate for the Device, Alert, or Web server.....	52
Updating IBM Spectrum Control data collector trusted certificates after replacing default SSL certificate for the Device server.....	54
Replacing the default SSL certificate for the Export server.....	55
Generating a new default self-signed SSL certificate for the Export server.....	56
Enabling TLS 1.0 and 1.1 for ports.....	57
Enabling TLS 1.1 and 1.0 for IBM Spectrum Control ports.....	57
Configuring Db2, AIX, and Linux for IPv6-only environment.....	58
Chapter 2. Administering.....	61
Administering resources and data sources.....	61
Storage systems.....	61
Hypervisors and VMware data sources.....	67
Switches and fabrics.....	69
Servers and Storage Resource agents.....	71
SMI-S providers.....	85
SNMP agents.....	87
Starting and stopping the IBM Spectrum Control servers.....	88
Starting the servers by using the GUI.....	89
Starting the servers by using scripts.....	89
Stopping the servers by using the GUI.....	90
Stopping the servers by using scripts.....	90
Checking the version and license of IBM Spectrum Control.....	91
Checking IBM Spectrum Control status.....	91
Troubleshooting problems with the IBM Spectrum Control component and servers.....	92
Opening PMRs and packaging IBM Spectrum Control system log files for IBM Software Support...	93
Increasing the memory allocation for the Data server.....	96
Increasing the memory allocation for the Data server that is running on AIX.....	96
Increasing the memory allocation for the Data server that is running on Linux.....	97
Increasing memory allocation for Data server that is running on Windows.....	97
Changing passwords.....	98
Changing passwords by using the password tool.....	98
Changing passwords on AIX and Linux systems using the Command Line Interface (CLI).....	104
Changing passwords on Windows systems from the Command Line Interface (CLI)	104
Granting local administrative privileges to a domain account.....	105
Collecting diagnostic information about IBM Spectrum Control.....	106
Service tool overview.....	106
Collecting service logs for IBM Software Support troubleshooting.....	108
Creating a compressed file for a Storage Resource agent	109
How to customize the service tool.....	110
Administering the IBM Spectrum Control database.....	112
Backing up the database.....	112
Restoring the database.....	116
Disaster recovery.....	117
Maintaining and improving the performance of the database.....	117
Repository copy tool.....	120
Administering Db2.....	121
Using the command line on UNIX and Linux.....	121
Manually starting Db2 on Windows.....	122
Manually stopping Db2 on Windows.....	122
Starting the IBM Data Studio full client	123
Monitoring Db2	123
Appendix A. Reference.....	125

Return codes used by Storage Resource agent.....	125
Agent types for monitoring fabrics and switches.....	128
Supported storage systems providing full disk encryption and solid-state drives.....	129
agent.sh command.....	129
dataCollector command.....	130
Configuration files.....	130
server.config file.....	131
scheduler.config file.....	132
TPCD.config file.....	133
Specifying the tablespace size for IBM Spectrum Control.....	134
agent.config file.....	134
Log files.....	135
Default locations of log files.....	135
Script parameters.....	136
Opening IBM Spectrum Control on Windows operating systems	139
Opening IBM Spectrum Control GUIs and CLIs.....	139
Accessing administration tools.....	140
Windows services used by IBM Spectrum Control.....	142
Frequently Asked Questions.....	143
Protocols and standards.....	143
Web Based Enterprise Management.....	143
Storage Management Initiative Specification.....	144
Service Location Protocol.....	145
Simple Network Management Protocol.....	145
Fibre Channel Methodologies of Interconnects.....	146
Appendix B. Accessibility features for IBM Spectrum Control.....	149
Legal notices.....	151
Privacy policy considerations	152
Trademarks.....	153
Glossary.....	155
Index.....	157

About this guide

IBM Spectrum Control manages storage infrastructure by centralizing, automating, and simplifying the management of complex and heterogeneous storage environments. This guide provides task-oriented administration information that helps you to obtain optimal product performance.

Who should read this guide

This guide is intended for administrators who are configuring and maintaining IBM Spectrum Control. A single administrator can manage IBM Spectrum Control, or several people can share administrative responsibilities.

Administrators should be familiar with the following topics:

- General procedures for managing software and services on Microsoft Windows, IBM® AIX®, and Linux.
- Storage area network (SAN) concepts
- IBM Spectrum Control concepts
- IBM DB2® and database concepts
- Simple Network Management Protocol (SNMP) concepts

Publications

A number of publications are provided with IBM Spectrum Control.

The following section describes how to access these publications online.

Accessing publications online

Use the following table to view and download publications for IBM Spectrum Control. Translated documents are available for some products.

<i>Table 1. Locations of publications for IBM Spectrum Control and related products</i>	
Product	Online location
IBM Spectrum Control	To search across all publications or to download PDF versions of individual publications, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/ .
IBM DB2 Database for Linux, UNIX, and Windows	https://www.ibm.com/support/knowledgecenter/SSEPGG/welcome
Jazz® for Service Management	http://www.ibm.com/support/knowledgecenter/SSEKCU/welcome
Tivoli® Netcool/Impact	https://www.ibm.com/support/knowledgecenter/SSSHYH/welcome

IBM Redbooks

The IBM Redbooks® are publications about specialized topics.

You can order publications through your IBM representative or the IBM branch office serving your locality. You can also search for and order books of interest to you by visiting the IBM Redbooks home page at <http://www.redbooks.ibm.com>.

Languages

Non-English publications are available from IBM Knowledge Center, which is available in certain non-English languages. It is displayed in the language that is appropriate for the browser locale setting.

When a locale does not have a non-English version, the information is displayed in English, which is the default language. Non-English PDFs are available when the information is translated.

Providing feedback about publications

Your feedback is important to help IBM provide the highest quality information.

To provide comments or suggestions about the product documentation, go to the IBM Knowledge Center for IBM Spectrum Control: <http://www.ibm.com/support/knowledgecenter/SS5R93>. Click **Feedback** at the bottom of any page and complete the form.

IBM Spectrum Control technical community

Connect, learn, and share with storage professionals: product support technical experts who provide their perspectives and expertise.

Access the IBM Spectrum Control technical community at <https://www.ibm.com/developerworks/servicemanagement/>.

Use IBM Spectrum Control technical community in the following ways:

- Become involved with transparent development, an ongoing, open engagement between other users and developers of IBM products.
- Connect one-on-one with the experts to collaborate and network about IBM and the Storage Management community.
- Read blogs to benefit from the expertise and experience of others.
- Use forums to collaborate with the broader user community.

Contacting IBM Software Support

You can contact IBM Software Support by phone, and you can register for support notifications at the technical support website.

- Go to the IBM Spectrum Control technical support website at http://www.ibm.com/support/entry/portal/product/tivoli/ibm_spectrum_control/ibm_spectrum_control_standard_edition.

To receive future support notifications, sign in under **Subscribe to support notifications**. You are required to enter your IBM ID and password. After you are authenticated, you can configure your subscription for IBM Spectrum Control technical support website updates.

- Customers in the United States can call 1-800-IBM-SERV (1-800-426-7378).
- For international customers, go to <https://www.ibm.com/planetwide/>.

You can also review the *IBM Software Support Handbook*, which is available at <http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html>.

The support website offers extensive information, including a guide to support services; frequently asked questions (FAQs); and documentation for all IBM Software products, including Redbooks and white papers. Translated documents are also available for some products.

When you contact IBM Software Support, be prepared to provide identification information for your company so that support personnel can readily assist you. Company identification information might also be needed to access various online services available on the website. See [“Reporting a problem” on page ix](#).

Reporting a problem

Provide IBM Software Support with information about the problems that you report.

Have the following information ready when you report a problem:

- The IBM Spectrum Control version, release, modification, and service level number.
- The communication protocol (for example, TCP/IP), version, and release number that you are using.
- The activity that you were doing when the problem occurred, listing the steps that you followed before the problem occurred.
- The exact text of any error messages.

Conventions used in this guide

Information is given about the conventions that are used in this publication.

This publication uses several conventions for special terms and actions, and for operating system-dependent commands and paths.

The following typeface conventions are used in this publication:

Bold

- Flags that display with text
- Graphical user interface (GUI) elements (except for titles of windows and dialogs)
- Names of keys

Italic

- Variables
- Values that you must provide
- New terms
- Words and phrases that are emphasized
- Titles of documents

monospace

- Commands and command options
- Flags that display on a separate line
- Code examples and output
- Message text
- Names of files and directories
- Text strings that you must type, when they display within text
- Names of Oracle Java™ methods and classes
- HTML and XML tags that display like `this`, in monospace type

For syntax notations, remember the following details.

- In AIX, the prompt for the root user is `#`.
- In AIX and Linux, the commands are case-sensitive, so you must type commands exactly as they are shown.

Chapter 1. Configuring

After IBM Spectrum Control is installed, you can configure it according to the standards and requirements of your storage environment.

Starting IBM Spectrum Control

You can start IBM Spectrum Control by opening a web browser and entering a web address for the IBM Spectrum Control logon page. For example, you might enter `https://storage.example.com:9569/sim`.

Before you start IBM Spectrum Control, ensure that you are using a supported web browser. For a list of web browsers that you can use with IBM Spectrum Control, see [IBM Spectrum Control 5.3.x - Platform Support: Servers, Agents, and Browsers - Web Browsers](#).

Start the IBM Spectrum Control GUI to administer and monitor the condition, capacity, and relationships of the resources within your storage environment.

1. On a server running the Windows operating system, start **IBM Spectrum Control GUI**. If you are not on a server running the Windows operating system, start a web browser and enter the following address in the address field:

```
https://host_name:port/sim
```

In the preceding address, specify the following values:

host_name

The IBM Spectrum Control server. You can specify the host name as an IP address or a Domain Name System (DNS) name.

port

The port number for IBM Spectrum Control. The default port number for connecting to IBM Spectrum Control by using the HTTPS protocol is 9569. However, this port number might be different for your site. For example, the port number might be different if the default port range was not accepted during installation. If the default port number does not work, ask your IBM Spectrum Control administrator for the correct port number.

Tip: If you have a non-default port, check the value of the `WC_defaulthost_secure` property in `installation_dir/web/conf/portdef.props` file.

2. From the IBM Spectrum Control logon page, type your user name and password and click **Log in**. The GUI opens in the browser.

Tip: If you want to log on to the GUI with Windows Domain credentials, use this form: `domain_name\user`.

Overview of required user names for initial logon

The IBM Spectrum Control GUI requires a user ID and password. If you are logging in immediately after you installed the software, the user ID that you must use differs depending on the type of installation.

Immediately after you install IBM Spectrum Control, you must use the user name as described in the following information. After you log on, you can assign roles for users. When users log on, their roles determine their authorization level and the components that they can view and use.

Required user name for initial logon after installation on a single server when only the common user is defined

After you install IBM Spectrum Control in a single-server environment, the required user name for the initial logon is the common user name that was defined for the IBM Spectrum Control installation.

Required user name for initial logon after installation on multiple servers with a remote database schema

After you install the software on multiple servers with a remote database schema, you must use the user name that was defined for the installation of the IBM Spectrum Control server.

Required user name for initial logon after installation on multiple servers and IBM Spectrum Control reports are remote

After you install the software on multiple servers, and IBM Spectrum Control reports are remote, you must use the user name that was defined for the installation of the IBM Spectrum Control server.

Configuring history and data retention

Specify how long to retain the data that is collected about resources and the log files that are generated by IBM Spectrum Control. By specifying the number of weeks for history retention, you can control the amount of data that is retained and available for historical analysis and charting. The longer that you retain data, the more informative your analysis, but the more storage space that is required to store that data.

Data that IBM Spectrum Control collects about a storage environment is stored in a DB2 database repository. The amount of data that is retained about resources can grow over time, and thus require more storage space for the repository. You can use the **History Retention** page to modify the data retention settings according to the monitoring and storage requirements of your environment. You must be assigned the Administrator role to modify data retention settings.

1. In the menu bar, go to **Settings > History Retention**.
2. Click **Edit** to modify the following data retention settings:

Capacity history

Specify how long to retain a history of the capacity data that is collected about monitored resources. This value determines the amount of capacity data that is retained and available for historical analysis and charting. The longer that you retain data, the more informative your analysis, but the more storage space that is required.

Daily

Specify how long to retain capacity data that is collected daily about resources. You can retain daily data for up to 72 weeks and a minimum of 2 weeks.

Weekly

Specify how long to retain capacity data that is aggregated weekly for monitored resources. You can retain weekly aggregates for up to 96 weeks and a minimum of 4 weeks.

Monthly

Specify how long to retain capacity data that is aggregated monthly for monitored resources. You can retain monthly aggregates for up to 48 months and a minimum of 2 months.

Retention values from the stand-alone GUI: When you upgrade from Tivoli Storage Productivity Center V5.2 or earlier, the retention values that were defined in the stand-alone GUI are automatically consolidated and migrated. During the migration, IBM Spectrum Control ensures that the consolidated values are within acceptable boundaries. For example, if the monthly value for storage systems was set to 56 months in the stand-alone GUI, that value is changed to 48 months in the web-based GUI.

Performance data

Specify how long to retain data that is collected by performance monitors.

Sample

Specify how long to retain sample data that is collected by performance monitors. Sample data represents the data that is collected each time a performance monitor is run. Because sample data is collected frequently, retaining that data can require significant disk space in the database repository. The required disk space is determined by the types of switches, storage systems, and number of volumes that are being monitored. You can retain sample data for up to 12 weeks.

Hourly

Specify how long to retain hourly data that is collected by performance monitors. You can retain hourly data for up to 24 weeks.

Daily

Specify how long to retain daily data that is collected by performance monitors. You can retain daily data for up to 156 weeks.

Consolidating performance data: Performance data is collected at intervals. An interval represents the number of minutes over which samples of performance data are averaged. When performance history is retained, data that is collected at certain intervals is automatically consolidated, or rolled up, to higher intervals. For example, data collected at 1-minute intervals is consolidated into 5-minute data; data collected at 5-minute intervals is consolidated into 1-hour data; and so on.

Tip: If performance data is collected at 1-minute intervals, the amount of data that is stored in the database repository increases significantly. The product stores only 7 days of sample data that is collected at 1-minute intervals.

Data for missing resources

Specify how long to retain data about internal resources that are no longer detected by IBM Spectrum Control. You can retain the data of removed resources for up to 52 weeks.

If the internal resource of a top-level resource is not detected when that top-level resource is probed, data about the resource is removed when the time limit is reached. The internal resource is removed only from the top-level resource that is probed. For example, if two weeks are specified, the data for a pool that is missing from a storage system for more than two weeks will be removed.

Only internal resources are automatically removed according to this setting. Storage systems, servers, hypervisors, switches, and fabrics must be removed manually.

Alert logs

Specify how long to retain alerts. An entry is generated each time that an alert condition is detected on a resource. Any alert that is older than this value is deleted. You can retain alerts for up to 12 weeks.

Job logs

Specify the maximum number of logs that are retained for data collection jobs. A log file is created each time that a job is run. When this number is reached, the entry for the oldest log is deleted. For example, if you accept the default value 5, and then run a probe 6 times, the log file for the first run is deleted. You can retain up to 20 logs for a job.

3. Click **Save** to apply the retention settings.
4. Click **Restore Defaults** to restore the retention settings to their default values.

Configuring user authentication

When IBM Spectrum Control is installed, default repositories are created, which allow you to control user access to the product.

In the federated repositories framework, the following repositories are created:

File-based user repository

This repository contains the `tpcFileRegistryUser` user ID. This user password is the same as the Common User password that was entered during the IBM Spectrum Control installation.

When you use the password tools to change the IBM Spectrum Control passwords, the tpcFileRegistryUser user password gets changed so that it continues matching the Common User password.

If you encounter problems accessing IBM Spectrum Control using local operating system or LDAP credentials, you can log on to IBM Spectrum Control using the tpcFileRegistryUser user ID which is not affected by authentication configuration changes.

Operating system repository

In the federated repositories framework, the IBM Spectrum Control installation program creates two repositories on the IBM Spectrum Control web server. This server, which is in the `installation_dir/wlp/usr/servers/webServer` directory, is used as the primary WebSphere® Application Server Liberty server for user authentication in IBM Spectrum Control.

The Device server also runs on WebSphere Application Server Liberty, and it is only configured with the File-based user repository. If the web server is down, the Device server is used as the backup server to perform the user authentication and allows the common user name that was provided during IBM Spectrum Control installation and the tpcFileRegistryUser user ID to log on to IBM Spectrum Control.

You can add an LDAP repository and disable the operating system repository after you install IBM Spectrum Control; this configuration is completed in IBM Spectrum Control. The LDAP repository configuration settings are not propagated to the Device server. Therefore, if the web server is not running, the authorized LDAP users cannot log in to IBM Spectrum Control. The backup user authentication mechanism that is based on Device server allows the common user name that was entered during the IBM Spectrum Control installation, and the tpcFileRegistryUser user ID to be used to log on to IBM Spectrum Control.

If the computer is correctly configured with the Windows domain, the operating system repository also contains the domain users and groups that are managed by the Windows domain.

IBM Spectrum Control integrates with third party modules on the Linux and AIX operating systems for local user authentication. IBM Spectrum Control only supports the default module configuration settings with the AIX or Linux operating systems. The customization of configuration settings or using additional modules is not supported by IBM Spectrum Control.

The LDAP repositories that are supported by IBM Spectrum Control depend on WebSphere Application Server Liberty support. For more information, about the LDAP repositories that are supported, see <http://www.ibm.com/support/docview.wss?uid=swg27036471>.

WebSphere Application Server Liberty cannot resolve users or groups that are present in more than one repository in the federated repositories framework. Because of this limitation, you must select either the operating system repository or the LDAP repository for user authentication and authorization in IBM Spectrum Control. If you upgraded from an earlier version of IBM Spectrum Control with both the operating system repository and an LDAP repository configured, you can keep using both repositories. However, it is recommended that you select either the operating system repository or the LDAP repository.

The following table shows which user repositories are checked for IBM Spectrum Control authentication configurations when accessing IBM Spectrum Control using the IBM Spectrum Control GUI, the CLI, or the REST API:

Table 2. Authentication configurations and associated user repositories	
Authentication configuration	User repositories checked
Local OS (default configuration)	Local operating system repository and file-based user repository
LDAP	LDAP repository and file-based user repository
LDAP and Local OS	Local operating system repository, LDAP repository, and file-based user repository

Authorizing users

After IBM Spectrum Control is installed, you can assign roles to the user groups that are contained in the authentication repository. Roles determine the functions that are available to the users that are in a group.

The authentication repository can be an operating system repository or a Lightweight Directory Access Protocol (LDAP) repository. When IBM Spectrum Control is installed, the following user and groups are automatically configured for authentication to the product:

- User: tpcFileRegistryUser
- Windows group: Administrators group
- UNIX and Linux group: root
- AIX group: system

There are three IBM Spectrum Control roles that you can assign to user groups:

- Administrator (the Administrator, root, and system groups are automatically assigned to this role)
- Monitor
- External Application

Each role provides access to a specific set of functions. For more information about the functions that are available in each role, see [“Role-based authorization” on page 5](#).

Role-based authorization

Roles determine the functions that are available to users of IBM Spectrum Control. When a user ID is authenticated to IBM Spectrum Control through the GUI, CLI, or APIs, membership in an operating system or LDAP group determines the authorization level of the user.


In Version 5.2, the roles that were previously defined in IBM Spectrum Control were consolidated into a smaller set of roles. The following table shows how the roles in versions earlier than 5.2 are mapped to the current set of roles:

Table 3. How roles in previous versions of IBM Spectrum Control are mapped to the roles in version 5.2 and later		
Roles in previous versions	Roles in version 5.2 and later	Authorization level
Superuser Productivity Center administrator Disk administrator Fabric administrator Data administrator Tape administrator	Administrator	This role has full access to all monitoring and administrative functions. At least one group must have the Administrator role. Note: When IBM Spectrum Control is first installed, the following operating system groups are assigned the Administrator role: <ul style="list-style-type: none">• Windows: Administrators• UNIX and Linux: root• AIX: system

Table 3. How roles in previous versions of IBM Spectrum Control are mapped to the roles in version 5.2 and later (continued)

Roles in previous versions	Roles in version 5.2 and later	Authorization level
Disk operator Fabric operator Data operator Tape operator	Monitor	<p>This role has access to the following read-only functions:</p> <ul style="list-style-type: none"> • Viewing and exporting information about monitored resources • Viewing, acknowledging, and removing alerts • Viewing tasks and data collection jobs • Opening management GUIs • Opening logs • Viewing chargeback, consumer, predefined capacity and inventory, and custom reports <p>Exception: Users with the Monitor role can provision storage if they are granted permission in a service class. A service class is a logical entity that describes storage capabilities and characteristics and can be used to specify requirements for storage provisioning. For more information about service classes, see .</p>
This role did not exist in versions 5.1 or earlier.	External Application	<p>If you assign the External Application role to the user, you must also assign one or more service classes to the user.</p> <p>This role does not enable users to log in to the IBM Spectrum Control GUI.</p>

Tips:

- To determine the role of the user who is logged in, click the user icon  In the upper-right corner of any page in the GUI.
- If a user belongs to multiple groups and the groups have different roles, the role with the highest level of authorization is granted to the user. For example, if a user belongs to a group that is assigned the Administrator role and also belongs to a group that is assigned a Monitor role, the user is granted the authorization of the Administrator role.
- If a user is not a member of a group that is assigned a IBM Spectrum Control role, no access is granted to that user.
- If assigned the Monitor role, a user can only open and view logs from the **Data Collection** page for the selected resource.

Nested groups are not supported: Adding active directory or any other type of domain user group to a local operating system group is not supported in IBM Spectrum Control. You can configure IBM Spectrum Control to authenticate domain IDs that rely on the operating system to perform the authentication operation against the active directory, but it cannot resolve nested groups.

Alternatively, you can configure LDAP authentication to perform queries against active directory user repositories and assign domain groups directly to roles within IBM Spectrum Control.

Assigning a role to a group

Assign an IBM Spectrum Control role to one or more user groups. The role that is assigned to a group determines the product functions that are available to the users in that group.

If you are using LDAP authentication and you are using Microsoft Active Directory as your LDAP repository, do not assign the Active Directory Primary group for a user to an IBM Spectrum Control role. IBM Spectrum Control cannot identify user membership in a Primary group. Assign an IBM Spectrum Control role to a group that is not the Primary group for the user.

To assign a role to a group, complete the following steps:

1. In the menu bar in the web-based GUI, go to **Settings > User Management**.
2. Click **Add Group** to search for groups that are defined in the authentication repository.
You can type the name of a group if you know its name, or specify a filter to search for existing groups in the authentication repository. For filters, use an asterisk (*) to represent unknown characters. You must enter at least one character in addition to an *.
For example, type `tpc*` to search for groups that begin with the letters "tpc" or "TPC". Type `*t` to search for groups that begin with or contain the letter "t" or "T".
3. In the list of groups, select one or more groups to which you want to assign a role.
4. In the **Role** field, select the role to assign to the group.
5. Click **OK** to assign the role.
The role that you select is applied to all the groups that you are adding. You can change the role assignments at any time after the group is added.

Related tasks

[“Determining the groups to which a user belongs” on page 7](#)

You can determine the groups to which a user belongs to and ensure that the user is in a group or groups that are assigned the correct IBM Spectrum Control role.

Related reference

[“Role-based authorization” on page 5](#)

Roles determine the functions that are available to users of IBM Spectrum Control. When a user ID is authenticated to IBM Spectrum Control through the GUI, CLI, or APIs, membership in an operating system or LDAP group determines the authorization level of the user.

Determining the groups to which a user belongs

You can determine the groups to which a user belongs to and ensure that the user is in a group or groups that are assigned the correct IBM Spectrum Control role.

Use a command prompt to find the groups to which a user belongs.

To determine the groups to which a user belongs, complete the following steps depending on your operating system:

1. Log on to the computer where the IBM Spectrum Control servers are installed, open a command prompt, and enter:

Option	Description
Windows standalone operating system	<code>net user <username></code>
Windows Domain	<code>net user <username> /DOMAIN</code>
Linux and AIX operating system	<code>groups <username></code>
LDAP	See your LDAP administrator for more information.

2. Verify that the user is in a group or groups that are assigned the correct IBM Spectrum Control role.

Modifying the authentication mechanism

To modify how IBM Spectrum Control authenticates users and user groups, configure the authentication repository.

You must be assigned the Administrator role to modify the authentication repository and manage role and group assignments.

The authentication mechanism determines how IBM Spectrum Control authenticates users and the user groups that are available for assigned roles. During the installation process, the WebSphere Application Server Liberty is configured with federated repositories. By default, authentication is configured to use the federated repositories, which contain a file repository and an operating system repository. The operating system repository includes the operating system users and groups that are defined on the server where IBM Spectrum Control is installed. For a server that is a member of a Windows domain, the operating system repository also includes the users and groups that are defined in that domain.

Important: WebSphere Application Server Liberty cannot resolve users or groups that are present in more than one repository in the federated repositories framework. Because of this limitation, you must select either the operating system repository or the LDAP repository for user authentication and authorization in IBM Spectrum Control. If you upgraded from an earlier version of IBM Spectrum Control with both the operating system repository and an LDAP repository configured, you can keep using both repositories. However, it is recommended that you select either the operating system repository or the LDAP repository.

To modify your authentication, complete the following steps:

1. In the menu bar, go to **Settings > User Management**.
2. On the **User Management page**, click **Edit Authentication**.
The **Authentication Configuration** page is displayed.
3. Make your modifications.

Related concepts

[“Configuring user authentication” on page 3](#)

When IBM Spectrum Control is installed, default repositories are created, which allow you to control user access to the product.

Related tasks

[“Changing from operating system to LDAP authentication” on page 12](#)

You can configure IBM Spectrum Control to communicate with an external LDAP repository, for example, IBM Tivoli Directory Server or Microsoft Active Directory. This enables you to make IBM Spectrum Control available to a larger set of users and groups and you are able to log in to IBM Spectrum Control with one set of credentials.

Actions that are available based on role

Your IBM Spectrum Control role and product license determine the actions that are available in the product.

Users who are assigned the Administrator role or the Monitor role can use product functions. The actions that are available for each function depend on the role that is assigned to the user:

Administrator role

Users who are assigned the Administrator role have access to all monitoring and administrative actions and are limited only by license restrictions.

Monitor role

Users who are assigned the Monitor role can view information about monitored resources and other objects such as tasks, alerts, and service classes. They can acknowledge alerts and resource statuses, open logs, and open management GUIs.

Users who are assigned the Monitor role do not have access to administrative functions, but they can be granted permission in a service class to provision storage by using the service class. If so, they can provision storage and create a provisioning task. Users can delete provisioning tasks that they create. If the service class specifies that administrator approval is not required, the users can run or schedule the provisioning tasks that they create.

To use some functions, you must have the IBM Spectrum Control Advanced Edition license. If you have the IBM Spectrum Control Standard Edition license or the IBM Spectrum Control Standard Select Edition license, the following functions are not available:

- Storage tier optimization.
- Pool balancing.
- Block storage provisioning. You are not able to provision volumes by provisioning storage. However, there are no license restrictions for file storage provisioning, therefore, Network Attached Storage (NAS) file shares can be provisioned.
- Chargeback and consumer reporting.
- Exporting of chargeback and consumer information using the REST APIs.

The following table outlines the actions that are available only for the Administrators role. All other actions are available to the Monitor and Administrator roles. In addition to the restrictions listed in this table, users who are assigned the Monitor role do not have access to user management functions.

<i>Table 4. Product actions that are available only to users with the Administrator role</i>	
Function	Actions that require the Administrator role
Single dashboard view of the storage environment that you can use to manage storage systems, hypervisors, servers, and Fibre Channel fabrics.	<ul style="list-style-type: none"> • Adding and removing resources • Administering connections • Scheduling data collection • Changing and viewing the automated probe schedule • Viewing and editing history retention settings • Modifying license compliance settings
Performance monitoring for storage systems and Fibre Channel networks.	<ul style="list-style-type: none"> • Scheduling performance monitors • Starting or stopping performance monitors
Capacity and usage monitoring of resources.	<ul style="list-style-type: none"> • Scheduling probes • Starting or stopping probes • Provisioning storage to servers and hypervisors • Modifying Storage Resource agents • Enabling automatic zoning
Health and alerting for hypervisors, networks, servers, and storage systems.	<ul style="list-style-type: none"> • Creating, modifying, and deleting alert policies • Setting which alert policy manages a resource • Adding and modifying resources for management by an alert policy • Defining and modifying alert definitions • Editing alert notification settings
Capacity and performance of the storage that applications, departments, and general groups use.	<ul style="list-style-type: none"> • Creating applications, departments, and general groups • Creating, modifying, and removing filters to add resources to applications • Adding and removing resources in applications and general groups, directly • Adding applications as members of other applications • Adding departments to other departments • Adding applications to departments

Table 4. Product actions that are available only to users with the Administrator role (continued)

Function	Actions that require the Administrator role
Storage pool balancing, block storage provisioning, file provisioning, and storage reclamation.	<ul style="list-style-type: none"> • Balancing pools • Provisioning block storage • Viewing volumes that can be reclaimed • Creating, modifying, deleting service classes • Creating, modifying, and deleting capacity pools • Scheduling, running, and deleting tasks
Analytics-driven tiering that automatically moves volumes to the most cost-effective tier.	<ul style="list-style-type: none"> • Optimizing storage tiering • Transforming storage volumes • Creating, modifying, and deleting capacity pools
Roll-up reporting, in which capacity data is combined from multiple instances of IBM Spectrum Control for reporting purposes.	<ul style="list-style-type: none"> • Adding and removing subordinate servers • Starting a probe for a subordinate server • Modifying the connection information for a subordinate server
<p>Predefined Reports</p> <ul style="list-style-type: none"> • Predefined capacity reports allow users to quickly create reports about capacity anomalies and shortfalls, which can be scheduled and sent by email or saved to the user's file system, or both. • Predefined inventory reports allow users to quickly create reports about their storage resources, which can be scheduled and sent by email or saved to the user's file system, or both. 	<ul style="list-style-type: none"> • Creating, deleting, and editing reports • Configuring the email server • Emailing reports • Saving reports to the file system

Table 4. Product actions that are available only to users with the Administrator role (continued)

Function	Actions that require the Administrator role
<p>Custom reports</p> <p>From any table view in the GUI, custom reports can be created, which can be scheduled and sent by email or saved to the user's file system, or both, about capacity of storage resources, the configuration and attributes of storage resources, and the performance of storage resources.</p>	<ul style="list-style-type: none"> • Creating, deleting, and editing reports • Configuring the email server • Emailing reports • Saving reports to the file system
<p>Chargeback and consumer reports</p> <ul style="list-style-type: none"> • Chargeback reports show the capacity and the cost of the storage that is used by applications, departments, hypervisors, and physical servers. • Consumer reports show the capacity and the cost of the block storage that is used by an application, department, hypervisor, and physical server. 	<ul style="list-style-type: none"> • Creating, deleting, and editing reports • Configuring the email server • Emailing reports

Managing authentication

The IBM Spectrum Control installation program establishes a default authentication configuration using the federated repositories feature of the WebSphere Application Server Liberty. You can configure and manage IBM Spectrum Control for LDAP authentication as a post-installation activity.

Important: WebSphere Application Server Liberty cannot resolve users or groups that are present in more than one repository in the federated repositories framework. Because of this limitation, you must select either the operating system repository or the LDAP repository for user authentication and authorization in IBM Spectrum Control. If you upgraded from an earlier version of IBM Spectrum Control with both the operating system repository and an LDAP repository configured, you can keep using both

repositories. However, it is recommended that you select either the operating system repository or the LDAP repository.

Changing from operating system to LDAP authentication

You can configure IBM Spectrum Control to communicate with an external LDAP repository, for example, IBM Tivoli Directory Server or Microsoft Active Directory. This enables you to make IBM Spectrum Control available to a larger set of users and groups and you are able to log in to IBM Spectrum Control with one set of credentials.

When you change the authentication configuration, IBM Spectrum Control is available to users and groups in other repositories.

Important: WebSphere Application Server Liberty cannot resolve users or groups that are present in more than one repository in the federated repositories framework. Because of this limitation, you must select either the operating system repository or the LDAP repository for user authentication and authorization in IBM Spectrum Control. If you upgraded from an earlier version of IBM Spectrum Control with both the operating system repository and an LDAP repository configured, you can keep using both repositories. However, it is recommended that you select either the operating system repository or the LDAP repository.

1. Back up the `ldapregistry.xml` file in the `installation_dir/wlp/usr/servers/webServer/registry/` directory.
2. Log on as an administrator to the IBM Spectrum Control GUI.
3. Click **Settings > User Management**.
4. Click **Edit Authentication**.
5. On the **Authentication Configuration** page, select **LDAP**.
6. Click **Download Files**.
7. Save and extract the `ldapExamples.zip` file to the computer where you run your browser.
8. Use the information to edit the XML template file for your vendor.
For example, if your LDAP server is IBM Tivoli Directory Server, edit the `IBMDirectoryServer.xml` file and if your LDAP server is Microsoft Active Directory, edit the `ActiveDirectoryServerDefault.xml` file.

Edit the following parameters:

id

The unique identifier for the LDAP repository, which identifies the repository in the realm, for example, `LDAP1`.

host

The host name of the primary LDAP server. The host name is either the IP address or the computer name in a domain name system (DNS).

sslEnabled

Indicates whether SSL is used to connect to the LDAP server.

Important: If you set this parameter to `true`, and set the **port** parameter to the LDAP server secure communications port, when you upload the edited XML template file, IBM Spectrum Control downloads the SSL certificate from the LDAP server. Then, it is added to the Web server keystore. You must restart the Web server.

port

The port number for the LDAP server. By default, the port number for secure communication is 636, and for non-secure communication is 389.

Tip: Depending on the configuration of your LDAP server, you can specify a different port number.

baseDN

The baseDN (Distinguished Name) is the starting point for searches for users in the LDAP directory server. For example, if you have a DN value of `cn=John Doe, ou=rochester, o=ibm, c=us`, you can specify the LDAP base entry as any of the following options:

- ou=rochester, o=ibm, c=us
- o=ibm, c=us
- c=us

Important: The DN value that you enter in this field must be extensive enough to include all of the groups to which the users belong. For example, if a user in ou=rochester, o=ibm, c=us is also a member of groups that are in ou=stategroups, o=ibm, c=us, enter o=ibm, c=us.

If you want to set multiple **baseDN** parameters for your LDAP authentication configuration, then you must create a separate <ldapRegistry> entry in the XML template file for each unique **baseDN** parameter. For example:

```
<server description="IBM Web Server">
  <ldapRegistry activeFilters="active_dir_server1"
    baseDN="ou=Marketing,dc=storage,dc=ibm,dc=com"
    bindDN="cn=Administrator,cn=users,dc=storage,dc=ibm,dc=com" bindPassword="password"
    host="ldap.storage.ibm.com" id="LDAP1" ignoreCase="true" ldapType="Microsoft Active
    Directory"
    port="389" realm="TPCRealm" sslEnabled="false"/>
    <activeLdapFilterProperties groupFilter="(&(cn=%v)(objectcategory=group))"
    groupIdMap="*:cn" groupMemberIdMap="memberof:member"
    id="active_dir_server1" userFilter="(&(sAMAccountName=%v)(objectcategory=user))"
    userIdMap="user:sAMAccountName"/>
    <ldapRegistry activeFilters="active_dir_server2"
    baseDN="ou=Sales,dc=storage,dc=ibm,dc=com"
    bindDN="cn=Administrator,cn=users,dc=storage,dc=ibm,dc=com" bindPassword="password"
    host="ldap.storage.ibm.com" id="LDAP2" ignoreCase="true" ldapType="Microsoft Active
    Directory"
    port="389" realm="TPCRealm" sslEnabled="false"/>
    <activeLdapFilterProperties groupFilter="(&(cn=%v)(objectcategory=group))"
    groupIdMap="*:cn" groupMemberIdMap="memberof:member"
    id="active_dir_server2" userFilter="(&(sAMAccountName=%v)(objectcategory=user))"
    userIdMap="user:sAMAccountName"/>
    <ldapRegistry activeFilters="active_dir_server3"
    baseDN="ou=Management,dc=storage,dc=ibm,dc=com"
    bindDN="cn=Administrator,cn=users,dc=storage,dc=ibm,dc=com" bindPassword="password"
    host="ldap.storage.ibm.com" id="LDAP3" ignoreCase="true" ldapType="Microsoft Active
    Directory"
    port="389" realm="TPCRealm" sslEnabled="false"/>
    <activeLdapFilterProperties groupFilter="(&(cn=%v)(objectcategory=group))"
    groupIdMap="*:cn" groupMemberIdMap="memberof:member"
    id="active_dir_server3" userFilter="(&(sAMAccountName=%v)(objectcategory=user))"
    userIdMap="user:sAMAccountName"/>
    <federatedRepository>
      <primaryRealm allowOpIfRepoDown="true" name="TPCRealm">
        <participatingBaseEntry name="ou=Marketing,dc=storage,dc=ibm,dc=com"/>
        <participatingBaseEntry name="ou=Sales,dc=storage,dc=ibm,dc=com"/>
        <participatingBaseEntry name="ou=Management,dc=storage,dc=ibm,dc=com"/>
        <!-- The next two entries must NOT be changed -->
        <participatingBaseEntry name="o=TPCRealm"/>
        <participatingBaseEntry name="o=OSRealm"/>
      </primaryRealm>
    </federatedRepository>
  </server>
```

The preceding example contains the following information:

- Each <ldapRegistry> entry contains the identical values for the **host**, **port**, **sslEnabled**, **bindDN**, and **bindPassword** parameters.
- Each <ldapRegistry> entry contains a unique value for the **baseDN** and **id** parameters.
- Each <ldapRegistry> entry references its' own unique <activeLdapFilterProperties> entry.
- The <federatedRepository> entry contains multiple <participatingBaseEntry> entries, with each one matching one of the baseDN values in the <ldapRegistry> sections.

bindDN

The distinguished name that WebSphere Application Server Liberty uses when it binds to the LDAP repository. If no name is specified, WebSphere Application Server Liberty binds anonymously to the LDAP repository. In most cases, the **bindDN** and **bindPassword** parameters are required. However, when an anonymous bind satisfies all of the required functions, the

bindDN and **bindPassword** parameters are *not* required. If you are not sure whether an anonymous bind satisfies the required functions, contact your LDAP server administrator.



Attention: No single value for the **bindDN** parameter is correct for every Active Directory Server or for every LDAP server. The correct value for the **bindDN** parameter depends on the configuration of your Active Directory Server or your LDAP server. If you are unsure about the correct value to use for the **bindDN** parameter, contact your LDAP server administrator.

If you are using Active Directory as your LDAP repository and you know the *Active_Directory_user's_samAccountName_value*, but you want the Active Directory user full distinguished name in order to use that value as the **bindDN** parameter, run the following command on the Active Directory machine:

```
dsquery user -samid Active_Directory_user's_samAccountName_value
```

Example:

```
C:\Users\Administrator>dsquery user -samid SCAdministratorMSAD  
"CN=SCAdministratorMSAD,CN=Users,DC=vcloud101dc,DC=local"
```

For more information about the **dsquery** command, see <https://social.technet.microsoft.com/wiki/contents/articles/2195.active-directory-dsquery-commands.aspx?PageIndex=3>

bindPassword

The password that WebSphere Application Server Liberty uses when it binds to the LDAP repository.

If the **bindPassword** parameter is already encrypted in the XML file, enter only an LDAP user name and password to test the pending LDAP authentication configuration. After your LDAP credentials are validated, you must immediately map an LDAP group to an IBM Spectrum Control role in the GUI before you log out with your Local OS credentials.

participatingBaseEntry

You must set this value to the same value as you set for the **baseDN** parameter or the federation for the LDAP repository fails. For example, if you set the **baseDN** parameter to `ou=rochester, o=ibm, c=us`, you must set the **participatingBaseEntry** parameter to:
`<participatingBaseEntry name="ou=rochester, o=ibm, c=us" />`.

Important: Do not change these **participatingBaseEntry** parameters in the XML template file:

```
<participatingBaseEntry name="o=TPCRealm" />  
<participatingBaseEntry name="o=OSRealm" />
```

9. Save the XML template file.
10. On the **Authentication Configuration** page, click **Browse**.
11. On the **File Upload** page, select the XML template file that you previously edited and click **Open**.
The XML template file is then uploaded to the IBM Spectrum Control server.
12. After IBM Spectrum Control downloads the SSL certificate from the LDAP server and adds it to the Web server keystore, click **Restart Web Server**.
Note: While the Web server is restarting, do not refresh your browser or attempt to navigate to another part of the GUI.
13. When the Web server is back online, on the **LDAP Settings** page, enter your LDAP user name, password, group name and click **Save**.

Note: The user name must be a member of the group.

If your change from Local OS authentication to LDAP authentication is successful, you are logged out of the IBM Spectrum Control GUI. You can log into the GUI using your LDAP credentials. You cannot log into the GUI using your operating system credentials.

If your change from Local OS authentication to LDAP authentication is *not* successful, click **Discard**. After the confirmation, your previous Local OS authentication is restored and you are returned to the User Management page.

Tip:

If you encounter any issues with above mentioned procedure, see [“Configuring user authentication alternatives” on page 16](#).

You have changed from local operating system authentication to LDAP authentication in IBM Spectrum Control. You can log on to the IBM Spectrum Control GUI with LDAP credentials.

Related tasks

[“Exporting SSL certificate from the IBM Security Directory Server to a file” on page 17](#)

To secure communications between IBM Spectrum Control and IBM Security Directory Server, you must export the SSL certificate to a file. The file that is created can then be added to the keystore for IBM Spectrum Control.

[“Adding the SSL certificate for the LDAP server to the web server keystore that uses the IKEYCMD command” on page 18](#)

To secure communications between the IBM Spectrum Control server and the LDAP server, you must add the SSL certificate from the LDAP server to the web server keystore for IBM Spectrum Control.

Related reference

[“Role-based authorization” on page 5](#)

Roles determine the functions that are available to users of IBM Spectrum Control. When a user ID is authenticated to IBM Spectrum Control through the GUI, CLI, or APIs, membership in an operating system or LDAP group determines the authorization level of the user.

Changing from LDAP to operating system authentication

To change from LDAP authentication to operating system authentication in IBM Spectrum Control, you can use the IBM Spectrum Control GUI.

WebSphere Application Server Liberty cannot resolve users or groups that are present in more than one repository in the federated repositories framework. Because of this limitation, you must select either the operating system repository or an LDAP repository for user authentication and authorization in IBM Spectrum Control. If you upgraded from an earlier version of IBM Spectrum Control with both the operating system repository and an LDAP repository configured, you can keep using both repositories. However, it is recommended that you select either the operating system repository or the LDAP repository.

The use of the IBM Spectrum Control single sign-on feature is limited when you change from LDAP authentication to operating system authentication in IBM Spectrum Control. Storage system element managers do not support the operating system repository for single sign-on, even if the element manager is installed on the same system as IBM Spectrum Control.

1. Back up the `ldapregistry.xml` file in the `installation_dir/wlp/usr/servers/webServer/registry/` directory.
2. Log on as an administrator to the IBM Spectrum Control GUI.
3. Click **Settings > User Management**.
4. Click **Edit Authentication**.
5. On the **Authentication Configuration** page, select **Local OS** and click **Save**.
6. On the **OS Settings** page, enter your local operating system user name, password, group name and click **Save**.

Note: The user name must be a member of the group.

If your change from LDAP authentication to Local OS authentication is successful, you are logged out of the IBM Spectrum Control GUI. You can log into the GUI using your local operating system credentials. You cannot log into the GUI using your LDAP credentials.

If your change from LDAP authentication to Local OS authentication is *not* successful, click **Discard**. After the confirmation, your previous LDAP authentication is restored and you are returned to the User Management page.

You have changed from LDAP authentication to local operating system in IBM Spectrum Control. You can log on to the IBM Spectrum Control GUI with your local operating system credentials.

Configuring user authentication alternatives

If you encounter any issues with the recommended procedures for configuring user authentication, see the following topics for support.

Enabling secure communication between IBM Spectrum Control and the LDAP repository

You can use the Secure Socket Layer (SSL) protocol to secure the communication between IBM Spectrum Control and the LDAP repository that you are using for user authentication. The SSL protocol provides security and data integrity for communications over Transmission Control Protocol/Internet Protocol (TCP/IP) networks.

You added an LDAP repository to the federated repositories for IBM Spectrum Control and your system is operating properly with non-secure communication between IBM Spectrum Control and the LDAP repository. Before you implement the following procedure, add the SSL certificate from the LDAP server to the IBM Spectrum Control web server keystore or the connectivity between IBM Spectrum Control and the LDAP server fails.

1. Log in to the IBM Spectrum Control GUI as an LDAP user with the Administrator role.
2. In the menu bar, go to **Settings > User Management**.
3. On the **User Management** page, click **Edit Authentication**.
4. On the **Authentication Configuration** page, click **Advanced Configuration Options**.

Depending on the LDAP user account that you used to log into the IBM Spectrum Control GUI, you might have to explicitly log into the Liberty Admin Center as the Common User or the file-based user.

5. On the **Server Config** page, click **LDAP User Registry**.
6. Change the value in the **Ldap ssl enabled** field from **false** to **true**.
7. Change the value of the **Port** field to the LDAP server port that listens for secure communications.
The typical value is 636. Depending on your LDAP server configuration, you can specify a different port. If you do not know which port to use, contact your LDAP server administrator.
8. Click **Save** and log out of the Liberty Admin Center.
9. On the **Authentication Configuration** page, click **Cancel**.

Secure communications are established between IBM Spectrum Control and the LDAP repository with SSL protocol.

Related tasks

[“Exporting SSL certificate from the IBM Security Directory Server to a file” on page 17](#)

To secure communications between IBM Spectrum Control and IBM Security Directory Server, you must export the SSL certificate to a file. The file that is created can then be added to the keystore for IBM Spectrum Control.

[“Exporting SSL certificate from the Microsoft Active Directory to a file” on page 18](#)

To secure communications between IBM Spectrum Control and Microsoft Active Directory, you must export the SSL certificate from the Microsoft Active Directory to a file. The file that is created can then be added to the web server keystore for IBM Spectrum Control.

[“Adding the SSL certificate for the LDAP server to the web server keystore that uses the IKEYCMD command” on page 18](#)

To secure communications between the IBM Spectrum Control server and the LDAP server, you must add the SSL certificate from the LDAP server to the web server keystore for IBM Spectrum Control.

Disabling secure communication between IBM Spectrum Control and the LDAP repository

You can disable the Secure Socket Layer (SSL) protocol between IBM Spectrum Control and the LDAP repository at any time using the IBM Spectrum Control GUI.

1. Log in to the IBM Spectrum Control GUI as an LDAP user with Administrator role.
2. In the menu bar, go to **Settings > User Management**.
3. On the **User Management** page, click **Authentication Configuration**.
4. On the **Authentication Configuration** page, click **Advanced Configuration Options**.
Depending on the LDAP user account that you used to log into the IBM Spectrum Control GUI, you might have to explicitly log into the Liberty Admin Center as the Common User or the file-based user.
5. On the **Server Config** page, click **LDAP User Registry**.
6. Change the value of the **Ldap ssl enabled** field from **true** to **false**.
7. Change the value of the **Port** field to the LDAP server port that listens for non-secure communications.
The typical value is 389. Depending on your LDAP server configuration, you can specify a different port. If you do not know which port to use, contact your LDAP server administrator.
8. Click **Save** and log out of the Liberty Admin Center.
9. On the **Authentication Configuration** page, click **Cancel**.

Exporting SSL certificate from the IBM Security Directory Server to a file

To secure communications between IBM Spectrum Control and IBM Security Directory Server, you must export the SSL certificate to a file. The file that is created can then be added to the keystore for IBM Spectrum Control.

Important: This topic is an example of exporting the SSL certificate from the IBM Security Directory Server to a file.

If your LDAP server is the IBM Security Directory Server verify that the Web Administration tool is installed with your IBM Security Directory Server because it includes the correct IBM Key Management (iKeyman) utility.

For more information about exporting the SSL certificate from the LDAP server, see your LDAP administrator and the documentation for your specific LDAP server product.

1. Open the IBM Key Management utility in your IBM WebSphere Application Server directory structure.
2. Select **Key Database File > Open**.
3. Complete the following steps:
 - a) In **Key database type** field, select **CMS**.
 - b) In the **File Name** field, click **Browse** and go to the location of the key database (.kdb) file that is associated with your IBM Security Directory Server.
 - c) Click **Open**.
 - d) Click **OK**.
4. On the **Password Prompt** page, enter the correct password for the key database file and click **OK**.
5. In the **Personal Certificates** list, select the certificate that is the SSL certificate for the IBM Security Directory Server and click **Extract Certificate**.
6. Select **Base64-encoded ASCII data** as the data type and provide a **Certificate file name, Location**, and click **OK**.

The SSL certificate is exported from IBM Security Directory Server to a file so it can be added to the web server keystore for IBM Spectrum Control.

Exporting SSL certificate from the Microsoft Active Directory to a file

To secure communications between IBM Spectrum Control and Microsoft Active Directory, you must export the SSL certificate from the Microsoft Active Directory to a file. The file that is created can then be added to the web server keystore for IBM Spectrum Control.

Important: This topic is an example of exporting the SSL certificate from the Microsoft Active Directory to a file.

You can use the Certification Authority tool to export the SSL certificate.

For more information about exporting the SSL certificate from the LDAP server, see your LDAP administrator and the documentation for your specific LDAP server product.

1. Open the Certification Authority tool.
2. Select **Certification Authority > Issued Certificates**.
3. Select your current SSL certificate for the Microsoft Active Directory and open the certificate.
4. On the **Certificate** page, click the **Details** tab and click **Copy to File**.
5. In the **Certificate Export Wizard**, select **Base-64 encoded X.509 (.CER)** and click **Next**.
6. Provide a file name and click **Next**.
7. Review your settings to verify that you have the correct Base-64 encoded X.509 (.CER) file and click **Finish**.

The SSL certificate is exported from Microsoft Active Directory to a file so it can be added to the web server keystore for IBM Spectrum Control.

Adding the SSL certificate for the LDAP server to the web server keystore that uses the IKEYCMD command

To secure communications between the IBM Spectrum Control server and the LDAP server, you must add the SSL certificate from the LDAP server to the web server keystore for IBM Spectrum Control.

Tip: Contact your LDAP administrator and obtain the SSL certificate for your LDAP server. The SSL certificate must be in the form of a Base64-encoded file.

You can use the IBM Key Management (IKEYCMD) command to add the LDAP SSL certificate to the IBM Spectrum Control web server keystore.

1. Copy the Base64-encoded file to the location of your IBM Spectrum Control server.
2. Log on to the IBM Spectrum Control server with administrative privileges.
3. Open a command prompt and go to *installation_dir/jre/bin* directory.
4. Choose one of these options to add the SSL certificate for the LDAP server to the keystore for the web server:
 - For Windows operating systems:

```
ikeycmd -cert -add -db installation_dir\wlp\usr\servers\webServer\resources
\security\key.p12 -pw password -label label -file LDAP SSL certificate
```

- For AIX and Linux operating systems:

```
./ikeycmd -cert -add -db installation_dir/wlp/usr/servers/webServer/resources
/security/key.p12 -pw password -label label -file LDAP SSL certificate
```

Where the *label* value is for the LDAP SSL certificate you are adding to the IBM Spectrum Control web server keystore. The *password* value is the password that is associated with the keystore. The *default* value for this password is *default*. The *LDAP SSL certificate* value is the Base64-encoded file that contains the SSL certificate from your LDAP server.

5. Restart the IBM Spectrum Control web server.
6. Choose one of these options to verify that the SSL certificate for LDAP was added to the keystore for the web server:

- For Windows operating systems:

```
ikeycmd -cert -list -db installation_dir\wlp\usr\servers\webServer
\resources\security\key.p12 -pw password
```

- For AIX and Linux operating systems:

```
./ikeycmd -cert -list -db installation_dir/wlp/usr/servers/webServer
/resources/security/key.p12 -pw password
```

The SSL certificate from the LDAP server was added to the IBM Spectrum Control web server keystore to enable secure communications.

Related tasks

[“Starting and stopping the IBM Spectrum Control servers” on page 88](#)

You can start and stop the IBM Spectrum Control servers in the GUI or by running scripts. Note: IBM Spectrum Control servers start automatically on Windows, Linux, or AIX® operating systems when the operating system is started.

[“Exporting SSL certificate from the IBM Security Directory Server to a file” on page 17](#)

To secure communications between IBM Spectrum Control and IBM Security Directory Server, you must export the SSL certificate to a file. The file that is created can then be added to the keystore for IBM Spectrum Control.

[“Exporting SSL certificate from the Microsoft Active Directory to a file” on page 18](#)

To secure communications between IBM Spectrum Control and Microsoft Active Directory, you must export the SSL certificate from the Microsoft Active Directory to a file. The file that is created can then be added to the web server keystore for IBM Spectrum Control.

Using the `ldapEntityType` element for advanced LDAP configuration

To narrow the IBM Spectrum Control view of your LDAP structure so that you can find and map your groups to IBM Spectrum Control roles, you need to configure the `ldapEntityType` element within the `ldapRegistry` element.

Example: LDAP user and group scenario

In this scenario, you want to provide access to LDAP users that reside in a different node of the LDAP structure than your LDAP groups. You also want to prevent authorization of LDAP users and groups that are not associated with IBM Spectrum Control.

In this scenario, the LDAP users use the following distinguished names:

- LDAP user 1: `cn=LDAPUser1,ou=MarketingUsers,dc=storage,dc=company,dc=com`
- LDAP user 2: `cn=LDAPUser2,ou=SalesUsers,dc=storage,dc=company,dc=com`
- LDAP user 3: `cn=LDAPUser3,ou=ManagementUsers,dc=storage,dc=company,dc=com`

In this scenario, the LDAP groups use the following distinguished names:

- LDAP user 1 is a member of LDAP group 1:
`cn=LDAPGroup1,ou=MarketingGroups,dc=storage,dc=company,dc=com`
- LDAP user 2 is a member LDAP group 2:
`cn=LDAPGroup2,ou=SalesGroups,dc=storage,dc=company,dc=com`
- LDAP user 3 is a member of LDAP group 3:
`cn=LDAPGroup3,ou=ManagementGroups,dc=storage,dc=company,dc=com`

In this scenario, `LDAPUser1` and `LDAPUser2` are in different nodes of the LDAP structure than the associated LDAP groups, `LDAPGroup1` and `LDAPGroup2`. You need to find and map `LDAPGroup1` and `LDAPGroup2` to the IBM Spectrum Control roles and be able to log in to IBM Spectrum Control as the `LDAPUser1` and `LDAPUser2`.

When you configure IBM Spectrum Control for LDAP authentication and you encounter this scenario, set the baseDN value in your LDAP XML template file to `dc=storage,dc=company,dc=com`.

In following example, this baseDN value is common to all LDAP users and groups.

Example of the LDAP XML template file that implements this baseDN value:

```
<server description="IBM Web Server">
  <ldapRegistry activeFilters="active_dir_server" baseDN="dc=storage,dc=company,dc=com"
    bindDN="cn=Administrator,cn=users,dc=storage,dc=company,dc=com" bindPassword="password"
    host="ldap.storage.company.com" id="LDAP1" ignoreCase="true"
    ldapType="Microsoft Active Directory"
    port="389" realm="TPCRealm" sslEnabled="false">
  </ldapRegistry>

  <activeLdapFilterProperties groupFilter="(&(cn=%v)(objectcategory=group))" groupIdMap="*:cn"
    groupMemberIdMap="memberof:member" id="active_dir_server"
    userFilter="(&(sAMAccountName=%v)(objectcategory=user))" userIdMap="user:sAMAccountName" />

  <federatedRepository>
    <primaryRealm allowOpIfRepoDown="true" name="TPCRealm">
      <participatingBaseEntry name="dc=storage,dc=company,dc=com"/>
      <!-- The next two entries must NOT be changed -->
      <participatingBaseEntry name="o=TPCRealm"/>
      <participatingBaseEntry name="o=OSRealm"/>
    </primaryRealm>
  </federatedRepository>
</server>
```

When you use this example LDAP XML template file, you also are able to find and map LDAPGroup3 to an IBM Spectrum Control role. This behavior enables LDAPUser3 to log in to IBM Spectrum Control, which is not part of the successful outcome. Use the `ldapEntityType` element within the `ldapRegistry` element so you can only find and map LDAPGroup1 and LDAPGroup2 to IBM Spectrum Control roles.

Tip: Whenever you modify the `ldapRegistry` element, in the LDAP XML template file, verify that the XML file is valid by opening it in a web browser and checking the results.

This is the previous example of the LDAP XML template file that was edited to use the `ldapEntityType` element within the `ldapRegistry` element:

```
<server description="IBM Web Server">
  <ldapRegistry activeFilters="active_dir_server" baseDN="dc=storage,dc=company,dc=com"
    bindDN="cn=Administrator,cn=users,dc=storage,dc=company,dc=com" bindPassword="password"
    host="ldap.storage.company.com" id="LDAP1" ignoreCase="true" ldapType="Microsoft Active Directory"
    port="389" realm="TPCRealm" sslEnabled="false">

    <ldapEntityType name="Group">
      <objectClass>group</objectClass>
      <searchBase>ou=MarketingGroups,dc=storage,dc=company,dc=com</searchBase>
      <searchBase>ou=SalesGroups,dc=storage,dc=company,dc=com</searchBase>
    </ldapEntityType>

    <ldapEntityType name="PersonAccount">
      <objectClass>user</objectClass>
      <searchBase>ou=MarketingUsers,dc=storage,dc=company,dc=com</searchBase>
      <searchBase>ou=SalesUsers,dc=storage,dc=company,dc=com</searchBase>
    </ldapEntityType>

  </ldapRegistry>

  <activeLdapFilterProperties groupFilter="(&(cn=%v)(objectcategory=group))"
    groupIdMap="*:cn" groupMemberIdMap="memberof:member" id="active_dir_server"
    userFilter="(&(sAMAccountName=%v)(objectcategory=user))"
    userIdMap="user:sAMAccountName" />

  <federatedRepository>
    <primaryRealm allowOpIfRepoDown="true" name="TPCRealm">
      <participatingBaseEntry name="dc=storage,dc=company,dc=com"/>
      <!-- The next two entries must NOT be changed -->
      <participatingBaseEntry name="o=TPCRealm"/>
      <participatingBaseEntry name="o=OSRealm"/>
    </primaryRealm>
  </federatedRepository>
</server>
```

When you use the LDAP XML template that implements the `ldapEntityType` element, it prevents you from finding and mapping LDAPGroup3 to IBM Spectrum Control role. However, you can find and map LDAPGroup1 and LDAPGroup2 to IBM Spectrum Control roles and LDAPUser1 and LDAPUser2 can log in to IBM Spectrum Control.

Adding customized text to the logon page

On the logon page for IBM Spectrum Control, you can show customized text when users access the GUI.

1. Open the directory that was created to install IBM Spectrum Control:
 - The default installation directory for Windows operating systems is C:\Program Files\IBM\TPC.
 - The default installation directory for AIX or Linux operating systems is /opt/IBM/TPC.
2. Go to the customization directory:
 - On Windows operating systems**
The customization directory is in the \wlp\usr\servers\webServer\ path.
 - On AIX or Linux operating systems**
The customization directory is in the /wlp/usr/servers/webServer/ path.
3. Open the LoginText.html file in a text editor:
 - a) Type the text that you want to show to the user before they log on to the GUI.
 - Tip:** To format the text that you want to add, you can use HTML tags, such as paragraph tags, list tags, bold tags, and italic tags.
 - b) Save the LoginText.html file.
4. Open the GUI.

The customized text that you added is shown below the **logon** page.

Configuring switches

IBM Spectrum Control can discover devices in the SAN and collect data about the performance of those devices. You must correctly configure the switches in your SAN to enable IBM Spectrum Control to complete these tasks.

IBM Spectrum Control is designed to operate using industry-based standards for communicating with Fibre Channel switches and other SAN devices. This communication can be done using simple network management protocol (SNMP) agents, Storage Management Initiative (SMI) agents, or a combination of these agent types. The supported switch vendors are Brocade, Cisco, and other switch types. IBM and other vendors often sell these switches under their own labels.

Determining the agent type or types to use with a switch

For Cisco switches and fabrics, an SNMP agent is required. SNMPv3 is the preferred version.

For Brocade switches and fabrics, the preferred type of agent is the SMI agent. The SMI agent provides most fabric functions, and other agent types can be added for redundancy.

To learn more about the information that is gathered by each type of agent, see [Agent types for switch and fabric functions](#).

Using SNMP agents

IBM Spectrum Control uses the SNMP protocol to send queries across the IP network to management information bases (MIBs) supported on the switch. IBM Spectrum Control uses the Fibre Alliance FC Management MIB and the Fibre Channel FE MIB. The queries are sent only to switches that were added to IBM Spectrum Control for use as SNMP agents. SNMP information is collected for a single switch. The SNMP discovery registers each switch.

For a Cisco switch to successfully receive and respond to queries from IBM Spectrum Control, the following basic requirements must be met:

- IBM Spectrum Control can use SNMPv3 (preferred) or SNMPv1 to probe switches and fabrics. The SNMPv3 protocol is preferred because it provides better security, but switches that use the SNMPv1 protocol are also supported. Some switches are configured to use SNMPv3 by default.
- If the switch uses an SNMP agent, the Fibre Alliance FC Management MIB (FA MIB) and Fibre Channel Fabric Element MIB (FE MIB) must be enabled on the switch.
- When using the SNMPv1 protocol, the community string that is configured in IBM Spectrum Control must match one of the community strings that are configured on the switch with read access. Cisco switches must additionally have a community string match for write access. The default community strings in IBM Spectrum Control are "public" for read access and "private" for write access. Other community strings can be defined on the switches, but are not used. Community strings are not relevant when using the SNMPv3 protocol.
- SNMP access control lists must include the IBM Spectrum Control system. These access control lists are defined and configured on the switches. Some lists automatically include all hosts, while others exclude all by default.
- The Fibre Channel (FC) or Fibre Channel over Ethernet (FCoE) protocols must be enabled on the switch. Some switches, such as the Cisco Nexus 5000 series, require you to enable these protocols. Otherwise, IBM Spectrum Control will not recognize the switch when you try to add it using the **Add Switches and Fabrics for Monitoring** dialog. For instructions on how to configure Cisco switches for FCoE enablement, go to the Cisco product website at <http://www.cisco.com> and click **Support**.

Another aspect of the SNMP configuration includes trap notification. SNMP traps are generated by the switch and directed to IBM Spectrum Control as an indication that something in the fabric changed and that a discovery must occur to identify the changes. The default configuration for handling switch traps is to send them from the switch to port 162 on the IBM Spectrum Control system. To successfully generate and receive traps, there are some configuration requirements:

- The trap destination parameter on the switch must be set. This parameter is the host that receives the trap and sends it to IBM Spectrum Control. The parameter is set on the switch.
- The destination port parameter on the switch must be set. IBM Spectrum Control listens on port 162 by default. The parameter is set on the host.
- The traps must be sent as SNMPv1. This parameter is set on the switch.
- The trap severity level must be set to generate traps for change conditions. This level typically means to send error level traps and anything more severe. This parameter is set in IBM Spectrum Control.

Using SMI agents

You must install or enable an SMI agent to perform the following tasks for Brocade switches and fabrics, including:

- Scheduling probes to gather switch and fabric information.
- Gathering asset, status, and performance data about Brocade fabrics and switches.
- Creating and managing alerts.

For information about installing or enabling an SMI agent for a switch, contact the switch vendor.

Managing a SAN without agents

You can manage a SAN when there are no agents.

In the following situations, there might not be any agents on the SAN:

- The hosts do not currently have a Storage Resource agent or Fabric agent installed.
- The host operating system is not supported by the Storage Resource agent or Fabric agent.
- The customer requirements do not require the deployment of a Storage Resource agent or Fabric agent.

In these cases, it is recommended that an agent is installed on the Device server itself. This action allows the Device server to use advanced features like Remote Node Identification, which requires an agent.

Normally the Device server does not have a Fibre Channel host bus adapter. In this configuration, the following steps are taken:

1. A Fibre Channel host bus adapter is added to the manager.
2. An agent is installed on the Device server (the Device server is installed first).
3. All storage devices are verified to ensure that they use LUN masking techniques. The LUN masking techniques prevent the Device server from accessing the disks used by the host systems.
4. The Fibre Channel host bus adapter is attached to the SAN to be managed. This host is added to each zone that is intended to be managed by the Device server.

Setting timeout values for the Device server

If a probe or discovery of a storage subsystem times out before the operation completes, you can increase the timeout values for the Device server.

If a probe or discovery of a storage subsystem times out before the operation completes, you receive the following error message:

```
HWN021650E Encountered timeout while connecting to CIMOM IP:port.  
Check the CIMOM or increase timeout value.
```

where *IP* is the IP address, and *port* is the port number. If you determine that the Common Information Model Object Manager (CIMOM) is not the cause of the problem, you can use the command-line interface (CLI) to increase the timeout values for the Device server.

For those storage systems that use native interfaces to connect to IBM Spectrum Control you see this error message:

```
HWN020103E The external process exceeded the timeout limit and was cancelled.
```

The following storage systems use native interfaces to connect to IBM Spectrum Control:

- System Storage® DS8000®
- SAN Volume Controller
- The XIV®
- IBM Spectrum Accelerate
- Storwize® V3500
- Storwize V3700
- Storwize V7000
- Storwize V7000 Unified
- FlashSystem 9100
- FlashSystem V840
- FlashSystem V9000
- IBM SONAS
- IBM Spectrum Scale
- IBM Cloud Object Storage

1. Run the **getdscfg** command to determine the current values of the timeout properties. From the command prompt, enter the following command:

```
cli>tpctool getdscfg -user user -pwd password -url host:port  
-property timeout_property
```

where:

- *user* is an IBM Spectrum Control user ID.

- *password* is the password for the IBM Spectrum Control user ID.
- *host* is the host name or IP address, and *port* is a valid port number for the HTTP service of the Device server. The default value for *port* is typically 9550.
- *timeout_property* is one of the following strings:
 - httpTimeout
 - CIMClientWrapper.Timeout
 - Probe.Timeout.Array
 - Probe.Timeout.LMM
 - Discovery.Timeout
 - CIMOMManager.TestConnectionTimeout

Important: Timeout properties are displayed in milliseconds. If the value is **0** (zero), it means that there is no timeout.

For the storage systems that use the native interface, the *timeout_property* strings are:

- NAPI.Timeout.TestConnection
- NAPI.Timeout.Probe
- NAPI.Timeout.EventPoll

2. Run the **setdscfg** command to increase the timeout value. Run the following command:

```
cli>tpctool setdscfg -user user -pwd password -url host:port
-property timeout_property timeout_value
```

Tip: For IBM SONAS and Storwize V7000 Unified, the refresh of configuration data from the storage system can take some time to complete and might cause the probe to time out, even if the timeout value is increased. To reduce the duration of the probe run for IBM SONAS and Storwize V7000 Unified, run the following command:

```
cli>tpctool setdscfg -user user -pwd password -url host:port
-property Probe.GetRecentSONASData -context DeviceServer false
```

This command changes the probe configuration to use cached configuration data from the storage system, which reduces the duration of the probe run. However, the information that is collected by the probe might be slightly out of date.

For more information about **tpctool**, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/com.ibm.spectrum.sc.doc/fqz0_r_tpctool_command.html. You also can view help from the command line by issuing the command with the **-help** option.

Configuring Service Location Protocol

You can enable IBM Spectrum Control to discover a larger set of storage devices through Service Location Protocol (SLP). In addition to some of the more common SLP configuration issues, there is also information about router configuration, SLP directory agent configuration, and environment configuration.

For additional information about SLP, see the **Service Location Protocol Request for Comments** website at <http://www.ietf.org/rfc/rfc2165.txt>.

Note: The storage systems that use the native interfaces (DS8000, XIV, SAN Volume Controller, and Storwize V7000) do not use SLP discovery.

Router configuration

Configure the routers in the network to enable general multicasting or to allow multicasting for the SLP multicast address and port, 239.255.255.253, port 427. The routers of interest are the ones associated

with subnets that contain one or more storage devices that are to be discovered and managed by IBM Spectrum Control.

To configure your router hardware and software, refer to your router and configuration documentation.

SLP directory agent configuration

Review these suggestions when you configure the SLP directory agent.

Configure the SLP directory agents (DAs) to circumvent the multicast limitations. With statically configured DAs, all service requests are unicast by the user agent. Therefore, it is possible to configure one DA for each subnet that contains storage devices that are to be discovered by IBM Spectrum Control. One DA is sufficient for each of the subnets. Each of these DAs can discover all services within its own subnet, but no other services outside its own subnet. To allow IBM Spectrum Control to discover all the devices, it needs to be statically configured with the addresses of each of these DAs. This operation can be accomplished by using the IBM Spectrum Control Discovery Preference panel.

You can use this panel to enter a list of DA addresses. IBM Spectrum Control sends unicast service requests to each of these statically configured DAs, and sends multicast service requests on the local subnet on which IBM Spectrum Control is installed. Configure an SLP DA by changing the configuration of the SLP service agent (SA) that is included as part of an existing CIM Agent installation. This action causes the program that normally runs as an SLP SA to run as an SLP DA.

Note: The change from SA to DA does not affect the CIMOM service of the subject CIM Agent, which continues to function normally, sending registration and deregistration commands to the DA directly.

Environment configuration

This section provides information about the configuration of your environment.

It might be advantageous to configure SLP DAs in the following environments:

- In environments where there are other non-IBM Spectrum Control SLP UAs that frequently perform discovery on the available services, an SLP DA must be configured. This action ensures that the existing SAs are not overwhelmed by too many service requests.
- In environments where there are many SLP SAs, a DA helps decrease network traffic that is generated by the multitude of service replies. It also ensures that all registered services can be discovered by a given UA. The configuration of an SLP DA is recommended when there are more than 60 SAs that need to respond to any given multicast service request.

SLP registration and `slptool`

IBM Spectrum Control uses Service Location Protocol (SLP) discovery, which requires that all the discovered CIM agents are registered by using the SLP.

In a non-multicast network environment, SLP can only discover CIM agents that are registered in its IP subnet. For CIM agents outside of the IP subnet, you need to use an SLP DA and register the CIM agents by using **`slptool`**. Ensure that the **`CIM_InteropSchemaNamespace`** and **`Namespace`** attributes are specified.

For example, enter the following command:

```
slptool register service:wbem:https://myhost.com:port
```

Where *myhost.com* is the name of the server that is hosting the CIM agent, and *port* is the port number of the service, for example 5989.

Note: **`slptool`** is installed with a CIM agent. Run the command from the computer that is hosting the CIM agent.

SLP discovery

A common problem with SLP discovery is due to IP multicasting being disabled on the network router. Communication between the SLP SA and UA is done with IP multicasting. Follow these recovery procedures when there are SLP discovery problems and IP multicasting is disabled on the network router.

Note: The storage systems that use native interfaces, for example, DS8000, XIV, SAN Volume Controller, and Storwize V7000 do not use SLP discovery.

There are two recovery procedures when there are SLP discovery problems and IP multicasting is disabled on the network router:

1. Configure one DA for each subnet within the environment.
2. Enable IP multicasting on the router which is disabled by default. Here is a list of common router configurations for multicasting:
 - Internet Group Management Protocol (IGMP) is used to register individual hosts in particular multicast groups and to query group membership on particular subnets.
 - Distance Vector Multicast Routing Protocol (DVMRP) is a set of routing algorithms that use a technique called reverse path forwarding. These algorithms provide the best solution for how multicast packets are to be routed in the network.
 - Protocol-Independent Multicast (PIM) comes in two varieties: dense mode (PIM-DM) and sparse mode (PIM-SM). The dense mode and sparse mode routines are optimized for networks where either a large percentage of nodes requires multicast traffic (dense) or a small percentage of nodes requires the sparse traffic.
 - Multicast Open Shortest Path First (MOSPF) is an extension of OSPF. It is a link-state unicast routing protocol that attempts to find the shortest path between any two networks or subnets to provide the most optimal packet routing.

To properly configure the routers for multicasting, see the reference and configuration documentation from the router manufacturer.

Configuring IP addressing

This section provides information about configuring IP addressing.

Configuring IBM Spectrum Control with multiple IP addresses

If the system where IBM Spectrum Control is to be installed has multiple IP addresses, then a configuration value must be set manually as a post-installation task by using the **tpctool setdscfg** command. The value to be set is for the local IP address, which must be used for subscription for CIM Indications for CIM agents.

Restriction: This task does not apply to storage systems that use the native interfaces, for example, DS8000, XIV, SAN Volume Controller, and Storwize V7000.

If you are using IPv6 computers, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/com.ibm.spectrum.sc.doc/fqz0_r_planning_ipv6.html.

For multiple IPv6 addresses, the IPv6 address to use for CIM indication subscription by IBM Spectrum Control can be specified by setting the property `System.LocalIPv6Address` as described.

With dual stack IPv4 and IPv6 IBM Spectrum Control servers, two IP addresses are required to subscribe to IPv4 CIMOMs and IPv6 CIMOMs. The configuration property `System.LocalIPv6Address` is used for IPv6 CIMOMs and the property `System.LocalIPAddress` is used for IPv4 CIMOMs.

To change the IP address, follow these steps:

1. Open a command prompt window on the server system.
2. Change to the following directory:

```
cd installation_dir\cli
```

3. Enter the following command:

```
tpctool setdscfg -user user_ID -pwd password -url  
host:port -property System.LocalIPv6Address value
```

Where:

user_ID

Is the user ID.

password

Is the password for the user.

host

Is either the host name or IP address of the system that is running IBM Spectrum Control.

port

Is a valid port number for the HTTP service of the Device server (the default is 9550).

value

Is the local IP address, which must be used for subscription for CIM Indications for CIM agents.

4. Verify that the command was successful by entering this command:

```
tpctool getdscfg -user user_ID -pwd password  
-url host:port -property System.LocalIPv6Address
```

Changing the HOSTS file

When you install IBM Spectrum Control on your Windows operating systems, you must follow these steps to avoid addressing problems with the systems you want to manage. These problems are caused by the address resolution protocol that returns the host short name rather than the fully qualified host name. You can avoid this by modifying the entries in the corresponding host tables on the DNS server and on the local computer system. The fully qualified host name must be listed before the short name in each entry that is associated with systems managed by IBM Spectrum Control.

The **HOSTS** file is in the %SystemRoot%\system32\drivers\etc\ directory. To change the HOSTS file, follow these steps:

1. Open the HOSTS file in a text editor.
2. Add, remove, or modify the host entries. In the following example of a HOSTS file, the short name is incorrectly listed before the fully qualified host name. This can cause address resolution problems in IBM Spectrum Control.

```
# Copyright (c) 1993-2009 Microsoft Corp.  
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#      102.54.94.97      rhino.acme.com      # source server  
#      38.25.63.10      x.acme.com         # x client host  
#  
192.168.123.146        jason            jason.groupa.mycompany.com
```

3. In the following example, the order of the host names has been changed so that the fully qualified host name is placed before the short name. The host names must be entered in the order that is shown so IBM Spectrum Control can locate the host. Use this format for any hosts that are associated with IBM Spectrum Control.

```
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com         # x client host
#
192.168.123.146      jason.groupa.mycompany.com      jason
```

Note: Host names are case-sensitive. This is a WebSphere requirement. For example, if your computer shows the name as JASON (uppercase), then you must enter JASON in the HOSTS file.

Deploying Storage Resource agents

You can manage your Storage Resource agent deployments.

Deploy Storage Resource agents through the user interface rather than a separate installation wizard. You can have only one agent per host that points to the same IBM Spectrum Control server.

Before you begin: Before you deploy Storage Resource agents, see [“Deployment guidelines and limitations for Storage Resource agents”](#) on page 28 for a list of considerations.

If you deploy Storage Resource agents on multiple computers at the same time, the computers must have the same administrative user ID and password. IBM Spectrum Control uses these user credentials to log on to the computers when the Storage Resource agents are deployed.

To deploy Storage Resource agents, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. Click **Add Server**.
3. Select **Deploy an agent for full server monitoring**.
4. Select one of the following methods for adding a server:
 - Add a server by manually entering information about the server and the Storage Resource agent.
 - Add one or more servers by importing configuration information from a comma-delimited file.
5. Configure deployment information for the Storage Resource agents.
6. Schedule the agent deployment and the data collection for the servers.
7. Click **Finish** to deploy the Storage Resource agents.

Deployment guidelines and limitations for Storage Resource agents

You must consider the following guidelines and limitations when you manage Storage Resource agents in your environment.

Use the following information when you deploy Storage Resource agents:

- [Multiple Storage Resource agents that are probing or scanning the same storage resources](#)
- [Platforms that support the deployment of Storage Resource agents](#)
- [Product functions that are not available for storage devices monitored by Storage Resource agents](#)
- [Required authority for deploying Storage Resource agents](#)
- [Orphan zones](#)
- [Firewalls and Storage Resource agents deployments](#)
- [Deploying Storage Resource agents on multiple computers](#)
- [Communication between the IBM Spectrum Control server and a Storage Resource agent](#)
- [Daemon and non-daemon services](#)
- [Port numbers for Storage Resource agents deployed as a daemon service](#)
- [Authentication between the IBM Spectrum Control server and a Storage Resource agent](#)
- [Replacing default SSL certificates](#)

- [Storage Resource agents on the same computer](#)
- [Time zones for computers monitored by Storage Resource agents](#)
- [Connections for Linux and AIX operating systems by using Remote Shell protocol \(RSH\)](#)
- [Deployments on Windows - NetBIOS setting](#)
- [Deployments on Windows - User Account Control \(UAC\) remote restrictions](#)

Multiple Storage Resource agents that are probing or scanning the same resources

If multiple Storage Resource agents are set up to probe or scan the same storage resources, the Storage Resource agent that was added to IBM Spectrum Control first is used for the probe or scan. Therefore, only data that is gathered by the first Storage Resource agent is shown.

Platforms that support the deployment of Storage Resource agents

For a list of platforms on which you can deploy Storage Resource agents, see the [IBM Spectrum Control interoperability matrix](#) and go to the *Agents, Servers and Browsers* section.

Product functions that are unavailable for resources that are monitored by Storage Resource agents

Before you deploy a Storage Resource agent, ensure that the product functions you want to use on the monitored resources are available for those agents. The following functions are not available for resources that are monitored by Storage Resource agents:

- Certain relational database monitoring. For list of relational databases that can be monitored by Storage Resource agents, see the [IBM Spectrum Control interoperability matrix](#) and go to the *Agents, Servers and Browsers* section.
- The reporting of HBA, fabric topology, or zoning information for fabrics that are connected to hosts that are running Linux on IBM System z® hardware. These limitations also apply to Storage Resource agents on all guest operating systems for VMware configurations.

Required authorities for deploying and running Storage Resource agents

Before you can create deployment schedules and deploy Storage Resource agents on target computers, you must meet the following requirements:

- To create deployment schedules, you must be logged in to IBM Spectrum Control with a user ID that has the **Administrator** role. For information about user roles, see [“Authorizing users” on page 5](#).
- To deploy Storage Resource agents on target computers, you must provide a user ID that has administrative rights on those computers. You enter this ID when you create a deployment schedule. IBM Spectrum Control uses this ID to log on to the target computers and install and configure the necessary runtime files for the agents.

The user under which a Storage Resource agent (daemon or non-daemon) runs must have the following authorities on the target computers:

- On the Linux or AIX operating systems, the user must have root authority. By default, an agent runs under the user 'root'.
- On the Windows operating systems, the user must have Administrator authority and be a member of the Administrators group. By default, a Storage Resource agent runs under the 'Local System' account.

Orphan zones

Storage Resource agents do not collect information about orphan zones. An orphan zone is a zone that does not belong to at least one zoneset.

Firewalls and Storage Resource agent deployments

Before you can deploy a Storage Resource agent on a computer, you must turn off the firewall on that computer. If you do not turn off the firewall, the deployment fails.

To turn off the firewall on a Windows 2008 computer, complete the following steps:

1. Open Administrative Tools. For information about how to open Administrative Tools, see [“Accessing administration tools” on page 140](#).
2. Click **Windows Firewall with Advanced Security**.

3. Click **Windows Firewall Properties**.
4. Change the **Firewall state** field to **Off** on the following tabs:
 - **Domain Profile**
 - **Private Profile**
 - **Public Profile**
5. Click **OK** to accept the changes and exit.
6. Deploy a Storage Resource agent to the Windows 2008 computer.

Deploying Storage Resource agents on multiple computers

If you deploy Storage Resource agents on multiple computers at the same time, the computers must have the same administrative user ID and password. IBM Spectrum Control uses these user credentials to log on to the computers when you install Storage Resource agents.

Tip: When you deploy Storage Resource agents on multiple computers, a globally unique identifier (GUID) is created for each computer (if one does not exist).

Communication between the IBM Spectrum Control server and a Storage Resource agent

The IBM Spectrum Control server connects to a monitored computer when a Storage Resource agent is deployed and whenever a data collection schedule runs against that agent.

During deployment, the server communicates with the target computer by using one of the following protocols:

- Windows server message block protocol (SMB)
- Secure Shell protocol (SSH)
- Remote execution protocol (REXEC)
- Remote shell protocol (RSH)

After deployment, the type of communication between the server and agent on that computer depends on whether you deployed the agent as daemon service or non-daemon service.

Daemon and non-daemon services

You can deploy a Storage Resource agent as a daemon or non-daemon service:

- A Storage Resource agent that is deployed as a daemon service runs in the background on the monitored computer and listens for requests from the IBM Spectrum Control server. Connectivity between the server and agent is established by using SSL. The server and agent have their respective certificates and no additional information is required besides those certificates and the security that is provided by the SSL protocol.
- A Storage Resource agent deployed as a service on demand (non-daemon service) runs as a stand-alone executable file on the monitored computer. Communication from the server to the agent uses the same protocol that was used during the deployment of the agent. Communication from the agent to the server uses SSL.
- A Storage Resource agent that is deployed as a daemon service on AIX, Linux, and Windows servers monitors disk paths in near real-time to detect errors. When deployed as a daemon service on an AIX server, the agent also monitors disk error events in near real-time.

If the Storage Resource agent detects path status changes or disk errors, they are included in the status of the disks and paths. You can define alerts so that you are notified of changes to the status of the paths on monitored disks.

Only status changes for existing paths are detected. If a new path is added, or an existing path is removed, the number of paths that is displayed is not updated immediately. The number of paths is updated after the next scheduled probe collects data.

If a disk on an AIX server has an error status and you fix the error, you might want the new status of the disk to be displayed immediately. To display the new status immediately, you must reset the

status indicator for the disk. To reset the status indicator, use the **errclear** command to clear the error log. To clear the error log, use the following syntax:

```
errclear -d H -N disk_name 0
```

For example, if you fixed an error on hdisk4, and want to display the new status immediately, run the following command:

```
errclear -d H -N hdisk4 0
```

If you do not reset the status indicator for the disk, the status changes automatically after a few hours.

For information about the **errclear** command, see the product documentation at http://www.ibm.com/support/knowledgecenter/ssw_aix_71/com.ibm.aix.cmds2/errclear.htm.

Port numbers for Storage Resource agents deployed as a daemon service

The following port numbers are used by Storage Resource agents that are deployed as daemon service:

- 9567 (For the Storage Resource agent that is deployed on the same server as IBM Spectrum Control.)
- 9510 (For Storage Resource agents that are deployed on remote servers.)

Storage Resource agents that are deployed as a non-daemon service do not use a port.

Authentication between the IBM Spectrum Control server and a Storage Resource agent

IBM Spectrum Control requires the correct authentication information (user name, password, port, certificate location, or passphrase) for monitored computers each time it communicates with Storage Resource agents on those computers. If the authentication information changes for a host computer on which a Storage Resource agent is deployed, the authentication information for that agent must be updated by using the **Modify Agents > Update Credentials** action on the **Servers** page in the GUI.

Replacing default SSL certificates

IBM Spectrum Control provides default SSL certificates for communication between the Data server and Storage Resource agent.

IBM Spectrum Control Version 5.2.2 uses SSL certificates with 2048-bit encryption keys whereas previous versions of IBM Spectrum Control used 1024-bit encryption keys. If you upgrade IBM Spectrum Control from a version earlier than 5.2.2, your SSL certificates are not updated automatically. If you want to use 2048-bit encryption keys with previous versions of IBM Spectrum Control, you must replace the default SSL certificates with custom SSL certificates.

For information about how to replace SSL certificates, see [“Replacing default SSL certificates with custom certificates”](#) on page 38.

Storage Resource agents on the same computer

You cannot deploy a Storage Resource agent on a computer where a Storage Resource agent is already installed and pointing to the same Data server. You can deploy a Storage Resource agent on the same computer as another Storage Resource agent if those agents communicate with different Data servers and use different ports when you listen for requests.

Time zones for computers that are monitored by Storage Resource agents

The time zones of computers that are monitored by Storage Resource agents are shown as Greenwich mean time (GMT) offsets in IBM Spectrum Control reports. For example, a computer in Los Angeles shows the following time zones in the By Computer report in Asset reporting:

```
(GMT-8:00) GMT-8:00
```

Connections for Linux and AIX operating systems by using Remote Shell protocol (RSH)

If RSH is configured to use a user ID and password, the connection fails. To successfully connect to a system by using RSH, you must set up the `.rhosts` file (in the home directory of the account). RSH must be configured to accept a login from the system that is running your application.

Deployments on Windows operating systems - NetBIOS setting

To install a Storage Resource agent on Windows targets, the **Enable NetBIOS over TCP/IP** option must be selected in the Control Panel settings for the computer's network connections properties. To set this option, complete the following steps:

1. Open Windows Control Panel. For information about how to open Windows Control Panel, see [“Accessing administration tools”](#) on page 140.
2. Select **Network and Dial-Up Connections > some_connection > Properties > Internet Protocol (TCP/IP) > Advanced > WINS > Enable NetBIOS over TCP/IP**.

To determine whether these ports are not blocked for inbound requests, see the documentation for your firewall.

To determine whether security policies are blocking the connection ports, open Administrative Tools. For information about how to open Administrative Tools, see [“Accessing administration tools”](#) on page 140..

Depending on whether your policies are stored locally or in Active Directory, follow these directions:

Policies that are stored locally

For policies that are stored locally, complete the following steps:

1. Open Windows Administrative Services.
2. Click **Local Security Policy > IP Security Policies on Local Computer**.

Policies that are stored in Active Directory

For policies that are stored in Active Directory, examine the IP security policies and edit or remove filters that block the ports:

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

For all Windows systems, the Server service must be running to connect to a Windows system by using the Windows protocol.

The following table lists the ports that are reserved for NetBIOS. Ensure that these ports are not blocked.

Port	Description
135	NetBIOS Remote procedure call. (Not currently used.)
137	NetBIOS name service.
138	NetBIOS datagram. (Not currently used.)
139	NetBIOS session (for file and print sharing).
445	CIFS (on Windows XP).

For Windows Server 2008, shares must be shared for the Guest or Everyone accounts, and password protected sharing must be disabled. To disable password protected sharing, follow these steps:

1. Click **Control Panel > Networking and Sharing Center**.
2. Click the down arrow next to **Password protected sharing**.
3. Click **Turn off password protected sharing**.
4. Click **Apply**.
5. Exit from the Control Panel.

Deployments on Windows 2008 - User Account Control (UAC) remote restrictions

To install Storage Resource agents remotely on a Windows 2008 operating system, you must disable the User Account Control (UAC) remote restrictions on the Windows operating system. User Account Control is a security component on Windows operating systems.

Tip: To disable UAC restrictions, you must modify the computer registry. Serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if problems occur. For information about how to back up and restore the registry, see <http://support.microsoft.com/kb/322756/>.

To disable UAC remote restrictions, follow these steps:

1. Open the Windows **Run** window. For information about how to open the **Run** window, see [“Accessing administration tools”](#) on page 140.
2. Enter **regedit** and click **OK**.
3. Locate and click the following registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System
```

4. If the LocalAccountTokenFilterPolicy registry entry does not exist, follow these steps:
 - a. On the **Edit** menu, click **New > DWORD Value**.
 - b. Enter LocalAccountTokenFilterPolicy as the name for the DWORD value and click **Enter**.
 - c. Click **LocalAccountTokenFilterPolicy**, and click **Modify**.
 - d. In the **Edit DWORD Value** window, enter **1**, then click **OK**.

This value can be 0 or 1:

0

This value builds a filtered token. This value is the default value. The administrator credentials are removed.

1

This value builds an elevated token.

- e. Exit the registry editor.

Creating a certificate for SSH protocol

Before you install the Storage Resource agents by using the SSH protocol, you can optionally create a certificate.

Note: The Storage Resource agent only supports either DES-EDE3-CBC encryption or no encryption for the private key used in SSH protocol communication between the server and agent. The default encryption that is used in the **ssh-keygen** command on UNIX is always DES-EDE3-CBC. However, with Windows Cygwin, the **ssh-keygen** command generates a key with AES-128-CBC encryption if a passphrase is specified. If there is no passphrase, the private key is generated without encryption. For more information about encryption, see <https://www.openssl.org/docs/man1.0.2/apps/enc.html>.

Creating a certificate for SSH protocol (non-Windows)

The Storage Resource agent only supports either DES-EDE3-CBC encryption or no encryption for the private key used in SSH protocol communication between the server and agent. The default encryption used in the **ssh-keygen** command on UNIX is always DES-EDE3-CBC but with Windows Cygwin, it is using AES-128-CBC encryption if a passphrase is specified. If there is no passphrase, the private key is generated without encryption.

To create a certificate for SSH protocol, complete the following steps:

1. Telnet to the remote machine using the root user ID.

2. To create an SSH certificate on AIX, you must first install the following packages (if not already installed):

```
openssl.base.openssh.base.client  
openssh.base.server
```

3. Go to the directory where you want to create the certificate:

```
cd ~/.ssh
```

4. Enter **ssh-keygen -t rsa**. Accept the default names (for example, **id_rsa**).

5. Enter the passphrase.

6. Two files are created:

id_rsa

The private key.

id_rsa.pub

The public key.

7. Create an `authorized_key` file in the same location as `id_rsa.pub` by entering the following command:

```
cat id_rsa.pub >> authorized_keys
```

8. Copy the `id_rsa` (private key) to your server machine. For example, to copy the `id_rsa` file to `:\keys\id_rsa` on the IBM Spectrum Control server (user responses are in boldface type):

```
# ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (//.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
You identification has been save in //.ssh/id_rsa.  
Your public key has been save in //.ssh/id_rsa.pub.  
The key fingerprint is:  
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx root@server  
# cat id_rsa >> authorized_keys  
# ls -l  
total 24  
-rw-r--r-- 1 root system 1743 Oct 15 09:40 authorized_keys  
-rw--- 1 root system 1743 Oct 15 09:39 id_rsa  
-rw-r--r-- 1 root system 399 Oct 15 09:39 id_rsa.pub  
#
```

Note: You must copy the file in binary mode.

9. To connect to the remote system by using the private key, enter the following information in the Remote Agent Machines window of the GUI, when you install the Storage Resource agent:

- User
- Certificate Location (c:\keys\id_rsa)
- Passphrase

Setting up an SSH daemon on Windows

On Windows Server 2003, Windows XP, Windows Server 2008, or Windows Vista, you must run the **ssh-host-config** command.

Note: Cygwin is not a prerequisite for the Storage Resource agent on Windows. To use the SSH protocol on Windows, an SSH software program must be used because Windows does not come with an SSH service. Cygwin is a free software program providing SSH access to a Windows server. Cygwin can be used if you want to run the Storage Resource agent by using the SSH protocol.

You must be in a Cygwin window or be an X term user to create the **sshd** service. In most cases, you click the `cygwin.bat` file to start the Bash shell.

Complete the following steps:

1. Install Cygwin.
2. Set up your **sshd** service in Cygwin.
3. Create the certificate.

Installing Cygwin

To install Cygwin, go to <http://cygwin.com>. This page contains a link that displays help for the setup program and a link to download the setup program. Read the help before running the setup program. Then download the Cygwin program by clicking the **Install Cygwin now** link. Start the setup program on your computer by running the **setup.exe** program. Select the appropriate download option (**Install from Internet**, **Download from Internet**, or **Install from Local Directory**) as described in the help files.

If you are upgrading from an older version of Cygwin to a newer version, you need to remove the **sshd** service before installing the new version of Cygwin.

Accept the default installation options as they are presented to you (Root Directory, Install For, Default Text File Type, and so on). Select a download mirror that is geographically close to your location. Some sites require an FTP account before you can install Cygwin. You can either request an account or simply select another mirror.

During the installation process, a Select Packages list is displayed. Expand the plus sign (+) next to the Admin category and select **cygrunsrv** and the **Bin** check box. Expand the plus sign (+) next to the Net category and select **openssh**. Expand the plus sign (+) next to the Util category and select **diffutils**. Click **Next** to resume the setup program. The time required to download the packages depends on how busy the mirror is, and on the speed of your internet connection. With **openssh** and **cygrunsrv**, the downloaded files require approximately 70 MB of disk space. Allow 20 minutes to 30 minutes for the download and installation to complete.

Setting up your sshd service in Cygwin

Here is an example of the sequence of steps and responses. The responses to the prompts are in boldfaced type.

1. Run the **ssh-host-config** command.

Note: With Cygwin, you might experience permission problems when running the **ssh-host-config** command. If you have permission problems, run these commands:

```
chmod +r /etc/passwd
chmod +r /etc/group
chmod 777 /var
```

\$ ssh-host-config

```
*** Info: Generating missing SSH host keys
*** Query: Overwrite existing /etc/ssh_config file? (yes/no) yes
*** Info: Creating default /etc/ssh_config file
*** Query: Overwrite existing /etc/sshd_config file? (yes/no) yes
*** Info: Creating default /etc/sshd_config file

*** Info: StrictModes is set to 'yes' by default.
*** Info: This is the recommended setting, but it requires that the POSIX
*** Info: permissions of the user's home directory, the user's .ssh
*** Info: directory, and the user's ssh key files are tight so that
*** Info: only the user has write permissions.
*** Info: On the other hand, StrictModes don't work well with default
*** Info: Windows permissions of a home directory mounted with the
*** Info: 'noacl' option, and they don't work at all if the home
*** Info: directory is on a FAT or FAT32 partition.
*** Query: Should StrictModes be used? (yes/no) no
*** Info: Updating /etc/sshd_config file

*** Query: Do you want to install sshd as a service?
*** Query: (Say "no" if it is already installed as a service) (yes/no) yes
*** Query: Enter the value of CYGWIN for the daemon: [] ntsec
*** Info: On Windows Server 2003, Windows Vista, and above, the
*** Info: SYSTEM account cannot setuid to other users -- a capability
*** Info: sshd requires. You need to have or to create a privileged
*** Info: account. This script will help you do so.

*** Info: It's not possible to use the LocalSystem account for services
*** Info: that can change the user id without an explicit password
*** Info: (such as passwordless logins [e.g. public key authentication]
*** Info: via sshd) when having to create the user token from scratch.
*** Info: For more information on this requirement, see
*** Info: https://cygwin.com/cygwin-ug-net/ntsec.html#ntsec-nopasswd1

*** Info: If you want to enable that functionality, it's required to create
*** Info: a new account with special privileges (unless such an account
*** Info: already exists). This account is then used to run these special
*** Info: servers.

*** Info: Note that creating a new user requires that the current account
*** Info: have Administrator privileges itself.

*** Info: No privileged account could be found.

*** Info: This script plans to use 'cyg_server'.
*** Info: 'cyg_server' will only be used by registered services.
*** Query: Do you want to use a different name? (yes/no) no
*** Query: Create new privileged user account 'local_address\cyg_server'
*** Query: (Cygwin name: 'cyg_server')? (yes/no) yes
*** Info: Please enter a password for new user cyg_server. Please be sure
*** Info: that this password matches the password rules given on your system.
*** Info: Entering no password will exit the configuration.
*** Query: Please enter the password:password
*** Query: Reenter:password

*** Info: User 'cyg_server' has been created with password 'password'.
*** Info: If you change the password, please remember also to change the
*** Info: password for the installed services which use (or will soon use)
*** Info: the 'cyg_server' account.

*** Info: The sshd service has been installed under the 'cyg_server'
*** Info: account. To start the service now, call 'net start sshd' or
*** Info: 'cygrunsrv -S sshd'. Otherwise, it will start automatically
*** Info: after the next reboot.

*** Info: Host configuration finished. Have fun!
```

2. Start the **sshd** service:

- Open a command prompt window.
- Enter **net start sshd** or in a Bash prompt, enter **cygrunsrv -S sshd**.
- Verify that the daemon is running.
- Enter **ps -a**. Examine the output to see if /usr/sbin/sshd is contained in the list of running processes.

To stop the service from a Windows command prompt, enter **net stop sshd**. Alternatively, you can change to the C:\cygwin\bin directory (or open a Bash shell) and enter **cygrunsrv -E sshd**.

3. When you have started the **sshd** service, test it by entering the following command from a Bash shell prompt:

```
ssh localhost
or
ssh host_name
```

If **localhost** does not work, use the short host name. If you receive a message indicating that the authenticity of localhost cannot be established, answer **Yes** to the question "Are you sure you want to continue connecting?" When prompted for your account password on **localhost**, enter the password you use when logging in to the computer.

4. Set the TEMP environment variable. For information about setting the environment variable, see <http://www.cygwin.com/cygwin-ug-net/setup-env.html>.

Here is an example of setting the environment variable:

- a. Click **My Computer > Properties > Advanced > Environment Variables**.
- b. Under **System variables**, find out the value of TEMP. For example, "C:\WINNT\TEMP"
- c. Set the TEMP environment variable to point to the Cygwin format of TEMP in the ~/ .bashrc file. For example run the following command:

```
export TEMP=/cygdrive/c/WINNT/temp
```

Uncomment and modify this line in the ~/ .bashrc file from the default:

```
# export TEMP=/tmp
to
export TEMP=/cygdrive/c/WINNT/temp
```

The Cygwin **sshd** service must be added as a service that starts automatically. To verify this step, click **Start > Settings > Control Panel > Administrative Tools > Services**. Look for **CYGWIN sshd** in the name list. Verify that it is started and configured to start automatically.

Creating the certificate

To create a certificate for SSH protocol, complete the following steps:

1. Run this command:

```
cd ~/.ssh
```

2. Generate the public and private keys with a passphrase. The passphrase is required.

From the Bash shell prompt, here is an example of the input and output (user responses are in boldface type):

```

Administrator ~/.ssh
$ openssl genrsa -des3 -out key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (0x10001)
Enter pass phrase for key:passphrase
Verifying - Enter pass phrase for key:passphrase

Administrator ~/.ssh
$ chmod 600 ~/.ssh/key
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/Administrator/.ssh/id_rsa): key_pairs
Enter passphrase (empty for no passphrase):passphrase
Enter same passphrase again:passphrase
Your identification has been saved in key_pairs.
Your public key has been saved in key_pairs.pub.
The key fingerprint is:
SHA256:ew00cta24Qw917tRqPcn9hETlRakksKcTgGrPkh4UZs Sheila@IBM243-PC0CJ5EF
The key's randomart image is:
+---[RSA 2048]-----+
|  . . . . .o+ |
|  . o + o . .o. |
|  . E . * o . . |
|  . . . oo. . . . |
|  . o .. S.B . oo. |
|  o o + O B . oo |
|  . o . * o + . |
|  . . . .o+o |
|  . . . .o+ |
+---[SHA256]-----+
Administrator ~/.ssh
$ cat id_rsa.pub >> authorized_keys
$

```

3. Copy the id_rsa (private key) to the IBM Spectrum Control server.
4. To connect to the remote system by using the private key, enter the following information in the GUI, when you install the Storage Resource agent:
 - User
 - Certificate Location (c:\keys\id_rsa)
 - Passphrase

Replacing default SSL certificates with custom certificates

IBM Spectrum Control provides default SSL certificates for communication between the Data server and Storage Resource agent. You can replace the default certificates with your own custom certificates.

Overview of replacing a default certificate for SSL protocol

IBM Spectrum Control uses SSL certificates for communication between the Data server and Storage Resource agents. IBM Spectrum Control provides default SSL certificates for this communication. If you want to use your own certificates, you can replace the default certificates with your custom certificates

Server certificate

The IBM Spectrum Control Data server uses the TPCDataServer.jks and server.pwd files for communication with the Storage Resource agents. If you are using custom certificates, you must replace these files.

Storage Resource agent certificate

The Storage Resource agent uses the certificate files sra.pem and sra.pwd for communication with the Data server. These two files are compressed into the certs.zip file on the server system for deployment purposes. If you are using custom certificates, you must replace these files.

There are two ways you can replace the certificates:

- Before deployment of the agent

- After deployment of the agent

These are the general steps for replacing default certificates:

1. Generate the custom certificates.
2. Stop the Data server (and the Storage Resource agent, if the agent is already deployed).
3. Replace the custom certificates on the Data server and Storage Resource agent or on the product electronic installation image or the Storage Resource Agent installation image.
4. Start the Data server (and the Storage Resource agent, if the agent is already deployed).

Note: When you generate custom SSL certificates, the certificates have a start date, end date, and time when they are valid. These dates and times are related to the system where these custom certificates were generated (which is usually the server system). When you install a Storage Resource agent on a remote system, you must check the date and time on the Storage Resource agent system. If the server and agent systems are in the same time zone, they must have the same date and time. Otherwise, the time zone difference should be set.

For example, if the server system is 8:00 PM, the agent system should also be 8:00 PM. If the agent system is set at a different time (for example, 6:00 PM) at the time the SSL custom certificates are generated on the server system with a time of 8:00 PM, the deployment of the Storage Resource agent fails.

How to generate custom certificates

The script file `createSRACerts.sh` (for Linux or UNIX) or `createSRACerts.bat` (for Windows) is in the following directory:

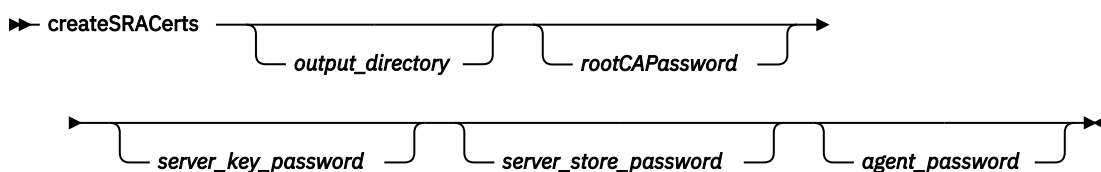
```
installation_dir/data/sra/tools/certs
```

Where *installation_dir* is the directory where the IBM Spectrum Control servers are installed. The default directory is `/opt/IBM/TPC` for Linux or UNIX or `C:\Program Files\IBM\TPC` for Windows.

To generate custom certificates, follow these steps:

1. Create the custom certificates.

The `createSRACerts` script creates the custom certificates. The syntax is:



output_directory

Directory where the certificates are created.

rootCAPassword

Root CA password (root common authority password). The default non-encrypted password is: `s5umEvApR6cafruhustu`.

server_key_password

Server key password. The default non-encrypted password is: `drUtahaswefraf9uth`.

server_store_password

Server store password. The default non-encrypted password is: `wr4d5Xekaqafehet5u2a`.

agent_password

Agent password. The default non-encrypted password is: `jawUchezuthew6azEjef`.

Note: You are prompted for the password when the script is run. Provide the value of the `rootCAPassword` on the command line (if specified on the command line). Otherwise, use the default values in the `createSRACerts.sh` or `createSRACerts.bat` script when prompted for the password (twice).

The following example creates the SSL certificate by using the default output directory and default passwords.

```
createSRACerts
```

The following examples create the SSL certificates by using the directory /tmp on UNIX and C:\temp on Windows. These examples use the default passwords. The certificate files are created in the following directory:

Windows

```
C:\temp\sra_certs_out
```

Here is an example:

```
createSRACerts C:\temp
```

UNIX or Linux

```
/tmp/sra_certs_out
```

Here is an example:

```
./createSRACerts.sh /tmp
```

The following examples create SSL certificates in the directory /tmp on UNIX and C:\temp on Windows. These examples use non-default passwords for root CA and server key. The certificate files are created in the following directory:

Windows

```
C:\temp\sra_certs_out
```

Here is an example of creating a non-default password for the root CA password and server key password:

```
createSRACerts C:\temp newpasswordforrootCA newpasswordforserver
```

UNIX or Linux

```
/tmp/sra_certs_out
```

Here is an example of creating a non-default password for the root CA password and server key password:

```
createSRACerts.sh /tmp newpasswordforrootCA newpasswordforserver
```

2. Regenerate the certificates again if you have a failure. Delete the files in the output directory before you rerun the createSRACerts script.
 3. Stop the Storage Resource Agents (if any are deployed and running) and the Data Server. To remotely stop agents from the Data or Storage Resource agents table, complete one of the following steps:
 - For Storage Resource agents that are running as a daemon service, in the **Select Action** menu, select **Shutdown**. For Storage Resource agents that are running as non-daemon agents, you do not need to stop the agent. Non-daemon processes do not need to be started or stopped.
- Note:** For Storage Resource agents that are running as a non-daemon service, search the IBM Spectrum Control product documentation for *agent.sh command*.
- At the command prompt, enter the following command:

```
"Storage_Resource_Agent_installation_directory/agent/bin/agent.[sh|bat] stop"
```

This command must be run locally on each system where an agent is running. On the Linux and UNIX operating systems, enter the `agent.sh` command, and on the Windows operating system, enter the `agent.bat` command.

For more information about starting or stopping IBM Spectrum Control services, see [“Starting and stopping the IBM Spectrum Control servers” on page 88](#).

4. Replace the certificates. There are four scenarios:

- Replacing the certificates after the server is installed.
- Replacing the certificates after the agent is installed.
- Replacing the certificates before the agent is locally.

Replacing the certificates after the server is installed

The new server certificates are created in the following directory:

```
output_directory/sra_certs_out/server
```

By default `output_directory` is the directory where the `createSRACerts` script is run:

```
installation_dir/data/sra/tools/certs
```

These files are the server certificate files:

```
TPCDataServer.jks  
server.pwd
```

For the server certificate, copy the server certificate files to the following directory:

```
installation_dir/data/sra/certs
```

The server certificate files are created in the `certs.zip` file in the following directory:

```
output_directory/sra_certs_out/agent
```

Copy the `certs.zip` file into each agent directory:

```
installation_dir/data/sra/agent_operating_system
```

```
installation_dir/data/sra/server_operating_system
```

Extract the `certs.zip` file into the following directory:

```
installation_dir/data/sra/server_operating_system
```

`agent_operating_system` is the operating system of an agent that is remotely deployed.
`server_operating_system` is the operating system on which the Data server is installed.

Replacing the certificates after the agent is installed

The new agent certificates were created on the server in the following directory:

```
output_directory/sra_certs_out/agent
```

By default, `output_directory` is:

```
installation_dir/data/sra/tools/certs
```

You must copy the `certs.zip` file to the agent system before you extract it in the `storage_resource_agent_install_directory/certs` directory. The Storage Resource agent is installed in the `storage_resource_agent_install_directory`.

Replacing the certificates before the agent is installed locally

Restriction: This process assumes that the Storage Resource agent disk image can be modified. You must copy the installation files to a writable location before proceeding.

Before the agent can be installed locally, the custom certificate must be copied to the agent system. Copy the `certs.zip` Storage Resource agent certificate file from the `output_directory/sra_certs_out/agent` directory on the IBM Spectrum Control server to the agent system.

By default, the `output_directory` is where the `createSRACerts` script was run. An example of this directory path is:

```
installation_dir/data/sra/tools/certs/
```

- a. On the agent system, extract the Storage Resource agent installation image in the `SRA_image_install_directory`.
- b. Extract the custom `certs.zip` file in the following directory:

```
storage_resource_agent_install_directory/agent/certs
```

directory.

Note: `SRA_image_install_directory` is the directory where the Storage Resource agent image was extracted. `agent_operating_system` is the directory that is named for the operating system where the agent is installed.

- c. Install the Storage Resource agent with the wanted option.
5. Start the Data server and the Storage Resource agent. If the Data server is stopped for replacement of the certificates, start the Data server after the replacement of the certificates.

If the Storage Resource agent is stopped for replacement of certificates, start the Storage Resource agent after the replacement of the certificates.

Configuration guidelines for 500 or more agents

You can use this information to help you manage 500 or more Storage Resource agents in IBM Spectrum Control.

If you have 500 or more Storage Resource agents communicating with IBM Spectrum Control, complete the following steps:

1. Probe the servers at least once a day or more, depending on when you want to test for alert conditions.
2. Set the following parameters in the `server.config` file:

MaxConnections=1200

The default is 500. Agents can have multiple connections to the server.

routerThreads=3 (max)

Incoming connections need to be routed to the correct Data Manager "service" queue and can stack up behind this thread. The server service runs the router and the agent service is where the connections are queued once routed and saved by any of three threads here to the repository.

3. Set the following parameter in the `Scheduler.config` file:

MaxSubmitthreads=8

Tells how many threads are used to tell the agents to start a job. Agent connections can queue up the scheduler service. After a job is run, the agent makes a connection to communicate with this thread to give it the job status.

Including a Storage Resource agent with a server master image

If you use a master operating system image to deploy new servers in your environment, you can include the Storage Resource agent on that master image. The master image enables the agents to start and register with the IBM Spectrum Control server automatically upon deployment. This support applies only to Storage Resource agents running in daemon mode.

The default agent directory is:

- For Windows: C:\Program Files\IBM\TPC\agent
- For UNIX: /opt/IBM/TPC/agent

Follow these instructions to include the IBM Spectrum Control agent on a master image.

1. Install the Storage Resource agent in daemon mode on the master image system.
2. Stop the Storage Resource agent on the master image system.

For the Windows system: Click **Start > Settings > Control Panel > Administrative Tools > Services**. Stop the following service: **IBM Spectrum Control Storage Resource Agent - *directory***. *directory* is where the Storage Resource agent is installed. The default directory is `installation_dir\agent`.

For the UNIX or Linux system, run the following commands:

```
cd /opt/IBM/TPC/agent/bin/  
./agent.sh stop
```

3. Create one of the following files in the root directory for the agent. These files can be empty. Any content in these files is ignored.

REGISTERSRA

The file name must be uppercase with no file extension. This file causes the agent to run a probe and then register with the server. This file will use the existing Globally Unique Identifier (GUID).

REGISTERSRA_REGENGUID

The file name must be uppercase with no file extension. This file causes the agent to regenerate a new Globally Unique Identifier (GUID), run a probe, and then register with the server.

4. Delete the contents of the `agent_installation_directory/logs` directory. This clears any existing log messages so that you can view new messages that are logged.
5. Create the master image copies of this system.
6. When a new system is preinstalled from this image and then started, the REGISTERSRA or REGISTERSRA_REGENGUID file is run. The Storage Resource agent automatically registers with the new IBM Spectrum Control server. You can then use the GUI to manage the Storage Resource agent deployment. For example, to confirm that the Storage Resource agent was deployed successfully, go to the **Servers** page and refresh the list.

Configuring LUN provisioning for Oracle Solaris

Tivoli Storage Productivity Center for Data provides a file system extension feature that can be used to automatically increase file system capacity for managed hosts when utilization reaches a specified level. This function allows for the automatic provisioning of (TotalStorage Enterprise Storage Server®, DS6000™, DS8000) LUNs when there is not enough space available in a volume group to extend a file system. There is also information about LUN provisioning for Solaris.

LUNs can be provisioned for file system hosts that run Solaris, but you must configure the hosts must to avoid a restart after provisioning. Before you install the Storage Resource agent, complete the following steps:

1. Assign TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUNs to Solaris Host Bus Adapters (HBAs).
2. Modify the HBA configuration file to include persistent name binding.

3. Modify the SCSI Disk configuration file to allow the maximum number of LUNs.
4. If you are using multipathing, ensure that TotalStorage Enterprise Storage Server, DS6000, or DS8000 multipaths are detected by the Veritas Dynamic Multipathing (VxDMP) utility.

This section provides basic instructions for performing these configuration steps. For detailed information, see the HBA and VxDMP documentation.

Assigning TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUNs to Oracle Solaris HBAs

This section provides information about assigning TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUNs to Solaris HBAs.

You must assign at least one TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUN to each HBA on the Solaris host.

If you are using multipathing, there are different ways to configure either the host and TotalStorage Enterprise Storage Server, DS6000, or DS8000. For example:

- For an TotalStorage Enterprise Storage Server, DS6000, or DS8000 without internal multipath configuration, assign the same LUNs to the World Wide Port Node (WWPN) of each HBA.
- For an TotalStorage Enterprise Storage Server, DS6000, or DS8000 with internal multipath configuration, assign the LUNs to the WWPN of one HBA or assign the same LUNs to the WWPNs of two or more HBAs.

Modifying the HBA configuration file

The HBA configuration file must be modified to include Persistent Name Binding on HBAs and targets so that both the controller and target numbers remain the same across system reboots. This section provides information about what to modify in the configuration file.

The HBA configuration file (for example, `qla2200.conf`) must be modified to include Persistent Name Binding on HBAs and targets so that both the controller and target numbers remain the same across system reboots. You must reboot the system with the new configuration for the changes to take effect.

QLogic QLA2200 and QLA2300 HBAs have been tested for use with IBM Spectrum Control. You can use the QLogic SANblade Control FX (**scfx**) application to modify the configuration file for these HBAs. The **scfx** application is included as part of the device driver installation package. The **scfx** application is installed in the `/opt/QLogic_Corporation/SANblade_Control_FX` directory.

To configure newer models of the QLogic HBAs, use the QLogic SANSurfer software, which is included with the device driver installation package for newer QLogic models. Consult the QLogic support documentation to be sure you are using the appropriate configuration software.

Setting Persistent Name Binding for QLogic HBAs by using the appropriate software

This section describes how to set Persistent Name Binding in the HBAs by using the **scfx** command for LUN provisioning under Oracle Solaris. To configure newer models of the QLogic HBAs, use the QLogic SANSurfer software, which is included with the device driver installation package for newer QLogic models. Consult the QLogic support documentation to be sure you are using the appropriate configuration software.

Follow these steps:

1. Install the QLogic HBA Driver, Common API Library, and QLogic SANblade Control FX (**scfx**) application if you have not already done so. For installation instructions, see the *SANblade 2200 Series User's Guide* or *SANblade 2300 Series User's Guide*. After these packages are installed successfully, restart and reconfigure the system by using the **reboot -- -rv** command.
2. After the system is rebooted, use **scfx** to configure Persistent Bind on HBAs and Targets in the `/kernel/drv/qla2xxx.conf` file.

- a. Start the **scfx** application. For example:

```
# /opt/QLogic_Corporation/SANblade_Control_FX/scfx
```

The main window of the **scfx** application consists of three sections:

Menu Bar

The menu bar provides three options: **File**, **Tools**, and **Help**.

HBA Tree

The HBA Tree displays the host with its connected adapters (HBAs), devices and LUNs. The HBAs are displayed with a model name and instance number. For example, Adapter 2200 (Instance #0). If a device is connected to an HBA, it has a plus sign (+) by the HBA, which can be expanded to view the list of attached devices. The devices are listed with their World Wide Port Names (WWPN).

Click the plus sign next to a device to expand the tree to show all the LUNs in that device. For a RAID device, such as an TotalStorage Enterprise Storage Server, DS6000, or DS8000, there are multiple LUNs per device.

Note: Expand all the devices to search the TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUNs assigned to the system and note the WWPN of the target device. This information is required to identify the SCSI Target ID assigned or specified for the Persistent Bind Targets Setting.

Tabbed Pages

The contents of the Tabbed Pages changes depending on what is currently selected in the HBA Tree.

- b. Select an HBA.

Select an adapter in the HBA Tree. The Tabbed Pages show the **HBA Information**, **HBA Options**, **Target Settings**, **Boot Device**, **Diagnostics**, and **Utilities** tabs.

- c. Select the Persistent Bind HBA Setting.

Click the **HBA Options** tab. In the **Select Parameter Section** drop-down list, select **Advanced Host Parameters**. Select the check box for **Persistent Bind HBA**. Click **Save**.

- d. Select the Persistent Bind Target Setting.

Click the **Target Settings** tab. Select the check box for each target in the **Bind** column. If the check boxes are already checked and disabled, proceed to the next step. In the **Target ID** column, you can either accept the pre-selected SCSI Target ID or change to a different value. Each SCSI target ID must be unique and range from 0 to 255.

Note: Write down the selected Target ID for each TotalStorage Enterprise Storage Server subsystem device.

Click **Save**.

- e. Repeat Steps b through d for the next HBA.

- f. Exit the **scfx** application.

From the **Menu Bar**, select **File | Exit**. A Reboot Reminder dialog is displayed. Click **OK** to exit.

3. Restart and reconfigure the system by using the **reboot -- -rv** command.

Modifying the SCSI disk configuration file

You must configure the SCSI disk configuration file for the maximum number of LUNs per target for LUN provisioning for Oracle Solaris.

You must configure the SCSI disk (sd.conf) configuration file for the maximum number of LUNs (256) per target. The system must then be rebooted with the new configuration for the changes to take effect. Follow these steps:

1. Identify the SCSI Target ID assigned to the TotalStorage Enterprise Storage Server.

2. Edit the `/kernel/drv/sd.conf` file to include all the possible target and LUN mappings for the RAID device.

For example, assume the SCSI Target ID assigned for an TotalStorage Enterprise Storage Server is 2. You can allow up to 256 LUNs (0 - 255) for this target:

```
name="sd" class="scsi" target=0 lun=0;
name="sd" class="scsi" target=1 lun=0;
name="sd" class="scsi" target=2 lun=0;
name="sd" class="scsi" target=2 lun=1;
name="sd" class="scsi" target=2 lun=2;
:
:
name="sd" class="scsi" target=2 lun=253;
name="sd" class="scsi" target=2 lun=254;
name="sd" class="scsi" target=2 lun=255;
name="sd" class="scsi" target=3 lun=0;
name="sd" class="scsi" target=4 lun=0;
:
:
name="sd" class="scsi" target=253 lun=0;
name="sd" class="scsi" target=254 lun=0;
name="sd" class="scsi" target=255 lun=0;
```

In this example, the system can detect up to 256 targets with 1 LUN (for example, multiple RAID devices with a total of 256 LUNs) and up to 256 LUNs for target 2 (for example, a RAID device with a total of 256 LUNs).

3. Restart and reconfigure the system by using the **reboot -- -rv** command.

Checking for TotalStorage Enterprise Storage Server, DS6000, or DS8000 multipaths in VxDMP

If you are using IBM TotalStorage Enterprise Storage Server, DS6000, or DS8000 LUNs with multipaths, you must ensure that all the paths are detected by Veritas Dynamic Multipathing (VxDMP) utility. This section provides information about how to check for multipathing in the VxDMP utility.

The VxDMP utility is an administrative interface to the Veritas Volume Manager (VxVM) Dynamic Multipathing (DMP) facility. It lists the paths under a DMP device, gets the DMP device corresponding to a path, lists all the disk controllers on the system, lists all the paths through a host disk controller, lists all the DMP nodes through a disk array, and enables or disables a host disk controller on the system. For more information, and detailed instructions, see the VxDMP documentation.

To list all disk controllers on the system, enter the following command:

```
# vxdmpadm listctlr all
```

The following sample output shows that controllers c3 and c4 are connected to the IBM TotalStorage Enterprise Storage Server with an Enclosure Type of IBM_SHARK and an Enclosure Name of IBM_SHARK0.

CTLR-NAME	ENCLR-TYPE	STATE	ENCLR-NAME
c1	Disk	ENABLED	Disk
c3	IBM_SHARK	ENABLED	IBM_SHARK0
c4	IBM_SHARK	ENABLED	IBM_SHARK0

To list all subpaths for controller c3, enter the following command:

```
# vxdmpadm getsubpaths ctlr=c3
```

The following sample output shows that the **DMPNODENAME** is the same as the device name for each TotalStorage Enterprise Storage Server LUN:

NAME	STATE	PATH-TYPE	DMPNODENAME	ENCLR-TYPE	ENCLR-NAME
c3t4d0s2	ENABLED	-	c3t4d0s2	IBM_SHARK	IBM_SHARK0
c3t4d1s2	ENABLED	-	c3t4d1s2	IBM_SHARK	IBM_SHARK0

To list all subpaths for controller c4, enter the following command:

```
# vxddmpadm getsubpaths ctrlr=c4
```

The following sample output shows that the **DMPNODENAME** for each TotalStorage Enterprise Storage Server LUN is from controller c3. This means that VxDMP refers to the TotalStorage Enterprise Storage Server, DS6000 or DS8000 LUNs as devices from controller c3 and mask devices on controller c4 from VxVM:

NAME	STATE	PATH-TYPE	DMPNODENAME	ENCLR-TYPE	ENCLR-NAME
c4t4d0s2	ENABLED	-	c3t4d0s2	IBM_SHARK	IBM_SHARK0
c4t4d1s2	ENABLED	-	c3t4d1s2	IBM_SHARK	IBM_SHARK0

Checking for a fully qualified host name

IBM Spectrum Control requires fully qualified host names. Some machines might be configured to return a short host name, such as `system1` instead of a fully qualified host name, such as `system1.tpc.example.com`. This topic provides information on how to check for a fully qualified host name.

Checking for a fully qualified host name for AIX systems

This topic provides information on how to verify a fully qualified host name for AIX.

The default domain name search order is as follows:

1. Domain Name System (DNS) server
2. Network Information Service (NIS)
3. Local `/etc/hosts` file.

If the `/etc/resolv.conf` file does not exist, the `/etc/hosts` file is used. If only the `/etc/hosts` file is used, the fully qualified computer name must be the first one that is listed after the IP address.

Verify that the `/etc/resolv.conf` file exists and contains the appropriate information, such as:

```
domain mydivision.mycompany.com
nameserver 123.123.123.123
```

If NIS is installed, the `/etc/irs.conf` file overrides the system default. It contains the following information:

```
hosts = bind,local
```

The `/etc/netsvc.conf` file, if it exists, overrides the `/etc/irs.conf` file and the system default. It contains the following information:

```
hosts = bind,local
```

If the `NSORDER` environment variable is set, it overrides all of the preceding files. It contains the following information:

```
export NSORDER=bind,local
```

Checking for a fully qualified host name for Linux systems

This topic provides information on how to verify a fully qualified host name for Linux.

Linux uses a resolver library to obtain the IP address corresponding to a host name. The `/etc/host.conf` file specifies how names are resolved. The entries in the `/etc/host.conf` file tell the

resolver library what services to use, and in what order, to resolve names. Edit the `host.conf` file using the **vi** editor to add the following lines:

```
# Lookup names through DNS first then fall back to /etc/hosts.
order bind,hosts
# Machines with multiple IP addresses.
multi on
# Check for IP address spoofing.
nospoof on
```

The **order** option indicates the order of services. The sample entry specifies that the resolver library should first consult the name server to resolve a name and then check the `/etc/hosts` file. It is recommended to set the resolver library to first check the name server, `bind` file, and then the `hosts` file (`hosts`) for better performance and security on all your servers. You must have the DNS and BIND software installed for this configuration to work.

The **multi** option determines whether a host in the `/etc/hosts` file can have multiple IP addresses. Hosts that have more than one IP address are said to be multihomed, because the presence of multiple IP addresses implies that the host has several network interfaces.

The **nospoof** option takes care of not permitting spoofing on this machine. IP-Spoofing is a security exploit that works by tricking computers into a trust relationship that you are someone that you really are not. In this type of attack, a machine is set up to look like a legitimate server and then issue connections and other types of network activities to legitimize end systems, other servers, or large data repository systems. This option must be set ON for all types of servers.

Checking for a fully qualified host name for Oracle Solaris

This topic provides information about how to verify a fully qualified host name for Oracle Solaris systems.

Verify that the `/etc/resolv.conf` file exists and contains the appropriate information, such as:

```
domain mydivision.mycompany.com
nameserver 123.123.123.123
```

A short name is used if the `/etc/nsswitch.conf` file contains a line that begins as follows and if the `/etc/hosts` file contains the short name for the computer:

```
hosts: files
```

To correct this problem, follow these steps:

1. Change the line in the `/etc/nsswitch.conf` file to the following:

```
hosts: dns nis files
```

2. Enter the following command to stop the **inet** service:

```
/etc/init.d/inetd stop
```

3. Enter the following command to restart the **inet** service:

```
/etc/init.d/inetd start
```

Checking for a fully qualified host name for Windows systems

Verify the fully qualified host name on Windows operating systems.

1. Choose one of these options:

Option	Description
Windows Server 2012	<ol style="list-style-type: none">a. On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start.b. Click Control Panel, and then click System.

Option	Description
	c. Click Change Settings , click Change , and then click Change again.
Windows 7, Windows 2008	a. Click Start > Control Panel > System and Security . b. Click System , and then click Change Settings . c. On the Computer Name tab, click Change .
Windows XP, Windows Vista	a. On the desktop, right-click My Computer , and then click Properties . b. On the Computer Name tab, click Change . .

2. In the **Computer name** field, enter the fully qualified host name, and then click **More**.
3. Verify that the **Primary DNS suffix** field contains a domain name, and then click **OK**.

Importing authentication information for a Storage Resource agent

The Storage Resource agent is installed as a non-daemon or daemon process. IBM Spectrum Control stores the authentication information to connect to the host on which the Storage Resource agent has installed for the non-daemon agent. This authentication information can be changed depending on the environment.

To change the authentication information for a Storage Resource agent for non-daemon service, follow these steps:

1. Export the authentication information for a Storage Resource agent.
2. The data file exported contains information such as the host name, user ID, password, certificate location, and passphrase for every agent selected. The information is separated by the pipe character (|). For example,

```
agent_host|user|password|certificate|passphrase
```

You can update the password or passphrase in encrypted format or plain text format. If you want to update the password or passphrase in encrypted format, then you can use the **tpctool**. For example, go to this directory and run the **tpctool**:

```
cd installation_dir/cli
tpctool encrypt string_to_be_encrypted
```

This generates an encrypted string. Place this string in the data file to be imported and add @ENC@ to the end of the encrypted string. For example,

```
agent_host|usera|encrypted_password@ENC@|certificate|
encrypted_passphrase@ENC@
```

encrypted_password is the encrypted string for the password and *encrypted_passphrase* is the encrypted string for the passphrase.

3. Import the data file.

Installing and configuring the IBM Spectrum Control server with multiple NIC cards

If your IBM Spectrum Control server has multiple network interface cards (NIC), install the IBM Spectrum Control server using a fully qualified hostname that resolves to the IP address of NIC card you want to use. After you install the server, all incoming and outgoing communication are successfully handled.

Installing IBM Spectrum Control for a multiple network configuration

If the IBM Spectrum Control server you are installing has multiple NIC, and is configured to use multiple network addresses, ensure that you use the fully qualified hostname that resolves to the appropriate IP address during installation. You can either setup the HOSTS file or the DNS to resolve the fully qualified host names to appropriate IP addresses.

Outgoing communication initiated by the IBM Spectrum Control server

All the outgoing communication that is initiated by the IBM Spectrum Control server is not affected if the server is configured for a multiple network environment.

For example, if you have a IBM Spectrum Control server with two IP addresses: 10.10.10.11 and 9.9.9.10, and 10.10.10.11 is used during installation, all outgoing transmissions can be sent to the devices and agents in both networks.

The following list includes examples of outgoing communication that is initiated by the IBM Spectrum Control server:

Storage systems using native interfaces

Run probe, performance monitor, and provisioning. Examples of storage systems that use the native interface include SAN Volume Controller, Storwize V7000 Unified, Storwize V7000, and XIV system.

Switches (SNMP and SMIS-S providers)

Run SNMP and SMI-S provider probes.

SMI-S providers

IBM Spectrum Control uses SMI-S providers (CIM agents) for the managed objects to gather information about the resource.

VMware vCenter

Run probes.

Agents (Storage Resource agents)

Deploy agents, run data collection, and run scripts.

IBM Spectrum Control servers

Run data collection.

Incoming communication that is initiated by the resources, agents, and GUI

Incoming communication that is initiated by the resources or agents can work with only the IP address that is specified during the installation with the exception of DS8000 events.

For DS8000 events, the IBM Spectrum Control server must initiate and establish a socket connection directly with the Hardware Management Console (HMC) to receive events. The DS8000 HMC uses that socket connection to send events. As long as the IBM Spectrum Control server can initiate the communication to the HMC, DS8000 events can be received.

IBM Spectrum Control informs resources and agents to initiate communication to the IP address provided during the installation. This example uses the IP address 10.10.10.11. However, depending on the communication, you might be able to change the IP address. For example, IBM Spectrum Control does not configure SAN switches to send SNMP traps to IBM Spectrum Control, so you can use either 9.9.9.10 or 10.10.10.11.

The following list includes examples of incoming communication that are initiated by the resources, agents, and the GUI:

DS8000 events

Events sent by the HMC to the IBM Spectrum Control server

SNMP trap notifications

SNMP traps sent from the switches and other resources

CIM indications

Indications sent by the SMI-S providers (CIM agents).

Servers (agents)

Job results and registration

IBM Spectrum Control GUI

Any request.

CIM indications

A CIM indication is an event that occurs on a managed object, for example, the completion or failure of an operation. The CIM indications are managed by the CIM object manager. IBM Spectrum Control uses the SMI-S providers for the managed objects to gather information about the resource.

Manually customize CIM indications on a IBM Spectrum Control system that has multiple IP addresses. To configure IBM Spectrum Control to receive CIM indications in an IPv4, IPv6, and dual stack (IPv4 and IPv6) environment, see [“Configuring IBM Spectrum Control with multiple IP addresses” on page 26](#).

The manual customization task does not apply to storage devices that use the native interfaces.

Creating an SSH certificate for the root user ID

You can create a Secure Shell (SSH) certificate for authentication for the Virtual I/O Server. Follow the certificate-generation instructions. However, if you want to use Telnet to connect to the Virtual I/O Server using the padmin user ID, you must follow this procedure.

To create an SSH certificate using the padmin user ID, follow these steps:

1. Telnet to the remote system using the padmin user ID.
2. Set up the AIX environment. Run the following command:

```
oem_setup_env
```

3. Change to the following / .ssh directory.
4. Enter **ssh-keygen**. Accept the default names (for example, id_rsa).
5. Enter the passphrase. Two new files are created:

id_rsa

This is the private key.

id_rsa.pub

This is the public key.

6. Create an authorized_key file in the same location as the id_rsa . pub file. Enter the following command:

```
cat >> id_rsa.pub >> authorized_keys
```

The following example shows the command input and output (the commands are in bold):

```
# ssh-keygen

Generating public/private rsa key pair.
Enter file in which to save the key (//.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been save in //.ssh/id_rsa.
Your public key has been save in //.ssh/id_rsa.pub.
The key fingerprint is:
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx root@<server>

# cat id_rsa >> authorized_keys

# ls -l

-rw-r--r- 1 root system 1743 Oct 15 09:40 authorized_keys
-rw--- 1 root system 1743 Oct 15 09:39 id_rsa
-rw-r--r- 1 root system 399 Oct 15 09:39 id_rsa.pub
```

7. Copy the `id_rsa` (private key) to your server machine.

Note: You must copy the file in binary mode.

8. To connect to the remote system by using the private key, enter the following information in the web-based GUI when you install the Storage Resource agent:

- User
- Certificate Location (c:\keys\id_rsa)
- Passphrase

Replacing the default SSL certificate for the Device, Alert, or Web server

To replace the default SSL certificate for the Device, Alert, or Web server, use the IBM Key Management (iKeyman) utility.

If you have strong security requirements, you might want to replace the default certificate for the Web server so that you can securely connect to the Web server while you use the `https` protocol. When you replace the existing certificate, it can remove web browser certificate error warnings.

1. Log on to the server where IBM Spectrum Control is installed. Ensure that you log on with the appropriate user privileges.
2. Open the `/jre/bin` directory where IBM Spectrum Control is installed.
3. Enter the iKeyman utility command.

For Windows operating system, enter the following command:

```
ikeyman.exe
```

For AIX or Linux operating system, enter the following command:

```
./ikeyman
```

4. Click **Key Database File > Open**.

5. Complete the following tasks:

- a. Set the Key database type to **PKCS12**.
- b. In the **File Name** field, click **Browse**.

To replace the default SSL certificate for the Device server, go to the `installation_dir/wlp/usr/servers/deviceServer/resources/security/` directory, select the key `.p12` file, and click **Open**.

To replace the default SSL certificate for the Alert server, go to the `installation_dir/wlp/usr/servers/alertServer/resources/security/` directory, select the key `.p12` file, and click **Open**.

To replace the default SSL certificate for the Web server, go to the *installation_dir/wlp/usr/servers/webServer/resources/security/* directory, select the key .p12 file, and click **Open**.

c. Click **OK**.

6. On the **Password Prompt** page, type default, and click **OK**.

The Personal Certificates list contains only the certificate with the default label.

To replace the default certificate with a new self-signed certificate, complete the following tasks:

a. Click **New Self-Signed**.

b. On the **Create New Self-Signed Certificate** page, enter a unique value in the **Key Label** field.

c. Provide values for the other fields, and click **OK**.

The list of Personal Certificates contains your new self-signed certificate and the certificate with the default label.

d. Select the certificate with the default label and click **Rename**.

e. Enter a new label for the certificate, and click **OK**.

f. Select the new certificate and click **Rename**.

g. Enter default as the new label, and click **OK**.

To replace the default certificate with a new certificate that is signed by an external certificate authority, complete the following tasks:

a. In the iKeyman utility, select **Create > New Certificate Request**.

b. Enter a unique value in the **Key Label** field and provide values for the other fields.

c. Pay special attention to the value you provide in the **Enter the name of a file in which to store the certificate request** field and click **OK**.

A message is displayed that informs you the location of the file, that contains your new certificate request. You need to send the new certificate request file to your external certificate authority.

d. On the **Message** page, click **OK**.

The external certificate authority signs your new certificate request and sends back your new certificate. The external certificate authority might send their signer certificate or the external certificate authority might assume that you already have their signer certificate in the key database file.

If the external certificate authority sends their signer certificate, complete the following tasks:

a. Select **Signer Certificates** and click **Add**.

b. Provide the **File Name** and **Location** values of the file that contains the Signer Certificate and click **OK**.

If the external certificate authority assumes that you already have their signer certificate in the key database file, complete the following tasks:

a. Select **Signer Certificates** and click **Populate**.

b. Search the lists of CA Certificates, select the one(s) for the external certificate authority that signed your new certificate request, and click **OK**.

If the lists of CA Certificates do not contain the one(s) for the external certificate authority that signed your new certificate request, ask your external certificate authority to send their signer certificate.

When you have the signer certificate for the external certificate authority that signed your new certificate request, complete the following tasks:

a. Select **Personal Certificates** and click **Receive**.

b. Provide the **File Name** and **Location** values of the file that contains your new certificate and click **OK**.

- c. Select the certificate with the default label and click **Rename**.
 - d. Enter a new label for the certificate and click **OK**.
 - e. Select your new certificate and click **Rename**.
 - f. Enter default as the new label and click **OK**.
7. In the iKeyman utility, click **Key Database File > Exit**.
 8. Stop and start the Device, Alert, or Web server.

Related tasks

[“Starting and stopping the IBM Spectrum Control servers” on page 88](#)

You can start and stop the IBM Spectrum Control servers in the GUI or by running scripts. Note: IBM Spectrum Control servers start automatically on Windows, Linux, or AIX® operating systems when the operating system is started.

Updating IBM Spectrum Control data collector trusted certificates after replacing default SSL certificate for the Device server

Use the **keytool** command to update the IBM Spectrum Control data collector trusted certificates after you replace the default SSL certificate for the IBM Spectrum Control Device server.

If you replace the default SSL certificate for the IBM Spectrum Control Device server, you must update the IBM Spectrum Control data collector trusted certificates or else the data collector does not communicate properly with the Device server.

1. Log on to the server where IBM Spectrum Control is installed. Ensure that you log on with the appropriate user privileges.
2. Stop the Device server.
3. Open the `/jre/bin` directory where IBM Spectrum Control is installed.
4. Enter the following command to export the default SSL certificate from the Device server keystore.

For Windows operating system, enter the following command:

```
keytool.exe -exportcert -alias default
-keystore "installation_dir\wlp\usr\servers\deviceServer\resources\security\key.p12" -storetype pkcs12
-storepass device_server_keystore_password -file deviceServer.cert
```

Where `device_server_keystore_password` is the Device server keystore password and the default value for this password is *default*.

For AIX or Linux operating system, enter the following command:

```
./keytool -exportcert -alias default
-keystore installation_dir/wlp/usr/servers/deviceServer/resources/security/key.p12 -storetype pkcs12
-storepass device_server_keystore_password -file deviceServer.cert
```

Where `device_server_keystore_password` is the Device server keystore password and the default value for this password is *default*.

5. Enter the following command to delete the previous IBM Spectrum Control Device server SSL certificate from the IBM Spectrum Control data collector trusted certificates.

For Windows operating system, enter the following command:

```
keytool.exe -delete -alias deviceServer -keystore "installation_dir\jre\lib\security\cacerts" -storepass
data_collector_keystore_password
```

Where `data_collector_keystore_password` is the IBM Spectrum Control data collector keystore password and the default value for this password is *changeit*.

For AIX or Linux operating system, enter the following command:

```
./keytool -delete -alias deviceServer -keystore installation_dir/jre/lib/security/cacerts
-storepass data_collector_keystore_password
```


Where *data_collector_keystore_password* is the IBM Spectrum Control data collector keystore password and the default value for this password is *changeit*.

6. Enter the following command to add the default SSL certificate from the IBM Spectrum Control Device server to the IBM Spectrum Control data collector trusted certificates.

For Windows operating system, enter the following command:

```
keytool.exe -importcert -noprompt -trustcacerts -alias deviceServer -file deviceServer.cert  
-keystore "installation_dir\jre\lib\security\cacerts" -storepass data_collector_keystore_password
```

Where *data_collector_keystore_password* is the IBM Spectrum Control data collector keystore password and the default value for this password is *changeit*.

For AIX or Linux operating system, enter the following command:

```
./keytool -importcert -noprompt -trustcacerts -alias deviceServer -file ./deviceServer.cert  
-keystore installation_dir/jre/lib/security/cacerts -storepass data_collector_keystore_password
```

Where *data_collector_keystore_password* is the IBM Spectrum Control data collector keystore password and the default value for this password is *changeit*.

7. Start the Device server.

Related tasks

[“Starting and stopping the IBM Spectrum Control servers” on page 88](#)

You can start and stop the IBM Spectrum Control servers in the GUI or by running scripts. Note: IBM Spectrum Control servers start automatically on Windows, Linux, or AIX® operating systems when the operating system is started.

Replacing the default SSL certificate for the Export server

You can replace the default SSL certificate for the Export server by adding the certificate and private key file to the appropriate directory and restarting the Export server.

The Export server is used by the Web server to generate certain types of reports. By default, the certificate for the Export server is self-signed and the corresponding private key does not have a password. However, if you have strong security requirements, you might want to replace the default certificate and the corresponding private key used by the Export server.

1. Stop the Export server.
2. If your signed certificate has an accompanying chain certificate, append the contents of the chain certificate to the bottom of your signed certificate file.
3. Place the signed certificate in the *installation_dir/export/conf/export.cert* directory.
4. Place the matching private key file in the *installation_dir/export/conf/export.key* directory.
5. If your private key file requires a password, create and place the password in the *installation_dir/export/conf/ssl.pwd* directory.
6. Start the Export server again.

Related tasks

[“Starting and stopping the IBM Spectrum Control servers” on page 88](#)

You can start and stop the IBM Spectrum Control servers in the GUI or by running scripts. Note: IBM Spectrum Control servers start automatically on Windows, Linux, or AIX® operating systems when the operating system is started.

Generating a new default self-signed SSL certificate for the Export server

You can generate a new, default self-signed SSL certificate for the Export server by using the **openssl** command.

You must have the extracted IBM Spectrum Control installation image files present on the IBM Spectrum Control server where you are going to generate a new, default self-signed SSL certificate for the Export server.

1. Log on to the server where IBM Spectrum Control is installed.
Ensure that you log on with the appropriate user privileges.
2. Stop the Export server.
3. Enter the **openssl** command to generate a new, default self-signed SSL certificate for the Export server.

For the Windows operating system, enter the following command:

```
installation_dir\data\sra\tools\openssl\openssl req
-config extracted_image_dir\scripts\export\openssl.cfg
-new -newkey rsa:2048 -x509 -nodes -keyout installation_dir\export\conf\export.key
-out installation_dir\export\conf\export.cert
-days 3650 -subj /C=us/O=ibm/OU=exportServer/CN=machine_FQDN
```

Where *installation_dir* is the location where IBM Spectrum Control is installed, *extracted_image_dir* is the location where the IBM Spectrum Control installation image is extracted, and *machine_FQDN* is the fully qualified domain name of the machine where you installed IBM Spectrum Control. For example, *myserver.mycompany.com*.

If your *installation_dir* or *extracted_image_dir* location contains spaces, use double quotes around those paths.

For example:

```
"C:\Program Files\IBM\TPC\data\sra\tools\openssl\openssl" req
-config C:\Downloads\SC-Image\SC\scripts\export\openssl.cfg
-new -newkey rsa:2048 -x509 -nodes -keyout "C:\Program Files\IBM\TPC\export\conf\export.key"
-out "C:\Program Files\IBM\TPC\export\conf\export.cert" -days 3650
-subj /C=us/O=ibm/OU=exportServer/CN=myserver.mycompany.com
```

For the AIX or Linux operating systems, enter the following command:

```
installation_dir/data/sra/tools/openssl/openssl req
-config extracted_image_dir/scripts/export/openssl.cfg
-new -newkey rsa:2048 -x509 -nodes -keyout installation_dir/export/conf/export.key
-out installation_dir/export/conf/export.cert -days 3650
-subj /C=us/O=ibm/OU=exportServer/CN=machine_FQDN
```

Where *installation_dir* is the location where IBM Spectrum Control is installed, *extracted_image_dir* is the location where the IBM Spectrum Control installation image is extracted, and *machine_FQDN* is the fully qualified domain name of the machine where you installed IBM Spectrum Control. For example, *myserver.mycompany.com*.

4. Start the Export server.

Related tasks

[“Starting and stopping the IBM Spectrum Control servers” on page 88](#)

You can start and stop the IBM Spectrum Control servers in the GUI or by running scripts. Note: IBM Spectrum Control servers start automatically on Windows, Linux, or AIX® operating systems when the operating system is started.

Enabling TLS 1.0 and 1.1 for ports

IBM Spectrum Control uses Transport Layer Security (TLS) to secure communications between IBM Spectrum Control components. Note: IBM Spectrum Control ports have TLS 1.1 and 1.0 disabled by default for increased security.

Enabling TLS 1.1 and 1.0 for IBM Spectrum Control ports

To enable TLS 1.1 and 1.0 for IBM Spectrum Control ports, update the `java.security` file (Alert, Data, Device, and Web server) and the `server.config` file (Export server).

IBM Spectrum Control ports have TLS 1.1 and 1.0 disabled by default for increased security. Therefore, IBM Spectrum Control will not be able to communicate with resources that do not support TLS 1.2. If you want to upgrade your resources to a version that supports TLS 1.2, contact your vendor. You can also re-enable TLS 1.1 and 1.0 for IBM Spectrum Control ports.

1. Stop all IBM Spectrum Control servers.
2. Open the `installation_dir/jre/lib/security/java.security` file.
3. To enable TLS 1.1 and 1.2 in the Alert, Data, Device, and Web server, remove the "TLSv1.1 ," text from the `jdk.tls.disabledAlgorithms` line.

BEFORE:

```
jdk.tls.disabledAlgorithms=MD5withRSA, DH keySize < 1024, TLSv1, TLSv1.1 , EC keySize < 224, anon, NULL
```

AFTER:

```
jdk.tls.disabledAlgorithms=MD5withRSA, DH keySize < 1024, TLSv1, EC keySize < 224, anon, NULL
```

To enable TLS 1.0, 1.1, and 1.2 in the Alert, Data, Device, and Web server, remove the "TLSv1, TLSv1.1 ," text from the `jdk.tls.disabledAlgorithms` line.

BEFORE:

```
jdk.tls.disabledAlgorithms=MD5withRSA, DH keySize < 1024, TLSv1, TLSv1.1 , EC keySize < 224, anon, NULL
```

AFTER:

```
jdk.tls.disabledAlgorithms=MD5withRSA, DH keySize < 1024, EC keySize < 224, anon, NULL
```

4. Open the `installation_dir/export/conf/server.config` file.
5. To enable only TLS 1.1 in the Export server, change the "secureProtocol" value from "TLSv1_2_method" to "TLSv1_1_method".

For example:

```
"secureProtocol": "TLSv1_1_method"
```

To enable only TLS 1.0 in the Export server, change the "secureProtocol" value from "TLSv1_2_method" to "TLSv1_method".

For example:

```
"secureProtocol": "TLSv1_method"
```

To enable TLS 1.0, 1.1, and 1.2 in the Export server, change the "secureProtocol" value from "TLSv1_2_method" to "".

For example:

```
"secureProtocol": ""
```

You cannot configure the Export server such that only TLS 1.1 and 1.2 are enabled.

6. Restart the IBM Spectrum Control servers.

Configuring Db2, AIX, and Linux for IPv6-only environment

Use this information to configure Db2, AIX, and Linux for an IPv6-only environment.

Configuring the AIX system for IPv6 only

For IPv6 support, the AIX operating system must have level TL 5300–06 installed.

To configure the AIX operating system for IPv6, complete the following steps:

1. Obtain the most recent versions of **openssh** and **openss1** packages for AIX and install them. Some older version of **openssh** does not work in an IPv6-only environment.
2. Change **sshd** (Secure Shell Daemon) on AIX system to accept IPv6 connections.
 - a. In the `/etc/ssh/sshd_config` file, uncomment the line "ListenAddress:".
 - b. Restart **sshd** with the following commands:

```
stopsrc -g ssh
startsrc -g ssh
```

- c. From another IPv6 system, verify that you contact AIX over IPv6 (by using ssh).
3. In SMIT, set the IPv4 address to 0.0.0.0 for all interfaces. Save the file.
 4. Edit the `/etc/resolv.conf` file to use IPv6 DNS server or servers.

Configuring Db2 on AIX for IPv6 systems

To get Db2 on AIX operating systems to work on IPv6 systems, complete the following steps:

1. Identify the host name that is used by Db2 in the `db2nodes.cfg` file:

```
# cat ~db2inst1/sqllib/db2nodes.cfg
0 myhost 0
#
```

2. Edit the `/etc/hosts` file and make sure that the host name found in the `db2nodes.cfg` file resolves to an IPv6 address. Use the **vi** editor to verify that the host name is not on any line with an IPv4 address. In particular, ensure that the host name is not listed as an alias for the IPv4 loopback address 127.0.0.1.

```
# vi /etc/hosts
127.0.0.1 loopback localhost
::1 localhost
2001:db8:0:0:209:6bff:fe09:63fa myhost.mydomain myhost
```

3. Stop Db2 and set Db2 to use IPv6 addressing. Restart Db2.

- a. Source the Db2 profile:

```
. ~db2inst1/sqllib/db2profile
```

- b. Stop Db2:

```
db2stop
```

- c. Configure Db2 to use IPv6.

```
db2set
```

An example of the output is: DB2FCMCOMM=TCPIP6.

d. Start Db2.

```
db2start
```

In some installations, the AIX server does not have a graphical console that is attached to the server. In this situation, you can select another system with an X11 server to display the IBM Spectrum Control installation and IBM Spectrum Control application. The X11 server must have IPv6 configured and an SSH client installed. Open an SSH connection from a shell on the X11 server desktop with the -X option to permit forwarding of X11 applications from the remote AIX server. Start the IBM Spectrum Control installation program or application from the SSH shell.

```
ssh -X my_IPv6_host  
/opt/IBM/TPC/gui/TPCD.sh
```

Configuring Db2 on Linux for IPv6-only systems

To get Db2 on Linux systems to work in an IPv6-only environment, follow these steps:

1. Install Db2 in dual-stack configuration.
2. Stop Db2 and set Db2 to use IPv6 addressing:
 - a. As the root user from the Linux command-line, run this command:

```
su - db2inst1
```

b. Stop Db2 by running this command:

```
db2stop
```

c. Configure Db2 to use IPv6 by running this command:

```
db2set
```

An example of the output is: DB2FCMCOMM=TCPIP6.

The host name in the db2nodes .cfg file resolves to an IPv6 address. This action can require you to change the domain or search directive in the /etc/resolv.conf file to specify a domain in which the host name can resolve to IPv6. You can also edit the /etc/hosts file so that the host name resolves to an IPv6 address.

d. Start Db2 by running this command:

```
db2start
```

Chapter 2. Administering

Administer IBM Spectrum Control and its components to ensure that your storage environment is being monitored as intended. Some administering tasks include stopping and starting product services, increasing memory allocation, monitoring the health of product components, and managing storage resources and data sources. You can use the Db2 command-line interface or IBM Data Studio to administer Db2.

Administering resources and data sources

Administer monitored resources and the data sources that are associated with those resources. Data sources can be agents that manage resources or VMware vCenter servers. An agent might be a CIM agent or a Storage Resource agent.

Storage systems

Administer the storage systems that are monitored by IBM Spectrum Control. Administering actions include adding and removing storage systems, updating credentials, and testing connections.

Viewing information about storage systems

View detailed information about storage systems that are monitored by IBM Spectrum Control.

To view information about storage systems, complete the following steps:

1. Depending on how the storage system is configured, go to **Storage > Block Storage Systems**, **Storage > File Storage Systems**, or **Storage > Object Storage Systems**.

Storage systems can be configured in the following ways:

Block storage system

Storage systems that are configured for storing or retrieving data only in block format include System Storage DS series, SAN Volume Controller, Storwize V7000, and other SAN-based storage systems.

Storage systems that can be configured for both file and block data include Storwize V7000 Unified and NetApp Filers.

File storage system

Storage systems that are configured for storing or retrieving data only in file format include IBM SONAS and other network-attached storage (NAS) based storage systems.

Storage systems that can be configured for both file and block data include Storwize V7000 Unified and NetApp Filers.

Object storage system

The storage system that can be configured for both file and object data is IBM Spectrum Scale storage system.

The storage system that can be configured only for object data is IBM Cloud Object Storage.

Information about monitored storage systems is displayed.

2. Right-click a storage system and select **View Properties** to view the key properties for the system.

Updating the credentials for storage systems

Change the credentials that IBM Spectrum Control uses to authenticate to a storage system or the CIM agent that manages a storage system. You can also change the host name or the IP address.

If the storage system is managed by multiple data sources, for example multiple CIM agents, the menu is displayed as **Connections > Modify Connection > data_sources**. Select the data source for which you want to update the credentials.

The type of storage system determines the credentials that you can update.

Updating the credentials for a System Storage DS8000 storage system

Change the credentials that IBM Spectrum Control uses to authenticate to a System Storage DS8000 storage system.

To update the credentials for a System Storage DS8000 storage system, complete the following steps. You can update the host name or IP address for the secondary HMC that is used to manage the storage system, the user name, and the password.

1. In the menu bar, go to **Storage > Block Storage Systems**.
Information about monitored storage systems is displayed.
2. Right-click a storage system and click **Connections > Modify Connection**.
3. Change the secondary HMC host name or IP address, the user name, or the password, and then click **OK**.

Updating the credentials for an XIV or IBM Spectrum Accelerate

Change the credentials that IBM Spectrum Control uses to authenticate to an XIV or IBM Spectrum Accelerate.

To update the credentials for an XIV or IBM Spectrum Accelerate, complete the following steps. You can update the IP address or host name, the user name, and the password.

1. In the menu bar, go to **Storage > Block Storage Systems**.
2. Right-click a storage system and click **Connections > Modify Connection**.
3. Change the host name or IP address, user name, or password, then click **OK**.

Updating the credentials for storage systems that run IBM Spectrum Virtualize

Change the credentials that IBM Spectrum Control uses to authenticate to a SAN Volume Controller, IBM Spectrum Virtualize, IBM Spectrum Virtualize for Public Cloud, or Storwize family storage system.

You can update the IP address or host name, the user name, and the password.

1. In the menu bar, go to **Storage > Block Storage Systems**.
Information about monitored storage systems is displayed.
2. Right-click a storage system and click **Connections > Modify Connection**.
3. Update the following credentials as required and then click **OK**:

Authentication

You can use a user name and password or a private Secure Shell (SSH) key to log on to the storage system. The authentication method that you select determines the options that are displayed.

User name/Password

The user name and password for logging on to the storage system.

Secure Shell (SSH)

Use an existing SSH key or upload a new key to the storage system. Select one of the following actions:

Use an existing SSH key

Use an SSH key that was uploaded to the storage system by using a method other than through IBM Spectrum Control, such as the storage system web interface.

SSH key

The location of the SSH key.

The default location is `${device.conf}\tpc_svc.pem`, which represents the IBM Spectrum Control default key file `tpc_svc.pem`. The `tpc_svc.pem` file is in the `conf` directory where the Device server is installed.

You can enter another location or select **Browse** to search for a key file. If you select **Browse**, the following fields are displayed:

Select file

The location of the SSH key file. You can click **Browse** to search for a file.

Passphrase

The passphrase for the SSH key pair. If you do not have a passphrase, leave this field blank.

The SSH key file is transferred from the computer where the web browser is located to the computer where the IBM Spectrum Control server is located.

Upload a new SSH key

Provide the following information to upload an SSH key to the storage system:

SSH key

The location of the SSH key. The key must exist on the system where you are running the IBM Spectrum Control user interface.

The SSH key must be in OpenSSH format or in PuTTY (.ppk) format that is not password protected.

Passphrase

The passphrase for the SSH key pair. If you do not have a passphrase, leave this field blank.

User name, Password

The name and password for a user that belongs to the storage system Security Administrator role for the cluster that contains the storage system.

IBM Spectrum Control uses this value to configure the SSH key for the user that is entered in the **Associate user** field. The user name that is entered in the **User name** field must have privileges to modify other user accounts, otherwise IBM Spectrum Control cannot configure the SSH key.

Associate user

The user that is associated with the SSH key. If the user name does not exist, it is created and assigned to the storage system Administrator role.

You can click **Get Users** to retrieve all of the existing users from the storage system. You must select a user that belongs to the storage system Administrator role.

The SSH key file is transferred from the computer where the web browser is located to both the computer where the IBM Spectrum Control server is located and to the storage system.

Updating the credentials for a Storwize V7000 Unified storage system

Change the credentials that IBM Spectrum Control uses to authenticate to a Storwize V7000 Unified storage system.

To update the credentials for a Storwize V7000 Unified storage system, complete the following steps. You can update the IP address or host name, the user name, and the password.

1. In the menu bar, go to **Storage > Block Storage Systems**.
Information about monitored storage systems is displayed.
2. Right-click a storage system and click **Connections > Modify Connection**.
3. Update the following credentials as required, and then click **OK**:

Authentication

You can use a user name and password or a private Secure Shell (SSH) key to log on to the storage system. The authentication method that you select determines the options that are displayed.

User name/Password

The user name and password for logging on to the storage system.

Secure Shell (SSH)

Use an existing SSH key or upload a new key to the storage system. Select one of the following actions:

Use an existing SSH key

Use an SSH key that was uploaded to the storage system by using a method other than through IBM Spectrum Control, such as the storage system web interface.

SSH key

The location of the SSH key.

The default location is `${device.conf}\tpc_svc.pem`, which represents the IBM Spectrum Control default key file `tpc_svc.pem`. The `tpc_svc.pem` file is in the `conf` directory where the Device server is installed.

You can enter another location or select **Browse** to search for a key file. If you select **Browse**, the following fields are displayed:

Select file

The location of the SSH key file. You can click **Browse** to search for a file.

Passphrase

The passphrase for the SSH key pair. If you do not have a passphrase, leave this field blank.

The SSH key file is transferred from the computer where the web browser is located to the computer where the IBM Spectrum Control server is located.

Upload a new SSH key

Provide the following information to upload an SSH key to the storage system:

SSH key

The location of the SSH key. The key must exist on the system where you are running the IBM Spectrum Control user interface.

The SSH key must be in OpenSSH format or in PuTTY (.ppk) format that is not password protected.

Passphrase

The passphrase for the SSH key pair. If you do not have a passphrase, leave this field blank.

User name, Password

The name and password for a user that belongs to the storage system Security Administrator role for the cluster that contains the storage system.

IBM Spectrum Control uses this value to configure the SSH key for the user that is entered in the **Associate user** field. The user name that is entered in the **User name** field must have privileges to modify other user accounts, otherwise IBM Spectrum Control cannot configure the SSH key.

Associate user

The user that is associated with the SSH key. If the user name does not exist, it is created and assigned to the storage system Administrator role.

You can click **Get Users** to retrieve all of the existing users from the storage system. You must select a user that belongs to the storage system Administrator role.

The SSH key file is transferred from the computer where the web browser is located to both the computer where the IBM Spectrum Control server is located and to the storage system.

Use different authentication credentials for file storage

Storwize V7000 Unified contains block-level and file-level data. If the credentials are different for block storage and file storage, select this check box to define the credentials for file storage. The options and fields that are displayed are described previously under **Authentication**.

Tip: If you use an SSH key to log on to the file module, the user that you associate with the key must exist on the Storwize V7000 File Module.

Updating the credentials for an IBM SONAS storage system

Change the credentials that IBM Spectrum Control uses to authenticate to an IBM SONAS storage system.

To update the credentials for an IBM SONAS storage system, complete the following steps. You can update the host name or IP address of the storage system, the user name, and the password.

1. In the menu bar, go to **Storage > File Storage Systems**.

2. Right-click a storage system and click **Connections > Modify Connection**.
3. Update the following credentials as required, and then click **OK**.

Authentication

You can use a user name and password or a private Secure Shell (SSH) key to log on to the storage system. The authentication method that you select determines the options that are displayed.

User name, Password

The user name and password for logging on to the storage system.

Secure Shell (SSH)

Use an existing SSH key or upload a new key to the storage system. Select one of the following actions:

Use an existing SSH key

Use an SSH key that was uploaded to the storage system by using a method other than through IBM Spectrum Control, such as the storage system web interface.

SSH key

The location of the SSH key.

The default location is `${device.conf}\tpc_svc.pem`, which represents the IBM Spectrum Control default key file `tpc_svc.pem`. The `tpc_svc.pem` file is in the `conf` directory where the Device server is installed.

You can enter another location or select **Browse** to search for a key file. If you select **Browse**, the following fields are displayed:

Select file

The location of the SSH key file. You can click **Browse** to search for a file.

Passphrase

The passphrase for the SSH key pair. If you do not have a passphrase, leave this field blank.

The SSH key file is transferred from the computer where the web browser is located to the computer where the IBM Spectrum Control server is located.

User name, Password

The name and password for a user that belongs to the storage system Security Administrator role for the cluster that contains the storage system.

IBM Spectrum Control uses this value to configure the SSH key for the user that is entered in the **Associate user** field. The user name that is entered in the **User name** field must have privileges to modify other user accounts, otherwise IBM Spectrum Control cannot configure the SSH key.

Associate user

The user that is associated with the SSH key. You must create the user on the storage system before you add the storage system.

You can click **Get Users** to retrieve all of the existing users from the storage system. You must select a user that belongs to the storage system Administrator role.

Upload a new SSH key

Provide the following information to upload an SSH key to the storage system:

SSH key

The location of the SSH key. The key must exist on the system where you are running the IBM Spectrum Control user interface.

The SSH key must be in OpenSSH format or in PuTTY (.ppk) format that is not password protected.

Passphrase

The passphrase for the SSH key pair. If you do not have a passphrase, leave this field blank.

User name, Password

The name and password for a user that belongs to the storage system Security Administrator role for the cluster that contains the storage system.

IBM Spectrum Control uses this value to configure the SSH key for the user that is entered in the **Associate user** field. The user name that is entered in the **User name** field must have privileges to modify other user accounts, otherwise IBM Spectrum Control cannot configure the SSH key.

Associate user

The user that is associated with the SSH key. You must create the user on the storage system before you add the storage system.

You can click **Get Users** to retrieve all of the existing users from the storage system. You must select a user that belongs to the storage system Administrator role.

The SSH key file is transferred from the computer where the web browser is located to both the computer where the IBM Spectrum Control server is located and to the storage system.

Updating the credentials for a storage system that is managed by a CIM agent

Change the credentials that IBM Spectrum Control uses to authenticate to a CIM agent.

IBM Spectrum Control communicates with SMI-S providers to collect information about the following resources:

- TotalStorage Enterprise Storage Server
- System Storage DS4000®
- System Storage DS5000
- System Storage DS6000
- Non-IBM storage systems that are managed by SMI-S certified Common Information Model Object Manager (CIMOM), such as Dell EMC storage systems other than Unity, Hitachi, and NetApp
- Switches: Brocade

To update the credentials for a CIM agent for a storage system, complete the following steps. You can update the host name or IP address, user name, password, and other information. You can also update the CIM agent credentials for other devices, such as switches, from the GUI pages for those devices.

1. In the menu bar, go to **Storage > Block Storage Systems**.
Information about monitored storage systems is displayed.
2. Right-click a storage system and click **Connections > Modify Connection**.
3. Change the CIM agent host name or IP address, the user name, or the password. Under **Advanced**, you can also specify the protocol, port, and namespace. Click **OK**.

Testing the connection to a storage system

Verify that IBM Spectrum Control can communicate with a monitored storage system. For storage systems that are managed by a CIM agent or Storage Resource agent, the connection to the agent is tested.

To test the connection to a storage system, complete the following steps:

1. Depending on the type of storage system that you want to test, go to **Storage > Block Storage Systems**, **Storage > File Storage Systems**, or **Storage > Object Storage Systems**.
Information about monitored storage systems is displayed.
2. Right-click a storage system and click **Connections > Test Connection**.
A message that shows the results of the test is displayed.

Collecting CIM agent logs

You can collect logs for certain IBM CIM agents using the command line interface.

Remember: Storage systems that use the native interfaces (for example, DS8000, the XIV, SAN Volume Controller, and Storwize V7000) do not use CIM agents.

1. Change to the directory where the CIM agent is installed.

- On Linux operating systems, DS3000, DS4000, DS5000, DS6000 are installed at /opt/IBM/cimagent/cimom
- On Windows operating systems, DS3000, DS4000, DS5000, DS6000 are installed at C:\Program Files\IBM\cimagent\cimom

2. Run one of the following commands:

On Linux operating systems

collectLogs.sh

On Windows operating systems

collectLogs.bat

A **collectedLogs.zip** file is created.

Important: This file is overwritten if you run the script again.

Removing storage systems

Remove storage systems that you no longer want to monitor with IBM Spectrum Control.

To remove a storage system, complete the following steps:

1. In the menu bar, go to **Storage** and select the type of storage system that you want to remove.
2. Right-click a storage system and click **Remove**.
3. Click **Remove** to confirm that you want to remove the storage system.

Hypervisors and VMware data sources

Administer the hypervisors, vCenter Server Appliance systems and vCenter Server systems that are monitored by IBM Spectrum Control. vCenter Server Appliance systems and vCenter Server systems are data sources that can monitor multiple hypervisors. A hypervisor can be an ESX or ESXi host. Each hypervisor can host multiple virtual machines.

Checking permissions to browse data stores

Determine if the user name that you specified for a VMware data source has permission to browse through the data stores on a hypervisor.

When you add a VMware data source in IBM Spectrum Control, the user name that you specify must have permission to browse through the data stores on VMware. IBM Spectrum Control must browse through the data stores to collect information from the hypervisors. However, the "Read Only" role as defined by VMware does not allow IBM Spectrum Control to browse the data stores. You can use the "Virtual Machine Power User" role if you do not want to use the Administrator role, or you can create a custom role with the required permissions.

To verify that a VMware user is assigned the correct role and privileges to monitor VMware data sources, follow these steps:

1. Ensure that the user role has the required VMware datastore permissions by completing the following steps:
 - a) Connect the vSphere Web Client to the VMware data source.
The data source can be an ESX server, a vCenter Server Appliance, or a vCenter Server.
 - b) From the Inventories view, select **Hosts and Clusters**.
 - c) Select a host, and click the **Related Objects** tab.
 - d) View the datastores by clicking the **Datastores** tab.

- e) Right-click a datastore, and select **File Browser**. If you can view the **Files** tab for the datastore, your browse permission is working correctly.
2. Determine the role that is assigned to the user by logging in to the vSphere Web Client by using the administrator user ID. From the Administration view, select **Roles**. Verify the role name that is assigned to the user.
3. Determine the privileges that are assigned to the role by selecting the user's role and clicking **Privileges**. Expand the privilege groups to view the specific privileges.
4. Optional: If you must edit the privileges for the role, select the role and click the **Edit role action** icon. Select privilege groups or expand to select specific privileges.

For more information about VMware user roles, go to the [VMware documentation center](#) and search for *vSphere users and permissions*.

Viewing information about hypervisors

View detailed information about hypervisors that are monitored by IBM Spectrum Control.

To view information about hypervisors and vCenter servers, complete the following steps:

1. Go to **Servers > Hypervisors**

Information about monitored hypervisors and vCenter servers is displayed.

2. Right-click a hypervisor and select **View Properties** to view the key properties of that hypervisor.
3. Optional: Right-click a hypervisor and select **View Details** to view more detailed information about that hypervisor, such as triggered alerts, data collection schedules, and information about its internal and related resources.

Updating the credentials for a hypervisor

You can change the user name and password that IBM Spectrum Control uses to log in to a hypervisor. You can also change the host name or IP address of the hypervisor.

1. In the menu bar, go to **Servers > Hypervisors**.
2. Right-click a hypervisor and select **Connections > Modify Connection**.
3. Update the host name or IP address, user name, or password for the hypervisor.

The user name and password must contain the following valid characters:

- A through Z (uppercase characters)
- a through z (lowercase characters)
- 0 through 9 (numeric characters)
- Special characters: ! # % & * + - / = ? ^ _ { } () . ,

Restrictions:

- User names and passwords cannot contain spaces and must have at least one character.
 - The maximum length of a user name or password is 128 characters.
 - The user name must have permission to browse the data stores on a hypervisor. For more information about permissions, see [“Checking permissions to browse data stores” on page 67](#).
4. Click **OK**.

Removing hypervisors and VMware data sources

Remove hypervisors and VMware vCenter servers that you no longer want to monitor with IBM Spectrum Control.

To remove hypervisors and vCenter servers, complete the following steps:

1. Go to **Servers > Hypervisors**

Information about monitored hypervisors and vCenter servers is displayed.

2. Right-click a hypervisor and select **Remove**.

The hypervisor and all its data are removed from IBM Spectrum Control immediately. Any data collection jobs and alerts are also removed.

When you remove a vCenter Server, the hypervisors that it manages are also removed from IBM Spectrum Control. However, information about the hypervisors is not removed immediately, but is retained according to the **Data for missing resources** setting on the **History Retention** page. The default setting is 14 days. If the default setting is used, all information about the hypervisors is deleted 14 days after the related vCenter Server was removed.

Tips: After a vCenter Server is removed, but before its managed hypervisors are removed according to the retention settings, the following conditions occur:

- Any data collection jobs that are scheduled for the hypervisors fail.
- Because data is no longer collected, any alerts that were based on that data are not generated.

Switches and fabrics

Administer the switches and fabrics that are monitored by IBM Spectrum Control. Administering actions include adding and removing switches and fabrics, modifying connection information, and testing connections.

Viewing information about switches and fabrics

View detailed information about switches and fabrics that are monitored by IBM Spectrum Control.

To view information about switches and fabrics, complete the following steps:

1. In the menu bar in the web-based GUI, go to **Network > Switches** or **Network > Fabrics**. Information about monitored switches or fabrics is displayed.
2. Right-click a switch or fabric and click **View Properties** to view the key properties for the switch or fabric.

Updating the connection information for switches and fabrics

Change the connection information that IBM Spectrum Control uses to authenticate to a data source that manages a switch or fabric.

Depending on the functions that you want to enable, you can use CIM agents or SNMP agents to manage switches and fabrics in your enterprise. You can update the connection information for a switch and fabric to change its data source at any time. The type of data source determines the connection information that you can update.

Updating the connection information for a switch

Change the connection information that IBM Spectrum Control uses to authenticate to a data source that manages a switch. The data source can be a CIM agent or an SNMP agent.

To update the connection information for a switch, complete the following steps:

1. In the menu bar, go to **Network > Switches**. Information about monitored switches is displayed.
2. Right-click a switch and click **Connections > Modify Connection**.

Tip: If a switch is managed by multiple data sources, for example multiple CIM agents, the menu is displayed as **Connections > Modify Connection > data_sources**. Select the data source for which you want to update the connection information.

3. Update the following information as required and then click **OK**.

The information that is displayed depends on the type of data source.

CIM agent

CIM agent host name or IP address

The IP address or host name of the CIM agent that manages the switch.

User name, Password

The user name and password for logging on to the CIM agent.

Advanced

Protocol

The https or http protocol.

Port

The 5989 or 5988 port.

Namespace

The /interop namespace.

SNMPv3 agent**SNMP version**

The SNMP version of the agent.

User name

The user name used to log in to the switch.

Authentication password

The password for the user logged in to the switch.

Authentication protocol

The protocol or digest used for authentication to the switch.

Encryption protocol

The protocol used for encryption.

SNMPv1 agent**SNMP version**

The SNMP version of the agent.

Read community

The SNMP community string. The default is **public**.

Write community

The SNMP community string. The default is **private**.

Updating the connection information for a fabric

Change the connection information that IBM Spectrum Control uses to authenticate to a data source that manages a fabric. The data source can be a CIM agent or an SNMP agent.

To update the connection information for a fabric, complete the following steps:

1. In the menu bar, go to **Network > Fabrics**.
Information about monitored fabrics is displayed.
2. Right-click a fabric and click **Connections > Modify Connection**.

Tip: If a fabric is managed by multiple data sources, for example multiple CIM agents, the menu is displayed as **Connections > Modify Connection > data_sources**. Select the data source for which you want to update the connection information.

3. Update the following information as required and then click **OK**.
The information that is displayed depends on the type of data source.

CIM agent**CIM agent host name or IP address**

The IP address or host name of the CIM agent that manages the switch.

User name, Password

The user name and password for logging on to the CIM agent.

Advanced**Protocol**

The https or http protocol.

Port

The 5989 or 5988 port.

Namespace

The /interop namespace.

SNMPv3 agent

SNMP version

The SNMP version of the agent.

User name

The user name used to log in to the switch.

Authentication password

The password for the user logged in to the switch.

Authentication protocol

The protocol or digest used for authentication to the switch.

Encryption protocol

The protocol used for encryption.

SNMPv1 agent

SNMP version

The SNMP version of the agent.

Read community

The SNMP community string. The default is **public**.

Write community

The SNMP community string. The default is **private**.

Testing the connection to a switch or fabric

Verify that IBM Spectrum Control can communicate with the data source that manages a switch or fabric.

To test the connection to the data source that manages a switch or fabric, complete the following steps:

1. In the menu bar in the web-based GUI, go to **Network > Switches** or **Network > Fabrics**.
Information about monitored fabrics or switches is displayed.
2. Right-click a switch or fabric and click **Connections > Test Connection**.
A message that shows the results of the test is displayed.

Removing switches and fabrics

Remove a switch or fabric that you no longer want to monitor with IBM Spectrum Control.

To remove a switch or fabric, complete the following steps:

1. In the menu bar in the web-based GUI, go to **Network > Switches** or **Network > Fabrics**.
Information about monitored fabrics or switches is displayed.
2. Right-click a fabric or switch and select **Remove**.

Note: To remove a Cisco fabric, you must remove all the switches in that fabric. The Cisco fabric is then automatically removed.

3. Follow the directions that are presented in the information message.

Servers and Storage Resource agents

Administer servers and the Storage Resource agents that collect asset, status, and file system information about servers.

Fixing deployments

Use the **Servers** page to monitor servers that are added to IBM Spectrum Control by deploying a Storage Resource agent. You can identify agents that failed to deploy, investigate and resolve the problems that caused the deployment failure, and deploy the agents again.

To use the **Fix Deployment** action, you must have Administrator privileges.

When you use the **Fix Deployment** action, the existing agent deployment on the server is automatically overwritten when the agent is deployed again.

Use the following steps to identify and fix Storage Resource agents that failed to deploy:

1. Use the Status column on the **Servers** page to identify agents that failed to deploy. A status of Failed deployment indicates that an error occurred when the agent was deployed.
2. Use the deployment log to investigate the problems that prevented the agent from deploying.
Tip: The **Open Logs** action is not available if you select multiple server rows. The **Fix Deployment** action is available if you select a single server row or multiple server rows.
3. Use the **Fix Deployment** action to change the deployment settings for the agents and deploy the agents again.

The following examples show some of the problems that cause agent deployments to fail and the actions that you might take to resolve the problems:

Errors that do not require changes to the deployment settings

The log message indicates that the Db2 database or the Data server is not running. Start the service that is not running and use the **Fix Deployment** action to deploy the agent. You do not need to change the deployment settings.

Errors that require changes to the deployment settings

The log message indicates that the port number on which the agent listens for requests from IBM Spectrum Control is in use by another service. Use the **Fix Deployment** action to change the setting for the Port field and to deploy the agent.

1. In the menu bar, go to **Servers > Servers**.
2. Locate the servers with failed agent deployments that you want to fix.
3. For each server with a status of Failed deployment, complete the following steps:
 - a) To view the error messages, right-click the server row and click **Open Logs**.
 - b) Investigate and resolve the errors.
4. Click a single or multiple servers with a status of Failed deployment and click **Actions > Fix Deployment**.
5. On the **Deploy Agent** page, change the settings that caused the deployment errors.
For example, if the deployment fails because there is not enough disk space at the location that is specified in the Installation path field, you might change the installation location for the agents.

If you selected multiple servers with different operating systems, separate configuration pages are displayed for agents that are deployed on Windows servers and agents that are deployed on UNIX servers.

Tip: If you select multiple servers, the following rules are used to determine the settings for the agent deployment fields:

- a. If the servers use different authentication methods, you cannot change the authentication settings. **Keep current settings** is displayed in the Authentication field and the fields that are used to configure the authentication settings are hidden.
 - b. If the servers are configured with different daemon modes, you can specify the daemon mode to apply to all the selected servers.
 - c. For other fields, if the servers have the same value for the field, the value is displayed. If the servers have different values for the field, the field is blank.
6. On the **Configure** page, if the setting for the Location field caused a deployment error, change the field setting.
 7. Schedule the deployment of the Storage Resource agents.

If you are fixing the agent deployment for multiple servers, a time span is calculated during which the agents are deployed. The agents are deployed at regular intervals during the time span to avoid excessive load on the IBM Spectrum Control server.

8. Schedule the time and frequency that probes are run for the servers.

If you are fixing the agent deployment for multiple servers, a time span is calculated during which the servers are probed.

9. Click **Finish** to deploy the agents.

The changes are applied to the servers that have a status of Failed deployment. If you select servers that have other statuses, for example, Pending deployment, those servers are not affected by the action.

A probe is automatically run for a server after the agent is successfully deployed.

To monitor the status of the agent deployment, check the **Agent State** column on the **Servers** page.

Canceling deployments

Use the **Servers** page to cancel the deployment of Storage Resource agents.

To use the **Cancel Deployment** action, you must have Administrator privileges.

Check the **Agent State** column on the **Servers** page to identify the agent deployments that you can cancel. You can cancel the agent deployment for servers with a status of Failed deployment or Pending deployment.

1. In the menu bar, go to **Servers > Servers**.
2. Locate the servers with the agent deployments that you want to cancel.
3. Click a single or multiple servers with a status of Failed deployment or Pending deployment, and then click **Actions > Cancel Deployment**.

The agent deployment is canceled for the servers with a status of Failed deployment or Pending deployment. If you select servers that have other statuses, for example, Deploying, those servers are not affected by the action.

When you cancel the agent deployments, the servers are removed from IBM Spectrum Control. To add the servers again, click **Deploy Agent**.

Modifying deployment schedules

Use the **Servers** page to modify deployment schedules for Storage Resource agents.

To use the **Modify Deployment Schedule** action, you must have Administrator privileges.

Check the **Agent state** column on the **Servers** page to identify the agent deployments that you can modify. You can modify the deployment schedules for servers that have a status of Pending deployment.

The **Modify Deployment Schedule** action is available if you click a single server row or multiple server rows.

1. In the menu bar, go to **Servers > Servers**.
2. Locate the servers with the agent deployments that you want to modify.
3. Click a single or multiple servers with a status of Pending deployment, and then click **Actions > Modify Deployment Schedule**.
4. On the **Modify Deployment Schedule** window, the current schedule values for the agent deployments are shown. You can change the date and time that agents are deployed.

If you are modifying the deployment schedule for multiple agents, a time span is calculated during which the agents are deployed. The agents are deployed at regular intervals during the time span to avoid excessive load on the IBM Spectrum Control server.

Tips:

- If you select multiple servers and the servers have the same value for a field, the value is displayed. For example, if the selected servers have the same deployment date, the date is displayed. If the servers have different values for the field, the field is blank.
- The scheduled time for an agent deployment is based on the time zone of the IBM Spectrum Control server, not the time zone of the server where the agent is deployed.

5. Click **Save**.

The deployment schedules are modified for the servers that have a status of Pending deployment. If you select servers that have a status other than Pending deployment, the changes to the deployment schedule are not applied to those servers.

Viewing information about Storage Resource agents

View detailed information about the Storage Resource agents that are deployed on monitored resources.

To view information about a Storage Resource agent, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed and select **View Properties**.
3. In the properties notebook, click the **Agent** tab.

Detailed information about the agent is shown, such as the agent state and version, and the date and time when the agent was last updated.

If the Storage Resource agent has a state of Upgrade needed, the agent must be upgraded to the same version level as the IBM Spectrum Control server to which it is communicating.

Viewing Storage Resource agent log files

The log files for a Storage Resource agent contain informational, warning, and error messages for the actions that were taken by the agent. You can use the content of the log files to troubleshoot any errors that might occur when a Storage Resource agent is started, processing data, or shut down.

By default, the log files are located in the following directories on the server where an agent is deployed:

Windows

C:\Program Files\IBM\TPC\agent\log\SRV1\agent.log

Linux, UNIX, and AIX

/opt/IBM/TPC/agent/log/*computer_name*/agent.log




where *computer_name* represents the name of the server where IBM Spectrum Control is installed. If an agent communicates with more than one installation of IBM Spectrum Control, a subfolder is created for each installation. For example, if the agent communicates with servers named SRV1 and SRV2, the following folders are created:

- C:\Program Files\IBM\TPC\agent\log\SRV1\agent.log
- C:\Program Files\IBM\TPC\agent\log\SRV2\agent.log

To view the log file for a Storage Resource agent, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, locate the server that contains the Storage Resource agent that you want to analyze.
3. Right-click the server row and select **Logs > View Agent Log**.
4. Optional: To view only the log entries that have a Warning or Error status, select an option from the **Show all** list.

You can choose to view only entries that have the following statuses:

-  Only error entries
-  Only warning entries
-  Error and warning entries

5. Optional: To view an explanation of the message that is associated with a log entry, click the link in the **ID** column.

Disabling Storage Resource agents

Disable Storage Resource agents so that they no longer collect data or run IBM Spectrum Control jobs.

You might want to disable a Storage Resource agent under the following conditions:

- The monitored server is undergoing maintenance and is unavailable. This action prevents IBM Spectrum Control from flagging the agent as "down" if it cannot reach the agent. The number of times that the

server tries to contact the agent is defined by the **agentErrorLimit** parameter in the `server.config` file.

- The monitored server is busy with resource-intensive processing and you do not want to add any IBM Spectrum Control jobs to that processing load.

To disable a Storage Resource agent, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed and select **Modify Agents > Disable**.
3. Click **OK** to confirm that you want to disable the agent.

The state of the agent is changed to Disabled and remains in that state until it is enabled again. You can disable agents on multiple servers at the same time.

When you disable a Storage Resource agent that is deployed as a daemon service, the service is shut down, and the agent is disabled. IBM Spectrum Control no longer sends requests to the agent or contacts it for job processing. A Storage Resource agent that is deployed as a non-daemon agent runs as a stand-alone process. Because a service is not required for this type of agent, it is not necessary to shut down the agent before it is disabled.

Enabling Storage Resource agents

You can enable Storage Resource agents that are in a Disabled or Down state. After an agent is enabled, the IBM Spectrum Control server resumes communication with that agent.

If the IBM Spectrum Control server cannot contact an agent, the agent is automatically flagged as "down". You can use the **Enable** action to reestablish communication between the agent and the IBM Spectrum Control server. The number of times that the IBM Spectrum Control server tries to contact the agent is specified in the **agentErrorLimit** parameter in the `server.config` file. The default value for the **agentErrorLimit** parameter is 3.

By default, the `server.config` file is located in the following directory:

Windows

`C:\Program Files\IBM\TPC\Data\config`

Linux or UNIX

`/opt/IBM/TPC/Data/config`

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed and select **Modify Agents > Enable**.
You can enable agents on multiple servers at the same time.
3. Click **OK** to confirm that you want to enable the agent.
4. If the agent is running as a daemon service, enter the user ID, password, and other credentials for the server where the agent is deployed. Click **OK** to start the service and enable the agent.

The agent is enabled and the state of the agent is updated to reflect its current condition, such as Up or Upgrade needed. If the agent is deployed as a daemon service, the service is started when you enable the agent.

Testing the connection with a Storage Resource agent

Verify that the IBM Spectrum Control server can communicate with the server where a Storage Resource agent is deployed.

Use the **Test Connection** action in the web-based GUI to verify the state of the Storage Resource agent. For example, if the agent has a state of Down or Unreachable on the **Servers** page, you can test the connection to verify the state of the agent.

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the Storage Resource agent is deployed and select **Modify Agents > Test Connection**.

3. Optional: If the process is slow, click **Close** in the **Testing Agent Connection** window to run the operation in the background.

When the operation is complete, the server status and the agent state are automatically updated on the **Servers** page.

Changing credentials for Storage Resource agents

You can change Storage Resource agent credentials, such as the user name and password that IBM Spectrum Control uses for logging on to the server where the agent is deployed.

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed and select **Modify Agents > Update Credentials**.
3. In the **Enter User Credentials** window, change the credentials for logging on to the server where the agent is installed.

You can change the following credentials:

User name, Password

The user name and password that IBM Spectrum Control uses for logging on to the server where the Storage Resource agent is deployed. The user name must have administrative or root privileges on the server. This action is available only for Storage Resource agents that were deployed as non-daemon services.

The user name and password must contain valid characters. You can enter the following characters:

- A - Z (uppercase characters)
- a - z (lowercase characters)
- 0 - 9 (numeric characters)
- Series of punctuation marks or special characters: ! # % & * + - / = ? ^ _ { } () . ,

Restrictions:

- User names and passwords cannot contain spaces and must have at least one character.
- The maximum length of a user name or password is 128 characters.

Certificate location

The fully qualified path of the certificate file for the Storage Resource agent, for example, `installation_dir/data/sra/operating_system/certs/sra.pem`. This file is on the computer where the IBM Spectrum Control server is installed. If the agent uses Secure Shell (SSH) protocol for communication, the certificate location field is displayed.

Passphrase

The passphrase for the certificate file. The passphrase was created when the certificate was generated.

4. Click **OK** to save the changes.

For more information about using certificates after you install a Storage Resource agent, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/com.ibm.spectrum.sc.doc/fqz0_r_planning_agent_protocols.html.

Collecting service data

Collect service data about the selected Storage Resource agent. Service data includes diagnostic information such as logs, trace files, configuration information, and computer details. Use this information to troubleshoot any errors that might occur during startup, processing, or shutdown of a Storage Resource agent.

To collect service data for a Storage Resource agent, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. Right-click a server and select **Logs > Collect Agent Logs**.

A message is displayed that shows the location where the service file is stored on the IBM Spectrum Control server.

3. In a command line or other navigation tool, go to the directory where the service file is located and unpack its contents.

If the collection of service data is successful, a message is displayed that shows the location of the resulting service file (.zip). The file is stored in a directory on the same computer as the IBM Spectrum Control server. The file is in the following default directories:

- Windows operating system: C:\Program Files\IBM\TPC\data\log\SRATraces\agent_computer_name\TPCServiceInfo.zip
- UNIX or Linux operating system: /opt/IBM/TPC/data/log/SRATraces/agent_computer_name/TPCServiceInfo.zip

Where *agent_computer_name* represents the name of the server on which a Storage Resource agent is deployed. If an agent communicates with more than one installation of IBM Spectrum Control, a subfolder is created for each installation.

If the collection of service data fails, an error message is displayed. For more information about why a data collection failed, see the server log file or the services script. These files are in the following default directories:

- Server log file (on the computer where the IBM Spectrum Control server is installed):
 - Windows operating system: c:\Program Files\IBM\TPC\data\log
 - UNIX or Linux operating system: /opt/IBM/TPC/data/log
- Services script file (on the server where the Storage Resource agent is deployed):
 - Windows operating system: C:\Program Files\IBM\TPC\agent\service\agent_computer_name\TPCServiceInfo.html
 - UNIX or Linux operating system: /opt/IBM/TPC/agent/service/agent_computer_name/TPCServiceInfo.html

Where *agent_computer_name* represents the name of the server on which the Storage Resource agent is deployed.

Enabling or disabling scripts for Storage Resource agents

You can enable or disable scripts that are sent from the IBM Spectrum Control server to Storage Resource agents.

If you enable scripts to run, the Storage Resource agent runs the scripts that are sent from the IBM Spectrum Control server.

If you disable scripts from running, the Storage Resource agent only runs the scripts that are stored on the server where the agent is deployed. The agent does not run scripts that are sent from the IBM Spectrum Control server.

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed. Select **Modify Agents > Enable running scripts on agent** or **Modify Agents > Disable running scripts on agent** to enable or disable scripts from running.

Enabling or disabling the monitoring of fabrics by Storage Resource agents

You can enable or disable fabric monitoring by Storage Resource agents. Fabric monitoring is enabled by default. When you enable fabric monitoring, the agent collects information about fabrics that the server is connected to.

After you install a Storage Resource agent on a server, you can enable or disable the monitoring of fabrics that the server is connected to. If you enable fabric monitoring, the agent collects information about the SAN and zoning.

If you disable fabric monitoring, the agent cannot collect fabric information or monitor fabrics that the server is connected to. If the agent is the only data source that is managing the fabric, the fabric is no longer managed. A state of Unreachable is shown for the fabric on the **Fabrics** page.

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed. Select **Modify Agents > Enable Fabric Functions** or **Modify Agents > Disable Fabric Functions** to enable or disable fabric monitoring.

Using the help command for Storage Resource agents

The **help** command for Storage Resource agents provides information about the parameters for installing, uninstalling, and upgrading Storage Resource agents.

For information about the Storage Resource agent commands, run the **help** command. Follow these steps:

1. Go to the installation location for the Storage Resource agent:

```
cd <installation_location>
```

2. Run the following command:

```
bin/Agent -help
```

3. The output from the **help** command is as follows:

```
Usage:
Agent -INSTALL
      [-COMMTYPE DAEMON -AGENTPORT portnumber]
      [-FORCE]
      -INSTALLLOC pathname
      -SERVERIP address[,address,...]
      -SERVERPORT portnumber
      [-USERID username -PASSWORD password -CERT file -PASSPHRASE phrase]

Agent -UNINSTALL
      [-FORCE]
      -SERVERNAME servername

Agent -UPGRADE
      -INSTALLLOC pathname
```

Removing servers

You can remove servers that you no longer want to monitor with IBM Spectrum Control.

You can use the GUI to remove servers. If a Storage Resource agent is deployed to the server, the agent is uninstalled.

When the server is removed, it is no longer monitored by IBM Spectrum Control. All the data that was collected about the server is removed from the database repository.

Tip: When you remove a server, it is only removed from IBM Spectrum Control. The server is not physically deleted from the storage environment.

To remove a server, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. On the **Servers** page, right-click the server where the agent is deployed and select **Remove**.
3. Click **Remove** to confirm that you want to remove the server.

Registering a Storage Resource agent with a different IBM Spectrum Control server

You can register a Storage Resource agent with a different IBM Spectrum Control server.

A Storage Resource agent is registered with IBM Spectrum Control server A. You want the Storage Resource agent to point instead to IBM Spectrum Control server B.

To register a Storage Resource agent with a different IBM Spectrum Control server, use these steps:

1. From server B, in the menu bar, go to **Servers > Servers**. Click **Add Server**, select **Deploy an agent for full server monitoring**, and click **Manually**.
2. On the **Deploy Agent** page, configure deployment information for the Storage Resource agent. Specify the same port number and installation location that are used for the Storage Resource agent on server A. Select **Overwrite previously installed agents**.
3. On the **Configure** page, schedule the deployment of the Storage Resource agent and click **Finish**.

When the deployment job completes, the Storage Resource agent is registered with server B.

Server A can no longer communicate with the Storage Resource agent. To remove the Storage Resource agent from server A, on the **Servers** page in the web-based GUI, right-click the server that the Storage Resource agent is deployed on and click **Remove**.

Manually changing the Windows service logon

Change the Windows service logon for a Storage Resource agent.

1. Start Windows Services.
2. On the **Services** window, right-click **IBM Spectrum Control Storage Resource agent - 'C:\Program Files\IBM\TPC\'**.
3. Select **Properties**.
4. Click the **Log On** tab.
5. Change the values for **This account**, **Password**, and **Confirm password** to the login credentials that you want to use.

If your IBM Spectrum Control server is part of a Windows domain, change this logon to <domain> \<account>. For example: mydomain\myaccount.

Important: The Storage Resource agent requires that the domain account has local administrator privileges and the "Log on as a service" and "Act as part of the operating system" user rights.

6. Click **Apply** and then **OK** to save your changes.

Managing the daemon Storage Resource agent service on the Virtual I/O Server

Use this information to start and stop the daemon Storage Resource agent service for the Virtual I/O Server.

Starting and stopping the daemon Storage Resource agent service

To start or stop the daemon service, follow these steps:

1. Log in to the Virtual I/O Server using the **padmin** user ID.
2. Run the following command to set up the AIX environment:

```
oem_setup_env
```

3. Change to the base directory where the Storage Resource agent is located. For example:

- To stop the service, run this command:

```
/SRA_install_directory/agent/bin/agent.sh stop
```

- To start the service, run this command:

```
/SRA_install_directory/agent/bin/agent.sh start
```

Deployment guidelines and limitations for Storage Resource agents

You must consider the following guidelines and limitations when you manage Storage Resource agents in your environment.

Use the following information when you deploy Storage Resource agents:

- [Multiple Storage Resource agents that are probing or scanning the same storage resources](#)
- [Platforms that support the deployment of Storage Resource agents](#)
- [Product functions that are not available for storage devices monitored by Storage Resource agents](#)
- [Required authority for deploying Storage Resource agents](#)
- [Orphan zones](#)
- [Firewalls and Storage Resource agents deployments](#)
- [Deploying Storage Resource agents on multiple computers](#)
- [Communication between the IBM Spectrum Control server and a Storage Resource agent](#)
- [Daemon and non-daemon services](#)
- [Port numbers for Storage Resource agents deployed as a daemon service](#)
- [Authentication between the IBM Spectrum Control server and a Storage Resource agent](#)
- [Replacing default SSL certificates](#)
- [Storage Resource agents on the same computer](#)
- [Time zones for computers monitored by Storage Resource agents](#)
- [Connections for Linux and AIX operating systems by using Remote Shell protocol \(RSH\)](#)
- [Deployments on Windows - NetBIOS setting](#)
- [Deployments on Windows - User Account Control \(UAC\) remote restrictions](#)

Multiple Storage Resource agents that are probing or scanning the same resources

If multiple Storage Resource agents are set up to probe or scan the same storage resources, the Storage Resource agent that was added to IBM Spectrum Control first is used for the probe or scan. Therefore, only data that is gathered by the first Storage Resource agent is shown.

Platforms that support the deployment of Storage Resource agents

For a list of platforms on which you can deploy Storage Resource agents, see the [IBM Spectrum Control interoperability matrix](#) and go to the *Agents, Servers and Browsers* section.

Product functions that are unavailable for resources that are monitored by Storage Resource agents

Before you deploy a Storage Resource agent, ensure that the product functions you want to use on the monitored resources are available for those agents. The following functions are not available for resources that are monitored by Storage Resource agents:

- Certain relational database monitoring. For list of relational databases that can be monitored by Storage Resource agents, see the [IBM Spectrum Control interoperability matrix](#) and go to the *Agents, Servers and Browsers* section.
- The reporting of HBA, fabric topology, or zoning information for fabrics that are connected to hosts that are running Linux on IBM System z hardware. These limitations also apply to Storage Resource agents on all guest operating systems for VMware configurations.

Required authorities for deploying and running Storage Resource agents

Before you can create deployment schedules and deploy Storage Resource agents on target computers, you must meet the following requirements:

- To create deployment schedules, you must be logged in to IBM Spectrum Control with a user ID that has the **Administrator** role. For information about user roles, see [“Authorizing users” on page 5](#).
- To deploy Storage Resource agents on target computers, you must provide a user ID that has administrative rights on those computers. You enter this ID when you create a deployment schedule. IBM Spectrum Control uses this ID to log on to the target computers and install and configure the necessary runtime files for the agents.

The user under which a Storage Resource agent (daemon or non-daemon) runs must have the following authorities on the target computers:

- On the Linux or AIX operating systems, the user must have root authority. By default, an agent runs under the user 'root'.
- On the Windows operating systems, the user must have Administrator authority and be a member of the Administrators group. By default, a Storage Resource agent runs under the 'Local System' account.

Orphan zones

Storage Resource agents do not collect information about orphan zones. An orphan zone is a zone that does not belong to at least one zoneset.

Firewalls and Storage Resource agent deployments

Before you can deploy a Storage Resource agent on a computer, you must turn off the firewall on that computer. If you do not turn off the firewall, the deployment fails.

To turn off the firewall on a Windows 2008 computer, complete the following steps:

1. Open Administrative Tools. For information about how to open Administrative Tools, see [“Accessing administration tools” on page 140](#).
2. Click **Windows Firewall with Advanced Security**.
3. Click **Windows Firewall Properties**.
4. Change the **Firewall state** field to **Off** on the following tabs:
 - **Domain Profile**
 - **Private Profile**
 - **Public Profile**
5. Click **OK** to accept the changes and exit.
6. Deploy a Storage Resource agent to the Windows 2008 computer.

Deploying Storage Resource agents on multiple computers

If you deploy Storage Resource agents on multiple computers at the same time, the computers must have the same administrative user ID and password. IBM Spectrum Control uses these user credentials to log on to the computers when you install Storage Resource agents.

Tip: When you deploy Storage Resource agents on multiple computers, a globally unique identifier (GUID) is created for each computer (if one does not exist).

Communication between the IBM Spectrum Control server and a Storage Resource agent

The IBM Spectrum Control server connects to a monitored computer when a Storage Resource agent is deployed and whenever a data collection schedule runs against that agent.

During deployment, the server communicates with the target computer by using one of the following protocols:

- Windows server message block protocol (SMB)
- Secure Shell protocol (SSH)
- Remote execution protocol (REXEC)
- Remote shell protocol (RSH)

After deployment, the type of communication between the server and agent on that computer depends on whether you deployed the agent as daemon service or non-daemon service.

Daemon and non-daemon services

You can deploy a Storage Resource agent as a daemon or non-daemon service:

- A Storage Resource agent that is deployed as a daemon service runs in the background on the monitored computer and listens for requests from the IBM Spectrum Control server. Connectivity between the server and agent is established by using SSL. The server and agent have their

respective certificates and no additional information is required besides those certificates and the security that is provided by the SSL protocol.

- A Storage Resource agent deployed as a service on demand (non-daemon service) runs as a stand-alone executable file on the monitored computer. Communication from the server to the agent uses the same protocol that was used during the deployment of the agent. Communication from the agent to the server uses SSL.
- A Storage Resource agent that is deployed as a daemon service on AIX, Linux, and Windows servers monitors disk paths in near real-time to detect errors. When deployed as a daemon service on an AIX server, the agent also monitors disk error events in near real-time.

If the Storage Resource agent detects path status changes or disk errors, they are included in the status of the disks and paths. You can define alerts so that you are notified of changes to the status of the paths on monitored disks.

Only status changes for existing paths are detected. If a new path is added, or an existing path is removed, the number of paths that is displayed is not updated immediately. The number of paths is updated after the next scheduled probe collects data.

If a disk on an AIX server has an error status and you fix the error, you might want the new status of the disk to be displayed immediately. To display the new status immediately, you must reset the status indicator for the disk. To reset the status indicator, use the **errclear** command to clear the error log. To clear the error log, use the following syntax:

```
errclear -d H -N disk_name 0
```

For example, if you fixed an error on hdisk4, and want to display the new status immediately, run the following command:

```
errclear -d H -N hdisk4 0
```

If you do not reset the status indicator for the disk, the status changes automatically after a few hours.

For information about the **errclear** command, see the product documentation at http://www.ibm.com/support/knowledgecenter/ssw_aix_71/com.ibm.aix.cmds2/errclear.htm.

Port numbers for Storage Resource agents deployed as a daemon service

The following port numbers are used by Storage Resource agents that are deployed as daemon service:

- 9567 (For the Storage Resource agent that is deployed on the same server as IBM Spectrum Control.)
- 9510 (For Storage Resource agents that are deployed on remote servers.)

Storage Resource agents that are deployed as a non-daemon service do not use a port.

Authentication between the IBM Spectrum Control server and a Storage Resource agent

IBM Spectrum Control requires the correct authentication information (user name, password, port, certificate location, or passphrase) for monitored computers each time it communicates with Storage Resource agents on those computers. If the authentication information changes for a host computer on which a Storage Resource agent is deployed, the authentication information for that agent must be updated by using the **Modify Agents > Update Credentials** action on the **Servers** page in the GUI.

Replacing default SSL certificates

IBM Spectrum Control provides default SSL certificates for communication between the Data server and Storage Resource agent.

IBM Spectrum Control Version 5.2.2 uses SSL certificates with 2048-bit encryption keys whereas previous versions of IBM Spectrum Control used 1024-bit encryption keys. If you upgrade IBM Spectrum Control from a version earlier than 5.2.2, your SSL certificates are not updated automatically. If you want to use 2048-bit encryption keys with previous versions of IBM Spectrum Control, you must replace the default SSL certificates with custom SSL certificates.

For information about how to replace SSL certificates, see [“Replacing default SSL certificates with custom certificates”](#) on page 38.

Storage Resource agents on the same computer

You cannot deploy a Storage Resource agent on a computer where a Storage Resource agent is already installed and pointing to the same Data server. You can deploy a Storage Resource agent on the same computer as another Storage Resource agent if those agents communicate with different Data servers and use different ports when you listen for requests.

Time zones for computers that are monitored by Storage Resource agents

The time zones of computers that are monitored by Storage Resource agents are shown as Greenwich mean time (GMT) offsets in IBM Spectrum Control reports. For example, a computer in Los Angeles shows the following time zones in the By Computer report in Asset reporting:

(GMT-8:00) GMT-8:00

Connections for Linux and AIX operating systems by using Remote Shell protocol (RSH)

If RSH is configured to use a user ID and password, the connection fails. To successfully connect to a system by using RSH, you must set up the `.rhosts` file (in the home directory of the account). RSH must be configured to accept a login from the system that is running your application.

Deployments on Windows operating systems - NetBIOS setting

To install a Storage Resource agent on Windows targets, the **Enable NetBIOS over TCP/IP** option must be selected in the Control Panel settings for the computer's network connections properties. To set this option, complete the following steps:

1. Open Windows Control Panel. For information about how to open Windows Control Panel, see [“Accessing administration tools”](#) on page 140.
2. Select **Network and Dial-Up Connections > some_connection > Properties > Internet Protocol (TCP/IP) > Advanced > WINS > Enable NetBIOS over TCP/IP**.

To determine whether these ports are not blocked for inbound requests, see the documentation for your firewall.

To determine whether security policies are blocking the connection ports, open Administrative Tools. For information about how to open Administrative Tools, see [“Accessing administration tools”](#) on page 140..

Depending on whether your policies are stored locally or in Active Directory, follow these directions:

Policies that are stored locally

For policies that are stored locally, complete the following steps:

1. Open Windows Administrative Services.
2. Click **Local Security Policy > IP Security Policies on Local Computer**.

Policies that are stored in Active Directory

For policies that are stored in Active Directory, examine the IP security policies and edit or remove filters that block the ports:

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

For all Windows systems, the Server service must be running to connect to a Windows system by using the Windows protocol.

The following table lists the ports that are reserved for NetBIOS. Ensure that these ports are not blocked.

Port	Description
135	NetBIOS Remote procedure call. (Not currently used.)

Port	Description
137	NetBIOS name service.
138	NetBIOS datagram. (Not currently used.)
139	NetBIOS session (for file and print sharing).
445	CIFS (on Windows XP).

For Windows Server 2008, shares must be shared for the Guest or Everyone accounts, and password protected sharing must be disabled. To disable password protected sharing, follow these steps:

1. Click **Control Panel > Networking and Sharing Center**.
2. Click the down arrow next to **Password protected sharing**.
3. Click **Turn off password protected sharing**.
4. Click **Apply**.
5. Exit from the Control Panel.

Deployments on Windows 2008 - User Account Control (UAC) remote restrictions

To install Storage Resource agents remotely on a Windows 2008 operating system, you must disable the User Account Control (UAC) remote restrictions on the Windows operating system. User Account Control is a security component on Windows operating systems.

Tip: To disable UAC restrictions, you must modify the computer registry. Serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if problems occur. For information about how to back up and restore the registry, see <http://support.microsoft.com/kb/322756/>.

To disable UAC remote restrictions, follow these steps:

1. Open the Windows **Run** window. For information about how to open the **Run** window, see [“Accessing administration tools”](#) on page 140.
2. Enter **regedit** and click **OK**.
3. Locate and click the following registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System
```

4. If the LocalAccountTokenFilterPolicy registry entry does not exist, follow these steps:
 - a. On the **Edit** menu, click **New > DWORD Value**.
 - b. Enter LocalAccountTokenFilterPolicy as the name for the DWORD value and click **Enter**.
 - c. Click **LocalAccountTokenFilterPolicy**, and click **Modify**.
 - d. In the **Edit DWORD Value** window, enter **1**, then click **OK**.

This value can be 0 or 1:

0

This value builds a filtered token. This value is the default value. The administrator credentials are removed.

1

This value builds an elevated token.

- e. Exit the registry editor.

SMI-S providers

Administer SMI-S providers that are associated with storage resources that are monitored by IBM Spectrum Control. SMI-S providers enable communication between IBM Spectrum Control and certain types of storage systems and switches.

IBM Spectrum Control communicates with SMI-S providers to collect information about the following resources:

- TotalStorage Enterprise Storage Server
- System Storage DS4000
- System Storage DS5000
- System Storage DS6000
- Non-IBM storage systems that are managed by SMI-S certified Common Information Model Object Manager (CIMOM), such as Dell EMC storage systems other than Unity, Hitachi, and NetApp
- Switches: Brocade

IBM Spectrum Control communicates directly with the following storage systems and does not require SMI-S providers:

- System Storage DS8000
- SAN Volume Controller
- The XIV
- IBM Spectrum Accelerate
- Storwize family of storage systems
- IBM FlashSystem® family of storage systems
- IBM SONAS
- IBM Cloud Object Storage
- Dell EMC Unity

Adding a CIM agent

Add storage systems and switches that are managed by CIM agents. When you enter information about a storage system or switch, you must enter connection information for the CIM agent that manages it.

You must specify connection information for CIM agents when you add the following resources:

- TotalStorage Enterprise Storage Server
- System Storage DS4000
- System Storage DS5000
- System Storage DS6000
- Non-IBM storage systems that are managed by SMI-S certified Common Information Model Object Manager (CIMOM), such as Dell EMC storage systems other than Unity, Hitachi, and NetApp
- Switches: Brocade


Tips:

- If a CIM agent manages multiple resources, all the resources that it manages are added to IBM Spectrum Control.
- CIM agents must comply with SMI-S standards.
- For a complete list of resources and their CIM agents that you can add, see the *Switches & Directors* and *Storage* sections in the [IBM Spectrum Control interoperability matrix](#).

To add storage system or switch that is managed by a CIM agent, complete the following steps:

1. In the menu bar, go to the resource that you want to add.
To add a storage system, go to **Storage** and select the type of storage system you want to monitor. To add a switch, go to **Network > Switches**.

2. Click **Add resource**, where *resource* represents the type of resource that you want to add.
To add a storage system, click **Add Storage System** and select the type of storage system that you want to add. To add a switch, click **Add Switch**.
3. Specify information about the CIM agent that manages the resource.

Help tips in the GUI: To view descriptions of the information that you must enter for a CIM agent, hover the mouse pointer over the related help icons .

4. Complete adding a storage system or switch that is managed by a CIM agent.

This procedure does not physically add a CIM agent, but enables IBM Spectrum Control to communicate with that agent and collect data about its managed resources.

Verifying that a CIM agent is running

You can verify that a CIM agent is running from the command line interface.

To verify that a CIM agent is up and running, run the following command:

```
telnet <IP> <port>
```

Where <IP> is the IP address of the system where the CIM agent is installed, and <port> is the port number. By default, this is 5989 for a secure connection and 5988 for an unsecure connection.

Replacing a CIM agent for block storage systems, fabrics, and switches

You can replace the Common Information Model (CIM) agent for storage resources without interrupting the collection of performance data or losing historical data.

Attention: Before you begin, check whether a probe job is already in progress for the resource or is scheduled to occur while you replace the CIM agent. Plan the replacement during a time when the probe job is not occurring.

You might want to replace a CIM agent for a storage resource for the following reasons:

- The CIM agent might need to be upgraded to support data collection for the storage resource.
- The CIM agent might run on a different operating system, network, or with a different IP address.

You can replace a CIM agent on IBM System Storage DS4000, IBM System Storage DS5000, and IBM System Storage DS6000. You can also replace a CIM agent on a third-party block storage system, such as an Dell EMC storage system. You cannot replace a CIM agent on IBM System Storage DS8000 (the DS8000 uses a native API (NAPI) connection, rather than a CIMOM).

To replace a CIM agent, follow these steps:

1. Using the instructions that came with your CIM agent software, install the new CIM agent and add the storage resource that it manages. The procedure varies, depending on the type of storage resource.
2. Choose one of the following procedures:

Type of storage resource	Procedure for adding a storage resource to the CIM agent configuration
To add a storage system	See the topic about adding storage systems in the <i>IBM Spectrum Control User's Guide</i> PDF, located in the <i>IBM Spectrum Control Knowledge Center</i> . To view the guide, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/ .
To add a fabric or a switch	See the topic about adding fabrics and switches in the <i>IBM Spectrum Control User's Guide</i> PDF, located in the <i>IBM Spectrum Control Knowledge Center</i> . To view the guide, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/ .

3. In IBM Spectrum Control, run the Add Device Wizard for the new CIM agent.

After the wizard discovers the storage resource, a message is displayed to confirm that the data source (CIM agent) was added for monitoring. Close the window.

4. In the IBM Spectrum Control web GUI, right-click the storage resource and click **Connections > Test Connection > [IP address of the new CIM agent]**.

Verify that the test was successful.

5. Remove the storage system or fabric switch from the old CIM agent.
6. Shut down the old CIM agent services or the device that runs the old CIM agent.
7. Restart the probe to continue the collection of asset, capacity, and configuration data for the resource.
8. Check the status of the probe and performance monitor to ensure that the data is being collected for the storage resource.

The CIM agent is replaced. Depending on your resource or CIM agent, the old association of storage resource and CIM agent might continue to display with the new association in the **Connections** menu. The old CIM agent does not interfere with operation. It cannot be selected as a CIM agent for the storage resource.

For more information, see [SMI-S providers](#) in the *IBM Spectrum Control Knowledge Center*.

Interop namespaces for SMI-S providers for switches and storage systems

This section describes the namespaces for switches and storage system SMI-S providers (also called CIM agents or CIMOMs) that are used in IBM Spectrum Control.

If you specify an incorrect namespace the following issues might occur:

- The connection test fails when the SMI-S provider is added.
- The discovery does not discover all information of the system that is managed by the SMI-S provider.
- The probe fails.
- The function that you want to perform on the system might fail (for example, collecting performance data).

For information about the interoperability namespaces for storage systems, see the [IBM Spectrum Control interoperability matrix for storage systems](#).

For information about the interoperability namespace for switches and directors, see the [IBM Spectrum Control interoperability matrix for switches and directors](#).

SNMP agents

SNMP agents are switches and directors that communicate with IBM Spectrum Control through SNMP.

IBM Spectrum Control uses SNMP to send queries across the IP network to management information bases (MIBs) supported on switches and directors. IBM Spectrum Control uses the Fibre Alliance FC Management MIB and the Fibre Channel FE MIB specifications. The queries are sent only to switches that were added to IBM Spectrum Control for use as SNMP agents. Information is collected from each switch that is configured to use SNMP. The SNMP discovery registers each switch.

You add a switch as an SNMP agent on the **Network > Switches** page. You can then perform actions on the switch, including:

- running an immediate probe job, or scheduling a probe job to collect data from the switch at a specified time
- viewing information about the switch, such as the condition of the switch, the status of the most recent probe job, and other information
- modifying the connection information and credentials for the switch
- removing the switch so it is no longer managed by IBM Spectrum Control.

For information about adding switches to IBM Spectrum Control, go to the product documentation at [Adding fabrics and switches](#).

Displaying information about an SNMP agent

You can view information about an SNMP agent including the IP address, user name, and password.

To display information about an SNMP agent, follow this procedure:

1. In the menu bar, go to **Network > Switches**. Information about monitored switches is displayed.
2. Right-click an SNMP switch and click **Connections > Modify Connection**.
3. The following information is displayed.

SNMPv3 agent

SNMP version

The SNMP version of the agent.

User name

The user name used to log in to the switch.

Authentication password

The password for the user logged in to the switch.

Authentication protocol

The protocol or digest used for authentication to the switch.

Encryption protocol

The protocol used for encryption.

SNMPv1 agent

SNMP version

The SNMP version of the agent.

Read community

The SNMP community string. The default is **public**.

Write community

The SNMP community string. The default is **private**.

Removing an SNMP agent

To remove an SNMP agent that is being managed by IBM Spectrum Control, you must remove the switch or fabric that the SNMP agent is monitoring. Data collected by the agent is not removed from the database repository.

To remove an SNMP agent, follow this procedure:

1. In the menu bar of the GUI, go to **Network > Switches** or **Network > Fabrics**.
2. Right-click a switch or fabric and select **Remove**.

To remove a Cisco fabric, you must remove all the switches in that fabric. The Cisco fabric is then automatically removed.

3. Follow the directions that are presented in the information message.

Starting and stopping the IBM Spectrum Control servers

You can start and stop the IBM Spectrum Control servers in the GUI or by running scripts. Note: IBM Spectrum Control servers start automatically on Windows, Linux, or AIX® operating systems when the operating system is started.

IBM Spectrum Control provides scripts for starting and stopping the servers that run within the product. To run these scripts, on a Windows operating system, you must have Administrator authority.


Tip: The default *installation_dir* is C:\Program Files\IBM\TPC.

Starting the IBM Spectrum Control servers by using the GUI

Start the IBM Spectrum Control Data server, Device server, or Alert server by using the **System Management** page in the GUI.

1. In the menu bar, go to **Home > System Management**.
2. Click **Component Servers** in the **Components** section.
3. Click **Start Server** next to the server that you want to start.

Tip: To start the Web server, use scripts that are provided with the product.

In the **Overview** section of the **System Management** page, the running icon  is displayed next to the server to indicate that it is running.

Starting the IBM Spectrum Control servers by using scripts

Run scripts to start the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems. Note: IBM Spectrum Control servers start automatically on all platforms when the operating system is started.

Starting the IBM Spectrum Control servers on Windows

Important: IBM Spectrum Control provides scripts for starting and stopping the servers that run within the product. To run these scripts, you must have Administrator authority.

Tip: The default *installation_dir* is C:\Program Files\IBM\TPC.

To start the servers on the Windows operating system, enter the following commands in the following order:

Data server

```
installation_dir\scripts\startTPCData.bat
```

Device server

```
installation_dir\scripts\startTPCDevice.bat
```

Alert server

```
installation_dir\scripts\startTPCAalert.bat
```

Export server

```
installation_dir\scripts\startTPCExport.bat
```

Web server

```
installation_dir\scripts\startTPCWeb.bat
```

Storage Resource Agent - *directory*

Tip: The **Storage Resource Agent service** is started on the Windows operating system by using Windows Services.

To start the **Storage Resource Agent** service on Windows, complete the following steps:

1. Open Windows **Services**. For information about how to start Services, see [“Accessing administration tools”](#) on page 140.
2. Start the **IBM Storage Resource Agent - *directory*** service where *directory* is where the Storage Resource agent is installed.

Starting the IBM Spectrum Control servers on Linux or AIX

Note: The default *installation_dir* is /opt/IBM/TPC.

To start the servers on the Linux or AIX operating systems, enter the following commands in the following order:

Data server

```
/installation_dir/scripts/startTPCData.sh
```

Device server

```
/installation_dir/scripts/startTPCDevice.sh
```

Alert server

```
installation_dir/scripts/startTPCAAlert.sh
```

Export server

```
installation_dir/scripts/startTPCExport.sh
```

Web server

```
/installation_dir/scripts/startTPCWeb.sh
```

Storage Resource Agent


```
/installation_dir/agent/bin/agent.sh start
```

Stopping the IBM Spectrum Control servers by using the GUI

Stop the IBM Spectrum Control Data server, Device server, or Alert server by using the **System Management** page in the GUI.

1. In the menu bar, go to **Home > System Management**.
2. Click **Component Servers** in the **Components** section.
3. Click **Stop Server** next to the server that you want to stop.

Tip: To stop the Web server, use scripts that are provided with the product.

In the **Overview** section of the **System Management** page, the error icon  is displayed next to the server to indicate that it is stopped. While a server is stopped, some product functions are not available. For example, if the Alert server is stopped, the ability to detect alert conditions on resources and send notifications is not available.

Stopping the IBM Spectrum Control servers by using scripts

Run scripts to stop the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems.

Stopping the IBM Spectrum Control servers on Windows

Important: IBM Spectrum Control provides scripts for starting and stopping the servers that run within the product. To run these scripts, you must have Administrator authority.

Tip: The default *installation_dir* is C:\Program Files\IBM\TPC.

To stop the servers on the Windows operating system, enter the following commands in the following order:

Storage Resource agent

To stop the **Storage Resource Agent** service on Windows, complete the following steps:

1. Open Windows Services. For information about how to open Windows Services, see [“Accessing administration tools”](#) on page 140.
2. Stop the **IBM Storage Resource Agent - *directory*** service where *directory* is where the Storage Resource agent is installed.

Web server

```
installation_dir\scripts\stopTPCWeb.bat
```

Export server

```
installation_dir\scripts\stopTPCExport.bat
```

Data server

```
installation_dir\scripts\stopTPCData.bat
```

Device server

```
installation_dir\scripts\stopTPCDevice.bat
```

Alert server

```
installation_dir\scripts\stopTPCAAlert.bat
```

Stopping the IBM Spectrum Control servers on Linux or AIX

Tip: The default *installation_dir* is /opt/IBM/TPC.

To stop the servers on Linux or AIX operating systems, enter the following commands in the following order:

Storage Resource Agent

```
/SRA_installation_dir/agent/bin/agent.sh stop
```

Web server

```
/installation_dir/scripts/stopTPCWeb.sh
```

Export server

```
/installation_dir/scripts/stopTPCExport.sh
```

Data server

```
/installation_dir/scripts/stopTPCData.sh.
```

Device server

```
/installation_dir/scripts/stopTPCDevice.sh
```

Alert server

```
installation_dir/scripts/stopTPCAAlert.sh
```

Checking the version and license of IBM Spectrum Control

The version and license of IBM Spectrum Control that is installed on your system determine the IBM Spectrum Control functions that are available.

Check the version of IBM Spectrum Control that is installed on your system to verify that you are using the correct level of the documentation.

Check the license that is installed on your system if documented functions are not available. The functions might be restricted to a different license.

To check the version and license of IBM Spectrum Control that is installed, complete the following steps in the web-based GUI:

1. Click the question mark icon in the banner pane of the window to display a list of help topics.
2. From the list of help topics, select **About**.

Checking IBM Spectrum Control status

The **System Management** page shows a high-level summary of the status of the server or servers on which IBM Spectrum Control is installed. Use the System Management page to troubleshoot problems with the system, create trace logs, and get technical support.

The following system status information is available:

- The state of component servers, such as the Data server, Device server, and Alert server, and the Db2 database. In a multiple-server environment, the Tivoli Common Reporting server or the Db2 database can run on a separate server from the Data server, Device server, and Alert server. In such a multiple-server environment, the **System Management** page shows which components are installed on each server.
- A chart showing the amount of used and available file system space on the server over time. Use this chart to view the storage usage trends on the server to identify or predict performance problems. In a multiple-server environment, a separate chart is shown for the two servers.
- A set of charts showing performance information for the storage system volumes that the server writes to and reads from most often. The charts show the following information for the volumes:

- Volume utilization
- I/O rate
- Data rate
- Response time
- Read cache hits

In a multiple-server environment, these charts are shown for each server.

- Alert conditions detected on the server or servers on which IBM Spectrum Control is installed.

Troubleshooting problems with the IBM Spectrum Control component and servers

If IBM Spectrum Control is not running or its performance has degraded, you can use the **System Management** page of the IBM Spectrum Control GUI to assess the overall condition of the system. You can also view the file system capacity and volume performance trends to help you anticipate future needs and prevent problems.

To view file system capacity information, the Storage Resource agent on the IBM Spectrum Control server must be running. In a multiple-server environment, a Storage Resource agent must be installed and running on the secondary server to view file system capacity information for the secondary server.

To view performance information for storage system volumes, the storage systems must be managed by IBM Spectrum Control and have performance monitors running.

The **System Management** page shows a high-level summary of the condition of the server or servers on which IBM Spectrum Control is installed.

To troubleshoot problems with IBM Spectrum Control, complete the following steps:

1. In the menu bar, go to **Home > System Management**.
2. Use the **System Management** page to view the status of the IBM Spectrum Control system.
 - Check the state of each component server and the DB2 database to verify that they are all running. To examine the status and resource usage of component resources in detail and, if necessary, to restart the Data server, Device server, or Alert server, complete the following steps:
 - a. Click **Component Servers** in the **Components** section. View the state, memory use, and database connections for each component server.
 - b. Optional: If the Data server, Device server, or Alert server is not running, click the **Start Server** button to restart the server. If the Device server is running, but one or more of its services are not running, click the **Start Services** button to restart the services.
 - If the performance of the IBM Spectrum Control is slow, examine the chart for available file system space and the volume performance charts.
 - Check whether there are any alerts for the server or servers on which IBM Spectrum Control is installed. The **Alerts** link in the **Overview** section shows the number of alerts and the greatest alert severity. Click **Alerts** in the **Overview** section to view the alerts.
3. Optional: You can also view the status of the product servers on Windows:
 - a) On the Windows desktop, click **Start > Control Panel > Administrative Tools > Services**.

Tip: For information about how to view information about services on different versions of Windows, see http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.5/com.ibm.spectrum.sc.doc/fqz0_t_windows_start_tools.html.
 - b) On the **Services window**, locate the names of the server services. For example, the service for the Alert server is **IBM Spectrum Control - Alert Server**.
 - c) View the **Status** column to determine if the service is running or stopped.
 - d) Optional: If a server is not running and you want to restart it, right-click the service name for that server and click **Start**.

Opening PMRs and packaging IBM Spectrum Control system log files for IBM Software Support

To provide trace information to IBM Software Support about the performance of IBM Spectrum Control, you can open a PMR and package a set of log files. The log files contain trace information for component servers such as the Data server, Device server, Web server, and Alert server.

To package IBM Spectrum Control system log files, you must be assigned to the Administrator role.

The **Home > System Management** page shows an overview of IBM Spectrum Control system status, and can be used to troubleshoot performance problems. If you are unable to resolve the problems, click **Get Support** to open a PMR (Problem Management Record), collect log files, and upload a package of those log files to IBM Software Support.

When the IBM Spectrum Control component servers are running, they write trace information to log files. From the **System Management** page, you can save log files. When you save log files, IBM Spectrum Control packages the log files from all the component servers into a single compressed file that you can send to IBM Software Support.

Tip: Only one version of the log file package is retained at a time. When you create a new package, the previous package is overwritten.

Before you package the log files, you can, optionally, adjust the level of trace recording for each component server. For the Device server, you can adjust the trace level for individual services. By selectively setting trace levels, you can provide IBM Software Support with more information on particular component servers that are the suspected source of the problem. You can also reduce the trace level for a particular component server to improve system performance.

To package IBM Spectrum Control log files for IBM Software Support, complete the following steps:

1. In the menu bar, go to **Home > System Management**.
2. Optional: To adjust the trace level for any of the component servers, complete the following steps:
 - a) Click **Component Servers** in the **Components** section. In the **Component Servers** pane, you can view performance information for each component server. The current trace level for each component server and the Device server services is highlighted.
 - b) Adjust the trace level for a component server or a Device server service by clicking **Low**, **Medium**, or **High**.

Tip: If you adjust the trace level for one or more component servers, wait at least several hours before you package the log files. If you package the log files too soon after you adjust the trace levels, the logs will not contain enough traces at the new level. Before you create the logs, you might want to try to re-create the problem so that the log files contain the relevant trace data.
3. Click **Get Support** in the **General** section.
4. Optional: On the **Get Support** page, click **Open PMR** if you do not already have a PMR associated with your issue.

A PMR is used by IBM Support to track and manage your issue and is required when you upload a log file package.
5. Click **Collect Log** to create a package of log files and upload that package to IBM Support.

You can automatically upload the package to IBM Support, or you can upload it manually by using the FTP transfer methods that are described on the **Get Support** page. For more information about uploading and resolving any FTP-related problems when you upload the package, see [“Troubleshooting FTP transfers”](#) on page 94.

It can take 20 minutes or longer for IBM Spectrum Control to generate and package the log files. You can do other work or log out of IBM Spectrum Control while the package is being created. When the process completes, you can download the package by clicking the provided link on the **System Management** page.

Depending on the environment, the size of the log file package can vary. Its size is determined by the following factors:

- How frequently the product is used

- The number of resources that are monitored, the type of data that is being collected, and how frequently that data is collected
- The length of time that the product has been up and running

For example, if the product monitors five storage systems over a period of three days, and collects asset and performance each day, the size of the package might be 200 - 300 MB.

Troubleshooting FTP transfers

When you attempt to send files to IBM by using FTP, such as a log package from the **System Management** page or a compressed file from the service tool, the upload cannot be completed. This problem might occur because of network or firewall restrictions.

When IBM Spectrum Control uploads a log package to IBM Software Support, it is sent to the Enhanced Customer Data Repository (ECuRep) by using standard FTP protocol. The upload is secure and the data is encrypted with AES-128 key for each file part and RSA-2048 key for the key exchange. The name of the FTP server that receives the upload is ftp.ecurep.ibm.com.

If IBM Spectrum Control cannot connect to the FTP server because of firewall restrictions in your organization, you must open the necessary ports for FTP transfers from the IBM Spectrum Control server. Because standard, unencrypted FTP in passive mode is used for uploads (encryption is done at the data level, not the connection level), the firewall must be configured to allow passive FTP connections to ftp.ecurep.ibm.com. Contact your network administrator for assistance.

For older firewalls, open port 21 (the default FTP) and ports 65024 - 65535 (for passive FTP). For more information, see http://www.ibm.com/de/support/ecurep/send_ftp.html.

If your organization uses a proxy server for FTP, complete the following steps to troubleshoot uploads from IBM Spectrum Control:

1. Use a text editor to create a file that is named `ibmsdduu.config`.
2. In `ibmsdduu.config`, specify the proxy configuration to use.
 - a) To determine the specific information that must be included in `ibmsdduu.config` for your FTP proxy, review the following instructions:

SOCKS Server and HTTP Proxy Support

```
-socks4 enable SOCKS 4 support
-socks5 enable SOCKS 5 support
-http_proxy enable support for http proxy tunneling

-socks4 -sock5 and -http_proxy are exclusive, the last switch in
command line is used

-proxyhost=<host> define the address of the proxy or SOCKS server

-proxyport=<port>   define the port of the proxy.
                   default: 1080 for SOCKS4 and SOCKS5
                   8080 for http_proxy

-proxyuser=<userid> define the userid for the proxy or SOCKS server
-proxypw=<password> define the password for the proxy or SOCKS server

proxy userid and proxy password are optional
```

FTP Proxies

ftp proxy support is enabled with a separate command line option. This enables the combination of SOCKS server and a ftp proxy if necessary.

```
-ftp_proxytype=<type> enables ftp proxy support and define the type of
                     the proxy. <type> is an integer, see
                     ftp proxy types below
                     Default: 0 - no proxy

-ftp_proxyuser      userid for the ftp proxy

-ftp_proxypw        password for the ftp proxy

-ftp_proxyhost      hostname or ip address of the ftp proxy
```



```
-ftp_proxyport port number of the ftp proxy
                        Default: 21
```

FTP Proxy Types

There are several ftp proxy types known. Each type is using a different login procedure and needs different commands to connect to the target ftp server.

In the list of supported ftp proxy types <server>,<user>,<password> are referring to the target ftp server, <p_user> and <p_passwd> to the ftp proxy account.

```
-ftp_proxytype=0
    no ftp proxy is used ( this is the default )

-ftp_proxytype=1
    connect; USER <p_user>; PASS <p_passwd>;
    SITE <server>; USER <user>; PASS <passwd>

-ftp_proxytype=2
    connect; SITE <server>; USER <user>; PASS <passwd>

-ftp_proxytype=3
    connect; USER <p_user>; PASS <p_passwd>;
    OPEN <server>; USER <user>; PASS <passwd>

-ftp_proxytype=4
    connect; OPEN <server>; USER <user>; PASS <passwd>

-ftp_proxytype=5
    connect; USER <user>@<server>; PASS <passwd>

-ftp_proxytype=6
    connect; USER <p_user>@<server>; PASS <p_passwd>;
    USER <user>; PASS <passwd>

-ftp_proxytype=7
    connect; USER <user>@<server> <p_user>;PASS <p_passwd>;
    ACCT <passwd>

-ftp_proxytype=8
    connect; USER <user>@<server> <p_user>;PASS <passwd>;
    ACCT <p_passwd>

-ftp_proxytype=9
    connect; USER <user>@<p_user>@<server>;PASS <passwd>;
    ACCT <p_passwd>

-ftp_proxytype=10
    connect; USER <user>@<p_user>@<server>;PASS <p_passwd>;
    ACCT <passwd>

-ftp_proxytype=11
    connect; USER <p_user>; PASS <p_passwd>;
    USER <user>@<server>; PASS <passwd>

-ftp_proxytype=12 (CheckPoint Firewall 1)
    connect; USER <user>@<p_user>@<server>
    PASS <passwd>@<p_passwd>
```

- b) Based on the type of FTP proxy server that you use, copy and paste the appropriate section from step 2a into `ibmsdduu.config`.
- c) For the section that you pasted into `ibmsdduu.config`, provide information such as host name, port, user ID, and password, as needed.
- For example:

```
-ftp_proxytype=1
-ftp_proxyuser=my_user_id
-ftp_proxypw=my_password
-ftp_proxyhost=ftp_proxy.my_company.com
-ftp_proxyport=21
```

Where:

- `my_user_id` and `my_password` represent the authentication credentials for connecting to the FTP proxy server.
 - `ftp_proxy.my_company.com` represents the DNS name of the FTP proxy server.
3. Save the file to `installation_dir/services`, where `installation_dir` represents the directory where IBM Spectrum Control is installed.

The default installation directory is as follows:

- Windows: `C:\Program Files\IBM\TPC`
- Linux / AIX: `/opt/IBM/TPC`

4. Try to upload the log package or compressed file again.

If you still cannot automatically upload a log package in the IBM Spectrum Control GUI, you can try uploading it manually. For information about how upload files to ECuRep manually, see the following topics:

- [FTP Transfer](#)
- [Upload through browser](#)

Log packages are stored on the IBM Spectrum Control server at the following location:

`installation_dir/wlp/usr/servers/webServer/apps/WebServer.ear/TPC-GUI.war/serviceLog`

Increasing the memory allocation for the Data server

If the data memory that is allocated for your Data server is insufficient, you can increase the memory. The default maximum memory for the Data server is set to 1024 MB.

You cannot increase the memory for the Device server. The memory for the Device server is set to the maximum heap size for the JVM.

Increasing the memory allocation for the Data server that is running on AIX

Increase the memory allocation for the Data server that is running on AIX.

To increase the memory that is allocated for the Data server, complete the following steps:

1. Log on as a user with root authority.
2. Stop the Data server. From the command line, run the following command:

```
/TPC_install_directory/scripts/stopTPCData.sh
```

Where `TPC_install_directory` is the installation directory. The default directory is `/opt/IBM/TPC`.

3. Using a text editor, open the `/TPC_install_directory/data/server/tpcdsrv1` file.
4. Locate the following line:

```
exec $JAVAEXE -Dsun.net.inetaddr.ttl=300 -Xrs -XmxXXXXm
-cp $CLASSPATH com.tivoli.itsm.server.Server &
```

where `XXXX` is the memory allocated for the Data server. The default is 1024m (1024 MB).

5. Increase the memory that is allocated for the Data server. For example, to increase the memory to 1536 MB, change the line to read as follows:

```
exec $JAVAEXE -Dsun.net.inetaddr.ttl=300 -Xrs -Xmx1536m
-cp $CLASSPATH com.tivoli.itsm.server.Server &
```

6. Save the modified `tpcdsrv1` file.
7. Start the Data server by running the following command:

```
/TPC_install_directory/scripts/startTPCData.sh
```

Increasing the memory allocation for the Data server that is running on Linux

Increase the memory allocation for the Data server that is running on Linux.

To increase the memory that is allocated for the Data server, complete the following steps:

1. Log on as a user with root authority.
2. Stop the Data server.
3. From the command line, run the following command:

```
/installation_dir/scripts/stopTPCData.sh
```

Where *installation_dir* is the installation directory. The default directory is */opt/IBM/TPC*.

4. Using a text editor, open the */installation_dir/data/server/tpcdsrv1* file.
5. Locate the following line:

```
exec $JAVAEXE -Dsun.net.inetaddr.ttl=300 -Xrs -XmxXXXXm  
-cp $CLASSPATH com.tivoli.itsrm.server.Server &
```

Where XXXX is the memory that is allocated for the Data server. The default is 1024m (1024 MB).

6. Increase the memory that is allocated for the Data server. For example, to increase the memory to 1536 MB, change the line to read as follows:

```
exec $JAVAEXE -Dsun.net.inetaddr.ttl=300 -Xrs -Xmx1536m  
-cp $CLASSPATH com.tivoli.itsrm.server.Server &
```

7. Save the modified *tpcdsrv1* file.
8. Start the Data server by running the following command:

```
/installation_dir/scripts/startTPCData.sh
```

Increasing memory allocation for Data server that is running on Windows

Increase the memory allocation for the Data server that is running on Windows.

To increase the memory that is allocated for the Data server, complete the following steps:

1. Open the **Run** window. For information about how to open the **Run** window, see [“Accessing administration tools”](#) on page 140.
2. Type `regedit` and click **OK**. The **Registry Editor** window is displayed.
3. Expand the **HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > IBM > TSRM > 1** in the **Registry Editor** window.
4. Right-click the **1** folder and click **New > String Value**.
5. Type `SRVJPARGS` as the name of the string.
6. Right-click the name of the string and click **Modify**.
7. Enter `-XmxXXXXm` in the **Value data** field, where XXXX represents the number of megabytes for the server maximum heap size. Click **OK**.

The default size is 1024 MB. The largest possible value for the maximum heap size is 1536 MB. If the value is set to something larger than 1536, that value is ignored and 1536 MB is used as the maximum heap size.

8. Stop and restart the server to have the changes take effect. To stop the server, complete the following steps:
 - a) Open Windows Services. For information about how to open Services, see [“Accessing administration tools”](#) on page 140.
 - b) Right-click **IBM Spectrum Control - Data Server** and click **Stop**.
To restart the server, right-click the service and click **Start**.

Changing passwords

IBM Spectrum Control provides a GUI and non-GUI password tool; however, both tools achieve the same purpose.



Attention: For Linux and AIX operating systems, it is recommended that you use the GUI password tool. However, if you use the non-GUI password tool for future updates, then *do not* use the GUI password tool to update your passwords on the same system at a later time or the IBM Spectrum Control servers might not operate properly.

If you installed IBM Spectrum Control and used the same Db2® user ID and password for the items IBM Spectrum Control requires, then when you change the Db2 password, you must also change the passwords for the items that the Db2 password applies to.

The Db2 administrative password might also apply to the following items:

- The database administration user ID and password (for the Data or Device server to connect to the database).
- The database user ID and password to create the database schema.
- The host authentication password (for the Storage Resource agents to communicate with the Device server).
- The Storage Resource agent service login user ID and password (for Windows only, if this user ID does not exist).

Changing passwords by using the password tool

Use the password tool to change the passwords for Db2 and IBM Spectrum Control so that they can continue to authenticate to one another whenever you change a password.



Attention: For Linux and AIX operating systems, it is recommended that you use the GUI password tool. However, if you use the non-GUI password tool for future updates, then *do not* use the GUI password tool to update your passwords on the same system at a later time or the IBM Spectrum Control servers might not operate properly.

If you are logged on to IBM Spectrum Control by using a domain user account, which is also a member of the local administrator group, when you run the change password tool, passwords are not updated. If you run the tool by using a local OS user account, and an error occurs, complete these steps.

To run the password tool when you log in by using a domain user account, choose one of the following methods:

- Right-click the `changepasswords.bat` file and select **Run as administrator**.

Or

1. Click **Start > All Programs > Open Administrative Tools > Local Security Policy**.
2. On the **Local Security Policy** window, disable **User Account Control: Run all administrators in Admin Approval Mode**.
3. Restart your computer.

Single server installation where components use the same logon credentials

Use the password tool to change the password for IBM Spectrum Control when it is installed on a single server and the Common User and the Db2 User are identical and use the same logon credentials. The credentials are usually *db2admin* on a Windows operating system or *db2inst1* on AIX and Linux operating systems.

Before you use the password tool, ensure that you know the existing password or passwords that you want to change. Stop the IBM Spectrum Control servers.

Use the following steps to change the Db2 password in the Windows, AIX, or Linux operating systems. Then, use the IBM Spectrum Control password tool to update the IBM Spectrum Control servers to use the new Db2 password.

To change a password in the Windows operating system, follow these steps:

1. Open the Control Panel. For more information, see [“Accessing administration tools” on page 140](#).
 - a) Select **User Accounts** and click **Change account type**.
 - b) Select the user account of the password that you want to change.
 - c) Select **Change password**.
 - d) Enter and confirm the new password and click **Change password**.

If the password, for the Windows domain user ID that you used as the IBM Spectrum Control Common User expired, change that password in the Windows domain before you continue. If you see the following error or a similar error after you run the password tool, verify that the password for your Common User Windows domain user ID did not expire:

```
com.tivoli.itsrm.tools.changepasswords.ChangePasswords error  
SEVERE: The DB2 password is invalid.
```

If necessary, change the Common User Windows domain password and run the password tool again.

To change a password in the AIX or Linux operating system, follow these steps:

2. Log in as the root user.
 - a) Run the following command:

```
passwd username
```

Where *username* is the user whose password you want to change.

- b) Enter the new password and confirm that new password is correct.

To use the IBM Spectrum Control password tool to update the IBM Spectrum Control servers to use the new password, follow these steps:

3. Open a command prompt and change the directory to the following directory:

Windows operating systems

```
Spectrum_Control_Installation_dir\service
```

Linux or UNIX operating systems

```
Spectrum_Control_Installation_dir/service
```

4. Start the password tool by running the following command:

Windows operating systems

```
changepasswords.bat
```

Linux or UNIX operating systems

```
./changepasswords
```

5. Select **Change the IBM Spectrum Control and DB2 Passwords** and click **OK..**
6. Enter and then confirm the same new password that you entered when you changed the password in the operating system in Step 1 or Step 2. Verify that the **Restart servers** option is selected.
7. Click **OK**.
8. In the **Confirm password change** window, click **Yes**.
9. When the tool finishes, click **Back To Main**.
10. Click **Exit program..**

Tip: To verify that the password changes were successful, review the log file that is located in the `Spectrum_Control_installation_dir\service\log` directory.

Related tasks

[“Single-server installation where components use different logon credentials” on page 100](#)

Use the password tool to change the passwords for IBM Spectrum Control when it is installed on a single server and the Common User and the Db2 User are different and use different logon credentials.

[“Multiple-server installation where Db2 is remote” on page 102](#)

Use the password tool to change the passwords for IBM Spectrum Control when the IBM Spectrum Control database repository and the IBM Spectrum Control servers are installed on different servers.

Related reference

[“Stopping the IBM Spectrum Control servers by using scripts” on page 90](#)

Run scripts to stop the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems.

[“Changing passwords by using the password tool” on page 98](#)

Use the password tool to change the passwords for Db2 and IBM Spectrum Control so that they can continue to authenticate to one another whenever you change a password.

Single-server installation where components use different logon credentials

Use the password tool to change the passwords for IBM Spectrum Control when it is installed on a single server and the Common User and the Db2 User are different and use different logon credentials.

Before you use the password tool, ensure that you know the existing password or passwords that you want to change. Stop the IBM Spectrum Control servers.

Use the following steps to change the passwords in the Windows, AIX, or Linux operating systems. Then, use the IBM Spectrum Control password tool to update the IBM Spectrum Control servers to use the new passwords.

To change a password in the Windows operating system, follow these steps:

1. Open the Control Panel. For more information, see [“Accessing administration tools” on page 140](#).
 - a) Select **User Accounts** and click **Change account type**.
 - b) Select the user account of the password that you want to change.
 - c) Select **Change password**.
 - d) Enter and confirm the new password and click **Change password**.

If the password, for the Windows domain user ID that you used as the IBM Spectrum Control Common User expired, change that password in the Windows domain before you continue. If you see the following error or a similar error after you run the password tool, verify that the password for your Common User Windows domain user ID did not expire:

```
com.tivoli.itsrm.tools.changepasswords.ChangePasswords error  
SEVERE: The DB2 password is invalid.
```

If necessary, change the Common User Windows domain password and run the password tool again.

To change a password in the AIX or Linux operating system, follow these steps:

2. Log in as the root user.
 - a) Run the following command:

```
passwd username
```

Where *username* is the user whose password you want to change.

- b) Enter the new password and confirm that new password is correct.

To use the IBM Spectrum Control password tool to update the IBM Spectrum Control servers to use the new passwords, follow these steps:

3. Open a command prompt and change the directory to the following directory:

Windows operating systems

```
Spectrum_Control_Installation_dir\service
```

Linux or UNIX operating systems

```
Spectrum_Control_Installation_dir/service
```

4. Start the password tool by running the following command:

Windows operating systems

```
changepasswords.bat
```

Linux or UNIX operating systems

```
./changepasswords
```

5. To change the Common User's password in IBM Spectrum Control, do the following in the password tool:
 - a) Select **Change IBM Spectrum Control Passwords** and click **OK**.
 - b) Enter and then confirm the same new password that you entered when you changed the Common User's password in the operating system in Step 1 or Step 2.
 - c) Click **OK**.
 - d) In the **Confirm password change** window, click **Yes**.
 - e) When the process is completed, click **Back to Main**.
6. To change the Db2 User's password in IBM Spectrum Control, do the following in the password tool:
 - a) Select **Change DB2 password** and click **OK**.
 - b) Enter and confirm the same new password as you entered when changing the Db2 User's password in the operating system in Step 1 or Step 2. Verify that the **Restart servers** option is selected.
 - c) Click **OK**.
 - d) In the **Confirm password change** window, click **Yes**.
 - e) When the process is completed, click **Back to Main**.
7. Click **Exit Program**.

Tip: To verify that the password changes were successful, review the log file that is located in the `Spectrum_Control_installation_dir\service\log` directory.

Related tasks

[“Single server installation where components use the same logon credentials” on page 98](#)

Use the password tool to change the password for IBM Spectrum Control when it is installed on a single server and the Common User and the Db2 User are identical and use the same logon credentials. The credentials are usually `db2admin` on a Windows operating system or `db2inst1` on AIX and Linux operating systems.

[“Multiple-server installation where Db2 is remote” on page 102](#)

Use the password tool to change the passwords for IBM Spectrum Control when the IBM Spectrum Control database repository and the IBM Spectrum Control servers are installed on different servers.

Related reference

[“Stopping the IBM Spectrum Control servers by using scripts” on page 90](#)

Run scripts to stop the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems.

[“Changing passwords on Windows systems from the Command Line Interface \(CLI\)” on page 104](#)

Use the `changepasswords.bat` script to change the stored passwords of the user IDs used by IBM Spectrum Control.

Multiple-server installation where Db2 is remote

Use the password tool to change the passwords for IBM Spectrum Control when the IBM Spectrum Control database repository and the IBM Spectrum Control servers are installed on different servers.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has Db2 and the IBM Spectrum Control database repository installed. *Server B* has the IBM Spectrum Control servers installed.

Before you use the password tool, ensure that you know the existing passwords that you want to change. Stop the IBM Spectrum Control servers on *Server B*.

Use the following steps to change the passwords in the Windows, Linux, or AIX operating system on *Server A* and *Server B*. Then, use the IBM Spectrum Control password tool on *Server A* and *Server B* to update IBM Spectrum Control to use the new passwords.

To change a password in the Windows operating system, follow these steps:

1. Open the Control Panel.

For more information, see [“Accessing administration tools”](#) on page 140.

- a) Select **User Accounts** and click **Change account type**.
- b) Select the user account of the password that you want to change.
- c) Select **Change password**.
- d) Enter and confirm the new password and click **Change password**.

If the password for the Windows domain user ID that you used as the IBM Spectrum Control Common User expired, change that password in the Windows domain before you continue. If you see the following error or a similar error after you run the password tool, verify that the password for your Common User Windows domain user ID did not expire:

```
com.tivoli.itsrm.tools.changepasswords.ChangePasswords error  
SEVERE: The DB2 password is invalid.
```

If necessary, change the Common User Windows domain password and run the password tool again.

To change a password in the AIX or Linux operating system, follow these steps:

2. Log in as the root user.
 - a) Run the following command:

```
passwd username
```

Where *username* is the user whose password you want to change.

- b) Enter the new password and confirm that new password is correct.

To use the IBM Spectrum Control password tool to update IBM Spectrum Control to use the new passwords, follow these steps:

3. On *Server A*, open a command prompt and change the directory to the following directory:

Windows operating systems

```
Spectrum_Control_Installation_dir\service
```

Linux or UNIX operating systems

```
Spectrum_Control_Installation_dir/service
```

4. On *Server A* start the password tool by running the following command:

- For Windows operating system:

```
changepasswords.bat
```


- For Linux or AIX operating system:

```
changepasswords
```

5. Select **Change DB2 password** and click **OK**.
6. Enter and confirm the same new password as you entered when changing the Db2 User's password in the operating system in Step 1 or Step 2. Verify that the **Restart servers** option is selected.
7. Click **OK**.
8. In the **Confirm password change** window, click **Yes**.
9. When the process is completed, click **Back to Main**.
10. Click **Exit Program**.
11. On *Server B*, open a command prompt window and change the directory to the following directory:

Windows operating systems

```
Spectrum_Control_Installation_dir\service
```

Linux or UNIX operating systems

```
Spectrum_Control_Installation_dir/service
```

12. On *Server B* start the password tool by running the following command:
 - For Windows operating system:


```
changepasswords.bat
```
 - For Linux or AIX operating system:


```
changepasswords
```
13. To change the Common User's password in IBM Spectrum Control on *Server B*, do the following in the password tool:
 - a) Select **Change IBM Spectrum Control Passwords** and click **OK**.
 - b) Enter and then confirm the same new password that you entered when you changed the Common User's password in the operating system in Step 1 or Step 2.
 - c) Click **OK**.
 - d) In the **Confirm password change** window, click **Yes**.
 - e) When the process is completed, click **Back to Main**.
14. To change the Db2 User's password in IBM Spectrum Control on *Server B*, do the following in the password tool:
 - a) Select **Change DB2 password** and click **OK**.
 - b) Enter and confirm the same new password as you entered when you changed the Db2 User's password in the operating system on *Server A* in Step 1 or Step 2. Verify that the **Restart servers** option is selected.
 - c) Click **OK**.
 - d) In the **Confirm password change** window, click **Yes**.
 - e) When the process is completed, click **Back to Main**.
15. Click **Exit Program**.

Tip: To verify that the password changes were successful, review the log file that is located in the `Spectrum_Control_installation_dir\service\log` directory.

Related tasks

[“Single server installation where components use the same logon credentials” on page 98](#)

Use the password tool to change the password for IBM Spectrum Control when it is installed on a single server and the Common User and the Db2 User are identical and use the same logon credentials. The

credentials are usually *db2admin* on a Windows operating system or *db2inst1* on AIX and Linux operating systems.

[“Single-server installation where components use different logon credentials” on page 100](#)

Use the password tool to change the passwords for IBM Spectrum Control when it is installed on a single server and the Common User and the Db2 User are different and use different logon credentials.

Related reference

[“Stopping the IBM Spectrum Control servers by using scripts” on page 90](#)

Run scripts to stop the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems.

[“Changing passwords on Windows systems from the Command Line Interface \(CLI\)” on page 104](#)

Use the `changepasswords.bat` script to change the stored passwords of the user IDs used by IBM Spectrum Control.

Changing passwords on AIX and Linux systems using the Command Line Interface (CLI)

Use the `changepasswords_noX.sh` script to change the passwords for IBM Spectrum Control on an AIX or Linux server that does not have the X Windows System installed.



Attention: It is recommended that you use the GUI password tool. However, if you use the non-GUI password tool for future updates, then *do not* use the GUI password tool to update your passwords on the same system at a later time or the IBM Spectrum Control servers might not operate properly.

Before you use the `changepasswords_noX.sh` script, ensure that you know the existing passwords that you want to change. Stop the IBM Spectrum Control servers.

Use the following steps to change the Db2 password in the Windows, AIX, or Linux operating systems. Then, use the IBM Spectrum Control `changepasswords_noX.sh` script to update the IBM Spectrum Control servers to use the new passwords.

To change a password in the AIX or Linux operating system, follow these steps:

1. Log in as the root user.
 - a) Run the following command:

```
passwd username
```

Where *username* is the user whose password you want to change.

- b) Enter the new password and confirm that new password is correct.

To use the IBM Spectrum Control `changepasswords_noX.sh` script to update the IBM Spectrum Control servers to use the new passwords, follow these steps:

2. Open a command prompt and change the directory to the following directory:

```
Spectrum_Control_Installation_dir/service
```

3. Start the `changepasswords_noX.sh` script by running the following command:

```
./changepasswords_noX.sh
```

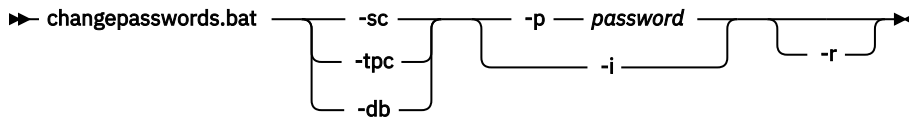
4. Enter the corresponding option for the password that you want to change: `tpc` or `db`.
5. Enter the same new password that you entered when you changed the user password in the operating system in Step 1.
6. When you are finished using the `changepasswords_noX.sh` script, enter `quit` in the prompt window.

Changing passwords on Windows systems from the Command Line Interface (CLI)

Use the `changepasswords.bat` script to change the stored passwords of the user IDs used by IBM Spectrum Control.

Before you use the `changepasswords.bat` to update the passwords in IBM Spectrum Control, you must change the passwords for the user IDs on the Windows operating system.

Note: The `changepasswords.bat` file is located in the `installation_dir/service` directory.



Required Parameters:

-sc OR -tpc

Changes the password stored for the user ID for IBM Spectrum Control.

-db

Changes the password stored for the database administrator user ID.

-p

Enter the new password.

-i

The new password is read from standard input, that is, you enter the password when prompted by the `changepasswords.bat` script.

Optional Parameters:

-r

Restart the IBM Spectrum Control server services.

Granting local administrative privileges to a domain account

Automatically grant administrative privileges to Windows domain accounts. The user account for the Storage Resource agent requires local administrative rights. Because these rights are not necessarily guaranteed for domain users in a Windows domain environment, you are shown how to grant local administrative rights to domain users. Using this procedure, you do not have to manually process each machine in the domain.

Note: These steps are for a Windows system that is a member of a Windows domain and not for the Windows Domain Primary Domain Controller.

To use Group Policy to grant local administrative privileges to a domain account, complete the following steps:

1. On the domain controller, go to **Administrative Tools > Active Directory Users and Computers** (you must be running with Domain Administrator privileges).
2. Right-click on the Organizational Unit (OU) upon which you want to apply the Group Policy. Click **Properties**.
3. The Group Policy Properties panel is displayed. Select the Group Policy tab and click **New** to create a Group Policy.
4. Designate a name for the new Group Policy. Select the new Group Policy and click **Edit**.
5. The Group Policy Object Editor panel is displayed. Go to **New Group Policy Object your_policy > Computer Configuration > Windows Settings > Security Settings > Restricted Groups**. Right-click **Restricted Groups**, and then click **Add Group**.
6. For example, name the new group Administrators. Under Properties, add the user Administrator, and the domain accounts or groups upon which you want the Group Policy in effect for. For example, you can add TPC\storageadmin, TPC\storagegroup, and TPC\TestGroup. Click **OK**.
7. Add these user rights to the domain account:
 - Act as part of the operating system
 - Log on as a service

In the Group Policy Object Editor, go to **New Group Policy Object *your_policy* > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignments**. In the content pane, select "Log on as a service" and double-click. Add the domain user for whom you are granting user rights and click **OK**. Repeat this step for "Act as part of the operating system."

8. The group policy is now enforced for the Organizational Unit to include the domain accounts and groups specified under the local Administrators group on each computer in the Organizational Unit. In addition, the domain user has been granted the necessary rights. To verify the user rights, log in to a domain computer and open the Computer Management console. Select **Groups**, double-click the Administrators group, and verify the membership of the domain users.

Collecting diagnostic information about IBM Spectrum Control

You can use the service tool to collect diagnostic information about IBM Spectrum Control. The tool detects the system configuration, collects the applicable information, and creates a compressed file that can be sent to IBM Software Support.

Related tasks

[“Creating a compressed file for a Storage Resource agent ” on page 109](#)

Run the service tool on Storage Resource agents that were deployed by using the web-based GUI to create a compressed file that can be sent to IBM Software Support.

[“Collecting service logs for IBM Software Support troubleshooting” on page 108](#)

Run the service tool to create a compressed file of service logs that can be sent to IBM Software Support for problem determination.

Related reference

[“Service tool overview” on page 106](#)

The service tool collects information from all installed IBM Spectrum Control components. The tool detects the system configuration, collects the applicable information, and creates a compressed file that can be sent to IBM Software Support.

[“How to customize the service tool” on page 110](#)

The default behavior of the service tool is to collect data about all IBM Spectrum Control components, but you can use the service tool to collect data about specific components. You can also use command-line parameters to specify a location to place the data that is collected, specify that the data is compressed, or to specify both.

Service tool overview

The service tool collects information from all installed IBM Spectrum Control components. The tool detects the system configuration, collects the applicable information, and creates a compressed file that can be sent to IBM Software Support.

The service tool collects the following information:

- Host name
- IP address and configuration information
- Operating system and version. On the Windows operating system, a `msInfo.txt` report is also generated
- Java home, version, and class path
- Java Virtual Machine (JVM) implementation name and version
- Protocol statistics
- Internet Protocol network connections for IBM Spectrum Control, including listening ports
- Diagnostic information about the system and its services
- Listing of all library files, for example, server and library and agent and library
- HOSTS file
- IBM Spectrum Control version and license files

When the service tool is run on the system where the Data server or the Device server are installed, it also collects the following information:

- For the Data server, information about all of the remote and local graphical user interfaces (GUIs) that are associated with it
- For the Export server, information about this component configuration and logs
- For the Device server, Alert server, and web server, information about their profiles in IBM WebSphere Application Server Liberty
- For the Data server, Device server, Alert server, web server, and data collector - all Javacore files, the most recent Java heap dump file, and the most recent snap trace file.

The service tool can collect Java core dump files for these IBM Spectrum Control components, but it *does not* by default. The values for the **javaCoreFiles**, **heapDumpFiles**, **snapFiles**, and **coreFiles** parameters in the `installation_dir/service/service.properties` file dictate which types of files and how many of each file type are collected by the service tool.

- All applied interim fixes
- Installation logs
- The contents of the `log` and `logs` directory, including subdirectories
- The contents of the `conf` and `config` directory
- Directory listing of the `lib` and `bin` directory
- The contents of the `log` and `conf` subdirectories of the web directory
- For the IBM Spectrum Control GUI, information about its profile in the embedded WebSphere Application Server Liberty
- Information from the **ipconfig /all** command on Windows operating systems
- Information from the **ipconfig -a** command on Linux and AIX operating systems
- Information from the **netstat -an** command on all operating systems

When the service tool is run on the system where the database repository is installed, it also collects the DB2 support information.

When the service tool runs on the Storage Resource agent computer, it collects the following information:

- All applied interim fixes
- Everything in the `config`, `log`, `nls`, `output`, and `service` directories, including subdirectories
- Everything in the `opt/IBM/CAP` directory on Linux and AIX operating systems
- Directory listing of the `ProgramData\Application Data\IBM\CAP` directory on Windows operating systems
- Directory listing of the `agent` directory
- Directory listing of the `bin` directory
- Listing of version numbers for the Storage Resource agent component
- Information from the **ipconfig /all** command on Windows operating systems
- Information from the **ifconfig -a** command on Linux and AIX operating systems
- Information from the **netstat -an** command on all operating systems

By default, the service data is collected in one of the following directories:

For Windows operating systems:

`installation_dir\service\data`

For Linux and AIX operating systems:

`installation_dir/service/data`

For more information about changing the default directory, see [“How to customize the service tool” on page 110](#).

You can run the service tool on IBM Spectrum Control regardless of whether you configured it on a single server or on multiple servers. The service tool automatically recognizes the installed components and collects service data about them. For more information about running the service tool for servers, see [“Collecting service logs for IBM Software Support troubleshooting” on page 108.](#)

Collecting service logs for IBM Software Support troubleshooting

Run the service tool to create a compressed file of service logs that can be sent to IBM Software Support for problem determination.

You must have administrator authority on Windows operating systems or root authority on AIX and Linux operating systems.

In order to run the service tool when you log in by using a Windows domain user account, you must grant Db2 SYSADM authority to that Windows domain user account.

To run the service tool when you log in by using a domain user account, choose one of the following methods:

- Right-click the `service.bat` file and select **Run as administrator**.
- Or
- Click **Start > All Programs > Open Administrative Tools > Local Security Policy**.
- On the **Local Security Policy** window, disable **User Account Control: Run all administrators in Admin Approval Mode**.
- Restart your computer.

The compressed file contains data about the following IBM Spectrum Control components: Alert server, Data server, Device server, Web server, Storage Resource agent, DB2, CLI, and installation.

You can customize the service tool to collect data about specific IBM Spectrum Control components.

To run the service tool for all components, follow these steps:

1. Log on to the system where IBM Spectrum Control is installed.
2. Go to the following directory:

Windows operating systems:

`installation_dir\service\`

Linux or AIX operating systems:

`installation_dir/service/`

3. Run the following program:

Windows operating systems:

`service.bat`

Linux or AIX operating systems:

`service.sh`

A compressed file, `SCServiceFiles_all.zip`, is created in the following directory:

Windows operating systems:

`installation_dir\service\data\`

Linux or AIX operating systems:

`installation_dir/service/data/`

Tip: You can customize the data that is collected by the service tool. For more information, see [“How to customize the service tool” on page 110.](#)

Related tasks

[“Creating a compressed file for a Storage Resource agent ” on page 109](#)

Run the service tool on Storage Resource agents that were deployed by using the web-based GUI to create a compressed file that can be sent to IBM Software Support.

Related reference

[“How to customize the service tool” on page 110](#)

The default behavior of the service tool is to collect data about all IBM Spectrum Control components, but you can use the service tool to collect data about specific components. You can also use command-line parameters to specify a location to place the data that is collected, specify that the data is compressed, or to specify both.

Creating a compressed file for a Storage Resource agent

Run the service tool on Storage Resource agents that were deployed by using the web-based GUI to create a compressed file that can be sent to IBM Software Support.

You must have administrator authority on Windows operating systems or root authority on AIX and Linux operating systems.

To run the service tool on the Storage Resource agents, complete the following steps:

1. In the menu bar, go to **Servers > Servers**.
2. Right-click the server where the Storage Resource agent is deployed, and select **Logs > Collect Agent Logs**.

The following compressed files are created:

Windows operating systems:

C:\Program Files\IBM\TPC\data\log\SRATraces*SRA_computer_name*
\SCServiceInfo.zip

AIX and Linux operating systems:

/opt/IBM/TPC/data/log/SRATraces/*SRA_computer_name*/SCServiceInfo.zip

where *SRA_computer_name* represents the name of the computer on which the Storage Resource agent is located.

If the compressed file cannot be created, a message indicates that the job was unsuccessful.

For more information about the error, see the server log file or the services script information file. The files are in one of the following default directories:

Server log file

This file is on the system where IBM Spectrum Control is installed:

Windows operating systems:

c:\Program Files\IBM\TPC\data\log

AIX or Linux operating systems:

/opt/IBM/TPC/data/log

Services script information file

This file is on the computer on which the Storage Resource agent is installed:

Windows operating systems:

c:\Program Files\IBM\TPC*SRA_computer_name*\services\SCServiceInfo.log

AIX or Linux operating systems:

/opt/IBM/TPC/*SRA_computer_name*/services/SCServiceInfo.log

For more information about customizing the data that is collected by the service tool, see [“How to customize the service tool” on page 110](#).

Related tasks

[“Collecting service logs for IBM Software Support troubleshooting” on page 108](#)

Run the service tool to create a compressed file of service logs that can be sent to IBM Software Support for problem determination.

How to customize the service tool

The default behavior of the service tool is to collect data about all IBM Spectrum Control components, but you can use the service tool to collect data about specific components. You can also use command-line parameters to specify a location to place the data that is collected, specify that the data is compressed, or to specify both.

Specifying help and output command-line parameters

To obtain information about the service tool usage, use the **-help** command-line parameter.

To specify the data that is collected by the service tool, use the following command-line parameters when you run service tool:

-output *directory_path*

Places the files that contain the data that was collected in a directory that you specify. If you specify a directory that does not exist on your system, that directory is created. If you do not use the **-output *directory_path*** parameter, the files are placed in the default directory:

Windows operating systems

installation_dir\service\data

Linux or AIX operating systems

installation_dir/service/data

Restriction: If you specify a directory, the directory path cannot contain spaces. This restriction refers to the **-output** option.

-pmr

The number of the PMR to which the support information is related. Use the following format to enter the number: nnnnn, nnn, nnn where n represents a number, such as 12345, 123, 123. If you enter a value for the **-pmr** parameter, the service tool automatically uses FTP to upload the service information to IBM. If the service tool cannot upload the service information to IBM from the IBM Spectrum Control server, the generated file must be uploaded manually. The **-pmr** parameter is ignored if the **-nozip** parameter is used.

-nozip

When you use this parameter, the compressed collected data archives are no longer created. The service tool creates separate directories for each component for which data was collected. You can then create compressed archives for the collected files. In this way, you can control the size and content of each compressed file. To specify a directory other than the default directory, use the **-output *directory_path*** parameter.

Tip: You can specify more than one parameter, for example, C:\Program Files\IBM\TPC\service>service **-install -nozip**.

Specifying Javacore, Java heap dump, snap trace, and Java core dump file collection

By default, the service tool collects all Javacore files, the most recent Java heap dump file, and the most recent snap trace file for the Data server, Device server, Alert server, web server, and data collector. The service tool can collect Java core dump files for these IBM Spectrum Control components, but it *does not* by default. You can edit the following parameters in the *installation_dir*/service/service.properties file in order to control which types of files and how many of each file type are collected by the service tool:

coreFiles=0

Specifies how many Java core dump files are collected. The default value is 0 because Java core dump files are generally very large. The valid values for this parameter are 0 or a positive integer. Any other value results in the default behavior.

javaCoreFiles=-1

Specifies how many Javacore txt files are collected. The default value of -1 means that all Javacore txt files are collected. The valid values for this parameter are 0 or a positive integer. Any other value results in the default behavior.

heapDumpFiles=1

Specifies how many Java heap dump files are collected. The default is to collect the most recent Java heap dump file. The valid values for this parameter are 0 or a positive integer. Any other value results in the default behavior.

snapFiles=1

Specifies how many snap trace files are collected. The default is to collect the most recent snap trace file. The valid values for this parameter are 0 or a positive integer. Any other value results in the default behavior..

Collecting data for specific IBM Spectrum Control components

You can use the service tool to collect data about specific IBM Spectrum Control components.

Use the following parameters to specify the components:

-all

All components. The default behavior is to collect data about all components.

-install

Installation component files.

-data

Data server component files.

-device

Device server component files.

-datacollector

Data collector component files.

-alert

Alert server component files.

-export

Export server component files.

-sra

Storage Resource agent component files.

-db

Db2 files.

-cli

Command-line interface files.

-gui

Collects data about GUI files.

If you collect information about a particular component, and you do not specify the **-nozip** parameter, you can identify the contents of a compressed service file from its name. For example, if you specify the **-db -gui** parameters but did not specify the **-nozip** parameter, a file named `SCServiceFiles_db_gui.zip` is created.



Warning: An existing compressed file is overwritten when another file of the same name is created. For example, if you run `C:\Program Files\IBM\TPC\service>service -db -gui`, a file named `SCServiceFiles_db_gui.zip` is created. If you rerun the tool with the same component options, a new file named `SCServiceFiles_db_gui.zip` is created. This new file overwrites the previously created file unless you specify the **-nozip** parameter, or use the **-output** parameter to specify a different path.

If you specify the **-nozip** parameter, a directory is created for the components that you specified in the parameter. If you did not specify a specific component, data is collected for all installed components, and the data is placed in files in the following directory:

Windows operating systems:

installation_dir\service\data

Linux or AIX operating systems:

installation_dir/service/data

Files for particular components are then placed in a directory that corresponds to that component. Common files, such as `license.txt`, are placed in the following directory:

Windows operating systems:

installation_dir\service\data

Linux or AIX operating systems:

installation_dir/service/data

Restriction: You cannot specify a specific component as a command-line parameter when you specify the **-all** parameter. Also, when you specify a component that is not installed on the computer, the service tool displays an error message.

Administering the IBM Spectrum Control database

The IBM Spectrum Control database is the repository for information that is collected about the monitored resources in your environment.

Backing up the database

Choose and then implement the Db2 backup method for securing the data that is collected and stored in the database for IBM Spectrum Control.

Backup types

To back up your database, choose one of the following options:

Offline (Default)

When the data is being backed up, you can neither access nor connect to the database.

Online

When the data is being backed up, you can access and connect to the database. Unlike the offline option, the database remains available to you and the applications that use the database. To configure this option, requires a good knowledge of Db2.

Output locations

To specify the location of the data that is backed up, choose one of the following options:

File system (Default)

Back up the data on a file system.

You can copy the file system that you specified to a removable tape or use IBM Spectrum Protect to back up the file system.

IBM Spectrum Protect

Back up the data to IBM Spectrum Protect. To back up the data, use IBM Spectrum Protect Backup/Archive client and client API on the same computer that hosts the IBM Spectrum Control Db2 databases.

Logging types

In the event of a system failure, the log files are used to recover data. You can choose either circular logging or archive logging.

The types of logging are:

Circular (Default)

This type of logging is used with IBM Spectrum Control for an offline backup.

Archive

This type of logging is used with an online backup. With archive logging, you can enable a rollforward recovery of the database to a specific date and time. A good knowledge of Db2 is needed to manage this type of logging.

Related concepts

[“Comparison of database backup methods” on page 113](#)

The method that you choose to back up your data determines whether IBM Spectrum Control remains online or offline during the backup process.

Related information

[Restore overview](#)

[Recover overview](#)

[IBM Redbook: IBM Tivoli Storage Productivity Center Beyond the Basics](#)

Comparison of database backup methods

The method that you choose to back up your data determines whether IBM Spectrum Control remains online or offline during the backup process.

Advantages of an offline backup

The advantages of the offline backup method are:

- The offline backup method is the default method and it is easier than the online method to configure and to maintain.
- The circular type of logging that is used for offline backups is easier to configure and maintain than the type of logging that is used for online backups.

Disadvantages of an offline backup

The disadvantages of the offline backup method are:

- You must stop IBM Spectrum Control when you back up the data. So data is not collected and your storage resources are not being monitored during the back up process.
- You cannot collect performance data for the disk subsystems and SAN fabrics when data is being backed up.
- You might miss critical events, for example, failures within a SAN fabric, that occur during the backup process.

Tip: To minimize the loss of data for your storage resources and to ensure that you do not miss critical events, back up your data when your storage resources are not being used or when storage usage is low.

Advantages of an online backup

The advantages of the online backup method are:

- You continue to collect data and monitor your storage resources during the backup process because you do not have to stop IBM Spectrum Control.
- You continue to receive alerts and can respond quickly to critical events at any time of day.
- You continue to collect performance data for your disk subsystems and SAN fabrics.

Disadvantages of an online backup

The disadvantages of the online backup method are:

- The archive type of logging that is used with this type of backup is a more advanced method; it requires a good knowledge DB2 operation and administration.
- Software upgrades to IBM Spectrum Control that involve changes to the layout of the database might not complete successfully. In such cases, you can use circular logging to ensure that the software upgrade succeeds. You can switch back to archive logging after the software upgrade is installed.

Related information

[DB2 documentation](#)

[IBM Redbook: IBM Tivoli Storage Productivity Center Beyond the Basics](#)

Backing up the database offline using the command line

By default, the IBM Spectrum Control database (TPCDB) is configured to use circular logging that requires backups to be performed offline. You can use the command line to perform the offline backup.

To back up the database using a command line, complete the steps 1-8. To back up the database using IBM Data Studio client, complete the tasks in step 10:

1. Close the IBM Spectrum Control GUI.
2. Stop the IBM Spectrum Control services.
For more information about how to stop the services, see [“Stopping the IBM Spectrum Control servers by using scripts”](#) on page 90.
3. On Windows operating systems, complete these steps to initialize the DB2 environment:
 - a) Open a command window.
 - b) Run the **db2cmd** command.

On Linux and AIX operating systems run the **db2profile** command.

Restriction: You must have DB2 administrator privileges to run these commands.

4. In the DB2 command window, run the **db2 force application all** command and the **db2 terminate** command to prevent all users or applications from accessing DB2.
5. In the DB2 command window, run the **db2 list applications** command to ensure that applications are not accessing DB2.
6. Create a directory to back up the DB2 output data.

Tip: Choose a directory location that has enough free space to hold the number of backups that you plan to retain. Use a separate file system rather than the file system that contains the DB2 database. You can choose to use a location that is a remotely mounted Common Internet File System (CIFS) or Network File System (NFS), so the backup data is secured to another server.

7. Run the backup command: `DB2 BACKUP DATABASE TPCDB USER user_name USING password TO location COMPRESS`

Where *user_name* is the user who owns the DB2 instance where the IBM Spectrum Control database is located, *password* is the password that is associated with that user name, and *location* is the directory (created in step 7) where the backup is stored.

Examples:

- Windows operating system: `DB2 BACKUP DATABASE TPCDB USER johndoe USING password1234 TO C:\DB_Backup COMPRESS`
 - Linux and AIX operating systems: `DB2 BACKUP DATABASE TPCDB USER johndoe USING password1234 TO /tmp/DB_Backup COMPRESS`
8. Restart the IBM Spectrum Control services.
For more information about how to start the services, see [“Starting the IBM Spectrum Control servers by using scripts”](#) on page 89. After the services are restarted, the backup is complete.

The offline database backup to a file system is run and the IBM Spectrum Control services are started again.

Related reference

[BACKUP DATABASE command](#)

Stopping the IBM Spectrum Control servers by using scripts

Run scripts to stop the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems.

Starting the IBM Spectrum Control servers by using scripts

Run scripts to start the IBM Spectrum Control servers on the Windows, Linux, or AIX operating systems.

Note: IBM Spectrum Control servers start automatically on all platforms when the operating system is started.

Related information

[IBM Data Studio documentation](#)

[DB2 documentation](#)

[IBM Redbook: IBM Tivoli Storage Productivity Center Beyond the Basics \(Chapter 3\)](#)

Backing up the database offline using IBM® Data Studio client

By default, the IBM Spectrum Control database (TPCDB) is configured to use circular logging that requires backups to be performed offline. You can use the IBM Data Studio client to perform the offline backup.

1. Stop the IBM Spectrum Control services.
2. Start the IBM Data Studio client.

To start the IBM Data Studio client from a command window, enter:

- On Windows operating system:

```
product_installation_directory\eclipse.exe
```

- On Linux operating system:

```
.product_installation_directory/eclipse
```

3. On the **New Connection** page, select **DB2 for Linux, UNIX and Windows** and configure your IBM Spectrum Control database connection parameters.
4. Click **Next**.
5. On the **Database Administration - IBM Data Studio** page, expand **DB2**.
6. Right-click **DB2** and select **TPCDB > Back Up and Restore > Back Up**.
7. On the **Back up TPCDB** page, confirm the details of your database.
8. Click **Backup Type**.
9. Click **Backup Image** and select **File System** as the media type.
10. Click **Backup Options**.
11. In the **Backup options compression and throttle** section, select the **Compress backup image** and **Throttle this utility to regulate the performance impact on the database workload** check boxes.
12. Click **Backup Performance**.
To accelerate the backup process, you can increase the number of table spaces and buffers.
13. After you have set all of the options, click **Run** or **Preview Command** to see the actual Db2 command that is run to backup the data.
14. Restart the IBM Spectrum Control services.

The offline database backup to a file system is run and the IBM Spectrum Control services are started again.

Backing up the database online using IBM® Data Studio client

You can use the online method to back up a IBM Spectrum Control database and ensure continuous availability of the database and the applications that use it.

When you use the online backup method, DB2 does not clean up old archive log files. You need to have processes in place to clean up the old log files after a specific amount of time to prevent the system from filling up. You also need to plan for the amount of space you might need. The log space that is required for a IBM Spectrum Control database can grow larger than the DB2 database over period of time.

To backup the database, complete these steps:

1. Open IBM Data Studio client.
2. Start the IBM Data Studio client.

To start the product from a command window, enter:

- On Windows operating system:

```
product_installation_directory\eclipse.exe
```

- On Linux operating system:

```
.product_installation_directory/eclipse
```

3. On the **New Connection** page, select **DB2 for Linux, UNIX and Windows** and configure your IBM Spectrum Control database connection parameters.
4. Click **Next**.
5. On the **Database Administration - IBM Data Studio** page, expand **DB2**.
6. Right-click **DB2 for Linux, UNIX and Windows** and select **TPCDB > Set Up and Configure > Configure Database Logging**.
7. On the **Configure Database Logging TPCDB** page, click **Logging Type** and select **Archive**.
8. Click **Logging Size** and enter your log file size information. For example, 2500.
9. Click **Log Location** and enter the DB2 log path information.
10. On the **Database Administration - IBM Data Studio** page, expand **DB2**.
11. Right-click **DB2** and select **TPCDB** and select **Back Up and Restore > Back Up**.
12. Click **Backup Image** and select **File System** as the media type.
13. Click **Backup Options**.
14. In the **Backup options compression and throttle** section, select the **Compress backup image** and **Throttle this utility to regulate the performance impact on the database workload** check boxes.
15. Click **Backup Performance**.
You can increase the number of table spaces and buffers, from the default values, to improve performance.
16. After you set all of the options, click **Run** or **Preview Command** to see the actual DB2 command that is run as part of the backup.

The online database backup to a file system is run and the backup is complete.

Tip: You can also perform an online backup of the IBM Spectrum Control databases to a Tivoli Storage Manager server. The significant difference between online and offline backup is the need to enable archive logging on the databases. When you use the online method, it provides many backup and recovery benefits at the expense of increased complexity in the database operation. Set up and test your DB2 to Tivoli Storage Manager integration before you implement the online method to the Tivoli Storage Manager output destination to verify the communication is working properly.

Related information

[IBM Data Studio documentation](#)

[DB2 documentation](#)

[IBM Redbook: IBM Tivoli Storage Productivity Center Beyond the Basics](#)

Restoring the database

To restore the IBM Spectrum Control database (TPCDB), use the IBM Data Studio client.

Download and install the IBM Data Studio client. For more information about how to download and install the IBM Data Studio client, see <http://www.ibm.com/developerworks/downloads/im/data/>.

Before you can use the IBM Data Studio client to restore the IBM Spectrum Control database, you must add a connection to the database in the IBM Data Studio client.

Restriction:

Do not restore the IBM Spectrum Control database from one version of IBM Spectrum Control into another version. For example, do not restore a backup from IBM Spectrum Control 5.2.14 into 5.2.15, or any other version.

1. Stop the IBM Spectrum Control services.
2. Start the IBM Data Studio client.
3. Click the **Administer** tab in the **Data Studio client Task Launcher**, then click **Connect and browse a database**.
4. On the **Connection Parameters** page, click **DB2 for Linux, UNIX, and Windows** and configure your IBM Spectrum Control database connection parameters.
5. Click **Next**.
6. On the **Database Administration - IBM Data Studio** page, expand **DB2**.
7. Right-click **TPCDB**, then click **Back Up and Restore > Restore**.
8. On the **Restore Database TPCDB** page, click **Restore backup to the current database** to set the restore type.
9. Click **Restore Objects**, and then click **Restore the entire database**.
10. Select the backup image that you want to restore.
11. On the **Restore Database TPCDB** page, click **Run**.
12. Restart the IBM Spectrum Control services.

Related tasks

[Starting the IBM Data Studio full client](#)

You can start the Data Studio full client on your workstation from either a menu option or the command line.

Related information

[IBM Data Studio documentation](#)

[DB2 documentation](#)

Disaster recovery

Back up your database regularly to be prepared for disaster recovery if a disaster event occurs.

Disaster recovery is the rebuilding of a database or table space after a disaster event such as media or storage failure, power interruption, or application failure occurs. If a disaster event occurs and a database or table space is damaged or corrupted, you can restore one of your backups.

Related tasks

[Restoring the database](#)

To restore the IBM Spectrum Control database (TPCDB), use the IBM Data Studio client.

Related reference

[Backing up the database](#)

Choose and then implement the Db2 backup method for securing the data that is collected and stored in the database for IBM Spectrum Control.

Related information

[Data recovery](#)

Maintaining and improving the performance of the database

You can use the database maintenance tool to calculate statistics for the IBM Spectrum Control database. The tool can also reorganize the database to restore efficiency and improve performance.

By default, the database maintenance tool runs the Db2 **runstats** command on all database tables that are used by IBM Spectrum Control. By using the **runstats** command, the database maintenance tool updates statistics about the characteristics of a table and its associated indexes. Because Db2 uses the statistics to determine access paths to data, when you run the database maintenance tool you help to ensure the effectiveness of the paths that are selected.

By specifying an option of the database maintenance tool, you can instruct the tool to reorganize the database tables, if necessary. A set of formulas are applied to the statistics that were collected about the database to determine if reorganization is necessary. Tables are reorganized by reconstructing rows to eliminate fragmented data and by compacting information. Index data is reorganized into unfragmented, physically contiguous pages.

You can customize the reorganization function in the database maintenance tool by updating a properties file. Properties determine which formulas can trigger database reorganization. You can specify properties that exclude tables from being reorganized based on size. Also, you can specify a property to force database reorganization.

Updating database statistics

Use the database maintenance tool to update statistics about the databases that are used by IBM Spectrum Control. Because DB2 uses these statistics to select access paths to data, when you run the database maintenance tool, you can help to improve the effectiveness of the paths that DB2 selects.

Run the database maintenance tool to make substantial changes to the IBM Spectrum Control database, such as numerous table space updates, deletions, or insertions. The database maintenance tool uses the **RUNSTATS** command to update statistics about the physical characteristics of a table and the associated indexes.

Note:

The database maintenance script for updating statistics for IBM Spectrum Control can be run online or offline.

To update statistics for databases, follow these steps:

1. Log on to the computer where you installed IBM Spectrum Control.
2. Change the directory.

Linux and UNIX operating systems

```
/opt/IBM/TPC/data/server/tools/
```

Windows operating systems

```
C:\Program files\IBM\TPC\data\server\tools\
```

3. Enter the following command to run the database maintenance tool:

Linux and UNIX operating systems

```
runTPCDBMaintenance
```

Windows operating systems

```
runTPCDBMaintenance.bat
```

Note: To monitor the progress of a statistical update for the database, redirect your output to a file.

```
runTPCDBMaintenance > /tmp/tpcdb_update_stats.txt
```

Reorganizing database tables

Use the database maintenance tool to analyze the database tables that are used by IBM Spectrum Control. If necessary, the database maintenance tool reorganizes the database tables and indexes.

The database maintenance tool uses a set of formulas to analyze the physical location of rows, and the size of the tables; it analyzes the indexes and their relationship to the table. If the calculated result of a formula exceeds set boundaries, the tool reorganizes the tables and indexes as needed. The tool reorganizes database tables, if necessary, by reconstructing rows to eliminate fragmented data. The tool reorganizes index data, if necessary, into unfragmented, physically contiguous pages.

Tips:

- Run the database maintenance script for analyzing database tables while IBM Spectrum Control is offline; no database workload is present.
- Ensure that you have enough available space to reorganize the database tables. An offline reorg might require an amount of available space that is 2 to 3 times the size of the existing IBM Spectrum Control tables.

To analyze and reorganize databases, follow these steps:

1. Log on to the computer where you installed IBM Spectrum Control.
2. Change the directory.

Linux and UNIX operating systems

`/opt/IBM/TPC/data/server/tools/`

Windows operating systems

`C:\Program files\IBM\TPC\data\server\tools\`

3. Enter the following command to run the database maintenance tool to analyze and reorganize databases:

Linux and UNIX operating systems

`runTPCDBMaintenance reorg`

Windows operating systems

`runTPCDBMaintenance.bat reorg`

```
runTPCDBMaintenance reorg > /tmp/tpcdb_reorg.txt
```

Note: To monitor the progress of the database reorganization, redirect your output to a file.

Customizing the reorganization function of the database maintenance tool

You can customize the database maintenance tool to specify which formulas determine whether a database is reorganized.

To specify which formulas can trigger a database reorganization, edit the properties in the `TPCDBMaintenance.properties` file. For example, you can customize the tool to ignore tables that are smaller or larger than the defined size limits, or customize it to always reorganize the database.

To analyze and reorganize databases, follow these steps:

1. Log on to the system where IBM Spectrum Control is installed.
2. Change to the following directory:

Linux and UNIX operating systems

`/opt/IBM/TPC/data/server/tools/`

Windows operating systems

`C:\Program files\IBM\TPC\data\server\tools\`

3. Open `TPCDBMaintenance.properties` in a text editor and modify the property settings as needed.

The f1-f8 properties all refer to the same formulas that are used by the DB2 **REORGCHK** command. For more information about any of these formulas, see the DB2 product documentation about the

REORGCHK command at <http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

You can modify the following properties:

f1= {true | false}

Specifies whether the result of formula 1 can trigger a database table reorganization. Formula 1 checks the number of overflow rows in a table.

f2= {true | false}

Specifies whether the result of formula 2 can trigger a database table reorganization. Formula 2 checks the effective space utilization of data pages.

f3= {true | false}

Specifies whether the result of formula 3 can trigger a database table reorganization. Formula 3 checks the number of empty pages. Pages can become empty after rows are deleted.

f4= {true | false}

Specifies whether the result of formula 4 can trigger the reorganization of index data. Formula 4 checks the clustering ratio of an index.

f5= {true | false}

Specifies whether the result of formula 5 can trigger the reorganization of index data. Formula 5 checks the space that is reserved for index entries.

f6= {true | false}

Specifies whether the result of formula 6 can trigger the reorganization of index data. Formula 6 determines whether re-creating an index would result in a tree with fewer levels.

f7= {true | false}

Specifies whether the result of formula 7 can trigger the reorganization of index data. Formula 7 checks the number of pseudo-deleted RIDs on non-pseudo-empty pages.

f8= {true | false}

Specifies whether the result of formula 8 can trigger the reorganization of index data. Formula 8 checks the number of pseudo-empty leaf pages.

maxReorgTableSize= {size_in_bytes | none}

Specifies the maximum size that a database table must be to be considered for reorganization.

minReorgTableSize= {size_in_bytes | none}

Specifies the minimum size that a database table must be to be considered for reorganization.

forceReorg= {true | false}

Specifies whether the database is always reorganized by the database maintenance tool when the `reorg` argument is specified. If this property is set to `true`, all other properties in the file are ignored.

4. Save `TPCDBMaintenance.properties`.

Repository copy tool

You can use the Repository copy tool, **repocopy**, to export all the tables in the IBM Spectrum Control database repository for purposes of debugging problems.

You can send the exported data to IBM Software Support to help debug problems.

Tip: If you want to export only performance data from the IBM Spectrum Control repository, you can create performance support packages. You can create performance support packages for storage systems or fabrics. For more information about exporting performance support packages, see [Exporting performance data for storage systems and fabrics](#).

Exporting repository data

Use the Repository copy tool to export data from an existing repository into a text file.

To export repository data, follow these steps:

1. Go to the following default directory:

Windows operating systems:

`c:\Program Files\IBM\TPC\data\server\tools`

Linux or AIX operating systems:

`/opt/IBM/TPC/data/server/tools`

2. Issue the **repocopy** command:

Windows operating systems:

repocopy.bat

Linux or AIX operating systems:

repocopy.sh

3. Select **Export data from repository tables** and click **Next**.
4. In the **Options for Import/Export** window, enter information in the following fields:

Directory for Export

Enter the directory where the comma-delimited file is saved.

Delimiter

Enter a delimiter for the delimited file format (a comma is the default).

Quote

Enter the symbol that contains string data (double quotation marks is the default).

IBM Spectrum Control exports the data into the comma-delimited file that you specify, and places it in a file named *tablename.txt*. Click **Next**.

5. Select one of the following options and click **Next**.

- Export by using DB2 native format.
- Export by using text files (the preferred method).

6. Select one of the following options and click **Next**.

- Export base tables (always export the base tables)
- Export Performance Manager tables, if requested by IBM Software Support
- Export history tables that are used for Tivoli Storage Productivity Center for Data history reports, only if requested by IBM Software Support

The information that is detected in the `server.config` file is displayed in the **Connection Properties** window within the following fields:

- Database Types
- User name
- Password
- Driver Class
- Driver URL
- Database
- DB Creator
- Classpath

If you want to export data from a different database from the one listed in the `server.config` file, you can select the database from the **Database Types** list box. Manually enter the database information.

7. Click **Finish**.

8. Click **Run**.

As you progress through the export process, messages are written to a progress log that is displayed. You can track the steps through the progress log.

When the **repocopy** command is used with a remote database, the DB2 shared library is not available for loading the `libTSRMinsudb.so` file. You can ignore this message. Click **OK** and continue.

Administering Db2

Administer IBM® Db2® by backing up the IBM Spectrum Control database, starting the IBM Data Studio full client, and starting and stopping Db2®.

Using the command line on UNIX and Linux

This topic describes how to use a command line to perform actions against a IBM® Db2® instance under UNIX or Linux.

If the Db2 Control Center is unavailable or you do not have access to a graphical user interface, you can use a command line to execute Db2 commands such as starting and stopping an instance.

Important: If you are using DB2 Version 10.1 or higher, you must use the command-line interface.

To use a command line to perform actions against an instance of Db2, complete the following steps:

1. Log in with a user ID or name that has ROOT, SYSADM, SYSCTRL, or SYSMAINT authority on the instance; or log in as the instance owner.

2. Run the startup script:

- For Bourne or Korn shell, type: **. HOME/sqlllib/db2profile.**
- For C shell, type: **source HOME/sqlllib/db2cshrc.**

where HOME is the home directory of the instance you want to use.

3. To start the instance using the command line, type **db2start**.

Note: When you run commands to start the database manager instance, the Db2 database manager applies the command to the current instance.

4. To stop the instance using the command line, type **db2stop**.

Note: When you run commands to stop the database manager instance, the Db2 database manager applies the command to the current instance.

Manually starting Db2 on Windows

Start IBM® Db2on Windows operating systems.

To start Db2 manually, complete the following steps:

1. Start the following Windows services:

- DB - DB2-0
- DB2DAS - DB2DAS00
- DB2 JDBC Applet Server
- DB2 License Server
- DB2 Security Server

2. Open a Db2 command window.

3. From the Db2 Command window, run the **db2start** command.

Manually stopping Db2 on Windows

Stop IBM® Db2® manually on Windows.

1. Stop the following Windows services:

- DB2 Security Server
- DB2 License Server
- DB2 JDBC Applet Server
- DB2DAS - DB2DAS00
- DB2 - DB2-0

Note: When you stop the **DB2 Security Server** service, you are prompted to stop the Warehouse logger and Warehouse Serve. Click **Yes**.

2. To open a Db2® command window, click **Start > Programs > IBM DB2 > Command Line Tools > Command Window**.

3. From the **Db2 Command** window, issue the **db2stop** command.

To restart Db2, issue the **db2start** command from the **Db2 Command** window. Before you can issue the command, you must first start these services on the Windows Services panel:

```
DB2 - DB2-0
DB2DAS - DB2DAS00
DB2 JDBC Applet Server
DB2 License Server
DB2 Security Server
```

Starting the IBM Data Studio full client

You can start the Data Studio full client on your workstation from either a menu option or the command line.

Opening IBM Data Studio Administration client on Windows operating systems

1. Choose one of these options:

Option	Description
Windows Server 2012	<ol style="list-style-type: none">a. On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start.b. On the Start page, right-click, and then click the All apps taskbar button.
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start > All Programs .

2. Click **IBM Data Studio > Data Studio Administration Client**.

Open IBM Data Studio Administration client on Linux and AIX operating systems

On the command line, issue the following command:

```
DS_install_dir/eclipse
```

where DS_install_dir is the directory where you installed the full client.

/opt/IBM/DS3.1.1/eclipse

Monitoring Db2

The minimum user authority level needed for monitoring IBM® Db2® instances is a user with Db2® system maintenance authority (SYSMAINT).

To check and set SYSMAINT authority, follow these steps:

1. Run this command in the Db2 command prompt window to check to see if there is an operating system user group defined to have SYSMAINT authority:

```
db2 get dbm cfg
```

In the output file, look for this information:

```
SYSADM group name      (SYSADM_GROUP) =  
SYSCTRL group name    (SYSCTRL_GROUP) =  
SYSMAINT group name   (SYSMAINT_GROUP) =  
SYSMON group name     (SYSMON_GROUP) =
```

If the setup for the operating system group has not been done, you do not see a value set.

If the setup has been done, this example shows what you can expect to see:

```
SYSADM group name      (SYSADM_GROUP) =  
SYSCTRL group name    (SYSCTRL_GROUP) =  
SYSMAINT group name   (SYSMAINT_GROUP) = ADMINISTRATORS  
SYSMON group name     (SYSMON_GROUP) =
```

In this example, the "ADMINISTRATORS" group has SYSMAINT_GROUP authority.

2. If the setup has been done, add the user you want to use to the ADMINISTRATORS group using the operating system utilities or use a user that already belongs to the ADMINISTRATORS group.

If you want to give a user group "SYSMAINT_GROUP" authority, follow these steps:

- a. If a user (for example `userA`) belongs to an operating system group called `db2monitor`, here is an example of setting the `db2monitor` group with `SYSMAINT` authority. From the Db2 command prompt window, run the following command:

```
db2 update dbm cfg using SYSMAINT_GROUP db2monitor
```

- b. After issuing the **db2 update** command, restart Db2 by running the following command from the Db2 command prompt window or restarting the system:

```
db2 force application all
```

This command might need to be issued a few times to stop all the database connections.

- c. Run the following commands from the Db2 command prompt window:

```
db2stop  
db2start
```

- d. `UserA` can now monitor the Db2 database.

Appendix A. Reference

View reference information that is related to IBM Spectrum Control. Topics include information about alerts, fabrics, commands, configuration and log files, performance metrics, protocols, standards, and accessibility features.

Return codes used by Storage Resource agent

This topic lists the return codes used by the Storage Resource agent.

The following table lists the return codes used by the Storage Resource agent during installation, uninstallation, and upgrade.

Table 5. Storage resource agent return codes	
Return code	Explanation
1	There is a problem uninstalling the Fabric agent. For more information about what caused the uninstallation to fail, check the uninstallation logs for the Fabric agent.
2	Command not valid.
3	Option provided is not valid.
5	Argument is not valid.
6	Missing value for argument (e.g. -installLoc <Value>, where <Value> is missing).
7	Missing localized string in message file.
8	Probe is running.
9	Failed to open file for write.
10	Failed to close file.
11	Logfile not specified.
19	Failed in tracing.
21	Cannot spawn a probe because it is busy.
30	This is an internal error in initializing tracing. Save the error message and error log and contact your service representative for assistance in resolving the error.
32	Invalid socket.
33	Start service failed.
34	Registry entry not found.
35	Deployment of the agent failed, error creating startup scripts.
36	File does not exist.
40	Missing upgrade files.
41	Failed to extract files in upgrade process.
42	Failed to stop probe in upgrade process.
43	Failed to stop Agent.
44	Failed to start Agent.

Table 5. Storage resource agent return codes (continued)

Return code	Explanation
45	Agent Registration to server failed.
46	File extraction needs more space.
47	Failed to open archive file.
48	Agent did not start after upgrade.
49	Installation directory not valid at upgrade time.
50	Probe is running.
51	Data file not found.
52	Exit code not in the output file.
53	Failed to send job status.
54	Failed to copy certificate files.
55	Failed to create directory.
56	Failed to remove directory.
57	Exec command failed.
58	Conversion of wide character failed.
59	Installation directory not valid.
60	Server name not defined.
61	Error in removing entries from configuration file.
62	Failed to stop probe at uninstall time.
63	Failed to remove registry entry at uninstall time.
64	Failed to remove service entry at uninstall time.
65	Failed to stop service at uninstall time.
66	Specified server name is not valid.
67	There is an error installing the Storage Resource agent as part of the migration process. For more information about what caused the installation to fail, check the installation logs for the Storage Resource agent.
71	Failed to spawn process.
73	Failed to spawn probe process.
101	Failed to create lock at installation time.
102	Failed to stop probe at re-installation time.
103	Failed to stop agent at re-installation time.
104	Failed to create registry at installation time.
105	Failed to extract files at installation time.
106	Failed to create entries in configuration file at installation time.
107	Failed to stop service at re-installation time.
108	Service already exists.

Table 5. Storage resource agent return codes (continued)

Return code	Explanation
109	Failed to create service.
110	Failed to start service.
111	Probe failed at installation time.
112	Creation of daemon failed.
113	Installation of GUID failed.
114	Commtype parameter is not valid.
115	Specified port is in use.
116	Installation/Upgrade does not have enough space.
117	Installation in progress.
118	Cannot get server name from Server.
119	Installation location is not empty.
120	Missing parameter Server Name.
121	Missing parameter Server Port.
123	Missing parameter Server IP.
124	Missing parameter Agent Port.
125	Missing parameter Installation location.
126	A value has not been specified for parameter userID. A value for this parameter is required when using RXA-based communication to deploy a Storage Resource agent as a non-daemon service. IBM Spectrum Control uses this user ID when connecting to the computer on which the agent will be installed.
127	Deployment from Windows to Linux failed.
130	Failed to send probe results.
131	Failed to initialize Agent.
133	Missing port number for Service.
134	Get data file stat failed.
135	Get data file read failed.
137	Failed to send data to server.
138	Failed to receive data from server.
139	Full path not specified for copy file.
140	Create file failed in copy file function.
141	Write file failed in copy file function.
142	Open file failed in copy file function.
143	Read file failed in copy file function.
145	UCS conversion failed.
146	Server connection failed.

Table 5. Storage resource agent return codes (continued)

Return code	Explanation
148	Failed to create zip file.
149	Failed to unzip file.
160	Failed to send scan results.
161	Failed to send TSM status results.
164	Failed to validate user.
165	Job file was not found.
166	Job was not stopped.
168	Not enough free space available while copying file from server.
169	Multipath driver not found.
170	Multipath device not found.
171	Multipath policy is not supported.
172	Only Round Robin policy is supported for Multipath DM driver.
175	The command failed to run.
176	The command ran, but failed to complete successfully.

Agent types for monitoring fabrics and switches

Depending on the type of switch you want to manage, you can use a CIM agent or SNMP agent as the data source for the switch.

Table 6. Agent types for switch and fabric functions.

The SMI-S providers can be referred to by various names, such as CIM agent, CIMOM (CIM Object Manager) agent, or SMI-S agent.

Function	Brocade	Cisco	Other
Monitor performance	SMI agent	SNMP agent	Other fabric vendor switches cannot be used for performance monitoring.
Collect information about switches and switch ports	SMI agent	SNMP agent	SMI agent or SNMP agent
Collect information about topology connectivity	SMI agent	SNMP agent	SMI agent or SNMP agent
Collect information about zoning information and zone control	SMI agent	SNMP agent	SMI agent
Generate alerts	SMI agent	SNMP agent	SMI agent or SNMP agent

Check the [IBM Spectrum Control interoperability matrix](#) for switches and directors for information about the switches and directors that are supported by IBM Spectrum Control, and limitations that you need to know about when you use these devices.

Supported storage systems providing full disk encryption and solid-state drives

IBM Spectrum Control supports full disk encryption and solid-state drives in the IBM System Storage DS8000 and IBM System Storage DS5000 Storage Manager systems described in this topic.

DS8000 4.2 and later

IBM Spectrum Control supports full disk encryption and solid-state drives in DS8000 4.2 and later.

IBM System Storage DS5000 Storage Manager series

IBM Spectrum Control supports full disk encryption and solid-state drives in the following DS5000 series systems:

- DS5100 and DS5300 - full disk encryption, solid-state drives, 1 TB SATA drives
- DS5020 - full disk encryption

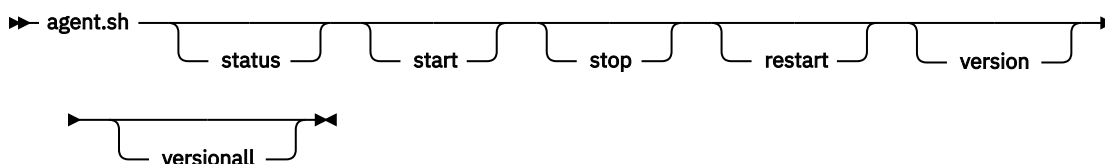
To support full disk encryption and solid-state drives in DS5000, the LSI SMI-S Provider is required. For more information about the LSI SMI-S Provider, see the LSI website at <http://www.lsi.com>.

agent.sh command

The **agent.sh** command lets you start, stop, and restart the Storage Resource agent. You can also display the status and version of the Storage Resource agent.

Note:

- You must have root authority to run this command.
- For Windows, the status, stop, and start functions are handled through the Windows Services panel.



Parameters:

status

Displays the current status of the Storage Resource agent. The status is returned is running or not running.

start

Starts the Storage Resource agent.

stop

Stops the Storage Resource agent.

restart

Stop and then start the Storage Resource agent.

version

Displays the current version of the Storage Resource agent.

versionall

Displays the version of the Storage Resource agent and its related components.

dataCollector command

The **dataCollector** command is used to start and stop the data collector service.

The asset, capacity, and performance metadata for the storage systems in your data centers is collected by the data collector, analyzed, and then shown on the IBM Spectrum Control GUI. The data collector service is part of the Device server. When you stop and start the Device server, the data collector stops and starts automatically.

Note:

Important: Do not use the **dataCollector** command unless you are directed by IBM Support.

On Windows operating systems, you must have Administrator rights to stop or start the data collector service. On AIX® or Linux operating systems, you must have root privileges to stop or start the data collector service.

1. Log on to the server where the IBM Spectrum Control servers are installed.
2. Open a command window or shell script and go to the data collector directory.
The data collector service is installed in the *installation_dir*/datacollector directory.
3. Choose one of the following options to stop or start the data collector service:
 - a) On a Windows operating system, click the **Start** menu, enter `services.msc` and press **Enter**.
 - b) Select **IBM Spectrum Control data collector** and then stop or start it.

Or

- a) Run the **dataCollector.bat** script with the **stop** or **start** parameter.

Or

- a) On an AIX or Linux operating system, run the **dataCollector.sh** script with the **stop** or **start** parameter.

Configuration files

Use the parameters in IBM Spectrum Control configuration files to help resolve problems.

The parameters in the configuration files are case-sensitive.

The default *installation_dir* for IBM Spectrum Control installations is as follows:

Windows operating systems:

c:\Program Files\IBM\TPC

Linux or AIX operating systems:

/opt/IBM/TPC

The default file locations for the configuration files for IBM Spectrum Control are as follows:

IBM Spectrum Control:

Windows operating systems:

installation_dir\config

Linux or AIX operating systems:

installation_dir/config

Data server:

Windows operating systems:

installation_dir\data\config

Linux or AIX operating systems:

installation_dir/data/config

Device server:**Windows operating systems:**

installation_dir\device\conf

Linux or AIX operating systems:

installation_dir/device/conf

Storage Resource agent:**Windows operating systems:**

installation_dir\agent\config\agent.config

Linux or AIX operating systems: operating systems:

installation_dir/agent/config/agent.config

Restriction: On Windows installations, if you installed IBM Spectrum Control by using a domain user account, you must disable User Account Control to edit the configuration files.

server.config file

The following information lists the parameters that are set in the `server.config` file. These parameters include controller, logging, repository, and service.

Controller parameters**name**

The Data Manager server name is the name of the host computer.

port

The port on which the server listens for requests. The default is 9549.

maxConnections

The maximum number of concurrent sockets that the server opens. The default is 500.

routerThreads

The number of threads that redirect incoming requests to the appropriate service provider. The default is 1.

serviceThreads

The number of threads to allocate for the internal service provider of the server. The default is 2.

agentErrorLimit

The number of consecutive attempts to reach an agent before the agent is displayed as DOWN. The default is 3. When an agent is in this state, no attempts to connect are made until either the agent contacts the server or the agent status is manually changed to UP.

adminGroup

The name of the group a user must be a member of to perform administrative functions from the GUI, the default is `isadm`.

commEncrypted

The switch that secures communication between the Server or Agent and the Server/GUI by encrypting the `DataStream`.

- 0 = Off. Do not encrypt the `DataStream`.
- 1 = On. Encrypt the `DataStream`.

FileSystemScan NFSTimeout

Determines the numbers of seconds that a Storage Resource agent waits for a status system call on a Network File System (NFS) before it times out.

hostAlias

This parameter is displayed if the `HOST_ALIAS` is not specific and represents the name of the server. The value for this parameter is used when multiple computers have the same name or the name cannot be determined.

Logging parameters

logsKept

The number of server logs to keep. The default is 5.

messagesPerLog

The maximum number of messages in a log. When this number is reached the log is closed and a new log is created. The default is 100,000.

Repository parameters

driver

The name of the JDBC driver to use, normally:

- `Db2:COM.ibm.db2.jdbc.app.DB2Driver`

url

The URL used to connect to the database, normally:

- `Db2:jdbc:db2:database_name`

user

The user name that IBM Spectrum Control uses to connect to the repository.

connectionPool

The number of database connections in a pool of reusable open connections. The default is 10.

Service parameters

name

Repeating section that indicates the service providers that are required to start.

The REQUIRED parameters are as follows:

- `TStorm.server.svp.GuiSvp`
- `TStorm.server.svp.AgentSvp`
- `scheduler.Scheduler`

scheduler.config file

The following information lists the parameters that are set in the `scheduler.config` file. These parameters include concurrency parameters and jobs parameters.

Concurrency parameters

maxSubmitThreads

The maximum number of threads to create that handle the submission of jobs. The default is 3.

maxCompleteThreads

The maximum number of threads to create to handle job completions. Initially creates a pool of half the number of threads specified that can grow to the maximum. The default is 3.

Jobs parameters

minutesAdvanced

The number of minutes in advance of scheduled time to begin the scheduling process. The default is 1. Use this option to allow for the processor time that is involved in scheduling a job so that the job starts close to the scheduled time.

delayLimitMinutes

Number of minutes after scheduled start time that the Scheduler continues to attempt to start a job for a selected resource, so that resource state is not in a down state or, connection status is not in a failed state. The default is 120.

Location of the scheduler.config file

The scheduler.config file is in the following directories:

Windows operating systems:

installation_dir\data\config

Linux or AIX operating systems:

installation_dir/data/config

TPCD.config file

The list of parameters that are set in the TPCD.config file include server parameters and GUI parameters.

The following list describes the server parameters:

threadPoolSize

Number of initial threads to create for handling requests. The default is 3.

abbreviatedProbe

Only SCSI commands are sent to disk drives for inquiry and disk capacity information. The default is 1.

maxThreads

Set the maximum number of threads for handling requests. The default is 8.

pingReceiveTimeout

Number of seconds to wait before it indicates that a ping failed. The default is 10.

skipAutoFS

Set to 1 if you want to skip the **automount** process during discovery on the Oracle Solaris Storage Resource agent. By default, discovery always processes **automount** on all Oracle Solaris Storage Resource agents managed by the Data server.

saveNonRoot

Set to 1 if you want to monitor non root exports. The default is 0.

If you do not set this parameter, the export paths that are not at the root of the file system are discarded. If the NAS server has only non root exports accessible to the agent, it will not be added. Restart the Data server for this setting to take effect.

batchPartitionWaitRetryCount

Specify the number of times that the Storage Resource agent tries to get a report partition before the Storage Resource agent fails with an error.

Large batch reports are generated in partitions. The partitions are placed on the IBM Spectrum Control server, and the Storage Resource agent gets them from the server when the batch report is created.

The following list describes the GUI parameters:

threadPoolSize

Number of initial threads to create for handling user interface requests. The default is 3.

maxThreads

Set the maximum number of threads for handling user interface requests. The default is 10.

reportRowLimit

Maximum number of rows that are sent at a time to the user interface. If this number is exceeded, a **More** button is displayed over the table, along with a warning message. The default is 5000.

keepCachedReport

Number of minutes to retain incomplete reports in the tmp directory for the server. The default is 120.

Specifying the tablespace size for IBM Spectrum Control

This section provides information on the size of the tablespace to specify when you install IBM Spectrum Control

When you install IBM Spectrum Control, you can specify the tablespace size of the repository database or accept the default values. The space needed for the IBM Spectrum Control database schema varies significantly with storage network configuration, data collection, data retention period, and other factors.

The following table provides space estimates for a storage configuration containing 5000 volumes with some general assumptions.

Table 7. Tablespace allocation for the IBM Spectrum Control database schema			
Tablespace	Description of tablespace usage	Recommended size for a 5000 volume configuration	Assumptions
KEY	This tablespace is used for configuration data which is constantly used. For example, the key entity and relationships data (T_RES_STORAGE_SUBSYSTEM, T_RES_STORAGE_VOLUME, and the normalization tables, and so forth)	500 MB	
NORMAL	This tablespace is used for snapshots and miscellaneous data	500 MB	A table that uses significant space is T_RES_STORAGE_VOLUME_SNAPSHOT. This table uses about 2500 bytes for each record. The number of snapshots depends on the data collection activities.
BIG	This tablespace is used for performance statistics	2 to 3 GB or 400 MB per day of performance data	The data collected for performance data for storage volumes can use a significant amount of space (about 200 bytes for each record). For 5000 volumes, if performance data is collected every 5 minutes, the data for one day would be 300 MB. If the data is kept for 7 days, the data collected would take about 2 to 3 GBs. If the data is kept longer, the storage must be scaled up accordingly.
TEMP	This tablespace is used for temporary data for query processing and other temporary tables	1GB	

agent.config file

The `agent.config` file contains configuration parameters for the Storage Resource agent. These parameters are set when the Storage Resource agent is installed. The parameters can also be changed manually by editing the file.

The following list contains the parameters for the `agent.config` file.

Servename

Fully qualified host name of the system on which the Data server is installed.

Portnumber

Port on which the Data server listens for communications from the Storage Resource agent. By default, the port is set to 9549.

IPAddress

IP address of the server on which the Data server is installed.

Log files

When you have a problem, you can check several product log files.

Default locations of log files

Check the log files to view detailed information about IBM Spectrum Control processing and to troubleshoot problems.

The following list shows the default log file locations for IBM Spectrum Control and other components.

Device server

The IBM WebSphere Liberty Profile log files for the Device server are in the following directories:

Windows operating systems.

installation_dir\wlp\usr\servers\deviceServer\logs

Linux or AIX operating systems.

installation_dir/wlp/usr/servers/deviceServer/logs

The operational log files for the Device server are in the following directories:

Windows operating systems.

installation_dir\device\log

Linux or AIX operating systems.

installation_dir/device/log

The log files for the data collector are in the following directories:

Windows operating systems.

installation_dir\datacollector\log

Linux or AIX operating systems.

installation_dir/datacollector/log

Alert server:

The IBM WebSphere Liberty Profile log files for the Alert server are in the following directories:

Windows operating systems.

installation_dir\wlp\usr\servers>alertServer\logs

For example, C:\Program Files\IBM\TPC\wlp\usr\servers>alertServer\logs

Linux or AIX operating systems.

installation_dir/wlp/usr/servers/alertServer/logs

The operational log files for the Alert server are in the following directories:

Windows operating systems.

installation_dir>alert\log

For example, C:\Program Files\IBM\TPC>alert\log

Linux or AIX operating systems.

installation_dir/alert/log

Data server

Windows operating systems.

installation_dir\data\log

Linux or AIX operating systems.

installation_dir/data/log

Export server

Windows operating systems.

installation_dir\export\logs

Linux or AIX operating systems.

installation_dir/export/logs

Web server log files

Windows operating systems.

installation_dir\wlp\usr\servers\webServer\logs

Linux or AIX operating systems.

installation_dir/wlp/usr/servers/webServer/logs

IBM Spectrum Control GUI

Windows operating systems.

installation_dir\web\log

Linux or AIX operating systems.

installation_dir/web/log

Storage Resource agents

installation_dir/agent/log/name_of_server_SRA_communicates_with

Tips:

- For Windows operating systems, the default *installation_dir* is C:\Program Files\IBM\TPC.
- For Linux or AIX operating systems, the default *installation_dir* is /opt/IBM/TPC.

Script parameters

Script parameters provide specific information on the alert that triggered the script to be run.

The parameters that are passed to a script depend on the type of alert that was triggered. The following table describes all the script parameters:

Script Parameter	Description
amount	Threshold exceeded amount.
archive-file-count	The number of log files in the archived log directory.
archive-log-directory	Name of the archive log directory that triggered the archive log directory Instance alert.
available-extents	The number of extents still available to the segment for growth. This value equals the maximum extents available to the object minus the extents that are currently allocated to the segment.
available-space	Available pool space after a change
blade	Name of a blade.
chained-row-count	The number of chained rows in a table that triggered the Chained Row table alert.
computer	Computer name where the triggering condition occurred.

Script Parameter	Description
consecutive-failures	Number of consecutive failed attempts to ping the computer.
controller	Name of a back-end controller.
cluster-name	The name of an HACMP or MSCS cluster.
creator.name	Creator of the ping, probe, or scan schedule. Name of the schedule.
current-grown-defects	Current number of grown defects on the disk.
current-node-name	When an HACMP or MSCS cluster resource group moves, this parameter identifies the cluster node that now hosts the cluster resource group.
current-RAM MB	Current value of the RAM in megabytes.
current-VM MB	Current value of the sum of the RAM and the swap space in megabytes.
database	The name of the database where the triggering condition occurred.
database-tablespace	The name of the database or table space where the triggering condition occurred.
device-name	Name of a device.
disk-array	Name/alias of a disk array.
dump-date	The date when the last memory dump was performed.
endpoint	Name of an endpoint device.
extent-count	The number of extents that are allocated to a segment, or the number of free extents in the table space (depends on Alert type).
failed-jobs	Number of failed jobs in the run. (Each job runs on a different computer).
file-of-violating-files	Temporary file that contains a list of files that violate the constraint. The files are listed as one file per line.
file-of-violating-owners	Temporary file that contains a list of owners who owns the violating files.
free-inodes	Maximum number of files available to be created on this file system.
free space size-designator	Total amount of free space, in KB, MB, or GB.
from-entity-type	Type of new fabric connection from an entity.
HBA-driver	HBA driver
HBA-firmware	HBA firmware
io-group	Name of the I/O group.
largest-extent-size size-designator	Total amount of the largest free extent in the table space, which is measured in KB, MB, or GB.
manufacturer/serial-number	Manufacturer of the disk. Serial number of the disk.
mdisk	Name of an MDisk.
mdisk-group	Name of an MDisk group.
mount-point	Path to the file system.
new-capacity	New capacity of a storage subsystem, volume, or pool.
new-version	New version of the HBA driver, firmware, or a subsystem.
node	Name of a node.

Script Parameter	Description
old-capacity	Previous capacity of a storage subsystem, volume, or pool.
old-grown-defects	Previous number of grown defects on the disk.
old-node-name	When an HACMP or MSCS cluster resource group moves, this parameter identifies the cluster node that previously hosted the cluster resource group.
old-RAM MB	Previous value of the RAM in megabytes.
old-version	Previous version of the HBA driver, firmware, or a subsystem.
old VM MB	Previous value of the sum of the RAM and the swap space in megabytes.
path	Path to the directory.
percent-of-capacity %	Percentage of capacity of the file system, database, or table space.
percent-of-table-size	The percentage of space that is allocated to a segment that is empty and unused (the percentage of space over the "high-water mark"). Available on the Empty Used Segment Space table alert.
percent-of-total-rows %	The percentage of table rows that are chained.
pool	Name of a storage pool.
port	Name of a port.
rdbms-instance-name	Oracle SID, SQL Server name, Sybase Server name, UDB Instance name
rdbms-type	Oracle, SQL Server, or Sybase
run-number	Number of the run.
segment	The name of the table segment that triggers the alert.
segment-type	<p>The type of segment that triggers the alert. The following list includes the possible types of segments.</p> <ul style="list-style-type: none"> • TABLE • TABLE PARTITION • TABLE SUBPARTITION • NESTED TABLE • CLUSTER • INDEX • INDEX PARTITION • INDEX SUBPARTITION • LOBINDEX • LOBSEGMENT • LOB PARTITION • LOB SUBPARTITION
storage-volume	Name of a storage volume
subsystem	Name of a storage subsystem
switch	Name of a switch
table	The name of the table that triggered the alert condition.
table space	The name of the table space that triggered the alert condition.

Script Parameter	Description
threshold	Value that you set for the triggering condition. If the value unit was specified as a %, then a % follows this value.
threshold thr-designator	Value of the triggering condition, in KB, MB, or GB, or % (value units).
to-entity-type	Type of new fabric connection to an entity.
total-jobs	Total number of jobs in a run.
total-file-size size designator	Total amount of storage that is consumed by the archive log directory, which is measured in KB, MB, or GB.
usage size-designator	Value of used disk space, in KB, MB, or GB.
violating-file-count	Number of files that met the conditions that are defined in the constraint.
virtual-server-name	The name of an HACMP or MSCS cluster resource group.
zone	Name of a zone.
zoneset	Name of a zone set.
zone-alias	Name of a zone alias
zone-member	Name of a zone member

Opening IBM Spectrum Control on Windows operating systems

You can open IBM Spectrum Control CLIs and GUIs and administer IBM Spectrum Control on Windows operating systems.

Opening IBM Spectrum Control GUIs and CLIs

To manage and monitor storage resources, open IBM Spectrum Control GUIs and CLIs.

You can open the following GUIs and CLIs:

- [“Opening IBM Spectrum Control GUI” on page 139](#)
- [“Opening Db2 Command Window” on page 140](#)
- [“Opening IBM Data Studio Administration client on Windows operating systems” on page 140](#)
- [“Opening IBM Tivoli Monitoring Services” on page 140](#)

Opening IBM Spectrum Control GUI

1. Choose one of these options:

Option	Description
Windows Server 2012	<ol style="list-style-type: none"> a. On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start. b. On the Start page, right-click, and then click the All apps taskbar button.
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start > All Programs .

2. Click **IBM Spectrum Control > IBM Spectrum Control**.

Opening Db2 Command Window

1. Choose one of these options:

Option	Description
Windows Server 2012	a. On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start . b. On the Start page, right-click, and then click the All apps taskbar button.
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start > All Programs .

2. Click **IBM DB2 > Command Line Tools > Command Window**.

Opening IBM Data Studio Administration client on Windows operating systems

1. Choose one of these options:

Option	Description
Windows Server 2012	a. On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start . b. On the Start page, right-click, and then click the All apps taskbar button.
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start > All Programs .

2. Click **IBM Data Studio > Data Studio Administration Client**.

Opening IBM Tivoli Monitoring Services

1. Choose one of these options:

Option	Description
Windows Server 2012	a. On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start . b. On the Start page, right-click, and then click the All apps taskbar button.
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start > All Programs .

2. Click **IBM Tivoli Monitoring > IBM Tivoli Monitoring Services**.

Accessing administration tools

To manage and maintain IBM Spectrum Control, access the Windows system administration tools.

To complete tasks in IBM Spectrum Control, you must open the following administration and maintenance facilities:

- [“Accessing the Control Panel” on page 141](#)
- [“Accessing Administrative Tools” on page 141](#)
- [“Accessing Windows Services” on page 141](#)

- “Accessing Computer Management” on page 141
- “Accessing Programs and Program Features” on page 141

Accessing the Control Panel

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start .

2. Click **Control Panel**

Accessing Administrative Tools

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows 7, Windows 2008	Click Start .
Windows XP, Windows Vista	Click Start > Control Panel .

2. Click **Administrative Tools**

Accessing Windows Services

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows 7, Windows 2008	Click Start .
Windows XP, Windows Vista	Click Start > Control Panel .

2. Click **Administrative Tools > Services**

Accessing Computer Management

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start .

2. Click **Control Panel > Computer Management**

Accessing Programs and Program Features

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start .

2. Click **Control Panel > Programs and Program Features**.

Accessing Window Run

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows 7, Windows 2008, Windows Vista, Windows XP	Click Start .

2. Click **Run**.

Windows services used by IBM Spectrum Control

To start, stop, or restart a component or related program in IBM Spectrum Control, use the Windows Services panel.

The following table provides a list of Windows services.

Table 8. List of Windows services used by IBM Spectrum Control

Program	Service name	Comment
IBM DB2	DB2 - DB2COPY1 - DB2 - 0 DB2 Governer (DB2COPY1) DB2 License Server (DB2COPY1) DB2 Management Service (DB2COPY1) DB2 Remote Command Server (DB2COPY1) DB2DAS - DB2DAS00 DB2TS - DB2COPY1 - DB2-0	The service account owner is db2admin . The account needs to be part of Administrators and DB2ADMNS.
IBM Spectrum Control Data server	IBM Spectrum Control - Data Server	
IBM Spectrum Control Device server	IBM Spectrum Control - Device Server	
IBM Spectrum Control Alert server	IBM Spectrum Control - Alert Server	
IBM Spectrum Control Storage Resource agent	IBM Spectrum Control Storage Resource Agent	
IBM Spectrum Control Web server	IBM Spectrum Control - Web Server	

Table 8. List of Windows services used by IBM Spectrum Control (continued)

Program	Service name	Comment
IBM Spectrum Control Export server	IBM Spectrum Control - Export Server	
IBM Spectrum Control data collector	IBM Spectrum Control data collector	

Frequently Asked Questions

View answers to common questions about IBM Spectrum Control.

How do you know if your storage system is supported by IBM Spectrum Control and which SMI-S agents are supported?

To confirm whether your storage system is supported and which SMI-S agent is supported for that system, review the supported products list for the current release of IBM Spectrum Control at [IBM Spectrum Control interoperability matrix for storage systems](#).

You encounter errors while collecting performance data on SAN Volume Controller. You fail to associate SAN Volume Controller performance data from non-configuration node with SAN Volume Controller performance data from configuration node. You encounter incomplete SAN Volume Controller performance data sample.

This issue is caused by a configuration issue with SAN Volume Controller (time zone). Reset the time zone on SAN Volume Controller by logging into the SAN Volume Controller through putty. Run this command first:

```
svctask settimezone -timezone 509
```

This forces the cluster into the Universal time zone. To get the time zone you want the cluster to be in, run this command:

```
svctask settimezone -timezone
```

Protocols and standards

This section provides an overview of the protocols and standards that are used within IBM Spectrum Control.

Web Based Enterprise Management

Web Based Enterprise Management (WBEM) is an initiative of the Distributed Management Task Force (DMTF) with the objective to enable the management of complex IT environments. It defines a set of management and internet standard technologies in order to unify the management of complex IT environments.

The WBEM initiative is composed of three main conceptual elements:

Common Interface Model (CIM)

CIM is a formal object-oriented modeling language that is used to describe the management aspects of systems.

xmlCIM

This is the grammar to describe CIM declarations and messages used by the CIM protocol.

Hypertext Transfer Protocol (HTTP)

HTTP is used as a way to enable communication between a management application and a device that both use CIM.

The WBEM architecture defines the following elements:

CIM Client

The CIM Client is a management application like IBM Spectrum Control that uses CIM to manage devices. A CIM Client can reside anywhere in the network, because it uses HTTP to talk to CIM Object Managers and Agents.

CIM Managed Object

A Managed Object is a hardware or software component that can be managed by a management application by using CIM.

CIM Agent

A CIM Object Manager that includes the provider service for a limited set of resources. An agent may be embedded or hosted and can be an aggregator for multiple devices.

CIM Provider

A CIM Provider is the element that translates CIM calls to the device-specific commands. A provider is always closely linked to a CIM.

CIM Object Manager (CIMOM)

The central component of the CIM Server responsible for the communication between the CIM server components.

CIM Server

A server that receives and processes CIM Operation Message Requests and issues CIM Operation Message Responses.

Storage Management Initiative Specification

The Storage Networking Industry Association (SNIA) defines a standard that is used within IBM Spectrum Control to create and develop a universal open interface for managing storage devices including storage networks.

For information about SMI-S, see <http://www.snia.org>.

SNIA has fully adopted and enhanced the Common Information Model (CIM) standard for storage management in its Storage Management Initiative - Specification (SMI-S). SMI-S was launched to create and develop a universal open interface for managing storage devices including storage networks. SMI-S provides:

- A comprehensive specification for the management of heterogeneous storage and storage area networks (SANs).
- The information available to a WBEM client from an SMI-S compliant CIM server (provider).
- Profiles organized by:
 - Storage
 - Fabric
 - Host
 - Common profiles and subprofiles
- An object-oriented CIM and XML-based interface for managing SAN devices, services, and fabrics.
- An initial discovery, which is SLP based.

The idea behind SMI-S is to standardize the management interfaces so that management applications can utilize these and provide cross-device management. This means that a newly introduced device can be immediately managed as it will conform to the standards.

The models and protocols in the SMI-S implementation are platform-independent, enabling application development for any platform, and enabling them to run on different platforms. The SNIA will also provide interoperability tests which will help vendors test their applications and devices if they conform to the standard.

Service Location Protocol

The Service Location Protocol (SLP) is an Internet Engineering Task Force (IETF) standard. SLP provides a scalable framework for the discovery and selection of network services.

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers that are concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF includes formal standards for SNMP and MIBs. For more information about IETF, see <http://www.ietf.org>.

SLP enables the discovery and selection of generic services, which can range in function from hardware services such as those for printers or fax machines, to software services such as those for file servers, email servers, web servers, databases, or any other possible services that are accessible through an IP network.

Traditionally, to use a particular service, a user, or client application provided the host name or network IP address for the service. With SLP, however, it is not necessary for the user or client application to know individual host names or IP addresses. Instead, the user or client application can search the network for the required service type and an optional set of qualifying attributes.

For example, a user can search for all available printers that support Adobe PostScript. Based on the service type such as printers and the attributes such as PostScript, SLP searches the user's network for matching services, and returns the discovered list to the user.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an Internet Engineering Task Force (IETF) protocol for monitoring and managing systems and devices in a network. Functions supported by the SNMP protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.

SNMP is a protocol that enables a management application to query information from a managed device. The managed device has software running that sends and receives the SNMP information. This software module is usually called the SNMP agent.

An SNMP management application can read information from an SNMP agent in order to monitor the device that the SNMP agent is running on. Therefore, the device needs to be polled on an interval bases. The SNMP manager can also change the configuration of a device, by setting certain values to corresponding variables. A device can also be set up to send a notification to the SNMP manager (this is called a trap) to asynchronously inform this SNMP manager of a status change.

Depending on the existing environment and organization it is very likely that your environment already has an SNMP management application in place. IBM Spectrum Control can be set up to send traps.

SNMP uses a hierarchical structured Management Information Base (MIB) to define the meaning and the type of a particular value. A MIB defines managed objects that describe the behavior of the SNMP entity, which can be anything from an IP router to a storage subsystem. The information is organized in a tree structure.

For users planning to make use of the IBM Spectrum Control SNMP trap alert notification capabilities, an SNMP MIB is included in the server installation.

The MIB is provided for use by your SNMP management console software. Most SNMP management products provide a program called a MIB compiler that can be used to import MIBs. This will allow you to view IBM Spectrum Control generated SNMP traps from within your management console software. Refer to your management console software documentation for instructions on how to compile or import a third party MIB.

For a Cisco switch to successfully receive and respond to queries from IBM Spectrum Control, the following basic requirements must be met:

- IBM Spectrum Control can use SNMPv3 (preferred) or SNMPv1 to probe switches and fabrics. The SNMPv3 protocol is preferred because it provides better security, but switches that use the SNMPv1 protocol are also supported. Some switches are configured to use SNMPv3 by default.

- If the switch uses an SNMP agent, the Fibre Alliance FC Management MIB (FA MIB) and Fibre Channel Fabric Element MIB (FE MIB) must be enabled on the switch.
- When using the SNMPv1 protocol, the community string that is configured in IBM Spectrum Control must match one of the community strings that are configured on the switch with read access. Cisco switches must additionally have a community string match for write access. The default community strings in IBM Spectrum Control are "public" for read access and "private" for write access. Other community strings can be defined on the switches, but are not used. Community strings are not relevant when using the SNMPv3 protocol.
- SNMP access control lists must include the IBM Spectrum Control system. These access control lists are defined and configured on the switches. Some lists automatically include all hosts, while others exclude all by default.
- The Fibre Channel (FC) or Fibre Channel over Ethernet (FCoE) protocols must be enabled on the switch. Some switches, such as the Cisco Nexus 5000 series, require you to enable these protocols. Otherwise, IBM Spectrum Control will not recognize the switch when you try to add it using the **Add Switches and Fabrics for Monitoring** dialog. For instructions on how to configure Cisco switches for FCoE enablement, go to the Cisco product website at <http://www.cisco.com> and click **Support**.

IBM Spectrum Control uses port 162 to listen for SNMP traps. This is the default port. For switches, you must configure the switch to send SNMP traps to the Device server IP address. If you need to change the default port number, use the **setdscfg** command. The attribute to set is **SNMPTrapPort**.

System administrators must set up their SNMP trap ringer with the provided MIB files in order to receive SNMP traps from IBM Spectrum Control. These files are located in the following directories on the product installation DVD:

For the Data server:

```
data\snmp\tivoliSRM.mib
```

For the Device server :

```
device\snmp\fabric.mib
```

Fibre Channel Methodologies of Interconnects

IBM Spectrum Control supports the ANSI T11 Fibre Channel FC-MI (Fibre Channel Methodologies of Interconnects) for the automated discovery of FC SAN assets and topology.

ANSI T11 Fibre Channel FC-MI includes the following for the automated discovery of FC SAN assets and topology:

- Hosts (HBAs)
- FC interconnects
- FC storage devices

The T11 FC-MI also includes the following:

- FC-GS-3/4 (discovery, zoning, and so forth)
- RNID (advanced device recognition)
- Platform registration (device recognition and launch)
- Common HBA API (fabric and storage views)
- Name server (connectivity)
- Management server (SAN connectivity and topology)
- RSCN (advanced event detection)
- SCSI queries (storage views, volume information, and so forth)
- SNMP Fabric Element (FE) MIB
- SNMP FC Management MIB (discovery, performance statistics, and so forth)

- SNMP alerts

Appendix B. Accessibility features for IBM Spectrum Control

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Spectrum Control:

- Keyboard-only operation in the GUI.
- A Knowledge Center that includes the following accessibility features:
 - The Knowledge Center is provided in XHTML 1.0 format, which is viewable in most web browsers. With XHTML, you can view documentation according to the display preferences that are set in your browser. XHTML supports screen readers and other assistive technologies.
 - All documentation for IBM Spectrum Control is available in Adobe Portable Document Format (PDF) by using the Adobe Acrobat Reader. To access PDFs, go to [Printable documentation](#).
 - All images in the Knowledge Center are provided with alternative text, so that visually impaired users can understand the contents of the images.
- Interfaces that are commonly used by screen readers.

The setting for the automatic-refresh button in the screen reader is toggled to the ON position by default. If you want the screen reader to read the previous text, complete the following steps:

1. Navigate to the Accessibility Settings Navigation region by using the arrow keys. The region is located after the IBM Spectrum Control application title.
2. Click **Enter** to toggle the automatic-refresh button to the OFF position. (An alert sounds to make you aware that the turn-off automatic-refresh toggle button was pressed.)
3. To move backward to the previously read text so that the screen reader can read it again, use the arrow keys. You can move backwards and forwards through the page.
4. When you are ready to move on, click **Enter** to toggle the automatic-refresh button to the ON position and to refresh the page. (An alert sounds to make you aware that the turn-on, automatic-refresh toggle button was pressed.)

Tip: Alternatively, let the toggle setting persist, and refresh as needed by pressing the F5 key.

Keyboard navigation

Most of the features of the IBM Spectrum Control GUI are accessible by using the keyboard. For those features that are not accessible, equivalent function is available by using the command-line interface (CLI), except as noted in the product release notes.

You can use keys or key combinations to perform operations and initiate many menu actions that can also be done through mouse actions. The following sections describe the keys or key combinations for different parts of the GUI:

For navigating in the GUI and the context-sensitive help system:

- To navigate to the next link, button, or topic within a panel, press Tab.
- To move to the previous link, button, or topic within a panel, press Shift+Tab.
- To select an object, when the object is in focus, press Enter.

For actions menus:

- To navigate to the grid header, press Tab.

- To reach the drop-down field, press the Left Arrow or Right Arrow key.
- To open the drop-down menu, press Enter.
- To select the menu items, press the Up Arrow or Down Arrow key.
- To start the action, press Enter.

For filters:

To specify a filter option and text:

1. Press Tab to navigate to the magnifying glass icon.
2. Press the Up Arrow or Down Arrow key to navigate the filtering list.
3. Press Enter to select a filtering option.
4. When a filtering option is selected, the cursor moves to the filter text box. Type the filter text and press Enter. To reset a filter, press Enter.

For text fields:

- To navigate to text fields, press Tab.
- To navigate to the fields that are available for editing, press Tab.
- To navigate to the next field or to the **Submit** button, press Tab.

For tables or lists:

- To navigate between column headers, focus on a column header and use the Left Arrow and Right Arrow keys to move to other column headers.
- To navigate between data cells, focus on a data cell and use the Left, Right, Up, Down, Pageup, and Pagedown Arrow keys.
- To sort a column, focus on a column header and press Enter. The focus remains on the column header after the sort occurs.
- To change the size of a column, focus on the column header, hold Shift+Control, and press the Left or Right Arrow keys.
- To follow a link in a data cell, focus on a data cell and press Shift+F9.
- To open a menu for a table row, focus on the row and press Shift+F10.
- To select consecutive rows, select the first row and hold Shift, press the Up or Down Arrow keys to go to the last row in the range, and press the Space bar to add the new rows to the selection.
- To select non-consecutive rows, select a row and hold Control, press the Up or Down Arrow keys, and press the Space bar to add the new row to the selection.

Restriction: For Chinese languages, the keyboard combination Control+Space bar is not enabled for selecting multiple rows at the same time.

IBM and accessibility

For more information about IBM's commitment to accessibility, see the IBM Human Ability and Accessibility Center website at <http://www.ibm.com/able>.

Legal notices

This information was developed for products and services offered in the U.S.A. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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

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

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

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

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation
224A/101
11400 Burnet Road
Austin, TX 78758
U.S.A*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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 measurements 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.

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.

COPYRIGHT LICENSE: This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <https://www.ibm.com/legal/us/en/copytrade.shtml>.

Intel, Intel logo, Intel Xeon, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Linux is a registered 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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Glossary

A glossary is available with terms and definitions for the IBM Spectrum Control family of products.

You can view the glossary in the IBM Spectrum Control product documentation at <http://www.ibm.com/support/knowledgecenter/SS5R93>.

To view glossaries for other IBM products, see <http://www.ibm.com/software/globalization/terminology/>.

Index

A

- about this document [viii](#)
- accessibility features
 - for IBM Spectrum Control [149](#)
- adding
 - CIM agents [85](#)
 - SMI-S providers [85](#)
- adding resources
 - canceling agent deployment [73](#)
 - fixing agent deployment problems [71](#)
 - hypervisors [67](#)
 - modifying deployment schedules for agents [73](#)
- agent.config [134](#)
- agent.sh command
 - syntax [129](#)
- agents
 - changing credential for a Storage Resource agent [76](#)
 - CIM agents [85](#)
 - deploying Storage Resource agents [28](#)
 - deployment considerations for Storage Resource agents [28, 80](#)
 - enabling a Storage Resource agent [75](#)
 - enabling or disabling scripts for a Storage Resource agent [77](#)
 - enabling or disabling the monitoring of fabrics by a Storage Resource agent [77](#)
 - preparing Storage Resource agents for installation [28, 80](#)
 - registering with a different server [79](#)
 - SMI-S providers [85](#)
 - testing the connection with the server where a Storage Resource agent is deployed [75](#)
 - uninstalling a Storage Resource agent [78](#)
 - viewing information about Storage Resource agents [74](#)
 - viewing Storage Resource agent log files [74](#)
- Alert server
 - troubleshooting [92](#)
- assigning roles [7](#)
- authentication mechanism, modify [8](#)
- authorizing users
 - assigning roles [7](#)

B

- backup considerations
 - Tivoli Storage Productivity Center [113](#)
- Brocade [128](#)

C

- certificates
 - creating for Storage Resource agents [33](#)
 - replacing for Storage Resource agents [38](#)
- Cisco fabrics
 - removing [71](#)
- CIM agent

- CIM agent (*continued*)
 - moving [86](#)
 - replacing [86](#)
- CIM agents
 - adding [85](#)
 - collecting logs [67](#)
 - verify they are running [86](#)
- Cisco [128](#)
- commands
 - agent.sh [129](#)
 - dataCollector [130](#)
 - repocopy [120](#)
- comments, sending [viii](#)
- common user, about [1](#)
- configuration
 - assigning roles to groups [5](#)
 - authorizing users [5](#)
 - for switches [21](#)
- configuration files
 - agent.config [134](#)
 - default locations [130](#)
 - encryption [131](#)
 - for IBM Spectrum Control [130](#)
 - scheduler.config [132](#)
 - server.config [131](#)
 - TPCD.config [133](#)
- configuring
 - data retention [2](#)

D

- data collection
 - configuring data retention [2](#)
- data collector trusted certificates for IBM Spectrum Control [54](#)
- Data server
 - increasing memory [96](#)
 - increasing memory on AIX [96](#)
 - increasing memory on Linux [97](#)
 - increasing memory on UNIX [97](#)
 - increasing memory on Windows [97](#)
 - troubleshooting [92](#)
- Data Studio
 - data studio [123](#)
- database
 - administering the IBM Spectrum Control database [112, 117](#)
 - reorganizing [118](#)
 - updating statistics [118](#)
- database backups
 - IBM Spectrum Control [112](#)
- database maintenance tool
 - collecting statistics about the database [117](#)
 - customizing [119](#)
 - maintaining the database [117](#)
 - reorganizing tables in the database [117](#)
- dataCollector command [130](#)

- Db2
 - command line [121](#)
 - monitoring [123](#)
- DB2
 - starting [142](#)
 - stopping [142](#)
- Db2, stop [122](#)
- Device server
 - setting timeout values [23](#)
 - troubleshooting [92](#)
- disaster recovery [112](#), [114](#), [115](#)
- Distributed Management Task Force (DTMF) [143](#)
- domain account
 - how to grant local administrative privileges [105](#)

E

- encryption [131](#)
- Export server
 - starting [142](#)
 - stopping [142](#)

F

- Fabric zone configuration [128](#)
- fabric.mib file [145](#)
- fabrics
 - changing connection information [70](#)
 - changing credentials [70](#)
 - connection information [70](#)
 - removing [71](#)
 - testing connection [71](#)
 - updating connection information [69](#)
 - viewing information [69](#), [70](#)
- federated repositories
 - changing authentication for IBM Spectrum Control [12](#), [15](#)
 - configuring alternative user authentication for federated repositories in IBM Spectrum Control [16](#)
- federated repository [8](#)
- fibre channel
 - methodologies of interconnects [146](#)
- file system [114](#), [115](#)
- ftp [94](#)
- full disk encryption
 - support for [129](#)
- fully qualified host name
 - checking for on AIX [47](#)
 - checking for on Linux [47](#)
 - checking for on Solaris [48](#)
 - Windows, verify [48](#)

G

- generate, default, Export server [56](#)

H

- historical trending
 - configuring data retention [2](#)
- hypervisors
 - adding [67](#)
 - updating credentials [68](#)

I

- IBM Spectrum Control
 - configuration files [130](#)
 - log files [135](#)
- IBM Spectrum Control data collector
 - starting [142](#)
 - stopping [142](#)
- installing
 - Storage Resource agent considerations [28](#), [80](#)
 - Storage Resource agents [28](#)
 - Storage Resource agents remotely [28](#), [80](#)
- Internet Engineering Task Force (IETF) [145](#)
- interop namespaces [87](#)
- IPv6
 - configuring
 - AIX for IPv6 [58](#)
 - Db2 on AIX for IPv6 [58](#)
 - Db2 on Linux for IPv6 [59](#)
 - configuring Db2 on Linux [59](#)
 - configuring for AIX [58](#)
 - configuring for Db2 on AIX [58](#)

L

- LDAP
 - managing user authentication in IBM Spectrum Control [11](#)
- LDAP authentication
 - advanced configuration [19](#)
- LDAP federated repositories framework
 - alternative user authentication for federated repositories in IBM Spectrum Control [16](#)
- LDAP repository
 - changing from LDAP to operating system authentication in IBM Spectrum Control [15](#)
- LDAP server to a file
 - exporting SSL certificate from IBM Security Directory Server to a file [17](#)
 - exporting SSL certificate from Microsoft Active Directory LDAP Server to a file [18](#)
- ldapEntityType element
 - configuring [19](#)
- license
 - check [91](#)
- license restrictions [8](#)
- Linux
 - IBM Data Studio, start [123](#)
- log files
 - for IBM Spectrum Control [135](#)
 - packaging [93](#)
- logon page
 - terms and conditions, add [21](#)
 - terms and conditions, show [21](#)

M

- Management Information Base (MIB) files [145](#)
- memory
 - increasing allocation for Data server on AIX [96](#)
 - increasing allocation for Data server on Linux [97](#)
 - increasing allocation for Data server on Windows [97](#)
- memory allocation

memory allocation (*continued*)
Data server [96](#)

N

namespaces, interop [87](#)

O

offline backup
IBM Spectrum Control [114](#), [115](#)
online backup
Tivoli Storage Productivity Center [115](#)
operating system authentication
changing from operating system to LDAP authentication
in IBM Spectrum Control [12](#)

P

packaging log files [93](#)
parameters [136](#)
passwords
changing [98](#)
changing using password tool [98](#), [100](#), [102](#)
changing when no X Window System is installed [104](#)
same logon credentials [98](#)
single server installation [98](#)
planning
authorization for users [1](#)
PMRs
opening [93](#)
problems
report [ix](#)
product
license, check [91](#)
version, check [91](#)

R

reader feedback, sending [viii](#)
removing
Cisco fabrics [71](#)
fabrics [71](#)
storage systems [67](#)
switches [71](#)
replace, Export server [55](#)
replace, servers [52](#)
repocopy command
exporting data [120](#)
repocopy tool
exporting data [120](#)
reporting problems [ix](#)
Reporting server
troubleshooting [92](#)
Repository Copy tool [120](#)
resources
adding hypervisors for monitoring [67](#)
retaining data [2](#)
updating credentials for hypervisors [68](#)
updating credentials for storage systems [61](#)
restrictions
based on license [8](#)
based on role [8](#)

return codes [125](#)
role restrictions [8](#)
roles
assigning [7](#)

S

SAN Volume Controller
publications [vii](#)
scheduler.config [132](#)
scripts
parameters [136](#)
Secure Socket Layer (SSL)
disabling [17](#)
enabling [16](#)
security [5](#)
sending comments [viii](#)
server.config [131](#)
servers
adding by deploying an agent [71](#), [73](#)
canceling agent deployment [73](#)
fixing agent deployment problems [71](#)
modifying deployment schedules [73](#)
removing [78](#)
starting [89](#)
stopping [90](#)
service [viii](#)
Service Location Protocol (SLP)
overview [145](#)
service management connect [viii](#)
service tool
for servers [108](#)
Service tool
for agents [109](#)
services
starting [89](#)
starting by using the GUI [89](#)
stopping [90](#)
stopping by using the GUI [90](#)
SMC [viii](#)
SMI-S providers [85](#)
SNMP
MIBs [145](#)
overview [145](#)
traps [145](#)
solid-state drives
support for [129](#)
SSH protocol
creating a certificate [33](#)
SSL certificate ldap
adding SSL certificates to web server keystore [18](#)
SSL certificate LDAP IBM Security Directory Server to file
exporting SSL certificate from LDAP server to a file [17](#)
SSL certificate Microsoft Active Directory LDAP Server to file
exporting SSL certificate from LDAP server to a file [18](#)
SSL certificates
replacing a certificate [38](#)
starting
Alert server [142](#)
Data server [142](#)
DB2 [142](#)
Device server [142](#)
IBM Spectrum Control web-based GUI [1](#)

- starting product servers [89](#)
- starting product services [89](#)
- stopping
 - agents
 - starting [142](#)
 - stopping [142](#)
 - Alert server
 - starting [142](#)
 - stopping [142](#)
 - Data server
 - starting [142](#)
 - stopping [142](#)
 - DB2 [142](#)
 - Device server
 - port numbers [142](#)
 - starting [142](#)
 - stopping [142](#)
- stopping product servers [90](#)
- stopping product services [90](#)
- Storage Management Initiative - Specification (SMI-S) [144](#)
- Storage Networking Industry Association (SNIA) [144](#)
- Storage Resource agent
 - changing credentials [76](#)
 - changing the Windows service logon [79](#)
- Storage Resource agents
 - creating certificates for [33](#)
 - deploying [28](#)
 - deployment considerations [28](#), [80](#)
 - enabling [75](#)
 - enabling or disabling scripts [77](#)
 - enabling or disabling the monitoring of fabrics [77](#)
 - importing authentication information [49](#)
 - installing [28](#)
 - registering with a different server [79](#)
 - replacing SSL certificates [38](#)
 - testing the connection with IBM Spectrum Control [75](#)
 - uninstalling using GUI [78](#)
 - viewing information [74](#)
 - viewing log files [74](#)
- storage subsystems
 - overview [61](#)
- storage system
 - testing connection [66](#)
- storage systems
 - removing [67](#)
 - updating credentials [61](#)
- support [viii](#)
- Support
 - contact [ix](#)
- Switch Performance Management [128](#)
- switches
 - changing connection information [69](#)
 - changing credentials [69](#)
 - configuring [21](#)
 - connection information [69](#)
 - removing [71](#)
 - testing connection [71](#)
 - updating connection information [69](#)
 - viewing information [69](#)
- SYSMAINT authority
 - checking and setting [123](#)
- system maintenance authority
 - checking and setting [123](#)
- system management

- system management (*continued*)
 - saving trace logs [91](#)
 - troubleshooting [91](#)

T

- T11 FC-MI [146](#)
- terms and conditions
 - logon page, show [21](#)
- testing connection
 - fabrics [71](#)
 - storage system [66](#)
 - switches [71](#)
- timeout values
 - setting for Device server [23](#)
- tivoliSRM.mib file [145](#)
- tools
 - repository copy [120](#)
- TPCD.config [133](#)
- trademarks [153](#)
- translations
 - browser locale requirement [viii](#)
- traps for SNMP [145](#)
- troubleshooting [92](#)

U

- update, servers [54](#)
- updating connection information
 - fabrics [69](#)
 - switches [69](#)
- updating credentials
 - fabrics [69](#)
 - hypervisors [68](#)
 - storage systems [61](#)
 - switches [69](#)
- uploading logs [94](#)
- user authentication
 - configuring [3](#)
 - managing in IBM Spectrum Control [11](#)
 - Secure Socket Layer (SSL)
 - disabling [17](#)
 - enabling [16](#)
- users
 - assigning roles [5](#)
 - determining group membership [7](#)

V

- version
 - check [91](#)

W

- Web Based Enterprise Management (WBEM) [143](#)
- Web server
 - troubleshooting [92](#)
- web server keystore
 - adding SSL certificates to web server keystore [18](#)
- Windows
 - host names, verify [48](#)
 - IBM Data Studio, start [123](#)
- Windows service logon

Windows service logon (*continued*)
changing for a Storage Resource agent [79](#)



Product Number: 5725-F93, 5725-G33, 5725-Y23, 5725-Y24

SC27-8768-05

