IBM Spectrum Protect for Workstations
Version 8 Release 1

Central Administration Console Installation and User's Guide

IBM

IBM Spectrum Protect for Workstations
Version 8 Release 1

Central Administration Console Installation and User's Guide

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 87.

This edition applies to Version 8 release 1 modification 0 of IBM Spectrum Protect for Workstations (product number 5725-X12) and to all subsequent releases and modification until otherwise indicated in new editions.

Contents

About this publication

This publication provides information about how to install and use the IBM® Spectrum Protect for Workstations Central Administration Console. You must install the Central Administration Console so that you can administer and monitor client systems that are running IBM Spectrum Protect™ for Workstations backup activities. This publication describes how to configure the Central Administration Console to administer activity on client systems. This publication does not contain information about how to install and use IBM Spectrum Protect for Workstations on client systems. For information about setting up IBM Spectrum Protect for Workstations, see *IBM Spectrum Protect for Workstations Client Installation and User's Guide*.

Who should read this publication

This publication is intended for administrators who use the Central Administration Console to manage client systems that are running IBM Spectrum Protect for Workstations.

Publications

The IBM Spectrum Protect for Workstations product family includes IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for databases, and several other storage management products from IBM.

For more IBM product documentation, see http://www.ibm.com/support/knowledgecenter.

You can view or download PDF versions of IBM publications from the IBM Publications Center (http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss).

New for administrators

New features and enhancements are available in IBM Spectrum Protect for Workstations Central Administration Console in version 8.1.0.

Changes since the previous edition are marked with a vertical bar (|) in the left margin. Ensure that you are using the correct edition for the level of the product.

Version 8.1.0 includes the following enhancements:

Reduced installation time
: Beginning with this release, the Central Administration Console server runs in a IBM WebSphere® Application Server Liberty Profile environment rather than on Tivoli® Integrated Portal. In the new environment, installation time for the Central Administration Console is significantly reduced. For example, installation on a typical system is approximately 15 minutes. For information about the installation steps, see "Installing the Central Administration Console" on page 7.

Display of report results in graphical format
: A function to display the results of a backup report in graphical format is added to the Central Administration Console. You can use this function to

review the backup activity of clients as a bar chart. For information about how to create and run reports, see "Reporting client activity" on page 50.

Related concepts:

"Product overview for the Central Administration Console" on page 1
With the IBM Spectrum Protect for Workstations Central Administration Console, you can centrally manage many IBM Spectrum Protect for Workstations clients.

Chapter 1. Product overview

The IBM Spectrum Protect for Workstations Central Administration Console provides functions to administer and monitor back up activity on client systems.

Product overview for the Central Administration Console

With the IBM Spectrum Protect for Workstations Central Administration Console, you can centrally manage many IBM Spectrum Protect for Workstations clients.

With the Central Administration Console, you can manage IBM Spectrum Protect for Workstations clients in the following ways:

- Discover existing IBM Spectrum Protect Continuous Data Protection for Files and IBM Spectrum Protect for Workstations clients.
- Monitor the activity of clients to determine the health of your data protection system.
- Tune performance of clients and react to potential problems to maintain the highest level of data protection. You can update configurations and send command scripts.
- Deploy software updates throughout the enterprise.

The Central Administration Console is a tool for monitoring and managing the clients. The Central Administration Console makes an administrator's job easier, but is not a requirement for protecting your data. IBM Spectrum Protect for Workstations clients can protect your data without the Central Administration Console. If you do not install the Central Administration Console or if the Central Administration Console is not running, your data is still protected by the IBM Spectrum Protect for Workstations clients.

IBM Spectrum Protect for Workstations can store backup copies on a IBM Spectrum Protect server, but there is no requirement to use IBM Spectrum Protect. IBM Spectrum Protect for Workstations is a stand-alone product and has no dependencies on IBM Spectrum Protect.

The following concepts are key to understanding the Central Administration Console: *groups* and *administration folders*:

Groups
: With the Central Administration Console, you can administer many clients at a time. You can filter and select clients based on several criteria, but a typical filter is achieved by assigning clients with similar data-protection needs to the same group.

Administration folders
: The Central Administration Console communicates with clients by sharing information with clients in administration folders.

Groups

Groups allow you to manage many clients with a single action.

A *group* defines a configuration of protection settings for a IBM Spectrum Protect for Workstations client. The same protection settings can be set with the **Settings Notebook** of the client.

A group can have 0 or more client members. All clients that are added to the group adopt the group configuration.

Rather than managing single clients, you can put many clients into one group, and manage all clients in that group with a single action. When you change the configuration of the group, you change the configuration of all client members. In the **Clients** task, you can filter clients by group, then select all members of a group, then perform an action on all selected clients.

For example, assume that you assign all clients in an accounting department to a group. Assume that the accounting department adopts a new tool that produces files of a type that are not currently protected by the IBM Spectrum Protect for Workstations clients. With a single action from the Central Administration Console, you can change the configuration of all IBM Spectrum Protect for Workstations clients in the accounting group to protect the new file type.

Administration folders

Clients gather configuration information, commands, and software updates from administration folders. The Central Administration Console manages clients by sharing information with clients in administration folders.

Managing clients

When the client and the Central Administration Console access the same administration folder, they exchange information in the administration folder. The client sends reports to the folder. The Central Administration Console collects the reports and presents the information to the administrator. The Central Administration Console pushes software updates, configuration information, and command scripts to the administration folder. The client periodically pulls the updates, configuration, and command scripts.

If the Central Administration Console and a client are not configured to access the same administration folder, the Central Administration Console cannot manage that client.

By default, the Central Administration Console service uses a local system account to log on. A local system account can access administration folders on the Central Administration Console server, but cannot access administration folders on shared drives on other computers. If the clients use administration folders on remote computers, run the Central Administration Console service in an account that has access to the remote administration folders.

Determining administration folders for clients

Clients whose configuration files are created with the Central Administration Console access the administration folder that you identify in the Central Administration Console. The Central Administration Console periodically scans the administration folder for reports from new clients. When the client is installed, the client accesses this administration folder, and the Central Administration Console discovers the client. The Central Administration Console locks the value of the administration folder for the new client.

If a IBM Spectrum Protect for Workstations client is not discovered by the Central Administration Console, you can specify the administration folder with the client. In this case, the administration folder defaults to the `\RealTimeBackup\` subfolder of the remote storage area. When such a client is discovered by the Central Administration Console, the Central Administration Console sets and locks the value of the administration folder.

If a remote storage area is not configured, or if the client uses remote storage on a IBM Spectrum Protect server, there is no default administration folder.

IBM Spectrum Protect for Workstations OEM Edition clients have a **Central Administration Settings** panel that you can use to explicitly configure the administration folder location. If the **Central Administration Folder** field is configured, that value overrides the default administration folder location. The Central Administration Console can discover and manage the following clients:

- Clients that are configured with no remote storage
- Clients that are configured with remote storage on a IBM Spectrum Protect

However, you can change the administration folder to a location that is not known to the Central Administration Console. In this case, the Central Administration Console cannot manage the client.

Standard IBM Spectrum Protect for Workstations clients and Starter Edition clients do not have a **Central Administration Settings** panel where a user can explicitly configure the administration folder location. If these clients use IBM Spectrum Protect server remote storage, there is no administration folder. You can configure an administration folder for such a client only by using the **`fpa config-set`** command. If you use the **`fpa config-set`** command to identify a folder that is accessible to the client, the Central Administration Console discovers the client.

The **`fpa config-set`** command sets the administration folder for any client, even one that was discovered by the Central Administration Console. Start the command from a Command Prompt window at the installation directory, for example:

```
fpa config-set GlobalManagementArea="\\MyServer\MyShare\MyAdminFolder"
```

Replace `\\MyServer\MyShare\MyAdminFolder` with the CIFS (Common Internet File System) URL of a folder that is accessible to the client and the Central Administration Console.

Administration folder subfolders

The administration folder contains two levels of administrative subfolders.

Computer-specific subfolders

These folders apply to only one computer. The Central Administration Console communicates with clients through the computer-specific subfolders. The following subfolders are in the computer-specific subfolder:

`Reports`

The client stores status reports in the `Reports` folder. You can view the reports in the Central Administration Console. The full path of the reports folder is *administration_folder_location*\ *computer_name*\BackupAdmin\Reports\.

Downloads

When you put product upgrades or configuration files in the Downloads folder, the client automatically adopts the product upgrades or configuration. The full path is *administration_folder_location**computer_name*\BackupAdmin\Downloads\.

Group administrative subfolders

These folders apply to all computers that share this administration folder. In each group administrative subfolder, there is a Downloads subfolder. When you put product upgrades or configuration files in the Downloads subfolder, all clients that share this group administrative folder automatically adopt the upgrades or configuration.

Maintaining control of the clients

You can maintain control of the clients by upgrading the clients to IBM Spectrum Protect for Workstations and by using a configuration file.

Complete these guidelines to maintain control of the clients:

- Upgrade IBM Spectrum Protect Continuous Data Protection for Files clients to IBM Spectrum Protect for Workstations clients. Upgrading to IBM Spectrum Protect for Workstations eliminates the opportunity for users to set their administration folder location with the **Central Administration Settings** panel.
- Deploy IBM Spectrum Protect for Workstations clients with a configuration file that is created by the Central Administration Console. This configuration file defines an administration folder location that users cannot change.

Related tasks:

"Identifying administration folders" on page 42
Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

"Deploying new clients" on page 41
Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

Information currency

The client information that is listed in the Central Administration Console is as current as the reports received from the clients.

The Central Administration Console scans administration folders on an interval that also can be configured in the Central Administration Console.

The client information in the Central Administration Console is not real-time information. It is delayed by configured communication intervals between the client and the Central Administration Console, and can also be delayed by client issues.

You can find out how to configure email settings and scan intervals in the "Configuring the scan interval and email alert" on page 15 section.

Clients push reports to the administration folder and pull information from the Central Administration Console on an interval that can be configured in the Central Administration Console. The default interval is 1 hour. Beyond the configured interval, a client report can be delayed because of issues with the client. Some issues that can prevent the client from reporting are listed:

- The client computer is turned off.
- The client computer cannot reach the administration folder.
- The IBM Spectrum Protect for Workstations client is not running.

You can determine the information currency for a particular client by examining the date in the **Last Report** column in the **Health** view of the **Clients** task.

You can define an alert condition that is based on the time that elapsed since a client last reported.

Related tasks:

"Configuring the scan interval and email alert" on page 15
Configure the interval that the Central Administration Console uses to scan administration folders to collect information about clients. Configure the Central Administration Console to send an email when an alert arises from a scan. The Central Administration Console scans all administration folders at the interval that you set. During these scans, the Central Administration Console updates the status of clients and discovers new clients.

Chapter 2. Installing the Central Administration Console

An installation wizard helps you to install and configure the IBM Spectrum Protect for WorkstationsCentral Administration Console. During the installation, the wizard requests essential account information that you must provide so that you can log on to the Central Administration Console service. This user account must be a member of the Administrators group.

System requirements

The IBM Spectrum Protect for Workstations Central Administration Console requires a Windows server with minimum levels of hardware and software.

For software and hardware requirements, see IBM Spectrum Protect for Workstations Hardware and Software Requirements (http://www.ibm.com/support/docview.wss?uid=swg21643334).

Installing the Central Administration Console

Install the IBM Spectrum Protect for Workstations Central Administration Console from a product DVD or from an installation program that you can download.

About this task

The installation program for the Central Administration Console is one of the following executable files, depending on your system requirements:

- Microsoft Windows 32-bit systems: `8.1.0-IBM-SP4WKSTNS-CAC-x86_windows.exe`
- Microsoft Windows 64-bit systems: `8.1.0-IBM-SP4WKSTNS-CAC-x64_windows.exe`

You must have administrative privileges to install the Central Administration Console.

Procedure

Complete the following steps to install the Central Administration Console. Several of these installation steps take several minutes to complete. The total installation time is approximately 15 minutes on a typical system.

1. Start the installation by inserting the product DVD into the system DVD drive or double-click the installation executable file that you download.
2. Accept the default language or select your preferred language and click **OK**. The Preparing to Install window is displayed while the installation files are extracted.
3. In the Welcome window, click **Next**.
4. Read the License Agreement and accept the terms of the agreement. Click **Next**.
5. Enter the account details for a valid local system account that is part of the Administrators group. This account is used to log on to the Central Administration Console service. Click **Next**.

   Account information: To be valid for running the Central Administration Console service, a user account must meet the following conditions:

- Must be a member of the Administrators group.
- Must have access to local drives.
- Must have access to administration folders on the network.

Record the details for the local account that is used to log on to the Central Administration Console service. If the account is not valid or if the password is not correct, the Central Administration Console service does not start during the installation process. You can use the Window Services tool to enter the Central Administration Console service information manually after the installation is completed.

6. Accept the default user details that are used to log on to the Central Administration Console service, or enter new values.

   Changes to the default user values: If you delete the default user name and leave the password field blank, the Central Administration Console server is started as Local System but default.
7. Accept the default port values, or enter different port values and click **Next**.
8. Click **Next** to accept the items for installation, or click **Change** to modify items. The Custom Setup for the ISA data collector window is displayed. This function is set to install by default. Click **Next**.
9. Click **Next** to accept the default installation path for the Central Administration Console or click **Change** and enter a different installation path.

   Restriction: You must use ASCII characters for the installation directory name and path. If non-ASCII characters are used in the directory name or path, the installation succeeds but the application fails to operate.
10. If you want to review or change any of your installation settings, click **Back**. To exit the installation, click **Cancel**. To begin the installation, click **Install**. A progress bar indicates that the necessary files are being installed on your computer. A command window opens as the installation program runs several scripts.
11. If a previous version is encountered during the installation, the uninstaller for the previous version is activated. If that uninstall operation is canceled or fails, the Central Administration Console service for the previous version is stopped and disabled. The desktop shortcut for the previous version is removed, and an error message is displayed.

    Required action to continue the installation: Click **OK** in the error message to continue the installation. If the error message is not currently active, click the flashing icon in the toolbar to display the message.
    For instructions about how to manually remove a previous version of the software, see "Uninstalling the Central Administration Console manually" on page 10.
12. Click **Finish** when the installation is completed. When the installation is complete, the installation program starts the Central Administration Console in the default browser.
13. Enter the user account details to log on to the Central Administration Console and click **OK**.

Starting the Central Administration Console GUI

Start the Central Administration Console graphical user interface (GUI) to monitor and manage the IBM Spectrum Protect for Workstations clients. Use the GUI to change the administration settings and group configurations.

About this task

When you are not logged in to the Central Administration Console GUI, the Central Administration Console service continues to monitor clients.

Procedure

Start the Central Administration Console GUI by completing the following steps:

1. Start the GUI by using one of the following methods:
   - Click the desktop icon **IBM Spectrum Protect for Workstations Central Administration Console**.
   - Click **Start** > **All Programs** > **Spectum Protect** > **IBM Spectrum Protect for Workstations Central Administration Console**.
   - Open a web browser on the Central Administration Console server and go to the following URL:

     Port value: The port value that is used in the following example is the default value. You must set the port value to the port that you are using.

     `https://`*`localhost_address`*`:16326/FBFWCentralAdmin`
   - Open a web browser on another computer and go to the following port on the Central Administration Console server:

     `16326/FBFWCentralAdmin`
2. Enter your user name and password, and click **Log in**.
3. To work with the Central Administration Console functions, click one of the items in the task activity list.

   Session expiry time: If the GUI session is inactive for some time, the session expires. The default inactive time is 10 minutes. You might be prompted for your user name and password when you log on after a session timeout.
4. To change the password that you use to log on to the Central Administration Console GUI, complete the following steps:
   a. Click **cacadmin** > **Change password**.
   b. Enter the new password in the **Verify new password** field.
   c. Click **OK**.
5. To log out of the Central Administration Console GUI, click **cacadmin** > **Logout**.

Related tasks:

"Starting or stopping the Central Administration Console service" on page 63
The Central Administration Console service monitors IBM Spectrum Protect for Workstations clients. Whether you open the Central Administration Console GUI, the Central Administration Console service monitors clients and sends alerts. The Central Administration Console service starts after a successful installation and every time the computer starts. In most cases, you do not have to start or stop the Central Administration Console service. You can start or stop the service to troubleshoot the service functionality.

Uninstalling the Central Administration Console

The standard method to uninstall IBM Spectrum Protect for Workstations Central Administration Console is to delete the software from the list of programs in the Windows Programs list. If the standard Windows method of uninstalling the software fails, you must uninstall the software manually.

About this task

You must have administrative privileges to uninstall IBM Spectrum Protect for Workstations Central Administration Console.

Procedure

Complete the following steps to uninstall the Central Administration Console by using the standard Windows method:

1. Click **Start** > **Control Panel** > **Programs** > **Uninstall a program**.
2. Select **IBM Spectrum Protect for Workstations Central Administration Console**.
3. Right-click and click **Uninstall**.

What to do next

If the uninstallation fails, see “Uninstalling the Central Administration Console manually.”

Uninstalling the Central Administration Console manually

If an attempt to uninstall a version of IBM Spectrum Protect for Workstations Central Administration Console fails, you must remove the software manually.

Before you begin

When you upgrade from an earlier version of IBM Spectrum Protect for Workstations, you must uninstall the previous version of the Central Administration Console. For instructions about how to uninstall the Central Administration Console by using the standard method, see “Uninstalling the Central Administration Console.”

About this task

If the standard method of uninstalling the previous version of Central Administration Console fails, you must uninstall the software manually. In versions of IBM Spectrum Protect for Workstations prior to version 7.1.1, the Central Administration Console ran on the Tivoli Integrated Portal. If no other programs are using the Tivoli Integrated Portal, this software must also be removed as part of the manual uninstallation process.

Procedure

Complete the following steps to manually uninstall the Central Administration Console.

1. Remove the Central Administration Console by completing the following steps:

a. Delete the IBM Spectrum Protect for Workstations installation directory that is relevant to your installation. Depending on your system, the installation directory is in one of the following locations:

```
C:\Program Files\Tivoli\TSM\IBM FB4WCA Console
C:\Program Files (x86)\Tivoli\TSM\IBM FB4WCA Console
```

b. Delete the following directory, if the directory exists:

```
C:\fbfw_tmp
```

c. Click **Start** > **Run** and run `regedit.exe`. Delete the following registry entries if these entries exist:

```
HKEY_LOCAL_MACHINE\SOFTWARE\FbfwCA

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\FbfwCA

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
App Management\ARPCache\IBM FB4WCA Console

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
IBM FB4WCA Console

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CAC
```

2. Remove Tivoli Integrated Portal by completing the following steps:

a. Locate and run either of the following batch files, depending on where Tivoli Integrated Portal is installed on your system:

```
C:\IBM\tivoli\tipv2\profiles\TIPProfile\bin\zaptip.bat
C:\IBM\tivoli\tipv2_fbfw\profiles\TIPProfile\bin\zaptip.bat
```

If the batch file command fails or the batch file is not present, continue to the following steps.

b. Remove the Tivoli Integrated Portal installation directory. Depending on your installation, Tivoli Integrated Portal is installed in one of the following directories:

```
C:\IBM\tivoli\tipv2\
C:\IBM\tivoli\tipv2_fbfw
```

c. Click **Start** > **Run** and run `services.msc`. Review the services list to see whether any Tivoli Integrated Portal services are running. For example:

`V2.1_TIPProfile_Port_`*16310*

d. If Tivoli Integrated Portal services are running, stop the services. Click **Start** > **Run**, run `regedit.exe` and delete the entries. For example:

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\IBMWAS70Service
- V2.1_TIPProfile_Port_16310

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\IBMWAS70Service
- V2.1_TIPProfile_Port_16310
```

3. If Tivoli Integrated Portal fails to uninstall correctly, some entries might remain in the Deployment Engine database. Remove any Deployment Engine entries by completing the following steps:

a. Run the following command to list the Deployment Engine entries and look for `TIPCore` and `ewas` entries.

Location of the Deployment Engine directory: The Deployment Engine might be installed in the following directory on 64-bit systems:

`C:\Program Files (x86)`

`C:\"Program Files\IBM\Common\acsi\bin\listIU.cmd"`

If the Deployment Engine database contains Tivoli Integrated Portal entries only

Remove the Deployment Engine by running the following commands:

```
 C:\"Program Files\IBM\Common\acsi\setenv.cmd"
 C:\"Program Files\IBM\Common\acsi\bin\si_inst.bat"
-r -f
```

If the Deployment Engine database contains entries for other products and entries for Tivoli Integrated Portal

Delete only those Deployment Engine entries that are related to Tivoli Integrated Portal. In the following example, the entries are typical but the value of `RootIU` might change from release to release. You can verify the `RootIU` value by using the `listIU.cmd -v` command.

```
C:\"Program Files\IBM\Common\acsi\bin\manageiu.bat"
-o delete -r

C:\"IBM\Tivoli\Tipv2_fbws" -d
RootIUTypeID[2ADC4A33F09F4E85AD27963E850290C3,2.2.0.9]

C:\"Program Files\IBM\Common\acsi\bin\manageiu.bat"
-o delete -r

C:\"IBM\Tivoli\Tipv2_fbws" -d
RootIUTypeID[C00DA95AFD9B7E0397153CD944B5A255,7.0.0.15]
```

b. Close down your system.

c. Start your system again.

What to do next

Even if you successfully complete the manual process for uninstalling the Central Administration Console, you must ensure that all components of Tivoli Integrated Portal are removed. For instructions about how to verify that all components of Tivoli Integrated Portal are removed, see "Cleaning up the removal of Tivoli Integrated Portal components."

For more information, see Recovering from a failed uninstallation on Windows systems.

Cleaning up the removal of Tivoli Integrated Portal components

If you manually uninstall a version of IBM Spectrum Protect for Workstations Central Administration Console, you must ensure that all of the software components are correctly removed.

Before you begin

When you manually uninstall the Central Administration Console, you must also remove the Tivoli Integrated Portal, providing that no other programs are using the software. For instructions about how to manually remove the Central Administration Console, see "Uninstalling the Central Administration Console manually" on page 10.

About this task

When you remove the Tivoli Integrated Portal manually, you must ensure that no components for this software remain on your system.

Procedure

Complete the following steps to ensure that all components for the Tivoli Integrated Portal are removed from your system.

1. Remove any Tivoli Integrated Portal components that might still be running on your system, by completing the following steps:
   a. Click **Start** > **Run** and run `services.msc`. Review the services list to see whether any Tivoli Integrated Portal services are running. For example:
   ```
   V2.1_TIPProfile_Port_16310
   ```
   b. If Tivoli Integrated Portal services are running, stop the services. Click **Start** > **Run**, run `regedit.exe` and delete the entries. For example:
   ```
   HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\IBMWAS70Service
   - V2.1_TIPProfile_Port_16310

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\IBMWAS70Service
   - V2.1_TIPProfile_Port_16310
   ```
   c. Close down your system.
   d. Start your system again.
2. If Tivoli Integrated Portal fails to uninstall correctly, some entries might remain in the Deployment Engine database. Remove any Deployment Engine entries by completing the following steps:
   a. Run the following command to list the Deployment Engine entries and look for `TIPCore` and `ewas` entries.

   Location of the Deployment Engine directory: The Deployment Engine might be installed in the following directory on 64-bit systems:
   ```
   C:\Program Files (x86)
   ```
   ```
   C:\"Program Files\IBM\Common\acsi\bin\listIU.cmd"
   ```
   If the Deployment Engine database contains Tivoli Integrated Portal entries only
   Remove the Deployment Engine by running the following commands:
   ```
    C:\"Program Files\IBM\Common\acsi\setenv.cmd"
    C:\"Program Files\IBM\Common\acsi\bin\si_inst.bat"
   -r -f
   ```
   If the Deployment Engine database contains entries for other products and entries for Tivoli Integrated Portal
   Delete only those Deployment Engine entries that are related to Tivoli Integrated Portal. In the following example, the entries are typical but the value of `RootIU` might change from release to release. You can verify the `RootIU` value by using the `listIU.cmd -v` command.
   ```
   C:\"Program Files\IBM\Common\acsi\bin\manageiu.bat"
   -o delete -r

   C:\"IBM\Tivoli\Tipv2_fbws" -d
   RootIUTypeID[2ADC4A33F09F4E85AD27963E850290C3,2.2.0.9]

   C:\"Program Files\IBM\Common\acsi\bin\manageiu.bat"
   -o delete -r

   C:\"IBM\Tivoli\Tipv2_fbws" -d
   RootIUTypeID[C00DA95AFD9B7E0397153CD944B5A255,7.0.0.15]
   ```
   b. Close down your system.

c. Start your system again.
3. Ensure that the directory where Tivoli Integrated Portal was installed is empty.

   Default installation directory:

   `C:\IBM\Tivoli\ tipv2_fbfw`

Related tasks:

"Uninstalling the Central Administration Console manually" on page 10
If an attempt to uninstall a version of IBM Spectrum Protect for Workstations Central Administration Console fails, you must remove the software manually.

Backing up the Central Administration Console database

If the Central Administration Console database is removed or deleted, the database is created again the next time the server is started. However, the new database does not contain the most recent data. After you install the Central Administration Console, set up a scheduled backup for the Central Administration Console. The database must be backed up frequently to ensure that you do not lose data.

Procedure

To ensure that you have the most recent data in the database, complete the following steps:

1. Configure IBM Spectrum Protect for Workstations for backups on your system.
2. Set up the following database folder for frequent backups:

   Install_Location\CAC\wlp\usr\servers\FBFWCAServer\fbfw\CA_DB

   Tip: For information about how to set up IBM Spectrum Protect for Workstations for backups, see the IBM Spectrum Protect for Workstations Client Installation and User's Guide.

Chapter 3. Configuring the Central Administration Console

You can configure administrative tools that monitor IBM Spectrum Protect for Workstations clients. This monitoring includes identifying the conditions that trigger alerts, and identifying who is alerted.

Configuring the Central Administration Console monitoring tools

You can configure the Central Administration Console tools that alert you to potential problems with IBM Spectrum Protect for Workstations clients.

Configuring the scan interval and email alert

Configure the interval that the Central Administration Console uses to scan administration folders to collect information about clients. Configure the Central Administration Console to send an email when an alert arises from a scan. The Central Administration Console scans all administration folders at the interval that you set. During these scans, the Central Administration Console updates the status of clients and discovers new clients.

About this task

The Central Administration Console can automatically send email notifications when there is a potential problem. To complete this task, you must identify your SMTP mail server.

Procedure

1. Open the Central Administration Console GUI.
2. Click **Administration Settings**.
3. In the Alerts Configuration section, click **Actions** > **Configure the Scan Interval and Email for Alerts**.
4. In the Scan Setting section, set the scan frequency.
5. In the Email Configuration section, provide the information for the email server.
   - SMTP email server. The SMTP email server has an address in the following format: `smtp.mailserver.com`, for example `smtp.gmail.com`.
   - Email server authorization information
   - Email server port number
6. Select the encryption type. For SSL mail, you must download the certificate from the email server. The download method depends on the server. With some servers, you can connect through Mozilla Firefox and download the SSL certificate from the address bar. Other servers require that you to use OpenSSL. If you use OpenSSL, complete the following steps:
   a. Start OpenSSL by running the **`openssl.exe`** command.
   b. To connect to the mail server, enter the following commands in the OpenSSL command window, where *smtp.mailserver.com* and *portnumber* are specific to the mail server that is used:
   ```
   OpenSSL> s_client -connect smtp.gmail.com:465
   OpenSSL> s_client -connect smtp.mailserver.com:portnumber
   ```

c. Copy the command output, including the begin certificate and end certificate tags. Save the certificate into a file named `email.cert`.

```
----BEGIN CERTIFICATE-----
...
...
...
----END CERTIFICATE-----
```

d. Copy the `email.cert` file into the *Install_Location\TSM\CAC\wlp\usr\servers\FBFWCAServer* directory.

e. Open another command window and go to the `FBFWCAServer` directory.

f. If a certificate was previously imported or an error displays that indicates that the `alias mykey` is already present, run the following command:

```
"%CAC_INSTALL_DIR%\java\jre\bin\java" -cp fbfwca.jar com.tivoli.fbfw.ca.backend.security.CaSec
```

g. To add the email certificate, enter the following command in the `FBFWCAServer` directory:

```
"%CAC_Install_Location%\java\jre\bin\java"
-cp fbfwca.jar com.tivoli.fbfw.ca.backend.security.CaSecurity -add email.cert
```

h. Stop and start the Central Administration Console server.

7. To prevent alert emails from being blocked as spam, specify an address in the field **Specify the From email address to be used for all alert emails sent via the SMTP server**. This address must be a valid email address on the SMTP server.
8. To test the alert settings, enter an email address in the **Test** email field and click **Test**.
9. To save the alert settings, click **OK**.

Related tasks:

"Identifying administration folders" on page 42
Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

Defining alert conditions

Define the conditions that trigger an alert. Determine whether the conditions trigger a change in the health status of a client, or an e-mail notification, or both.

Before you begin

If any alerts trigger e-mail notifications, you must identify the SMTP e-mail server with the **Configure the Scan Interval and Email for Alerts** action.

Procedure

1. Open the **Administration Settings** task. The administration tables are displayed.
2. In the **Alerts Configuration** section, click the **Actions** menu.
3. Click **Define Alert Conditions**. The **Define Alert Conditions** panel is displayed.
4. Type the name of the alert.
5. Provide a message for operators who are notified by the alert. The message appears in e-mail notifications and in the **Alerts** table in the **Health Monitor** task.
6. Identify the e-mail addresses of operators who receive alert notifications.
7. In the **Set client health status** section, determine if these alert conditions change the health status of a client.

8. In the **Conditions** section, identify the conditions that trigger this alert.
9. Click **OK**. The new alert conditions appear in the **Alerts Configuration** table.

Related tasks:

"Configuring the scan interval and email alert" on page 15
Configure the interval that the Central Administration Console uses to scan administration folders to collect information about clients. Configure the Central Administration Console to send an email when an alert arises from a scan. The Central Administration Console scans all administration folders at the interval that you set. During these scans, the Central Administration Console updates the status of clients and discovers new clients.

Modifying alert conditions

Change the conditions that trigger an alert or determine whether the conditions trigger a change in the health status of a client, or an email notification, or both.

Before you begin

If any alert conditions trigger email notifications, you must identify the SMTP email server with the **Configure the Scan Interval and Email for Alerts** action.

Procedure

1. Open the **Administration Settings** task. The administration tables are displayed.
2. In the **Alerts Configuration** section, click the **Actions** menu.
3. Click **Modify Alert Conditions**. The **Modify Alert Conditions** panel is displayed.
4. Change any of part of the alert conditions except the alert name.
5. Click **OK**. The modified alert conditions are saved by the Central Administration Console.

Related tasks:

"Configuring the scan interval and email alert" on page 15
Configure the interval that the Central Administration Console uses to scan administration folders to collect information about clients. Configure the Central Administration Console to send an email when an alert arises from a scan. The Central Administration Console scans all administration folders at the interval that you set. During these scans, the Central Administration Console updates the status of clients and discovers new clients.

Creating a script for clients

Create your own, custom scripts for clients. Create commands or use commands that are provided with the Central Administration Console.

About this task

A client can run a script automatically when the client is first discovered by the Central Administration Console. A typical script at initial discovery contains a command to back up all files. This action creates an initial backup copy of all files that you identified for protection. Without this action, files are backed up only when they are changed.

You can also send a script to clients to address a problem. For example, if your network is impacted by remote backup activity, you can send a command to specific clients to immediately pause remote backup activity. If you want to reduce the network traffic that occurs at a later, scheduled backup time, you can send a command to specific clients to immediately back up email files and other files that are typically backed up at the scheduled time.

Procedure

1. Open the **Administration Settings** task. The three administration tables are shown.
2. In the **Custom Scripts** section, click the **Actions** menu.
3. Click **Create a Script**. The **Create a Script** panel is shown.
4. Type a name for the script. Optionally, you can provide a description.
5. In the **Number of simultaneous clients** field, enter the maximum number of clients that can run this script at the same time. Some commands, such as **Back up all files**, can use considerable network resources. You can limit the number of clients that run this script at the same time.
6. In the **Script acceptance timeout** field, enter the maximum time for the client to begin running the script. If the client does not start the script in this time, there are the following consequences:
   - The script is removed from the administration folder of the client.
   - The client is no longer counted as one that is running the script simultaneously with other clients.
   - The audit log records that the client failed to start the script in this time.
   - The script is sent to the client at a later time.
7. In the **Script completion timeout** field, enter an estimate of the time it takes for a client to complete the script. The Central Administration Console is not notified when a client completes a script. When the **Script completion timeout** time elapses, the Central Administration Console removes the client from the list of clients that are running the script. If the number of clients running the script is constrained by the value of **Number of simultaneous clients**, the Central Administration Console can send the script to another client.
8. In the **Script** box, select a command from the list. The list contains useful commands. You can also create your own commands by directly editing the text area. The command is appended to the end of the list of commands.
9. Add more commands, if needed. You can add, modify, or delete commands by editing the text area.
10. Click **OK**. The new script is shown in the **Custom Scripts** table.

What to do next

You can send this script to one or more clients.

Related tasks:

"Sending a script to clients" on page 59
You can create scripts to manage activities or resolve issues of IBM Spectrum Protect for Workstations clients. You can send your customized scripts to one or more clients.

Enhancing Central Administration Console performance by modifying JVM memory settings

You can enhance the performance of the Central Administration Console by modifying the memory settings for the Java™ virtual machine (JVM).

Before you begin

The value of the JVM `maximumHeapSize` setting directly affects the ability of the Central Administration Console to manage many IBM Spectrum Protect for Workstations clients. When the value is too low, the Central Administration Console might become slow to respond, fail to load, or even stop.

About this task

You can modify the `maximumHeapSize` setting to prevent performance issues when you are managing many clients. The following table shows the settings for the best results for managing clients on a system with 32 GB of memory.

Table 1. JVM memory settings for managing different numbers of clients

Number of clients	JVM `maximumHeapSize` setting
500,000	2048 MB
800,000 or more	4096 MB

Procedure

Complete the following steps to modify the `maximumHeapSize` setting:

1. Open the Central Administration Console installation directory:
   `*Install_Location*\Tivoli\TSM\CAC\wlp\usr\servers\FBFWCAServer`
2. In the `FBFWCAServer` directory, open the `jvm.options` file.
3. Review the values of the following JVM parameters:

Table 2. JVM parameters for memory settings

JVM Parameter	Description	Default value	Memory size
`-Xms*`	Initial memory allocation pool for a JVM	`-Xms64m`	64 MB
`-Xmx*`	Maximum memory allocation pool for a JVM	`-Xmx1024m`	1024 MB

4. To modify the maximum heap size, edit the `-Xmx***` parameter. For example, to increase the maximum heap size of the JVM to 1536 MB, change the parameter value to `-Xmx1536m`.
5. Save the `jvm.options` file.
6. Stop and start the Central Administration Console server.

Chapter 4. Administering IBM Spectrum Protect for Workstations

Information is available for administering IBM Spectrum Protect for Workstations with the Central Administration Console.

Preparing to manage groups of clients

Prepare for central administration by organizing users into groups with similar data-protection needs. Create groups in the Central Administration Console.

Planning groups of users

Determine which users have similar needs, and organize these users into groups.

Before you begin

You need some knowledge of the applications, network issues, and business processes of the IBM Spectrum Protect for Workstations users.

About this task

Keep in mind that group membership is not static. If you find that the original groups need to change, you can move clients from one group to another.

However, if you move a client to a group that uses a different storage target, existing backup copies cannot be restored by the client.

Procedure

1. Consider the backup protection needs of the users. Consider the following items:
   - What file types must be continuously protected?
   - Are there some files that must be excluded from protection? (This can save storage and network resources).
   - Do some folders need to be vaulted?
   - How much space is needed for backup copies on the user's computer and on a remote storage device?
   - What mail programs must be protected?
   - What other files must be protected on a schedule?
   - Will the administration folder be unique for each group, or will several groups share the administration folder?
   - When files are transferred to remote storage, do they need to be encrypted or compressed?
   - When files are transferred to remote storage, what are appropriate restrictions on file size and transfer rate?
2. As you consider the protection needs, note which users have the same or similar needs. Users that have similar needs can be managed as a group.

Example

As an example, assume a small business with the following teams.

- The engineering team use similar tools for their CAD (Computer-assisted design) work. All members of this team require protection of their CAD files and email.
  - Some engineers work at the main office. They are the only users whose workstations are connected to a backup server by a high-speed data connection.
  - Some engineers work at remote locations.
- Members of the sales team create sales presentations and keep in touch with their customers. They need protection of their presentation files, customer information spreadsheet files, and email. Occasionally when traveling they can go for long periods without network access to the remote backup server. At these times, they can use local storage on their mobile computers for backups.
- Members of the accounting team must protect their spreadsheet files, accounting reports, and email.
  - The principal accountant has some unique responsibilities. When an accounting cycle closes, you want to vault her files associated with that accounting project.

You decide to organize the users by the teams listed, with two exceptions:

- You organize the engineers into a local group and a remote group.
- The principal accountant has unique needs. You can create a group for this one client, or you can manage it with no group. When you create a group, the Central Administration Console stores the configuration settings. With stored configuration settings, you can generate the configuration file or create a similar configuration file for a user with slightly different needs. You decide to create a group for this one user.

Each of these teams has different data-protection needs. All members within a group have the same data-protection needs, and can be served by the same data-protection configuration.

What to do next

When you decide how to organize the users, you are ready to create the groups.

Related concepts:

"Groups" on page 2
Groups allow you to manage many clients with a single action.

Related tasks:

"Creating a group" on page 23
Use the **Groups Configuration** task to create a group from scratch, or to create a group that is like an existing group. You can use a group to manage many clients at one time. A group defines a client configuration.

Creating a group

Use the **Groups Configuration** task to create a group from scratch, or to create a group that is like an existing group. You can use a group to manage many clients at one time. A group defines a client configuration.

About this task

The **Groups Configuration** wizard of the Central Administration Console is like the initial configuration wizard of the client. Both wizards guide you to configure the data-protection settings for clients. Unlike the initial configuration wizard of the client, the **Groups Configuration** wizard includes all data-protection settings, and identifies a name and description for the group.

Procedure

1. Open the **Groups Configuration** task. The table of groups is displayed.
2. From the **Actions** menu, click **Create a Group**. The **Groups Configuration** wizard opens.

   Create a Group provides default settings, which you can modify in the wizard.

   Create a Group Like an Existing Group provides settings of an existing group, which you can modify in the wizard. Choose **Create a Group Like an Existing Group** if the new group is like an existing group. **Create a Group Like a Client** is enabled when you select one group from the table. The **Welcome** page of the **Groups Configuration** wizard is displayed.
3. Accept the default configuration settings, or enter your own settings. In the **Group** field, enter alphanumeric characters or any of the following special characters for the group name:
   - Dash (`-`)
   - Period (`.`)
   - Space ( )
   - Underscore (`_`)

   The following example is a valid group name: `valid_name for a group.`
4. Click **Finish** to create the group. The new group is added to the table of groups.

What to do next

You can add existing clients to this group, and they adopt the configuration.

If you associate this group with an administration folder, you increase your ability to manage clients in two ways:

- You can use the configuration of this group to create a configuration file for an installation package.
- When clients initially contact the administration folder, they become members of this group.

Related concepts:

"Groups" on page 2
Groups allow you to manage many clients with a single action.

"**Groups Configuration** notebook: field explanations" on page 25
You use the **Groups Configuration** notebook to configure the data-protection settings for IBM Spectrum Protect for Workstations clients.

Related tasks:

"Creating a group with the configuration of an existing client"
Create a group with a configuration that is imported from an existing client.

"Deploying new clients" on page 41
Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

"Identifying administration folders" on page 42
Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

Creating a group with the configuration of an existing client

Create a group with a configuration that is imported from an existing client.

Before you begin

To create a group with the configuration of an existing client, the Central Administration Console must discover a client.

Procedure

Complete the following steps to create a group with a configuration that is imported from an existing client:

1. Open the **Clients** task. The **Clients** panel displays the following tabs: **Health**, **Storage**, and **Deployment**.
2. Select a client.
3. Click the **Actions** menu.
4. Click **Create a Group Like a Client**. The Group Wizard opens, populated with the same configuration values as the group that is associated with the client.
5. In the Group Wizard, alter any of the configuration values that you want to modify.
6. Review the **Groups Configuration** task to find the new group in the table of groups.

What to do next

You can add clients to the group. You can use the configuration of this group when you deploy new clients.

Related tasks:

"Creating a group" on page 23
Use the **Groups Configuration** task to create a group from scratch, or to create a group that is like an existing group. You can use a group to manage many clients at one time. A group defines a client configuration.

"Deploying new clients" on page 41
Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

Modifying all clients in a group

You can modify the data protection configuration of all clients in a group.

Before you begin

This task assumes the following conditions:

- The Central Administration Console discovered clients.
- Clients are assigned to a group.

About this task

When you modify a group, the Central Administration Console automatically sends the new configuration to all clients in the group.

Procedure

1. Open the Central Administration Console and click **Groups Configuration**.
2. Select the group that you want to modify.
3. Click **Actions** > **Modify a Group**.
4. In the **Groups Configuration** notebook, modify the configuration settings for the group.
5. Click **OK**.

Related concepts:

"**Groups Configuration** notebook: field explanations"
You use the **Groups Configuration** notebook to configure the data-protection settings for IBM Spectrum Protect for Workstations clients.

"Modifying the data protection configuration of a single client" on page 60
Data protection requirements might vary for different clients. You can modify the data protection configuration of a single client.

Related tasks:

"Deploying software updates to existing clients" on page 58
Deploy software updates to IBM Spectrum Protect for Workstations clients that are already installed.

Groups Configuration notebook: field explanations

You use the **Groups Configuration** notebook to configure the data-protection settings for IBM Spectrum Protect for Workstations clients.

The **Groups Configuration** notebook of the Central Administration Console is similar to the **Settings Notebook** of the client.

Continuous Protection panel of Groups Configuration

Use the **Continuous Protection** panel to set the maximum space on local storage for backup copies and the maximum versions of backup copies on local storage.

How many versions to keep field

IBM Spectrum Protect for Workstations can save more than one backup version of each file. When you restore a file, you can choose which version of the file you want to restore. When the configured number of versions is reached, older versions of a file are deleted. Keeping more versions requires more local storage space, but allows you more choices when restoring a file.

Maximum space for backups field

Specify how much space to use for all backup copies on local storage. When the storage area becomes full, older versions of files are deleted until the storage area is at about 80 percent of the configured maximum. If, after deleting all versioned backup copies, local storage space is still insufficient, IBM Spectrum Protect for Workstations will delete the oldest non-versioned files.

Note: No warning message displays when the maximum space is reached.

The default space for local backups is 500 MB.

Note: If you try to back up a file which is larger than the space you have allocated for your storage area, IBM Spectrum Protect for Workstations purges all older versions of your files, and then fails to back up the file. Make sure that the maximum space for your storage areas is greater than the file size limit in the **Advanced** page of the IBM Spectrum Protect for Workstations.

Continuous protection level list

IBM Spectrum Protect for Workstations offers two levels of protection for your files: continuous protection and scheduled protection.

Use this box to select which storage areas to use for continuously protected files.

None Files are not protected.

Local storage only
IBM Spectrum Protect for Workstations creates backup copies only on the local storage area.

Remote storage only
IBM Spectrum Protect for Workstations creates backup copies only on the remote storage area.

Local and remote storage
IBM Spectrum Protect for Workstations creates backup copies on both the local and remote storage areas. This choice provides the most protection for your files, and is the default choice.

If your continuous protection level includes local storage, IBM Spectrum Protect for Workstations creates backup copies in the `\RealTimeBackup\` folder on the nonremovable drive with the most free space.

Note: The client can specify the drive for local storage, but the Central Administration Console cannot. The Central Administration Console defines a configuration that potentially applies to many clients, and it is possible that not all the target computers have the same hardware configuration. Hence, the Central Administration Console configuration specifies the default drive for local storage, which is the nonremovable drive with the most free space.

Files to Protect panel of Groups Configuration

Enter the files and folders that you want to continuously protect, and the files and folders that you want to vault. Exclude files from backup protection and from vaulting.

Enter one file specification per line. You can use wildcard characters in the file specifications.

For example, assume that you want to protect all files in `c:\Projects\`, `c:\Contacts\`, and `d:\Art\`. However, you do not want to protect anything with `\junk\` in the file path. You also do not want to protect any files that end with `.tmp`.

- In the **Folders and files** box, enter the following command:

  ```
  c:\Projects\*
  c:\Contacts\*
  d:\Art\*
  ```

- In the **Excluded folders and files** box, enter the following command:

  ```
  \junk\
  *.tmp
  ```

The following topics provide conceptual information to help you protect the correct files.

Protected drives:

All files that meet the include and exclude specifications, and that appear to IBM Spectrum Protect for Workstations as internal drives, are protected.

In some cases, an external USB drive looks like an internal drive, and IBM Spectrum Protect for Workstations tries to protect the files on that drive. If you do not want to protect that drive, add the drive letter to the exclusion list so that all files on the USB drive are excluded from protection. For example, if your `E:` drive is a USB drive, add `E:\` to the list of excluded items.

Including and excluding files from protection:

Protected files are specified by including files and by explicitly excluding files.

Continuous and scheduled protection (not vaulted)

IBM Spectrum Protect for Workstations keeps a list of files that are included for protection, and a list of files that are explicitly excluded from protection. The list of included files is separated into those files that are included for continuous protection, and those files that are included for scheduled protection. If a file is excluded, it is excluded from both continuous and scheduled protection.

- A file is on the include list for continuous protection if it is defined in the **Protected Folders and Files** field in the **Files to Protect** panel of the **Groups Configuration** notebook of the Central Administration Console.
- A file is on the include list for scheduled protection if it is defined in the **Email Protection** panel in the **Groups Configuration** notebook of the Central Administration Console. A file can be defined in the **Email application data files or folders** field or in the field of additional files or folders you want to be backed up when your email is backed up.

- A file is on the exclude list if it is defined in the **Excluded Folders and Files** field in the **Files to Protect** panel in the **Groups Configuration** notebook of the Central Administration Console.
- If a file (or folder) is on the exclude list, it is not protected by continuous protection or by scheduled protection. Even if the file or folder is also on an include list, it is not protected.
- If a file is on an include list and not on the exclude list, it is protected.
- If a file is not on an include list, it is not protected.
- It is possible that a file can be on both the include list and the exclude list.

The following table summarizes the interaction of inclusion and exclusion.

Table 3. Inclusion and exclusion. File protection by Include list and Exclude list.

	File is not specified in Include list.	**File is specified in Include list.**
File is specified in Exclude list.	File is not protected.	File is not protected.
File is not specified in Exclude list.	File is not protected.	File is protected.

If you have leading or trailing blank spaces in your file specifications, or if you use wildcards in your file specifications, the specifications in your files list can match more than one folder or file. See "Wildcard characters in file specifications" for an explanation of how specifications match file and folder names.

For example, consider a small variation to an excluded specification: `\temp\`. If you use instead `\temp` (without the closing folder delimiter), there is a different effect. This small change has a potentially large impact. All files which have `\temple`, `\temptation\`, `\temperature\`, `\template\`, and other variations of `\temp*`, would be excluded from protection.

Consider another example. You choose to exclude `*.gif` so you can avoid backing up files saved by your browser when you open different websites. This specification also excludes all `.gif` files in `\My Pictures\` folder.

Vaulted folders

Vaulted folders, and the files in them, are not affected by the lists of files that are included for continuous or scheduled protection. However, excluded files and folders are not vaulted. All objects that you define in the **Vaulting** box in the **Files to protect** panel of the **Groups Configuration** notebook of the Central Administration Console are vaulted, unless they are excluded.

Wildcard characters in file specifications:

You can use wildcard characters to specify the files that you want to protect.

You can enter the complete path of a file that you want to protect. The complete path must match a single file. You can use asterisks and blanks as wildcard characters to specify several files.

An asterisk matches any number of characters in a file path. If there are no asterisks, IBM Spectrum Protect for Workstations matches any file whose fully expanded path name has that exact pattern anywhere in the path or filename. The pattern is not case-sensitive.

Apply the following guidelines for using wildcard characters:

- If there are no asterisks, blank spaces are interpreted as asterisks before or after the pattern. For example, `\myDocs\` and `*\myDocs\*` yield the same matches. If there are asterisks in the pattern, blank spaces do not match any characters before or after the pattern. For example, `\myDir\`, `*\myDir\`, and `\myDir\*` can yield three different matches.

  For example, assume a pattern `fish`. This pattern matches the following files and folders:
  - `C:\dir\fish.doc`
  - `C:\fish\anyfile.doc`
  - `c:\Dirfishfood\something`
- If the file specification includes slashes, for example `\fish\`, the specification matches any object with `\fish\` somewhere in the path. For example, this pattern produces the following matches and non-matches:
  - Matches `C:\fish\anyfile.doc`
  - Does not match `C:\dir\fish.doc`
  - Does not match `c:\Dirfishfood\something`

The following table provides examples of how patterns match files and folders.

Table 4. File and folder pattern matches

Pattern	Matches for folders and files on your computer:
\myDir\ or \mYdiR\ or *\myDir* or *\mydir*	c:\myDir\ c:\myDir\Contacts\ c:\myDir\Contacts\contacts.txt c:\Projects\myDir\ c:\Projects\myDir\myThings\ c:\Projects\myDir\myThings\things.doc c:\Projects\myDir\myThings\myPhoto.jpg d:\Notes\myDir\
*\myDir\	c:\myDir\ c:\Projects\myDir\ d:\Notes\myDir\
d:*\mydir*	d:\Notes\myDir\
\my best	c:\Books\My Best.doc c:\Photos.jpg\My Best Photo\ c:\Photos.jpg\My Best Photo\Best.jpg f:\Projects\My Best Project\ f:\Projects\My Best Project\Dream.xls
.jpg	c:\Photos.jpg\ c:\Photos.jpg\myHouse.bmp c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
*.jpg	c:\Photos.jpg\ c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
E:\ E:*	All files and folders on the E: drive.

Vault duration:

You can specify the duration of vaulting by using special folder names. Files in these folders are vaulted for a specific period. After the time expires, the files are not vaulted.

To specify duration of vaulting, create a folder that is named `\KeepSafe\` in any vaulted area. In the `\KeepSafe\` folder, create folders that indicate the vaulting period. For example, `C:\MyImportantDir\KeepSafe\Retain 3 years\`. Any files that are created in that folder are prevented from alteration or deletion for three years. After the expiration time, the file is no longer vaulted. There are three ways to indicate the vaulting period. Each way requires that you use a keyword in the folder name.

1. **`\KeepSafe\RetainForever\`**
   Files in this folder are vaulted forever. Such material can never be moved to another folder with shorter vaulting duration. Material can be moved within the folder tree and to other folders of the same duration.
2. **`\KeepSafe\Retain Duration\`**

   Specify exact vaulting periods by using English terminology. Duration is specified by a combination of the following time units:

   Years

   Days

   Hours

   Minutes

   Seconds

   Use 1 or more time units. Each time unit that you use must be preceded by a number up to 5 digits long. You can include spaces or underlines or dashes and mix case in the folder name. The following are valid examples:

   ```
   \Retain23days4hours\
   \Retain 3years\
   \Retain_3years\
   \Retain-23DAYS_4minutes\
   \Retain 1000 days\
   ```
3. **`\KeepSafe\RetainUntil Date\`**
   Specify a date after which the vaulting expires. The date must include year, month, and day in the following format: `yyyymmddhhmmss`. The hours, minutes, and seconds are optional. The default time is 00:00:00. The following examples specify valid dates:

   ```
   \RetainUntil20191231235959\
   \RetainUntil 20200101\
   \RetainUntil20200101\
   \RetainUntil_20200101\
   ```

Note: You cannot create a `\Retain...` folder within a vaulted `\Retain...` folder. You cannot move material that is in one vaulted `\Retain...` folder to a `vaulted` `\Retain...` folder that has an earlier expiration date.

Email Protection panel of Groups Configuration

Select the email applications and other files that you want to protect on a schedule. Select a schedule for protection.

Because email files typically are large, they are not backed up continuously, but only on the schedule that you select.

Email files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, IBM Spectrum Protect for Workstations backs up the email files when the remote storage area becomes available.

Email Application list

Select one of the email applications in the list.

If your application is not listed, select **Other**.

Email application data files or folders field

If you choose your email application from the **Email Application** list, the default file type for that application appears in this box, and you are not able to update the file specification. You can update this field only if you select **Other** in the **Email Application** list.

Additional files or folders you want to be backed up when your email is backed up field

Identify more files or folders to back up on the schedule. You can use a specification with wildcards to identify files. Enter each specification on a separate line.

How many versions to keep field

Indicate how many backup versions to save. The value applies to email files and other files that are backed up on a schedule. For example, if you select 3, the most recent three backup versions are saved. When the next backup version is created, the oldest version is deleted. If you need to restore a file, you can choose which of the three most recent backup copies you want to restore.

How often to protect your email list

You can schedule email protection at one of several intervals:

- **Never**: Email is not protected.
- **Hourly**: Email files will be backed up every hour, just after the hour.
- **Daily**: If you choose this interval, also select the time for the backup.
- **Weekly**: If you choose this interval, also select the day and time for the backup.
- **Monthly**: If you choose this interval, also select the day of the month and time for the backup.

What to consider before you set up scheduled backups:

You configure IBM Spectrum Protect for Workstations to protect appropriate files on a schedule, and prepare the files for backup.

Files that are appropriate to protect on a schedule

Large or frequently saved files can consume considerable computing or network resources when they are backed up. You can schedule periodic backups of these files when the burden on computing or network resources are least inconvenient.

Some files are not often closed and saved, but must be backed up periodically. Files that are protected by schedule are backed up even if they are open.

Scheduled backups can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but there are fewer versions to restore a file.

Conditions for a scheduled backup to occur

The files that you select for scheduled protection are backed up at the scheduled time, if they change during the scheduled interval. If a file changed several times during the schedule, only the last version of the file is backed up at the scheduled time.

If the remote storage area is not available at the scheduled backup time, changed files are noted. These files are backed up when the remote storage becomes available. If a noted file changes after the scheduled backup time, and before the remote storage becomes available, only the last version of the file is backed up.

If the computer is shut down or IBM Spectrum Protect for Workstations is not running at the schedule time, the scheduled backup runs when the computer is powered on and IBM Spectrum Protect for Workstations is running.

If you shut down a computer or stop the IBM Spectrum Protect for Workstations client when a scheduled backup is running, the backup is suspended. The backup resumes when the client is started again and the remote storage is available. If you forced a backup of scheduled files during the 10 minutes before the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

IBM Spectrum Protect for Workstations backs up all files that changed during the schedule interval, including files that are open at the time of backup.

Tip: If a file is open during the backup, the copy of the file can be corrupted. To avoid this issue, close applications before a scheduled backup.

At the beginning of a scheduled backup, IBM Spectrum Protect for Workstations attempts to close all files that are listed in the file `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. IBM Spectrum Protect for Workstations sends a close command to each instance of every program that is included in the `closeapps.txt` file. The IBM Spectrum Protect for Workstations does not send a start command to any of those programs when the scheduled backup is finished.

Remote Storage panel of Groups Configuration

Specify the remote storage for the backups of your protected files.

Storing files in a remote storage area protects the files in case local copies are lost. Backups of continuously protected files, and files protected on a schedule, are stored in the same remote area. IBM Spectrum Protect for Workstations is tolerant of intermittently available networks. If the remote storage area is temporarily unavailable, IBM Spectrum Protect for Workstations queues backup copies until the remote storage becomes available.

Remote Storage server or device name and location:

Use the Remote Storage page to specify the remote storage server or device and its location for your backup copies. You can also specify how many versions to keep.

Select the type of storage device or server for the backup files to be stored to.

Backup Identifier

In this field, type the name that helps you to identify your backup files on the remote server. The default is your logon name. The backup identifier is only used for recovery purposes, and not for typical file restore. The backup identifier is used to locate the remote server location for a computer when restoring the configuration with the configuration wizard.

Location for the External Device or File Server

Select a file server or removable disk to store the backup copies. The remote device can be another computer (such as network-attached storage or a file server), a remote disk, or a removable disk.

If you choose a remote server in the **Location** field, you can use Universal Naming Convention (UNC) specifications for the file server instead of drive letters. Drive letters can change after you restart the system and often do not reconnect automatically.

If you choose a USB external device, you can select the drive letter. However, removable external device drive letters can change. To configure USB drives for remote storage, see Instructions on how to setup a USB device as the remote backup location., available at https://www.ibm.com/support/docview.wss?uid=swg21245761.

IBM Spectrum Protect for Workstations creates backup copies in a subfolder called `\RealTimeBackup\`*`computer name`*. For example, if a computer name is Computer1, and the remote storage location is configured with the value `\\remote\share`, backup copies are stored in `\\remote\share\RealTimeBackup\Computer1\`.

If you log on to your computer with a user name and password that is also valid on your remote storage location, IBM Spectrum Protect for Workstations authenticates your credential at that location. If the user name and password is not valid on your remote storage location, you must log on to the network using another account with regular privileges. You can log in interactively by using the **`Net Use`** command.

Some versions of Microsoft Windows use simplified file sharing, which allows one computer to connect to another computer over the network. The resulting connection allows only limited file system capabilities, and inhibits the creation of backup copies. Some information such as access control lists or file streams might be lost. You can disable simplified file sharing on the remote storage area.

WebDAV Server storage location

Some Internet Service Providers (ISPs) provide Web-based Distributed Authoring and Versioning, or WebDAV. With the WebDAV protocol, you can create, change, and move documents on a remote server. The WebDAV protocol is useful for authoring the documents that a web server serves, but can also be used for general web file storage. If your ISP provides WebDAV functions, IBM Spectrum Protect for Workstations can store backups on a web-based server.

In the **Location** field, enter your WebDAV server location using the following format: `https://MyISP.com/MyAcct`.

When using WebDAV, IBM Spectrum Protect for Workstations can use the basic authentication method. Because this authentication method sends the password as clear text over the network, the web server is configured to use secure sockets.

IBM Spectrum Protect for Workstations storage location

IBM Spectrum Protect for Workstations can store backup copies on a IBM Spectrum Protect server.

In the **Location** field, specify the IBM Spectrum Protect server location, using the following format: *tsm://Host.com*. You can also use an IP address for the server address.

You can use IBM Spectrum Protect server version 6.1 or later with IBM Spectrum Protect for Workstations.

Configure the IBM Spectrum Protect server before you connect from IBM Spectrum Protect for Workstations. Register the computer as a IBM Spectrum Protect node. IBM Spectrum Protect for Workstations prompts you for the password for this node in order to connect to the IBM Spectrum Protect server. For more information about registering a IBM Spectrum Protect node for your computer, see *IBM Spectrum Protect for Windows Administrator's Guide*.

If you specify a IBM Spectrum Protect server as the backup target and you want encryption or compression features applied to the backup, you must specify these options in the `dsm.opt` file in the IBM Spectrum Protect for Workstations subfolder of the "Accessing the program data folder" on page 36.

Restriction: You cannot use a subfile backup feature when the IBM Spectrum Protect server is the backup target.

In addition to backing up data directly to a IBM Spectrum Protect server, you can back up data using a two-stage method. First, use IBM Spectrum Protect for Workstations to create remote backups on a file server. Then, schedule a IBM Spectrum Protect backup-archive client on that file server to back up the files to a IBM Spectrum Protect server.

Restriction: If you use IBM Spectrum Protect for Workstations encryption, you cannot use IBM Spectrum Protect compression.

To manage storage space, the IBM Spectrum Protect administrator must grant authority to the IBM Spectrum Protect client node to delete backup copies. To assign authority to delete backup copies, see *Client Node Lacks Authority to Delete Backup Copies*.

To avoid problems when using the IBM Spectrum Protect server, see the topic in the problem determination section of the client documentation: *Files are not backed up to IBM Spectrum Protect server*.

How many versions to keep:

Specify how many backup versions of a file to keep on remote storage.

IBM Spectrum Protect for Workstations can store more than one backup version of each file. When you restore a file, you can choose which version of the file you want to restore. When the configured number of versions is reached, older versions of a file are deleted. Keeping more versions requires more storage space, but allows you more choices when restoring a file.

Remote Storage advanced settings:

Depending on the remote storage location that you specified, use the advanced settings in the Remote Storage page to select to encrypt or compress files. You can specify whether to use subfile copies when backing up larger files.

Tip: The default size for the remote storage area is 40 GB. If you increase the number of backup versions to keep, consider increasing your storage area size. If you are unsure of how much space to allocate, you can monitor the space usage on the Status panel and adjust the version and space settings accordingly.

When the storage space becomes full, IBM Spectrum Protect for Workstations deletes older backup copy versions of files that have several backup copy versions. If more space is needed for new backup copies, IBM Spectrum Protect for Workstations deletes backup copies of files to make room for the newest backup copy.

If you try to remotely back up a file that is larger than the space you have allocated, IBM Spectrum Protect for Workstations purges all older file versions, and the backup might fail. Ensure that the maximum space for your remote storage areas is greater than the maximum file size for remote backup in the **Advanced** page of the Settings Notebook. For example, if you decrease the maximum space for backups to 1 GB, you must decrease the maximum file size for remote backup from the default of 1 GB.

Advanced settings

When storing data onto an external device or file server, you can specify the following advanced settings. Select one option:
- Do not encrypt or compress backups
- Encrypt backups
- Compress backups

When storing data onto an external device or a file server you can choose to use sub-file copy function. Select this option to send only changed portions of a file to remote storage and to reduce network traffic. The changed portions are saved to a separate file on the remote storage.

The preceding options are not available when you use the IBM Spectrum Protect as the remote storage server. If you must encrypt or compress your data, then use the IBM Spectrum Protect server compression or encryption features.

Encrypt backups feature:

IBM Spectrum Protect for Workstations provides AES256 encryption for files that are stored on the remote server. The encryption feature for backups provides an extra layer of security for files in the remote storage area.

To set up encryption, click **Encrypt backups**. When the first file backup occurs, you are prompted to enter an encryption password. This password is cached and also saved in an encrypted file in the `ProgramData` folder. The password is required to restore files that are backed up by IBM Spectrum Protect for Workstations. If you disable encryption and enable encryption again, you are not prompted to create a new password.

Preserve your password: Ensure that you make a secure record of your password. If you lose your password, files might be unrecoverable.

The IBM Spectrum Protect product does not support prompted encryption. Therefore, if you specify the IBM Spectrum Protect server as your remote storage area, you must configure non-prompted encryption in the IBM Spectrum Protect `dsm.opt` options file. In the `dsm.opt` file, use the following statement to create the encryption key:

```
encryptkey generate
```

See *IBM Spectrum Protect for Windows Backup-Archive Client Installation and User's Guide* for information about how to set encryption options in the `dsm.opt` file. The `dsm.opt` file is stored in the `ProgramData` folder. For information about how to access the `ProgramData` folder, see "Accessing the program data folder."

The following usage rules apply to the encrypt backups feature:
- You cannot encrypt files that are stored in the local storage area.
- You cannot configure both encryption and compression.

IBM Spectrum Protect for Workstations cannot protect backup copies that are encrypted. In other words, you cannot create encrypted backup copies and then use IBM Spectrum Protect for Workstations to make backup copies of those backup copies. You can use IBM Spectrum Protect or another backup solution to protect the encrypted backup copies on the file server.

Accessing the program data folder:

Passwords for encrypted files are kept in the program data folder.

The following list indicates the location of the program data folder for Microsoft Windows 7 and Windows 8.

Tip: `\ProgramData\` is a hidden folder. To see the folder, modify your view preferences in Windows Explorer to show hidden files and folders.
- For a fresh installation of IBM Spectrum Protect for Workstations Version 8.1.0, the program data folder is in the following directory:
  `C:\ProgramData\Tivoli\TSM\FastBack_for_Workstations`

- For an upgrade from IBM Spectrum Protect Continuous Data Protection for Files to IBM Spectrum Protect for Workstations Version 8.1.0, the program data folder is in the following directory:

  ```
  C:\ProgramData\Tivoli\CDP_for_files
  ```

Compress backups option:

Set compression for remote backup copies.

Use compression to save space on your remote storage location. The compression feature is not compatible with the encryption feature. You can use compression or encryption, but not both simultaneously. Files that are backed up using the compression function must be restored by using IBM Spectrum Protect for Workstations.

If you select both options, subfile copy has precedence. The file that is larger than the minimum for subfile copy is not compressed. Only files smaller than the minimum size for subfile copy are compressed.

You can choose to select either encryption or compression.

Use sub-file copy option:

Set the sub-file copy option for remote storage backup copies.

Initially, an entire file is copied to the storage areas. When sub-file copy is turned on and the file size exceeds the sub-file limit, if the file changes only the changed information is copied to the storage area. The sub-file copies are saved as separate files on the remote storage areas.

Sub-file copy can significantly reduce the amount of network traffic. However, sub-file copy uses more processing resources on your computer. The default setting is to use sub-file copy for files larger than 50 MB. If you need to conserve more network resources, you can reduce the size setting so sub-file copy is not used on even smaller files.

To use sub-file copy to remote storage, you must have a backup copy of your files on local storage. In the **General** panel of the **Groups Configuration**, set the **Continuous protection level** field to **Local and remote storage**. Then you can set the sub-file backup option.

Check the check box to turn on sub-file copy. In the **Use sub-file copy for files larger than** field, specify the file size threshold for using sub-file copy. For files larger than this size, only the changed information is copied to the storage area.

Advanced panel of Groups Configuration

Use the **Advanced** panel to control messages and tune performance.

Allow program messages to open

For certain types of activities or notifications, IBM Spectrum Protect for Workstations opens messages from the icon in the system tray. To prevent the messages from opening, clear the check box.

Note: If messaging is disabled, important program messages regarding the failure of IBM Spectrum Protect for Workstations operations is suppressed, which could lead to potential loss of data.

Lock the configuration

Set this option to prevent a user from changing the configuration of the client.

How often to check for updates

Set the interval that the client checks the administration folder for command scripts, software upgrades, and configuration changes.

Performance Settings

Do not locally back up files larger than: field
Limit the size of files that are backed up to your local storage area. If you try to back up a file that is larger than the space you have allocated for your storage area, IBM Spectrum Protect for Workstations purges all older versions of your files, and then fails to back up the file. Make sure that the file size limit in this field, and the size limit for files backed up to remote storage, is less than the maximum space for your storage areas.

Do not remotely back up files larger than: field
Limit the size of files that are backed up to your remote storage area.

Maximum remote transfer rate: field
You can set a limit on the volume of data that IBM Spectrum Protect for Workstations transfers to remote storage. Consider limiting the transfer rate if you need to ease the burden on your network.

Note: This option is only used by IBM Spectrum Protect for Workstations client version 6.1 or earlier.

What to consider before you set up scheduled backups:

You configure IBM Spectrum Protect for Workstations to protect appropriate files on a schedule, and prepare the files for backup.

Files that are appropriate to protect on a schedule

Large or frequently saved files can consume considerable computing or network resources when they are backed up. You can schedule periodic backups of these files when the burden on computing or network resources are least inconvenient.

Some files are not often closed and saved, but must be backed up periodically. Files that are protected by schedule are backed up even if they are open.

Scheduled backups can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but there are fewer versions to restore a file.

Conditions for a scheduled backup to occur

The files that you select for scheduled protection are backed up at the scheduled time, if they change during the scheduled interval. If a file changed several times during the schedule, only the last version of the file is backed up at the scheduled time.

If the remote storage area is not available at the scheduled backup time, changed files are noted. These files are backed up when the remote storage becomes available. If a noted file changes after the scheduled backup time, and before the remote storage becomes available, only the last version of the file is backed up.

If the computer is shut down or IBM Spectrum Protect for Workstations is not running at the schedule time, the scheduled backup runs when the computer is powered on and IBM Spectrum Protect for Workstations is running.

If you shut down a computer or stop the IBM Spectrum Protect for Workstations client when a scheduled backup is running, the backup is suspended. The backup resumes when the client is started again and the remote storage is available. If you forced a backup of scheduled files during the 10 minutes before the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

IBM Spectrum Protect for Workstations backs up all files that changed during the schedule interval, including files that are open at the time of backup.

Tip: If a file is open during the backup, the copy of the file can be corrupted. To avoid this issue, close applications before a scheduled backup.

At the beginning of a scheduled backup, IBM Spectrum Protect for Workstations attempts to close all files that are listed in the file `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. IBM Spectrum Protect for Workstations sends a close command to each instance of every program that is included in the `closeapps.txt` file. The IBM Spectrum Protect for Workstations does not send a start command to any of those programs when the scheduled backup is finished.

Discovering existing clients and assigning the clients to groups

Discover IBM Spectrum Protect for Workstations clients that exist before you install the Central Administration Console. You can use the Central Administration Console to add existing clients to groups.

Before you begin

Complete this task in the following cases:
- IBM Spectrum Protect for Workstations clients are already installed before you install the Central Administration Console.
- Existing clients were installed without a configuration file that was generated by the Central Administration Console.

If you want to manage the clients by groups, you must create the groups.

About this task

Complete the following steps to discover and manage existing IBM Spectrum Protect for Workstations clients.

Procedure

1. Identify the administration folders that are used by the existing clients.
   a. Open the **Administration Settings** task.

b. In the **Administration Folders** section, click **Actions** and click **Identify an Administration Folder**.
c. In the **Identify an Administration Folder** panel, type an alias name for the administration folder in the **Alias** field.
d. In the **Administration folder** field, type the path for the administration folder. If you do not know the exact name of the **Administration folder**, click **Search** and browse for the folder.

   The values of the **Select a group for new clients** and **Select a script for new clients** fields do not affect existing clients. If there are existing clients in the folder, you must manually add the clients to the group. If you enter a search location that contains many files and folders, the search might take a long time. To cancel the search, click **Cancel**.
e. Click **OK**.

The existing clients are discovered by the Central Administration Console.

2. Optional: If you want to manage the clients by groups, assign the clients to appropriate groups. Clients that exist before you install the Central Administration Console are not automatically added to groups.
   a. Open the **Clients** task.

      The **Clients** panel contains the following sections:
      - **Health**
      - **Storage**
      - **Deployment**
   b. In any view of the **Clients** task, click the **Group** column heading.
   c. Scroll the list of clients to find the clients that belong to group **none**.

      When an existing client is discovered, the client is not automatically added to a group. Find existing clients in the table by filtering clients that belong to group **none**.
   d. Select all the clients that you want to add to one group.
   e. In the **Actions** menu, click **Assign Clients to a Group**, and select a group from the list.
   f. Click **OK**.

      The clients are shown in the table in the **Clients** task again. The clients are members of the group that you selected.

Related tasks:

"Creating a configuration file" on page 45
Create a configuration file that you can use to deploy clients.

"Identifying administration folders" on page 42
Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

Deploying new clients

Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

Before you begin

This task assumes that you created one or more groups, and that you have a IBM Spectrum Protect for Workstations installer file.

About this task

With the Central Administration Console, you can create a configuration file. You must obtain the IBM Spectrum Protect for Workstations client installer, and deploy the installer and configuration file to users.

Procedure

1. Create a script that a IBM Spectrum Protect for Workstations client runs when the software is first deployed. A typical script contains a command to back up all files.
2. Identify an administration folder for the clients. Select a group for the clients from the **Select a group for new clients** list.
3. Create a configuration file.
4. Deploy the installer and configuration file to other computers. The clients are installed and discovered by the Central Administration Console. The Central Administration Console can automatically assign the clients to groups.

Creating a script for clients

Create your own, custom scripts for clients. Create commands or use commands that are provided with the Central Administration Console.

About this task

A client can run a script automatically when the client is first discovered by the Central Administration Console. A typical script at initial discovery contains a command to back up all files. This action creates an initial backup copy of all files that you identified for protection. Without this action, files are backed up only when they are changed.

You can also send a script to clients to address a problem. For example, if your network is impacted by remote backup activity, you can send a command to specific clients to immediately pause remote backup activity. If you want to reduce the network traffic that occurs at a later, scheduled backup time, you can send a command to specific clients to immediately back up email files and other files that are typically backed up at the scheduled time.

Procedure

1. Open the **Administration Settings** task. The three administration tables are shown.
2. In the **Custom Scripts** section, click the **Actions** menu.
3. Click **Create a Script**. The **Create a Script** panel is shown.

4. Type a name for the script. Optionally, you can provide a description.
5. In the **Number of simultaneous clients** field, enter the maximum number of clients that can run this script at the same time. Some commands, such as **Back up all files**, can use considerable network resources. You can limit the number of clients that run this script at the same time.
6. In the **Script acceptance timeout** field, enter the maximum time for the client to begin running the script. If the client does not start the script in this time, there are the following consequences:
   - The script is removed from the administration folder of the client.
   - The client is no longer counted as one that is running the script simultaneously with other clients.
   - The audit log records that the client failed to start the script in this time.
   - The script is sent to the client at a later time.
7. In the **Script completion timeout** field, enter an estimate of the time it takes for a client to complete the script. The Central Administration Console is not notified when a client completes a script. When the **Script completion timeout** time elapses, the Central Administration Console removes the client from the list of clients that are running the script. If the number of clients running the script is constrained by the value of **Number of simultaneous clients**, the Central Administration Console can send the script to another client.
8. In the **Script** box, select a command from the list. The list contains useful commands. You can also create your own commands by directly editing the text area. The command is appended to the end of the list of commands.
9. Add more commands, if needed. You can add, modify, or delete commands by editing the text area.
10. Click **OK**. The new script is shown in the **Custom Scripts** table.

What to do next

You can send this script to one or more clients.

Related tasks:

"Sending a script to clients" on page 59
You can create scripts to manage activities or resolve issues of IBM Spectrum Protect for Workstations clients. You can send your customized scripts to one or more clients.

Identifying administration folders

Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

Before you begin

If you want to associate an administration folder with a group, you must first create a group.

Procedure

1. Open the **Administration Settings** task. The administration tables are shown.
2. In the **Administration Folders** section, click **Actions**.
3. Click **Identify an Administration Folder**. The **Identify an Administration Folder** panel is shown.

4. Enter data in the required fields.

Alias Enter a name that helps you identify this administration folder. Each alias must be unique.

Administration folder
Enter a Common Internet File System (CIFS) file server web address. For example, `\\server\sharename\folder`. The administration folder must be accessible to both the clients and the Central Administration Console. Each administration folder must be unique.

If you do not know that exact name of the **Administration folder** you can find it by clicking **Search**. A new window opens and you are asked to enter a location to search and click **Search**. You can then select a folder from the search results and click **OK**.

Note: If you enter a search location that contains a large number of files or folders, it might take a long time to complete the search. You can cancel the search by clicking **cancel**.

5. Select optional items.

Select a group for new clients
Selecting a group has the following consequences.

You can create a configuration file for installation packages.

When an administration folder is associated with a group, you can create a configuration file that has the protection settings of the group. The created configuration file contains a setting for the administration folder.

If a group is associated with more than one administration folder, you can create similar configuration files. Each created configuration file has the same protections settings except for the value of the administration folder.

If an administration folder is not associated with a group (**Group = none**), you cannot create a configuration file when you select that administration folder.

When a new client initially contacts the administration folder, the client is added to the group.
Using the configuration file that you created, a new client accesses the administration folder, and becomes a member of the group.

Existing clients that contact this administration folder and are members of group none are added to the group.

If a client belongs to any group besides **none**, changing the value of **Select a group for new clients** does not assign the client to the selected group.

Select a script for new clients

When a new client initially contacts the administration folder, this script is sent to the client.

If a client was discovered at this administration folder, changing the value of **Select a script for new clients** does not send a script to the client. Similarly, if a client was using this administration folder before the administration folder is identified to the Central Administration Console, changing the value of **Select a script for new clients** does not send a script to the client.

6. Click **OK**. The administration folder is shown in the table in the **Administration Folders** section.

Related concepts:

"Groups" on page 2
Groups allow you to manage many clients with a single action.

Related tasks:

"Creating a group" on page 23
Use the **Groups Configuration** task to create a group from scratch, or to create a group that is like an existing group. You can use a group to manage many clients at one time. A group defines a client configuration.

Related reference:

"Administration folders" on page 2
Clients gather configuration information, commands, and software updates from administration folders. The Central Administration Console manages clients by sharing information with clients in administration folders.

Example: Preparing to deploy clients to the sales group

Identify an administration folder for the clients that you deploy to the sales group.

Before you begin

Create a plan for grouping your users according to their data-protection needs. Create groups for the users.

About this task

Assume that you create groups with the following aliases:

- engineers local
- engineers remote
- sales people
- accountants

You plan to use `\\server1\fbwsadmin\sales` as the administration folder for the IBM Spectrum Protect for Workstations clients of the sales team. You must identify the administration folder: `\\server1\fbwsadmin\sales`.

Procedure

1. In the **Identify an Administration Folder** section, in the **Administration folder** field, enter the CIFS web address: `\\server1\fbwsadmin\sales`.
2. In the **Select a group for new clients** field, select the group sales people, and click **OK**.

What to do next

Create a configuration file for the IBM Spectrum Protect for Workstations clients that you deploy to the sales team.

Creating a configuration file

Create a configuration file that you can use to deploy clients.

Before you begin

Before you can create a configuration file, you must create a group. You must also identify an administration folder. When you identify the administration folder, you must select a group for new clients.

Procedure

1. Open the **Administration Settings** task. The administration tables are opened.
2. In the **Administration Folders** section, select one administration folder.
3. In the **Actions** menu, click **Create a Configuration File**. The **Create a Configuration File** panel opens.
4. Click **Get Configuration**. The Central Administration Console generates the XML configuration code of the group that is associated with the administration folder. The XML code displays in the text box. The configuration also contains the location of the administration folder.
5. Copy the code in the text box and paste it into a file.
6. Rename the file. If the configuration file is used when you initially install a client, rename the file to `fpa.txt`. If the configuration file is pulled by an existing client from the administration folder, rename the file to `fpcommands.xml`.

What to do next

After you create a configuration file, you can deploy IBM Spectrum Protect for Workstations clients to other computers. Rename the configuration file to `fpa.txt`. You must also have a client installer.

Change the configuration of existing clients that have not been discovered by the Central Administration Console by putting the configuration file in the downloads folder of the client. The client pulls the new configuration information from the downloads folder. If the configuration file is used to change the configuration of an existing client in this way, rename the file to `fpcommands.xml`.

You can change the configuration of clients assigned to groups by changing the settings in the **Groups Configuration** panels. For this task, it is not necessary to create a configuration file.

Related tasks:

"Identifying administration folders" on page 42
Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

Methods of deploying the client to other computers

You can use several methods to deploy the initial installation of the IBM Spectrum Protect for Workstations client to other computers.

- Use Microsoft Systems Management Server to install the IBM Spectrum Protect for Workstations.msi package. For more information, see Microsoft Systems Management Server documentation.
- Use IBM Tivoli Provisioning Manager Express®. For more information, see the product website at IBM Tivoli Provisioning Manager Express.
- Place the installer on a file server and ask users to start the installer.

When the IBM Spectrum Protect for Workstations client is initially installed, the installer retrieves configuration data from the files `\System32\fpa.txt`, `\System32\dsm.opt`, `\System32\networks.xml`, or `\System32\machinename.txt` in the Windows installation folder. You can also specify another directory to store the configuration files by using the **`CUSTOM_CONFIG_FILES_PATH`** command-line parameter. If these files do not exist, IBM Spectrum Protect for Workstations is installed with the default configuration settings.

Restriction: If more than one client is backing up files to the same remote file server, you must configure the server Access Control List (ACL) settings. For more information about the configuration tasks, see the Problem Determination section of the *IBM Spectrum Protect for Workstations Client Installation and User's Guide*.

Windows installation folder

The IBM Spectrum Protect for Workstations client references the Windows installation folder during installation. During the installation, the client can get configuration information from files in the `\System32\` subfolder in the Windows installation folder. The files are named `fpa.txt`, `dsm.opt`, `networks.xml`, and `machinename.txt`.

The Windows installation directory is also known by the environment variable `%WINDIR%`, and as shared drive `ADMIN$`. Typically, the Windows installation directory is `C:\Windows`.

You can also use the **`CUSTOM_CONFIG_FILES_PATH`** installation parameter to specify another directory path for the configuration files.

Monitoring the activity of clients

Monitor the activity of clients and the Central Administration Console

Viewing the status of all clients

View the status of your data-protection system. The **Health Monitor** section lists a summary of all clients, and provides links for more information and actions.

Before you begin

This task assumes that the Central Administration Console discovers clients.

Procedure

1. Open the Central Administration Console GUI.
2. Click **Health Monitor**. The **Clients Summary** section lists summary information about the status of clients. The status of each client can be listed as: **Fatal**, **Critical**, **Warning**, **Normal**.

3. Click a client status to see details of clients with that status. The **Health** view of the **Clients** task lists all clients with that status.
4. Optional: Filter the client entries that are displayed.
   a. In the filter text field, type a text string and click the arrow next to the filter text field.
   b. In the **Filter On** list, select one or more column names. If you select more than one column name, the filter yields all clients that have matching text in any of the selected columns.
   c. Click **OK**. The table displays the clients that match the text string that you entered. The filter is case-sensitive.

      More strings are matched when you use wildcard characters in the filter text. You can use an asterisk to replace several characters. Use a question mark to replace one character. If you use a wildcard character in the filter text, the blank space beyond the end of your filter text matches any text. The following table shows examples of search strings that you can enter.

Table 5. Filter strings and matching text

Filter text string	Matching text
Jupiter	Jupiter
Jupiter?	Jupiter Jupiter_bright_moon_light Jupiter_moon
Jupiter?moon	Jupiter_moon
*moon	Jupiter_bright_moon_light Jupiter_moon moon Saturn_moon Saturn_moon_light

5. Optional: Order the entries by sorting on the values in any column:
   a. Click a column heading. The entries in the column are in ascending order.
   b. Click the same column heading again. The entries in the column are in descending order.
   c. Click another column heading. The entries in the column are in ascending order.

What to do next

You can further investigate a client by viewing the activity log of a client or viewing the current configuration of a client.

If you determine that some action is needed, you can deploy software updates, change the configuration of a client, or send a script to a client.

Related concepts:

"Investigating a client" on page 52
View the health, storage, and deployment data of one or more clients. View the activity log and the current configuration of a client.

"Responses to client issues" on page 57
You can respond to IBM Spectrum Protect for Workstations client issues by updating IBM Spectrum Protect for Workstations client software, sending data-protection configurations and command scripts, and modifying groups.

Monitoring status by viewing the audit log

Monitor the status of the data-protection system by viewing the audit log of the Central Administration Console server. The audit log lists all interaction with the Central Administration Console and with the clients.

About this task

The audit log is a record of events from theCentral Administration Console server. If you are interested only in the events of an individual client, see the activity log for that client. The default location for the audit log folder is in `C:\Program Files\Tivoli\TSM\CAC\wlp\usr\servers\FBFWCAServer`.

The audit logs are composed of 10 files, starting with `audit.log.0`, which contains the most recent activity to `audit.log.9`, which contains the least recent activity.

Procedure

1. Open the **Health Monitor** task. The most recent events are listed in the **Audit Logs** section,
2. Optional: To display more events, click **More log entries**.
3. Optional: Filter the log entries that are displayed:
   a. In the filter text field, type a text string.
   b. Click the arrow next to the filter text field.
   c. From the list of names in the **Filter On** box, select one or more column names.
   d. Click **OK**. The log entries are filtered according to your filter criteria.

      For example, if you typed `*fail` and selected the **Message Text** column name, all entries with `fail` in the message text are displayed.

      More strings are matched when you use wildcard characters in the filter text. You can use an asterisk to replace several characters. Use a question mark to replace one character. If you use a wildcard character in the filter text, the blank space beyond the end of your filter text matches any text. The following table shows examples of search strings that you can enter.

Table 6. Filter strings and matching text

Filter text string	Matching text
Jupiter	Jupiter
Jupiter?	Jupiter Jupiter_bright_moon_light Jupiter_moon
Jupiter?moon	Jupiter_moon
*moon	Jupiter_bright_moon_light Jupiter_moon moon Saturn_moon Saturn_moon_light

4. Optional: Order the entries by sorting on the values in any column:
   a. Click a column heading. The entries in the column are in ascending order.
   b. Click the same column heading again. The entries in the column are in descending order.
   c. Click another column heading. The entries in the column are in ascending order.

What to do next

If you see an activity problem with one or more clients, you can investigate the attributes, logs, and current configuration of those clients in the **Clients** task.

Related concepts:

"Investigating a client" on page 52
View the health, storage, and deployment data of one or more clients. View the activity log and the current configuration of a client.

Resolving recent alerts

View all recent alerts about the status of IBM Spectrum Protect for Workstations clients. When an alert occurs, you must resolve the condition that triggered the alert and delete the alert from the list of recent alerts.

Procedure

1. Open the **Health Monitor** task. The most recent alerts are listed in the **Alerts** section.
2. Optional: Filter the log entries that are displayed:
   a. In the filter text field, type a text string.
   b. Click the arrow next to the filter text field.
   c. From the list of names in the **Filter On** box, select one or more column names.
   d. Click **OK**. The log entries are filtered according to your filter criteria.

      For example, if you typed `*fail` and selected the **Message Text** column name, all entries with `fail` in the message text are displayed.

      More strings are matched when you use wildcard characters in the filter text. You can use an asterisk to replace several characters. Use a question mark to replace one character. If you use a wildcard character in the filter text, the blank space beyond the end of your filter text matches any text. The following table shows examples of search strings that you can enter.

Table 7. Filter strings and matching text

Filter text string	Matching text
Jupiter	Jupiter
Jupiter?	Jupiter Jupiter_bright_moon_light Jupiter_moon
Jupiter?moon	Jupiter_moon
*moon	Jupiter_bright_moon_light Jupiter_moon moon Saturn_moon Saturn_moon_light

3. Optional: Order the entries by sorting on the values in any column:
   a. Click a column heading. The entries in the column are in ascending order.
   b. Click the same column heading again. The entries in the column are in descending order.
   c. Click another column heading. The entries in the column are in ascending order.
4. Resolve the condition that triggered an alert.

5. Delete the alert from the list of recent alerts.

   Tip: Always delete an alert immediately after you resolve the condition that triggered the alert. An alert is not sent again for this condition until the alert is deleted from the list of recent alerts.
   a. Select the alert that you want to delete in the list of recent alerts.
   b. Right-click and select **Delete**.

What to do next

To further investigate a client, you can view the health, deployment, and storage data for that client in the **Clients** task. In the **Clients** task, you can also view the activity log of a client or view the current configuration of a client.

If you determine that some action is required, you can deploy software updates, change the configuration of a client, or send a script to a client in the **Clients** task.

Related concepts:

"Responses to client issues" on page 57
You can respond to IBM Spectrum Protect for Workstations client issues by updating IBM Spectrum Protect for Workstations client software, sending data-protection configurations and command scripts, and modifying groups.

Reporting client activity

Use the Reporting task in the Central Administration Console to generate reports about the activity of clients.

Running reports of backup activity

IBM Spectrum Protect for Workstations provides default reports that you can modify to create your own reports of backup activity for clients and servers. The Reporting task of the Central Administration Console includes functions for modifying the example reports.

Before you begin

Discover some clients and servers with the Central Administration Console.

Procedure

1. In the task list of the Central Administration Console, click **Reporting**.
2. Select a report from the list in the Reporting panel and click the highlighted report.
3. To run the report, click **Run**.
4. To save the report results to file, click the **Save to File** icon in the Actions bar.
5. To view a graph of the report results, click the **Graph Report Data** icon in the Actions bar.

Creating a report of backup activity

You can create a report of backup activity for IBM Spectrum Protect for Workstations clients and servers. The Reporting task of the Central Administration Console includes functions for creating reports.

Before you begin

Discover some clients and servers with the Central Administration Console.

Procedure

1. In the task list of the Central Administration Console, click **Reporting**.
2. Click **Actions** > **Create Report**.
3. Enter a name for the report in the **Name** field.
4. Modify the fields in the report as required. To change the time and date details of the activity report, click the arrow next to the **Report Period** field and select **Custom**.
5. To save the report, click **Save**.

Creating a report of backup activity from an existing report

You can modify an existing report to create a report of backup activity for IBM Spectrum Protect for Workstations clients and servers. The Reporting task of the Central Administration Console includes functions for creating reports.

Before you begin

Discover some clients and servers with the Central Administration Console.

Procedure

1. In the task list of the Central Administration Console, click **Reporting**.
2. Select a report that is listed in the Reporting panel and click **Actions** > **Create Like Report**.
3. Enter a name for the report in the **Name** field.
4. Modify the fields in the report as required. To change the time and date details of the activity report, click the arrow next to the **Report Period** field and select **Custom**.
5. To save the report, click **Save**.

Administering clients

Investigate a IBM Spectrum Protect for Workstations client. Respond to client issues.

Creating a group with the configuration of an existing client

Create a group with a configuration that is imported from an existing client.

Before you begin

To create a group with the configuration of an existing client, the Central Administration Console must discover a client.

Procedure

Complete the following steps to create a group with a configuration that is imported from an existing client:

1. Open the **Clients** task. The **Clients** panel displays the following tabs: **Health**, **Storage**, and **Deployment**.
2. Select a client.
3. Click the **Actions** menu.
4. Click **Create a Group Like a Client**. The Group Wizard opens, populated with the same configuration values as the group that is associated with the client.
5. In the Group Wizard, alter any of the configuration values that you want to modify.
6. Review the **Groups Configuration** task to find the new group in the table of groups.

What to do next

You can add clients to the group. You can use the configuration of this group when you deploy new clients.

Related tasks:

"Creating a group" on page 23
Use the **Groups Configuration** task to create a group from scratch, or to create a group that is like an existing group. You can use a group to manage many clients at one time. A group defines a client configuration.

"Deploying new clients" on page 41
Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

Investigating a client

View the health, storage, and deployment data of one or more clients. View the activity log and the current configuration of a client.

Viewing the health, storage, and deployment data of one or more clients

The **Clients** table displays information about the clients.

Before you begin

This task assumes that the Central Administration Console discovered some clients.

Procedure

1. Open the **Clients** task.
2. Click the tab that contains information that you want to view. Each tab has a table that shows different information about the clients. Information is also shared among the three tabs.
3. Optional: Filter the client entries that are displayed.
   a. In the filter text field, type a text string and click the arrow next to the filter text field.
   b. In the **Filter On** list, select one or more column names. If you select more than one column name, the filter yields all clients that have matching text in any of the selected columns.
   c. Click **OK**. The table displays the clients that match the text string that you entered. The filter is case-sensitive.

      More strings are matched when you use wildcard characters in the filter text. You can use an asterisk to replace several characters. Use a question mark to replace one character. If you use a wildcard character in the filter text, the blank space beyond the end of your filter text matches any text. The following table shows examples of search strings that you can enter.

Table 8. Filter strings and matching text

Filter text string	Matching text
Jupiter	Jupiter
Jupiter?	Jupiter Jupiter_bright_moon_light Jupiter_moon
Jupiter?moon	Jupiter_moon
*moon	Jupiter_bright_moon_light Jupiter_moon moon Saturn_moon Saturn_moon_light

4. Optional: Order the entries by sorting on the values in any column:
   a. Click a column heading. The entries in the column are in ascending order.
   b. Click the same column heading again. The entries in the column are in descending order.
   c. Click another column heading. The entries in the column are in ascending order.

What to do next

With the data that is provided, you can decide what action is required to maintain the health of a client.

For example, if the **Storage** view indicates that all clients in the accounting group are using more than 90% of their allocated storage space, you can do several things.

Define alert conditions for high space usage.
: If you did not yet define alert conditions for high space usage, you can define those conditions. In this case, you discovered the current high space-usage situation by browsing the storage data, but next time you want to alert the correct people sooner. You can define conditions to alert operators when space usage reaches 80%, and another set of conditions to alert operators when space usage reaches 90%.

Gather more information about what is causing the high space usage.
: Reconsider the data-protection needs of the users. Verify that the group configuration matches the data-protection needs. Consider whether appropriate file types are being protected, and if the clients are saving the appropriate number of versions of each file. You can check activity logs of clients and even view the backup copies on the remote storage locations.

  If you notice a problem with a single client, check the current configuration file of that client to confirm that the user did not modify data-protection settings.

Modify the data-protection configuration of the group.
: Perhaps you decide that the clients in the accounting group require more storage space than is allocated in their current configuration. You can modify the group configuration in the **Groups Configuration** task. The new configuration is automatically sent to all clients in the accounting group.

Related concepts:

"Responses to client issues" on page 57
You can respond to IBM Spectrum Protect for Workstations client issues by updating IBM Spectrum Protect for Workstations client software, sending data-protection configurations and command scripts, and modifying groups.

Viewing the activity log of a client

View the log of activity for a single client. The activity log provides information for one client. In the client GUI, this log is called the activity report.

Before you begin

This task assumes that the Central Administration Console discovers some clients.

About this task

An activity log records events for a single client. If you are interested in the events of the central administration server, view the audit log.

Procedure

1. Open the **Clients** panel.
2. Click **Health**.
3. Select the client whose activity log you want to see.
4. To view the log entries, click **Actions** > **View Activity Log**.
5. Optional: Filter the log entries that are displayed:
   a. In the filter text field, type a text string.
   b. Click the arrow next to the filter text field.

c. From the list of names in the **Filter On** box, select one or more column names.
d. Click **OK**. The log entries are filtered according to your filter criteria.

   For example, if you typed `*fail` and selected the **Message Text** column name, all entries with `fail` in the message text are displayed.

   More strings are matched when you use wildcard characters in the filter text. You can use an asterisk to replace several characters. Use a question mark to replace one character. If you use a wildcard character in the filter text, the blank space beyond the end of your filter text matches any text. The following table shows examples of search strings that you can enter.

Table 9. Filter strings and matching text

Filter text string	Matching text
Jupiter	Jupiter
Jupiter?	Jupiter Jupiter_bright_moon_light Jupiter_moon
Jupiter?moon	Jupiter_moon
*moon	Jupiter_bright_moon_light Jupiter_moon moon Saturn_moon Saturn_moon_light

6. Optional: Order the entries by sorting on the values in any column:
   a. Click a column heading. The entries in the column are in ascending order.
   b. Click the same column heading again. The entries in the column are in descending order.
   c. Click another column heading. The entries in the column are in ascending order.

What to do next

After you review the activity log, you can gather more information or you can act on the information.

For example, assume that you investigate the activity log of client23 because this client is near the maximum capacity for remote storage. The activity log for client23 indicates that client23 is backing up many audio and video files. You know that client23 belongs to a group that excludes audio and video files from backups.

You view the current configuration file for client23, and you notice that the configuration file does not contain the same settings as the group.

You contact the user, and confirm that the audio and video files are not to be backed up. You can resend the group configuration to client23 by assigning client23 to the group again.

Related concepts:

"Responses to client issues" on page 57
You can respond to IBM Spectrum Protect for Workstations client issues by updating IBM Spectrum Protect for Workstations client software, sending data-protection configurations and command scripts, and modifying groups.

Related tasks:

"Monitoring status by viewing the audit log" on page 48
Monitor the status of the data-protection system by viewing the audit log of the Central Administration Console server. The audit log lists all interaction with the Central Administration Console and with the clients.

Viewing the last reported configuration of a client

View configuration data reported from the client. Because clients can modify their data-protection settings, the current configuration can be different from a configuration that the administrator deployed.

Before you begin

This task assumes that the Central Administration Console discovered some clients.

About this task

The client periodically pushes configuration information to the administration folder. If you send a script that contains the `Report` command, the client responds with a report that includes configuration information. The configuration information is as recent as the date in the **Last Report** column in the **Health** view of the **Clients** task.

Procedure

1. Open the **Clients** task. The **Clients** panel displays the following tabs: **Health**, **Storage**, and **Deployment**.
2. Select the client whose current configuration you want to see.
3. Click the **Actions** menu.
4. Click **View the Last Known Configuration of a Client**. The current data-protection settings are displayed.

What to do next

If the current configuration does not match the group configuration, you can resend the group configuration to the client. To resend the group configuration to the client, reassign the client to the group.

Related concepts:

"Responses to client issues" on page 57
You can respond to IBM Spectrum Protect for Workstations client issues by updating IBM Spectrum Protect for Workstations client software, sending data-protection configurations and command scripts, and modifying groups.

Configuring alerts (from the Clients task)

From the **Clients** task, you can open the **Administration Settings** task to configure alerts.

Procedure

1. Open the **Clients** task. The **Clients** panel displays three tabs: **Health**, **Storage**, and **Deployment**.
2. Click the **Health** tab.
3. In the **Actions** menu, click **Configure Alerts**. The **Administration Settings** task opens. You can define, modify, and delete alerts in the **Alerts Configuration** section.

Responses to client issues

You can respond to IBM Spectrum Protect for Workstations client issues by updating IBM Spectrum Protect for Workstations client software, sending data-protection configurations and command scripts, and modifying groups.

Conditions for upgrading a client

You can upgrade the client from previous releases as well as from a previous build of the current release.

The client installer file must have the following characteristics:

- The file name includes the string `SP4WKSTNS`.
- The file type is `exe`, for example: `8.1.0-IBM-SP4WKSTNS-x86_windows.exe`.
- The date of the new installer file must be more recent than the date of the installer file that was used for the current product level.

Removing old data files after uninstallation

If you uninstall the client, you must remove old data files before you install the client again. When the client is uninstalled, some files are not removed by the installer. The old files can cause problems when you reinstall the client.

Remove files in the following data folders:

Local storage area
The local storage area is the `RealTimeBackup` folder on a local drive. Rename this folder if you want to save the backup copies.

Remote storage area for the computer
The remote storage area is in the `RealTimeBackup\`*`computer_name`* folder of the remote device that you configured for the previous installation. Rename this folder if you want to save the backup copies.

Installation folder
The default installation location for the client is the `c:\Program Files\Tivoli\TSM\FastBack_for_Workstations` directory. If you upgraded from IBM Spectrum Protect Continuous Data Protection for Files, the default installation location is the `C:\Program Files\Tivoli\CDP_for_Files` directory.

The program data folder
The program data folder varies according to operating system and previously installed versions. The default program data folder for Windows 7 and Windows 8 is `C:\Programs\Tivoli\TSM\FastBack_for_Workstations`.

Upgrade from Continuous Data Protection for Files

If you upgrade from IBM Spectrum Protect Continuous Data Protection for Files, your IBM Spectrum Protect Continuous Data Protection for Files client must be at version 3.1 or later.

IBM Spectrum Protect Continuous Data Protection for Files clients that are older than version 3.1.5.9 accept client installer files with a name such as `TivoliCDP_CDPForFiles_3.1.8.0_windows.exe`. The installer name must include `CDP` and must be file type `exe`. IBM Spectrum Protect Continuous Data Protection for Files clients of version 3.1.5.9 and later accept client installer files with `CDP` or

SP4WKSTNS in the file name. IBM Spectrum Protect for Workstations client installer files have a name such as 8.1.0-IBM-SP4WKSTNS-x86_windows.exe for a full installation or 8.1.0-IBM-SP4WKSTNS-x86_windows-FP0000.exe for a patch installation. The installer file name for a IBM Spectrum Protect for Workstations client must contain SP4WKSTNS.

Therefore, if you want a IBM Spectrum Protect Continuous Data Protection for Files client earlier than version 3.1.5.9 to pull an upgrade to IBM Spectrum Protect for Workstations, you have the following options:

- You can rename the IBM Spectrum Protect for Workstations installer file to include CDP in the file name.
- You can first upgrade the IBM Spectrum Protect Continuous Data Protection for Files client to version 3.1.5.9 or later. The client can then pull an installer file with CDP or SP4WKSTNS in the file name.

Accessing the program data folder

Passwords for encrypted files are kept in the program data folder.

The following list indicates the location of the program data folder for Microsoft Windows 7 and Windows 8.

Tip: \ProgramData\ is a hidden folder. To see the folder, modify your view preferences in Windows Explorer to show hidden files and folders.

- For a fresh installation of IBM Spectrum Protect for Workstations Version 8.1.0, the program data folder is in the following directory:

  C:\ProgramData\Tivoli\TSM\FastBack_for_Workstations
- For an upgrade from IBM Spectrum Protect Continuous Data Protection for Files to IBM Spectrum Protect for Workstations Version 8.1.0, the program data folder is in the following directory:

  C:\ProgramData\Tivoli\CDP_for_files

Deploying software updates to existing clients

Deploy software updates to IBM Spectrum Protect for Workstations clients that are already installed.

Before you begin

Before you can deploy software to the IBM Spectrum Protect for Workstations clients, the following conditions must be met:

- The Central Administration Console discovered clients.
- You have an installer file that you can use for updating client software.

  The client installer file must have the following characteristics:
  - The file name includes the string SP4WKSTNS.
  - The file type is exe, for example: 8.1.0-IBM-SP4WKSTNS-x86_windows.exe.
  - The date of the new installer file must be more recent than the date of the installer file that was used for the current product level.

Procedure

Complete the following steps to upgrade software for existing IBM Spectrum Protect for Workstations clients:

1. Place the client installer file in the following subfolder of the Central Administration Console installation path:

Install_Location\wlp\usr\servers\FBFWCAServer\fbfw\deployments

2. Open the Central Administration Console GUI and click the **Clients** task.
3. Click the **Deployment** tab and select the clients that you want to update.
4. Click **Actions** > **Deploy Software Updates**.
5. In the Deploy Software Updates section, select the client installer file and click **OK**.

Related tasks:

"Assigning clients to a group" on page 61
You can assign one or more clients to a group so that they all have the same data protection configuration. You can move clients to another group, and you can assign clients that are not assigned to a group.

"Deploying new clients" on page 41
Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

Sending a script to clients

You can create scripts to manage activities or resolve issues of IBM Spectrum Protect for Workstations clients. You can send your customized scripts to one or more clients.

Before you begin

This task assumes that you created a script and that the Central Administration Console discovered clients.

Tip: To send a script to a client when the client is initially discovered, set the **Select a script for new clients** field when you identify the administration folder of the new client.

Procedure

To send a script to a client after the initial discovery, complete these steps:

1. Open the Central Administration Console and click **Clients**.
2. Select one or more clients to which you want to send a script.
3. Click **Actions** > **Send Clients a script**.

Related tasks:

"Creating a script for clients" on page 17
Create your own, custom scripts for clients. Create commands or use commands that are provided with the Central Administration Console.

"Identifying administration folders" on page 42
Identify a folder that is accessible to the Central Administration Console and IBM Spectrum Protect for Workstations clients.

Modifying the data protection configuration of a single client

Data protection requirements might vary for different clients. You can modify the data protection configuration of a single client.

Because data protection configurations are associated with groups, you must determine the consequence for the group. If all clients in the group require the modification, modify the group.

If other clients in the group do not require the modification, assign the client to a group with an appropriate configuration. If no groups have an appropriate configuration, create a group with the configuration for this client.

If the client is not assigned to a group, consider whether existing groups are appropriate. If no groups have an appropriate configuration, create a group with the configuration for this client.

Related tasks:

"Assigning clients to a group" on page 61
You can assign one or more clients to a group so that they all have the same data protection configuration. You can move clients to another group, and you can assign clients that are not assigned to a group.

"Creating a group" on page 23
Use the **Groups Configuration** task to create a group from scratch, or to create a group that is like an existing group. You can use a group to manage many clients at one time. A group defines a client configuration.

"Modifying all clients in a group" on page 25
You can modify the data protection configuration of all clients in a group.

"Restoring the data protection configuration of clients" on page 62
Restore a group configuration to a client that was changed by the user. If you do not lock the configuration of a group, users can modify the data protection settings of their clients. You can use the Central Administration Console to restore the data-protection configuration of the group that the client belongs to.

Modifying all clients in a group

You can modify the data protection configuration of all clients in a group.

Before you begin

This task assumes the following conditions:

- The Central Administration Console discovered clients.
- Clients are assigned to a group.

About this task

When you modify a group, the Central Administration Console automatically sends the new configuration to all clients in the group.

Procedure

1. Open the Central Administration Console and click **Groups Configuration**.
2. Select the group that you want to modify.
3. Click **Actions** > **Modify a Group**.
4. In the **Groups Configuration** notebook, modify the configuration settings for the group.
5. Click **OK**.

Related concepts:

"**Groups Configuration** notebook: field explanations" on page 25
You use the **Groups Configuration** notebook to configure the data-protection settings for IBM Spectrum Protect for Workstations clients.

"Modifying the data protection configuration of a single client" on page 60
Data protection requirements might vary for different clients. You can modify the data protection configuration of a single client.

Related tasks:

"Deploying software updates to existing clients" on page 58
Deploy software updates to IBM Spectrum Protect for Workstations clients that are already installed.

Assigning clients to a group

You can assign one or more clients to a group so that they all have the same data protection configuration. You can move clients to another group, and you can assign clients that are not assigned to a group.

Before you begin

This task assumes the following conditions:

- You created a group.
- The Central Administration Console discovered clients.

Procedure

1. Open the Central Administration Console GUI and click **Clients**.
2. In any view of the **Clients** section, select the clients that you want to assign to a group.
3. Click **Actions** > **Assign Clients to a Group**.
4. In the **Assign Clients to a Group** section, select a group from the list and click **OK**.

Related tasks:

"Deploying new clients" on page 41
Deploy new clients with a configuration file generated by the Central Administration Console. When the clients are installed and discovered by the Central Administration Console, the Central Administration Console can automatically assign them to a group and send them a script.

"Restoring the data protection configuration of clients" on page 62
Restore a group configuration to a client that was changed by the user. If you do not lock the configuration of a group, users can modify the data protection settings of their clients. You can use the Central Administration Console to restore the data-protection configuration of the group that the client belongs to.

Restoring the data protection configuration of clients

Restore a group configuration to a client that was changed by the user. If you do not lock the configuration of a group, users can modify the data protection settings of their clients. You can use the Central Administration Console to restore the data-protection configuration of the group that the client belongs to.

Before you begin

This task assumes the following conditions:

- The Central Administration Console discovered clients.
- Clients are assigned to a group.

About this task

Assign the client to the group again, and the Central Administration Console automatically sends the group configuration to the client.

Procedure

1. Open the Central Administration Console GUI and click **Clients**.
2. In any view of the **Clients** task, select the clients that you want to reassign to a group.
3. Click **Actions** > **Assign Clients to a Group**.
4. In the **Assign Clients to a Group** section, select a group and click **OK**.

Chapter 5. Troubleshooting with the Central Administration Console

You can use the Central Administration Console to resolve issues with clients. You can also recover the Central Administration Console database.

Starting or stopping the Central Administration Console service

The Central Administration Console service monitors IBM Spectrum Protect for Workstations clients. Whether you open the Central Administration Console GUI, the Central Administration Console service monitors clients and sends alerts. The Central Administration Console service starts after a successful installation and every time the computer starts. In most cases, you do not have to start or stop the Central Administration Console service. You can start or stop the service to troubleshoot the service functionality.

Procedure

Complete the following steps to start or stop the Central Administration Console service:

1. Click **Start** > **All Programs** > **Administrative Tools** > **Services**.
2. Click the **IBM Spectrum Protect for Workstations Central Administration Console** service.

   Accessing administration folders on other computers: The Central Administration Console service uses the user account to log on that was specified during installation. This user account must be a member of the Administrators group. Change the properties of the service to log on to an account that has access to administration folders on other computers.
3. Click the action that you want to take, such as **Stop**.

Recovering the Central Administration Console database from a backup

When you log on to the Central Administration Console user interface, no data is displayed without an error or data from earlier releases is displayed. If this error occurs, you must install the database again from a backup.

Before you begin

You must have a backup of the Central Administration Console database.

Best practise: To ensure that you have the most recent data when you recover the database, back up the database frequently. For information about backing up the database, see "Backing up the Central Administration Console database" on page 14.

About this task

To complete this task, you must stop and start the Central Administration Console server. You can stop and start the server by stopping or starting the Central

Administration Console service. For steps to stop or start this service, see "Starting or stopping the Central Administration Console service" on page 63.

Procedure

To recover the Central Administration Console database from a backup, complete the following steps:

1. Open the following folder:

   `Install_Location\Tivoli\TSM\CAC\wlp\usr\servers\FBFWCAServer\fbfw\CA_DB`
2. Determine when the database was created, by reviewing the date and time for the file `service.properties`. For the database to be up-to-date, the date and time must correspond to the most recent installation or upgrade of IBM Spectrum Protect for Workstations. If the date and time are more recent, then the database was created again because the original database was removed or deleted.
3. Stop the Central Administration Console service.
4. Find the most recent backup of the Central Administration Console database in your backup system.
5. Find the `CA_DB` folder in the backup.
6. Copy the `CA_DB` folder from the backup to the following location on your system:

   `Install_Location\Tivoli\TSM\CAC\wlp\usr\servers\FBFWCAServer\fbfw\CA_DB`
7. Start the Central Administration Console service.

Limit user access to files on a target file server

Set up the security permissions on a target file server to make sure that users have access only to the files that they back up.

By default, the first client that connects to a specific server share creates the `RealTimeBackup` directory. Permissions that are assigned to the `RealTimeBackup` directory do not prevent users from reading files that they do not own.

The settings that are used in this example assume one primary user of IBM Spectrum Protect for Workstations on the client. This primary user is the first user that connects to the server and creates the subdirectory for files that are backed up from the client. If IBM Spectrum Protect for Workstations operates from other accounts on that client, failures might occur when copying files to the remote server. Error messages such as `Failed to open the destination file` are logged to the activity report.

Windows file server

This example assumes that the following conditions exist:

- The Windows server shares a directory named `c:\fileservertest`.
- The accounts that are used to access the server are members of the `Users` group.

Access Control List settings for the `RealTimeBackup` directory

Access Control List (ACL) settings enable client accounts to create directories that are only accessible by the account that creates the directories. As a result, the directory that contains data for a node is not created until that node connects to the server.

Using Windows Explorer, set the ACL for the `c:\fileservertest\RealTimeBackup` directory according to the settings in ACL settings for the `RealTimeBackup` directory.

Important condition for ACL settings: Do not select the check box **Apply these permissions to objects and/or containers within this container only**.

Table 10. ACL settings for the `RealTimeBackup` directory

Type	Name	Permission	Applies to
Allow	Administrators	Full Control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	This folder, subfolders, and files
Allow	Users	Special	This folder only
Allow	OWNER RIGHTS*	Full Control	This folder, subfolders, and files

*The OWNER RIGHTS object must be added for Windows 2008 Servers.

The ability for objects to inherit permissions from the parent is not set. As a result, set the `Special` access for the `Users` group to provide the following settings:

```
Traverse Folder / Execute Allow
List Folder / Read Data Allow
Read Attributes Allow
Read Extended Attributes Allow
Create Files / Write Data Allow
Create Folders / Append Data Allow
Delete subfolders and files Allow
Read Permission's Allow
```

To verify that the ACL settings are correct, run the following command:

```
Cacls
```

The following output for the `Cacls` command shows the correct ACL settings:

```
CREATOR OWNER:(OI)(CI)(IO)F
```

If the parameter `(NP)` is included in the command output, set the ACL settings again to exclude `(NP)`. To ensure that the `(NP)` is excluded, verify that the check box **Apply these permissions to objects and/or containers within this container only** is not selected.

ACL settings for the `RealTimeBackup\BackupAdmin` directory

The `RealTimeBackup\BackupAdmin` directory is used by the IBM Spectrum Protect for Workstations client to download revisions and configurations. Nodes require read-only access to these directories:

`c:\fileservertest\RealTimeBackup\BackupAdmin`

Table 11. ACL settings for the `RealTimeBackup\BackupAdmin` directory

Type	Name	Permission	Applies to
Allow	Users	Read, Execute	This folder, subfolders, and files
Allow	Administrators	Full Control	This folder, subfolders, and files

The ability for objects to inherit permissions from the parent is not set. As a result, set the `Special` access for the `Users` group to provide only these settings:

```
Traverse Folder / Execute Allow
List Folder / Read Data Allow
Read Attributes Allow
Read Extended Attributes Allow
Delete subfolders and files Allow
Delete Allow
Read Permission's Allow
```

UNIX file server that is running Samba

This example assumes that the Samba server is set up to share a directory that is named `/fileservertest`.

These settings enable users to create directories under the `RealTimeBackup` directory:

```
chmod o+wrxt /fileservertest/RealTimeBackup
chmod o+rx /fileservertest/RealTimeBackup/BackupAdmin
chown root /fileservertest/RealTimeBackup/BackupAdmin
```

In the Samba configuration file (`smb.conf`), set the `create mask` and `directory mask` parameters to each specify `0700`. For example:

```
[fileservertest]
path = /fileservertest
writable = yes
create mask = 0700
directory mask = 0700
```

Remove incorrect highlighting in a report graph of client backup activity

When you display a Central Administration Console report graph for a IBM Spectrum Protect for Workstations client in the browser, labels in the graph might remain highlighted.

Problem

This problem is specific to only Microsoft Internet Explorer 9.0. The problem occurs in the following typical scenario:

1. Set Microsoft Internet Explorer 9.0. to be your default browser.
2. Open the Central Administration Console and discover approximately 200 IBM Spectrum Protect for Workstations clients.
3. Run a report in the Central Administration Console of client backup activity.
4. Create a graph of the report.
5. Change the report view to 100 or more clients per page.
6. Use the range slider to view the clients.

All of the labels in the report remain highlighted. This highlighting is a display problem specific to the browser.

Solution

You can use one of the following solutions to fix this problem:

- Use a different browser to display the report graph, for example Mozilla Firefox or Microsoft Internet Explorer 10 or later.
- If you must use the Microsoft Internet Explorer 9.0 browser, click on the report graph to deselect the highlighting.

Restore a missing page in the Central Administration Console

When you open a page in the Central Administration Console, no content is displayed in the page. You can modify the settings of the browser to display the content.

Problem

This problem is specific to only Microsoft Internet Explorer 9.0. The problem occurs in the following typical scenario:

1. Set Microsoft Internet Explorer 9.0. to be your default browser.
2. Open the Central Administration Console.
3. Click on one of the links in the navigation panel of the Central Administration Console, for example **Clients**.

The page opens in the Central Administration Console, but no content is displayed in the page. This display problem is specific to the browser.

Solution

You can use one of the following solutions to fix this problem:

- Use a different browser to display the report graph, for example Mozilla Firefox or Microsoft Internet Explorer 10 or later.
- If you must use the Microsoft Internet Explorer 9.0 browser, complete the following steps:
  1. On the browser menu bar, click **Tools** > **Internet Options**.
  2. Click **Advanced**.
  3. In the Security section, deselect the option **Do not save encrypted pages to disk**.

Appendix A. Messages issued by IBM Spectrum Protect for Workstations

Messages are issued by the IBM Spectrum Protect for Workstations client and the Central Administration Console to provide you with activity information. All of these messages have the prefix FBW.

Format of messages issued by IBM Spectrum Protect for Workstations

Each element of a message that is issued by IBM Spectrum Protect for Workstations provides information that can help you to understand and fix a problem.

Messages consist of the following elements:

- A three-letter prefix.
- A number that identifies the message.
- A one-letter severity code, also called the message type.
- Message text that is displayed on screen and written to message logs.
- Explanation and User Response texts. These texts elaborate on the message text, and are accessible only in documentation.

The severity codes give an indication of the severity of the issue that generated the message. The severity codes have the following meanings:

S Severe error. Processing cannot continue.

E Error. Processing cannot continue.

W Warning. Processing can continue, but problems might occur later.

I Information. Processing continues. A user response is not necessary.

Message variables in the message text are formatted in italic font.

Messages issued by the Central Administration Console

FBW messages with a message number of less than 5000 are issued by the IBM Spectrum Protect for Workstations Central Administration Console.

FBW0201I The IBM Spectrum Protect for Workstations servlet is starting.

Explanation: Starting the IBM Spectrum Protect for Workstations servlet.

User response: No action is required.

FBW0202I The IBM Spectrum Protect for Workstations servlet has started.

Explanation: The IBM Spectrum Protect for Workstations servlet is now accepting requests from the web browser.

User response: No action is required.

FBW0203E The ajax command is invalid.

Explanation: This is an internal error.

User response: Stop and start the Central Administration Console service. If the problem persists, install the Central Administration Console again.

FBW0204I The client *client name* was updated with a new configuration from the group *group name*.

Explanation: The client is running with a new configuration.

User response: No action is required.

FBW0205I A new client was discovered at *client address*.

Explanation: There was a scan of all the administration folders and a new client was discovered at the specified address.

User response: No action is required.

FBW0206I A new administration folder was identified at *folder address*.

Explanation: An administration folder was identified and a scan for this folder will be performed to discover new clients.

User response: No action is required.

FBW0207I The following administration folder was deleted from the database: *folder address*.

Explanation: An administration folder at the specified address was deleted.

User response: No action is required.

FBW0208I The configuration for client *client name* has changed.

Explanation: The specified client has accepted a new configuration.

User response: No action is required.

FBW0209I Starting the audit log.

Explanation: The audit log has started.

User response: No action is required.

FBW0210I The IBM Spectrum Protect for Workstations servlet stops.

Explanation: The IBM Spectrum Protect for Workstations servlet stops and no longer accepts requests from the web browser.

User response: Restart the Central Administration Console service.

FBW0211I The administration folder address *folder address* must be in UNC format. For example: \\\\server\\share.

Explanation: UNC is a Universal/Uniform Naming Convention. It describes the location of a volume, directory, or file on a local-area network (LAN). The format is \\\\server-name\\shared-resource-pathname.

User response: Enter a valid path for the administration folder and then retry the operation.

FBW0212I The administration folder *folder address* already exists.

Explanation: This administration folder has already been identified.

User response: Enter a different administration folder and then retry the operation.

FBW0213I The group *group name* already exists.

Explanation: This group name has already been defined.

User response: Enter a different group name and then retry the operation.

FBW0214I The group *group name* was not found.

Explanation: This is an internal error. The group specified is not in the database.

User response: Check the group name and then retry the operation.

FBW0215I The client *client name* was not found.

Explanation: This is an internal error. The client specified is not in the database.

User response: Check the client name and then retry the operation.

FBW0216I The client configuration at *filename* was not found.

Explanation: The file that contains the configuration has not been generated.

User response: Check if the client is online. Set the scan settings and the settings for how often the client checks for updates to a shorter interval. Then retry the operation.

FBW0217E There was an error accessing the client configuration at *filename*.

Explanation: The administration console cannot read the contents of the file that contains the configuration.

User response: Check the permissions on the configuration file.

FBW0218I The administration folder directory *folder address* was not found.

Explanation: It is possible that the administrator does not have the permissions to create the administration folder on the remote server.

User response: Check the permissions of the remote location.

FBW0219I The administration folder record *folder address* was not found.

Explanation: The administration folder may have been deleted by another user.

User response: Refresh the administration folder view to get an updated list of folders.

FBW0220I The configuration file for group *group name* was not found.

Explanation: This is an internal error. The configuration file may have been deleted.

User response: Ensure that the administration console has correct permissions to access the database.

FBW0221E There was an error accessing the configuration file *config file* for group *group name*.

Explanation: The administration console cannot read the content of the configuration file.

User response: Check the permissions on the configuration file. Verify that the service account has full access to the file.

FBW0222I The folder for the client *address* is missing.

Explanation: The folder for the client does not exist. It may have been deleted.

User response: No action is required.

FBW0223I The administration folder name *folder name* already exists in the database.

Explanation: The administration folder name has already been defined for another administration folder.

User response: Enter a different name for the administration folder and then retry the operation.

FBW0224I The client activity report at *directory* was not found.

Explanation: The file that contains the activities for this client has not been generated.

User response: Check if the client is online. Set the scan settings and the settings for how often the client checks for updates to a shorter interval. Then retry the operation.

FBW0225E There was an error accessing the client activity report at *filename*.

Explanation: The administration console cannot read the content of the client activity report.

User response: Check the permissions on the client activity report file. Verify that the service account has full access to the file.

FBW0226E The alert *name* was not found in the database.

Explanation: The alert may have been deleted.

User response: Refresh the alerts table to get an updated list of alerts.

FBW0227E The script *name* was not found in the database.

Explanation: The script may have been deleted.

User response: Refresh the scripts table to get an updated list of scripts.

FBW0228E An error was encountered when trying to send an email alert. Check the email settings.

Explanation: The administration console was unable to send an email alert with the specified settings.

User response: Verify the email settings are correct and then retry the operation.

FBW0229E An error was encountered when trying to send an email alert. No mail server is defined.

Explanation: The mail server name is not provided.

User response: Enter a valid mail server name and then retry the operation.

FBW0230E The request was denied because that alert name *alert name* already exists.

Explanation: This alert name has already been defined.

User response: Enter a different alert name and then retry the operation.

FBW0231E The request was denied because that script name *script name* already exists.

Explanation: This script name has already been defined.

User response: Enter a different script name and then retry the operation.

FBW0232E An unexpected error occurred while processing the request.

Explanation: This is an internal error.

User response: No action is required.

FBW0233E An error occurred while writing the script *script name* to the directory *directory*.

Explanation: The administration console cannot create the file for the script.

User response: Verify that the service account has full access to the directory and then retry the operation.

FBW0234W The client *client address* did not accept the script *script name* from the directory *directory*, in the specified time.

Explanation: The client failed to accept the script within the acceptance timeout limit.

User response: Verify the client is up and running. Verify the connectivity between the client and the remote server. Ensure the acceptance timeout is long enough.

FBW0235I The script *script name* was accepted for processing by client *client address*.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0236I The script *script name* has been sent to the client *client address* for processing.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0237E Unable to delete group *group name*. There are clients or administration folders that are still referencing this group.

Explanation: There are clients assigned to this group or an administration folder is still referencing this group. This group cannot be deleted.

User response: Ensure that no clients or administration folders are using this group.

FBW0243E Invalid condition value in condition *condition name*.

Explanation: The value for the alert condition is not valid.

User response: Correct the value and then retry the operation.

FBW0244E Invalid address syntax in address *address*.

Explanation: An email address consists of a user name, followed by an @ sign then the domain name. For example: youremail@yourcompany.com

User response: Enter a valid email address.

FBW0245I Package *package name* has been sent to client *address*.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0246I Package *package name* has been accepted by client *address*.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0247E An error occurred while deploying the package *package name* to client *client name*. The package is missing.

Explanation: An error occurred and the package is missing.

User response: Copy the package to the deployments directory or select another package.

FBW0248E Unable to cancel the search operation. The search id was not found.

Explanation: The search operation has already been cancelled.

User response: No action is required.

FBW0249I The search operation was cancelled.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0250I There were no administration folders found.

Explanation: The specified location does not have any administration folders.

User response: Enter a different location and then retry the operation.

FBW0251I The location to search ***location address*** **was not found.**

Explanation: The specified search path does not exist.

User response: Verify the remote location and then retry the operation.

FBW0252I The location to search ***location address*** **is not a directory.**

Explanation: The specified path is a file. The search location must be a directory.

User response: Correct the search location and then retry the operation.

FBW0253E An error occurred when an attempt was made to insert a backup entry into the reporting database. The entry is discarded.

Explanation: An error occurred when entries were read from a client activity log and an attempt was made to put the data into the report database.

User response: No action is required.

FBW0254E Invalid referrer in the HTTP request header.

Explanation: The request could be a cross-site request forgery. Request is denied.

User response: No action is required.

FBW0255E Invalid password. Password cannot contain these special characters `@!%&()-|;'"<>` or the password cannot be encoded.

Explanation: The password might contain one of these special characters `@!%&()-|;'"<>` or the user does not have administration privilege to encode the password.

User response: Verify that the user has administration privilege or change the password and try again.

FBW0256E A read or write error was encountered. The password was not changed.

Explanation: There was an error in reading or writing the password to file.

User response: Verify that the user has administration privilege and try again.

FBW1019E Group name is reserved for internal use. Enter a different group name.

Explanation: The group name that you specified is a reserved group name.

User response: Specify a different group name.

FBW1020E Specify a number to indicate when to remove backups of deleted files.

Explanation: In the Group Configuration page, you must specify a value in the **Remove backups of files deleted...** field before you click **Next**.

User response: Specify a number of days in the past in the **Remove backups of files deleted...** field. Backups of files that were deleted before this point in the past are removed.

Messages issued by the IBM Spectrum Protect for Workstations client

FBW messages with a message number of 5000 or greater are issued by the IBM Spectrum Protect for Workstations client.

FBW5001E No memory available for operation

Explanation: The program is low on memory. It is possible that there is a programming flaw that resulted in run-away memory usage, or that the system does not have enough memory.

User response: Open the Task Manager and ensure that the application is not using more memory over time. Then add more memory to the computer to resolve the issue.

FBW5003E The device driver could not be opened.

Explanation: In order for a user-mode program to talk to the kernel component driver, it must open a device node to communicate with the kernel. This error could be because the driver is not loaded, the device-node does not exist, or it has insufficient privileges.

User response: Reboot the system, if the problem persists contact support.

FBW5004E Unknown IOCTL value

Explanation: The user daemon program communicates with the kernel component by sending a binary value (an IOCTL) to the kernel. The kernel then interprets this value as a command. This error means that the kernel is unaware of the meaning of the specified value. This is likely to be caused by a mismatch of the kernel and daemon revision levels or by some non-authorized program sending arbitrary data.

User response: Ensure the driver Fp.sys and Filepathsrv.exe are the same version. You could also uninstall and reinstall the product.

FBW5010E The specified tracing level is not known.

Explanation: The specified tracing level is not known or incorrectly spelled.

User response: Ensure the specified tracing level is valid, in the correct format, and spelled correctly.

FBW5011E The specified logging device is unknown or unsupported on this platform.

Explanation: Typically, only the terms SCREEN and FILE are valid logging device key words. Not all platforms can support logging to a screen or terminal device.

User response: Ensure the specified device is valid and spelled correctly.

FBW5013E Error creating the HTML listener

Explanation: This is typically caused when the default port 9003 is already in use by another product.

User response: Change the default port used, refer to the technote: HOW TO MODIFY THE DEFAULT PORT 9003 IF ANOTHER APPLICATION IS CURRENTLY USING IT. This tech note is in the support portal.

FBW5018E The current operation is denied by the operating system due to permission.

Explanation: Some attempted operation such as a mkdir, is refused by the operating system due to insufficient privilege or permission.

User response: In a command window attempt the same operation that resulted in the error, this can sometimes give more information for the error. Ensure the user has the correct privledges for the particular directory or file.

FBW5019E Queue or queue transaction is corrupted

Explanation: The daemon is attempting to read or write to the kernel queue but the data does not validate as a known queue item.

User response: Internal error in the application, no action required.

FBW5022E Unable to access the specified file

Explanation: The file specified is unable to be accessed. Possibly spelled incorrectly, or bad path, or permissions.

User response: Ensure the user has the proper permissions for the file and directories involved and that the file and directory exist.

FBW5028E Specified named object does not exist

Explanation: An operation that is attempted to work on a database object, such as a rule or action, can not find the one specified.

User response: Ensure the rule or action name is correct and the database is configured properly.

FBW5029E The database query for the remote location returned an empty string or remote backup is disabled.

Explanation: The Group1Remote action was not found in the database or is disabled. The database was queried for the value before the initial configuration completed, a remote location was not specified in the GUI, or remote backup is disabled in the GUI.

User response: Ensure the remote backup is enabled and the remote location is specifed in the GUI.

FBW5037E Some items in the XML command were not recognized or consumed

Explanation: Not everything in the specified XML message was consumed. Possibly something is misspelled and thus not recognized or some other feature has been added in a newer release and is attempted but not known.

User response: No action required

FBW5040E The server does not have any space available.

Explanation: The storage pool on the server is full.

User response: Report to your system administrator to increase the storage pool on the server.

FBW5047E A system command such as mkdir, system, or unlink resulted in an error.

Explanation: Some intrinsic functions of the native operating system, such as mkdir, rm, or system, resulted in an error that was not anticipated.

User response: Ensure that the user has the correct permissions for the operation. Reboot the system if the problem persists.

FBW5053E File or path does not exist.

Explanation: Files have to be opened for reading or writing. For example database files or files for replication management. This error is because a file cannot be found.

User response: Ensure that the file exist, the pathname is valid, and is spelled correctly.

FBW5056E **Value specified for an error value is either missing or invalid**

Explanation: These error messages are processed. There must be a val= statement in the XML string. The value must be between 0 and 99999.

User response: The message file is corrupted and you need to reinstall the product. Contact support if the problem persists.

FBW5057E **The xml paragraph does not contain the MsgText and /MsgText tags**

Explanation: Incorrectly formed expression for an error-message.

User response: The message file is corrupted and you need to reinstall the product. Contact support if the problem persists.

FBW5077E **The source file for the backup operation was not found.**

Explanation: The file may have been deleted before the backup happened.

User response: Ensure that the file being backed up exists and that the path is correct.

FBW5078E **The source file for backup has a permission problem.**

Explanation: The permissions are not correct for the file.

User response: Ensure that the user has the proper access to the file and that the file exists.

FBW5079E **The destination file for backup has a permission problem.**

Explanation: The permissions are not correct for the file.

User response: Ensure the user has the proper access to the file.

FBW5080E **An operating system error reported trying to open the destination file for backup.**

Explanation: The permissions are not correct for the file.

User response: Ensure that the user permission on the file is correct and that the file is not in use by another application.

FBW5081E **An operating system error occured when trying to open the source file for backup.**

Explanation: The permissions are not correct for the file.

User response: Ensure that the user permissions on the file are correct and the file is not in use by another application at the time of the backup.

FBW5082E **Backup failed due to the operating system reporting no space.**

Explanation: Not enough space available for the backup.

User response: Increase the storage space available for the backup.

FBW5084I **This replication item is being skipped because the file size or date of the source is different from when the operation was recorded.**

Explanation: Replication events will be skipped if it appears that the event is older than the source file and thus there should be additional events forthcoming.

User response: Informational message no action required.

FBW5088E **A Retention specification did not specify any categories.**

Explanation: Retain commands must specify at least one category.

User response: Ensure that at least one category is used with Retain commands.

FBW5089E **The supplied item is not a RETAIN item.**

Explanation: A incorrectly formed retain command was given.

User response: Ensure that the retain command being used is valid.

FBW5090E **The specified retention name is not known.**

Explanation: An attempt to reference a given Retain is not known.

User response: Ensure the retain name being used is valid.

FBW5091E The replication.retain clause is missing and is required when doing generations.

Explanation: Replication actions that specify generations MUST have a Retain clause.

User response: Ensure the replication action is formatted correctly.

FBW5092E The duration value specified for a retention category must be greater than the previous duration value.

Explanation: Durations must be specified in increasing duration order.

User response: Change the duration for this category to be greater than the duration of the previous category.

FBW5095E The target file of a skip unset request is not currently in a skipped state.

Explanation: This is an internal error during an unset skip operation.

User response: No action is required.

FBW5101E The replication has failed and this may be because of an networking error, so it is possible to try again.

Explanation: This may be related to transient network or reliability issues.

User response: Make sure the network is connected or authenticate to the remote share.

FBW5103E The password is not correct for the specified user.

Explanation: An incorrect password has been supplied.

User response: Enter a correct password then retry the action.

FBW5105I This replication item is being skipped due to the source matching the target.

Explanation: The target file is identical to the one that is already at the target. This is based on the file size and the modification time.

User response: No action is required.

FBW5114E All backups in this queue have been cancelled by the user.

Explanation: The user has cancelled the operation.

User response: No action is required.

FBW5126I The current file backup was cancelled by the user.

Explanation: Backup operation for the file was cancelled.

User response: No action is required.

FBW5127I The backup directory cannot be deleted.

Explanation: You cannot delete the target directory because it is not empty.

User response: No action is required.

FBW5128I The backup item is being skipped because the destination does not exist.

Explanation: The backup cannot be carried out because the target does not exist.

User response: No action is required.

FBW5130E The file being deleted is a directory.

Explanation: Internal error. Attempted to delete a file but encountered a directory.

User response: No action is required.

FBW5132E The operating system is not currently supported.

Explanation: The operating system is not supported.

User response: See the System Requirements section at http://www.ibm.com/software/products/en/spectrum-protect-for-workstations

FBW5137I Data field for a rule in fpa.txt is too long and has been truncated.

Explanation: Internal error. A truncated data field is detected.

User response: No action is required.

FBW5138E The system configuration is locked against changes.

Explanation: Cannot change the system configuration because it is locked.

User response: Use the Central Administration Console to unlock the configuration.

FBW5139I The file is being skipped because it is larger than the configured maximum size for backup.

Explanation: The file size exceeds the maximum limit in the advanced setting tab.

User response: Change the maximum file size limit for this backup type.

FBW5140E Unexpected error with encryption. Detailed information maybe available in the event log or replication log.

Explanation: Internal error. Encryption failed with an error.

User response: No action is required.

FBW5143E The backup failed because the encryption library could not be loaded.

Explanation: The encryption library could not be found or was not the expected version.

User response: Download a new install image and reinstall the application.

FBW5144E The header in the encrypted or compressed file is corrupted.

Explanation: The header where all the file meta data is kept for the compressed or encrypted file has been corrupted.

User response: No action is required.

FBW6001I Last message repeated *number* times.

Explanation: Before the centralized logging system displays a message it checks to see if the message is the same as the previous message. If the messages are the same, the system does not display the new message. It counts the number of similar messages and displays information on how many times the message was repeated.

User response: No action is required.

FBW6002E Function: *function* failed to open file: [*filename*] Reason: *error*.

Explanation: The error may occur if the permissions are incorrect, if file or path does not exist, or if the file is corrupted.

User response: No action is required.

FBW6003E Failed to start the *name* thread. Reason: *error*.

Explanation: An unexpected error occured when a thread was created.

User response: Restart the daemon.

FBW6004E Command failed, result:(*retcode*) *error*.

Explanation: A command given to the fpa program or parse a configuration file has failed with the specified result-code and messages.

User response: Use the error code to troubleshoot the problem.

FBW6008E Socket *name* operation failed; Reason: *error*.

Explanation: One of the socket operations between the daemon and the html has failed with the operating system error given. Typically this happens when more than one html listener has been started.

User response: No action is required.

FBW6009E General error during function *name*: (*retcode*) *error*.

Explanation: An unexpected error occurred from a specified mid-level function. The error and associated message is also specified.

User response: No action is required.

FBW6010E Memory allocation failed of *number* bytes in function *name*.

Explanation: An attempt to allocate memory failed. Either the amount of memory was too high or there was a runaway process. The number of bytes desired and the function needing the memory are specified.

User response: No action is required.

FBW6011E Unknown or unsupported IOCTL value *number* was given.

Explanation: Internal error. It is possible that the driver and the daemon are out of sync.

User response: Restart the system or reinstall the software. Then retry the action.

FBW6012E Failed user exec-command [*command*] Result: *retcode*.

Explanation: An exec command resulted in an error. The full exec command is specified along with the operating system result value.

User response: No action is required.

FBW6013E Backup failed to open the log file: [*filename*] Reason: *error*.

Explanation: The log file for logging every backup transaction could not be opened. It is possible that this is related to a problem with the permissions or the pathname. The result is specified.

User response: No action is required.

FBW6018E An unexpected error occured during driver read operation to get next item from work queue, error (*retcode*) *error*.

Explanation: Internal error. The kernel component failed to retrieve the next item from the queue.

User response: No action is required.

FBW6019E User buffer is too small during driver read operation. User-buffer size:*maxsize* is not big enough for *size* bytes.

Explanation: This is an internal error. The daemon did not supply a large enough buffer to the driver. This should only occur if the driver and the daemon components are out of sync.

User response: Reinstall the software then retry the action.

FBW6020E Data (0x%x) sent to the driver from the daemon does not match any addresses in the queue.

Explanation: This is an internal error. Data relating to a write operation from the daemon to the kernel is invalid and could not be matched-up to a pending transaction.

User response: Reinstall the software then retry the action.

FBW6021E Too much data (*total* bytes) sent to the driver. The queue item can only hold *maxsize*.

Explanation: This is an internal error. A daemon write operation into the kernel provided too much data. This could be caused by incompatible versions.

User response: Reinstall the software then retry the action.

FBW6029I Trying to unload the driver but some files still active. Waiting...

Explanation: This is an informational message. When the driver is requested to unload, it tries to do so safely by waiting until all in-process file objects are complete. The driver will wait and periodically generate this message.

User response: No action is required.

FBW6030E The kernel audit buffer overflowed and some audits are lost.

Explanation: The kernel puts audit messages into a buffer that the user daemon must periodically drain. This error could be because the daemon is not running correctly, because too many messages are sent too quickly, or because the buffer is too small.

User response: Restart the daemon and start a full backup.

FBW6031E The HTML daemon did not start. Consult system error log.

Explanation: The HTML daemon was unable to start and the specific reason is shown in the system log. This could be because the intended port is in use. Another fpa daemon may be running, or some web-process is communicating with the port and keeping it in-use.

User response: Make sure that the port is not in use by other applications. Restart the system and retry the action. See the tech note at http://www-01.ibm.com/support/docview.wss?uid=swg21300055 for more information.

FBW6033I Driver loaded and ready.

Explanation: The driver has successfully completed all of its initialization and is ready to go to work.

User response: No action is required.

FBW6035I Driver unloading.

Explanation: The driver has started the processes of unloading. It can not log any messages.

User response: No action is required.

FBW6043E Replication or mirroring resulted in the destination path matching the source file:*filename*. Action name *action* is disabled.

Explanation: The destination can not have the same path as the source.

User response: No action is required.

FBW6045E The daemon was unable to unlink *filename*, error: *error*. The application will try again.

Explanation: An internal error occurrred during an unlink. This happens after a file has been replicated.

User response: No action is required.

FBW6046I The GUI messages file *filename* could not be opened, error: *error*

Explanation: The message file may be corrupted or missing from the installation folder. The installation folder may also be corrupted.

User response: Look in the installation folder for the message file. If the file exists, verify that the file has read permissions. You can also reinstall the product to fix this error.

FBW6047I The account must have the "Act as part of the operating system" privilege set.

Explanation: The service daemon needs to run with the "Act as part of the operating system" privilege or run as the local system account.

User response: Use the Windows Local Security Policy tool to set this privilege in the Local Policies->User Rights Assignment section. You can also change the service to run as the local system account.

FBW6048I Daemon started successfully.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6049I HTML listener started successfully and is listening on port ***number*****.**

Explanation: This message is for informational purposes only. It indicates the port that the HTML listener is listening on.

User response: No action is required.

FBW6051I The `fpa` command syntax.

Explanation: This message is for informational purposes.

User response: For details about the syntax of the **`fpa`** command, see technical document 1638130 on the IBM support site: http://www-01.ibm.com/support/docview.wss?uid=swg21638130.

FBW6054I You can not start both the HTML listener and the daemon in interactive mode at the same time.

Explanation: This occurs when the user specifies the -d flag with fpa and also specifies to start both daemons.

User response: Start either the HTML listener or the daemon in interactive mode only.

FBW6057I A special HOLD directory created: *directory*

Explanation: A special HOLD directory created for WORM (Write Once Write Many) or Retention. This message is for informational purposes only.

User response: No action is required.

FBW6058E Special WORM/Retention SHRED directory has non-numeric tail: ***directory*****.**

Explanation: The path name must end with a number.

User response: Change the path name so that it ends with a number.

FBW6059I Special WORM/Retention SHRED directory created: ***directory*****.**

Explanation: A SHRED directory or subdirectory was created.

User response: No action is required.

FBW6060E Special WORM/Retention RETAIN directory has improper format: *directory*

Explanation: The format of a path name should be 'Retain[nDays nHours nSeconds]'. For example: Retain10Days

User response: Use path name in the correct format.

FBW6061I Special WORM/Retention RETAIN directory created:*directory* **(***number* **Years,** *number* **Days,** *number* **Hours,** *number* **Minutes,** *number* **Seconds)**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6062E You can not create a RETAIN within a RETAIN tree:*path*

Explanation: Nested RETAIN is not allowed.

User response: Create the directory path with one instance of a RETAIN directory only.

FBW6063I You can not change the base name of a file. Source:*source filename* **Destination:***dest filename*

Explanation: This is an internal error. The file name can not be changed.

User response: No action is required.

FBW6069I The daemon has detected a network error that may be resolved easily. The network may be temporarily unavailable or the current logon information is incorrect. Check access to the network. The application will retry the action. File attempted: ***filename*****.**

Explanation: The client can not connect to the remote server.

User response: Verify that there is network access and that the logon information is correct.

FBW6070I The network appears to be functioning again. Backup resumed for *filename*.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6075E The restore location, *destination*, must be an absolute pathname.

Explanation: The restore process requires a full path name to a file or to a directory.

User response: Modify the restore destination then retry the action.

FBW6076I The remote target does not support the native Windows Backup-API for fully capturing file attributes. The application uses an alternative file-copy heuristic.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6077I The application has detected the target backup device is full. This may be a temporary issue. Create some free space at the target location. The application will retry the action.

Explanation: The backup target needs more storage.

User response: Delete some files to create free space at the target location. The remote storage state may be out of synch if you delete the backed up files.

FBW6085I Completed restore request. The client restored *number of* files.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6086E Fail to do *action string* file *source filename* to *dest filename*. Error: *error*. Extra information: *additional error*

Explanation: File can not be backed up.

User response: No action is required.

FBW6087I The application can not reach the network target. This may be a temporary issue. The application will retry the action.

Explanation: There is no network connection to the remote server. The computer may not be logged on to the network. This issue may also occur if the remote target was changed and there are files in the queue for backups to the previous remote target.

User response: Verify that the remote server is running and that the computer can ping the server. You may need to authenticate through a firewall or to logon to the network. If files are queued to a remote target that is no longer valid, you need to clear the queue to resolve this error.

FBW6088I The network appears to be functioning again. Backup resumes.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6089I The application has experienced a problem. Check for details in the View Report link from the Status page. Also check the Windows System Event log and Application log.

Explanation: An error occurred, check the error logs.

User response: If View Report link from the Status does not contain any details, check the Windows System Event log and the Application log.

FBW6091I Password information is needed for backup. Acknowledge the prompt or launch the user interface.

Explanation: The application requires password details to perform an action. The IBM Spectrum Protect server may need a password to perform backups. The WebDav server or the file server may need an encrytion password. The Lotus Notes® application may need a password.

User response: Enter the password when it is prompted.

FBW6092I A new version of the product is being installed.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6094I New software has been loaded and you must restart the machine to resume data protection.

Explanation: The machine must be restarted to run the new software.

User response: Restart the machine.

FBW6095I Your product trial evaluation period has expired.

Explanation: The trial period has ended.

User response: Uninstall the product or install the full product.

FBW6096I Driver was not loaded correctly. Data protection is not functioning.

Explanation: A problem may have occurred during the installation and the driver was not loaded correctly.

User response: Uninstall the product then reinstall it.

FBW6097E One or more delta files is missing or was not accessible during the restore operation.

Explanation: The version of the file being restored was corrupted or manually deleted from the remote storage.

User response: Restore an earlier version of the file.

FBW6101I The current version of Lotus Notes installed on this machine does not contain full support for this application. An upgrade of Lotus Notes is recommended. If you choose not to upgrade Lotus Notes, the application will still function, but it may need to wait and retry a Lotus Notes database backup if the files are being updated heavily while the backup is being performed.

Explanation: The application does not support the current Lotus Notes version.

User response: Upgrade to Lotus Notes 7.0 or later.

FBW6102I Warning: The My Documents folder in the include list does not match the location where the system stores your documents in. Add *folder*\\ to the include list.

Explanation: The system does not reference My Documents as your document folder. It might be called Documents.

User response: Add the specified folder to the include list.

FBW6103I *Product* **version** *product number* **is starting. The kernel driver version is** *kernel version number***.**

Explanation: This message is logged when the application starts the daemon and reads the version from the driver. This message is used for support purposes.

User response: No action is required.

FBW6104E The driver received a command before the initial configuration was loaded.

Explanation: Commands cannot be processed before the initial configuration is loaded.

User response: Wait until the initial configuration is loaded then retry the command.

FBW6105E The connection to the daemon could not be established.

Explanation: The commands are not processed.

User response: Ensure the daemon is running then retry the command.

FBW6107I Network '*adapter GUID***' is disconnected.**

Explanation: The specified network is disconnected.

User response: No action is required.

FBW6108I Setting the maximum backup speed to *number* **Kbps.**

Explanation: This is an informational message showing the throttle value used.

User response: No action is required.

FBW6109W This network rule already exists. Change the rule or click Cancel to exit this dialog.

Explanation: The same network rule is already defined for the selected network adapter.

User response: Change the rule or click Cancel to exit this dialog.

FBW6111I The throttle function was disabled because an internal error occurred. View the system error log for more details.

Explanation: An internal error disabled the throttle function. As a result, network changes or network rules settings did not update the throttle value.

User response: No action is required.

FBW6113W This network rule already exists or another network rule matches the same criteria. Modify the rule and issue the command again.

Explanation: The same network rule or another network rule that matches the criteria is already defined.

User response: Modify the rule and issue the command again.

FBW6114I **The daemon has detected a local storage error condition. Check the local storage settings. The application will retry for file:** *filename*

Explanation: The local backup directory may have been deleted.

User response: Check the local storage settings and ensure that the local backup directory exist.

FBW6115I **The local storage is available. Backup resumed for file** *filename*

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6116I **The application can not access the local storage. Check the local settings and reapply the settings if necessary.**

Explanation: The local backup directory may have been deleted. The drive letter where the directory resided may have changed.

User response: Check the local storage settings and reapply the settings if necessary. Ensure that the local backup directory exist with write permissions.

FBW6117I **The local storage appears to be available again. Backup resumes.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6209E **Errors have occurred.**

Explanation: Errors have occurred since the last time the replication log was viewed.

User response: Check the replication log for errors.

FBW6210W **Warnings have occurred.**

Explanation: Warnings have occurred since the last time the replication log was viewed.

User response: Check the replication log for errors.

FBW6211I **The fpcommands.xml file has been copied to the local machine for processing.**

Explanation: When an administrator publishes a new configuration, the client machine will copy the fpcommands.xml file to the clients machines data directory to be processed.

User response: No action is required.

FBW6212W **Existing configuration can not be restored. Database 'fpa.txt' was not backed up to this remote location** *remote location***. The default configuration is used. Use the Settings Notebook to change the default configuration.**

Explanation: There was an attempt to restore a configuration that was not backed up.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6213W **Restoring database 'fpa.txt' from the remote location** *remote location* **failed. Error returned:** *error***. The default configuration is used. Use the Settings Notebook to change the default configuration.**

Explanation: Failed to restore the database from the remote location.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6214E **Reset database 'fpa.txt' before the import of the restored database failed. Error returned:** *error***. The product must be reinstalled.**

Explanation: An internal error occurred during the reset of the database. The machine can not be recovered from this error.

User response: Uninstall then reinstall the product.

FBW6215E **Import database 'fpa.txt.bk' failed. Error returned:** *error***. The default configuration failed ro load, error** *retcode***. The product must be reinstalled.**

Explanation: An internal error occurred during the import of the restored database. The second attempt to load the default configuration failed. The machine can not be recovered from this error.

User response: Uninstall then reinstall the product.

FBW6216W Import database 'fpa.txt.bk' failed. Error returned: *error*. The default configuration was loaded. Use the Settings Notebook to change the default configuration.

Explanation: An internal error occurred during the import of the restored database. Loading of the default configuration was successful.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6217E Import database 'fpa.txt.save' failed. Error returned: *error*. The default configuration failed to load, error *retcode*. The product must be reinstalled.

Explanation: An internal error occurred during the import of the restored database. The second attempt to import the installed configuration database prior to recovery failed. The third attempt to load the default configuration also failed. The machine can not be recovered from this error.

User response: Uninstall then reinstall the product.

FBW6218W Import database 'fpa.txt.save' failed. Error returned: *error*. The default configuration was loaded. Use the Settings Notebook to change the default configuration.

Explanation: An internal error occurred during the import of the restored database. The second attempt to import the installed configuration database prior to recovery failed. Loading of the default configuration was successful.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6219W Import database 'fpa.txt.bk' failed. The previous saved configuration is loaded instead.

Explanation: An internal error occurred during the import of the restored database. The installed configuration saved before the import is now loaded.

User response: Use the Settings Notebook to change the default configuration.

FBW6220I Restoring 'identifier.txt' from *remote target* failed. Error returned: *error*. The default logon name is used as the identifier.

Explanation: An internal error occurred during the restore.

User response: Use the Settings Notebook to change the identifier value.

FBW6221I Restoring 'dsm.opt' from *remote target* failed. Error returned: *error*. The default dsm.opt file is used.

Explanation: An internal error occurred during the restore.

User response: Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6222I Host name was not specified on the restore command. The host name of the machine is used.

Explanation: This is an internal error where the host name was not specified on the restore command. The 'machinename.txt' file is not created.

User response: If the intent is to back up with a different host name, manually create the 'machinename.txt' file in the data folder with the correct host name.

FBW6223I Failed to create 'machinename.txt' to store the host name of the machine that the files ared recovered from. Host name of the current machine is used.

Explanation: The host name of the machine is used as the backup folder for the client unless 'machinename.txt' file exists and contains a different host name.

User response: If the intent is to back up with a different host name, manually create the 'machinename.txt' file in the data folder with the correct host name.

FBW6224I Synchronizing files with the remote server.

Explanation: After the configuration files are recovered, the files are synchronized with the remote server.

User response: No action is required.

FBW6225I Finished synchronizing files with the remote server.

Explanation: This message is for informational purposes only.

User response: No action is required.

Appendix B. Accessibility features for IBM Spectrum Protect for Workstations

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. IBM Spectrum Protect for Workstations provides various accessibility features that you can use.

Accessibility features

The following list includes the major accessibility features in IBM Spectrum Protect for Workstations:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices
- User documentation that is provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The IBM Spectrum Protect for Workstations Information Center, and its related publications, are accessibility-enabled.

Keyboard navigation

IBM Spectrum Protect for Workstations follows Microsoft conventions for most keyboard navigation and access. Drag and Drop support is managed by using the Microsoft Windows Accessibility option *MouseKeys*. For more information about MouseKeys and other Windows accessibility options, see the Windows Online Help. To open the Windows Online Help for accessibility options, click **Start** and enter `MouseKeys` in the search field.

The following access methods differ from Microsoft conventions.

In the Central Administration Console, access table toolbars in the following way:

1. Press Tab and Shift+Tab to navigate to a table. The first element in a table that receives focus is the toolbar. Typically, the refresh tool is the first tool in the toolbar.
2. Press Right Arrow and Left Arrow to navigate among the tools in the toolbar.
3. Press Enter to activate the tool.

In the Central Administration Console, access table elements in the following way:

1. Press Tab and Shift+Tab to navigate to a table. The first element in a table that receives focus is the toolbar.
2. Press Spacebar to navigate to the column headings.
3. Press Right Arrow and Left Arrow to navigate among the column headings.
4. Press Enter to at a column heading to sort the rows according to the values in that column.
5. Press Tab to navigate to the body of the table.
6. Use Up Arrow and Down Arrow to move from one row to another.

7. Use Right Arrow and Left Arrow to navigate the cells in a row.
8. To select or clear a check box in a row, complete the following steps:
   - Put the check box in focus and press Enter. You can now edit the cell, and you cannot use arrow keys to navigate the table cells.
   - Press Spacebar to select or clear the check box.
   - Press Esc to leave edit mode. You can now use the arrow keys to navigate the table cells.

Related accessibility information

You can view the publications for IBM Spectrum Protect for Workstations in Adobe Portable Document Format (PDF) by using the Adobe Acrobat Reader. You can access these files or any of the other documentation PDF files at IBM Publications Center at http://www.ibm.com/shop/publications/order/.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center at http://www.ibm.com/able.

Notices

This information was developed for products and services offered in the US. This material might 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, MD-NC119
Armonk, NY 10504-1785
US

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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 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.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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.

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

SoftLayer® is a registered trademarks of SoftLayer, Inc., an IBM Company.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
: These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

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.

Glossary

This glossary provides terms and definitions for the IBM Spectrum Protect for Workstations software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website.

A

absolute mode
: In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also mode, modified mode.

access control list (ACL)
: In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access mode
: An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume.

ACK See acknowledgment.

acknowledgment (ACK)
: The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See access control list.

activate
: To validate the contents of a policy set and then make it the active policy set.

active-data pool
: A named set of storage pool volumes that contain only active versions of client backup data. See also server storage, storage pool, storage pool volume.

active file system
: A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. See also inactive file system.

active policy set
: The activated policy set that contains the policy rules currently in use by all client nodes assigned to the policy domain. See also policy domain, policy set.

active version
: The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. See also backup version, inactive version.

activity log
: A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup
: A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client
: A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the server. See also backup-archive client.

administrative command schedule
: A database record that describes the planned processing of an administrative command during a specific time period. See also central scheduler, client schedule, schedule.

administrative privilege class
: See privilege class.

administrative session
: A period of time during which an

administrator user ID communicates with a server to perform administrative tasks. See also client node session, session.

administrator
A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

agent node
A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate
An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also logical file, physical file.

aggregate data transfer rate
A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

application client
A program that is installed on a system to protect an application. The server provides backup services to an application client.

archive
To copy programs, data, or files to another storage media, usually for long-term storage or security. See also retrieve.

archive copy
A file or group of files that was archived to server storage

archive copy group
A policy object containing attributes that control the generation, destination, and expiration of archived files. See also copy group.

archive-retention grace period
The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also bind.

association
The defined relationship between a client node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

audit
To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication rule
A specification that another user can use to either restore or retrieve files from storage.

authority
The permission level to access objects, resources, or functions. See also privilege class.

authorization rule
A specification that permits a user to either restore or retrieve files for another user from storage.

authorized user
A user who has administrative authority for the client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS
See automounted file system.

automatic detection
A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration
The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also demand migration, threshold migration.

automounted file system (AutoFS)
A file system that is managed by an automounter daemon. The automounter

daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client
A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. See also administrative client.

backup copy group
A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class. See also copy group.

backup retention grace period
The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set
A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection
A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version
A file or directory that a client node backed up to storage. More than one backup version can exist in storage, but only one backup version is the active version. See also active version, copy group, inactive version.

bind To associate a file with a management class name. See also archive-retention grace period, management class, rebind.

C

cache
To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file
A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD
See client acceptor daemon.

central scheduler
A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See also administrative command schedule, client schedule.

client
A software program or computer that requests services from a server. See also server.

client acceptor
A service that serves the Java applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX, UNIX, and Linux systems, the client acceptor is run as a daemon.

client acceptor daemon (CAD)
See client acceptor.

client domain
The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node
A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session
A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. See also administrative session.

client option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client options file
An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client-polling scheduling mode
A method of operation in which the client queries the server for work. See also server-prompted scheduling mode.

client schedule
A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also administrative command schedule, central scheduler, schedule.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file
A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. See also client user-options file, options file.

client user-options file
A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also client system-options file. See also client system-options file, options file.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. See also open registration.

collocation
The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool. Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group
A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point
A point in time when data is considered to be consistent.

communication method
The method by which a client and server exchange information. See also Transmission Control Protocol/Internet Protocol.

communication protocol
A set of defined interfaces that permit computers to communicate with each other.

compression
A function that removes repetitive characters, spaces, strings of characters, or binary data from the data being processed and replaces characters with control characters. Compression reduces the amount of storage space that is required for data.

configuration manager
A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also enterprise configuration, managed server, profile.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction. See also session.

copy backup
A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted.

copy group
A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also archive copy group, backup copy group, backup version, management class.

copy storage pool
A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also destination, primary storage pool, server storage, storage pool, storage pool volume.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which read errors have been detected.

database backup series
One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series. See also database snapshot, full backup.

database snapshot
A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also database backup series, full backup.

data center
: In a virtualized environment, a container that holds hosts, clusters, networks, and data stores.

data deduplication
: A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server
: A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover
: A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)
: A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

data store
: In a virtualized environment, the location where virtual machine data is stored.

deduplication
: The process of creating representative records from a set of records that have been identified as representing the same entities.

default management class
: A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

demand migration
: The process that is used to respond to an out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated. See also automatic migration, selective migration, threshold migration.

desktop client
: The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination
: A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated. See also copy storage pool.

device class
: A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file
1. For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.
2. For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

disaster recovery manager (DRM)
: A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan
: A file that is created by the disaster recover manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and

hardware that is used by the server, and the location of recovery media.

domain
A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See also policy domain.

DRM See disaster recovery manager.

DSMAPI
See data storage-management application-programming interface.

dynamic serialization
Copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive. See also shared dynamic serialization, shared static serialization, static serialization.

E

EA See extended attribute.

EB See exabyte.

EFS See Encrypted File System.

Encrypted File System (EFS)
A file system that uses file system-level encryption.

enterprise configuration
A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also configuration manager, managed server, profile, subscription.

enterprise logging
The process of sending events from a server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also event.

error log
A data set or file that is used to record error information about a product or system.

estimated capacity
The available space, in megabytes, of a storage pool.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process. See also enterprise logging, receiver.

event record
A database record that describes actual status and results for events.

event server
A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)
For processor, real and virtual storage capacities and channel volume, 2 to the power of 60 or 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude
The process of identifying files in an include-exclude list. This process prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup, from space management, or from both backup and space management.

exclude-include list
See include-exclude list.

expiration
The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file
A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend
To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)
Names or value pairs that are associated with files or directories. There are three

classes of extended attributes: user attributes, system attributes, and trusted attributes.

external library
A collection of drives that is managed by the media-management system other than the storage management server.

F

file access time
On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age
For migration prioritization purposes, the number of days since a file was last accessed.

file device type
A device type that specifies the use of sequential access files on disk storage as volumes.

file server
A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space
A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore, retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)
A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state
The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also migrated file, premigrated file, resident file.

file system migrator (FSM)
A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state
The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency
A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See file space ID.

FSM See file system migrator.

full backup
The process of backing up the entire server database. A full backup begins a new database backup series. See also database backup series, database snapshot, incremental backup.

fuzzy backup
A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy
A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified.

G

GB See gigabyte.

General Parallel File System (GPFS)
A high-performance shared-disk file system that can provide data access from nodes in a clustered system environment. See also information lifecycle management.

gigabyte (GB)
For processor storage, real and virtual storage, and channel volume, 10 to the

power of nine or 1,073,741,824 bytes. For disk storage capacity and communications volume, 1,000,000,000 bytes.

global inactive state
The state of all file systems to which space management has been added when space management is globally deactivated for a client node.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system. See also Universally Unique Identifier.

GPFS See General Parallel File System.

GPFS node set
A mounted, defined group of GPFS file systems.

group backup
The backup of a group containing a list of files from one or more file space origins.

GUID See Globally Unique Identifier.

H

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity. See also hierarchical storage management client, recall, storage hierarchy.

hierarchical storage management client (HSM client) A client program that works with the server to provide hierarchical storage management (HSM) for a system. See also hierarchical storage management, management class.

HSM See hierarchical storage management.

HSM client
See hierarchical storage management client.

I

ILM See information lifecycle management.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. See also active file system.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. See also active version, backup version.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also include-exclude list.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services. See also include-exclude file.

incremental backup
The process of backing up files or directories, or copying pages in the database, that are new or changed since the last full or incremental backup. See also selective backup.

individual mailbox restore
See mailbox restore.

information lifecycle management (ILM)
A policy-based file-management system for storage pools and file sets. See also General Parallel File System.

inode The internal structure that describes the individual files on AIX, UNIX, or Linux systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface. See also migration job.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

KB See kilobyte.

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 2 to the power of 10 or 1,024 bytes. For disk storage capacity and communications volume, 1,000 bytes.

L

LAN See local area network.

LAN-free data movement
The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network.

LAN-free data transfer
See LAN-free data movement.

leader data
Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library
1. A repository for demountable recorded media, such as magnetic disks and magnetic tapes.
2. A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client
A server that uses server-to-server communication to access a library that is managed by another storage management server. See also library manager.

library manager
A server that controls device operations when multiple storage management servers share a storage device. See also library client.

local
1. Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line. See also remote.
2. For hierarchical storage management products, pertaining to the destination of migrated files that are being moved. See also remote.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volume
Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See loopback virtual file system.

logical file
A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also aggregate, physical file, physical occupancy.

logical occupancy
The space that is used by logical files in a storage pool. This space does not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy. See also physical occupancy.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

logical volume
A portion of a physical volume that contains a file system.

logical volume backup
A back up of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)
Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)
A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LUN See logical unit number.

LVSA See Logical Volume Snapshot Agent.

M

macro file
A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. See also IBM Spectrum Protect command script.

mailbox restore
A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object
A definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server.

managed server
A server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also configuration manager, enterprise configuration, profile, subscription.

management class
A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also bind, copy group, hierarchical storage management client, policy set, rebind.

maximum transmission unit (MTU)
The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See megabyte.

media server
In a z/OS environment, a program that provides access to z/OS disk and tape storage for IBM Spectrum Protect servers that run on operating systems other than z/OS.

megabyte (MB)
For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes. For disk storage capacity and communications volume, 1,000,000 bytes.

metadata
Data that describes the characteristics of data; descriptive data.

migrate
To move data to another location, or an application to another computer system.

migrated file
A file that has been copied from a local file system to storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also file state, premigrated file, resident file, stub file.

migration
The process of moving data from one computer system to another, or an application to another computer system.

migration job
A specification of files to migrate, and actions to perform on the original files after migration. See also job file, threshold migration.

migration threshold
High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring
The process of writing the same data to multiple disks at the same time. The mirroring of data protects it against data loss within the database or within the recovery log.

mode A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See also absolute mode, modified mode.

modified mode
In storage management, a backup copy-group mode that specifies that a file

is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also absolute mode, mode.

mount limit
The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also mount point.

mount point
A logical drive through which volumes are accessed in a sequential access device class. For removable media device types, such as tape, a mount point is a logical drive associated with a physical drive. For the file device type, a mount point is a logical drive associated with an I/O stream. See also mount limit.

mount retention period
The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period
The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See maximum transmission unit.

N

Nagle algorithm
An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe
A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS file server
See network-attached storage file server.

NAS file server node
See NAS node.

NAS node
A client node that is a network-attached storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system
A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format
A format of data that is written to a storage pool directly by the server. See also non-native data format.

NDMP
See Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)
A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

network-attached storage file server (NAS file server)
A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System
See NetBIOS.

Network Data Management Protocol (NDMP)
A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate
A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

node name
A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class
A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also privilege class.

non-native data format
A format of data that is written to a storage pool that differs from the format that the server uses for operations. See also native format.

O

offline volume backup
A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup
A backup in which the volume is available to other system applications during the backup operation.

open registration
A registration process in which users can register their workstations as client nodes with the server. See also closed registration.

operator privilege class
A privilege class that gives an administrator the authority to disable or halt the server, enable the server, cancel server processes, and manage removable media. See also privilege class.

options file
A file that contains processing options. See also client system-options file, client user-options file.

originating file system
The file system from which a file was migrated. When a file is recalled, it is returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the server that the client node is contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

P

packet In data communication, a sequence of binary digits, including data and control signals, that are transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode
A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation
A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character
See wildcard character.

physical file
A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also aggregate, logical file, physical occupancy.

physical occupancy
The amount of space that is used by physical files in a storage pool. This space includes the unused space that is created when logical files are deleted from aggregates. See also logical file, logical occupancy, physical file.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy domain
A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain. See also active policy set, domain.

policy privilege class
A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also privilege class.

policy set
A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also active policy set, management class.

premigrated file
A file that has been copied to server storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in server storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. See also file state, migrated file, resident file.

premigrated files database
A database that contains information about each file that has been premigrated to server storage.

premigration
The process of copying files that are eligible for migration to server storage, but leaving the original file intact on the local file system.

premigration percentage
A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool
A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also copy storage pool, server storage, storage pool, storage pool volume.

privilege class
A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also authority, node privilege class, operator privilege class, policy privilege class, storage privilege class, system privilege class.

profile
A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also configuration manager, enterprise configuration, managed server.

profile association
On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

Q

quota

1. For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.
2. For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization
The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume
A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

rebind
To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also bind, management class.

recall
To copy a migrated file from server storage back to its originating file system using the hierarchical storage management client. See also selective recall.

receiver
A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the server console and activity log. See also event.

reclamation
The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold
The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recovery log
A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register
To define a client node or administrator ID that can access the server.

registry
A repository that contains access and configuration information for users, systems, and software.

remote
For hierarchical storage management products, pertaining to the origin of migrated files that are being moved. See also local.

resident file
On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in server storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from server storage and modified.

restore
To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention
The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve
To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool. See also archive.

root user
A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See storage area network.

schedule
A database record that describes client operations or administrative commands to be processed. See also administrative command schedule, client schedule.

scheduling mode
The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume
A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use. See also volume.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. See also IBM Spectrum Protect command script.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup
The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. See also incremental backup.

selective migration
The process of copying user-selected files from a local file system to server storage and replacing the files with stub files on the local file system. See also demand migration, threshold migration.

selective recall
The process of copying user-selected files from server storage to a local file system. See also recall, transparent recall.

serialization
The process of handling files that are modified during backup or archive processing. See also shared dynamic serialization, shared static serialization, static serialization.

server A software program or a computer that provides services to other software programs or other computers. See also client.

server options file
A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode
A client/server communication technique where the server contacts the client node when tasks must be done. See also client-polling scheduling mode.

server storage
The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from hierarchical storage management client nodes (space-managed files). See also active-data pool, copy storage pool, primary storage pool, storage pool volume, volume.

session
A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data for the duration of the session. See also administrative session.

session resource usage
The amount of wait time, processor time, and space that is used or retrieved during a client session.

shadow copy
A snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shadow volume
: The data stored from a snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shared dynamic serialization
: A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. The backup-archive client retries the backup or archive operation a number of times; if the file is being modified during each attempt, the backup-archive client will back up or archive the file on its last try. See also dynamic serialization, serialization, shared static serialization, static serialization.

shared library
: A library device that is used by multiple storage manager servers. See also library.

shared static serialization
: A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. The client attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also dynamic serialization, serialization, shared dynamic serialization, static serialization.

snapshot
: An image backup type that consists of a point-in-time view of a volume.

space-managed file
: A file that is migrated from a client node by the hierarchical storage management (HSM) client. The HSM client recalls the file to the client node on demand.

space management
: See hierarchical storage management.

space monitor daemon
: A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file
: A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file
: On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL
: See Secure Sockets Layer.

stabilized file space
: A file space that exists on the server but not on the client.

stanza
: A group of lines in a file that together have a common function or define a part of the system. Stanzas are usually separated by blank lines or colons, and each stanza has a name.

startup window
: A time period during which a schedule must be initiated.

static serialization
: A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the backup-archive client cannot back up or archive the file. See also dynamic serialization, serialization, shared dynamic serialization, shared static serialization.

storage agent
: A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)
: A dedicated storage network tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
: A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also storage pool.

storage pool
: A named set of storage volumes that is the destination that is used to store client

data. See also active-data pool, copy storage pool, primary storage pool, storage hierarchy.

storage pool volume
A volume that has been assigned to a storage pool. See also active-data pool, copy storage pool, primary storage pool, server storage, volume.

storage privilege class
A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also privilege class.

stub
A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file
A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from server storage. It also contains additional information that can be used to eliminate the need to recall a migrated file. See also migrated file, resident file.

stub file size
The size of a file that replaces the original file on a local file system when the file is migrated to server storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription
In a storage environment, the process of identifying the subscribers to which the profiles are distributed. See also enterprise configuration, managed server.

system privilege class
A privilege class that gives an administrator the authority to issue all server commands. See also privilege class.

T

tape library
A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix
The high-level-qualifier of the file name or the data set name in the standard tape label.

target node
A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See trusted communications agent.

TCP/IP
See Transmission Control Protocol/Internet Protocol.

threshold migration
The process of moving files from a local file system to server storage based on the high and low thresholds that are defined for the file system. See also automatic migration, demand migration, migration job, selective migration.

throughput
In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout
A time interval that is allotted for an event to occur or complete before operation is interrupted.

IBM Spectrum Protect command script
A sequence of IBM Spectrum Protect administrative commands that are stored in the database of the IBM Spectrum Protect server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic. See also macro file, script.

tombstone object
A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types. See also communication method.

transparent recall
The process that is used to automatically recall a migrated file to a workstation or file server when the file is accessed. See also selective recall.

trusted communications agent (TCA)
A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See Universal Naming Convention.

Unicode
A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus many classical and historical texts.

Unicode-enabled file space
Unicode file space names provide support for multilingual workstations without regard for the current locale.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier. See also Globally Unique Identifier.

Universal Naming Convention (UNC)
The server name and network name combined. These names together identify the resource on the domain.

UTF-8 Unicode Transformation Format, 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208. See also UCS-2.

UUID See Universally Unique Identifier.

V

validate
To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version
A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space
A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual mount point
A directory branch of a file system that is defined as a virtual file system. The virtual file system is backed up to its own file space on the server. The server processes the virtual mount point as a separate file system, but the client operating system does not.

virtual volume
An archive file on a target server that represents a sequential media volume to a source server.

volume
A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also scratch volume, server storage, storage pool, storage pool volume.

volume history file
A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service (VSS)
A set of Microsoft application-programming interfaces (APIs) that are used to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See Volume Shadow Copy Service.

VSS Backup
A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on IBM Spectrum Protect server storage.

VSS Fast Restore
An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a file-level copy method.

VSS Instant Restore
An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a hardware assisted restore method (for example, a FlashCopy operation).

VSS offloaded backup
A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the IBM Spectrum Protect server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore
: A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on IBM Spectrum Protect server storage to their original location.

W

wildcard character
: A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workload partition (WPAR)
: A partition within a single operating system instance.

workstation
: A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name (WWN)
: A 64-bit, unsigned name identifier that is unique.

WPAR See workload partition.

WWN See worldwide name.

Index

Product Number: 5725-X12

Printed in USA