IBM Tivoli Storage Manager FastBack for Workstations
Version 6.3

Central Administration Console Installation and User's Guide

SC27-2808-02

IBM Tivoli Storage Manager FastBack for Workstations
Version 6.3

Central Administration Console Installation and User's Guide

SC27-2808-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 53.

This edition applies to Version 6.3.0 of IBM Tivoli Storage Manager FastBack for Workstations (product number 5724-Y96) and to all subsequent releases and modification until otherwise indicated in new editions or technical newsletters.

Contents

Preface v
Who should read this publication v
Publications v
Tivoli Storage Manager FastBack for Workstations publications v
Support information vi
Getting technical training vi
Searching knowledge bases vi
Contacting IBM Software Support viii

Chapter 1. Product Overview 1
New for the central administration console in version 6.3.0 1
Introduction to Tivoli Storage Manager FastBack for Workstations central administration console 1
Groups 2
Administration folders 2
Information currency 4

Chapter 2. Installing Tivoli Storage Manager FastBack for Workstations . . 7
System requirements. 7
Installing the central administration console 7
Uninstalling the central administration console . . . 8
Starting the central administration console GUI. . . 9
Starting and stopping the central administration console service 10

Chapter 3. Configuring the central administration console 11
Configuring central administration console monitoring tools. 11
Configuring email settings and scan interval . . 11
Defining alert conditions 12
Modifying alert conditions 12
Creating a script for clients 13
Modifying Java virtual machine memory settings. . 14

Chapter 4. Administering Tivoli Storage Manager FastBack for Workstations . . 15
Preparing to manage groups of clients 15
Planning groups of users 15
Creating a group 16
Creating a group with the configuration of an existing client. 17
Modifying all clients in a group 17
Groups Configuration: field explanations . . . 18
Discovering preexisting clients and assigning them to groups 32
Deploying new clients. 33
Creating a script for clients 33
Identifying administration folders 35
Creating a configuration file. 36
Deploying the client to other computers. . . . 37
Monitoring 38
Viewing the health status of all clients 38
Viewing the audit log 39
Viewing recent alerts 41
Administering clients 42
Creating a group with the configuration of an existing client. 42
Investigating a client 42
Configuring alerts (from the **Clients** task) . . . 46
Responding to client issues 46

Appendix. Accessibility features for Tivoli Storage Manager FastBack for Workstations 51

Notices 53

Trademarks. 57

Index 59

Glossary 61

Preface

This publication helps you install and use Tivoli® Storage Manager FastBack for Workstations.

Who should read this publication

This publication is intended for administrators who use the central administration console to manage Tivoli Storage Manager FastBack for Workstations.

Publications

Publications for the IBM® Tivoli Storage Manager family of products are available online.

The IBM Tivoli Storage Manager product family includes IBM Tivoli Storage Manager FastBack products, IBM Tivoli Storage Manager servers and backup-archive clients, IBM Tivoli Storage FlashCopy® Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, IBM Tivoli Storage Manager for Mail, IBM Tivoli Storage Manager for Enterprise Resource Planning, and several other storage management products from IBM Tivoli.

Many IBM Tivoli Storage Manager publications are available at the Tivoli Storage Manager information center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r3.

IBM Tivoli Storage Manager FastBack publications are available at the Tivoli Storage Manager FastBack information center at http://publib.boulder.ibm.com/infocenter/tsmfbinf/v6/index.jsp.

You can download PDF versions of publications from the information centers or from the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Go to Tivoli Documentation Central to find information centers that contain official product documentation for current and previous versions of Tivoli products, including the Tivoli Storage Manager product family. You can find Tivoli Documentation Central at https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home.

You can also order some related publications from the IBM Publications Center website. The website provides information about ordering publications from countries other than the United States. In the United States, you can order publications by calling 1-800-879-2755.

Tivoli Storage Manager FastBack for Workstations publications

The following table lists the publications that make up the Tivoli Storage Manager FastBack for Workstations library.

Table 1. Tivoli Storage Manager FastBack for Workstations publications

Publication title	Order number
IBM Tivoli Storage Manager FastBack for Workstations Client Installation and User's Guide	SC27-2809-02
IBM Tivoli Storage Manager FastBack for Workstations Central Administration Console Installation and User's Guide	SC27-2808-02
IBM Tivoli Storage Manager FastBack for Workstations Messages	SC27-4045-00

Support information

You can find support information for IBM products from various sources.

Start at the IBM Support Portal: http://www.ibm.com/support/entry/portal/. You can select the products that you are interested in and search for a wide variety of relevant information.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to the following websites to sign up for training, ask questions, and to interact with others who use IBM storage products.

Tivoli software training and certification
Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at http://www.ibm.com/software/tivoli/education/.

Tivoli Support Technical Exchange
Technical experts share their knowledge and answer your questions in webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html.

Storage Management community
Interact with others who use IBM storage management products at http://www.ibm.com/developerworks/servicemanagement/sm/index.html.

Global Tivoli User Community
Share information and learn from other Tivoli users throughout the world at http://www.tivoli-ug.org/.

IBM Education Assistant
View short "how to" recordings designed to help you use IBM software products more effectively at http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp.

Searching knowledge bases

If you have a problem with Tivoli Storage Manager FastBack for Workstations, you can search for information in a knowledge base.

Search the Tivoli Storage Manager FastBack V6.3.0 Information Center at http://publib.boulder.ibm.com/infocenter/tsmfbinf/v6/index.jsp.

Search the internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem.

To search multiple Internet resources for your product, go to the support web site for the product: Tivoli Storage Manager FastBack® for Workstations support Web site at http://www.ibm.com/software/tivoli/support/storage-mgr-fastback-workstation/ and search support for the product. From this section, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®
- Forums and newsgroups

Using IBM Support Assistant

At no additional cost, you can install on any workstation the IBM Support Assistant, a stand-alone application. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use.

The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, see the IBM Support Assistant Web site at http://www.ibm.com/software/support/isa/.

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at http://www.ibm.com/support/docview.wss?uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM Support Assistant website.

About this task

To check what fixes are available for your product, follow these steps:

Procedure

- From the IBM Support Assistant Web site at http://www.ibm.com/support/entry/portal/, click **Downloads**.
- Click **Search for recommended fixes**.
- Choose content filters to find fixes for your product level and operating system.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about IBM products.

About this task

To sign up to receive notifications about IBM products, follow these steps:

Procedure

1. From the IBM Support Assistant Web site at http://www.ibm.com/support/entry/portal/, click **Sign in to create, manage, or view your subscriptions** in the **Notifications** pane.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** and complete the registration process.
3. Click **Manage all my subscriptions** in the **Notifications** pane.
4. Click the **Subscribe** tab and then click **Tivoli**.
5. Select the products for which you want to receive notifications and click **Continue**.
6. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM subscription and support contract and if you are authorized to submit problems to IBM.

About this task

To obtain help from IBM Software Support, complete the following steps:

Procedure

1. Ensure that you have completed the following prerequisites:
   a. Set up a subscription and support contract.
   b. Determine the business impact of your problem.
   c. Describe your problem and gather background information.
2. Follow the instructions in "Submitting the problem to IBM Software Support" on page ix.

Setting up a software maintenance contract

Set up a software maintenance contract. The type of contract that you need depends on the type of product you have.

Procedure

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft Windows or UNIX operating systems), enroll in IBM Passport Advantage® in one of the following ways:
  – **Online:** Go to the Passport Advantage Web page at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
  – **By Phone:** For the phone number to call in your country, go to the IBM Software Support Handbook Web page at http://techsupport.services.ibm.com/guides/contacts.html and click **Contacts**.
- For server software products, you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for server software products, go to the IBM Technical support advantage Web page at http://www.ibm.com/servers/eserver/techsupport.html.

What to do next

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. For a list of telephone numbers of people who provide support for your location, go to the Software Support Handbook page at http://www.ibm.com/support/customercare/sas/f/handbook/home.html.

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem you are reporting.

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing the problem and gathering background information

When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
- Are you using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support

You can submit the problem to IBM Software Support online or by telephone.

Online

Go to the IBM Software Support website at http://www.ibm.com/support/entry/portal/Open_service_request/Software/Software_support_(general). Sign in to access IBM Service Requests and enter your information into the problem submission tool.

By telephone

For the telephone number to call in your country, go to the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

Chapter 1. Product Overview

This chapter provides an introduction to the Tivoli Storage Manager FastBack for Workstations central administration console and briefly describes enhancements for this version of the product.

New for the central administration console in version 6.3.0

The Tivoli Storage Manager FastBack for Workstations central administration console is updated for version 6.3.0.

The updates include the following enhancements:

Security improvements
The central administration console (CAC) runs within the Tivoli Integrated Portal. A new role-based authorization is available on the CAC to control access to the functions of CAC.

Email configuration enhancements
A new test feature was added to the email settings configuration panel. It allows users to verify the email SMTP settings to help ensure that emails are successfully delivered when alerts are triggered.

Administration folder search capability
Users who have existing FastBack for Workstations clients and want to add a Central Administration Console can automatically search for existing administration folders without knowing the exact name.

Introduction to Tivoli Storage Manager FastBack for Workstations central administration console

With the Tivoli Storage Manager FastBack for Workstations central administration console, you can centrally manage many Tivoli Storage Manager FastBack for Workstations clients.

With the central administration console, you can manage Tivoli Storage Manager FastBack for Workstations clients in the following ways:

- Discover existing Tivoli Continuous Data Protection for Files and Tivoli Storage Manager FastBack 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. Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack for Workstations clients.

Tivoli Storage Manager FastBack for Workstations can store backup copies on a Tivoli Storage Manager server, but there is no requirement to use Tivoli Storage Manager. Tivoli Storage Manager FastBack for Workstations is a stand-alone product and has no dependencies on Tivoli Storage Manager or Tivoli Storage Manager FastBack.

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 Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack for Workstations clients. With a single action from the central administration console, you can change the configuration of all Tivoli Storage Manager FastBack for Workstations clients in the accounting group to protect the new file type.

Administration folders

Clients pull 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, and 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 computers other than the central administration console server, 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. After the client is discovered, the central administration console locks the value of the administration folder.

If a Tivoli Storage Manager FastBack 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 Tivoli Storage Manager server, there is no default administration folder.

Tivoli Continuous Data Protection for Files Standard Edition clients have a **Central Administration Settings** panel that allows a user to explicitly configure the administration folder location. If the **Central Administration Folder** field is configured, that value overrides the default administration folder location. This allows a client that is configured with no remote storage, or one that is configured with remote storage on a Tivoli Storage Manager, to be discovered and managed by the central administration console. However, a user can change the administration folder setting to a location that is not known to the central administration console. If this happens, the central administration console cannot manage the Tivoli Continuous Data Protection for Files client.

Tivoli Continuous Data Protection for Files Starter Edition clients do not have a **Central Administration Settings** panel that allows a user to explicitly configure the administration folder location. If a Starter Edition client uses Tivoli Storage Manager 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 specify a folder that is identified to the central administration console and 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 Tivoli Continuous Data Protection for Files installation directory, like this:

```
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. In the computer-specific subfolder, there are two subfolders:

The Reports folder
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\.

The Downloads folder

When you put product upgrades or configuration files in this 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 group administrative Downloads subfolder, all clients that share this group administrative folder automatically adopt the product upgrades or configuration.

Maintaining control of the clients

Follow these guidelines to maintain control of the clients:

- Upgrade Tivoli Continuous Data Protection for Files clients to Tivoli Storage Manager FastBack for Workstations clients. Upgrading to Tivoli Storage Manager FastBack for Workstations eliminates the opportunity for users to set their administration folder location with the **Central Administration Settings** panel.
- Deploy Tivoli Storage Manager FastBack 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.

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 configuring email settings and scan intervals in the "Configuring email settings and scan interval" on page 11 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 Tivoli Storage Manager FastBack 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 based on the time elapsed since a client last reported.

Chapter 2. Installing Tivoli Storage Manager FastBack for Workstations

This chapter contains information for installing and initially configuring Tivoli Storage Manager FastBack for Workstations.

System requirements

The Tivoli Storage Manager FastBack for Workstations central administration console requires a Windows server with minimum levels of hardware and software.

For current software and hardware requirements, see FastBack for Workstations Hardware and Software Requirements, available at http://www.ibm.com/support/docview.wss?uid=swg21572912.

Installing the central administration console

Install the Tivoli Storage Manager FastBack for Workstations central administration console.

About this task

This task assumes that Tivoli Integrated Portal is not installed on the computer.

The central administration console installer is an executable file with a name like `x.x.x.x-TIV-FB4WKSTNS-CAC_windows.exe`. You must have administrative privilege to install Tivoli Storage Manager FastBack for Workstations central administration console.

Procedure

1. Start the installer from the product CD or from a download image. The introduction panel gives an overview of the installation process. Click **Next**.
2. Accept the license agreement and click **Next**.
3. Provide the user name and password for Tivoli Integrated Portal.
   - If Tivoli Integrated Portal is not previously installed, you are prompted to set the Tivoli Integrated Portal user name and password.
   - If Tivoli Integrated Portal is installed, you are prompted for the Tivoli Integrated Portal user name and password.
4. Enter the installation path for Tivoli Storage Manager FastBack for Workstations central administration or chose the default path `C:\Program Files\Tivoli\TSM\IBM FB4WCA Console` and click **Next**.
5. If Tivoli Integrated Portal was not previously installed, enter the installation path for Tivoli Integrated Portal or choose the default path `C:\IBM\tivoli\Tipv2_fbws` and click **Next**.
6. Click **Next** when presented with the list of components and installation location. The installation path is predetermined, and cannot be changed.
7. A dialog asks if you want to change the Tivoli Integrated Portal service logon account. The default account is the local windows system account. Select this option if you want to change the default Tivoli Integrated Portal service logon

account. You are asked to input a user name and password for the Tivoli Integrated Portal service logon account to be used.

Note: 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 computers other than the central administration console server, run the central administration console service in an account that has access to the remote administration folders.

8. Click **Done** when presented with a summary of the installation. When installation is complete, the installer starts Tivoli Integrated Portal in the default browser.

What to do next

When the central administration console is installed you can manage user access to the application. The central administration console has a role called **fbwscaAdministrator**. In the Tivoli Integrated Portal you can create a user and assign them to this role. They can only access the Tivoli Storage Manager FastBack for Workstations central administration portlet, without having the same rights are the default **tipadmin** user.

Uninstalling the central administration console

Uninstall the Tivoli Storage Manager FastBack for Workstations central administration console.

About this task

You must have administrative privilege to uninstall Tivoli Storage Manager FastBack for Workstations central administration console.

Procedure

1. Navigate to the **Control Panel** and then the list of installed programs.

Option	Description
On a Windows 2003 server:	**Start** > **Control Panel** > **Programs** > **Programs and Features**
On a Windows 2008 server:	**Start** > **Control Panel** > **Add or Remove Programs**

   A list of installed programs is displayed.

2. Click IBM FB4WCA Console.

Option	Description
On a Windows 2003 server:	Click **Change/Remove**.
On a Windows 2008 server:	Click **Uninstall/Change**.

3. In the introduction panel of the uninstall wizard, click **Uninstall**.
4. When you are prompted, enter the TIP (Tivoli Integrated Portal) user name and password.
5. Check the **Remove TIP** box if TIP is to be removed, and click **Next**.

Note: Other products may be using TIP. Make sure that other products will not be adversely affected before removing TIP.

Results

Tivoli Storage Manager FastBack for Workstations central administration console is uninstalled. A message window indicates when uninstallation is complete.

Starting the central administration console GUI

Start the central administration console graphical user interface (GUI) to monitor and actively manage the Tivoli Storage Manager FastBack for Workstations clients. You can also change the administration settings and group configurations.

Before you begin

Before you start the central administration console GUI, you must install the central administration console.

About this task

When you are not logged in to Tivoli Integrated Portal and working with the central administration console GUI, the central administration console continues to monitor clients, and sends alerts when needed.

Procedure

1. Start the Tivoli Integrated Portal GUI.
   - From the **Start** menu, choose **Tivoli** > **TSM** > **IBM FB4WCA Console** > **IBM_TSM_F4WS_Console**
   - With a web browser on the central administration console server, go to https://localhost:16311/ibm/console/logon.jsp
   - With a web browser on another computer, go to port 16311/ibm/console/logon.jsp on the central administration console server. For example, if the central administration console server address is 9.1.80.80, go to https://9.1.80.80:16311/ibm/console/logon.jsp.

   The Tivoli Integrated Portal login panel prompts you for a user name and password.
2. From the list of Tivoli Integrated Portal tasks, choose FastBack for Workstations. The FastBack for Workstations subtasks are shown: **Health Monitor**, **Clients**, **Groups Configuration**, **Administration Settings**.

   If the GUI session is inactive for some time (30 minutes by default), Tivoli Integrated Portal closes the session. It is possible that Tivoli Integrated Portal will prompt you for user name and password two times when you log in after a session timeout.

What to do next

You can administer clients with the central administration console GUI. You can monitor the health of clients, perform actions on clients, modify group configurations, and modify administration settings.

Starting and stopping the central administration console service

Start and stop the service that monitors Tivoli Storage Manager FastBack for Workstations clients and alerts you to problems with clients.

Before you begin

This task assumes that you installed the central administration console.

About this task

The central administration console service is automatically started after a successful installation and every time the computer starts. Whether or not you open the central administration console GUI, the central administration console service monitors clients and sends alerts. In most cases you do not need to start and stop the central administration console service. If you need to stop or start the central administration console service, follow this procedure.

Procedure

1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**. A list of services is displayed.
2. Click the service with this name: Tivoli Integrated Portal - V2.1_TIPProfile_Port_XXXXX The **Services** panel indicates the log on account and whether you can stop, start, or restart the service.
3. Optional: Change the properties of the service to log on to an account that has access to administration folders on other computers. 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. Run the service in an account that has access to the administration folders.
4. Optional: Click the appropriate action (stop, start, or restart). The central administration console service is stopped or started, according to your choice.

Chapter 3. Configuring the central administration console

You can configure administrative tools that monitor Tivoli Storage Manager FastBack for Workstations clients. This includes identifying the conditions that trigger alerts, and identifying who is alerted.

Configuring central administration console monitoring tools

Customize the central administration console tools that alert you to potential problems.

Configuring email settings and scan interval

Configure the central administration console to send you email when there is an alert. Configure the interval that the central administration console uses to scan administration folders to collect information about clients.

About this task

The central administration console can automatically send email notifications when there is a potential problem. You must identify your SMTP mail server.

The central administration console scans all administration folders on a regular interval. During these scans, the central administration console updates the status of clients and discovers new clients.

Procedure

1. Open the **Administration Settings** task. The administration tables are opened.
2. In the **Alerts Configuration** section, click the **Actions** menu.
3. Click **Configure the Scan Interval and E-mail for Alerts**. The **Configure the Scan Interval and E-mail for Alerts** panel is opened.
4. Set the scan frequency.
5. Identify the SMTP email server. Identify email server authorization information, and mail server port number, if required. The SMTP email server has an address like `smtp.example.com`.
6. Select the encryption type. The SSL certificate must be added to the Tivoli Integrated Portal WebSphere Application Server Administration console before you can send email via SSL. If you select SSL as the encryption type, follow these steps.
   a. Open the WebSphere Application Server Administration console.
   b. Go to **Security** > **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates** > **Retrieve from Port**.
   c. Enter information in the **Host**, **Port**, and **Alias** fields and click **Recieve signer information**.
   d. Click **Save directly to the master configuration** to implement the changes.
   e. You must restart the Tivoli Integrated Portal service before the changes take effect.

7. Specify the From email address to be used for all alert e-mails sent by the specified SMTP server. This address must be a valid, recognized email address on the SMTP server. It helps prevent alert emails from being blocked as spam.
8. Test the alert settings by entering an email address in the test email field and clicking test.
9. Click **OK**. The email configuration and scan interval are saved by the central administration console.

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 E-mail 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.

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 e-mail notification, or both.

Before you begin

If any alert conditions trigger e-mail notifications, you must identify the SMTP e-mail server with the **Configure the Scan Interval and E-mail 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.

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.

Modifying Java virtual machine memory settings

Set Java virtual machine (JVM) memory settings to enhance central administration console performance.

Before you begin

The value of the JVM `maximumHeapSize` setting directly affects the ability of the central administration console to manage many Tivoli Storage Manager FastBack for Workstations clients. When the value is set too low, the central administration console might become slow to respond, fail to load, or even crash.

About this task

This task describes how to modify the `maximumHeapSize` setting in order to prevent performance issues when managing many clients. Complete this task on the system where the central administration console server is installed.

Procedure

1. Go to the `C:\IBM\Tivoli\Tipv2_fbws\bin` directory. Query the JVM settings by issue the following sequence of commands:

   Tip: You are prompted to enter the Tivoli Integrated Portal (TIP) user ID and password after issuing `wsadmin.bat`.

   ```
   wsadmin

   set server1 [$AdminConfig getid /Cell/TIPCell/Node/TIPNode/Server/server1/]

   set jvm [$AdminConfig list JavaVirtualMachine $server1]

   $AdminConfig show $jvm

   quit
   ```

   Identify the value of the `maximumHeapSize` setting in the command results. In this procedure, the default value is 256 MB.
2. In order to modify the value of the `maximumHeapSize` setting, create a text file that contains the following content:

   Note: This example uses text file `jvm.jacl` and modifies the value of the `maximumHeapSize` setting to 512 MB.

   ```
   set server1 [$AdminConfig getid /Cell/TIPCell/Node/TIPNode/Server/server1/]

   set jvm [$AdminConfig list JavaVirtualMachine $server1]

   $AdminConfig modify $jvm {{initialHeapSize 256} {maximumHeapSize 512}}

   $AdminConfig save
   ```
3. From the `C:\IBM\Tivoli\Tipv2_fbws\bin` directory, issue this command:

   ```
   wsadmin -f jvm.jacl
   ```
4. Stop and restart the central administration console server. The modified value of the `maximumHeapSize` setting is applied.

Chapter 4. Administering Tivoli Storage Manager FastBack for Workstations

Information is available for administering Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack 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.

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. A group allows you 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 exposes 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. Provide configuration settings as requested by the wizard. You can accept the configuration settings provided by the wizard, or change them.
4. At the last page, 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.

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

This task requires that the central administration console discovered a client.

Procedure

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**. In the **Groups Configuration** task, you can see the new group in the table of groups. The group has the configuration of the client that you selected.

What to do next

You can add clients to the group. You can use the configuation of this group when deploying new clients.

Modifying all clients in a group

Modify the data-protection configuration of all clients in a group.

Before you begin

This task assumes the following:

- You created a group.

- The central administration console discovered some clients.
- You assigned some clients 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 **Groups Configuration** task. The table of groups is displayed.
2. Select the group that you want to modify.
3. From the **Actions** menu, click **Modify a Group**. The **Groups Configuration** notebook displays the current settings for the group.
4. Modify the configuration settings.
5. Click **OK**. The group configuration is modified, and the new configuration is sent to all clients in the group. The clients adopt the new configuration settings.

Groups Configuration: field explanations

The **Groups Configuration** notebook allows you to configure the data-protection settings for Tivoli Storage Manager FastBack for Workstations clients.

The **Groups Configuration** notebook of the central administration console is like the **Settings Notebook** of the client. Most of the panel titles and field labels are the same.

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

Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack for Workstations.

Continuous protection level list

Tivoli Storage Manager FastBack 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
Tivoli Storage Manager FastBack for Workstations creates backup copies only on the local storage area.

Remote storage only
Tivoli Storage Manager FastBack for Workstations creates backup copies only on the remote storage area.

Local and remote storage
Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack for Workstations as internal drives, are protected.

In some cases, an external USB drive looks like an internal drive, and Tivoli Storage Manager FastBack 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)

Tivoli Storage Manager FastBack 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.

Table 1 summarizes the interaction of inclusion and exclusion.

Table 2. 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 "Wildcards 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.

Wildcards in file specifications:

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

You can enter the complete path of a file that you want to protect. For example, `C:\Documents and Settings\Administrator\My Documents\Soccer\2005AYSO\Parent Info U8B.doc`. The complete path must match a single file. You can use asterisks and blanks as wildcards to specify several files.

An asterisk matches any number of characters in a file path. If there are no asterisks, Tivoli Storage Manager FastBack 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.

If there are no asterisks, blank spaces before and after the pattern are interpreted as asterisks. For example, `\myDocs\` and `*\myDocs\*` yield the same matches. If there are asterisks in the pattern, blank spaces before or after the pattern match no characters. For example, `\myDir\`, `*\myDir\`, and `\myDir\*` can yield three different matches.

For example, assume a pattern `fish`. This pattern matches: `C:\dir\fish.doc` and `C:\fish\anyfile.doc` and `c:\Dirfishfood\something`.

If the pattern has slashes around it (`\fish\`), it matches any object with `\fish\` somewhere in the path. This pattern matches `C:\fish\anyfile.doc` but not `C:\dir\fish.doc` and not `c:\Dirfishfood\something`.

This table provides examples of how patterns match files and folders.

Table 3. File and folder pattern matches

This pattern ...	... matches these 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 of time and after that time the files are not vaulted.

To specify duration of vaulting, create a folder 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 file 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 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 you use must be preceded by a number up to five 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 are valid examples:

   \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.

E-mail Protection panel of Groups Configuration

Select the e-mail 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, Tivoli Storage Manager FastBack 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**.

E-mail application data files or folders field

If you choose your e-mail application from the **E-mail 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 **E-mail Application** list.

Additional files or folders you want to be backed up when your e-mail is backed up field

Identify additional 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 e-mail files and additional 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.

Considerations for scheduled backups:

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 protected by schedule are backed up even if they are open, but you can try to schedule the backup for a time when the files are closed.

Scheduled backup can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but offer fewer opportunities when you want to restore a file.

When does a scheduled backup 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, the files that have changed at that time are noted and 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 powered off or Tivoli Storage Manager FastBack for Workstations is not running at the schedule time, the scheduled backup runs when the computer is powered on and Tivoli Storage Manager FastBack for Workstations is running.

If you shut down a computer or stop the Tivoli Storage Manager FastBack for Workstations client when a scheduled backup is running, the backup resumes when the client is running again and the remote storage is available.

If you forced a backup of scheduled files during the 30 minutes prior to the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

Tivoli Storage Manager FastBack for Workstations backs up all files that have changed during the schedule interval, including files that are still open at the time of backup. The backup copies of files that are backed up while open can be corrupted. So it is suggested that you close applications before a scheduled backup. Tivoli Storage Manager FastBack for Workstations offers an opportunity to close applications before a scheduled backup.

At the beginning of a scheduled backup, Tivoli Storage Manager FastBack for Workstations attempts to close all files that are listed in a text file called `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. Tivoli Storage Manager FastBack for Workstations sends a close command to each instance of every program named in the `closeapps.txt` file. Note that Tivoli Storage Manager FastBack 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. Tivoli Storage Manager FastBack for Workstations is tolerant of intermittently available networks. If the remote storage area is temporarily unavailable, Tivoli Storage Manager FastBack 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.

Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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.

Tivoli Storage Manager storage location

Tivoli Storage Manager FastBack for Workstations can store backup copies on a Tivoli Storage Manager server.

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

You can use Tivoli Storage Manager server version 6.1 or later with Tivoli Storage Manager FastBack for Workstations.

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

If you specify a Tivoli Storage Manager 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 Tivoli Storage Manager FastBack for Workstations subfolder of the "Program data folder" on page 29.

Restriction: You cannot use a subfile backup feature when the Tivoli Storage Manager server is the backup target.

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

Restriction: If you use Tivoli Storage Manager FastBack for Workstations encryption, you cannot use Tivoli Storage Manager compression.

To manage storage space, the Tivoli Storage Manager administrator must grant authority to the Tivoli Storage Manager 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 Tivoli Storage Manager server, see the topic in the problem determination section of the client documentation: *Files are not backed up to Tivoli Storage Manager server*.

How many versions to keep:

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

Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack for Workstations deletes older backup copy versions of files that have several backup copy versions. If more space is needed for new backup copies, Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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 Tivoli Storage Manager as the remote storage server. If you must encrypt or compress your data, then use the Tivoli Storage Manager server compression or encryption features.

Encrypt backups:

Set encryption for remote backup copies.

The encryption feature provides extra security on your remote location. The encryptions feature can be useful if multiple people have access to the remote server location, and you need to ensure that data is protected from other users who have access to the remote server.

When you click the button labeled **Encrypt backups**, Tivoli Storage Manager FastBack for Workstations will present a dialog so you can create a password for the encrypted files. This password is required to view or access any files which are backed up by Tivoli Storage Manager FastBack for Workstations. The encrypted

password is kept in the “Program data folder.” If the files in the program data folder are lost, you will be prompted to enter a new password.

Once encryption has been enabled, the password is stored. If you disable encryption, then enable again, you are not prompted for a new password.

Tivoli Storage Manager FastBack for Workstations does not support prompted encryption. Hence, if you specify Tivoli Storage Manager server as your remote storage area, you must configure non-prompted encryption in the Tivoli Storage Manager `dsm.opt` options file. In the `dsm.opt` file, use the statement: `encryptkey generate`. See *Tivoli Storage Manager for Windows Backup-Archive Client Installation and User's Guide* for information about setting encryption options in Tivoli Storage Manager `dsm.opt` file. Tivoli Storage Manager FastBack for Workstations supports AES128 encryption but does not support AES56 encryption.

The dsm.opt file is in the “Program data folder.”

Files stored on the local storage area are not encrypted. Files that are compressed can not be encrypted, and the user interface does not allow you to configure both encryption and compression. Files that use sub-file copy can be encrypted.

Tivoli Storage Manager FastBack for Workstations cannot protect backup copies that it has encrypted. This means that Tivoli Storage Manager FastBack for Workstations cannot create encrypted backup copies, and then make backup copies (encrypted or not) of those backup copies.

If you configure Tivoli Storage Manager FastBack for Workstations to encrypt the backup copies to a file server, you must not use Tivoli Storage Manager FastBack for Workstations to protect the encrypted backup copies on that file server. You can use Tivoli Storage Manager or another backup solution to protect the encrypted backup copies on that file server.

You do not have to choose either encryption or compression. By clicking the buttons, you can clear both buttons, and select neither encryption or compression.

Program data folder: The program data folder varies according to the operating system and installation of the Tivoli Storage Manager FastBack for Workstations client. This list indicates the program data folder for each operating system and product version:

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 backed up using the compression function must be restored using Tivoli Storage Manager FastBack 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 neither 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, Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack 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, Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack for Workstations client version 6.1 or earlier.

Considerations for scheduled backups:

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 protected by schedule are backed up even if they are open, but you can try to schedule the backup for a time when the files are closed.

Scheduled backup can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but offer fewer opportunities when you want to restore a file.

When does a scheduled backup 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, the files that have changed at that time are noted and 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 powered off or Tivoli Storage Manager FastBack for Workstations is not running at the schedule time, the scheduled backup runs when the computer is powered on and Tivoli Storage Manager FastBack for Workstations is running.

If you shut down a computer or stop the Tivoli Storage Manager FastBack for Workstations client when a scheduled backup is running, the backup resumes when the client is running again and the remote storage is available.

If you forced a backup of scheduled files during the 30 minutes prior to the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

Tivoli Storage Manager FastBack for Workstations backs up all files that have changed during the schedule interval, including files that are still open at the time of backup. The backup copies of files that are backed up while open can be

corrupted. So it is suggested that you close applications before a scheduled backup. Tivoli Storage Manager FastBack for Workstations offers an opportunity to close applications before a scheduled backup.

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

Discovering preexisting clients and assigning them to groups

Manage Tivoli Continuous Data Protection for Files clients and Tivoli Storage Manager FastBack for Workstations clients that existed before you installed the central administration console.

Before you begin

This task assumes that you or client users installed Tivoli Continuous Data Protection for Files clients or Tivoli Storage Manager FastBack for Workstations clients before you installed the central administration console, or you installed the clients 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

You can complete this task to discover and manage Tivoli Continuous Data Protection for Files clients and Tivoli Storage Manager FastBack for Workstations clients.

Procedure

1. Identify the administration folders that are used by the preexisting clients.
   a. Open the **Administration Settings** task. The administration tables are shown.
   b. In the **Administration Folders** section, click **Actions**.
   c. Click **Identify an Administration Folder**. The **Identify an Administration Folder** panel is shown.
   d. Enter data in the **Alias** and **Administration folder** fields. 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**. The value of the **Select a group for new clients** and **Select a script for new clients** fields does not affect preexisting clients. If there are existing clients in the folder the user has to manually add them to the group.

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

e. Click **OK**.

The preexisting 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 existed before you installed the central administration console are not automatically added to groups.
   a. Open the **Clients** task. The **Clients** panel shows the following tabs: **Health**, **Storage**, and **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 a preexisting client is discovered, it is not automatically added to a group. Find preexisting 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 you selected.

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 Tivoli Storage Manager FastBack for Workstations installer file.

About this task

With the central administration console, you can create a configuration file. You must obtain the Tivoli Storage Manager FastBack for Workstations client installer, and deploy the installer and configuration file to end users.

Procedure

1. Create a script that a Tivoli Storage Manager FastBack for Workstations client runs when it 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.

Identifying administration folders

Identify a folder that is accessible to the central administration console and Tivoli Storage Manager FastBack 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.

Example: Prepare to deploy clients to the sales group

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

Before you begin

You have a plan for grouping your end users according to their data-protection needs. You created the groups.

About this task

Assume that you created 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 Tivoli Storage Manager FastBack for Workstations clients of the sales team. Hence, you must identify the administration folder: \\server1\fbwsadmin\sales.

Procedure

1. In the **Identify an Administration Folder** panel, 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

Now you can create a configuration file for the Tivoli Storage Manager FastBack 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 Tivoli Storage Manager FastBack 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.

Deploying the client to other computers

There are several ways to deploy the initial installation of the Tivoli Storage Manager FastBack for Workstations client to other computers.

- Use Microsoft Systems Management Server to install the Tivoli Storage Manager FastBack for Workstations.msi package. 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 Tivoli Storage Manager FastBack for Workstations client is initially installed, the installer retrieves configuration data from the files `\System32\fpa.txt`, `\System32\dsm.opt`, or `\System32\networks.xml` 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, Tivoli Storage Manager FastBack 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 *FastBack for Workstations Client Installation and User's Guide*.

Windows installation folder

The Tivoli Storage Manager FastBack for Workstations client references the Windows installation folder during installation. During the installation, the client can get configuration information from the file named `fpa.txt`, `dsm.opt` or `networks.xml` files in the `\System32\` subfolder in the Windows installation folder.

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`** install parameter to specify another directory path for the configuration files.

Monitoring

Monitor the activity of clients and the central administration console

Viewing the health status of all clients

View the health of your data-protection system. The **Health Monitor** panel 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 discovered some clients.

Procedure

1. Open the **Health Monitor** task. The **Health Monitor** panel has the following sections:
   - **Clients Summary**
   - **Audit Logs**
   - **Alerts**

   The **Clients Summary** section lists summary information about the health of clients. The status of each client can be listed as: **Fatal**, **Critical**, **Warning**, **Normal**.
2. Click a health status to see details of clients with that health status. The **Health** view of the **Clients** task lists all clients with that health status.
3. Optional: Filter the client entries that are displayed.
   a. In the text filter 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 table displays only the clients that match the text string that you entered. If you selected more than one column name, the filter yields only clients that have matching text in all selected columns. The filter is case-sensitive.

   For example, if you typed **none** and selected the **Group** column name, only the clients associated with no group (**Group** = **none**) are displayed.

   More strings are matched when you use wildcards in the filter text. An asterisk replaces several characters. A question mark replaces one character. If you use an asterisk or wildcard in the filter text, the blank space beyond the end of your filter text matches any text.

Table 4. 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 are ordered in ascending sequence according to the text in the cells of that column.
   b. Click the same column heading again. The entries are ordered in descending sequence according to the text in the cells of that column.
   c. Click another column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.

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.

Viewing the audit log

Monitor the health of the data-protection system by viewing the log of the central administration console server. The audit log records all interaction with the central administration console and with the clients.

About this task

The audit log records events from the central administration server. If you are interested only in the events of an individual client, see the activity log for that client.

The audit log is located in the IBM WebSphere Application Server profiles folder. The audit log folder in a default installation path is `C:\IBM\Tivoli\Tipv2_fbws\`

profiles\TIPProfile. The audit log is composed of 10 files, named audit.log.0, audit.log.1...audit.log.9. File audit.log.0 logs the most recent activity and audit.log.9 logs the least recent activity.

Procedure

1. Open the **Health Monitor** task. The **Health Monitor** panel displays the following sections:
   - **Clients Summary**
   - **Audit Logs**
   - **Alerts**

   In the **Audit Logs** section, the most recent events are listed.
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 wildcards in the filter text. An asterisk replaces several characters. A question mark replaces one character. If you use an asterisk or wildcard in the filter text, the blank space beyond the end of your filter text matches any text.

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

4. Optional: Order the entries by sorting on the values in any column.
   a. Click a column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.
   b. Click the same column heading again. The entries are ordered in descending sequence according to the text in the cells of that column.
   c. Click another column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.

What to do next

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

Viewing recent alerts

View all recent alerts.

Procedure

1. Open the **Health Monitor** task. The **Health Monitor** panel displays the following sections:
   - **Clients Summary**
   - **Audit Logs**
   - **Alerts**

   In the **Alerts** section, the most recent alerts are listed.
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 wildcards in the filter text. An asterisk replaces several characters. A question mark replaces one character. If you use an asterisk or wildcard in the filter text, the blank space beyond the end of your filter text matches any text.

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

3. Optional: Order the entries by sorting on the values in any column.
   a. Click a column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.
   b. Click the same column heading again. The entries are ordered in descending sequence according to the text in the cells of that column.
   c. Click another column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.

What to do next

If you need 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 needed, you can deploy software updates, change the configuration of a client, or send a script to a client in the **Clients** task.

Administering clients

Investigate a Tivoli Storage Manager FastBack 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

This task requires that the central administration console discovered a client.

Procedure

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**. In the **Groups Configuration** task, you can see the new group in the table of groups. The group has the configuration of the client that you selected.

What to do next

You can add clients to the group. You can use the configuation of this group when deploying new clients.

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. Select clients and take action.

Before you begin

This task assumes that the central administration console discovered some clients.

Procedure

1. Open the **Clients** task. The **Clients** panel displays three tabs: **Health**, **Storage**, and **Deployment**.
2. Click the tab that contains information that you want to view. Each tab has a table that shows different information about the clients. There is also information that is shared among the three tabs.
3. Optional: Filter the client entries that are displayed.
   a. In the text filter 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 table displays only the clients that match the text string that you entered. If you selected more than one column name, the filter yields only clients that have matching text in all selected columns. The filter is case-sensitive.

   For example, if you typed **none** and selected the **Group** column name, only the clients associated with no group (**Group** = **none**) are displayed.

   More strings are matched when you use wildcards in the filter text. An asterisk replaces several characters. A question mark replaces one character. If you use an asterisk or wildcard in the filter text, the blank space beyond the end of your filter text matches any text.

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

4. Optional: Order the entries by sorting on the values in any column.
   a. Click a column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.
   b. Click the same column heading again. The entries are ordered in descending sequence according to the text in the cells of that column.
   c. Click another column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.

What to do next

With the data provided, you can decide what action is needed 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. This time 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 end 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 noticed a problem with only a single client, you can check the current configuration file of that client to confirm that the end user did not modify some data-protection settings for the client.

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.

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 same log is called the activity report.

Before you begin

This task assumes that the central administration console discovered 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. The **Clients** panel has the following tabs: **Health**, **Storage**, and **Deployment**.
2. Click the **Health** tab.
3. Select the client whose log you want to see.
4. Click the **Actions** menu.
5. Click **View Activity Log** to view the log entries.
6. 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 wildcards in the filter text. An asterisk replaces several characters. A question mark replaces one character. If you use an asterisk or wildcard in the filter text, the blank space beyond the end of your filter text matches any text.

Table 8. Filter strings and matching text

Filter text string	Matching text
Jupiter	Jupiter
Jupiter?	Jupiter Jupiter_bright_moon_light Jupiter_moon

Table 8. Filter strings and matching text (continued)

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

7. Optional: Order the entries by sorting on the values in any column.
   a. Click a column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.
   b. Click the same column heading again. The entries are ordered in descending sequence according to the text in the cells of that column.
   c. Click another column heading. The entries are ordered in ascending sequence according to the text in the cells of that column.

What to do next

After viewing the activity log, you can gather more information or take action.

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 has backed up many audio and movie files. You know that client23 belongs to a group that excludes audio and movie files from backups.

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

You contact the end user, and determine that the audio and movie files should not be backed up. You can resend the group configuration to client23 by assigning client23 to the group again.

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.

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.

Responding to client issues

Update client software, resend data-protection configurations, send command scripts, modify groups.

Deploying software updates

Deploy software updates to the clients.

Before you begin

This task assumes that the central administration console discovered some clients, and that you have an installer file for updated client software.

About this task

This task upgrades the software of clients that are already installed. This task does not include installing a client.

The client installer file name must include FB4WKSTNS and must be file type `.exe`. A typical file name is `x.x.x.x-TIV-FB4WKSTNS-x86_windows.exe` .

Procedure

1. Put the client installer file in the `fbfw\deployments\` subfolder of the TIP WebSphere Application Server profiles folder. The deployments folder in a default installation path is `C:\IBM\Tivoli\Tipv2_fbws\profiles\TIPProfile\fbfw\deployments`.
2. Open the **Clients** task. The **Clients** panel has the following tabs: **Health**, **Storage**, and **Deployment**.
3. Click the **Deployment** tab.
4. Select the clients that you want to update.

5. In the **Actions** menu, click **Deploy Software Updates**. The **Deploy Software Updates** panel opens. Files in the `deployments` folder are viewable.
6. Select a client installer file from the list and click **OK**.

Results

The installer file is pushed to the Downloads subfolder of the administration folder of the client. The client pulls the installer file from the Downloads subfolder of the administration folder.

Considerations for upgrading a client:

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

The new client installer file name must contain the string FB4WKSTNS and end with .exe. For example, a typical name is `x.x.x.x-TIV-FB4WKSTNS-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.

Cleaning up after uninstallation

If you uninstall the client, you must clean your data files before installing the client again. When the client is uninstalled, some files are not removed by the installer. The old files can cause problems for a new installation of the client.

After uninstalling the client, and before installing it again, remove files in the following areas:

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 folder is `c:\Program Files\Tivoli\TSM\FastBack_for_Workstations`. If you upgraded from Tivoli Continuous Data Protection for Files, the default installation folder is `C:\Program Files\Tivoli\CDP_for_Files`.

The program data folder
The program data folder varies according to operating system and previously installed versions.

Upgrade from Continuous Data Protection for Files

If you upgrade from Tivoli Continuous Data Protection for Files, your Tivoli Continuous Data Protection for Files client must be at level 3.1 or later.

Tivoli Continuous Data Protection for Files versions older than 3.1.5.9 accept client installer files with a name like `TivoliCDP_CDPForFiles_3.1.8.0_windows.exe`. The installer name must include CDP and must be file type `.exe`. Tivoli Continuous

Data Protection for Files version 3.1.5.9 and later accepts client installer files with CDP or FB4WKSTNS in the file name. Tivoli Storage Manager FastBack for Workstations client installer files have a name like `x.x.x.x-TIV-FB4WKSTNS-x86_windows.exe`. The installer file name for a Tivoli Storage Manager FastBack for Workstations client must contain FB4WKSTNS. Hence, if you want a Tivoli Continuous Data Protection for Files client at less than version 3.1.5.9 to pull an upgrade to Tivoli Storage Manager FastBack for Workstations, you have two options.

- You can rename the Tivoli Storage Manager FastBack for Workstations installer file to include CDP in the file name.
- You can first upgrade the Tivoli Continuous Data Protection for Files client to version 3.1.5.9 or later. Then the client can pull an installer file with CDP or FB4WKSTNS in the file name.

Program data folder: The program data folder varies according to the operating system and installation of the Tivoli Storage Manager FastBack for Workstations client. This list indicates the program data folder for each operating system and product version:

Sending a script to clients

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 some clients.

About this task

To send a script to a client when the client is first installed and initially discovered by the central administration console, you can set the **Select a script for new clients** field when you identify an administration folder.

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

Procedure

1. Open the **Clients** task. The **Clients** panel displays the following tabs: **Health**, **Storage**, and **Deployment**.
2. Select one or more clients to which you want to send a script.
3. In the **Actions** menu, click **Send Clients a script**. The script is sent to the selected clients. The clients run the script.

Modifying the configuration of a single client

You can modify the configuration of a single client. Because configurations are associated with groups, you must determine the consequence for the group.

If all clients in the group need the same modification, then modify the group.

If other clients in the group do not need the same modification, you must assign the client to a group with an appropriate configuration. Consider whether any existing groups are appropriate. If no groups have an appropriate configuration, create a group with the appropriate configuration for just this client.

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

Modifying all clients in a group

Modify the data-protection configuration of all clients in a group.

Before you begin

This task assumes the following:

- You created a group.
- The central administration console discovered some clients.
- You assigned some clients 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 **Groups Configuration** task. The table of groups is displayed.
2. Select the group that you want to modify.
3. From the **Actions** menu, click **Modify a Group**. The **Groups Configuration** notebook displays the current settings for the group.
4. Modify the configuration settings.
5. Click **OK**. The group configuration is modified, and the new configuration is sent to all clients in the group. The clients adopt the new configuration settings.

Assigning clients to a group

Assign or reassign one or more clients to a group. 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:

- You created a group.
- The central administration console discovered some clients.

About this task

This task is for clients that are not assigned to a group, or for clients that you want to move to another group.

Procedure

1. Open the **Clients** task. The **Clients** panel displays the following tabs: **Health**, **Storage**, and **Deployment**.
2. In any view of the **Clients** task, filter and select the clients that you want to assign to a group.
3. In the **Actions** menu, click **Assign Clients to a Group**.
4. In the **Assign Clients to a Group** panel, select a group from the list and click **OK**. The clients are displayed in the table in the **Clients** task again. The clients are members of the group that you selected.

Restoring the configuration of clients

Restore a group configuration to a client that was changed by the user.

Before you begin

This task assumes the following:

- You created a group.
- The central administration console discovered some clients.
- You assigned some clients to a group.

About this task

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. Assign the client to the group again, and the central administration console automatically sends the group configuration to the client.

Procedure

1. Open the **Clients** task. The **Clients** panel shows the following tabs: **Health**, **Storage**, and **Deployment**.
2. In any view of the **Clients** task, filter and select the clients that you want to reassign to a group.
3. In the **Actions** menu, click **Assign Clients to a Group**.
4. In the **Assign Clients to a Group** panel, select a group from the list and click **OK**. The central administration console sends the group configuration to the clients.

Appendix. Accessibility features for Tivoli Storage Manager FastBack for Workstations

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features of Tivoli Storage Manager FastBack for Workstations are described in this topic.

Accessibility features

The following list includes the major accessibility features in Tivoli Storage Manager FastBack 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 provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The Tivoli Storage Manager FastBack for Workstations Information Center, and its related publications, are accessibility-enabled.

Keyboard navigation

Tivoli Storage Manager FastBack for Workstations follows Microsoft conventions for most keyboard navigation and access. Drag and Drop support is managed using the Microsoft Windows Accessibility option known as MouseKeys. For more information about MouseKeys and other Windows accessibility options, please refer to the Windows Online Help (keyword: MouseKeys).

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, do the following:
   - With focus on the check box, 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 Tivoli Storage Manager FastBack for Workstations in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. You can access these or any of the other documentation PDFs 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 U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

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 http://www.ibm.com/legal/copytrade.shtml.

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

Index

Special characters

fpa config-set command 2

A

accessibility features 51
activity log
  viewing in the central administration console 44
administering clients, overview 1
administration folders
  associating with a group 35
  Identify an Administration Folder panel 35
  identifying
    overview 2
  managing clients 2
Administration Settings
  Configure the Scan Interval and E-mail for Alerts panel 11
  Create a script panel 13, 34
  Define Alert Conditions panel 12
  Files to Protect panel 35
Advanced panel (Groups Configuration) 30
alerts
  configuring
    from Clients task 46
    modifying 12
    new 12
  viewing 41
audit log
  viewing 39

B

Back up to: drop down list 25

C

central administration console
  overview 1
  starting 9
central administration console service
  starting 10
central administration server
  log 39
clients
  assigning to a group
    after discovery 49
    initial deployment 35
  current configuration, viewing 45
  deploying
    example 36
    instructions 33
  deploying software updates 46
  Deployment view 42
  discovering 32
  group assignment, changing 49
clients *(continued)*
  health summary, viewing 38
  Health view 42
  import client configuration to a group 17, 42
  investigating 42
  logs
    viewing in the central administration console 44
  modifying 48
  modifying configuration
    central administration console 17, 49
  preexisting
    administering 32
  restoring configuration 50
  scan interval
    configuration 11
  sending a script 48
  Storage view 42
Clients panel 42
closeapps.txt 24, 31
Command timeout field 13, 34
Compress backups radio button 29
configuration
  fpa config-set command 2
  client current configuration, viewing 45
  clients
    changing group assignment 49
    restoring 50
  import from client 17, 42
configuration file
  creating 37
configuration of clients
  locking 30
  performance settings 30
Configure the Scan Interval and E-mail for Alerts panel 11
continuous protection
  specify files using wildcards 21
  specify which files are included and excluded 20
Continuous Protection panel (Groups Configuration) 18
Create a Script panel 13, 34
customer support
  contact viii

D

Define Alert Conditions panel 12
definitions 61
deploying the client 37
drives, protected 20

E

e-mail
  alerts 11
e-mail *(continued)*
  configuration 11
E-mail Protection panel (Groups Configuration) 23
education
  see Tivoli technical training vi
Email Application drop down list 23
Encrypt backups radio button 28
exclude files from protection 20
external device
  remote storage location 25

F

file server
  remote storage location 25
files
  specifying 21
Files to Protect panel (Groups Configuration) 19
fixes, obtaining vii, viii

G

glossary 61
groups
  assigning clients
    changing group 49
    restoring configuration 50
  assigning to a group
    preexisting clients 32
  creating 16
  deploying clients
    example 36
  import configuration from a client 17, 42
  modifying configuration
    central administration console 17, 49
  overview 2
  planning 15
  reassigning clients 49
  selecting for administration folder 35
Groups Configuration
  Advanced panel 30
  Continuous Protection panel 18
  E-mail Protection panel 23
  Files to Protect panel 19
  Remote Storage panel 25

H

Health Monitor panel 38
health status
  scan interval
    configuration 11
How many versions to keep: field 27
How often to protect your email drop down list 24

I

IBM Publications Center v
IBM Support Assistant vii
Identify an Administration Folder panel 35
include files for protection 20
information currency 5
Initial scan
  command in a script 13, 34
installation
  central administration console 7
  client
    pull upgrade considerations 47
    push to remote computers 37
  system requirements
    client 7
  uninstall
    central administration console 8
Internet, search for problem resolution vii
Internet, searching for problem resolution vii
interpreting file and folder patterns 21

K

knowledge bases, searching vi

L

Location text field 25
Lock the configuration of clients 30
logs
  central administration server 39
  client activity log, viewing
    central administration console 44
  viewing the audit log 39

M

Maximum space for backups: field 28
monitoring tools
  configuring 11

N

name patterns with wildcards 21
new for version 6.3.0
  central administration console 1
Number of simultaneous clients field 13, 34

P

patterns with wildcards 21
performance settings
  clients 30
problem determination
  describing problem for IBM Software Support ix
  determining business impact for IBM Software Support ix
  submitting a problem to IBM Software ix
product overview
  central administration console 1
protected drives 20
publications
  download v
  FastBack for Workstations vi
  order v
  search v
push the client installation to remote computers 37

R

reassigning clients to a group 50
remote storage
  WebDAV server 25
remote storage location
  external device 25
  file server 25
  Tivoli Storage Manager 25
  USB device 25
Remote Storage panel (Groups Configuration) 25

S

Scan and back up
  command in a script 13, 34
scan interval
  configuration 11
scheduled protection
  close applications prior to scheduled backup 24, 31
  scheduled backup considerations 24, 31
  specify files using wildcards 21
  specify which files are included and excluded 20
script
  creating 13, 34
  send to clients 48
scripts
  selecting for administration folder 35
Select a group for new clients field 35
Select a script for new clients field 35
silent installation
  push the client to remote computers 37
software support
  describing problem for IBM Software Support ix
  determining business impact for IBM Software Support ix
  submitting a problem ix
Software Support
  contact viii
software updates
  deploying 46
specifying files to protect 21
starting
  central administration console GUI 9
  central administration console service 10
status currency 5
status summary of clients, viewing 38
sub-file copy radio button 30
support information vi
system requirements
  client 7

T

Tivoli Storage Manager remote storage location 25
Tivoli technical training vi
training, Tivoli technical vi

U

uninstall
  central administration console 8
updates
  deploying client software 46
upgrade the client
  considerations for pull upgrade 47
USB device
  exclude from protection 20
  remote storage location 25
Use sub-file copy radio button 30

V

vault duration 22
vaulted protection
  specify vault duration 22

W

WebDAV server remote storage location 25
wildcards in file specifications 21
Windows installation folder 38
Windows, Notebooks, and Dialogs
  Administration Settings
    Configure the Scan Interval and E-mail for Alerts panel 11
    Create a Script panel 13, 34
    Define Alert Conditions panel 12
    Identify an Administration Folder panel 35
  Clients panel 42
  Groups Configuration
    Advanced panel 30
    Continuous Protection panel 18
    E-mail Protection panel 23
    Files to Protect panel 19
    Remote Storage panel 25
  Health Monitor panel 38

Glossary

This glossary includes terms and definitions.

To view glossaries for other IBM products, go to http://www.ibm.com/software/globalization/terminology.

The following cross-references are used in this glossary:

- *See* refers the reader from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- *See also* refers the reader to a related or contrasting term.

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 *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. For example, an access control list is associated with a file that identifies the users who can access that file 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. The access mode can be read/write, read-only, or unavailable. Volumes in primary storage pools can also have an access mode of destroyed. Volumes in copy storage pools can also have an access mode of offsite.

acknowledgment
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.

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. Contrast with *inactive file system*.

active policy set
The activated policy set that contains the policy rules in use by all client nodes that are assigned to the policy domain. See also *policy domain* and *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. Contrast with *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 Tivoli Storage Manager server. Contrast with *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 *client 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. Contrast with *client node session*.

administrator
A user who is registered to the server as an administrator, and who is authorized to perform tasks and issue commands through the assignment of an administrative privilege class.

Advanced Program-to-Program Communication (APPC)
An implementation of the SNA LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

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* and *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.

APPC See *Advanced Program-to-Program Communication*.

application client
A program that is installed on a system to protect an application. The Tivoli Storage Manager server provides backup services to an application client.

archive
To copy programs, data, or files to other storage media, usually for long-term storage or security. Contrast with *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.

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
(1) 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.

(2) 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.

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
The process of checking a user's password before permitting user access to the Tivoli Storage Manager server. Authentication can be turned on or off by an administrator with system privilege.

authentication rule
A specification that another user can use to either restore or retrieve files from storage.

authority
The right to access objects, resources, or functions. See also *privilege class*.

authorization rule
A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user
A user who has administrative authority for the Tivoli Storage Manager 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 *threshold migration* and *demand migration*.

automatic reconciliation
The process that is used to reconcile file systems at regular intervals. The intervals are set by a user with root user authority. See also *reconciliation*.

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. Contrast with *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.

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 server storage. More than one backup version can exist in server storage, but only one backup version is the active version. See also *active version* and *inactive version*.

bind To associate all versions of a file with a management class name. See *rebind*.

bindery
A database that consists of three system files for a NetWare server. The files contain user IDs and user restrictions.

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*.

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 *client schedule* and *administrative command schedule*.

client A software program or computer that requests services from a server.

client acceptor
An HTTP service that serves the 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, and is also called the *client acceptor daemon* (CAD).

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. Contrast with *administrative session*.

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 option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client-polling scheduling mode
A method of operation in which the client queries the server for work. Contrast with *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*.

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. This file is also called the dsm.sys file. See also *client user-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*.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. Contrast with *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 consistent.

Common Programming Interface for Communications (CPI-C)
A call-level interface that provides a consistent application programming interface (API) for applications that use program-to-program communications. CPI-C uses LU 6.2 architecture to create a set of interprogram services that can establish and end a conversation, send and receive data, exchange control information, and notify a partner program of errors.

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, or strings of characters from the data being processed and replaces the repetitive characters with control characters. Compression reduces the amount of storage space that is required for the 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 *managed server* and *profile*.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction.

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*, and *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 *primary storage pool* and *destination*.

CPI-C See *Common Programming Interface for Communications*.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which Tivoli Storage Manager has detected read errors.

data access control mode
A mode that controls whether a command can access a migrated file, see a migrated file as zero-length, or receive an input/output error if it attempts to access a migrated file. See also *execution mode*.

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.

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*. Contrast with *full backup*.

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.

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.

deduplication
See *data deduplication.*

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.

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.

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 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.

(2) 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.

device driver
A program that provides an interface between a specific device and the application program that uses the device.

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 recovery 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 *policy domain* or *client domain*.

DRM See *disaster recovery manager*.

DSMAPI
See *data storage-management application-programming interface*.

dynamic serialization
A type of 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.

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*, and *subscription*.

enterprise logging
The process of sending events from a Tivoli Storage Manager 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 (1) An administrative command or a client operation that is scheduled to be run using Tivoli Storage Manager scheduling.

(2) A message that an Tivoli Storage Manager server or client issues. Messages can be logged using Tivoli Storage Manager event logging.

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 storage, real and virtual storage, and channel volume, 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 and space management, backup only, or space management only.

exclude-include list
See *include-exclude list*.

execution mode
A mode that controls the space-management related behavior of commands that run under the **dsmmode** command.

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.

extent The part of a file that is created during the data-deduplication process. Extents are compared with other file extents to identify duplicates.

external library
A type of library that is provided by Tivoli Storage Manager that permits LAN-free data movement for StorageTek libraries that are managed by Automated Cartridge System Library Software (ACSLS). To activate this function, the Tivoli Storage Manager library type must be EXTERNAL.

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 *resident file*, *premigrated file*, and *migrated 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* and *incremental backup*. Contrast with *database snapshot*.

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. See also *backup version* and *archive copy*.

G

General Parallel File System
A high-performance shared-disk file system that can provide data access from nodes in a cluster environment.

gigabyte (GB)
In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

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. When

space management is globally deactivated, hierarchical storage management (HSM) cannot perform migration, recall, or reconciliation. However, a root user can update space management settings and add space management to additional file systems. Users can access resident and premigrated files.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system.

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.

hierarchical storage management (HSM) client
A client program that works with the Tivoli Storage Manager server to provide hierarchical storage management (HSM) for a system. See also *hierarchical storage management* and *space manager client*.

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. Contrast with *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. Contrast with *active 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.

incremental backup
(1) A copy of all database data that has changed since the most recent successful full backup operation. An incremental backup is also known as a *cumulative backup image* because each incremental backup includes the contents of the previous incremental backup.

(2) The process of backing up information in the database that is new or changed since the last full backup. Contrast with *full backup*. See also *database backup series*.

(3) For Data Protection for Microsoft Exchange Server, a backup in which the transaction logs are backed up and then cleared.

individual mailbox restore
See *mailbox restore*.

information lifecycle management (ILM)
GPFS policy-based file management for storage pools and file sets.

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 IP 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.

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

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 210 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. This process is also referred to as *LAN-free data transfer*.

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.

(2) For HSM products, pertaining to the destination of migrated files that are being moved.

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 volumes
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* and *physical file*.

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.

logical unit (LU)
An access point through which a user or application program accesses the Systems Network Architecture (SNA) network to communicate with another user or application program.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier that is 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 backup 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.

LU See *logical unit*.

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. Contrast with *Tivoli Storage Manager 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
In Tivoli Storage Manager, 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. In general, a managed object cannot be modified locally on the managed server. Objects can include policy, schedules, client option sets, server scripts, administrator registrations, server definitions, and server group definitions.

managed server
A Tivoli Storage Manager 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*, *subscription*, and *profile*.

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 *copy group*, *space manager client*, *bind*, and *rebind*.

maximum transmission unit
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 Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)
(1) 1 048 576 bytes (2 to the 20th power) when used in this publication.

(2) For processor storage, real and virtual storage, and channel volume, 2 to the power of 20 or 1 048 576 bits. For disk storage capacity and communications volume, 1 000 000 bits.

metadata
Data that describes the characteristics of data; descriptive data.

migrate
To move data from one storage location to another. In Tivoli Storage Manager products, migrating can mean moving data from a client node to server storage, or moving data from one storage pool to the next storage pool defined in the server storage hierarchy. In both cases the movement is controlled by policy, such as thresholds that are set. See also *migration threshold*.

migrated file
A file that has been copied from a local file system to Tivoli Storage Manager 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 *stub file* and *resident file*. For HSM clients on UNIX or Linux systems, contrast with *premigrated file*.

migrate-on-close recall mode
A mode that causes a migrated file to be recalled back to its originating file system temporarily. Contrast with *normal recall mode* and *read-without-recall recall mode*.

migration job
A specification of files to migrate, and actions to perform on the original files after migration. See also *job file*.

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 locations at the same time. Mirroring data protects against data loss 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 *modified mode* and *absolute 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*.

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
On the Tivoli Storage Manager server, a logical drive through which volumes in a sequential access device class are accessed. For removable-media device types, such as tape, a mount point is a logical drive that is associated with a physical drive. For the file device type, a mount point is a logical drive that is associated with an I/O stream. The number of mount points for a device class is defined by the value of the mount limit attribute for that device class. 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 See *network-attached storage*.

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 Tivoli Storage Manager server. Contrast with *non-native data format*.

NDMP
See *Network Data Management Protocol*.

NetBIOS
See *Network Basic Input/Output System*.

network-attached storage (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 (NetBIOS)
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 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.

normal recall mode
A mode that causes a migrated file to be copied back to its originating file system when it is accessed.

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. Contrast with *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. On Windows and NetWare systems, the file is called dsm.opt. On AIX, UNIX, Linux, and Mac OS X systems, the file is called dsm.sys.

originating file system
The file system from which a file was migrated. When a file is recalled using normal or migrate-on-close recall mode, it is always returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the Tivoli Storage Manager 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.

out-of-space protection mode
A mode that controls whether the program intercepts out-of-space conditions. See also *execution mode*.

P

pacing
In SNA, a technique by which the receiving system controls the rate of transmission of the sending system to prevent overrun.

packet In data communication, a sequence of binary digits, including data and control signals, that is 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. Password generation can be set in the options file (`passwordaccess` option). See also *options file*.

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* and *logical file*.

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 *physical file*, *logical file*, and *logical occupancy*.

plug-in
A self-contained software component that modifies (adds, or changes) the function in a particular system. When a plug-in is added to a system, the foundation of the original system remains intact.

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.

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* and *management class*.

premigrated file
A file that has been copied to Tivoli Storage Manager 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 Tivoli Storage Manager storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. Contrast with *migrated file* and *resident file*.

premigrated files database
A database that contains information about each file that has been premigrated to Tivoli Storage Manager storage. The database is stored in a hidden directory named `.SpaceMan` in each file system to which space management has been added.

premigration
The process of copying files that are eligible for migration to Tivoli Storage Manager 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 *destination* and *copy storage pool*.

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 *node privilege class*, *operator privilege class*, *policy privilege class*, *storage privilege class*, and *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* and *managed server*.

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.

read-without-recall recall mode
A mode that causes hierarchical storage management (HSM) to read a migrated file from storage without storing it back on the local file system. The last piece of information read from the file is stored in a buffer in memory on the local file system. Contrast with *normal recall mode* and *migrate-on-close recall mode*.

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*.

recall In Tivoli Storage Manager, to copy a migrated file from server storage back to its originating file system using the space management client. See also *transparent recall*, *selective recall*, and *recall mode*.

recall mode
A mode that is assigned to a migrated file with the **dsmattr** command that determines how the file is processed when it is recalled. It determines whether the file is stored on the local file system, is migrated back to Tivoli Storage Manager storage when it is closed, or is read from Tivoli Storage Manager storage without storing it on the local file system.

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 Tivoli Storage Manager 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 synchronizing a file system with the Tivoli Storage Manager server, and then removing old and obsolete objects from the Tivoli Storage Manager server.

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
(1) Pertaining to a system, program, or device that is accessed through a communication line.

(2) For HSM products, pertaining to the origin of migrated files that are being moved.

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 Tivoli Storage Manager 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 Tivoli Storage Manager storage and modified. Contrast with *stub file* and *premigrated file*. See *migrated file*.

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.

roll back
To remove changes that were made to database files since the last commit point.

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 *administrative command schedule* and *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.

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. Contrast with *Tivoli Storage Manager 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. Contrast with *incremental backup*.

selective migration
The process of copying user-selected files from a local file system to Tivoli Storage Manager storage and replacing the files with stub files on the local file system. Contrast with *threshold migration* and *demand migration*.

selective recall
The process of copying user-selected files from Tivoli Storage Manager storage to a local file system. Contrast with *transparent recall*.

serialization
The process of handling files that are modified during backup or archive processing. See *dynamic serialization*, *static serialization*, *shared static serialization*, and *shared dynamic serialization*.

server A software program or a computer that provides services to other software programs or other computers.

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. Contrast with *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 space manager client nodes (space-managed files). See also *active-data pool*, *primary storage pool*, *copy storage pool*, *storage pool volume*, and *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.

session resource usage
The amount of wait time, processor time, and space that is used or retrieved during a client session.

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. Tivoli Storage Manager retries the backup or archive operation a number of times; if the file is being modified during each attempt, Tivoli Storage Manager will back up or archive the file on its last try. See also *serialization*. Contrast with *dynamic serialization*, *shared static serialization*, and *static serialization*.

shared library
A library device that is used by multiple storage manager servers.

shared static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. Tivoli Storage Manager 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 *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *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 space manager client. The space manager client recalls the file to the client node on demand.

space management
The process of keeping sufficient free storage space available on a local file system for new data by migrating files to server storage. Synonymous with *hierarchical storage management*.

space manager client
A program that runs on a UNIX or Linux system to manage free space on the local file system by migrating files to server storage. The program can recall the files either automatically or selectively. Also called *hierarchical storage management (HSM) client*.

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. Each stanza is identified by a name that occurs in the first line of the stanza. Depending on the type of file, a stanza is ended by the next occurrence of a stanza name in the file, or by an explicit end-of-stanza marker. A stanza can also be ended by the end of the file.

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 storage manager cannot back up or archive the file. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *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 that is tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
(1) 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*.

(2) An arrangement of storage devices with different speeds and capacities. The levels of the storage hierarchy include: main storage, such as memory and direct-access storage device (DASD) cache; primary storage (DASD containing user-accessible data); migration level 1 (DASD containing data in a space-saving format); and migration level 2 (tape cartridges containing data in a space-saving format).

storage pool
A named set of storage volumes that are the destination that is used to store client data. A storage pool contains backup versions, archive copies, and files that are migrated from space manager client nodes. A primary storage pool is backed up to a copy storage pool. See also *primary storage pool*, *copy storage pool*, and *active-data pool*.

storage pool volume
A volume that has been assigned to a storage pool. See also *volume*, *active-data pool*, *copy storage pool*, and *primary storage pool*.

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 Tivoli Storage Manager storage. It also contains additional information that can be used to eliminate the need to recall a migrated 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 Tivoli Storage Manager 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 Tivoli environment, the process of identifying the subscribers that the profiles are distributed to. For Tivoli Storage Manager, a subscription is the process by which a managed server receives configuration information associated with a particular profile on a configuration manager. See also *managed server*, *configuration manager*, and *profile*.

system privilege class
A privilege class that gives an administrator the authority to issue all server commands. See also *privilege class*.

Systems Network Architecture (SNA)
The description of the logical structure, formats, protocols, and operational sequences for transmitting information through and controlling the configuration and operation of networks.

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 Tivoli Storage Manager storage based on the high and low thresholds that are defined for the file system. Contrast with *demand migration*, *selective migration*, and *migration job*.

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.

timestamp control mode
A mode that determines whether commands preserve the access time for a file or set it to the current time.

Tivoli Storage Manager command script
A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic.

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.

transparent recall
The process that is used to automatically recall a file to a workstation or file server when the file is accessed. See also *recall mode*. Contrast with *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 name*.

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 some classical and historical texts. The Unicode standard has a 16-bit character set defined by ISO 10646.

Unicode-enabled file space
Unicode file space names provide support for multilingual workstations without regard for the current locale.

Unicode transformation format 8
Unicode Transformation Format (UTF), 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.

Universal Naming Convention (UNC) name
A name that is used to access a drive or directory containing files shared across a network. The UNC name includes the system name and a SharePoint name that represents the shared drive or directory.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier.

UTF-8 See *Unicode transformation format 8*.

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 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*, and *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
A set of Microsoft application-programming interfaces (APIs) that you can use 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 Tivoli Storage Manager server storage.

VSS Fast 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 local shadow volumes.

VSS Instant Restore
A volume-level hardware-assisted Microsoft Volume Shadow Copy Service (VSS) function where target volumes that contain the snapshot are copied back to the original source volumes.

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 Tivoli Storage Manager 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 Tivoli Storage Manager 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.

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
A 64-bit, unsigned name identifier that is unique.

workload partition (WPAR)
A partition within a single operating system instance.

Product Number: 5724-Y96

Printed in USA

SC27-2808-02