Chapter 8 Managing Resources

Overview

This chapter describes how to:

- Manage your Protected Resource List
- Add and delete resources
- Upgrade TSAs by renaming resources
- Manage databases
- Re-arrange the Protected Resource List

Contents

Introduction

From Resource Manager you can back up all eligible files on a resource. You can perform restore operations on an entire resource or its File History Database, directory structure, or data. See Chapter 5, “Backing Up Data,” and Chapter 6, “Restoring Data,” for more information about these operations.

The Resource Manager's protected resource tree displays items currently protected by your Backup

Director installation. You can organize the protected resources using three different criteria.

To select a view of the Protected Resource List

> From Resource Manager, open the *View* menu and select one of the three tree views:

Sort by Target Service—The default view of the protected resource tree. The resources are organized by the target service to which they belong.

Sort by Type—The resources are organized by the type of resource they are. For example, workstations are grouped together, NetWare servers and their resources are grouped together.

Sort by Location—The resources are organized by the SMDR they communicate with.

From any of these views, you can perform backup, database maintenance, or restore operations on any protected resource.

To update the tree view and information tabs

> Open the Operations menu and select *Refresh the Tree*. The program will update any changes that have been made to the protected resources and/or information on the latest operation performed on the resources. Backup Director does not automatically reflect the most recent operations completed on the various resources.

See Appendix D, “Viewing Installation Information,” for descriptions of each parameter in the information tabs.

Resource Manager Tool Bar

The Resource Manager tool bar provides a short cut to commonly used operations:

Automatic job—Submit an automatic job for processing as soon as possible.

Backup—Perform a backup operation on the selected resource(s).

Restore—Perform a complete restore operation on selected resource. A complete restore consists of the resource's history database, directory structure, and data.

Add Resource—Add a resource located on the server or installation to the Protected Resource List.

Remove Resource—Remove the selected resource(s) from the Protected Resource List.

Help—View on-line help for Resource Manager.

Managing Your Protected Resources

Your storage management strategy is based on automatic operations backing up all active protected resources. Therefore, it is important to add, delete, and re-arrange your protected resources as your current data protection requirements change.

Resource Summary Report

The Resource Summary includes selected parameters from the information tabs. You may want to print this report if you:

- Have an extensive Protected Resource List that does not fit on the screen.
- Want to compare information for different resources.
- Want to fax a copy of your Protected Resource List to a Palindrome Technical Support representative who is helping you with a problem.

The Resource Summary report displays all of the maintain your protected resources is available in Console Manager on the Reports tab.

See chapter 7 for instructions on viewing and printing the Resource Summary report.

Adding Resources

Whether you are adding a server volume, workstation volume, NetWare Directory Services, etc., you must load the appropriate TSAs and related communications software before you add the resource to Resource Manager. Use the server preparation diskette to copy the appropriate TSAs to each server. When you installed Backup Director, the program automatically loaded the appropriate TSAs for your installation server. See the *Installation Guide* for detailed information about TSAs.

During an automatic job, Backup Director processes the protected resources in the order in which the resources appear in the Protected Resource List (see the Resource Sequence for Automatic Operations dialog box).

The resource at the top of the list is backed up first, the second resource is backed up next, etc. If you are backing up resources concurrently, this is the order in which the program assigns resources to available engines or devices.

Once you add a resource to the list, the Resource Manager displays the capacity of the resource and its File History Database location. The File History Database is created in your installation directory (the default) or the location you specify using Operations/*History Database Location*. If you are upgrading an existing installation, you should have already added protected resources and translated File History Databases during the installation process. See the *Installation Guide* for details regarding the *Translate History Database* menu option.

Use the following procedure to add one or more resources on an unprotected server.

To add a server

1. Highlight the installation icon on the protected resources tree.

2. Open the Operations menu and select *Add Resource*. The Choose a Server/SMDR dialog box appears with a list of servers that have TSAs loaded. The server and SMDR are almost always the same entity.

3. Click the server with the resource you want to add. The Choose a Target Service Agent dialog box appears. This dialog box displays a list of all the TSAs loaded on the server.

4. Select a TSA that is appropriate for the resource you want to add and choose **OK**. The Choose a Target Service dialog box appears. It displays a list of target services on the selected server.

5. Select the target service and choose **OK**. The Choose a Resource dialog box appears. It displays all of the resources on the selected server that are not already on the protected resource tree.

6. Select the resources you want to add.

TIP: Use <**Ctrl**> key-click to tag or select multiple items in a list or eligible tree. Use <**Shift**> key-click to define a range of items in a list or eligible tree.

7. Choose **OK**. The resource appears on the protected resource tree.

Use the following procedure to add one or more resources on a protected server.

To add a volume resource

1. Highlight the protected target service.

2. Open the Operations menu and select *Add Resource*. If there are multiple TSAs loaded on the target service, you must choose a TSA.

3. Choose one or more available resources from the Choose a Resource dialog box.

Use the following procedure to add a local drive to a protected workstation.

To add a local drive

1. Highlight the workstation target service.

2. Open the Operations menu and select *Add Resource*.

3. Choose the local drive from the Choose a Resource dialog box.

4. Choose **OK**.

De-activating a Resource

When you de-activate a resource, Backup Director excludes this resource from automatic jobs. However, the resource is still available for custom jobs because the File History Database has only been excluded from automatic jobs.

There are a two main reasons for de-activating a resource:

- You want to perform maintenance on a downed resource.
- You are experiencing problems with a resource during backups and you want to troubleshoot the problem.

Only Resource Manager and the Resource Summary report indicate which resources are excluded from automatic operations.

To temporarily exclude a resource from automatic jobs

1. On the protected resource tree, highlight the resource you want to de-activate.

2. Open the Operations menu and select *Edit Resource Info*. The Edit Protected Resource Attributes dialog box appears.

3. Turn off the **Included for Automatic Operations** option.

4. Choose **OK** to save your change. The Configure tab displays the change you made. The Resource Sequence for Automatic Operations dialog box also indicates which resources have

been included in automatic operations.

Removing a Resource

Removing the resource automatically excludes the resource from future operations. Usually, you'll remove a resource only when you no longer wish to protect it. If you think you may add the resource later, you have the option of keeping the File History Database.

> **WARNING:** Do not remove a resource and its File History Database if you intend to add it to Resource Manager at a later time. You will delete records of previous file versions and other session information that you may need for a restore operation.

To remove a resource

1. Highlight a resource.

2. Open the Operations menu and select *Remove Resource*. A prompt appears.

3. Choose **Yes** to confirm the removal of the resource and its database, if applicable. The resource no longer appears on the protected resource tree.

To remove a server

> Highlight each of the server's resources and delete these one by one. When all resources are deleted, the server is removed from the tree.

Re-arranging Resources

When you re-arrange resources, you are changing the order in which Backup Director performs automatic operations on the protected resources. There are a few reasons why you may want to re-arrange resources after you have installed or added resources:

- You suspect that a certain resource causes your operation to fail. By moving this resource to the last position, the program will have already protected the data of the other resources prior to failing on the problematic resource.
- You want to improve the efficiency of concurrent backup operations.

To re-arrange the sequence of resources for automatic jobs

1. Open the Operations menu and choose the *Change Sequence* menu option. The Resource Sequence for Automatic Operations dialog box appears; it displays the Protected Resource List.

2. Highlight the resource and choose the appropriate button. The **Up** and **Down** buttons move the highlighted resource one position from the resource's original position. The **Top** button moves the resource to the first position and the **Bottom** button moves the resource to the last position on the Resource Sequence for Automatic Operations dialog box.

   > Move the larger resources to the top of the list so that these resources complete at approximately the same time. When processing automatic operations,the program completes database maintenance operations on all resources before starting backup operations.

   > Separate workstation resources from the same workstation on the list. For example, if the last two resources are a C: and D: drive for the same workstation, the

program cannot process these concurrently.

3. Choose **OK** to save the new sequence.

Configuring Tracking Name Space

Backup Director allows you to configure the name space that it will use to track each resource. This is the name space that appears when viewing files within the user interface and the name space stored in the File History Database. Backup Director determines a default name space for volumes with multiple name spaces loaded.

When Backup Director encounters multiple name spaces, it prioritizes them in the following order:

1. OS/2

2. MAC

3. NFS

4. FTAM

5. DOS

For example, if you have the OS/2 and DOS name spaces loaded on this resource, Backup Director defaults to OS/2. Backup Director tries to take advantage of name spaces that allow longer names first. Files with longer names will most likely have their real names displayed as opposed to displaying them in a DOS name space which limits the file to eight characters (excluding the extension).

If you have only one name space loaded on a resource, Backup Director will use the loaded name space. Generally, you will not want to change the tracking name space unless you've removed the current tracking name space from the volume.

If you have multiple name spaces loaded, you can specify which name space you want Backup Director to use for this resource before running your first backup.

Changing Name Spaces

Once you have backed up a resource, Palindrome recommends that you **do not** change the tracked name space. Modifying the name space after a resource has been backed up can change the resource's history information.

Also, if you change the default name space, be sure the file rules in effect for the resource apply to your new tracked name space. If you remove a name space from a resource, you may want to change the name space tracking to a parameter other than the default.

If you select a case-sensitive name space to track a resource in (such as NFS), Backup Director will not allow you to change it to a name space that does not support case-sensitivity (such as DOS).

Changing name spaces in this manner would cause duplicate directory and file entries in the File History Database. If you must change from a case-sensitive name space, contact Palindrome Technical Support.

To change the tracking name space

1. From the protected resource tree, highlight the resource you want to configure.

2. Open the Operations menu and choose *Edit Resource Info*. The Edit Protected Resource Attributes dialog box appears.

3. Click the **Change Tracking Name Space** button. The list of name spaces available on the highlighted resource appears.

4. Click the name space you want to use from the list of available name spaces.

5. Choose **OK**. The selected name space now appears in the **Tracking Name Space** field.

6. Choose **OK** to close the dialog box.

Renaming a Resource

There are two reasons why you may need to rename a resource:

- The resource's Protected Resource Name, which includes the loaded TSA, has changed.

For example, if you upgraded from a Palindrome installation with pre-1994 TSAs, you would have observed the following system message:

PLSM-53 There are no Target Service Agents that match the <<ServerName>> pattern.

The problem occurs because the System Control Database still refers to the name of the former version of the Novell TSA (for example, “NetWare 3.11 File System”), which was in use when you last added the resource. The program does not recognize the name of the new TSA (“NetWare File System”).

- You recover a downed volume by redirecting it to a target volume and you rename it with the source volume name. By renaming the volume, you ensure continuity between the pre- and post-recovery File History Databases for the redirected data.

To rename a resource

1. In NetWare, change the name of the resource.

   > If the resource you are renaming is a workstation, you must change the name of the workstation in the configuration file first. See “*Editing the Workstation's Configuration Files*” section below.

2. Highlight the resource you want to rename.

3. Open the Operations menu and select *Edit Resource Info*. The Edit Protected Resource Attributes dialog box appears.

4. Choose the **Change Protected Resource Name** button. The SMS Target dialog box appears.

5. Specify the resource's server, the current TSA, the target service, and the resource.

6. Choose **OK** to save the name change.

Editing the Workstation's Configuration Files

To change the name of a DOS workstation

1. Unload TSADOS.NLM and WSMAN.NLM from the server that TSASMS.COM connects to.

2. Unload TSASMS.COM from the workstation.

3. Edit the workstation's NET.CFG file to reflect the new workstation name.

   NOTE: Be sure that the workstation is logged on when you name the resource in Resource Manager.

4. Load TSASMS.COM on the workstation.

To change the name of a protected OS/2 workstation

1. Edit the TSAOS2.CFG file on the workstation. Below is an example of what your TSAOS2.CFG may look like and an example of each parameter. Note that the TSAOS2.CFG file is not case-sensitive.

2. Save this file to the directory where TSAOS2.EXE is located (usually \NETWARE).

For more information on Target Service Agents, see the *Installation Guide.*

Changing Passwords

If you change a workstation's password, be sure to define the new password in Resource Manager so that the program can automatically open the workstation during operations.

To change a password

1. Highlight the workstation (target service).

2. Open the Operations menu and select *Edit Resource Info* . The Edit Protected Resource Attributes dialog box appears.

3. Choose the **Edit Login User** button.

4. Enter the password. Choose **OK** to save the new password and choose **OK** to close the dialog box.

Maintaining Databases

Backup Director automatically performs complete database maintenance operations at every rotation operation. Between rotation days, you may want to perform certain maintenance operations.

The **Check for Deleted Files** option ensures that deliberately deleted directories and files are not automatically restored if the volume needs to be recovered. Since the program performs this operation automatically on every rotation day, you do not have to initiate this operation.

The **Verify** option compares the File History Database against the System Control Database and corrects any minor discrepancies between the databases. The database verification also includes updating the status of media, such as recording retired and forgotten media. As a result, this option updates the file versions displayed in the History and Extended History windows.

Checking for Deleted Files

Perform this operation to avoid restoring deleted files if the resource crashes before the next rotation day.

> **WARNING:** Do not check for deleted files when you are in the process of recovering a resource. If you run this operation after you have restored the File History Database, but before you have recovered the data, the database will not be able to restore the data because the files have been marked as deleted.

To update deleted file records in the File History Database

1. Tag the resource with the File History Database you want to check. You can tag multiple resources.

2. Open the Operations menu and select *History Database Maintenance*. The Database Maintenance Options dialog box appears.

3. Select **Check for Deleted Files** to update media records in the File History Database.

4. Select any other job parameters.

5. Choose **OK** to submit the job to the job queue.

> **TIP:** After submitting a maintenance job, remember to close the job status window as soon as you are satisfied that the job is running smoothly. In most cases, leaving a job status window open increases the time required to perform the operation.

Verifying the File History Database

There are two reasons for performing this operation:

- You suspect a resource's File History Database is corrupt. In most cases, the program prompts you to perform a database verification through a system message. You can select this option to recover a copy of the File History Database following a recovery error.
- You have performed a retire or forget operation and want to update the status records immediately.

To verify the File History Database

1. Tag the resource(s) whose database(s) you want to verify.

2. Open the Operations menu and select *History Database Maintenance*. The Database Maintenance dialog box appears.

3. Select **Verify**.

4. Select any other job parameters

5. Choose **OK** to submit the job to the job queue.

6. View the database verification report. Every database verification job generates this report. This report is a file which is attached to a system message in the System Message window.

> > If the program determines that the File History Database is corrupt, a system message will indicate that you need to restore it. See chapter 6 for information about restoring an entire resource.

Configuring File History Database Locations

By default, Backup Director places a File History Database in the Backup Director installation directory for each resource you add to Resource Manager. This is known as the central location.

An alternative is to distribute the databases. Instead of placing a new resource's File History Database on the installation volume, Backup Director attempts to store the File History Database of newly added resources on another volume resource. You can specify each new resource as the default location. File History Databases for workstation and non-volume resources are always stored in the central location.

The benefits of centralizing databases on a single location are:

- You can easily locate File History Databases.
- If a volume is down, you can redirect restored data to another volume.
- Backup Director can access the File History Databases more quickly if the databases are on the installation server/volume.

The benefits of distributed databases are:

- You can minimize the amount of disk space required to maintain File History Databases on your installation server.
- The risk of simultaneously losing access to all File History Databases is reduced. If one volume goes down, the other protected volumes still have their File History Databases available.

NOTE: Changing the default File History Database location only affects resources that you add in the future. Existing File History Databases are not affected. If you want existing File History Databases at the new default location, you must move the databases individually.

To change the default File History Database location

1. From Resource Manager, open the Operations menu and select *History Database Location*. The History Database Location dialog box appears.

2. Select the new database location for new resources.

> To centralize the databases of new resources on a single volume, select **Always on the default SERVER/VOLUME**. Choose the **Configure** button to choose a the new server/volume location.

> To place each File History Database on its volume resource, select **On the Protected Resource when Possible**. Backup Director automatically places the File History Databases of non-volume resources on the default server/volume. The original default location still appears because this is the location where new non-volume resources will reside.

Moving File History Databases

You may want to relocate a File History Database(s):

- If you have them centralized on a server and you know the server is going to be off-line.
- If a volume's disk space is decreasing and you want to store its File History Database elsewhere.

Before relocating databases, verify that the new server has the required TSAs loaded, otherwise Backup Director will not be able to access the File History Database.

To move a File History Database

1. Highlight the resource whose File History Database you want to move.

2. Open the Operations menu and select the *Edit Resource Info* option. The Edit Protected Resource Attributes dialog box appears.

3. Choose the **Change History Database Location** button. The Choose a Server dialog box appears.

4. Select a server. The Choose a Resource dialog box appears.

5. Select the resource that you want to move the database to (the target resource).

6. If the target resource has a File History Database, you can abort the procedure or overwrite the existing File History Database.

7. If the target resource already has a File History Database for the source resource, you have the additional option of using the existing version of the database on the target resource.

_____