Yosemite Server Backup
User's Guide

Part number:
First edition: October 2010

Legal and notice information

Notice

Information in this document is subject to change without notice. Barracuda Networks, Inc. makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Barracuda Networks, Inc. reserves the right to revise this publication and to make changes without obligation to notify any person or organization of such revisions or changes.

Trademarks

Yosemite Server Backup is a trademark of Barracuda Networks, Inc..

Windows™ and Windows NT™ are registered trademarks of Microsoft Corporation.

Contents

Figures

Tables

Before you begin

Customer Support

Phone and Email Technical Support offered 24 x 7. Basic Support includes email and live chat support 24x7 and phone support between the hours of 9am and 5pm Monday through Friday in the USA (Pacific time zone). Enhanced Support provides 24x7 phone support. You can get customer support for Yosemite Server Backup in one of the following ways:

- Visit our website at http://www.barracudaware.com
- Phone us at +1 408 342 5300.
- Email us at support@barracuda.com.

Release Notes

Release notes are included with every release and service pack. Before using Yosemite Server Backup, please read the release notes for additional information. The release notes are available in HTML format in the root directory of the Yosemite Server Backup CD-ROM.

Document Conventions and Symbols

Convention	Element
Blue text: Document Conventions and Symbols	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.website.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables

⚠ **WARNING!**

Indicates that failure to follow directions could result in data loss.

△ **CAUTION:**

Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT:

Provides clarifying information or specific instructions.

NOTE:

Provides additional information.

TIP:

Provides helpful hints and shortcuts.

1 Overview

In this chapter

- Concepts
- A Simple, Immediate Backup
- Restore to a Different Location

⚠ **WARNING!**

Yosemite Server Backup security is disabled at installation to simplify the evaluation process. When installing the product in a production environment we recommend, at a minimum, that you set a user password for the Admin user. Doing so will result in the Administrator prompting the user for a password before starting. See Setting a User Password for details.

Concepts

Yosemite Server Backup is designed to operate within your existing network to protect your vital data. Each *machine* that will be protected must have Yosemite Server Backup installed. One machine acts as the Domain Server which houses the *catalog* and establishes a Backup Domain. Other machines become *clients* of the Backup Domain by identifying themselves as clients of the Domain Server during installation.

Yosemite Server Backup can back up data from clients over a network to a backup device attached to a remote machine. A client with an attached device acts as a *Media Server*.

When a machine is being backed up or restored it is operating the client role. When it is providing access to a backup device it is operating as a Media Server. And when a machine is hosting the catalog it is operating as the Domain Server. A single machine can operate in one or more roles at the same time.

Data on client machines is read and written with *agents* such as the File System, Windows System State, Microsoft SQL, and Microsoft Exchange agents. The configuration of agents is done on a client by client basis.

A typical installation of Yosemite Server Backup may look like Figure 1 below.

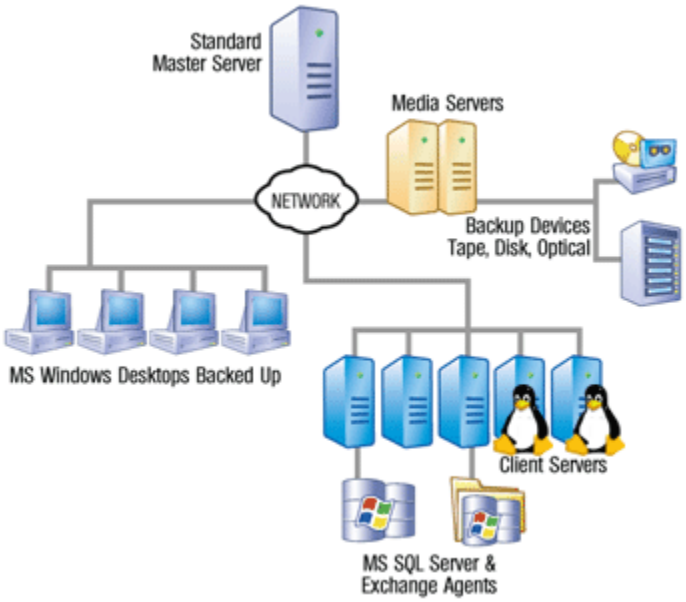

Figure 1 Basic Architecture

Terminology

The following terminology is used throughout this document ...

- *Clients*— A client is any computer (or *Machine*) in the Backup Domain other than the Domain Server. This includes file servers, application servers, and user PCs (desktops and laptops). All client computers must have Yosemite Server Backup installed. For licensing purposes, clients are classified as being *server* or *workstation* class machines. All clients are considered to be server class clients unless they are running Windows XP, Vista, or Windows 7.
- *Backup Domain*— A Backup Domain is a collection of computers and backup devices that is managed together as a group. A Backup Domain can encompass an entire company or each department could be a separate domain, even though they are all on the same network. All resources in a Backup Domain can be accessed by all members of the Backup Domain and centrally managed from a single Yosemite Server Backup interface. Each file server, application server, user PC, and attached peripherals such as backup devices can be the member of only one Backup Domain. Each Backup Domain has one and only one Domain Server.

NOTE:

A Backup Domain is completely independent of any Windows Active Directory domain.

The Yosemite Server Backup administrator can administer more than one Backup Domain from a single computer. However, the Yosemite Server Backup interface cannot manage more than one Backup Domain at the same time. The administrator must log off of one Backup Domain and log into another.

- *Domain Server*— Each Backup Domain has one and only one Domain Server. The Domain Server is responsible for coordinating the backup activities of all other machines in the Backup Domain. All license information is also contained on the Domain Server.
- *Catalog*— A catalog is a special-purpose database that contains all the information about a Backup Domain. There is one and only one catalog for each Backup Domain. The catalog must reside on the Domain Server machine.
- *Job*— A job is an object stored in the catalog that represents the settings for a task the user has configured. Jobs come in one of four types: backup, restore, verify, and copy media.
- *Backup devices*— A backup device is any device to which files can be backed up. This includes tape drives, tape libraries, hard disks (as virtual tape libraries), and Network Attached Storage (NAS) appliances. Backup devices are attached to media servers. Each Backup Domain must have at least one backup device, such as a tape device, tape library, virtual library, or CD device. This backup device can belong to only one Backup Domain; it cannot be shared among multiple domains. However, a Backup Domain could have multiple backup devices.
- *Media Server*— A media server is any machine in the Backup Domain to which a backup device is attached. Any machine in the Backup Domain can act as a media server. There can be multiple media servers in a Backup Domain. The media server allows its attached backup devices to be shared by all the machines in the same Backup Domain
- *Media*— Backed up files are written to media. Media can be a physical tape or a virtual “tape” in a virtual tape library on a disk drive. Media cannot be used in another Backup Domain without importing the media into the other Backup Domain.
- *Media Rotation* — Rotations are a means of efficiently using you available media to maintain data history. When using a rotation your backups alternate among a set of multiple media, reusing older media when necessary. The type of media rotation you select is based on how often you want to back up your data, how long you want to retain the data, and the number of media you want to use.
- *Disaster Recovery* (DR) — Disaster Recovery is the process of restoring a machine that has suffered a catastrophic failure such as hardware failure or critical system data loss. The recovery process entails reformatting the affected system’s hard drive and restoring the operating system, system settings, applications, and data from a backup. This feature replaces the traditional tedious task of finding installation disks, installing operating systems and applications, patching them and restoring data with a simple restore process directly from backups.

- *Full System Recovery* — Full system recovery is the process of recovering all of the data on a machine. It differs from DR in that a full system recovery does not reformat the disks prior to restoring the data.

A Simple, Immediate Backup

We will do a simple backup of selected files to a local backup device. This will illustrate many of the backup features available in Yosemite Server Backup. For many organizations, a simple backup such as this may be all that is needed. Organizations with more complex needs can use this simple backup as a starting point for exploring the other capabilities of Yosemite Server Backup.

1. Make sure the device is powered up and insert a blank piece of media. You do not need to format the media. Yosemite Server Backup will do that, if necessary, when it runs the job.
2. Start the Administrator. The initial view will show a list of tasks to choose from. Double-click the **Backup** icon to start creating a backup job.
3. Enter a job name, such as "My First Backup" and click **OK**. The job name is simply a friendly name used to identify each job.
4. Now you are ready to select folders and files for backup. Navigate down the network, machine and file system to locate the files that you wish to back up. Check the box to select the files/folders to be backed up. By checking the box next to a folder we are selecting all its subfolders and the files in them.

TIP:

The top left section of the property page is called the Task bar. It shows the different configuration tasks available to fully configure a job. Default values are supplied for many of the configuration values so you don't have to visit all of them. Your current position is highlighted by a bold label.

5. Now you need to select your device for backup. Click on the **Devices** link in the Task bar.

   You can click on the **+** to the left of a device type (e.g., **Tape Devices**) to display all available devices of that type. If not already selected, select the device you want to use for this backup by clicking the associated checkbox. The Device View allows you to locate and select devices by type, regardless of where they are in the network. The Network view allows you to locate select devices on specific machines. Select a class of decide, like Tape Devices, will configure the job to use all tape devices available when the job runs even in the drive was not available when the job was created.
6. Click on the **Encryption** link in the Task bar if you want to change the default encryption or compression settings. By default, encryption is off and compression is on. For more information, see Chapter 7.

NOTE:

This option should be used with care. It requires an encryption passphrase. If you lose the passphrase, you will not be able to recover your data.

7. Click on the **Configuration** link to see the job settings, the media that the job will use and how the media will be formatted. For this example, accept the default settings. For more information on backup job options, see Configuration.
8. You may ignore the **Advanced** options for this example.
9. Click **OK** to complete the backup job configuration. Click **Yes** at the prompt to see the new job (command) in your `Home` folder.
10. Select the new job object and click the **Run** button on the Command bar to start the job. Hold the cursor over the Yosemite Server Backup icon (the Quick Access program) in the Windows System tray, normally in the bottom right corner of your screen. You can see that the job is running.

NOTE:

During execution of the job you may notice a flashing red button in the lower right portion of the screen. This indicates an that requires your intervention. Click the button to open the alert details and resolve the issue.

NOTE:

The Quick Access program is installed and available on all clients but it only runs automatically on the Domain Server.

11. The status of the job is visible in the lower left hand pane, the **Info bar**, of the Administrator. Alternately, click on the **Status and Logs** link in the top left hand area — the **Navigation bar**. For more detailed information click on **Status** in the **Command bar**. The job's property page will open and show the status of the running job.
12. It is a good practice to check the logs after a job runs to ensure that there were no problems. Click **Status and Logs** in the Navigation bar. Locate your job in the list, click on the **+** sign to expand the job and select the most recent run. The property pane will show the firs page of the job log. To see the entire log, click the **View Log** button in the Command bar.
13. Select the log entry for the backup job and double-click to open it. Scroll through the log to check that everything is OK. If the **Next** button is bold, there are additional pages to check. Click **Close** when you have finished reading the log.
14. You have now created and run your first tape backup job.

Once you have created your backup (or any) job, it can be quickly and easily located again in your `Home` folder.

NOTE:

With the settings in this tutorial, this job will overwrite the media when you run it again. If you do not wish this to happen, you need to select a **Write Mode** of **Append to all media** in the **Modes** section of the **Configuration** page.

Restore to a Different Location

We will do a simple restore of selected files from the backup media we created in the previous step. This will illustrate many of the restore features available in Yosemite Server Backup.

1. Make sure the device is powered up and insert the backup media into it.
2. Select **Tasks** in the **Navigation bar** and double click the **Restore** icon.
3. Enter a name for the restore job, such as "My First Restore" and click **OK**.
4. Now you are ready to select folders and files for restore.

   Navigate down the network, machine and file system to locate the files that you included in your first backup. In this view, only files and folders that have been backed up will appear. Check the box to select the files/folders to be restored. By checking the box next to a folder, we are selecting all its subfolders and the files in them.
5. For this first restore job, we want to restore the files to a different location. This will allow you to compare the original files with the restored files.

   To do this task, we need the move functionality. Click on the **Move** icon in the **Tool bar**.

We recommend that you create a new folder to hold the restored files. In the Select destination for move operation dialog, select the `C:` drive, click on the **New** command, enter a name for your newly restored folder and click **OK**.

Select the new folder as the destination for the move operation and click **OK**.

Your new folder is now visible under the `C:` drive. Expand the folder to see how the files will be visible after the restore job is finished. You can refine the restore selection by clicking in the boxes to select or deselect the required folders and files. Only the selected folders and files will be restored.

As you navigate the restore view you will see a list of file and folder versions at the bottom of the view. That list represents each backup that the selected object was backed up in. When multiple versions of a file have been backed up, they will appear in this list and can be selected. If you don't select an item in the version list, the most recently backed up version will be restored.

6. Select the device containing your backup. Click on the **Devices** link in the **Task bar** as in the configuration of the backup job.
7. You may ignore the **Configuration** and **Advanced** links for this example.
8. Click **OK** to complete the job configuration. Click **Yes** at the prompt to see the new job (command) in your `Home` folder.
9. Select the new job object and click the **Run** button on the Command bar to start the job. If you have installed the Quick Access Control, hold the cursor over the Yosemite Server Backup icon in the Windows System tray, normally in the bottom right corner of your screen. You can see that the job is running.

NOTE:

During execution of the job you may notice a flashing red button in the lower right portion of the screen. This indicates an that requires your intervention. Click the button to open the alert details and resolve the issue.

---

10. The status of the job is visible in the lower left hand pane, the **Info bar**, of the Administrator. Alternately, click on the **Status and Logs** link in the top left hand area — the **Navigation bar**. For more detailed information click on **Status** in the **Command bar**. The job's property page will open and show the status of the running job.
11. It is a good practice to check the logs after a job runs to ensure that there were no problems. Click **Status and Logs** in the Navigation bar. Locate your job in the list, click on the **+** sign to expand the job and select the most recent run. The property pane will show the first page of the job log. To see the entire log, click the **View Log** button in the Command bar.
12. Select the log entry for the restore job and double-click to open it. Scroll through the log to check that everything is OK. If the **Next** button is bold, there are additional pages to check. Click **Close** when you have finished reading the log.
13. You have now created and run your first restore job.

2 Administering Backup

In this chapter

- Using the Administrator
- Using Quick Access from Taskbar
- About the Yosemite Server Backup Service

The entire Backup Domain can be managed and monitored centrally. The Administrator is the primary interface for administering the Backup Domain. The program displays an icon in the system taskbar and gives you a quicker way to perform the most common administrative operations.

Using the Administrator

The Yosemite Server Backup Administrator is a graphical user interface that manages and monitors your backups. The Administrator can be run on any machine on the same network as the machines in the Backup Domain. All machines in the Backup Domain are managed centrally from the Administrator.

Main Window

The Administrator window consists of a...

1. *Menu bar* — The menu bar is located at the top of the screen and contains several menus that group together similar commands. To invoke a command from a menu, open the menu and then select a command.
2. *Command bar* — The command bar is a context sensitive set of command buttons running along the top of the window below the menu bar. As the selected object changes the commands in the command bar will change to reflect the current selection.
3. *Navigation Bar* — The navigation bar is located in the top section of the left hand column of the Administrator. It contains links to the major views of the product:
   a. *Tasks View* — this view contains shortcuts for creating jobs and other common tasks.
   b. *Jobs and Media View* — this view shows the User's Home folder which contains all of his configured jobs and the media associated with them as well as media that has been imported or formatted. From this view you can run the jobs, modify their settings, and view their logs.
   c. *Status and Logs View* — this view contains a listing tasks and jobs that have happened in the Backup Domain
   d. *Devices View* — this view provides a view of all the devices in the Backup Domain. To perform media operations like identifying or importing media, use this view to navigate to the device containing the media in question and select the command you want from the command bar.
   e. *Advanced / Catalog View—*
   f. *Advanced / Security View —*
   g. *Advanced / Report View —*
   h. *Advanced / Instructions View*
4. *Info bar* — the info bar contains a summary of the object's most important properties like current status. It also contains command and control links for runnable jobs.
5. *View Pane* — The main part of the screen is the detail area. The layout of this pane will vary based on the view selected from the navigation bar.
   a. *Object Layout* — with this layout, the view pane contains a set of objects displayed as large icons. This view typically contains command objects as in the case of the Tasks View or objects as in the case of the Advanced Security View.

b. *Object Detail Layout* — with this layout, the panel is divided into a top and bottom portion. The top portion contains a list of objects. The bottom contains detailed information relevant to the object selected in the top portion. An example of this layout is the Status and Logs View.

c. *Tree View Layout* — with this layout the panel is divided into a left and a right section. The left hand side contains a tree view showing an organizational folder hierarchy and the right side contains a list of objects in the currently selected folder. Examples of this layout are the Jobs and Media View and the Devices View.

6. *Status bar* — The Status bar displays the current user's name, the Backup Domain to which the user is logged in, and the name of the machine at which the user is working. An Alert button appears in the lower right corner of the status bar when alerts are generated. This button flashes when there is an issue that requires attention.

Property Pages

Every object in the Yosemite Server Backup catalog has a set of *property* pages associated with it. Use these property pages to modify settings for an object and to view logs, messages, diagnostics or information that Yosemite Server Backup generates.

Opening Property Pages

Displaying the property page of an object can be accomplished several ways:

- Select the object with the mouse or keyboard, and then click **Properties** on the Command task pane.
- Right-click the object to display a **context** menu, then select **Properties**.
- Select the object, and then select **Properties** from the **File** menu.
- With the object selected, type **Alt-Enter.**

TIP:

Opening the property page for an object will open a non-modal dialog. You can leave property pages open when you return to working in the main Yosemite Server Backup window and you can have several property pages open at once.

The Property window consists of a...

1. *Navigation bar* — The navigation bar is located in the top section of the left hand column of window. It contains links to the various groups of properties of the object.
2. *Info bar* — the info bar contains a summary of the object's most important properties like current status. It also contains command and control links for runnable jobs.
3. *Property pane* — the property pane contains the actual properties that belong to the property group selected by the navigation bar.
4. *Command bar* — the command bar runs along the bottom of the dialog and contains the buttons for committing or cancelling changes made to the object and for dismissing the dialog.

Missing Features

If an option is not listed on a screen, for example Disaster Recovery or the SQL Agent, it may be for one of the following reasons ...

- The evaluation license for the option has expired. Optional features are installed automatically when you install Yosemite Server Backup. Once the evaluation license expires, you can no longer use an optional feature without purchasing and installing a license.
- The option is not available in the edition of Yosemite Server Backup you have installed.

- An error occurred when starting Yosemite Server Backup. Review the alerts to see if an option failed to start properly when you started the application.

Using Quick Access from Taskbar

In this section

The Yosemite Server Backup Administrator is very powerful and allows access to all the features of Yosemite Server Backup. Typically, though, only a subset of these features are used. The Quick Access taskbar icon allows fast access to these most commonly used features without needing to open the Administrator. The Quick Access application displays an icon in the system tray, usually at the bottom right of the screen. You can mouse over the icon to display status information or right click it to display a menu.

The Quick Access starts automatically on the Domain Server. On other client machines, it is installed but does not start automatically. You can launch through the system start menu. It can also be configured to start automatically on a client machine if desired.

Viewing Yosemite Server Backup status

The appearance of the Quick Access icon changes to indicate the state of Yosemite Server Backup, thus providing continuous feedback. Two or more states can occur at the same time, such as a job in progress and a pending alert. The icon can indicate only one state at a time, so it follows this order of precedence in which items earlier in the list take precedence over items later in the list:

Table 1 Icon viewing status

Icon Overlay	Meaning
	Disconnected
	Job failure
	Pending alerts
	Job in progress
No overlay	Idle

When you mouse over the Quick Access icon, a tool tip is displayed that contains additional status information.

Managing Yosemite Server Backup

When you right-click the Quick Access icon, a menu is displayed.

Managing Jobs

Click the **Jobs** menu item to create a new job or to view a list of the jobs that you have currently defined. If there are more jobs that aren't displayed, **More** is displayed below the list. Click **More** to open the Administrator to the Jobs and Media View, which contains the jobs and folders that you have defined.

In the Settings window, you can set the maximum number of jobs that you see in the list.

Creating jobs

When you select the **New** menu item, you can create the following types of jobs:

Table 2 Creating jobs

Choice	Description
Backup	Create a job to back up files.
Restore	Create a job to restore specific files.
Verify	Create a job to compare a file on a PC or server to the backed-up versions of the file.

Monitoring jobs

For each job that you select, you can:

- View and change the job's properties
- View the job's status
- Run, pause, or stop the job, depending on the job's status

Managing Alerts

Click the **Alerts** menu item to view a list of unhandled Yosemite Server Backup alerts. If there are more alerts that aren't displayed, the **More** menu item is displayed below the list. Click **More** or the **Open Alerts Window** menu item to view all alerts. Selecting an alert will open a dialog with the alert details. Click the **Clear Evaluation Alerts** menu item to remove all alerts having to do with the use of an evaluation license.

In the Settings window, you can set the maximum number of alerts that you see in the list.

Managing Logs

Select the **Logs** menu item to view a list of recent logs. If there are more logs that aren't displayed, the **More** menu item is displayed below the list. Click **More** or the **Open Logs Window** menu item to view all logs.

The logs in the list can be from multiple jobs. The logs in the list are named using the date of the run and the name of the job. To view the logs for a specific job, go to the Yosemite Server Backup Administrator, open the job, and select the **Logs** page.

In the Settings window, you can set the maximum number of logs that you see in the list.

Settings

Click the **Settings** menu item to change the settings for the Quick Access taskbar icon or for the Yosemite Server Backup service.

Login information Use the **Hostname** field to change the Domain Server to use. Enter the hostname or IP address of the server. Use the **Hostname** field to change the Domain Server to use. Enter the hostname or IP address of the server.

Icon appearance The tray icon will show a flashing overlay in the following situations:

- When alerts are pending
- When a job is running

- When a job has failed.

Deselect the box for each situation which you do not want the Quick Access icon to flash.

Automatically start this application when the operating system starts Deselect this check box if you want to manually start the Quick Access application. To manually start the Quick Access application, switch to the Yosemite Server Backup installation directory, and run ytwingqa for Windows or ytlingqa for Linux. Or on Windows, select the Quick Access link from the start menu.

Automatically log in on startup Deselect this check box if you do not want to automatically log into the application, using the user name and password provided here. A logon window will appear at startup if this box is deselected.

Maximum number of menu items for Jobs, Alerts, or Logs submenus Select the maximum number of jobs, alerts, or logs that you want to see.

Service settings Use the Service Settings window to manage the Yosemite Server Backup service on the local machine. These settings have the same meaning as those found in the operating system's service manager program. The Manual choice is not available on Linux.

Other Commands

Click the **Open Administrator** menu item to open the main Yosemite Server Backup Administrator window using the logon information from the Quick Access application.

Click the **Logout** menu item to log out from the Quick Access application. The application will disconnect from Yosemite Server Backup. Click **Login** to log back into the application.

Click the **Exit** menu item to exit the Quick Access application. If the Yosemite Server Backup service is still running, the application will continue to run. To restart the application, access the application in the **Start** menu.

Click the **Open Administrator** menu item to open the main Yosemite Server Backup Administrator window using the logon information from the Quick Access application.

About the Yosemite Server Backup Service

The Yosemite Server Backup Service lets you run backup jobs automatically and unattended. The service makes sure your scheduled backup jobs run even when the machine reboots after a power loss.

- Microsoft Windows and the Yosemite Server Backup Server
- Linux and the Yosemite Server Backup Daemon

Microsoft Windows and the Yosemite Server Backup Server

You can manage the Yosemite Server Backup service from the Windows Services screen. For an explanation of managing Windows services, please refer to the Microsoft documentation for the Service Control Manager

△ CAUTION:

Changing the Startup type for the Yosemite Server Backup service to Manual or Disabled means that other machines will not have access to this machine to perform backups unless Yosemite Server Backup is actually running. This means that files on this machine will not be backed up during routine backups for this machine. Before disabling the service, you should evaluate the impact that this decision will have on your company's backup and restore policies

Linux and the Yosemite Server Backup Daemon

On Linux platforms, the Yosemite Server Backup service, or daemon, is designed to run automatically each time the system is restarted.

The daemon program (`ytlinsvc`) is located in the Yosemite Server Backup directory. To access the service in the default installation directory you would

typecd `/usr/local/barracuda/yosemiteserverbackup/ytlinsvc`

and press **Enter**.

If you have disabled this automatic startup of the service, you can use one of the following commands to manage the service:

Install service type ./`ytlinsvc` –I

and press **Enter** to start the Yosemite Server Backup service automatically when your computer starts up. Your selection takes effect the next time your computer starts up.

To start or stop the service if it is already installed, use one of the following commands to manage the service:

Start service type ./`ytlinsvc` –s

and press **Enter** to start the Yosemite Server Backup service.

Stop service type ./`ytlinsvc` –x

and press **Enter** to stop the Yosemite Server Backup service.

3 Configuring Backup Jobs

In this chapter

- Selecting Files
- Selecting Devices for Jobs
- Chapter 7
- Configuration
- Advanced Settings

Backup jobs can be created from the **Tasks** view or the **Jobs and Media** view using the **New** command. When a new job is created the Administrator will open the job's Property page to allow configuration of the job. The Property page can be reopened at any time, even when the job is running. If the job is running the settings pages will not be editable.

Selecting Files

You use the **Selection** property page of a job to select the files to be backed up. Yosemite Server Backup provides powerful selection filters that allow you to select exactly the files you want and to automatically update your selection when the job is run.

Files, folders, and other containers (e.g., volumes and computers) are displayed in a tree view on the **Selection** page. All containers act similarly regarding selection, so any discussion about folders applies equally to any other container unless otherwise noted.

You can select or deselect a file or folder by checking or clearing the selection box next to the folder. When you select a folder or other container, you automatically select everything within it including all files within all subfolders. If the checkbox for a folder is clear, no files and subfolders within that folder are selected. If the checkbox for a folder is shaded, some, but not all, of the files or subfolders within it are selected.

You can select the contents of a folder in one of two ways: either by individually checking each file in that folder one-by-one or by checking the folder itself. Which method you choose is important because it affects which files Yosemite Server Backup included in the selection list *after changes have been made to that folder*.

△ CAUTION:

If you select each file in the folder individually, when new files are added to the folder, Yosemite Server Backup automatically selected for backup. However, if you select the folder *itself*, when new files are created in that folder, they are automatically selected for backup.

In general, when selecting files for backup, especially for jobs designed for disaster protection, begin by selecting containers at the top of the hierarchy. Then deselect containers or files lower in the hierarchy that you do not need to back up.

For example, you could begin by selecting the network icon at the top of the hierarchy. This will automatically select all of the machines on the network and all of the volumes on those machines. If there are machines, volumes or folders you do not want backed up, clear their check boxes. When new machines or volumes are added to the network (that is to the current Backup Domain), these new machines and volumes will automatically be selected for backup.

By default, Yosemite Server Backup backs up all volumes, folders and files that have been marked for the job. Selection filters let you identify specific criteria for excluding one or more of these marked objects. The filter criteria is applied when the job runs, in effect unmarking any objects that do not meet the criteria. Selection filters are optional. If no selection filter is specified, all of the files and folder that have been marked will be backed up per the job configuration settings. For further information, see the Yosemite Server Backup Technical Reference Guide.

Yosemite Server Backup can be configured to include mapped drives during backup. By default they are excluded. Once configured, these drives will appear on the **Selection** page of a job. For further information, see the Yosemite Server Backup Technical Reference Guide.

Selecting Devices

Selecting this link displays the Device view and allows you to select the device(s) to use in the job. See Selecting Devices for Jobs for more information about using the Device view.

Encryption

This step is optional. Data is neither encrypted nor compressed by default. If you would like to change these options, see Chapter 7.

Configuration

The Configuration page contains the settings that control when the job will run and how media will be managed. The page is divided into a number of sections, some of which are only visible based on the scheduling choice.

- Schedule Settings
- Mode Settings
- Scheduled Dates (only visible when Schedule Type is **Run on selected days**)
- Interval Settings (only visible when Scheduled Type is **Run repeatedly**)
- Media to be used
- Auto format mode

Schedule Settings

The **Schedule Settings** box contains several settings that control when jobs are run and how the jobs use media.

Schedule Type

This setting is the first step in choosing when the job will run. Once scheduled, the Yosemite Server Backup service will ensure the job is started. If one or more job runs are missed because the service is not running at the scheduled time, the service will determine the backup mode with the largest interval setting (Daily, Weekly, Monthly, Yearly) that was missed and run it.

Not scheduled The job will be run manually by the user when desired.

Run on selected days The job will run only on a selected day (or days) at a specified time. When this option is selected an additional setting, **Scheduled Dates**, will appear.

Run repeatedly The job will run on a regular interval. Use this setting to set up a job with media rotation. When this option is selected an additional set of options, **Interval Settings**, will appear. For more information see Chapter 6.

Start Time

This setting is only visible for jobs that will be run on a schedule. It specifies the time of day that the job should start. For jobs that are scheduled to run more than once, all runs will happen at the same time of day.

Rotation Type and Sets

This setting is only available when the job is scheduled to run repeatedly. The **Rotation type** and **Sets** controls allow you to specify a set of preconfigured rotations. The Custom Rotation type is a special case. It unlocks the user interface to allow the user to configure his own rotation. For more information about setting up rotations, see Chapter 6.

Type of Fixed Rotation

This setting is only available when creating a custom rotation. For more information about setting up rotations, see Chapter 6.

Mode Settings

The **Mode** box contains several settings the control the type of backup and automatic verify that will be performed, how used media will be treated, and what to do when a file won't fit on the current media. Man of these settings are set automatically when a schedule rotation is in effect. When a rotation controls theses settings they become disabled in the Administrator.

Backup mode

Yosemite Server Backup supports the back modes listed below. For scheduled automatic rotation jobs, Yosemite Server Backup uses the backup mode for each backup set as indicated on the **Schedule** page; for unscheduled or manual jobs, Yosemite Server Backup uses the settings set by the user.

Full This setting instructs Yosemite Server Backup to back up all selected files.

Differential This setting instructs Yosemite Server Backup to back up all selected files that have changed since the *last full* backup.

Incremental This setting instructs Yosemite Server Backup to back up all selected files that have changed since the *last* full, differential, or incremental backup.

Copy This setting instructs Yosemite Server Backup to back up *all* selected files, but it has no effect on any future scheduled job. Use this option when you wish to make a record of files or systems at a particular time, but do not wish to disrupt the normal backup schedule.

△ CAUTION:

Incremental jobs are the shortest and smallest jobs to run, but they present some issues related to full data recovery. The difference between an incremental and a differential backup is important -- incremental backup jobs back up only files that have changed since the last full, differential or incremental backup, while differential backup jobs back up all files changed since the last *full* backup. If incremental backup media sets are overwritten or recycled before another full backup is performed, this can create a gap in available data if you need to recover files from the overwritten media.

Exclusive use of incremental backup jobs to ensure full data recovery after a disaster is not recommended, *unless you are using a schedule that retains one full backup and all subsequent incremental backups* before overwriting any media. However, to ensure successful data recovery with incremental jobs, follow these guidelines:

Have at least as many incremental media as there are days between full or differential backup jobs. For example, if you run full backup jobs every five days, have at least four incremental media; if you run full backup jobs every seven days, have at least six incremental media.

Never recycle incremental media between differential or full backup jobs. If you run more than one incremental job in a row, be certain to not recycle any of the media used during this string of incremental jobs.

Auto verify mode

After Yosemite Server Backup backs up a set of data, it can verify that the data was backed up correctly. Yosemite Server Backup reads the files from the media and performs the selected verification type. If any discrepancies between the two files are found, the file is reported in the job log.

Full Verify This setting instructs Yosemite Server Backup to compare every selected file stored on the media with the original file from the PC desktop or file or application server. If the file has changed since it was backed up, the full verify process will report that the file on the media does not match the file on disk. This does not mean that the backup was unsuccessful.

Quick Verify This setting instructs Yosemite Server Backup to be certain that every file backed up onto the media is in readable condition. It does not verify that the data matches the file, only that the data stored on the media can be read.

No Verify This setting instructs Yosemite Server Backup to skip the verification step. It is not recommended.

TIP:

Verifying that data has been correctly written to the media is an essential part of a comprehensive backup program. Also, verifying the files ensures that the media and the media drive are working correctly.

Write mode

For automatic rotation jobs, Yosemite Server Backup overwrites all media. For other jobs, Yosemite Server Backup uses the write mode settings set by the user. This mode determines whether the old data on the media is *overwritten* with new data or whether the new data is *appended* to the end of the old data. When media is overwritten, all of the data previously stored on it is lost. Appending data will preserve the old data.

Append to all media This setting instructs Yosemite Server Backup to append all data to the end of the media. No data is overwritten. Select this setting for permanent storage.

Append to first media, overwrite others This setting instructs Yosemite Server Backup to append data to the end of the first media, but to overwrite all media that follows. For example, Yosemite Server Backup will not overwrite the first media inserted, but will overwrite the second, third and later media. This setting is useful if you have a set of media with old data you no longer need. By selecting this option, Yosemite Server Backup preserves your most recent data on the first media, but overwrites older, unneeded media.

Overwrite all media This setting instructs Yosemite Server Backup to overwrite all media. All data on media that is overwritten is lost. Use this option for media that are going to be recycled.

Split File

The Split File mode determines how Yosemite Server Backup will handle a file if the file is too large to fit on the current media. Selecting this option to instruct Yosemite Server Backup to split a file across two media if it will not fit on the current backup media. If this option is not selected then file that don't fit on the media will be restarted on the next media.

⚠ WARNING!

If you use the split file option, files that span two media will require both media for restore. If one is lost then the file cannot be recovered.

⚠ WARNING!

Files protected with split file mode cannot be restored during Disaster Recovery. They must be restored after the DR process has completed.

Scheduled Dates

This setting is only visible when the schedule type is set to run on selected days. It consists of a list of selected days to run the job. To add days to or remove days from the schedule, click the **Calendar...** button to open the schedule calendar. To schedule the job to run on a day, right-click on the day in the calendar and select **Daily**. To unschedule a day, right-click on it and select **None**.

Interval Settings

This setting is only visible when the job is scheduled to be run repeatedly. It contains controls for specifying which types of jobs (full, incremental, or differential) will be run on which intervals and the number of media sets that will be used. You can use the **Calendar...** button to view of the schedule. The calendar will show when daily, weekly, monthly and yearly backups will be run. Clicking a day will display a message along the bottom of the dialog explaining the type of job that will be run, the name of the media that will be created, and whether the media will be appended to or overwritten. To override the schedule on a an individual day, right-click on the day and select the new backup type or deselect the day to stop the backup on that day. For more information see Chapter 6.

TIP:

It's a good idea to deselect holidays from you schedule if you don't have a tape library or if nobody will be available to put the correct media into the device.

Media to be used

Select the folder in which the job will look for existing media that it can reuse. Note that the default folder is the current Job folder. If you wish to use media from another folder, specify which folder by clicking the Add button to open a catalog browser and navigating to the desired folder.

Auto format mode

Auto format mode

Before data can be written to media, the media must be formatted. When media is formatted, any data on it is lost and all record of the media is removed from the catalog.

No auto format Instructs Yosemite Server Backup to send an alert to the alert window if it encounters media that needs to be formatted (either blank or unrecognized media). While waiting for a user reply, Yosemite Server Backup scans the network for devices with the media it was expecting.

Auto format blank media only Instructs Yosemite Server Backup to automatically format all new or blank media. However, if Yosemite Server Backup encounters unrecognized media, it sends an alert to the alert window and then scans the network for the media it was expecting. This setting can help prevent data from being accidentally destroyed by formatting, while not needlessly querying the user before formatting a blank media.

Auto format all media Instructs Yosemite Server Backup to automatically format all of the media inserted into the tape drive which require formatting. With this setting selected, Yosemite Server Backup will automatically format all new or blank media and all unrecognized media.

New media location

Specifies the folder in which Yosemite Server Backup will store any new media created while the job is run. By default, Yosemite Server Backup stores media under the backup job to ensure the media isn't used by another backup job. To change the default, click the **Browse** button and select the folder from the **Browse** dialog box.

When Yosemite Server Backup runs any scheduled automatic rotation job, it automatically creates media folders for the job. The folders are organized by the name of the job and the various rotation sets in that job.

Move media to new media location on overwrite

Setting this checkbox moves media from the Media to be used folder to the New media location folder when it is used.

⚠ WARNING!

If this option is turned off it is possible for a job to exhaust its set of available media to use and stop running.

Rename media to new media

Setting this checkbox renames existing media being overwritten to the name which would have been used had it been freshly formatted. When this is off, previously formatted media used by this job will retain the name it was given when it was used previously.

New media name

Enter the name Yosemite Server Backup gives to any new media it creates while running the job. For scheduled automatic rotation jobs, Yosemite Server Backup automatically updates this setting to match the media's place in the rotation schedule and this setting has no effect.

For manual rotation and unscheduled jobs, Yosemite Server Backup assigns any new media it creates the name listed in this field. This is also true for automatic rotation jobs that are "forced" to run. If the job creates more than one media, the job will use this setting as a template to create a unique media name containing this setting.

Advanced Settings

In this section

Advanced Options

In general, the default values should be used. These options are provided only for advanced users who need to customize their backup jobs for unique circumstances.

△ CAUTION:

Unless you have specific needs that require changes to the advanced options, leave the default values unchanged.

Settings for all platforms

Eject media after use When this option is checked, Yosemite Server Backup automatically ejects the media at the end of the backup job. This feature only works on devices that support software eject.

Auto Retension When this option is checked, Yosemite Server Backup automatically re-tensions the media at the beginning of the backup job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto re-tension to use this feature.

Create DR bootable media Check this option to write DR system information to the backup media. This option is only useful when the backup media is bootable as in the case of OBDR tapes or optical media. However, leaving this option checked does not hurt the backup.

Update DR information on selected machine Check this option to generate DR system information for the selected machines. The generated system information will be saved on the Domain Server and can be used later to create DR media even after a failure of the original machine.

Native data streams format Different operating systems transmit data across the network to Yosemite Server Backup in different formats. If you plan to restore files to a different operating system than they were created, the data should be stored on media in a common data format, not in the native data streams format.

Settings for Windows

Enable snapshots By default, the backup job creates a temporary snapshot before backing up the selected file. Deselect this checkbox to disable snapshots.

A snapshot freezes the volume data at a point in time. Any changes after that point in time will not be backed up until the next backup job. The temporary snapshots are deleted after the job has finished. If this option is off, files open during backup may not be backed up. Failure to back up open files will be noted in the job logs.

Snapshots are currently implements only on Windows platforms. On Windows, the snapshots are created using Microsoft Volume Shadow Copy Services (VSS) for those operating system editions that support VSS.

Reparse points Check this option to back up the reparse point data. When this option is deselected, Yosemite Server Backup will back up the object as if it were a normal file or directory.

Mount Points When checked, Yosemite Server Backup includes the mount point information in the backup. If this option is not checked, Yosemite Server Backup treats the object as a directory.

Optimize backup order by size Will mix backing up large and small files in an attempt to maintain consistent throughput to the backup devices.

Volume restrictions When enabled, volume quota information will be backed up.

Log Options

These settings control how the results of the job are reported to the user. See Job Log options for details.

Execution

These settings allow the user to execute external programs before and after backing up objects on a client. For example, this feature can be used to shut down a custom database before backup and restart it upon completion. to ensure the files are quiescent during the backup. See Job Pre-Post Execution Commands for details.

Barcode Filter

These settings control which media can be used by the job by specifying the acceptable barcodes. This feature is designed for use with tape libraries that support barcodes. See Barcode Filters for Jobs for details.

Copy Policies

Copy policies are used to schedule a job to make a copy of the media created by the current job.

4 Configuring Restore and Verify Jobs

In this chapter

- Selecting Files
- Selecting Devices
- Configuration
- Advanced Settings

Restore jobs and verify jobs are similar in that they involve reading files that have been backed up. Whereas a restore job actually copies backed up files, verify job reads the backed up files and compares them to the current files at the original backup location on disk. Because of their similarities, they will be discussed together in this chapter.

Restore and Verify jobs can be created from the **Tasks** view or the **Jobs and Media** view using the **New** command. When a new job is created the Administrator will open the job's Propery page to allow configuration of the job. The Property page can be reopened at any time, even when the job is running. If the job is running the settings pages will not be editable. .

Selecting Files

Selecting Files

You select files to be restored the same way you select files to be backed up. However besides selecting which files you wish to restore, you must specify which version of the file you wish to restore. When you select a file to restore, the most recent version is selected by default. You can also change the name of the restored file or restore it to a new location.

To select files for restore and verify jobs

1. View the properties of the restore job and click on the **Selection** page.
2. Check the selection boxes next to the files, folders or other containers you wish to restore.
3. To select a specific version of the folder or file or folder you selected, highlight it and select the version from the list in the bottom part of the window. If you don't specifically select a version then the most recent version will be restored.
4. Optionally, click the **Selection filters** button on the tool bar and specify filter selection criteria. Filters are described in more detail in the Yosemite Server Backup Technical Reference Guide.
5. The selected files will be restored to or compared with their original locations.

Selecting Versions

Each time a file is backed up, a version of that file is created. There may be several versions of files stored on different media created by different backup jobs. Yosemite Server Backup keeps track of all the versions of each file in its catalog and the media on which each version is stored. When media is overwritten or deleted, Yosemite Server Backup deletes those versions from its catalog as well.

When you select an object (file, folder, database, etc.) for restoring, Yosemite Server Backup automatically selects the latest version. If you want to select a version other than the latest version, select the desired version from the version list below the object selection tree. The version list shows all of the versions of the object and the media on which those versions are stored and details about the object including the its backup date and its modify date.

When you select a folder, Yosemite Server Backup automatically selects the latest version for that folder and for every file within that folder. If you wish to restore as of another date, select the desired version from the version list. The version list shows all of the versions of the folder and the media on which those versions are stored. The selected folder version is used to the select files contained within that folder. Specifically, a file is selected for restoring only if a file version matches the folder version.

NOTE:

When you specify a version date for a folder, volume or other container, files stored in that container are *only selected when they have a version date that matches the version date of the container*. Many times, files will not have version dates that match the dates of the containers where they are stored.

For example, when you select a version date from an incremental or differential backup job, you must select the latest version available for that container to be sure you recover all of the files inside that container.

In general, if you want to restore a specific version of the file, you must select that file directly and specify which version you wish to restore in the **Versions of** window.

Restoring folders

You can select the contents of the folder in one of two ways: either by individually marking the selection box of each object in that folder one-by-one or by marking the selection box of the folder itself. Which method you choose is important because it affects which files Yosemite Server Backup includes in the selection list *after changes have been made to that folder.*

For example, if you select a folder for restoring by marking its selection box, all of the contents of that folder are restored. If a new backup job is run before the restore job is run, Yosemite Server Backup selects files for restoring using the new folder's contents. So, for example, if a new file is created in that folder, Yosemite Server Backup will also restore that file. Additionally, if you have selected a latest version of the folder, Yosemite Server Backup will use the latest version of each file in its catalog. These files may be newer than the files you originally selected.

Restoring a file with a new name

After a file has been selected for restoring, you can rename the file. When you rename the file, Yosemite Server Backup restores the file with the new name. This can be useful for not overwriting versions of the file that currently exist on disk.

To rename a file, right click the file name on the **Selection** page of the restore job, select **Rename** from the **context** menu and type the new name. Once you run the job the renamed file will be restored to the directory in which the original file was located.

NOTE:

When you rename a version, you are *only* renaming that file for the purposes of restoring it with this particular restore job. *Only the current restore job will assign the new name to that file*. When you create a new restore job, you will see the file displayed with its original name. Similarly, the **Catalog** view always displays files with the names they had when they were backed up.

Restoring files and folders to a different folder

You can also restore files and folders to different folders. When Yosemite Server Backup restores the object, it creates it in the new location. This is useful in order to prevent overwriting files and folders that currently exist on disk.

To restore to a different folder (also known as a *move restore*), right-click the file name on the **Selection** page of the restore job and select **Move** command from the command bar. In the **Select destination for move operation**

window, select a target location. Yosemite Server Backup will move the file to the destination you select. If the destination folder doesn't exist, you can create it directly from the dialog.

You can also restore folders and volumes in new locations. The contents of these containers move with them and are restored, along with the folder or volume, in the new location.

NOTE:

When you move a version on the **Selection** page of a restore job, the changes you make are only recorded for that restore job. Only the current restore job will assign the file or folder the new location. When you create a new restore job, you will see the files and folders in their original locations. Likewise, the **Catalog** view will continue to display files in their original locations.

Selecting Devices

Selecting this link displays the Device view and allows you to select the device(s) to use in the job. See Selecting Devices for Jobs for more information about using the Device view.

Configuration

Restore Job Settings To schedule a restore job to happen at a particular time, change the **Schedule Type** to **Run on specific day** and then set the start time and date. The service will ensure that the restore will happen at that time.

Verify Job Settings Like the restore job, you can schedule a verify to happen on a particular time as well. Additionally, you can specify whether the job is a Full or a Quick verify. A full verify will compare the contents of the backup media with the source files on disk. A quick verify will only validate that the media can be read from end to end.

Advanced Settings

In this section

- Advanced Restore Options
- Advanced Verify Options
- Log Options
- Execution Options
- Barcode Filter Options

Advanced Restore Options

These options apply to all restore jobs regardless of the operating system.

Eject media after use When this option is checked, Yosemite Server Backup automatically ejects the media at the end of the job. This feature only works on devices that support software eject.

Auto Retension When this option is checked, Yosemite Server Backup automatically re-tensions the media at the beginning of the job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto re-tension to use this feature.

Restore files that are in use Select this option to restore the backup copy of the open file. (On Windows platforms, you can access the restored file after you restart the computer.) If you select this option, the restored file will replace your open file. As a result, your current changes may be lost.

Deselect this option to skip over all selected files that are in use. This is useful if the open files are more current than the backed up files.

Omit security information This will remove any security information associated with the files and folders which were part of the backup. The files and folders will be restored as if they were freshly created, inheriting whatever permissions would belong to new files.

Reparse points [Windows only] Check this option to restore the reparse point data. When this option is deselected, Yosemite Server Backup will restore the object as a file or folder rather than as a reparse point.

Mount Points [Windows only] When checked, Yosemite Server Backup includes the mount point information in the restore. If this option is not checked, Yosemite Server Backup restores the object as a directory.

Volume restrictions [Windows only] When enabled, volume quota information will be restored.

Finalize recovery of Microsoft SQL and Exchange Server databases [Windows only] Check this option to process database transactions when the last incremental restore is complete.

Restore all registry keys / Restore hardware registry keys [Windows only] Controls whether/how Yosemite Server Backup will restore the described objects. These setting only applies if you are restoring the Registry System State object.

Restore DFS/FRS shares as primary replica (authoritative restore) [Windows only] Use this option to control how a DFS or FRS share is being restored. Only check it if you want an authoritative restore. See the Microsoft documentation for more information on authoritative restores.

NOTE:

Data filters, such as security information and directory attributes, cannot restore data that was not originally backed up to the media. For example, if you did not select **Volume restrictions** for the backup job, Yosemite Server Backup cannot restore this information because it was never stored on the media.

Advanced Verify Options

The following advanced options are available for Verify jobs

Eject media after use When this option is checked, Yosemite Server Backup automatically ejects the media at the end of the job. This feature only works on devices that support software eject.

Auto Retension When this option is checked, Yosemite Server Backup automatically re-tensions the media at the beginning of the job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto re-tension to use this feature.

Native data streams format When this option is selected, Yosemite Server Backup will compare the data in native format. When unselected, only the data portion of the file will be verified. This must match the mode used during backup.

Enable snapshots [Windows only] By default, the verify job creates a temporary snapshot before verifying the selected file. Deselect this checkbox to disable snapshots.

Reparse points [Windows only] Check this option to verify the reparse point data. When this option is deselected, Yosemite Server Backup will verify the object as a file or folder rather than as a reparse point.

Mount Points [Windows only] When checked, Yosemite Server Backup includes the mount point information in the restore. If this option is not checked, Yosemite Server Backup will verify the object as a directory.

Volume restrictions [Windows only] When enabled, volume quota information will be verified.

Log Options

These settings control how the results of the job are reported to the user. See Job Log options for details.

Execution Options

These settings allow the user to execute external programs before and after backing up objects on a client. For example, this feature can be used to shut down a custom database before backup and restart it upon completion. to ensure the files are quiescent during the backup. . See Job Pre-Post Execution Commands for details.

Barcode Filter Options

These settings control which media can be used by the job by specifying the acceptable barcodes. This feature is designed for use with tape libraries that support barcodes. See Barcode Filters for Jobs for details.

5 Working With Devices

In this chapter

- Selecting Devices for Jobs
- Device Properties
- Device Commands
- Working with Tape Libraries
- Sharing storage devices on a SAN

Yosemite Server Backup recognizes any installed device that is part of the Yosemite Server Backup management domain and displays them on the **Devices** view. You can use the **Devices** view to perform operations on any physical or virtual device.

Selecting Devices for Jobs

The **Device** page of a job's properties lets you select the devices that will be used. You may select as many devices as you wish for use in a job and Yosemite Server Backup will use the devices as efficiently as it can.

You can view the available devices by either a **Device view** or by **Network view** by selecting the appropriate tab.

The Device view allows you to locate devices according to their class — for example, tape drives. Since Yosemite Server Backup can read and write CDs and DVDs (optical media) a large domain may have dozens of devices, many of which are optical devices. This view make it simple to locate the tape drives or libraries in your network. Each class of device is represented as a node at the top of a tree hierarchy. By checking the box next to a class of device you are telling Yosemite Server Backupto use any device of that class it can find available when the job runs. This is a powerful concept because it allows you to add additional devices to your network and to your jobs without having to reconfigure your jobs. If you expand the class by clicking the **+** next to the class name you will see the names of each device of that class. Expanding the name will show you which machine the device is attached to. Selecting a specific device will ensure that only that device will be used in the job.

The Network view presents the same map of your devices but from a different perspective. At the top of the hierarchy is the **Network**. Next to each element in this list is a set of checkboxes representing the supported classes of devices. Selecting the Tape Devices box next to the Network configure the job to use all tape drives in the network at the time the job runs. Under the Network you will see machines. Selecting a class of devices next to a machine will limit the job to use only that class of device on that machine. Finally, when the machine is expanded, all connected devices are displayed. There will be a checkbox in the column appropriate for the class of device. Checking that box will select just that device for use with the job.

NOTE:

New devices added to the network after a job has started running will not be available to the job until the next run.

Device Properties

When you select a specific device in the **Devices** view and click **Properties**, you are able to perform the following configuration.

Status The Status page displays the current status information for the selected device. For example, it shows the current operation, if any, being performed on the device. It also shows the last time a write and read was done on the device.

TIP:

Yosemite Server Backup tracks the contents of devices and libraries while it is running. However, there may be times when someone changes media in a device or a library when Yosemite Server Backup is not running. The Probably qualification on element status indicates that Yosemite Server Backup has restarted and is operating under its previous understanding of the current element status but that the understanding may be incorrect. When Probably appears before an element status, the element's actual status will be determined the next time the element is used.

Table 3 Element status

Status	Description
Valid	The slot is known to hold media that is in the current catalog.
Probably Valid	The slot held valid media previously. Yosemite Server Backup verifies that the media is valid before using it. When you exit and restart Yosemite Server Backup, media marked Valid is reset to Probably Valid.
Invalid	The slot holds media that is definitely not in the current catalog.
Probably Invalid	The slot holds media that may not be in the current catalog. When you exit and restart Yosemite Server Backup, media marked Invalid is reset to Probably Invalid.
Empty	The slot is either known to be empty or a user changed its status to Empty.
Probably Empty	The slot was empty previously. When you exit and restart Yosemite Server Backup, slots marked Empty are reset to Probably Empty.
Unknown	The status of the slot is not known, usually because it has not been used yet.
Cleaning Tape	A user marked the slot as holding a cleaning cartridge. The number of remaining cleaning cycles also appears. Yosemite Server Backup does not verify that a cleaning cartridge was, in fact, inserted into this slot.
Probably Cleaning Tape	The slot previously contained a cleaning tape. When you exit and restart Yosemite Server Backup, slots marked Cleaning Tape are reset to Probably Cleaning Tape.
Reserved	The slot was disabled by a user. Yosemite Server Backup will ignore it during any job. You can only change the status of a reserved slot. Yosemite Server Backup changes the status of all other slots during normal operations.

Configuration You can set the size of the I/O buffer to be used for this device. Usually, you do not need to change the default. However, for some devices, you may be able to increase performance by adjusting the size of the I/O buffer.

Diagnostics The Diagnostics page displays diagnostic information about the device. This includes information about the driver, the inquiry information, device statistics, and buffer statistics. Often this information can assist in troubleshooting problems. The diagnostics can be saved to a file or emailed directly from the diagnostic screen.

Device Commands

There are several physical operations that can be performed on a selected device. Some of these operations affect the device itself, while others affect the current media in the device.

NOTE:

Not all operations are available on all devices. For example, an optical device does not support the Rewind command. Check your hardware documentation to determine which of the following commands are supported by your device. Only supported commands will appear on the **context** menu and the command bar.

Identify Use this command to get the name of the media currently loaded in the device. Yosemite Server Backup tries to identify the tape or other media that is currently loaded in the device. If Yosemite Server Backup cannot identify the media, it reads the media header, a process that may take up to several minutes. The name of the media appears on the log file for the media job and in the Media column of the device list.

Import This command allows you to use data on media that was created in another Yosemite Server Backup management domain. To use media that was not created in the current catalog, you must import that media into the current catalog.

You might import media in one the following situations:

- To use media created by an earlier version of Yosemite Server Backup.
- To use media created in a different Yosemite Server Backup management domain.
- To use media accidentally deleted from the catalog.

When you select the Import command a property page will open and prompt you for the media password and the encryption passphase. The media password is only applicable to media created with older version of Yosemite Server Backup and can usually be left empty.

An encryption passphrase is only required for encrypted media. If the supplied passphrase is not correct, the job log will present you with the hint supplied at the time of the media's creation.

Format Use this command to format media currently loaded in the selected device.

When you format new media, Yosemite Server Backup opens the **Format Media** dialog box. Use this dialog box to name the media and select a media folder in which to store the media. Yosemite Server Backup will format the media currently loaded in the device you select. If you select a library, select the storage slot that holds the media you want to use. When you format media, you can also set your choice of encryption levels. Any backup job that uses media pre formatted with encryption must specify the same encryption parameters.

NOTE:

Yosemite Server Backup is designed to manage your media for you. This command should only be used by knowledgeable users and only after determining that the built in media management does not provide the desired effects.

Erase This command erases the media currently loaded in the selected device. It has the following options:

- The **Quick Erase** option erases the first block and then writes an end of data marker to that first block. The other blocks of the tape are not erased, but when that tape is read, Yosemite Server Backup treats it as if it were blank because it encounters the end of data marker in the first block.
- The **Secure Erase** option erases every block on the tape. This operation can be very time consuming, lasting several hours. However, it will physically erase every block on the tape. If you want to destroy sensitive data, use this command.

Some devices support both options; some support only one of the two erase options. Only options supported by the selected device will be available.

Retension Media Occasionally when a tape is repeatedly fast-forwarded and rewound for only short distances, tension differences develop in the tape that cause the tape drive to falsely believe it has reached the end or beginning of the tape. You can use this command fast-forwards the tape to the end of the tape and then rewinds it to the beginning. This command can be useful in some circumstances. By retensioning on the tape, you can sometimes make an otherwise unusable tape operational again.

NOTE:

If you need to retension tapes regularly to use them, consider servicing your tape drive or replacing your tapes.

Eject You can use this command to eject media from the selected device or eject the media magazines from the selected library. Some device magazines will not be ejectable.

Restore Catalog The **Restore Catalog** command provides a quick method of restoring your current catalog, for example in case it has been corrupted. For example, you might use this command if the Yosemite Server Backup Domain Server has crashed. Use this command only when your current set of media is intact. .

The **Restore Catalog** command differs significantly from the **Import Media** command in that it command *replaces* the current catalog with the last known good catalog on that media. **The Import Media** command, on the other hand, *does not replace* the current catalog; it only adds additional data to it.

The advantage of the **Restore Catalog** command is that it provides a quick and easy way to replace a lost or corrupted Yosemite Server Backup catalog. You could use the **Import Media** command to restore a corrupted catalog, but this process requires importing all of your media rather than simply reading the media containing the catalog.

TIP:

It's a good idea to make a regular backup of the Yosemite Server Backup catalog. It will be included automatically in any full backup of the Backup Domain

NOTE:

All information in the current Yosemite Server Backup catalog will be lost when you use the **Restore Catalog** command. This command does not append data to the current catalog; it replaces the current catalog with the last known good catalog on that media.

NOTE:

You will be prompted stop and restart the service. Use the Yosemite Server Backup Service Control Manager to start and stop the Yosemite Server Backup service.

Clean Device The **Clean Device** command will run the backup device through a cleaning cycle.

This command is supported only by libraries. If a device in a library provides notification that it needs cleaning and the library has a cleaning cartridge available, a cleaning cycle will be performed automatically at the start of a backup job. If you are using a device that is not a library, you must manually clean the device at the manufacturer's suggested intervals.

To clean a device in a library, highlight the device and select **Clean Device** from the **Command** bar. Yosemite Server Backup will check to see if one of the slots holds a cleaning cartridge. If it does, the cleaning cycle will be performed in the background; if not, an error message is shown.

If the **Clean Device** command is missing, it is not available for your backup device. In this case, a cleaning cycle can often be performed by manually inserting a cleaning cartridge into the backup device.

Start, Stop and Rescan Sometimes you will need to restart a device that has, for some reason, failed to initialize properly. A device may have stopped for any number of reasons, such as a power failure or a connecting cable malfunction. Virtual devices on a network appear disabled if the network connection has failed.

When a device is not initialized, it appears with a yellow warning icon. Some devices may take some time to initialize, during which the warning icon will continue to appear. If a device shows the warning icon after it is initialized, press **F5** to refresh the device display.

If you don't see a device that you expect to see connected to a machine, select the **Device** folder under the machine and click the **Rescan for New Devices** command.

If there is some other problem with the device or the controller, the warning icon will not disappear. You must identify and correct the problem yourself. Then you must restart *both* Yosemite Server Backup and the Yosemite Server Backup service. When Yosemite Server Backup restarts, it will initialize the device driver again. Check the **Devices** view to see that the devices are now properly working and that they no longer display the warning icon. Any duplicate or old devices that are offline can be deleted from the **Catalog** view.

Working with Tape Libraries

In this chapter

- Installation and Configuration
- Barcodes and MIC (memory in cartridge)
- Barcode Filters
- Initialization Process
- Media Management

Tape libraries automate tape media handling which, in conjunction with the Yosemite Server Backup backup schedules, allows hands-off backup operations. A tape library contains one or more tape drives, some number of storage slots for tape media, and, in some cases, import/export slots to add or remove media from the library.

Yosemite Server Backup support for tape libraries allows you to automate and consolidate backup in network environments and manage media efficiently. Yosemite Server Backup has a built in media rotation schemes to help take advantage of the features of your library. Yosemite Server Backup tape library support includes managing media using barcodes, using the on-board memory in some tape cartridges, such as Ultrium Memory in Cartridge, and user-configurable tape media load ports (mail slots).

NOTE:

Always manage your tape media from the Yosemite Server Backup interface. Your tape library may provide a front panel that allows you to carry out various media management tasks but if you use this for media operations the Yosemite Server Backup catalog will not have the up-to-date media location information. For this reason, front panel media operations will require time-consuming inventory processes to update the catalog.

NOTE:

If your library supports multiple tape devices and you want to use a specific device, you must select that device to use it. If you select the library, Yosemite Server Backup will use the first available device in the library it finds.

Installation and Configuration

If the tape library is installed correctly, Yosemite Server Backup will automatically detect the tape library. When detected the tape library is added as an available device to the Yosemite Server Backup catalog.

Once you have installed Yosemite Server Backup, expand the **Devices** view to locate the tape library. Note how the components of the tape library are displayed so that you can see how many devices (tape drives), import-export Slots (mail slots) and storage slots are associated with the library.

Devices The tape drives in a tape library are viewed and managed in the same way as stand-alone tape drives.

Storage Slots The Storage Slots folder displays the number of available slots. Each slot may contain blank (new) media, media containing Yosemite Server Backup data, or media containing unknown (non-Yosemite Server Backup) data. Yosemite Server Backup inventories the media in the slots and displays the information about the media and its status in the view. This allows you to view all kinds of media, not just the media used by Yosemite Server Backup, but you will not be able to select non-Yosemite Server Backup media for a backup or restore job.

NOTE:

It can take a long time to inventory the tape media in a tape library, which is why Yosemite Server Backup usually performs a "light inventory" rather than running an identify job on all the slots in a loader. See the "Inventory Process" section below for more information.

Additional media slot configuration is accessed via the Element Status dialog for that slot, which is accessed by a right click on the desired slot. For example, you can use this to disable slots (using the 'Reserve' option) and identify a cleaning cartridge.

Import/Export Slots Some library devices provide special import/export mail slots an operator uses to enter or eject media to or from the device without removing the whole media repository or magazine. Depending on the device, more than one import/export slot can be provided. In case of a single mail slot, media are inserted one by one, while in case of multiple mail slots, a particular number of slots can be used in one enter/eject operation.

Barcodes and MIC (memory in cartridge)

If the tape library supports barcode and/or MIC (memory in cartridge), the details are added to the Yosemite Server Backup catalog. The barcode information is hidden by default; to display this detail, right-click anywhere in the column title row to see available column headings and click on **Media barcode** to make the barcode information visible in the slots view.

Barcode and MIC (memory in cartridge) technologies are used to reduce the time spent organizing and managing media in a library or an autoloader. In these devices, each medium is identified with a unique barcode or, where MIC is used, a chip is embedded in the tape cartridge which holds a unique identifier (as well as other information).

Barcodes and MIC enable Yosemite Server Backup to significantly reduce media recognition, labeling and cleaning tape detection times.

- Scanning the barcode or MIC of the media is faster than reading the medium header, because Yosemite Server Backup does not need to actually load the media into a tape.
- A barcode or MIC is a unique identifier for media in the Yosemite Server Backup catalog. You should not have duplicate barcodes in your environment.

Barcode Filters

The barcode filter allows users to control access to media by barcode. The user can specify ranges, wildcards, or explicit barcodes that either include or exclude media for use by the product. This property only applies to libraries. Stand alone devices are not restricted in any way by it.

The filter rules may be set for the whole domain and will be applied automatically to all tasks. Or, they may be set and applied at job level. Any filter rules applied at job level overwrite the default domain settings.

For more information on setting barcode filters, see Barcode Filter.

Initialization Process

The traditional loader inventory mechanism is accomplished by running an identify job on all the slots in a library. This complete inventory can take a very long time, so Yosemite Server Backup uses a "light inventory" process, which is known as an initialization process. This initialization process consists of ...

- Checking that the loader is ready for use. If the magazine door is open, this step will fail, and initialization will fail as a result.
- Querying the number of physical storage, import/export and device elements that the library contains. (These elements will be displayed in the Tape Library view.)
- Binding the loader to its physical devices. This ensures that the devices are associated with the library in the Yosemite Server Backup catalog.
- Updating the status for each element in the loader. Barcodes are read at this time, and are associated with each element regardless of status (i.e. both Invalid and Valid elements get a barcode shown in the loader status pane).

Initialization occurs when the library driver starts (at service startup or when the driver is manually started), when the user selects the Initialize command on the loader object or when Yosemite Server Backup detects that a user has changed the state of the loader (either by opening the front door or by using the front panel).

During initialization, the library will attempt to perform barcode based identification of media. If a match is found, the loader will set that element's status to Probably Valid. This means that if a user is using barcodes with their tape library, they will almost never need to run an identification job.

When the job loads the tape it makes sure that the tape is really what the catalog says it is and, if necessary, updates the catalog to indicate what is really there. If the tape is, in fact, not usable because of the supplied media rules, the tape is re-stowed and another media is tried.

TIP:

An Identify job will always physically mount media, and reassociate media to barcodes. This provides a mechanism for users to update barcodes on their media, should they ever need to. It also handles the case where barcodes are added to media after they have been used without barcodes.

Media Management

One benefit of using Yosemite Server Backup with tape libraries is the ease with which you can schedule different backups for different days of the week/month/year. There are no specific media tasks that must be carried out before you run a backup job. As long as the library has valid media loaded in it, Yosemite Server Backup will automatically use it automatically.

NOTE:

Media is invalid if it has been used by another backup product, is dirty or has been corrupted, or simply has not been identified.

Similarly, if you are restoring data from media that is already within the Yosemite Server Backup catalog, there are no media management tasks. However, if you are restoring media from a different domain, you must first import it so that Yosemite Server Backup can add the media to the database and associate all data objects on the tape with that media.

For a detailed description of all media management jobs, please refer to Device Commands.

Sharing storage devices on a SAN

Backup jobs automatically select devices to use based on their availability (whether or not they are in use). In a SAN environment, Yosemite Server Backup automatically recognizes that a single backup device attached to a SAN may be accessible from two or more servers, and treats the device as a single device.

NOTE:

All machines that need access to a SAN server must be included in the same Yosemite Server Backup management domain.

6 Scheduling, Rotations, and Media Management

In this chapter

- Backup Schedule Considerations
- Scheduling Concepts
- Media Rotation Types
- Running Jobs with Rotations

Ensuring that you have all the files needed to restore your system is a complex task. Typically, it is not practical — from either a time or a media perspective — to create a full backup every day. The solution involves running different types of jobs (full, incremental, differential or copy) on predefined schedule intervals using predefined numbers of media sets that get reused over time. The process of reusing media is referred to as *media rotation*. The media rotation type determines how and when each media set is used, how long it is retained once it contains data, and the granularity of your backup history.

A rotation defines the times it will run (see Intervals) and how many *sets* it will use (see Media Sets). When a job is configured to use a rotation in its schedule, the rotation set folders are created immediately. This allows the user to see what media sets the job will be requesting. If the rotation type is changed, the set folders are updated to reflect the new rotation type. When the job runs, it will look for media with specific names in specific folders. If it does not find the precise media it is looking for, it will format any available media according to the auto format rules or will prompt you to insert media into your device before it continues. When the number of rotation runs has been reached, the next backup run will select the oldest set in the interval to overwrite.

Yosemite Server Backup provides several built in media rotation types. In many cases, the name of the rotation type indicates the number media sets used in the rotation. For example, the Simple 4 rotation type will use four media sets (at least four individual tapes) to complete the rotation. The media set names can be based either on the scheduled interval or on the type of fixed rotation.

TIP:

It is strongly recommended that you let Yosemite Server Backup format your media. In most cases there is never a need to pre-format media using the Format command and doing so will, if used improperly, make your media unavailable to your jobs.

The **Jobs and Media** view displays jobs, media and folders in the Yosemite Server Backup catalog. When you first open the **Jobs and Media** view you will see a listing of your **Home** folder. Your **Home** folder is where Yosemite Server Backup stores the jobs you create and the media created by those jobs.

TIP:

When viewing the Jobs and Media view, clicking the **Folders** command will display a tree view of the **Home** folder hierarch that can be helpful in understanding the organization of media within jobs.

CAUTION:

When you delete media, Yosemite Server Backup deletes information about that media from its catalog. This includes any versions of files stored on that tape, which are also deleted from the catalog. Deleting media does not physically erase the media. The media remains unchanged; only the catalog is changed. You can still import that tape to another catalog or, if necessary, back into the original catalog.

Backup Schedule Considerations

Yosemite Server Backup lets you set up jobs that run automatically on regular schedules. To determine which type of backup job you should create, ask yourself these questions:

- How many days of data can you afford to lose?
- How large will a full backup job be?
- How much does your data change on a day to day basis?
- How many media does your budget allow?
- How much data can the backup media hold?
- If you have a library, how many tapes does it hold?
- Are there times when your tape drive will be unavailable?
- Will the amount of traffic on your network require that backup jobs be scheduled to run during non-peak periods?
- Are there certain days of the week when running lengthy jobs will interfere with other uses of your network?

As you review the following sections, keep these questions in mind to help you determine which backup job schedule to select for any particular job.

Scheduling Concepts

One of the greatest values of a data protection solution like Yosemite Server Backup is the ability to define data retention policies. Retention policies allow you to balance your data protection and historical retention needs with the economic realities of media material and management costs.

Media Sets

Yosemite Server Backup organizes media into sets based on the rotation type and schedule interval. Whether the job requires several or only one physical media to complete, they are identified in the Yosemite Server Backup catalog as a set. When more than one physical media is required for a job, Yosemite Server Backup will create a unique name for each media in the set.

When planning scheduled backup jobs, it is important to know whether one or several physical media will be required to complete a backup job. This can usually be estimated by comparing the size of the backup selection to the capacity of the selected media. If you do not want Yosemite Server Backup to use more than one media for a backup job, then you must select fewer files to back up.

NOTE:

The terms media can be used to refer to both physical media, like an LTO tape, or to the catalog object Yosemite Server Backup uses to keep track of file versions that have been backed up.

Intervals

Job schedules are defined using the Intervals **Daily**, **Weekly**, **Monthly**, and **Yearly**. Intervals are used to defined which days a job will run, what type of backup (full, incremental, differential, or copy) will be done, and how many sets of media are dedicated to the interval. The size of an interval refers to the amount of time between runs of that interval.

When the **Run repeatedly** schedule type is chosen the job **Configuration** page will show an additional section, **Interval settings**, that control the schedule parameters. Each interval type is listed along with a textual description of its current setting. To customize the settings for an interval , click on one of the interval buttons. Most schedules are defined in terms of the following intervals:

Daily — run on sequential weekdays.

Weekly — run once per week on the day specified by the user, for example, Friday.

Monthly — run once per month on a day specified by the user such as the first day, the last day, the first Monday, and others. You can also specify how many months should elapse between monthlies. Setting the monthly interval to every 3 months will create a backup every quarter.

Yearly — run once per year on a specified day of the year. By increasing the interval you can also schedule a job to run once every so many years.

NOTE:

There are also **Hourly** and Minutely intervals that are less commonly used. The concepts behind using them are similar to those of the intervals discussed above.

For all intervals there is a setting that controls the number of sets. This settings determines how many sets of that backup interval will be created before Yosemite Server Backup goes back and overwrites the first. For example, if your schedule starts in January and calls for three monthly sets, you will have a set for January, a set for February, and a set for March. In April, the job will overwrite the set from January.

When configuring a rotation the Calendar view displays the schedule graphically. The interval type for each day is displayed in the calendar. Clicking on a day in the calendar will display the type of backup, the write mode, and the name of the media that will be used on that day.

TIP:

You can change the interval for a given day of a schedule by right-clicking on the day in the calendar and selecting the desired type.

You can prevent the job from running on a given day. This is helpful for times when you know the job won't complete because you won't be able to supply the right media for the job — as in the case of holidays.

You can enable or disable jobs from running on specified days of the week by clicking the name of the day in the heading of the calendar view. For example, if you want daily backups on Saturdays.

Implications for Restoring Data

Intervals also define the granularity of the data you can restore. Rotations are set up to capture more granularity in the recent past and less granularity as data gets older. Larger intervals, like Yearly and Monthly, produce lower granularity data history. Smaller intervals, like Daily, produce higher granularity history. Take, for example, a rotation with three full monthly backup sets on the last day of each month, four full weekly backup sets created on each Friday, and four incremental daily backup sets created Monday through Thursday. Now suppose you have a critical file that changes daily. On Wednesday, you are asked to retrieve the file as of a specific date. With this rotation you can roll back to the Monday and Tuesday versions of the file in the current week and the Wednesday, Thursday, and Friday versions of the file in the previous week. Beyond that, you will only have the versions of the file as they existed on Friday for the previous four weeks previous to the current week. And beyond that you will only have the versions of the file that existed on the last day of the month for the previous three months.

The catalog keeps track of the files and versions that have been backed up so you don't have to remember what media they are on. This knowledge makes the restoration process very simple. You only need to specify the files you want restored and Yosemite Server Backup will prompt you for the media it needs restore the files. Full reconstruction of data may require multiple media sets. For example, to reconstruct the data for a Wednesday from a GFS 20 set rotation type, you will require the full backup media set from the previous end of week and all of the incremental media sets from that week (that is, Mondays, Tuesdays and Wednesdays). In some circumstances, the preceding full backup media set will be a monthly or yearly job and not a weekly job. As long as none of these media sets has been overwritten, full data recovery is possible.

NOTE:

When a full backup media set is reused, any incremental or differential backups relative to that full backup will no longer be usable for full system restores. However, files on those media are still recoverable.

NOTE:

Yearly backups only provide you with access to files present on your computer or network on that one day each year. No copy exists for files that were created after the oldest yearly backup and then deleted before the most recent yearly backup. It is the responsibility of the user to manage the retention of media containing critical business data.

Media Rotation Types

In this section

Yosemite Server Backup provides several default media rotation types. These type can be used as is or as examples for creating custom rotations.

NOTE:

Each media set may contain more than one tape or media. Several factors determine how much media you will need: the type of backup being performed (for example full, differential, incremental), the amount of data to be backed up during a full backup, and the media's storage capacity. If the total size of a full backup is larger than the capacity of the tape, additional tapes are required. Your historical usage is the best guide to determining how many tapes these jobs will require.

No Rotation Type

When no rotation type is selected the user may schedule the days to run on but Yosemite Server Backup will not manage the media. The user must supply the desire tapes each time the job runs and will manage the reuse of older media himself.

Fixed Rotation Types

Media sets are named for the interval that has been run. They follow the form *[Interval] Set [number]*.

Fixed by day of week for example of a daily media set is "*1st Monday*."

Fixed by week of month for example of a weekly media set is "*1st Week of the Month*."

Fixed by day of month for example of a monthly media set is "*1st Month*." An example of a yearly media set is "*Yearly 1*."

Fixed by day of year for example of a yearly media set is "First Day of Year 1."

Daily Append

This is a special rotation designed for users with a single backup device. It is the only rotation that appends data to media. It will perform a full backup on the specified day followed by daily incrementals on the remaining weekdays. At the end of the rotation, the user must insert new media for the job to use. This rotation assumes that an entire week of backups will fit on a single media.

Simple and GFS Rotation Types

These rotation types specify combinations of full and incremental backups that efficiently use a specific number of media sets. The main difference between the Simple and the GFS rotations are that only the GFS rotations specify Yearly backups.

Custom

Select this option to create your own rotation.

TIP:

You can select a rotation similar to the desired rotation prior to selecting the custom rotation type and the values from the previously selected rotation will remain as a starting place. The Calendar view is very helpful when creating custom rotations.

Comparing rotation types

Yosemite Server Backup provides a variety of media rotation types to select from. Or, you can define your own media rotation.

The following table compares the historical backups and full data recovery capabilities of each of the rotation types provided in Yosemite Server Backup.

Rotation Type	# of Sets	Yearly Sets	Monthly Sets	Weekly Sets	Daily Sets
Simple	4		1 full	1 full	2 full
Simple	6		2 full	1 full	3 full
Simple	10		3 full	3 full	4 incremental
Simple	11		3 full	4 full	4 incremental
Simple	12		4 full	4 full	4 incremental
Daily Append	N (def. 4)			N full	4 incremental appends
GFS	20	2 full	6 full	6 full	6 incremental
GFS	25	2 full	7 full	8 full	8 incremental
GFS	30	2 full	8 full	8 fill	12 incremental

Running Jobs with Rotations

The info bar displays the **Current rotation set** and the **Next rotation set** in the **Rotation Details** section of the info bar. Before the job is run the first time, both fields have the same value. Once the job runs successfully, the current rotation set field will display the media that has just been used and the next rotation set field displays the media that will be used next.

Initial run The initial run of a rotation job is uses the largest schedule interval in the rotation. For example, suppose a job is configured to use a GFS 20 rotation starting on a Thursday, October 28th, 2010. Even though

a Thursday in the middle of a month would normally be classified as a Daily backup, the first time the job is run, a Yearly backup will be performed.

Missed jobs If, for some reason, a run of the job was missed — for example, because the Domain Server was turned off at the scheduled run time — the scheduler will determine the largest interval missed and run it automatically a few minutes after Yosemite Server Backup starts again.

Failed jobs If a job fails, it will not automatically be run again. However, you can manually rerun by clicking the **Run** command in the command bar.

Pausing and continuing a schedule You can stop a scheduled job from running for a period of time by clicking the **Pause Schedule** command in the command bar. To turn the scheduled job back on, click the **Continue Schedule** command in the command bar. As with the initial and skipped jobs, the scheduler will start again with the largest schedule interval that was skipped.

Forcing a run At times it may be desirable to start a job before it's scheduled time. Clicking the **Run next schedule** command in the command bar will cause the next scheduled interval to be run immediately. The job will not be run again when it's originally scheduled time arrives. And forcing a run to start ahead of schedule will not affect the scheduling of subsequent runs. They will run at their normally scheduled time.

7 Encryption and Compression

In this chapter

- Encryption
- Compression
- Key Management

Encryption

Encryption is the process of changing data into a form that cannot be read until it is deciphered, protecting the data from unauthorized access and use. Company policy normally determines when encryption is required.

For example, it may be mandatory for company confidential and financial data, but not for personal data. Company policy will also define how encryption keys should be generated and managed.

The current version of Yosemite Server Backup provides the user with the ability to encrypt the data that is written to the media and fully implements the Advanced Encryption Standard (AES) for both hardware and software encryption.

- Hardware encryption is supported on some backup devices, such as HP LTO-4 tape drives. It is faster than software encryption and requires no processing on the backup server. The encryption strength is determined by the backup device. HP LTO-4 tape drives always provide strong AES-256 encryption. This feature can be managed by a backup application that supports hardware encryption, such as Yosemite Server Backup.
- Software encryption uses the encryption algorithms available within Yosemite Server Backup. The user selects an encryption strength: Low 56 bit, Medium 128-bit or High 256-bit. Each encryption key size causes the algorithm to behave slightly differently. Increasing software encryption strength makes the data more secure, but requires more processing power.

If your business requires you to use encryption, Yosemite Server Backup allows you to set the required encryption types and levels. This chapter contains important information about data encryption.

Cryptographic Algorithms

Cryptographic algorithms are the basic components of cryptographic applications. It is important to understand that as you increase the complexity of the encryption the information gets closer to impossible to read and the load on your machine, for software-based encryption, will increase.

Software Three cryptographic algorithms are provided. These three settings provide three levels of resistance which require progressively more CPU time to convert the same amount of data. The three options are for the software encryption mode only.

- Low – DES 56-bit
- Medium – AES 128-bit
- High – AES 256-bit

Hardware The cryptographic algorithm provided by hardware devices that provide this feature is not under Yosemite Server Backup control. The hardware provides configuration and operating parameters via a special encryption command. The device driver adjusts its crypto session settings from this input. Hardware encryption is an on/off feature, you do not have the ability to adjust the encryption level through the Yosemite Server Backup interface. By default Yosemite Server Backup will attempt to use the highest encryption algorithm supported on the device, if the device supports multiple algorithms. If the device does not support encryption, the user will be prompted with an alert telling them that the device cannot be used since it does not support hardware encryption.

Passphrase

The passphrase is a series of characters that must be provided by the user for input to the cryptographic key generation process.

- Passphrases must be no less than 8 logical characters. They may be created by the user or randomly generated by a separate application.
- If created by the user, the passphrase should be difficult to guess and should contain a mix of lowercase/uppercase letters, digits and special characters.
- The passphrase is one of the components Yosemite Server Backup uses to generate the encryption key. A longer or random passphrase will increase the strength of the encryption key even more.
- To aid the user in remembering the passphrase, the user may enter a hint message. The use of this field is optional and provided to the user as prompt for remembering the passphrase.
- If a backup job spans multiple media, the same passphrase will be used for all media in the set.

Passphrases for the media are stored in the Yosemite Server Backup catalog. This means the user is able to read and append to the encrypted media without being prompted for a passphrase as long as it is being accessed by the instance of Yosemite Server Backup that first encrypted it

Once a media is deleted or exported from the Yosemite Server Backup catalog the passphrase is also deleted. There are two instances when the user needs to know the passphrase:

- When importing the media to another machine or another instance of Yosemite Server Backup
- During disaster recovery

△ **CAUTION:**

Managing the passphrase is a critical component of any encryption system. Data may be stored for months or years, so passphrases must be archived securely. The user should keep a record or backup of encryption passphrases and store them in a secure place separate from the computer running Yosemite Server Backup. If the user is unable to supply the passphrase when requested to do so, neither the user nor Yosemite Server Backup Support will be able to access the encrypted data.

Encryption Options

Encryption is enabled on the job's **Encryption** page.

Off Both hardware and software encryption are disabled.

Automatic This selection will use hardware encryption, if it is available from the device; otherwise, software encryption will be used

Software Software encryption will be used. When **Software** is selected, the user can choose the strength of software encryption

Hardware Hardware encryption will be used, if the device supports it. If it does not support encryption and this option is selected, the user will be prompted with an alert stating that the device cannot be used since it does not support hardware encryption.

Software Strength Options for the software encryption strength are listed below as three selections, low, medium and high. **Low** is the easiest method to decipher by outside methods, **High** is the hardest method to decipher by outside methods. As you progress from low to high, the encryption algorithm requires more CPU computations for each block of data to be encrypted, which may slow down the data stream to the device and will increase CPU loading on the Media Server.

Encryption passphrase / Verify Passphrase The user supplied portion of the encryption key. Yosemite Server Backup will use this value, along with other information it generates, to calculate an encryption key for the media. The passphrase must be entered twice to minimize the change of making a mistake while typing.

Hint The text entered here will be added to the log file of an import job if the media later needs to be imported and the incorrect passphrase is supplied. Use this field to create a reminder of the passphrase as Yosemite Server Backup cannot recover a lost passphrase.

Key Management

Yosemite Server Backup has adopted a very simple key management strategy. A media is encrypted originally by configuring the job that creates it according to the parameters described above. From that point on, the media is known to the catalog. As long as the media is known, restore jobs may use the media without entering the passphrase again. If a media is unknown — because it was deleted from the catalog or because it came from a different catalog — you must import the media to make it known to the catalog again. The import process required you to supply the passphrase to complete the import. If the passphrase supplied does not match that used to encrypt the media, then the hint supplied at encryption time will be shown in the job log so you can try the import again.

When media is encrypted the media is depicted on the **Jobs and Media** view with a lock on it. The Platinum colored lock indicates hardware, whereas the gold lock indicates software encryption. The Media details window shows the type of encryption used.

Compression

Software encryption disables hardware compression, although you will still be able to select **Software compression.**

If the backup device has hardware compression then performance will be better if only hardware compression is used, and that there is little to no benefit of having both enabled. Enabling software compression in this circumstance will reduce performance.

If **Hardware** encryption is selected, we recommend that **Enable hardware compression** is also selected. Hardware encryption and hardware compression can be used on devices, such as the HP LTO-4 tape drive without any loss of backup speed.

8 Working with Third-Party Applications

In this chapter

Yosemite Server Backup provides agents for protecting a number of popular third-party applications. These agents protect the applications using the application specific backup interfaces provided by the application vendors to ensure complete protection of your data.

Microsoft Exchange Server

In this section

Supported Platforms

The Yosemite Server Backup Agent for Microsoft Exchange supports backup and restore operations for Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 and restoring from Microsoft Exchange Server 5.5 (if backed up with a previous version of Yosemite Server Backup)

Some editions of Yosemite Server Backup do not provide a license to backup Exchange data. By default, an evaluation version of the Yosemite Server Backup agent for Microsoft Exchange is installed automatically when you install Yosemite Server Backup on a Windows server machine that is running Microsoft Exchange. You can use this evaluation license for 60 days. To continue using the agent, contact your sales representative to purchase an edition of Yosemite Server Backupthat supports Application agents.

Configuring a Microsoft Exchange Server

As with any other objects that are configurable in Yosemite Server Backup, you can configure the Microsoft Exchange Server for backups if you have the correct permissions.

1. Open the **Administration** desk bar and select **Catalog** view.
2. Select **Network**, then locate and select the Microsoft Exchange Server on your system.

> **TIP:**
> Switch to the **Folders** view to display a hierarchical tree of the Yosemite Server Backup management domain.

3. Right-click the server and select the **Configuration** command.

Update the following settings that control how Yosemite Server Backup works with Microsoft Exchange Server.

Force Modes As explained in the next section, the **Backup mode** setting of a backup job affects Microsoft Exchange Server databases differently than file types. The **Force modes** settings control how Yosemite Server Backup backs up the databases.

NOTE:

The settings here are only applicable to Microsoft Exchange Server databases; all other file types are backed up in the job's default mode.

For example, if the **Backup mode** of a job is set to **Incremental** and the **Force modes** setting for incremental jobs is set to **Full**, Yosemite Server Backup will back up the Exchange Server databases in **Full** mode, but all other file types in **Incremental** mode.

TIP:

You can use this feature to ensure that the databases are always backed up in full mode, but that other objects are only backed up when changed. This guarantees the greatest security for the most crucial files (that is, the Exchange Server databases), while not making jobs unnecessarily large by not backing up the entire network (that is, by backing up only the changed files).

Full When the **Backup mode** of a job is set to **Full**, Yosemite Server Backup checks this setting to see how the job should be run with Microsoft Exchange Server databases. **Full** is the only possible setting, so the databases will be backed up in this mode. In this case, both the database files and the transaction logs are backed up.

Differential When the **Backup mode** of a job is set to **Differential**, Yosemite Server Backup checks this setting to see how the job should be run with Exchange databases. By default, Yosemite Server Backup runs the job as an incremental job and so only the transaction logs are backed up.

If you want jobs with a **Differential** backup mode to back up both the database files *and* the transaction logs, change this setting to **Full**. In this case, Yosemite Server Backup will treat the Exchange Server databases as if it were running a job in **Full** backup mode.

Incremental When the **Backup mode** of a job is set to **Incremental**, Yosemite Server Backup checks this setting to see how the job should be run with Exchange databases. By default, Yosemite Server Backup runs the job as an incremental job and so only the transaction logs are backed up.

If you want jobs with an **Incremental** backup mode to back up both the database files *and* the transaction logs, change this setting to **Full** . In this case, Yosemite Server Backup will treat the Exchange Server databases as if it were running a job in **Full** backup mode.

Backing up Microsoft Exchange Server

When you use Yosemite Server Backup to back up and restore Microsoft Exchange Server databases, you must pay special attention to the role Windows NT security serves in Microsoft Exchange and the backup mode of the Yosemite Server Backup backup jobs.

Microsoft Exchange and Windows NT Microsoft Exchange uses Windows NT security information for authentication and thus when planning a comprehensive backup program, you must consider the Windows NT operating system as well. Be certain to include backup and restoration of the Windows NT operating system as part of your Microsoft Exchange disaster recovery plan.

Backup modes You can use the **Options** tab of a job to set the **Backup mode** for any type of backup jobs: *full*, *incremental*, *differential* or *copy.* For scheduled automatic rotation jobs, Yosemite Server Backup automatically updates this job setting to the value indicated on the **Schedule** tab of the job.

When the **Backup mode** is set to **Full**, all files selected are backed up, including the entire information store and directory databases. Transaction logs are also backed up and then purged.

When the **Backup mode** is set to **Incremental**, only changes that have occurred since the last backup job are backed up. In particular, for databases, only the .log files are included in the backup job.

△ CAUTION:

These `.log` files are then purged.

When the **Backup mode** is set to **Differential**, for databases, only the `.log` files are included in the backup job, *but these files are not purged.*

When the **Backup mode** is set to **Copy**, Yosemite Server Backup runs the job similar to full backup. However, the transaction logs are not purged at then of a job run in Copy mode.

Backup modes and circular logging Microsoft Exchange Server supports database circular logging. Circular transaction logs differ from normal logs in that only a few log files are maintained. These files are purged automatically as new log files are created. When the transactions in the circular log files are recorded in the database, the log files are then deleted. New transactions are recorded in newly created log files.

If circular logging is enabled, *you cannot do incremental or differential backups.* These backup modes rely upon past transaction logs and thus are not available when circular logging in enabled. When circular logging in enabled, Yosemite Server Backup will revert to *full* backup mode.

You can check to see if circular logging in enabled for a particular server by examining the **Advanced** tab of that server's **Properties** window. If you turn circular logging off, Microsoft Exchange Server will stop the database service and restart it after making the changes.

Restoring Microsoft Exchange Databases

To restore the Microsoft Exchange Server databases, you must restore the database files and all of the log files created since the last full backup job. To do so, you either (1) restore the databases from the last full backup *if the last backup (the previous day's) was a full backup;* (2) restore the databases from the most recent full backup and the last differential backup *if the last backup was a differential backup;* or (3) restore the databases from the last full backup and all of the *incremental* backups made between that day and the present day.

To restore a Microsoft Exchange server, see Disaster Recovery with Microsoft Exchange Server.

NOTE:

When you restore the databases, you must create and run a separate job for each set of transaction logs you need to restore. You cannot skip any logs and the logs must be restored in sequential order. Thus, when recreating the databases, you must first restore the actual databases (created by a backup job running in *full* backup mode). Next, you must restore the transaction logs in the order created *and* in separate jobs. No log can be skipped when restoring.

For example, if you did a *full* backup on Monday and *incremental* backups each day Tuesday through Friday, in order to restore the databases to their state at the close of business Friday, you must run five separate jobs: one restoring the actual databases from Monday's full backup job and then four additional *separate* jobs restoring each transaction log in sequential order, beginning Tuesday and continuing with each log sequentially until Friday.

To restore the Microsoft Exchange Server Databases

1. Find the date of the last full backup of the databases.
2. Create a restore job.
3. On the **Selection** property page, locate and select the Microsoft Exchange Server storage group.
4. In the **Versions of** window, click the **Details** button.

5. Sequentially move through the versions in the Available versions list by date until you find the most recent full backup of the storage group. This version will be selected for restoring when it is selected in the **Available versions** list.
6. Click **OK** to restore that version.
7. If the most recent backup was a full backup, skip the rest of these steps and restart the Microsoft Exchange Server storage group. As the service is restarted, it automatically restores all of the transactions from the transaction logs.
8. If the most recent backup job was a differential job *and you have performed no incremental jobs between the date of the last full backup and the most recent backup*, then create and run a new restore job, selecting the latest version of the storage group. Then restart the Microsoft Exchange Server storage group. As the service is restarted, it automatically restores all of the transaction from the transaction logs.

NOTE:

If you have performed any incremental jobs since the date of the last full backup, continue with the next step.

9. If you have run an incremental backup job after the most recent full backup job, you must create and run a separate restore job for each backup performed after the most recent full backup. Sequentially select versions of the storage group from the **Available versions** field in the **Versions of** window of the storage group. Run and complete each restore job before creating and running a new restore job.
10. Continue to create and run restore jobs until you have restored the latest version of the storage group. Then restart the Microsoft Exchange Server storage group. As the service is restarted, it automatically restores all of the transaction from the transaction logs.

Disaster Recovery with Microsoft Exchange Server

The Yosemite Server Backup Agent for Microsoft Exchange lets you work with databases instead of individual information stores. Each storage group is identified as a single object, which you can back up and restore.

To recover from a disaster, first perform a general system-level disaster recovery to restore the basic system. See Disaster Recovery. Then perform the following steps.

System-level Disaster Recovery

A Microsoft Exchange Server requires the Windows Active Directory to be restored. Microsoft recommends restoring the entire Windows Active Directory system state. Follow the steps below to restore the Windows Active Directory.

1. When Windows restarts the first time after the recovery, the Starting Windows screen appears during startup. Press **F8**.
2. Select **Directory Services Restore Mode** and press **Enter**.
3. Log in to the system.
4. Start Yosemite Server Backup.
5. Create a restore job.
6. Select Active Directory Database for the restore job from the list on the **Selection** page.
7. Run the restore job.
8. Exit Yosemite Server Backup.

Preparing to Restore the Microsoft Exchange Server

1. Restart the computer, letting Windows load normally.
2. Verify that the various Microsoft Exchange services are loaded and running.
3. From the **Windows Start** menu, select **Microsoft Exchange, System Manager**.

4. For each storage group to be restored, dismount and change the properties for each store with a storage group:
   a. Right-click the store within the storage group. A pop-up menu appears.
   b. Select **Properties**. The **Properties** screen appears.
   c. Select the **Database** tab.
   d. Select **This database can be overwritten by a restore**.
   e. Click **OK**.
   f. Right-click the store again. A pop-up menu appears.
   g. Select **Dismount Store**, if the option is available.
   h. Click **Yes** to confirm. The store is dismounted, which means it can be restored.
   i. Exit the System Manager.
5. Access the Exchange Server subdirectory on the computer, for example, `c:\Program Files\Exchsrvr\mdbdata`.
6. Delete all storage group and log files associated with each storage group to be restored.

△ CAUTION:

Do NOT delete the actual subdirectories.

---

7. If you do not have a default installation, use the Exchange system manager to locate the following files and then delete them:
   a. Log file (`.LOG`) for each storage group.
   b. Exchange database (`.EDB`) for each store in the storage group.
   c. Exchange streaming database (`.STM`) for each store in the storage group.

Restoring the Microsoft Exchange MTA Database

1. Restore the Microsoft Exchange MTA (Message Transfer Agent) database.
   a. Access Yosemite Server Backup.
   b. Create a restore job.
   c. Click the Microsoft Exchange Server in the **Folders** panel to display the MTA database, **Queued Messages (MTA)**, in the list in the **Name** column to the right of the **Folders** panel.
   d. Select **Queued Messages (MTA)** from the list in the **Name** column to the right of the **Folders** panel.
   e. Run the restore job.
   f. Exit Yosemite Server Backup.
2. Start the MTA service:
   a. Right-click **My Computer** on the desktop. A pop-up menu appears.
   b. Select **Manage**. The **Computer Management** screen appears.
   c. Expand the `Services and Applications` folder.
   d. Scroll down and right-click on Microsoft Exchange MTA Stacks. A pop-up menu appears.
   e. Select **Start**.
   f. Close the Computer Management screen.

Restoring Microsoft Exchange Databases

1. Restore the appropriate Exchange databases:

a. Access Yosemite Server Backup.

b. Create a restore job.

c. Click the Microsoft Exchange Server in the **Folders** panel to display the storage groups in the list in the **Name** column to the right of the **Folders** panel.

d. Select the storage groups you want to include in the restore job from the list in the **Name** column to the right of the **Folders** panel.

e. Run the restore job.

f. Exit Yosemite Server Backup.

2. Mount the Exchange databases for each storage group that you restored:

a. From the **Start** menu, select **Microsoft Exchange, System Manager**.

b. Right-click the database within the storage group. A pop-up menu appears.

c. Select **Mount**. The system mounts the database.

d. Click **OK**.

e. Exit the System Manager.

Mailbox Backup and Recovery

The Mailbox Agent protects individual Exchange user mailboxes by exporting them as PST files. The agent supports full, differential, copy and incremental backups of selected mailboxes. The mailboxes can be recovered by merging them back into original mailboxes or by restoring them to PST files on disk.

The Exchange Mailbox Agent is intended to protect key mailboxes. The Mailbox Agent can significantly increase the backup time because of the inherent processing overhead of Exchange.

NOTE:

This method does not replace Exchange Database backups which are still required for the recovery of your entire Exchange Database. Mailbox backup supplements Exchange Database backups to enable the quick recovery of individual mailboxes when needed.

Configuration

The Mailbox Agent is disabled by default. This ensures that backups don't accidentally trigger multiple Exchange backups via the Exchange Database Agent and the Mailbox Agent. You can enable the Mailbox Agent by checking Enable Agent on its configuration page. You should specify a working directory location for Import/Export operation of mailboxes. The working location defaults to the Product "temp" directory.

Once enabled, the Administrator displays all Mailboxes under the Exchange Mailbox Agent and makes them selectable for backup.

Backing Up Mailboxes

The Backup process begins by exporting each selected mailbox as a PST file, one at a time, to the working directory. If sufficient disk space is not available for the operation in the working location, the backup fails and displays an error message. After a mailbox file is backed up, it is removed from the working directory to free up disk space. and the working directory is not backed up. You can configure the location of the working directory on the Agent's configuration page.

You can configure the Mailbox Agent to do full, copy, differential, or incremental backups of Exchange mailboxes by setting the backup job Mode.

Restoring Mailboxes

Mailboxes are recovered by restoring them to the working directory, then importing them to the Exchange Database, merging items with the original mailbox. Insufficient disk space in the working location causes the backup to fail and displays an error message. Exchange Server automatically skips the mailbox items that already exist and only restores missing items. Once mailbox items are imported to the mailbox, the temporary PST file is deleted from the working directory.

If you specify a folder name on the Agent's configuration page, the mailbox items will be recovered to this folder in the original mailbox.

Mailboxes can also be restored to a PST file on the File System. You can view the contents of the mailbox by using an Exchange client, such as Microsoft Outlook. This is useful when the Exchange Server environment is down and unable to host the mailboxes.

Mailboxes must be explicitly selected. If a user selects an entire machine for restore, the normal Exchange Mailbox Databases will be restored, but individual mailboxes will not be restored. Also, if one or more Exchange Databases are selected for recovery via the Exchange Server Agent, the restore job skips the mailboxes selected under the Mailbox Agent, as those will be restored from the Exchange Database.

Mailboxes that have been deleted from Exchange Server require you to create the mailbox in the Exchange Server before restoring the Mailbox items using the Mailbox Agent. A nonexistent mailbox cannot be restored.

Disaster Recovery

Mailboxes will not be restored during Bare Metal Disaster Recovery. To restore mailboxes, create a new restore job after Disaster Recovery completes, and select the necessary mailboxes to recover.

Requirements

Working Location

A working location must be specified on the Agent's configuration page. This location stores the temporary files generated during mailbox Import and Export operations. Free space in this location must be at least the size of the largest Mailbox in the Exchange Server. Once each operation completes, the temporary file is automatically deleted.

"Exchange Trusted Subsystem" must have Read/Write permissions to the working directory.

The working location defaults to Product "temp" directory.

Supported Exchange Server versions

Exchange Server 2010 SP1 is the minimum supported version.

Mailbox Permissions

An Active Directory User or a Group must be granted "Mailbox Import Export" role. Typically, running as Administrator, the product service already has necessary permissions for the mailboxes.

To manually grant this role, execute the following cmdlet in the Exchange Management Shell

Example 1. New-ManagementRoleAssignment –Role "Mailbox Import Export" –User Domain\User

Where, Domain is the Active Directory Domain name and User is the account granted permissions.

To grant necessary permissions to a group use:

Example 2. New-ManagementRoleAssignment -Role "Mailbox Import Export" -Name "Import Export Mailbox Admins" -SecurityGroup "Mailbox Support"

PowerShell Access

If the product service is running under an account that does not have access to PowerShell, you need to specify a valid account with permission to execute PowerShell cmdlets. Typically, running as the default, Local System account, the product service automatically has access to PowerShell.

Best Practices and Performance Considerations

You should perform frequent incremental backups of Exchange mailboxes in addition to full backups. Daily incremental backups followed by weekly full backups will reduce the recovery time and the backup size. Incremental backups also enable you to conveniently specify a restore window to recover mailbox items.

Consider the case where you wish to recover a few deleted messages from your inbox after the retention period has expired on the Exchange Server. If you know the date the original emails were sent or received, you can be back in action within seconds of running the mailbox restore. However, if you only had full backups of the mailbox, you would be forced to restore the entire mailbox, whose size could run to several gigabytes, so it would require a much longer restore time.

Backup performance is dependent on a number of factors including but not limited to:

1. Mailboxes in the Exchange Sever
2. Count of mail items in each mailbox
3. Type of Backup (Full, Copy, Differential, Incremental)
4. Hardware powering the Exchange Server deployment

There are no special requirements to improve backup performance of the Mailbox Agent. However, backup performance can be optimized by selecting only essential mailboxes from the Agent and performing incremental backups on a regular basis.

Working with Microsoft SQL Server

In this chapter

Overview

This section contains important information pertaining to backing up and restoring Microsoft SQL Server database instances. If you are using Yosemite Server Backup to back up and restore SQL Server database instances, be sure read these instructions carefully.

Supported platforms

The Yosemite Server Backup Agent for Microsoft SQL Server supports Microsoft SQL Server 7 and Microsoft SQL Server 2000.

Some editions of Yosemite Server Backup do not provide a license to backup Microsoft SQL data. By default, an evaluation version of the Yosemite Server Backup agent is installed automatically when you install Yosemite Server Backup on each Windows server. You can use this evaluation license for 60 days. To continue using

the agent, contact your sales representative to purchase an edition of Yosemite Server Backupthat supports Application agents.

Microsoft SQL server concepts

Microsoft SQL Server environments are frequently mission-critical and must be maintained 24 hours a day, seven days a week. Procedures and plans must be in place to ensure the quick recovery of data in the event of data loss.

Using the transaction logs associated with each database, you can quickly recover your databases. Transactions that were not committed can be rolled back, while transactions that were committed can be written to disk.

While transaction logs assure that only committed transactions are written and restored, in order to use them correctly, you must have a comprehensive backup plan that regularly backs up these logs. Additionally, when you reconstruct a database, you must restore the database files and logs using only the procedures set out below.

Configuring the Microsoft SQL Server

You can configure any Yosemite Server Backup feature by selecting the object from the **Catalog** view and updating information on its property pages.

1. Select the **Administration** desk bar and open the **Catalog** view.
2. Select **Network**, then select the Microsoft SQL Server on your system.
3. Expand the object until you see a list of database instances.

TIP:

Switch to the **Folders** view to display a hierarchical tree of the Yosemite Server Backup management domain.

---

4. Right-click the database instance and display its property pages.
5. Select the **Configuration** command to display the **Configuration** page.

NOTE:

We recommend that you use the default values on the **Configuration** page.

User name Yosemite Server Backup sends this name to Microsoft SQL Server whenever the SQL administrator user name is required. Type the Microsoft SQL administrator name in this field. The default is **sa**.

Password Yosemite Server Backup sends this SQL administrator password to Microsoft SQL Server with the SQL administrator's user name whenever required. There is no default value.

Force Modes As explained in the next section, the Backup mode setting of a backup job affects Microsoft SQL Server database instances differently than file types. The Force modes settings control how Yosemite Server Backup backs up the database instances.

NOTE:

The settings here are only applicable to Microsoft SQL Server database instances; all other file types are backed up in the job's default mode.

For example, if the **Backup mode** of a job is set to **Incremental** and the **Force modes** setting for incremental jobs is set to **Full** , Yosemite Server Backup will back up the SQL Server database instance in **Full** mode, but all other file types in **Incremental** mode

.

TIP:

You can use this feature to ensure that the databases in the instance are always backed up in full mode, but that other files are only backed up when changed. This guarantees the greatest security for the most crucial files that is, the SQL Server database instances, while not making jobs unnecessarily large by not backing up the entire network that is, by backing up only the changed files.

Full When the **Backup mode** of a job is set to **Full**, Yosemite Server Backup checks this setting to see how the job should be run with SQL database instances. **Full** is the only possible setting, so the database instances will be backed up in this mode. In this case, both the databases and the transaction logs are backed up.

Differential When the **Backup mode** of a job is set to **Differential**, Yosemite Server Backup checks this setting to see how the job should be run with SQL database instances. By default, Yosemite Server Backup runs the jobs as an incremental job and so only the transaction logs are backed up.

NOTE:

There is no distinct **Differential** job mode for SQL Sever database instances.

If you want jobs with a **Differential** backup mode to back up both the database and the transaction logs, change this setting to **Full**. In this case, Yosemite Server Backup will treat the SQL Server database instances as if it were running a job in **Full** backup mode.

Incremental When the **Backup mode** of a job is set to **Incremental** , Yosemite Server Backup checks this setting to see how the job should be run with SQL databases. By default, Yosemite Server Backup runs the jobs as an incremental job and so only the transaction logs are backed up.

If you want jobs with an **Incremental** backup mode to back up both the database and the transaction logs, change this setting to **Full**. In this case, Yosemite Server Backup will treat the SQL Server database files as if it were running a job in **Full** backup mode.

Backuping up Microsoft SQL Server

Two additional concerns are present when you back up SQL Server database instances: setting the **Backup mode** of a job to either **Full**, **Incremental ,** or **Differential**; and configuring Yosemite Server Backup to work with SQL Server's default backup routine.

NOTE:

Anytime Yosemite Server Backup returns an error message that is greater than 10000, a Microsoft SQL or Exchange error has occurred. Refer to your Microsoft documentation for more information as this is a Microsoft error code.

Microsoft SQL Server Databases and the backup mode

The **Backup mode** on the **Option s** tab of a job that backs up SQL Server database instances is especially critical.

Backup modes When the **Full** setting is selected, all files selected for backup are backed up, including SQL Server database instances and databases. However, when either the **Incremental** or **Differential** option is selected, Yosemite Server Backup backs up only the transaction logs for each database.

CAUTION:

There is no difference between **Incremental** and **Differential** jobs for SQL Server databases.

When the **Backup mode** is set to **Copy**, Yosemite Server Backup a creates a full backup of the database but does not truncate the logs.

Additional Conditions Master, Model, MSDB and Pubs databases support only full backups. The **Backup mode** option is automatically set to **Full** when backing up these databases.

If you set a job to run in either **Incremental** or **Differential** mode and the job can only run as a full backup (as a result of the provision above), the job will fail to run on each of its initial passes, but will run in **Full** backup mode on its final pass.

Using Yosemite Server Backup with SQL Server's Backup Routine

Microsoft SQL Server has default utilities and commands for backing up data. When you use Yosemite Server Backup to back up SQL Server databases, you can still use these default SQL Server utilities and commands.

For example, you can use the DUMP command to dump transaction logs to the dump device (preferably, a separate disk drive). You can set this up to occur at regular intervals, such as every 15 minutes or every hour. Next, you can create a backup job that backs up these transaction logs onto archival media every day.

In general, when you implement Yosemite Server Backup to back up your SQL Server databases, continue to use SQL Server's internal commands to duplicate and back up transaction logs. Set up a separate Yosemite Server Backup backup job to write these duplicated transaction logs to archival media.

Restoring Microsoft SQL Server

When restoring SQL Server databases, you must:

1. Restore a full backup of the SQL Server database.
2. Restore the logs in the order created.
3. Follow special procedures when renaming databases (if you rename databases).

> **NOTE:**
>
> Any time Yosemite Server Backup returns an error message that is greater than 10000, a Microsoft SQL or Exchange error has occurred. Refer to your Microsoft documentation for more information as this is a Microsoft error code.

Restoring Microsoft SQL Server databases and transaction logs When recreating a database, you must first restore the whole database (created by a backup job running in *full* backup mode).

Next, you must restore the transaction logs in the order created *and* in separate jobs. No log can be skipped when restoring.

For example, if you did a *full* backup on Monday and *incremental* backups each day Tuesday through Friday, you must run five separate jobs: one restoring the database from Monday's full backup job and then four additional *separate* jobs restoring each transaction log in sequential order, beginning Tuesday and continuing with each log sequentially until Friday.

You do not have to follow these procedures when restoring databases backed up with *full* backup jobs. (**Full** backup jobs back up the entire database, while **Incremental** and **Differential** jobs only back up the database logs.)

Restoring Microsoft SQL Server user databases

To restore a database, begin by restoring the most recent **full** backup of the database, followed by *all* the database logs, that is, backups made with the **Backup mode** set to either **incremental** or **differential**.

When a database is restored, if the database does not yet exist, Yosemite Server Backup will create the database where the database was originally located.

To restore a lost or damaged database

1. If the transaction log of the damaged or inaccessible user database is on an undamaged device, make a backup of the transactions before proceeding. (This lets you preserve up to the minute transactions that are not included on the backup tape.)

   You may use either a DUMP TRANSACTION statement on the SQL server or use a Yosemite Server Backup **Incremental** backup job to back up only the transactions logs.

2. If you are restoring the database because the data in the database is no longer needed or is incorrect, skip to step 3. The following instructions are for recreating database devices and the database which had existed previously.

   During the restore processes, Yosemite Server Backup will recreate the database and all segments exactly as they existed when the backup was performed.

   To do this, Yosemite Server Backup first determines if the database exists. If the database does exist, Yosemite Server Backup will use the database as is *without any further processing or changes*.

3. If the database does not exist, Yosemite Server Backup next identifies the database devices on which the database was originally located. If the appropriate database *device* already exists, Yosemite Server Backup will use that device as is without further processing.

   If the database *device* does not exist, Yosemite Server Backup *recreates* the database device at its *original* location and with its original size. After all the database devices are created, Yosemite Server Backup then creates the database with all the original options at the original locations.

TIP:

This method makes disaster recovery simple. The user simply create a restore job and allows Yosemite Server Backup to recreate whatever is needed in order to successfully restore the database.

NOTE:

If a disk drive fails and is not replaced, Yosemite Server Backup will be unable to restore your database because it will be unable to recreate a database device.

For example, if a segment of your database resides on a database named 'DATA' at `D:\MSSQL\DATA\DATA.DAT`, if `D:` is lost and not replaced, when Yosemite Server Backup attempts to recreate the database device, it will fail, since `D:` no longer exists.

To avoid this problem, manually recreate the database device at some other valid location. It must be at least as large as the original database device since Yosemite Server Backup will attempt to create a database segment on it the same size as the original database.

An alternative method is to manually create the entire database itself. Thus, when Yosemite Server Backup attempts to restore the database, since the database already exists, it will use that preexisting database. This allows you to restore a database in a new location, since Yosemite Server Backup does not check to see if it is the original device before restoring the database, because the database already exists.

NOTE:

An alternative method is to manually create the entire database itself. Thus, when Yosemite Server Backup attempts to restore the database, since the database already exists, it will use that preexisting database. This allows you to restore a database in a new location, since Yosemite Server Backup does not check to see if it is the original device before restoring the database, because the database already exists.

Using Yosemite Server Backup, create a restore job and run the job to restore the database. You must start with a full backup version of the database to restore which was created using a Full backup job.

4. Create additional restore jobs to restore each transaction log backed up after the full database you restored. You must create and run a separate restore job for each transaction log.

   For example, if you ran a full backup on Friday and incremental jobs (that is, jobs that backed up only the transaction logs) on the following Monday and Tuesday, you must first restore the database using Friday's version of the database. Next, create a run and restore job that restores Monday's version (Monday's transaction log). Finally, create and run a job that restores Tuesday's version (Tuesday's transaction log).

   In the *last* incremental restore job, click the **Advanced Options** button and select the **Finalize recovery of MS SQL databases** check box. If you do not select this check box, the database will be offline.

Restoring Microsoft SQL Server master databases

A damaged master database is evident by the failure of the SQL Server to start, by segmentation faults or input/output errors or by a report from DBCC. An example of an error might be damage caused by media failure in the area in which master database is stored.

The procedure used to recover a damaged master database is different from the procedure used to recover user databases. If the master database becomes unusable, it must be restored from a previous dump. All changes made to the master database after the last dump are lost when the dump is reloaded and therefore must be reapplied.

It is strongly recommended that the master database be backed up each time it is changed. This is best accomplished by prohibiting the creation of user-defined objects in the master database and by being aware of the statements and system procedures, and the equivalent actions in SQL Server Management Studio, that modify it.

Please refer to the documentation for Microsoft SQL Server for information on the proper way to restore the master databases.

Restoring Microsoft SQL Server 2000 master databases

A damaged master database is evident by the failure of the SQL Server to start, by segmentation faults or input/output errors or by a report from DBCC. An example of an error might be damage caused by media failure in the area in which master database is stored.

The procedure used to recover a damaged master database is different from the procedure used to recover user databases. If the master database becomes unusable, it must be restored from a previous dump. All changes made to the master database after the last dump are lost when the dump is reloaded and therefore must be reapplied.

It is strongly recommended that the master database be backed up each time it is changed. This is best accomplished by prohibiting the creation of user-defined objects in the master database and by being aware of the statements and system procedures, and the equivalent actions in SQL Enterprise Manager, that modify it.

The most common statements and system procedures that modify master are:

- `CREATE DATABASE`
- `ALTER DATABASE`
- `sp_dropremotelogin`
- `sp_addumpdevice`
- `sp_dropdevice`
- `sp_addlogin`
- `sp_droplogin`
- `sp_addserver`
- `sp_dropserver`
- `sp_addremotelogin`

If a user database is created, expanded or shrunk after the most recent dump (backup) of the master database and if it becomes necessary to reload the master database, then that user database and all data in will be lost and must be restored from backup.

△ CAUTION:

Because of this, always dump (back up) the master database after creating, expanding or shrinking user databases.

To recover a damaged master database

1. Stop the Yosemite Server Backup and SQL Server services
2. Rebuild the master database
3. Restart SQL Server in single-user mode
4. Restore the master database from the most recent backup
5. Apply changes to the master database any changes that were not included in the most recent backup.
6. Drop invalid databases from the newly restored master database.
7. Start the Yosemite Server Backup and SQL Server services
8. Restore the msdb database

Each of these steps is described below in more detail.

Stop the Yosemite Server Backup and SQL Server services

1. Exit Yosemite Server Backup.
2. Stop the Yosemite Server Backup service by using one of the following methods:
   a. Using the Windows Command Line
      i. Open a command prompt.
      ii. Switch to the following directory:

      ```
      C:\Program Files\Barracuda\Yosemite Server Backup
      ```

      iii. Type the following command at the command prompt:

      ```
      ytwinsvc -x
      ```

      This command stops the Yosemite Server Backup service on the local machine.
   b. Using the Microsoft Management Console (MMC):
      i. Right-click the **My Computer** icon and select **Manage**.
      ii. In the left pane of the window, select **Services and Applications Services**.
      iii. In the right pane of the window, locate the Yosemite Server Backup service.
      iv. Right-click the service and select **Stop**.
3. Stop the SQL Server service using the SQL Server Enterprise Manager.

Rebuild the master database

1. Open a command prompt.
2. Switch to the `Program Files\Microsoft SQL Server\80\Tools\Binn` directory.
3. Run `Rebuildm.exe`.
4. In the **Rebuild Master** dialog box, click **Browse**.
5. In the **Browse for Folder** dialog box, select the `\Data` folder on the SQL Server 2000 compact disc or in the shared network directory from which SQL Server 2000 was installed, and then click **OK**.

6. Click **Settings**. In the **Collation Settings** dialog box, verify or change settings used for the master database and all other databases.

   Initially, the default collation settings are shown, but these may not match the collation selected during setup. You can select the same settings used during setup or select new collation settings. When done, click **OK**.

7. In the **Rebuild Master** dialog box, click **Rebuild** to start the process.

NOTE:

To continue, you may need to stop a server that is running.

The Rebuild Master utility reinstalls the master database.

Restart SQL Server in single-user mode

1. Open a command prompt.
2. Switch to the `Program Files\Microsoft SQL Server\mssql\binn` directory.
3. Issue the following command:

   ```
   sqlservr -c -m
   ```

   If you are restoring the master database for a named instance, issue the following command instead:

   ```
   sqlservr -c -m -s name
   ```

   where name is the name of the named instance.
4. Leave the command prompt open.

Restore the master database from the most recent backup

1. Open Yosemite Server Backup with the service stopped.
2. Create a restore job, selecting only the master database.
3. Run the restore job.

NOTE:

This may take some time, typically 10 to 15 minutes, depending on the size of the master database. Restore only the master database while in single user mode. Do not restore any other databases.

If for some reason, your restore operation doesn't work, rebuild the master database and attach all of your databases that reside in the data directory. To attach databases:

- In Enterprise Manager, right-click Databases and select Attach Database.
- In Query Analyzer, write and run a script that is similar to the following sample:

```
EXEC sp_attach_db @dbname = N'test_database', @filename1 =
N'c:\Program Files\Microsoft SQL Server\MSSQL\Data\test_data-
base.mdf', @filename2 = N'c:\Program Files\Microsoft SQL
Server\MSSQL\Data\test_database.ldf'
```

Apply changes to the master database

1. Go to the SQL Server Manager and right-click the SQL server instance. Select **Properties** to open the SQL Server Properties window.
2. Under the **General** tab in the SQL Server Properties window, open the Startup Parameters window and remove "–m" from the list of existing parameters.
3. Restart the SQL server instance. (Right-click the SQL server instance and select **Stop**; right-click the SQL server instance and select **Start**.)

   If there have been no changes to the master database since the last dump, then proceed to Drop invalid databases

4. If login IDs or devices have been added to or dropped from the master database since the last backup, those changes must be reapplied. Restart the server and reapply the changes manually or from saved batch files.
5. If databases have been created, expanded or shrunk since the last dump of master, those databases must be dropped and then restored.

Drop invalid databases

- Use the SQL Enterprise manager to drop any invalid database devices and databases from the newly restored master database.

NOTE:

If you are recovering from a disaster where you have lost a database device file, the master database you have just restored still contains a reference to it. Yosemite Server Backup will not be able to restore any databases contained on the database device until the file is restored or the database device is dropped. If the database device is dropped, Yosemite Server Backup will automatically recreate the device when a database contained on the device is restored.

Start the Yosemite Server Backup and SQL Server services

1. Start the Yosemite Server Backup service by using one of the following methods:
   a. Using the Windows Command Line
      i. Open a command prompt.
      ii. Switch to the following directory:

      ```
      C:\Program Files\Barracuda\Yosemite Server Backup
      ```

      iii. Type the following command at the command prompt:

      ```
      ytwinsvc -s
      ```

      This command starts the Yosemite Server Backup service on the local machine.
   b. Using the Microsoft Management Console (MMC)
      i. Right-click the **My Computer** icon and select **Manage**.
      ii. In the left pane of the window, select **Services and Applications Services**.
      iii. In the right pane of the window, locate the Yosemite Server Backup service.
      iv. Right-click the service and select **Start**.
2. Restart the SQL Server service using the SQL Server Enterprise Manager.

Restore the msdb database

When restoring the msdb database, keep the following considerations in mind:

- The msdb database supports SQL Executive and provides a storage area for scheduling information. The schedules that you implement using SQL Enterprise Manager are maintained in the msdb database. This includes such things as the tasks that you schedule from the Task Scheduling window, the automatic backups you schedule from the Database Backup/Restore window and all replication tasks, which are automatically created by the system if the server is configured as a replication distributor.
- During installation of a server, the setup program automatically creates two devices (of 2MB and 1MB) on the same disk drive as the master database and then places the msdb database on the 2MB device (MSDBDATA) and its transaction log on the 1MB device (MSDBLOG). Scheduling information is then stored in this database.
- During a rebuild of the master database, the setup program drops and re-creates the msdb database, which results in a loss of all scheduling information.

Restoring Microsoft SQL Server 7 master databases

A damaged master database is evident by the failure of the SQL Server to start, by segmentation faults or input/output errors or by a report from DBCC. An example of an error might be damage caused by media failure in the area in which master database is stored.

The procedure used to recover a damaged master database is different from the procedure used to recover user databases. If the master database becomes unusable, it must be restored from a previous dump. All changes made to the master database after the last dump are lost when the dump is reloaded and therefore must be reapplied.

It is strongly recommended that the master database be backed up each time it is changed. This is best accomplished by prohibiting the creation of user-defined objects in the master database and by being aware of the statements and system procedures, and the equivalent actions in SQL Enterprise Manager, that modify it.

The most common statements and system procedures that modify master are:

- `DISK INIT`
- `CREATE DATABASE`
- `ALTER DATABASE`
- `DISK MIRROR`
- `DISK UNMIRROR`
- `DISK REMIRROR`
- `sp_dropremotelogin`
- `sp_addumpdevice`
- `sp_dropdevice`
- `sp_addlogin`
- `sp_droplogin`
- `sp_addserver`
- `sp_dropserver`
- `sp_addremotelogin`

If a user database is created, expanded or shrunk after the most recent dump (backup) of the master database and if it becomes necessary to reload the master database, then that user database and all data in will be lost and must be restored from backup.

△ **CAUTION:**

Because of this, always dump (back up) the master database after creating, expanding or shrinking user databases.

△ **CAUTION:**

You must rebuild using the same character set and sort order as the master database dump that will be reloaded

To recover a damaged master database

- Rebuild the master database
- Restart Microsoft SQL Server in single-user mode
- Restore the master database from the most recent backup
- Apply changes to the master database
- Drop invalid databases and database devices
- Restore the msdb database

Each of these six steps is described below in more detail:

Rebuild the master database

1. From Windows Explorer select **Start** > **Programs** > **Microsoft SQL Server** then select the **SQL Setup** icon.

   (Alternatively, from the distribution media, from the directory containing the software compatible with your hardware platform's processor architecture, run `SETUP.EXE`.)

2. Respond to the on-screen instructions until the **Options** window appears.
3. Select **Rebuild Master Database** and click **Continue**. A confirmation window appears.
4. Click **Resume**. The **Rebuild Options** window appears.
5. To specify the character set, click **Sets** and complete the **Select Character Set** window that appears. Skip this step if you are using the default character set (ISO 8859-1).

NOTE:

You must use the same character set and sort order that were previously used for this master database.

---

6. To specify the sort order, click **Orders** and complete the **Select Sort Order** window that appears. Skip this step if you are using the default sort order (dictionary order, case-insensitive).
7. In the **Rebuild Options** window, click **Continue**. The **SQL Server Installation Path** window appears.
8. If not correctly displayed in the **SQL Server Installation Path** window, enter the location of the existing SQL Server installation and click **Continue**.

   The Rebuild Master Database window appears.

9. If it is not correctly displayed in the Rebuild Master Database window, enter the location and name of the existing MASTER device. Also enter a MASTER device size and click **Continue**.

   The setup program will then rebuild the master database.

10. When rebuilding is complete and the completion window appears, click **Exit**.

NOTE:

The files `MASTER.DA@` and `MASTER.AL@` are stored in the `\MSSQL\INSTALL` directory. When rebuilding the master database (or when installing SQL Server), one of these two files is used by the setup program. When the default sort order and character set are selected, `MASTER.DA@` is expanded and copied onto the server, replacing `MASTER.DAT`. When an alternate character set and/or sort order is selected, `MASTER.AL@` is expanded, copied onto the server, and several SQL scripts are run.

Restart Microsoft SQL Server in single-user mode

Before you can restore the master database, you must start Microsoft SQL Server in single-user mode.

1. Go to the **SQL Server Manage**r and right-click the SQL server instance. Select **Properties** to open the **SQL Server Properties** window.
2. Under the **General** tab in the SQL Server Properties window, open the Startup Parameters window and type "–m" in the Parameter field.
3. Click the **Add** command, and then click **OK**. Close the SQL Server Properties window by clicking **OK**.
4. Restart the SQL server instance. (Right-click the SQL server instance and select **Stop**; right-click the SQL server instance and select **Start**.)

NOTE:

You may find it convenient to start the SQL Server in single-user mode using the command line program, `SQLSERVER.EXE`, with option "/m". This procedure will only work, however, if the SQL Server is configured to start using the current interactive user's account.

Restore the master database from the most recent backup

1. Create a restore job and select the most recent backup version of the master database.
2. Run the restore job.

NOTE:

This may take some time, typically 10 to 15 minutes, depending on the size of the master database. Restore only the master database while in single user mode. Do not restore any other databases.

Apply changes to the master database

1. Go to the SQL Server Enterprise Manger and right-click the SQL server instance. Select Properties to open the SQL Server Properties window.
2. Under the **General** tab in the SQL Server Properties window, open the Startup Parameters window and remove "–m" from the list of existing parameters.
3. Restart the SQL server instance. (Right-click the SQL server instance and select **Stop**; right-click the SQL server instance and select **Start**.)

   If there have been no changes to the master database since the last dump, then proceed to Drop invalid databases and database devices
4. If login IDs or devices have been added to or dropped from the master database since the last backup, those changes must be reapplied. Restart the server and reapply the changes manually or from saved batch files.
5. If databases have been created, expanded or shrunk since the last dump of master, those databases must be dropped and then restored.
6. If you have made many changes and have no recent dump, it is possible that by reloading master in some cases you can regain data in user databases that has been lost. This technique requires the use of `DISK REINIT` and `DISK REFIT` and can involve manual modifications to the master database tables.

   - Use `DISK REINIT` to recreate rows in sysdevices for all database devices that have been added after the most recent dump. `DISK REINIT` updates sysdevices just as `DISK INIT` does, but it does not format the physical disk file, so existing data is preserved.
   - Use `DISK REFIT` to recreate rows in sysusages and sysdatabases for all `CREATE` and `ALTER DATABASE` statements that were performed after the most recent dump.
   - `DISK REFIT` scans the physical file associated with each space that is allocated to databases. It also adds the corresponding sysdatabases entries. Some of the information is not reconstructed perfectly.

     For example, the original virtual device number is not assigned, because it is not known. Instead, virtual device numbers are assigned sequentially. The database owner is not extracted while scanning the physical files; ownership is set to the system administrator. It is also not possible to determine how many sysusages entries originally existed. `DISK REFIT` inserts a separate entry for each different segment type.

   - When this is done, correct the entries made by `DISK REFIT` to sysdatabases and sysusages (if desired) and also add to syslogins any login IDs that were not retained. Then shut down and restart SQL Server.

△ CAUTION:

Capturing the latest changes made to a database by using `DISK REFIT` and `DISK REINIT` to recreate the master database is possible, but it is preferable to keep the master database current by dumping it after creating or altering databases. Using `DISK REFIT` and `DISK REINIT` is a complicated process that can result in data loss because many of the changes made to a database often must be reconstructed manually in the master database. If you feel this technique is necessary, contact your primary support provider before beginning the recovery process.

Drop invalid databases and database devices

- Use the SQL Enterprise manager to drop any invalid database devices and databases from the newly restored master database.

NOTE:

If you are recovering from a disaster where you have lost a database device file, the master database you have just restored still contains a reference to it. Yosemite Server Backup will not be able to restore any databases contained on the database device until the file is restored or the database device is dropped. If the database device is dropped, Yosemite Server Backup will automatically recreate the device when a database contained on the device is restored.

Restore the msdb database

When restoring the msdb database, keep the following considerations in mind:

- The msdb database supports SQL Executive and provides a storage area for scheduling information. The schedules that you implement using SQL Enterprise Manager are maintained in the msdb database. This includes such things as the tasks that you schedule from the Task Scheduling window, the automatic backups you schedule from the Database Backup/Restore window and all replication tasks, which are automatically created by the system if the server is configured as a replication distributor.
- During installation of a server, the setup program automatically creates two devices (of 2MB and 1MB) on the same disk drive as the master database and then places the msdb database on the 2MB device (MSDBDATA) and its transaction log on the 1MB device (MSDBLOG). Scheduling information is then stored in this database.
- During a rebuild of the master database, the setup program drops and recreates the msdb database, which results in a loss of all scheduling information.

Protecting Microsoft Windows SharePoint Services

In this section

Overview

This section contains information for the backup and restore of Windows SharePoint Services.

Windows SharePoint Services protection concepts

Microsoft Windows SharePoint Services is a free component of certain Windows Server operating systems. Microsoft SharePoint Portal Server is a web-based collaboration application that runs on Microsoft Windows and uses SharePoint Services. SharePoint Services uses a Microsoft SQL Server database for storing data and metadata. The version of SQL Server depends upon the installation and whether SharePoint Portal Server is

installed. Windows SharePoint Services uses a special version of MSDE, known as SQL Server 2000 Desktop Engine (Windows) or WMSDE. If SharePoint Portal Server is installed, SQL Server 2000 Desktop Engine (MSDE) or SQL Server 2000 is used instead.

Yosemite Server Backup will automatically discover all SharePoint Services databases and manage them for backup and recovery as separate objects. Backing up an entire system will also include those databases.

If you are using Microsoft SharePoint Portal Server or Microsoft Office SharePoint Server, you need to use the Yosemite Server Backup Agent for Microsoft SQL Server to protect the SQL Server database.

Protecting Windows SharePoint Services

Yosemite Server Backup is designed specifically to protect the databases of Windows SharePoint Services. These databases will appear in the Yosemite Server Backup Administrator GUI with the name of the database instance. This name will depend on the version of SharePoint Services that is installed. When using SharePoint 2.0 “SHAREPOINT” is the default name. When using SharePoint Services 3.0, “Microsoft ##SSEE” is the default name. In addition to storing Web site content in a WMSDE/SSEE SQL database, Windows SharePoint Services stores certain files including Windows SharePoint Services virtual server configuration, style sheets (CSS), themes, and customization information for site definitions are stored in the SharePoint installation directory on the file system.

Regular backups of the “SHAREPOINT” databases in conjunction with File System backup will ensure protection and integrity of SharePoint Services virtual servers, the document repository, users, security settings, and permissions.

IMPORTANT:

It is recommended that the user enable Microsoft Windows Volume Shadow Copy Service (VSS) option for backup jobs when creating DR backup sets. Enabling the VSS option will ensure that the user can restore all WSS components in a consistent state during the disaster recovery process.

NOTE:

The instructions for the additional steps are outlined in the Disaster Recovery section of this appendix.

To allow a consistent restore the backup set for WSS must include the following components (if you select the entire system for backup, these components are all included):

1. WSS Installation directory This directory and its sub directories, `%BootVolume%\program files\Common Files\Microsoft Common Shared\web server extensions\12`, contain WSS installation and configuration files including binaries, site templates, style sheets, customization information for site definitions, etc.
2. Microsoft Internet Information Server (IIS) Virtual Servers WSS uses one or more virtual servers to host Web sites. Unlike ASP.NET, it does not configure each Web site using an IIS virtual directory. Alternately, WSS tracks all configuration information for WSS Web sites inside the configuration database and content databases. This implies that a backup of the configuration database will be required to ensure the protection of all SharePoint extended virtual servers.
3. WSS Databases By default, WSS installs a WMSDE/SSEE instance called SHAREPOINT or Microsoft ##SSEE and creates databases including a configuration database and a content database. The SHAREPOINT database instance can be backed up by selecting the instance in the Yosemite Server Backup Administrator GUI.
4. Usage Analysis logs Usage analysis for WSS allows one to track how Web sites on your server are being used. If usage analysis logging process is enabled, WSS log files are created daily to track usage information. These log files are stored in `%WinDir%\system32\LogFiles\STS` directory.

NOTE:

This path can be customized. In this case, one should add the appropriate path to the backup selection list.

5. Select the **Windows SharePoint SQL Databases** icon in the selection tree and expand the tree.
6. Select the server that houses Windows SharePoint Services and expand the tree until you are able to select the SharePoint database.

Restoring SharePoint Services

To restore Windows SharePoint Services you will need to select the following:

1. WSS Installation directory This directory and its sub directories, `%BootVolume%\program files\Common Files\Microsoft Common Shared\web server extensions\12`, contain WSS installation and configuration files including binaries, site templates, style sheets, customization information for site definitions, etc.
2. Microsoft Internet Information Server (IIS) Virtual Servers WSS uses one or more virtual servers to host Web sites. Unlike ASP.NET, it does not configure each Web site using an IIS virtual directory. Alternately, WSS tracks all configuration information for WSS Web sites inside the configuration database and content databases. This implies that a backup of the configuration database will be required to ensure the protection of all SharePoint extended virtual servers.
3. WSS Databases By default, WSS installs a WMSDE/SSEE instance called SHAREPOINT or Microsoft ##SSEE and creates databases including a configuration database and a content database. The SHAREPOINT database instance can be backed up by selecting the instance in the Yosemite Server Backup Administrator GUI.
4. Usage Analysis logs Usage analysis for WSS allows one to track how Web sites on your server are being used. If usage analysis logging process is enabled, WSS log files are created daily to track usage information. These log files are stored in `%WinDir%\system32\LogFiles\STS` directory.

NOTE:

This path can be customized. In this case, one should add the appropriate path to the backup selection list.

5. Select the desired databases to restore

Using Disaster Recovery with Windows SharePoint Services

There are two ways to recover a SharePoint Services installation after a system disaster.

1. If you have a successful full backup of the system with VSS enabled, the disaster recovery process will restore the entire system including the SharePoint Services. Your SharePoint sites should be functional after the DR process is complete. It is recommended that you enable VSS for your DR backup set to take advantage of this feature.
2. If a full backup of the system was performed with the VSS option disabled, the WSS database is not restored, since the files were open at backup. You will need to take further steps to complete the WSS recovery. Complete the following operations after the initial DR process has completed successfully.
   a. Re-install the Windows SharePoint Services component on your system. This will rebuild the master WMSDE/SSEE database. The master database is required to restore the SharePoint databases including configuration and content databases.

NOTE:

You may have to uninstall and reinstall SharePoint services to restore the SharePoint installation.

b. Open Yosemite Server Backup and create a restore job to restore the WSS database.

Working with Certificate Services

You can override the backup modes that jobs specify for backing up certificate services.

Force modes Set the modes to use when a job specifies **Full**, **Differential**, and **Incremental** modes For example, if you specify Full for the **Incremental** mode, Yosemite Server Backup will run a full backup even though a backup job specifies an incremental mode.

NOTE:

This is only applicable for backing up a server that has certificate services installed, e.g., Certificate Authority installed on Windows.

9 Disaster Recovery

In this chapter

- Important guidelines
- Preparing For a Disaster
- Recovering From a Disaster
- Limitations

Recovering from a catastrophic disaster can be a time and labor intensive task. Typically new hardware must be acquired and installed. The environment of the machine, including the operating system and applications, needs to be restored to the new hardware. Only then can backed up data be restored. You can configure your regular backups so you can accomplish disaster recovery from your backup media, quickly and easily, using theYosemite Server Backup Bare Metal Disaster Recovery (BMDR) agent.

The BMDR agent recovers your machine by booting it from bootable media, repartitioning its disks, and then restoring the machine's data. Bootable media, or boot images, which include a minimal OS, device drivers, and your backup software, are created by properly configuring your regular backup. During a backup of your system, you can create a boot image of any machine in the backup, save or update the boot image in the catalog, save the ISO to a file, or burn the boot image (of the media server) to the beginning of your backup media.

While you need boot media of your Backup Server on hand for disaster recovery, for all other machines in your backup domain, an updated boot image which can be burned to media, along with fully backed up data, is sufficient preparation for disaster recovery.

Once the machine boots, you can restore your backup data from a locally attached backup device, or for clients running supported Operating Systems, the restore can be run over the network. Some final steps to restore third party data and any incremental or differential backups complete the recovery of the machine.

To effectively use the BMDR agent you must prepare for disaster and test your preparations periodically.

Important guidelines

Disaster Recovery of a Backup Server requires bootable media on hand to start the disaster recovery process. Once the Backup Server boots, its data can be restored from backup media loaded in an attached device. All data on the media will be restored.

Disaster recovery of clients in the Backup Domain also requires bootable media. which can be created at disaster recovery time from up to date boot images stored in the catalog. Use Make bootable CD/DVD from the Task menu on the Backup Administrator, to burn the stored boot image of any client to CD/DVD, or to create a file of the ISO image which can be burned to media using third party software.

Once you boot a client, you can restore data from a locally attached device loaded with your backup data (all data on the backup media will be restored), or for client machines with supported Operating Systems, you can choose Network Disaster Recovery. Network Disaster Recovery allows you to configure a restore job, selecting the data you wish to restore using the Backup Administrator, and restoring data over the network.

Boot Media

Boot images must be written at the beginning of media, so they must be written to blank media, or must overwrite existing media. To create a bootable image for disaster recovery, you should select the Write Mode **Overwrite all media** on the backup job's Configuration page Settings. Yosemite Server Backup then writes system configuration information to the backup media in support of disaster recovery making the media bootable.

When to create new bootable media

You should keep bootable media on hand for every machine which may require disaster recovery.

Your bootable media may become *obsolete* whenever any of the following occurs:

1. Add or remove hardware from your computer.
2. Change firmware or update device drivers.
3. Change your disk drive configuration (e.g., modify volumes or partitions).

You should create new bootable media in any of the above cases.

Restoring to dissimilar hardware

When performing disaster recovery, the hardware on the target system must be nearly identical to the source system with the following exceptions:

- You may change your video adapter as long as the new video adapter is VGA compatible.
- You may increase the size of your hard disk.
- Your SCSI, ATAPI, Fibre Channel or USB tape drive and adapter *must be the same or use the same driver* as it did when the disaster recovery media was created.
- Your SCSI, IDE, Fibre Channel or USB tape drive and adapter must be the same or use the same driver as it did when the disaster recovery media was created.
- You may change network cards, USB ports and USB peripherals, *except* tape drives, without restriction.
- *You may not perform disaster recovery to a USB hard drive or to Fibre Channel devices* .

Disaster recovery allows device drivers to be added during a recovery in the event that hardware changes require additional drivers. Changing processors, motherboards, or other hardware components, will not prevent disaster recovery from working.

The Advantage of Bootable Backup Devices

Certain devices, bootable backup devices, allow you to create bootable media at backup time. The boot image is written directly to the beginning of the backup media, prepending the backed up data. Disaster Recovery with bootable media created this way is simplified because the backup media provides the boot image of the machine being recovered and the data, which is restored when the machine is booted with it.

If you create a backup to a bootable backup device that supports bootable media, as long as your backup is written from the beginning of the media, the media will be bootable and can be used for Bare-Metal Disaster Recovery.

Bootable backup devices that support bootable media and bare-metal recovery include:

- tape drives that support HP One-Button Disaster Recovery technology (see description below) and
- removable cartridge disk drives.

Removable cartridge disk drives support the creation of bootable media with both the boot image and the backed up data, as do tape drives with One-Button Disaster Recovery (OBDR). OBDR is a firmware feature which enables a tape drive to act like a bootable CD-ROM in Disaster Recovery mode. When you create a backup on an OBDR tape drive to new media, or select the Write Mode Overwrite all media (on the backup job's configuration settings page), Yosemite Server Backup automatically makes the media bootable. When you run One-Button Disaster Recovery, your tape drive goes into a special Disaster Recovery mode that enables it to restore your operating system, reboot from the most recent backup cartridge, and restore the backup data from the media.

Preparing For a Disaster

To prepare for a disaster, perform the following steps:

1. Run a backup of your system, configured as described in Configuring Backups to Support Disaster Recovery, and save boot images to the catalog.
2. Create bootable media. If not created automatically in step 1 (See The Advantage of Bootable Backup Devices), you will need to create bootable media for the Backup Server. You should also create bootable media for every machine in your backup domain that may require disaster recovery. See Create bootable media in this section.
3. Test the bootable media to make sure you have created it properly. See Test the media in this section.

NOTE:

You should create at least one extra set of bootable media as protection in the event of media failure during disaster recovery.

Configuring Backups to Support Disaster Recovery

1. Insert the first disaster recovery media.
2. Create a backup job and open its property page.
3. Select the machine to backup. A full backup is recommended for Disaster Recovery.
4. Select the backup device to which you will write the backed up data.
5. To prevent an out of sequence disaster recovery backup from affecting your current backup rotations:
   - On the Configuration page, you can set the Backup mode to Copy.
6. To create bootable media for the Backup Server on an attached bootable backup device, configure the following:
   a. On the Configuration page, set the Write mode to Overwrite all media.
   b. On the Configuration page, make sure Split File is unselected.
   c. On the Advanced > Options page, select Create DR Bootable Media (selected by default).
7. To update boot images of selected machines in the catalog, so they can be burned to bootable media in a separate step:
   - On the Advanced > Options page, select Update DR information on selected machine.
8. Save and Run the job; inserting additional media as required.
9. Once the backup job is complete, check the log page. You will be able to verify that the backup was successful. The Summary section of this page will also tell you if any items have failed. It is very important to check log files on a regular basis. If files have not been backed up, they cannot be restored.

NOTE:

If you have a bootable backup device, Yosemite Server Backup makes each media bootable for the machine attached to that device. For example, if the full backup uses three media, all three media are bootable.

Create bootable media

NOTE:

Even if you automatically created bootable media when you ran the disaster recovery backup (using a bootable backup device), you should consider creating another bootable media to protect against media failure.

Users can create bootable CD or DVD media from the Backup Administrator as follows:

1. Log in to the Administrator
2. Double-click Create Bootable CD-DVD from the Tasks view.
3. Select the machine for which you want to create a bootable CD/DVD. You can only select machines with bootable images in the catalog. The bootable CD/DVD is customized for the operating system and device drivers of the selected machine.
4. Select a CD or writable DVD drive on which to create the bootable CD/DVD.

5. Start Recording to create the bootable CD/DVD. This process takes time, and the Status Information area displays the status and a progress bar.

> **NOTE:**
>
> If you cannot create the bootable media directly from Yosemite Server Backup, or if you want to save the boot image to an ISO file, you can select Save the Disaster Recovery image to a file instead of burning it now. Then you can burn the file to media using a third party program.

6. As soon as you create the bootable media, test the disaster recovery media on a test computer. See Test the media. After a successful test, store the CD or DVD. You should create a bootable CD or DVD for each machine connected to the Yosemite Server Backup management domain.
7. After the test is successful, store the disaster recovery media. If you have backed up to a tape or removable cartridge, be sure to write protect the cartridge.

> **TIP:**
>
> Consider making duplicate bootable media in case the primary bootable media is unavailable or damaged. Write the ISO images to files so new media can be created if needed.

Test the media

Test your disaster recovery media as soon as you create it, to insure it will work in the event of a disaster. Consider creating alternative bootable media in case your new hardware does not support your current bootable media. For example, a bootable CD or DVD may not work with your new hardware, so if you created an additional set of bootable media for another bootable device you have, you could boot from that.

To test the disaster recovery media you have created, perform the following steps. You will not lose any data on your system. This procedure is completely safe.

1. Shut down your system normally.
2. If you are using a bootable CD or DVD, boot your computer from the disaster recovery media by:
   a. Inserting the disaster recovery CD or DVD into your computer.
   b. Turning on your computer.
   c. Performing any special steps for booting your computer from CD or DVD. (Refer to your system documentation.)
3. If you are using a bootable tape, boot your computer from the disaster recovery media by
   a. Removing all media from all tape drives and/or library magazine slots.
   b. Inserting the first bootable media:
      i. If you are using a single tape drive, insert the first bootable media into the drive.
      ii. If you are using a library, insert the first (or only) bootable media into slot 1 of the magazine. If the full backup used two or more media, insert the rest of the full backup media into the library magazine in their proper order.
   c. Performing any special steps for booting your computer from the tape drive. (Refer to your system documentation.) Most bootable drives use a combination of power cycling and pressing the Eject button on the front panel. Many also require that you update the computer BIOS.
4. If your system boots and displays any disaster recovery screen, the bootable media successfully passed the test and will function properly during an actual Disaster Recovery.

5. If you are using a bootable device and your system hangs during startup or your operating system does not boot from the device, your device is not compatible with the bootable media. You will need to make new bootable media for disaster recovery.
6. Select Exit and press Enter on the Disaster Recovery character screen or click Cancel on the Disaster Recovery Wizard screen.

Recovering From a Disaster

If you are unable to boot your system using your normal boot procedure, follow the appropriate procedure below:

- Disaster recovery for Windows 2008, Windows Vista, and newer
- Disaster recovery for Linux
- Disaster recovery for Windows 2003, Windows XP and earlier

NOTE:

For local disaster recovery, you should use only full backup media created with the Overwrite all media option. After your system boots, you can use the standard Yosemite Server Backup options to restore any incremental or differential media to your system. Standard Yosemite Server Backup restore procedures optimize restoration, restoring incremental and differential media faster than the disaster recovery process.

Recovering your system requires you to make the following choices described here. Do you want to recover your whole system or just the hard disk from which your system boots? If the volumes on your boot hard disk are split among multiple physical hard disks, you should recover the entire system and not just the boot disk. Otherwise, some system data may not be restored.

Do you want to recover your system from media and devices anywhere in the backup domain (network recovery)or do you want to recover your system using devices attached only to this machine (local recovery)? You need to consider how you plan to restore your backed up data. Once you have successfully booted the machine you are recovering, you can either restore your backed up data from a locally attached device reading the backup media, or you can run a restore job using the Backup Server to set up a restore task which restores the backed up data from over the network.

NOTE:

It is good practice to disconnect any drives you do not want modified during the recovery process. This protects you from inadvertently overwriting them.

Disaster Recovery with Libraries

When performing disaster recovery with an OBDR library, make sure the first bootable media from the most recent full backup is loaded into slot 1 of the library. Yosemite Server Backup will only boot from the tape in slot 1.

Yosemite Server Backup will restore all media that are contained in the library during the final recovery process. Therefore, make sure that you only load media in the library that you will need to restore during recovery.

Remove all media not associated with the recovery from the library. If the full backup spans more than one media, put the additional full backup media into additional slots.

Disaster recovery for Windows 2008, Windows Vista, and newer

To perform Disaster Recovery for one of the operating system listed above, do the following:

1. Insert the first bootable media into a drive or, if using a library, into any slot that can be booted from.
2. Perform any special steps for booting your computer from the bootable device. (Refer to your device and system documentation.).

NOTE:

If you are using a device that supports One-Button Disaster Recovery (OBDR) it may take several minutes to boot to a screen which indicates progress. During this time, the screen will appear blank.

3. When the computer boots from the recovery media, the **Disaster Recovery Wizard** welcome screen appears. Click the **Continue** button.
4. The **Disaster Recovery Wizard** starts up the skeleton operating system and the recovery manager.
5. If you are recovering a client machine, you need to choose the appropriate option indicating how you want to restore your data:
   a. To restore your data over the network, choose Recover your system from media and devices anywhere in the backup domain.
   b. To restore you data using only media read locally from an attached or internal device, choose recover your system using devices attached only to this machine.

NOTE:

Because you cannot perform Network Recovery on a Backup Server, when recovering the Backup Server, local restore is assumed and you are not given a choice.

6. Once the recovery manager has been started, if you selected Network Recovery in step 5 above, you will be instructed to use your Backup Administrator, running on another machine, to create and run a restore job to complete recovery. You can skip to step 11.

   If you selected Local Recovery in step 5 above, the Disaster Recovery Wizard displays a list of source and target devices available on the system.

   a. a. In the top list, select one or more source devices that you want to restore data from by placing a checkmark next to them.
   b. b. In the bottom list, select one or more target hard drives to restore. You do not need to restore all of them.

NOTE:

You must select at least one source device and at least one target device. If you don't see all of the devices in the list that you expect, you can load a driver or rescan for devices.

- To load a driver, click the Load a driver link and then browse to the driver file for the device. The driver must be Vista or Server 2008 compatible in order to be loaded.
- To rescan for devices, click the Refresh link. This is useful if you plug in a new SCSI device or some other device that is not plug and play compatible.

7. If you have a tape loader as a source device, you can select it and choose the slots from which you will restore data. By default, all slots are selected.
8. After clicking **Next**, you will see a list of all the volumes that were mounted when the backup was made. Each of these volumes is classified as critical or not critical, and mount points are shown as children of each volume.

   A volume classified as critical cannot be deselected. You can deselect non-critical volumes and the recovery manager will not restore any files from those volumes. If you are using local recovery, unrestored files will show up as skipped in the recovery status page.

   Click the **Next** button to start the recovery.
9. The status of the recovery is displayed while it is in progress.
10. When the recovery finishes or is cancelled, you will see a summary of what happened. If not all of the important objects were restored, you will be warned, with each important, unrestored object listed.

11. Once the recover has successfully completed, you will need to click the **Reboot** button to restart your system. After reboot, your system should be ready to log in and use.

NOTE:

If you used Local Disaster Recovery and you had incremental and differential backup media since the last full backup, use Yosemite Server Backup to restore the data from your incremental and differential backup media. SQL data and Exchange data from prior to Exchange 2010 will need to be restored in a separate step using a standard Restore job created through the Tasks menu on the Backup Server.

Disaster recovery for Linux

To perform Disaster Recovery for a Linux system, do the following:

1. Remove all media from all cartridge disk drives, tape drives and/or library magazine slots.
2. Insert the first bootable media:
   a. If you are using a single tape or removable disk drive, insert the first bootable media into the drive.
   b. If you are using a library, see Disaster Recovery with Libraries above.
3. Perform any special steps for booting your computer from the bootable device (refer to your device and system documentation).
4. Select Network Recovery to restore data from anywhere in the network, or Local Recovery to restore data from locally attached devices only.
5. Press **Enter**.
6. If a warning screen appears, read it and then press **F10**.
7. When the first confirmation message appears "**Are you sure?"**, select the appropriate **Yes** option and press **Enter**.
8. When the second confirmation message appears, select Yes, Perform the Recovery and press Enter. If you selected Network Recovery in step 4 above, you will be instructed to use your Backup Server to create and run a restore job to complete recovery.

   If you selected Local Recovery in step 4 above, the system does not require any input from you until it finishes restoring the first media to your system. Restoring the first media can take from minutes to hours, depending on the amount of data on the media, the speed and capabilities of the device, and whether you are recovering the entire system or just the boot disk.

   a. For Local Recovery, after the system has restored the first media, it asks for the next media to restore. Press **F10** to restore another media.
   b. After restoring the last media, remove the disaster recovery CD or DVD so that you can boot from the hard disk in subsequent steps.
9. Press **Esc**. A message screen appears.
10. Press **F10**. Yosemite Server Backup restarts your computer. After your computer has rebooted, log in.

NOTE:

If you used Local Disaster Recovery and you had incremental and differential backup media since the last full backup, use Yosemite Server Backup to restore the data from your incremental and differential backup media.

Disaster recovery for Windows 2003, Windows XP and earlier

To perform Disaster Recovery for Windows 2003, Windows XP and earlier, follow these steps:

1. Only disaster recovery media should be loaded in cartridge disk drives, tape drives and/or library magazine slots.
2. Insert the first bootable media:
   a. If you are using a single tape or removable disk drive, insert the first bootable media into the drive.
   b. If you are using a library, see Disaster Recovery with Libraries above.
3. Perform any special steps for booting your computer from the bootable device (refer to your device and system documentation).
4. When the Disaster Recovery screen appears, select one of the following options:
   a. Recover Boot Disk. Select this option to only recover the boot disk. Use it if your boot disk is corrupt or if you replaced the boot disk.
   b. Recover Entire System. Select this option to recover data to multiple hard disks, including the boot disk. Use this option if you replaced one or more hard disks.
5. Press Enter.
6. Proceed through screens, reading and then pressing F10 to advance to the next screen.
7. Because the re-partitioning of disks that follows this step is destructive, you are given two opportunities to confirm that you want to proceed with recovery, or you can cancel out of recovery. To continue with recovery, select the Yes option and press Enter each time.

   There are several phases to disaster recovery and your system will be rebooted at various points in the process. The machine may reboot several times if that is required by the operating system to complete certain recovery steps. Normally, you will only insert media when prompted to do so.

   The system does not require any input from you until it finishes restoring the first media to your system. Restoring the first media can take from minutes to hours, depending on the amount of data on the media, the speed and capabilities of the device and whether you are recovering the entire system or just the boot disk.
8. After the system has restored the media, it asks for the next media to restore. Select Yes to restore another media.
9. After restoring the last media, remove the disaster recovery media so that you can boot from the hard disk in subsequent steps.
10. Additional Restore jobs are required to finish the recovery of these systems. Any databases, such as Exchange and SQL, must be restored.

NOTE:

If you used Local Disaster Recovery and you had incremental and differential backup media since the last full backup, use Yosemite Server Backup to restore the data from your incremental and differential backup media. SQL data and Exchange data from prior to Exchange 2010 will need to be restored in a separate step using a standard Restore job created through the Tasks menu on the Backup Server.

Limitations

Some editions of Yosemite Server Backup do not support the Disaster Recovery feature. If your edition does not support Disaster Recovery, any job that attempts to use the feature will report that the feature is not licensed. If you need this feature, contact your reseller to purchase an edition of Yosemite Server Backup that supports Disaster Recovery.

Local Disaster Recovery (DR) operates without the benefit of the Yosemite Server Backup catalog. When it restores data it restores the entire contents of each media provided. The media can be supplied in any order but if there are incremental or differential backups on the media set along with the full backup, objects will be restored in the order they are found on media and the results may not contain the most current versions of the backed-up data.

Local DR does not currently support split spanning of objects. Any objects that are split spanned on the backup media will not be restorable during the DR process but must be restored after the DR process has completed. If the split objects are critical to the functioning of the system, your system may not function after the recovery process. Since there is no easy way to know which objects are split across media, it is best to unselect Split File in your backup properties configuration, when creating a DR backup.

Completing the Data Restore

At this point, your machine is backed up to the state of the backup media you restored. If you have incremental or differential backups since that backup, you will want to restore those as well.

In addition, some data requires that a system service be running to successfully recover it, including SQL databases and Exchange. These objects are skipped during the DR restore process and must be restored in a separate restore job once disaster recovery is complete. This applies if you are running an older Windows environment with SQL or Exchange. For a newer Windows environment with Exchange 2010, the recovery is done automatically through the disaster recovery procedures outlined in this section.

10 Backup Domain Configuration

In this chapter

- E-mail Settings
- Execution Options
- Barcode Filter
- Performance Settings
- Alert Settings
- Client Upgrade Settings
- Domain Security

To configure the Domain Server, select **Domain Configuration** command in the menu bar. This displays the **Properties** window for the domain. Select the particular property page you want to configure from the tasks list.

E-mail Settings

You can configure e-mail information for the Yosemite Server Backup management domain. Jobs can be configured to automatically e-mail log to the job owner upon completion. Before Yosemite Server Backup can send logs by email, the service must be configured to use an email server.

Server address Enter the address of the mail server

Server port Enter the appropriate SMTP port. The default is 25, which is usually the correct value. If you are using a proxy server, you may have to enter a different port.

From address Enter the e-mail address to be used in the *From* field for each job log e-mail. This e-mail address must be valid.

Execution Options

To limit pre- and post-commands to those in the script directory, you can check the box next to **Prevent execution of commands outside of script directory**. You might choose to do this for security reasons by tightly controlling the commands that are available in the script directory.

For more information on pre/post commands, see Job Pre-Post Execution Commands.

Barcode Filter

You can define ranges of media barcodes that are available to any job within the Backup Domain. Barcode ranges defined for a particular job are only available within that single job.

For more information on the use of barcode filters, see Barcode Filters for Jobs.

Performance Settings

The performance settings control the number of active clients (hosts) on the network and the number of active selection lists on the database. There are two parameters that can be configured to optimize resources consumed by Yosemite Server Backup.

Max number of active hosts This number controls how many clients can be started for all active backup jobs in the Backup Domain. This option is used to prevent packet loss from occurring if data is transmitted over a network with limited available bandwidth.

Max number of active selection lists This number controls how many hosts can build their selection list for all active backup jobs in the Backup Domain. This is used to limit use of the database and keep it responsive for active jobs.

Alert Settings

You can control the types of alerts that are logged in the operating system's event log by checking the boxes next to **Error**, **Warning**, **Information**, or **License**. We strongly recommend you always select the logging of **Error** and **Warning** alerts. By default, all alerts are logged.

Client Upgrade Settings

When the Backup Domain is updated to a new version, the executables for all supported platforms are stored on the Backup Domain. This allows members of the Backup Domain to be upgraded automatically whenever the Domain Server is upgraded to a new revision of Yosemite Server Backup. For installations with many clients, this feature can be a huge time and labor saver.

Enable automatic upgrade When this option is enabled, clients will detect when a new version is available and automatically update themselves. During an automatic client upgrade, the installer will close any running Yosemite Server Backup Administrator and Quick Access. The client is marked as offline during the upgrade process. If an automatic client upgrade fails, the upgrade will not be retried again unless the service is restarted. An upgrade might fail if there are running processes that cannot be killed or there are permission restrictions on the client.

Allow downgrade If you want the client to downgrade to an earlier version, you must explicitly select this option. Otherwise, the client will only automatically upgrade to a newer version.

Max number of active upgrade downloads Use this parameter to throttle how many clients will attempt to download a new version at one time.

Domain Security

Yosemite Server Backup supports rich user, group and permission based security policies. Contact Technical Support for more information. When Yosemite Server Backup is first installed, these features are disabled. The Administrator will not require a password to log in.

⚠ **WARNING!**

When security is disabled, anyone using the Administrator can gain access to your data. We recommend you turn security on and set a password for the **Admin** user.

Options

Enable Advanced Domain Security When enabled, the Administrator will present the user with a login screen at startup and all object property pages will have an additional page, **Permissions**, and the Logon Controls properties of Users and Groups will be enabled.

Setting a User Password

When security is enabled, a new view, **Security**, will appear under the **Advanced** link in the **Navigation** bar. Clicking it will display a list of Users and Groups. The system comes preconfigured with one User, **Admin**, and one Group, **Everyone**. To set a password for a user, select the user and click the **Change Password** command in the command bar. For many users, simply setting a password on the Admin user will be sufficient to meet their security needs.

For more details about the logon control properties, contact Technical Support.

11 Advanced Job Options

In this chapter

- Job Log options
- Job Pre-Post Execution Commands
- Barcode Filters for Jobs

The options in this chapter are common to backup, restore, verify and copy jobs. In most cases these settings can be left at their default values.

Job Log options

Yosemite Server Backup keeps a log of which files it processes while running a job. In addition to viewing the job log from the **Status and Logs** view, you can configure the job to e-mail it automatically to a designated e-mail address or save the log to a file for later viewing.

Log Type

Yosemite Server Backup has several different levels of logging control to communicate what was protected in a job.

Log only failed (default) This setting will log only files that could not be backed up because of some failure.

Log only failed and not attempted This setting is log files that could not be backed up because of a failure or because the machine hosting the file was offline or because the job was cancelled.

Log only completed This setting logs only the files that were successfully protected.

Log all This setting will log all files the job works on. Using this setting will generate a lot of log entries and can affect the length of the backup process.

None This setting is not recommended. However, using it can speed up the backup process.

Log file formats

Yosemite Server Backup can generate several file types. Select the log format that works best for you

Table 4 Log file formats

Format	Description
HTML	Choose this file type to save log files as fully formatted HTML files. These files can be read by most Internet browsers.
XML	Choose this file to save the log files as well-formed XML documents. These files can be read by most Internet browsers.
Excel CSV	Choose this file type to save the log files in a format that can be opened in Microsoft Excel. CSV stands for Comma Separated Value. The information saved to a file formatted for Excel CSV will display in columns and rows.
Plain Text	Choose this file type to save the log files in a format that can be read by any text editor.

Save log to a file

Log Format Choose a format from the drop down list.

Log will be saved to this file Yosemite Server Backup lets you select a file in which to store the job logs. Click the **Browse** button to select a file. Yosemite Server Backup always saves a copy of the log in the catalog in addition to the settings you choose here.

E-mail log

Log Format Choose a format from the drop down list.

Log will be sent to... Yosemite Server Backup lets you e-mail logs to one or more recipients. Enter a list of recipients separated by semicolons.

Auditing

In some cases, you may want positive confirmation that an object — like a database — was backed up but you don't want to wade through the log file generated by selecting Log All. You can accomplish this by setting the **Audit** property on the object when you select if for backup. Simply locate the object in the **Selection** page of the job properties, right-click on the object and select **Properties**, and check the **Enable Audit** box on the property page. By default, all Exchange and SQL databases are audited.

Job Pre-Post Execution Commands

You can define commands to be executed before the backup job runs and after the backup job runs. They are often used to perform custom OS-specific or application-specific tasks, such as to stop/start a database. Commands are defined on the **Execution** page of a backup job.

- Pre Execution Commands
- Post Execution Commands

Pre Execution Commands

The pre execution tab on jobs controls the command to be executed before the job is run, either on multiple hosts, or just the Domain Server. In addition there are options to control whether the job should stop, or whether the job should continue based on the outcome of the command.

Command path Specifies a full path or relative path, to a shell command, including command parameters. For instance `cmd.exe /c explorer.exe`, or `c:\windows\explorer.exe`. A macro syntax is also supported in this field, for many different uses. See the Yosemite Server Backup Technical Reference Guide for more information.

Run command on all hosts selected in job, as well as the Domain Server When checked, processes the command on all machines selected in job. When unchecked, only runs the command on the Domain Server.

Number of minutes to wait for command completion This value in minutes specifies how long the application should wait for the command to return. By default, it is set to Forever, meaning the application will wait for as long as possible for the command to complete. If set to something other then Forever, the application will terminate the command forcefully if it does not return in time.

Stop job if command fails to be executed When checked, causes the job to be stopped if the pre command is fails to be executed, such as if the command does not exist or the operating system cannot property determine how to execute the command.

Stop job if command returns error code When checked, causes the job to be stopped if the pre command executes but returns a non-zero code. When checked, enables the additional options beneath it.

Do not stop job if the following error code range is returned When checked, a range of error codes must be specified which are treated as warnings. If the return code is zero or is within the specified range, the job continues. However, if the return code is non-zero and outside of the specified range, the job to be stopped.

Post Execution Commands

The post execution job property controls what shell commands should be executed after the job completes with no error or with error.

Command to execute if job completes with no error This command will execute if the job completes with no final error. A job can complete with no error, even if all hosts are offline. This does not mean that anything was backed up, it just means that the job was not cancelled, or there wasn't some other major problem executing the job.

Command to execute if job completes with error This command will execute if the job completes with an error, such as no specified devices, or operator cancelled. This does not mean if any of the objects selected by the job fail to be backed up/restored/ or verified.

Command path Specifies a full path or relative path, to a shell command, including command parameters. For instance `cmd.exe /c explorer.exe` or `c:\windows\explorer.exe`. A macro syntax is also supported in this field, for many different uses. See the Yosemite Server Backup Technical Reference Guide for more information.

Run command on all hosts selected in job, as well as the Domain Server When checked, processes the command on all machines selected in job. When unchecked, only runs the command on the Domain Server.

Number of minutes to wait for command completion This value in minutes specifies how long the application should wait for the command to return. By default, it is set to **Forever**, meaning the application will wait for as long as possible for the command to complete. If set to something other than **Forever**, the application will terminate the command forcefully if it does not return in time.

Logs

The pre/post commands add detailed logs to the jobs which executed them. A new execution section was added to the job log, where all commands executed by the job are logged.

- *Command type*: Indicates what kind of command this was, whether a pre job/post job/fail job, or pre object/post object/fail object command.
- *Command path*: The fully macro expanded command path sent to the operating system for execution.
- *Host attempted on*: The host name where the command was attempted on.
- *Time executed*: The start time when the command was attempted.
- *Time completed*: The end time when the command either timed out and was killed, or when it completed on its own accord.
- *Execution result*: The result of the execution, either the execution failed, or the execution succeeded. If the execution succeeded, then the return code of the command will be logged here. If no return code is logged, then success is logged here.

Barcode Filters for Jobs

Many tape libraries support the use of barcodes to identify media. Each piece of physical media has a unique barcode that the tape library can read.

The **Barcode Filter** page allows you to define barcode filters for a job. The filter rules may be set for the whole domain and will be applied automatically to all jobs. Or, they may be set and applied at job level, using this page. Any filter rules applied at job level overwrite the default domain settings. All options will be grayed out initially. Deselecting **Inherit settings from domain** will enable the editing buttons and allow you to create job-specific filters.

There are three ways of assigning barcode filters.

Add an individual barcode This option allows you to specify an individual barcode for inclusion or exclusion. Up to 8 characters may be specified in this filter; the first 6 relate to the volume identifier and the last 2 relate to the media identifier. Wildcards may be used to increase the number of barcodes selected by the filter.

Add a range of barcodes This filter allows you to specify a range of volume identifiers and media identifiers to include. (Any media without a barcode or outside of the specified range will be excluded.) The following example would include LTO-3 (L3) media that fall within the volume range 791000 to 791044.

Add barcodes from media present in the library This filter displays a list of all libraries and their elements. Select the required barcodes from the list and click either the Exclude or the Include button, as appropriate.

Index

M

N

O

P

Q

R

S

T

U

V

W