Sun StorEdge™
Resource Management Suite
Version 6.0

Capacity Reporter Case Study

Version 6.0

Adobe PostScript

Contents

Preface

This guide is a reference tool for Capacity Reporter software users who have already installed the product and are interested in customizing the product to meet the needs of their environment.

Before You Read This Guide

Before you read this guide, install the Capacity Reporter software. For information on installing Capacity Reporter, see the *Sun StorEdge™ Capacity Reporter Configuration and Installation Guide*. For information on using Capacity Reporter, see the Capacity Reporter online Help.

How This Guide Is Organized

This guide is organized as follows:

Chapter 1 is a documentation roadmap that provides a list of related Capacity Reporter reference documents.

Chapter 2 presents key Capacity Reporter concepts that you must understand before reading the rest of the guide.

Chapter 3 contains a Capacity Reporter case study that demonstrates how the product has been implemented in a typical environment.

Chapters 4-14 provide examples of how Capacity Reporter is being used to solve distributed storage resource management problems and proactively manage storage resources.

Appendix A provides examples of how Capacity Reporter provides solutions and gives you a competitive edge.

Appendix B provides tips on how to provide on-going maintenance of your Capacity Reporter implementation.

Appendix C discusses Capacity Reporter's impact on system and network resources.

Related Documentation

To learn about:	See:	Located:
Late-breaking information about Capacity Reporter	*Sun StorEdge™ Capacity Reporter Release Notes*	Capacity Reporter CD-ROM
Screen-by-screen installation help	Capacity Reporter Installation Help	**Help** button on each dialog box in the installation
Page-specific descriptions of the product, including product usage, security, and troubleshooting tips	Capacity Reporter Online Help	**Help for this page** button in user interface. To access the entire help file, click **Contents** in the Help window.

Accessing Sun Documentation Online

The `docs.sun.com`^{SM} web site enables you to access a select group of Sun technical documentation on the Web. You can browse the `docs.sun.com` archive or search for a specific book title or subject at:

`http://docs.sun.com`

Ordering Sun Documentation

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at:

`http://www.fatbrain.com/documentation/sun`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

`docfeedback@sun.com`

Please include the part number (816-2259-11) of your document in the subject line of your email.

Documentation Roadmap

A wide variety of electronic and printed documentation is available for Capacity Reporter. The tables below show where to find the information you need.

Implementers

To learn about:	See this:	Located here:
Capacity Reporter prerequisites and some SQL configuration guidelines	*Sun StorEdge™ Capacity Reporter Configuration and Installation Guide*	Capacity Reporter CD-ROM
Screen-by-screen online help for Capacity Reporter Server and Capacity Reporter Agent installation	Installation Help	Capacity Reporter CD-ROM
Network bandwidth and system resources implications	Network and System Impact	Appendix C of this document

End Users

To learn about:	See this:	Located here:
Functional overviews of each product area "How do I …?" Report descriptions Page-specific help	Capacity Reporter online Help	**Help** button on Capacity Reporter main page; **Help for this page** button throughout Capacity Reporter

Everyone

To learn about:	See this:	Located here:
Prepurchase information	FAQ	http://www.sun.com/storage/software
Functional walk-through; overview of features	Evaluation Guide	Capacity Reporter CD-ROM

Introduction

The purpose of this guide is to familiarize you with basic concepts of Capacity Reporter, then show you, via a case study, how a company has implemented Capacity Reporter to solve some of its business problems by fully leveraging Capacity Reporter's rich feature set.

This guide assumes:

- You have successfully installed at least one Capacity Reporter Server and Capacity Reporter Agent
- Capacity Reporter has started to collect data
- You have started Capacity Reporter and have viewed some of its reports
- You are using Capacity Reporter's Tasks page as a starting point for your work

Architectural Overview

Capacity Reporter is based on a flexible, efficient architecture that can grow with your enterprise data and systems, including Windows NT®, UNIX®, Linux®, and NetWare®. Unlike other storage applications, which are based on older technologies that have been ported and force-fit to work on Windows NT, Capacity Reporter is designed from the ground up using industry standards, and puts to practical use many of Microsoft's Intranet tools and technologies.

Capacity Reporter has the following components:

Component	Description
Management Database	Central repository based on Microsoft SQL Server® that stores information collected by Capacity Reporter Agents.
Management Server	Service that runs on Windows NT 4.0 Server, Microsoft Internet Information Server 4.0®, or Windows 2000 that manages communication between the Management Database and the Capacity Reporter Agents. The Management Server also performs database management.
Capacity Reporter Agent	Service that runs on any Windows NT Workstation or Server, Windows 2000, Solaris®, AIX® Red Hat Linux®, HP-UX®, and NetWare. The Capacity Reporter Agent runs on behalf of the Management Server, and gathers computer, disk, file system, file, directory, and user information from the system on which it is installed.
Web	Collection of Active Server Pages, HTML and DHTML pages, and JavaScript that enables you to monitor your enterprise storage from any web browser.

In the illustration below, the following terms are used:

- NAS (Network Attached Storage) – These file servers connect to the network.
- SAN (Storage Area Network) – These Fibre Channel switches connect the network to storage devices.
- DAS (Dual Attached Stations) – These devices are part of the Fibre Distributed Data Interface, offering access to the LAN.
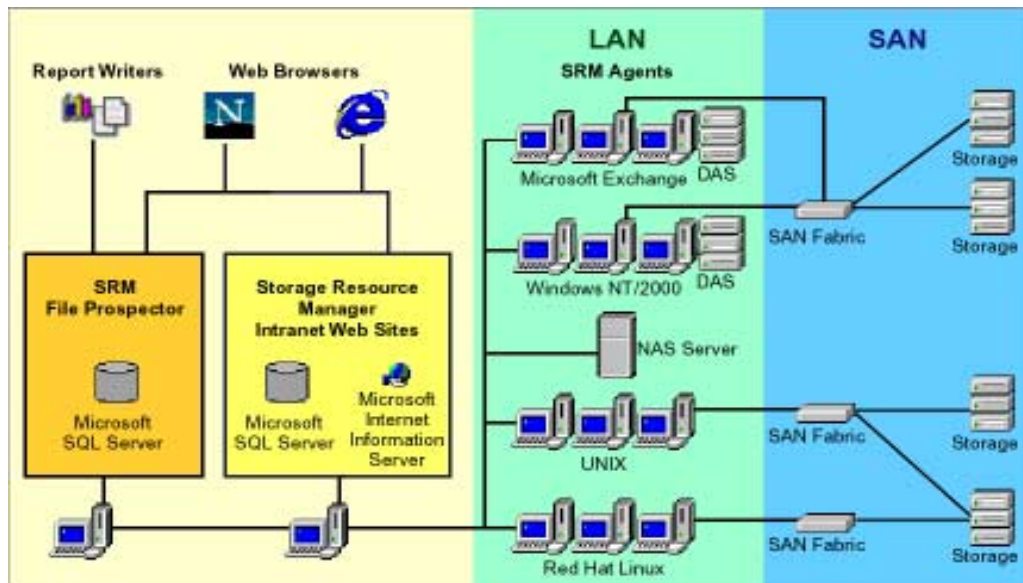
The illustration shows that SAN switches pass on data from storage devices. Within the LAN, Capacity Reporter Agents collect information, which is passed on to the management database. Queries are made and the resulting reports are displayed using the browsers shown here.

The Capacity Reporter architecture is efficient, and results in minimal network impact, because processing is distributed across the various components. The Capacity Reporter Agents "wake up" and execute scans according to network schedules that you determine, so no unnecessary polling takes place. Viewing Capacity Reporter's reports, graphs, and alerts also consumes little bandwidth, because you are simply contacting the Management Server and Database — just like viewing any Intranet web site.

Key Capacity Reporter Concepts

Before getting into the Capacity Reporter case study, it is important that you are familiar with the following key concepts:

- Security
- Groups
- Filters
- Scans

Security

Your user account security settings and the access control lists (ACLs) set on Capacity Reporter files determine your ability to view and set options. Capacity Reporter uses two Windows NT security groups — created when Capacity Reporter is installed — as shown below. Membership in these Windows 2000 groups is based on Windows NT *userid* and *password*.

Use this account:	To do this in Capacity Reporter:
SRMAdmin	View reports and make changes in Options pages
SRMUser	View reports only

For details on security, see Web Security in the Capacity Reporter Help.

Note – Users without proper privileges cannot perform most of the procedures described in this guide.

Groups

Grouping allows you to apply a set of alert and filter definitions and scan frequencies to multiple storage resources, making it a useful tool for chargeback and cost accounting. In addition, groups are used in setting alert conditions, including user space quotas.

All groups have the following attributes:

- Groups contain resources of a single type.
- Groups cannot contain other groups.
- A resource can belong to only one group at a time.
- A resource can belong to only its respective resource group type; for example, only computers (and NAS devices) can belong to a computer group.
- A group name or description can be altered without affecting the group's membership.
- If a group is deleted, the members revert to the default group.

Capacity Reporter automatically creates a set of default groups for your storage resources. In addition, Capacity Reporter lets you easily import existing Windows NT/2000 security groups, and create custom groups to organize your storage resources.

Default Groups

When Capacity Reporter is first installed, default groups for computers, file systems, directories, and users are created. These groups initially contain all managed resources.

Default group names are:
- Default Computer Group
- Default File System Group
- Default Directory Group
- Default User Group
- Default Database Group
- Default Plug-In Group

Default groups have the following attributes:
- You cannot delete a default group.
- You can change the name and description of a default group.
- Capacity Reporter places resources in their respective default groups when Capacity Reporter recognizes them as managed resources.
- All resources not assigned to a custom group are in the resource's default group.

Note – Windows NT/Windows 2000 user and directory groups are automatically assigned to the corresponding Capacity Reporter groups.

Custom Groups

Provided that you have the proper access privileges, Capacity Reporter allows you to create custom groups of:

- Computers
- File systems
- Directories
- Users
- Databases
- SAN objects

You populate custom groups by putting in members from other groups. When you delete a group, its members automatically return to the default group.

Custom groups have no members initially. Members of a new group are taken from either the default group or other custom groups. Use custom groups to do the following:

- Set alert conditions that are specific to a particular group. For example, you can have Capacity Reporter generate an alert when a user exceeds a space quota. Creating user or directory groups with defined quotas allows you to receive a notification when any group member exceeds the specified level.
- Schedule scans to meet your system and network capabilities, and to coordinate with time zones and regularly scheduled network batch jobs. If you have a large number of files and directories, you might want to create several file system groups, each with a different scan schedule. This practice distributes the traffic on your network and your Capacity Reporter Server.
- Manage file system space. You can set size thresholds on file system groups and receive an alert when the space used by a file system exceeds the specified size.

Windows NT/2000 Security Group Import

Capacity Reporter makes it easy for you to import existing Windows NT/2000 Security Groups as a basis for creating or populating custom user and/or directory groups, reducing group administrative overhead. The scheduled imports keep your group listings up-to-date, and priority selections provide a convenient way to manage group membership. For example, if John Smith were in both the Finance and the Project-Alpha Windows NT/2000 Security Groups, you might want to set the Finance group as a higher priority than the Project-Alpha group. This would ensure that he would be tracked only in the Finance group for storage quotas and departmental chargeback.

Importing a Windows NT/2000 security group is an option when you create a new group. Choose **Options>Groups>New**.

Note – The Active Directory feature in Windows 2000 is not supported at this time.

Defining Custom Groups

Before you start to create custom groups, you need to determine how you want your storage resources organized within Capacity Reporter. For example, should you organize your resources by business unit, geography, function, application, or as a mixture? You might want to group each resource type, or a set of resource types, by different criteria.

To help match your storage resources with your grouping requirements several worksheets are provided at the back of this guide. The Capacity Reporter case study uses these worksheets to illustrate how system administrators at one company have used Capacity Reporter to solve business problems.

When trying to determine how to group resources, keep in mind:
- What file filters do you want to apply, and to which file systems?
- How should quotas be defined?
- What is the time and system overhead required to scan groups of resources?

Filters

Capacity Reporter lets you filter the contents of File Reports and File Distribution Reports. Filtering allows you to see only files that interest you. Filters do not affect the calculation of quotas. To create a filter:

1. Define at least one criterion for the filter.

2. Assign the filter to at least one file report type.

3. Apply the filter to at least one file system group.

Filters obey the following rules:
- Only the file systems in the file system groups to which a filter is applied are filtered.
- A filter can be applied to multiple file system groups.
- A file system group can have multiple filters.
- Filters can exclude or include files based on a combination of location, type, name, owner, or size.
- Filters are applied when Capacity Reporter Agents are scanned, so the effects of a filter are seen when the next file system scan is complete.

Conflicts Between Include and Exclude Filters

When a conflict arises between an include and an exclude filter, the include filter overrides the exclude filter specification. For example, if you have a filter that excludes *.exe files, but another filter that includes files named doom*.exe, files whose names begin with "doom" and have an .exe extension are included in reports.

Capacity Reporter provides the following predefined exclude filters:

Filter Name	Directories, Files, or Users Filtered
Temporary Files	*.tmp, \temp, \tmp (includes all subdirectories)
Graphic Files	*.gif; *.bmp; *.jpg; *.jpeg; *.tif; *.png; *.psd; *.jif
NT Paging Files	pagefile.sys
Database Files	sql.log; *.mdb; *.ldb; *.db; *.ora; *.edb
Zip Files	*.zip
Administrator Files	*\Administrator (in the file owner criteria table)
Recycled Files	All files in the recycle directories (\RECYCLER and \RECYCLED)
Exclude All from Largest Files Report	All files

You can modify but not delete predefined filters. They do not affect reports by default; you must explicitly apply them to file system groups.

Scanning — Automatic Data Collection

Capacity Reporter scans computers with Capacity Reporter Agents for computer, disk, file system, user, and file information, and stores the results in its database. The stored information is then used in Capacity Reporter reports. Each scan can be scheduled or done on demand (**Scan Now**).

Capacity Reporter does the following types of scans.

Domain Scanner

Scans your networked domains and workgroups for unmanaged computers. Only domains and workgroups with Capacity Reporter Agents installed are scanned.

You can set the Domain Scanner to one of the following levels:

Level	Description
Off	The Domain Scanner is disabled.
Contact a domain controller...	Contacts the domain controller of your networked domains and workgroups with installed Capacity Reporter Agents and retrieves a list of all computers. Unmanaged Computer reports are updated accordingly. This type of scan is very fast, and is the default.
Contact each computer...	Scans each computer in all networked domains and workgroups with Capacity Reporter Agents installed. Retrieves details of unmanaged computers, and updates the unmanaged computer reports accordingly. This scan takes longer than contacting the domain controller

Computer Scanner

Scans managed computers, disks, and file systems, and discovers share points. Only computers with Capacity Reporter Agents installed are scanned. The Computer Scanner gathers only high-level resource information. The Computer Scanner does not gather file, directory, or user information. Computer scans are applied to computer groups. Each computer group can have a unique scan setting.

File System Scanner/Detailed Scanner

Scans the file systems in the file system groups for information for:

- Directory reports
- File and directory detail reports
- File distribution reports
- File reports
- User quotas
- User reports

The File System (detailed) Scanner puts the largest load on your managed computers. A file system scan is the equivalent of performing a FIND *.* operation. The more files and directories that you have on managed computers, the larger the load and server usage. Consider your network bandwidth and traffic when scheduling this scan. Typically, this scan is scheduled after normal working hours, and after backups have been completed, to provide up-to-date backup coverage analysis.

- **Import Scanner** — Scans your Windows NT security groups and Capacity Reporter user and directory groups, and updates your user and directory groups accordingly.
- **Plug-Ins** — Using Plug-Ins, Capacity Reporter can communicate with a number of devices, such as RAID, NAS, NetWare Servers, SAN, and Backup devices. The Capacity Reporter Agent is used with a proxy computer to retrieve scan data. For more information, see "Installing Plug-Ins" in the *Sun StorEdge™ Capacity Reporter Configuration and Installation Guide*.
- **Database Scanner** — Using a plug-in, Capacity Reporter collects and reports information about:
  - The database itself, including total allocated data space and total allocated free space
  - The files that contain the database, including size of the files and the amount of space allocated to the database, but not yet used
  - The Database Server Instance that serves the database, including the amount of space that is not allocated to the Capacity Reporter-managed database

  In addition, Capacity Reporter will alert you when the transaction log free space and/or the data free space falls below specified values.

When Users Appear in Capacity Reporter Reports

A new user does not appear in Capacity Reporter reports until the file system scanner scans one of the file systems on which the user owns a file. If a user does not own a file on a managed file system, the user does not appear in Capacity Reporter reports.

File System scans are applied to file system groups. Each file system group can have a unique scan setting.

Report Setting

The Reports page allows you to specify:

- Maximum number of entries to display in the Largest File, Largest Directories, and Most Vulnerable Files reports
- Number of days of history to be displayed in the line graphs
- Length of time that data for missing resources is kept in the database
- Report physical and logical sizes

Note – Data for missing resources (based on history settings) that have been unmanaged, removed, or deleted from your network is automatically removed from reports.

ABC Industries Case Study

This chapter illustrates how you can use Capacity Reporter software to assess and solve some common storage problems.

Note – All solutions in this document are stated in general terms. For detailed "How To" information, see the Capacity Reporter Help.

Company Overview

The ABC Industries corporate headquarters are in Massachusetts. It has several sales and production sites across the United States and Europe. Each site is its own single, Windows NT domain. Each domain has at least a one-way trust to the masterdomain at headquarters. The company's expanding Windows NT infrastructure looks like this:

Facilities:

- Corporate Headquarters
  - 150 Windows NT/2000 Servers
  - 25 UNIX Servers
  - 2 NetApp Filers
  - 10 NetWare File and Print Servers
  - 210 database servers supporting 1500 databases with a mix of Oracle and Sybase databases

    126 Oracle databases on Solaris

    27 Oracle databases on HP-UX

    27 Oracle databases on NT

    30 Sybase databases on Solaris

- 4 Regional Offices — 4+ NT Servers
- 15 Branch Offices — 1-2 NT Servers
- **Summary:** 193 file servers and 210 database servers within 20 locations.

Systems:

- Servers from Bull, Compaq, Dell, HP, IBM and Sun
- Windows NT 4.0, Solaris, HP-UX and AIX, Windows 2000
- Dual processors
- Minimum of 128 MB RAM
- Some Microsoft Cluster Servers
- Various RAID systems
- NetWork Appliance® (NetApp) File Servers (Filers), and proxy machines to scan them

Applications:

- File and Print Servers (Windows NT, NetWare, and AIX)
- Web servers for intranet and corporate web site
- Various servers running SQL-based applications
- Oracle applications on Solaris
- ERP applications on HP-UX

Network:

- 100 BaseT Ethernet-based LAN
- T1 leased lines to regional offices
- Fractional T1 leased lines to branch offices

ABC Industries has installed Capacity Reporter Agents on servers within each of its domains. Each remote site uses Capacity Reporter to manage most of its storage resources. Corporate headquarters uses Capacity Reporter to manage all its storage resources, as well as some of the storage resources at remote sites.

System administration is the responsibility of the corporate IT department. The director of IT, Janet, reports to the CTO. System administrators — Andy at corporate headquarters, and one at each remote office — report to Janet.

Company Goals

The ABC Industries IT department has the following goals:

- Ensure that every file, application, and database file system has enough free space to stay up and running.
- Reclaim unnecessary disk storage to avoid spending the IT department budget on extra disks, tape libraries, tapes, and backup servers unless required.
- Plan future storage needs and justify purchases, including deploying a SAN.
- Proactively manage Windows NT and UNIX shares, files, and directories by exception.
- Plan, manage and control disk-space usage for all users and charge departments for their usage.
- Ensure that every file (except stale ones) in the company's Windows NT environment is periodically backed up.
- Proactively manage storage allocated to databases.

Agent Machine Selection Process

ABC Industries planned to put a Capacity Reporter Agent on business-critical servers. To identify candidates for a Capacity Reporter Agent, Janet and Andy answered the following questions:

- How critical to the business is the server and its associated storage resources? What is the impact of losing data on this server? On such servers, the status of backups, the status of disks, and space usage are of special interest to the company.
- How fast are the machine's disks filling up? The company is growing, bringing new employees and new user and application files, making capacity planning a critical function for IT.
- How many users share the machine and the resources that the machine supports?
- Are user quotas needed?
- Is it important to know what files, and what types of files, are on the machine?
- Will the objectives of the IT department be realized, and will the efficiency of the system administrators be increased?

After answering these questions, they decided to install Capacity Reporter Agents on the NT File Servers and UNIX Application Servers at the home and remote offices.

Proxy Machines

Certain devices such as NetWare Servers and NetApp Filers cannot have a Capacity Reporter Agent installed. Instead, they require the use of proxy machines, computers that run the agent, which scans the devices. The proxy agents can run a computer scan of NetWare Servers and NetApp Filers, and run a file detail scan of NetWare volumes and NetApp Filer shares.

Managing and Reclaiming Disk Space

This chapter details how ABC Industries has used Capacity Reporter to solve many of its storage problems.

Objectives

The ABC Industries remote sites need to keep their storage costs to a minimum. They use Capacity Reporter to achieve four key objectives:

- Identify disk file systems at most risk of running out of space, enabling proactive actions to reclaim disk space and avoid costly downtime resulting from out-of-space conditions.
- Eliminate the time-consuming practice of using Windows NT Explorer to determine file system capacity and find files to delete.
- Identify disk space being wasted by unnecessary files and stale data to maximize use of existing storage resources and defer additional capital investments.
- Protect the backup window, the amount of time allotted for the system to run the backup.

Product Solutions

To meet its objectives, ABC Industries uses all the Capacity Reporter disk space reclamation features:

■ Disk Space by File System reports identify file systems most at risk of running out of space.
■ Capacity Reporter alerts notify system administrators when a free space threshold has been exceeded.
■ Largest Files reports, both networkwide and at the file system level provide an on-going file pruning effort. Various filters are applied to these reports to focus on problematic file types.
■ File Distribution reports (by access date) identify stale files, and identify data not accessed in a long period of time. Various filters are applied to these reports to detect specific file types.
■ File Details report views all files by access date to identify stale data and files owned by a specific user.
■ Directory drill-down provides quick and easy access to Windows NT directories containing files to be deleted.

Implementation

To implement the ABC Industries business solution, Andy had to:

1. Configure Capacity Reporter features.

2. Analyze the results of the configuration.

3. Take action based on the results.

4. Adjust the configuration.

Configuration Steps

Andy followed these steps to configure the ABC Industries business solution:

1. Where needed, he created file system groups based on server function — file and print Servers, web Servers, and so forth — via the Options page. He then populated those groups with file systems of most interest, keeping in mind that some file systems are in groups to solve other business problems. For example, he put all Solaris file systems in a single file system group.

2. He set threshold alerts on file system groups that reach a specified size. Threshold alerts notify system administrators when a file system is running out of free space. He tailored the alerts to the function of each server — because space usage on file and print servers is very dynamic, he set the free space threshold there at 20%. At the same time, he set thresholds as follows:
   - Web Server: 10%
   - Application Server: 10%

3. He created filters and applied them to the file and print Servers' file system group so that only those file types of interest would be displayed in Largest Files and File Distribution reports. For example, to ensure that the reports for these servers would include graphics files, he did the following:

   - Created a filter to exclude all files (*.*)
   - Activated Capacity Reporter's default graphics filter by applying it to the file system groups on the file and print servers
   - Created and applied a filter for graphics files not included in the default filter, such as .JPEG and .AVI files

4. He set the Report Size option to display a greater number of files to be reported in the Largest Files reports for the domain and file system levels — 250 files for the domain report, 50 files for file systems.

Analyze Results

To analyze the results of the Capacity Reporter configuration, Andy first ensured that all managed resources were scanned with the new settings. He did this by waiting until the scheduled scans had completed, or in some cases, by using the Scan Now option. He then reviewed the following Capacity Reporter reports:

See this Capacity Reporter Report …	To view …
Current Alerts	If any file systems exceeded their threshold definition
Disk Space by File System	Consolidated list of all file systems discovered
Capacity Planning by File System	Trends (graphs) for individual file systems
File Management — Largest	How to use directory drill-down to identify files that can be deleted to reclaim disk space
File Distribution by Access Dates	Space not accessed over a specified period of time

Action Taken

After viewing the Capacity Reporter reports, Andy took the following actions:

- He ensured that administrators who received over-quota alerts reviewed disk usage and took steps to reduce the amount of space used.
- He backed up unnecessary, stale, or duplicate large files, then deleted them.
- Because of the number of stale files, he made a case to management to acquire HSM to automate the process of moving stale files to near-line or offline storage, or deleted those not accessed in over a year, after ensuring that they had been safely been backed up.

Adjust Configuration

Over time, the environment and requirements for ABC Industries are expected to change. For example:

- Report sizes need adjusting.
- New filters are needed to include .EXE files.

Andy and the system administrators at remote sites monitor these changing needs, and periodically start the Configure-Analyze-Act-Adjust cycle again to address the changes.

Capacity Planning

Objectives

Janet and Andy compiled their objectives for the next phase of their solution. The list of objectives looked like this:

- Project future storage needs based on actual prior utilization.
- Justify budgeted storage resources based on actual prior utilization.
- Save valuable IT staff time by eliminating manual tracking of available disk space and the rate of consumption.
- Eliminate unnecessary purchases of disk drives and RAID.
- Understand and predict the rate at which applications consume space.
- Understand and predict the rate at which file servers, in particular AIX file servers, consume space.
- Answer three questions key to planning for additional disk space capacity:

  a. When will more disk space be required?

  b. How much additional disk space will be required?

  c. Where will additional disk space be required?

Available Capacity Reporter Solutions

Capacity Reporter gave ABC Industries capacity planning reports for four types of resources:

■ Networkwide resources
■ Computers and Network Attached Storage (NAS) servers
■ File systems
■ Directories

Next, Janet and Andy decided which of these reports to use.

Selected Capacity Reporter Solutions

After reviewing the reports available to them, Janet and Andy identified the reports that would help them achieve their objectives:

From the Tasks page, choose:	To do the following:
Capacity Planning Network wide	View the rate at which disk space is consumed on an aggregate level. This answers the first two capacity planning questions – when will more disk be required, and how much.
Capacity Planning By Computer	Determine which computers are consuming disk space at the fastest rate. This answers the third question – where should additional disk space be allocated.
Capacity Planning By File System	Determine which file systems are consuming disk space at the fastest rate. This answers the third question – where should additional disk space be allocated.

Implementation

To implement the ABC Industries business solution, Janet and Andy had to:

1. Configure Capacity Reporter features.

2. Analyze the results of the configuration.

3. Take action based on the results.

4. Adjust the configuration.

Configuration Steps

Janet and Andy followed these steps to configure the ABC Industries business solution:

1. They used Capacity Reporter's Report Size facility to make sure that Capacity Reporter was saving a full 365 days of historical data.

2. They let Capacity Reporter run for a few months to build up historical data to analyze.

Analyze Results

Janet went to Capacity Reporter's capacity planning reports and examined line charts to view trend lines. She looked at both Space Used (to see the disk usage trend) and Free Space (to predict when systems would run out of space if no action were taken). Once she had the trend reports in hand, she compared them with the following Capacity Reporter reports to perform capacity planning:

View this Capacity Reporter report …	To:
Capacity Planning Network wide	Determine aggregate rate of consumption and when and how much new disk space needs to be allocated. (View weekly data points to get a larger-grain view.)
Capacity Planning By Computer	Determine which computers are consuming disk space at the fastest rate and where to deploy additional physical storage.

Take Action

After reviewing the trend lines and Capacity Reporter reports, Janet took the following actions:

- She printed out Capacity Reporter capacity planning reports as an addendum to her budget.

- She prepared budget and purchase orders based on projections calculated from Capacity Reporter capacity planning reports.
- She asked Andy and the remote site administrators to deploy additional disk space where necessary on computers.
- She asked all the site administrators to periodically check the reports generated automatically by Capacity Reporter and to determine if corporate policies on disk space consumption (for example, by e-mail attachments, downloaded program files, and graphics files) needed to be updated.

Adjust Configuration

The capacity planning process used by ABC Industries has worked well. The system administrators perform one key task to keep the process up-to-date:

- They update computer group membership as new computers come online.

Managing Storage Resources with Alerts

Objectives

- Receive notifications of storage-related conditions.
- Save administration time by automating the monitoring of storage resources.

Product Solutions

ABC Industries wanted to closely monitor storage resources and events. To do this, they used many of the available alert conditions:

Level	Alert When…	Description
File System Group	Amount of free space falls below a threshold	In addition to managing their disk space, the system administrators also monitor the amount of space remaining in file systems. This allows them to respond to space-related conditions before they become issues.
Domain	New unmanaged computer is discovered	Alerts the system administrators when a new computer comes online. Previously, IT was not always informed when new Windows NT servers came online, and they might have wanted to add these servers to the nightly backup list.
Computer Group	Computer could not be contacted for a scan	ABC Industries uses this alert condition to receive notice about machines that might have crashed.
	Amount of RAM has changed between scans	IT wants to know when memory modules have failed or have been transferred between machines, so Janet uses Capacity Reporter to keep track of the RAM in the company computers.
	New or missing file systems or disks are discovered during scan	ABC Industries uses this alert condition to notify system administrators of changes in disk subsystem configurations. This can also indicate that a standalone disk has stopped spinning, or that a RAID box or controller has malfunctioned. The alert allows them to respond quickly with changes to the configuration of backup software and Capacity Reporter file-system groupings.

Level	Alert When...	Description
	New disk defect is discovered	ABC Industries uses hardware RAID; in addition, they need to monitor standalone drives and software RAID machines. Because these drives have no fault tolerance protection, the system administrators use this alert to signal when drives are showing signs of failure. Upon receipt of such an alert, the drive is replaced. This allows the administrators to avoid downtime by replacing failing drives during off-hours.
Directory Group	New managed directory is discovered	ABC Industries has a users' share point off which user home directories reside. As managers add and remove employee directories, the system administrators receive notifications. This practice ensures that they know when a new employee starts or when an existing employee is removed from the group. For more information, see Chapter 7, User Consumption Management.
	Directory Group Member exceeded quota	ABC Industries is implementing Capacity Reporter's quota management by directory as a means to educate, notify, and condition their user community on the consumption of disk space.
User Group	User Group Member exceeded quota	ABC Industries sites are implementing Capacity Reporter's quota management by user group as a way to educate, notify, and condition their user community on the consumption of disk space.

Implementation

Key Concepts

- File system groups
- User groups
- Directory groups
- Computer groups
- Default groups – Used to assign a default user quota, default directory size quota, and default file system free space threshold. All new resources are automatically placed into default groups. In addition, Windows NT security groups can be imported into custom Capacity Reporter groups.
- Scanning / data collection – Dictates how often the above alert conditions are checked and alerts triggered.

Configuration Steps

To implement Capacity Reporter alerts, Janet and Andy configured Capacity Reporter as follows:

1. Create groups

   a. Create file system groups based on the function of the server on which they reside. Janet and Andy have created groups for:

   - NetWare file and print servers
   - Web servers
   - Database applications servers
   - NetWare file server

   b. Create user groups – Import Windows NT security groups as Capacity Reporter user groups. This lets the administrators use predefined departmental groups, and automatically updates Capacity Reporter user groups as membership in the Windows NT groups changes.

   c. Create directory groups – Import Windows NT security groups as Capacity Reporter directory groups. This has the same benefit as user groups.

   d. Create computer groups based on geographical location.

2. Set scan time by group. Alert conditions are reported at scan time:

   a. Set the file system group/detailed file scan for file system groups. This scan picks up file-level details. Andy and the administrators at remote sites usually schedule these scans for off-hours, after the system backup completes, so that Capacity Reporter can identify vulnerable files, and because of the load this scan can put on the ABC Industries servers.

   b. For more information on the impact of scans on the network, see Appendix C, Network and System Impact.

   c. Set the scan interval for computer groups to every 15 minutes. To maintain a high level of server availability, ABC Industries wants to avoid downtime caused by out-of-space conditions. To achieve close to real-time monitoring, they set this scan interval to 15 minutes. This scan puts very little load on the network, and detects computer and file-system-level alert conditions.

   d. Set the scan interval for domain scans. Because IT cares only about the names of unmanaged computers and file systems, they always select the **Contact Domain Controller** option for faster performance and less load on the network.

3. Assign alert conditions and delivery vehicles by group:

a. Domain-level alert condition selected: **New unmanaged computer discovered**. Because it cannot be determined at which site the new unmanaged computer resides, all system administrators are notified via e-mail.

Alert When	Alert Via
☑ New unmanaged computer detected	☐ SNMP Traps (not enabled) (SNMP not installed)
☑ Number of SRM Agent licenses assigned exceeds number available	☑ Windows NT Event Log Messages
☑ Domain unreachable	☑ E-mail Message to:
☑ Import scan failed	`Hhoncho, Area1SysAdmin, Area2SysAdmin, Area2SysAdmin, HomeOfficeAdmin`
	Separate addresses with a comma (,).
☐ Send a test alert on Submit	
Submit Reset	

b. Computer group-level alerts selected:

Note – Because computers are grouped by region, computer group e-mail alerts are sent only to the system administrators at remote sites responsible for the computer group in which the alerting computer resides.

Alert When	Alert Via
☑ Computer could not be contacted for a scan	☑ SNMP Trap
☑ Amount of RAM changed between scans	☑ Windows NT Event Log Messages
☑ New or missing file systems or disks detected during a scan	☑ E-mail Message to:
☑ New disk defect detected	`Hhoncho,Area3SysAdmin`
☑ Disk health setting changed outside SRM	Separate addresses with a comma (,).

c. Because the conditions above could indicate server degradation, ABC Industries has configured alerts to be sent via the SNMP framework as well as to the Windows NT Event Log and via e-mail. Computer groups are set up by site.

File System group-level alert – Amount of space falls below a threshold. Threshold amount is set by group. The system administrators always use a percentage thresh-

old. The more mission-critical the applications are in a file system group, the higher the percentage specified.

    d. Directory group alerts

        i. New managed directory discovered – E-mail is sent to remote site system administrators. New directories are automatically assigned a quota, and administrators receive alerts about the new directories, so that they can change their group assignment.

        ii. Select the **Members exceed their quota** check box**,** and set the quota value – In addition to the department manager and remote site system administrators, automatically send e-mail to the over-quota user, restating the quotas by directory.

Alert When	Alert Via
☑ Directory not found	☐ SNMP Trap (SNMP service needs to be restarted)
☑ New managed directory	☑ Windows NT Event Log Messages
☑ Members exceed their 100 MB quota	☑ E-mail Message to: Hhoncho, Area3SysAdmin Separate addresses with a comma (,). ☑ E-mail Message to Over-Quota Directory Owner ▼

    e. User group-level alert – Select the **Members exceed their quota** check box. Set user quota level and automatically alert over-quota user(s) and send e-mail to the department manager and remote site system administrators.

Alert When	Alert Via
☑ Members exceed their 200 MB quota	☐ SNMP Trap (SNMP service needs to be restarted)
	☑ Windows NT Event Log Messages
	☑ E-mail Message to: Hhoncho, Area3SysAdmin Separate addresses with a comma (,). ☑ E-mail Message to Over-Quota User(s)

f. Event log - The ABC Industries system administrators always send Capacity Reporter alerts to the Windows NT Event Log. This practice gives the administrators an interface to a paging system. In addition, for those administrators using a Windows NT Event Log scraper, their centralized view of the distributed event logs contains the Capacity Reporter alerts.

4. Set alert "persistence":

Because Janet wants to closely manage by exception, the administrators set alerts to remain on Capacity Reporter's Current Alerts page for one day, so that alerts are recorded daily. They do this on the Options page under Alerts/Quotas.

Analyze Results

Once the system administrators have configured Capacity Reporter and at least one set of scans has successfully completed, they regularly review the following:

■ Alerts - The Current Alerts page contains a complete list of all alerts that have been triggered. The administrators view the page every morning and mid-afternoon to remain aware of key storage conditions. When necessary, they drill down from this page to view resources at risk.
■ Threshold levels - Are any file systems close to exceeding their assigned free space threshold?
■ Quota levels - Are too many users or directories already over quota?
■ User Consumption | Usage Report - Which users are the biggest consumers of space?

Take Action

Based on their findings, the system administrators work with their end-user community to refine the environment and adjust the Capacity Reporter configuration. The adjustments they make include:

■ Adjust quota levels - If too many resources are already over quota, quota levels might have been set too low. The administrators adjust the levels upward, and monitor the effect.
■ Identify at-risk systems - Having identified file systems that are often at risk of running out of free space, they take the appropriate action. If the data in these file systems is noncritical, they move it to offline or near-line storage; if it is critical, they plan to buy more storage.
■ Adjust disk allocations - The administrators revisit disk space allocations on servers that are most often running out of space, and adjust the allocations as necessary.

User Consumption Management

Objective

The ABC Industries CFO gave the IT department the task of reducing costs by controlling disk space consumption and the time required to manage disk space usage. Key to achieving these objectives is the implementation of a comprehensive user consumption management solution. This includes quota management, that addresses the high rate of consumption of disk space by end users.

ABC Industries has found that the placement of Internet downloads and e-mail attachments on corporate file servers is one of the primary causes of disk space consumption. Because of this, the IT staff also needs detailed usage reports that allow them to understand the nature of disk space consumption (what type of data users are placing on corporate file servers).

Another issue facing IT is dealing with space consumed by users who are no longer employees. After ensuring that these files have been backed up, the IT staff wants to reduce overall disk space usage by identifying and deleting these "orphan" files.

Further, ABC Industries has a corporate policy for charging departments based on their actual consumption of disk space. The IT staff needs a way to accurately and effectively report consumption by department or workgroup. For budgetary reasons, each department needs to project future usage based on prior consumption. This objective is discussed in Chapter 8, Storage Usage Chargeback.

Product Solutions

Capacity Reporter supports two methods of implementing user quotas:

- By user home directory
- Networkwide by file ownership, which associates a file ID with an account user name

These methods can be used in conjunction with each other to create a third method that combines user home directory and networkwide file ownership.

User Home Directory

Capacity Reporter enables the system administrators to set user consumption limits (quotas) on individual directories. When a directory reaches its defined limit, the system administrator, as well as the user who is associated with the directory, can receive an alert about the over-quota condition. This customizable e-mail includes, by default, a link to the URL of the user's single directory report, where the user or administrator can view the largest files in the directory, the rate at which space is being consumed in that directory, and more. A user is associated with a directory (or directories) via the name of the directory, the owner of the directory, or a manual link. For example, you can associate the Windows NT directory C:\users\ejones, or the UNIX directory usr/ejones, with a user account name of "ejones".

You can configure Capacity Reporter to automatically manage and assign quotas to first-level directories off a share point. For example, when a shared directory called "Users" is set to a state of "Manage Sub-Directories", directories such as Users\ejones, Users\hsmith, and so forth are automatically managed and assigned the quota associated with their respective group. When Windows NT security groups are used to create Capacity Reporter directory groups using Capacity Reporter's built-in import capabilities, Capacity Reporter also automatically places newly discovered directories in the appropriate group, eliminating the need for manual group membership management. These features automate the process of assigning quotas to new employee directories.

Networkwide by File Ownership

Capacity Reporter also lets administrators set networkwide quotas on individual users. This method uses the ownership attribute of individual files to calculate and alert on cross-server or networkwide disk space usage. This file ownership approach allows administrators to do the following:

- Identify all the storage space consumed by each user in a single report
- Receive alerts about over-quota users as well as automatically notifying them

File ownership can become clouded when files expected to be owned by an end user are reported as owned by "administrator" or "unknown". Files reported as owned by "administrator" were likely placed on the server with a user who is a member of the Administrators group. This can occur when files are migrated from one location to another. File ownership can also be inadvertently assigned to "administrator". However, as soon as the user saves such a file that they have modified, that user's ID is assigned as owner of the file. As users create new files on the file server, their user name is also assigned as the owner. As such, this approach effectively captures *incremental consumption* of disk space by users. Files reported as owned by "unknown" could be files owned by a user ID that no longer exists (at ABC Industries, this usually means former employees). Paging (swap) files could also be listed as unknown.

For NetWare, the owner of a file is the user who last modified the file, and the owner of a directory is the user who created it. If Capacity Reporter cannot determine file ownership, the file is unknown.

This method assigns quotas at the level of Capacity Reporter user groups. All members of a user group inherit the quota assigned to the group. When Windows NT security groups are used to create Capacity Reporter user groups, Capacity Reporter also automatically places newly discovered users (that is, user IDs) in the appropriate group, eliminating the need for manual group membership management. This feature automates the process of assigning quotas to new users.

Both User Home Directory and File Ownership

In environments where end users have the access privileges to save data in multiple locations in addition to their home directory, both of the above methods can be employed. This combination allows, for example, a quota to be assigned to a user's home directory as well as to other locations where they are consuming space, such as a project directory.

Selected Product Solutions

ABC Industries has different usage scenarios at the corporate office and the remote offices. Because of this, the IT staff uses all the Capacity Reporter user-consumption management features to implement the solution appropriate for each location. Andy and Janet also use Capacity Reporter reports to identify orphan files.

Corporate Office Implementation

The relatively large number of Windows NT and UNIX file servers in the corporate office has created a situation where users at the corporate office consume disk space on multiple servers. Each end-user at the corporate office has been assigned a user-specific home directory, and some have directories on Windows NT, UNIX, NetWare, and NAS servers. Users also place files in departmental share points and project directories. Because of this usage scenario, ABC Industries has decided to implement both of Capacity Reporter's user consumption management methods for their corporate-based users to gain complete coverage.

Implementation Steps

Creating the Directory Structures

1. Outside Capacity Reporter, Andy created a shared directory for each project.

2. Under each project-shared directory, he created a directory for each employee on the project.

3. If not already created, he also creates a **users** shared directory to host all user-specific home directories. He uses Windows NT User Manager to assign home directories to users off the **users** share point created above.

Note – Andy and Janet already had such a configuration, as is typical in Windows NT environments.

Viewing Usage Reports to Determine Quota Levels

Andy and Janet did not want to set an arbitrary quota level that might be too high or too low. Instead, they used Capacity Reporter's usage reports to determine an appropriate quota level to be assigned to user and directory groups.

1. They configured Capacity Reporter to manage the project and user directories noted above:

   - They initiated a **Scan Now** for the computer group(s) in which the computers hosting the newly created share reside.
   - They accessed the Directories-Share Points Report to view these automatically discovered share points and set their state to **Manage Subdirectories**.
   - They waited for the next detailed file system group scan to occur to update current usage levels of all first-level directories created off the share points managed above.

2. They viewed the Directories-Usage Report to see current consumption levels for user home directories to be assigned a quota.

3. They viewed the User Consumption-Usage Report to see current consumption levels for users to be assigned a quota.

Note – Users or User IDs per file ownership are automatically discovered. No additional post-installation configuration is required, as is the case with user home directories.

Setting Group Properties

1. Andy and Janet imported selected department-based Windows NT security groups as Capacity Reporter user groups and Capacity Reporter directory groups.

2. They also created a separate Capacity Reporter directory group for the project directories.

3. Janet set the following properties for each user and directory group via the group's Modify Alert Settings for Directory Group page (see the following screen):

   - Quota Level
   - Notification Vehicle
   - Select the **Email Message to Over-Quota Directory Owner** check box.
   - For directory groups containing end-user home directories, select "directory name".
   - For project directories, set the alias to the user(s) to be notified about an over-quota condition.

- Assign a system administrator to be notified when any member of the group exceeds the quota assigned to the group.

Alert When	Alert Via
☑ Directory not found	☐ SNMP Trap
	(SNMP service needs to be restarted)
☑ New managed directory	☑ Windows NT Event Log Messages
☑ Members exceed their 100 MB quota	☑ E-mail Message to:
	AHarty,JSilverheels, KHartshorn,MWesson, RSmith,SJones
	Separate addresses with a comma (,).
	☑ E-mail Message to Over-Quota Directory Owner ▼

Subject and body for the Notification:	
Custom Subject:	User Home Directory Exceeded
Custom Body:	Your user home directory, %5, has exceeded its space usage quota of %8. At the time of this message %5 was using %9 of space.
	For details on corporate storage usage policies and suggestions on how to reduce consumption, please view http://intranet.joindustries.com/policies/storage.htm.

Note – Quota conditions are checked and over-quota users notified as a result of the next scheduled detailed, file system group scans.

E-mail Customization

Andy and Janet decided that they wanted to customize the text of the e-mail message that is automatically sent to over-quota users. The default text includes the current usage levels and quota. It also includes a link to the URL of the single user or single directory report so that the over-quota user can view usage details. They decided to add a URL link to a location on the company intranet that discusses the corporate policy on disk space usage and makes suggestions on how to reduce consumption. Andy customized the text of the e-mail messages sent to over-quota users via the Options | Groups | Alerts/Quota configuration page, as shown in the screen above.

Remote Office Implementation

The typical ABC Industries remote office has 1-3 Windows NT Servers — a File Server or two. Because there is usually just a single file server, users at these locations are restricted to a user-specific home directory where they can consume disk space. Therefore, ABC Industries has implemented quotas by user home directory only for the remote offices.

These remote offices are very concerned with budgetary issues, because they are charged for their usage of computing resources, including disk space. The managers at the remote offices need to predict future usage for budgetary reasons. To accomplish this, Andy and Janet again created Capacity Reporter directory groups based on Windows NT security groups. They created the directory groups by office location, which provided them with usage reports.

Implementation Steps

Having performed the steps noted above for the corporate office, implementing the quota management solution for the remote offices was somewhat redundant, and therefore, easier. For this reason, this section simply references many of the steps performed for the corporate office configuration:

1. Janet and Andy created directory structures as discussed above for the user home directories, if necessary.

2. They viewed usage reports to determine quota levels per the steps provided above. This includes first managing the first-level directories off the **users** share point.

3. They set group properties.

The text of the e-mail that is automatically sent to over-quota users was already customized earlier, so they did not have to repeat this step.

Identifying and Deleting Files Owned by Former Employees

Files owned by former employees are reported as being owned by "unknown", if the former employee's user account has been removed. Andy performed the following steps in Capacity Reporter to identify and delete these files:

1. He ran the User Consumption-Usage Report.

2. He sorted the report by user and scrolled down to the "unknown" user.

3. He then accessed the Single User Report for user "unknown" and scrolled down the File Systems Reports to view all the disk file systems containing files owned by former employees.

4. He then accessed each Single File System Report to run the File Details Report.

5. He then used Microsoft Excel to sort by user name and scroll down to files owned by "unknown."

6. After double-checking the Backup Coverage-Vulnerable Files report to make sure that none of these files were in a vulnerable state (not backed up since the last time they were modified), Andy deleted these files.

Note – Before deleting any unknown files, make sure that they are not paging (swap) files or something else that should be saved.

To reclaim the disk space consumed in user-specific home directories of former employees, Janet simply deleted those directories off the file system, after making sure, using the steps above, that the contents of these directories had been successfully backed up.

Andy and Janet repeated these steps monthly to regularly reclaim significant disk space.

Analyze Results

Each month, Andy and Janet revisit the user consumption levels that they have assigned. They review how many users are over quota to determine whether appropriate quota values have been set, and to identify users who are consistently over their quota. They send e-mail to these users and to the department manager with a listing of files owned by that user. This e-mail reminds users of the corporate policy on disk space usage, and asks that they reduce their disk space consumption.

Andy and Janet also generate reports for total consumption of storage by group. These reports are also e-mailed to department managers for their review.

Janet also speaks with the Help Desk staff to review how many calls were placed to the Help Desk regarding the over-quota alerts. They discuss how the text sent in the e-mail can be improved to help users understand why they are being alerted and how to reduce their consumption of disk space.

Storage Usage Chargeback

Objective

ABC Industries has a corporate policy for charging departments based on their actual use and consumption of disk space. The IT department needs a way to equitably charge each department for its storage consumption on the company's file servers.

Product Solutions

ABC Industries has grouped its users by department to achieve effective quota management. Janet and Andy also use these departmental groupings for chargeback purposes. Capacity Reporter provides the following reports:

- Directories | Usage Reports — For overall directory usage
- Drill down to a Directory Group — For a listing of all configured directory groups
- Drill down to a Single Directory Group — For a detailed listing of each directory in the group and the usage

Implementation

Janet and Andy followed these steps to implement their Capacity Reporter solution:

1. Configure Capacity Reporter features.

2. Analyze the results of the configuration.

3. Take action based on the results.

4. Adjust the configuration.

Configuration Steps

Before implementing a corporate chargeback policy, Andy and Janet completed the following steps:

1. Andy and Janet analyzed IT's cost for the file servers along with their management and support costs to calculate a usage rate per MB that could be used to charge departments.

2. They created departmental groups by following the steps outlined in the User Consumption Management section. They used the departmental groupings for both quotas and chargeback.

3. Because Andy and Janet planned to bill departments monthly, they decided to wait until they had a full month's worth of usage before they implemented their policy. They e-mailed an explanation of the new policy to the department managers.

Analyze Results

On the first day of the following month, Janet and Andy viewed the Directories | Usage Reports from the Tasks page. From here, they viewed the Single Directory Group report for each department. This report details the total usage for the department and the usage for each individual user home directory.

Take Action

Andy and Janet then printed a report for each department and applied the calculated rate per MB to provide a total cost for usage. These reports were distributed to each department manager and the accounting department to implement the chargeback policy. They also e-mailed the Single Directory Group report URL to each department manager so they could view usage rates of their employees.

Adjust Configuration

To continue to support and optimize the chargeback policy, Janet and Andy must:

- Recalculate the rate per MB as new servers and/or applications are purchased.
- Keep Windows NT department listings up-to-date for the most accurate billing.

Backup Planning

Objective

ABC Industries needs to plan its backup strategy effectively. The network bandwidth, media throughput, and capacity are known, so now ABC Industries needs to understand the company's data growth and the amount of time available in its backup window.

Backups have been consistently overrunning the backup window. The backup window is the time allotted to complete the backup during off-hours, when data is unavailable due to the backup. IT has to terminate any backups that are still running in the morning, so that the backups do not interfere with production work during regular hours. Because the backups are unpredictable, the administrators cannot coordinate them with other nightly batch jobs. Also, IT does not adequately know where to add a backup server to increase bandwidth.

Product Solutions

Because Capacity Reporter reports on file trends, the IT department can use these reports to view the rate of file creation, access, and modification. Data can be displayed in either graphical or table format. Understanding file trends is key to understanding current and future backup requirements; the rate at which files are modified and created drives the size and duration of daily incremental backups.

Specifically, the ABC Industries system administrators use the following reports in their backup planning:

Review this Capacity Reporter Report...	To See...
In the **Tasks** tab, choose **Incremental Sizing** from the Backup Planning menu	Backup Sizing trend reports that show how much secondary storage is required for *incremental* backups and provide historical trends for planning future resource needs.
In the **Tasks** tab, choose **Full Sizing** from the Backup Planning menu	Backup Sizing trend reports that show how much secondary storage is required for *full* backups and provide historical trends for planning future resource needs.
In the **Tasks** tab, choose **Incremental Balancing** from the Backup Planning graphic	Backup Optimizing reports that show how many files and how much storage are modified daily by computer so backup clients and servers can be efficiently balanced and backup window problems avoided.
In the **Tasks** tab, choose **Full Balancing** from the Backup Planning menu	Backup Optimizing reports that show how much storage is consumed by computer, so backup clients and servers can be efficiently balanced for full backups and backup window problems avoided.

The trends detailed in these reports allow the administrators to:

- Understand the company's data growth rate and show how much secondary storage is required for both full and incremental backups.
- Predict when the amount of time required to perform a backup, with existing hardware and software, will exceed the window of opportunity.
- Balance backup clients and servers so backup window problems are avoided.

Implementation

To use Capacity Reporter as a backup planning tool, the administrators did the following:

- They set the report size and history depth to collect and report the amount of information that made sense for their sites, so they could see the historical trend of which servers were the busiest over time.
- They viewed the File Distribution trend reports on a regular basis. Based on the trends reported over a 60-day period, the administrators identified the following:
- Consistent growth in data to be backed up
- Computers with the most files being created and modified

The computers with the most files being created and modified are the best candidates for backup servers, because this reduces the amount of data being transferred across the network. They used this information to justify the purchase of new backup hardware and software before a crisis developed.

Configuration Steps

Backup growth is an evolutionary process that is directly tied to file growth. The ABC Industries system administrators continually monitor the rate of file creation, access, and modification. To optimize their backup strategy, they take the following steps:

- They place most file systems in separate groups.
- They set the File System Scanner to run daily at 5:00 P.M., so that the scans finish by 6:00 P.M., enabling the administrators to estimate before leaving the office how much longer the backups will run.
- Based on their monitoring of file activity, they change the start time of the backup job to accommodate the amount of data to be backed up.

Backup Coverage

Objective

The system administrators recognize that they need to close the gaps in the ABC Industries backup strategy and to ensure that all modified files are backed up. Unfortunately, most backup applications themselves do not offer robust reporting. And, data integrity is far too important for IT to rely on a single tool, such as a backup application — they must always be able to restore files.

Based on their use of Capacity Reporter as a backup planning tool, the administrators found multiple points of failure in their past client/sever backup deployment:

- Files were left open overnight, and, in the absence of an "open file" backup option, could not be backed up by their backup software.
- Changes in disk I/O subsystems (new disks) and in file system letters meant that backups needed to be reconfigured.
- New computers were brought online without being added to backups.
- Certain files were inadvertently excluded from backups using the backup program's "backup exclude" list.
- There were problems with backup agents.
- There were problems with tape devices.

Product Solutions

Capacity Reporter has two types of reports and several alerts that identify backup problems for Windows NT computers:

- File Distribution by Vulnerability reports identify the size and number of files that have been modified but not backed up. Data can be displayed in either table or graphical format. These reports can be accessed from the Backup Coverage button on Capacity Reporter's Tasks page or from any domain, computer, or file systems report. The *Network wide* report on the Backup Coverage menu provides a table that shows the number and size of files modified but not backed up daily, weekly, monthly, and yearly across the network and shows how long a file has been in a vulnerable state.
- The *Vulnerable Files* report from the Backup Coverage menu on Capacity Reporter's Tasks page identify all files that have not been backed up by automatically monitoring an NTFS file attribute called the "archive bit". Backup applications use the archive bit to indicate whether a changed file has been backed up.

Note – The archive bit feature is not available with UNIX.

- New disks, new file systems, and new computers can all be flagged via alerts to ensure that new storage resources are known about and included in the backup job.

Review This Capacity Reporter Report...	To See...
In the **Tasks** tab, choose **Network-wide** from the Backup Coverage menu	Size and number of files networkwide that have been modified but not backed up.
In the **Tasks** tab, choose **Vulnerable Files** from the Backup Coverage menu	Top *N* oldest files that have been modified but not backed up (files were open, files were excluded from backups, backup jobs failed, and so forth).
From the Main Page, choose **Alerts**	New disks, new file systems, and new computers can all be flagged via alerts to ensure that new storage resources are known about and included in the backup job.

The ABC Industries system administrators use both types of Capacity Reporter reports to analyze the effectiveness of their backups. For example, if they see that a large number of files on a file system have not been backed up, they make sure to schedule the file system backup.

Implementation

1. ABC set file report size for domain to 200, which restricts the number of files listed in the Most Vulnerable domain reports to a maximum of 200.

2. They set report history to a maximum of 90 days, which restricts the amount of data displayed in a report to the last 90 days.

3. They created filters to exclude from backup coverage reports files that purposely have not been backed up. For ABC Industries, these files include .SYS and .TMP files in the /winnt directory on their servers. The administrators match Capacity Reporter filters to backup application filters.

4. They apply the filters to all file system reports and all vulnerability reports. They adjust the filters as necessary to ensure that all files of interest to them appear in these reports, and no others.

5. They examine Vulnerability reports for type, number, date, and location of files not backed up to find holes in their backup strategy.

6. They monitor the Alerts page for new disks, file systems, and computers that need to be added to the backup list.

Backup planning and analysis is an on-going process. The ABC Industries system administrators continually monitor the effectiveness of their backups, and make changes to their backup configuration and strategies as needed.

Physical Disk Analysis

Objective

The IT department must regularly predict the failure of disks in the environment to avoid the costs associated with a sudden disk failure. The company uses mostly hardware RAID, but has some standalone drives not protected from failure with the fault-tolerant capabilities of a RAID array. Therefore, ABC Industries uses Capacity Reporter to protect against failures in standalone disk drives.

Product Solutions

The system administrators monitor Capacity Reporter's Disk Defect analysis alerts to provide protection against failures. Specifically, they look at the following reports:

- Disk Drive | Defect Rate — Disk defects are new SCSI defective areas on a disk. New defects or an acceleration in the number of new defects are indications that the disk might be failing.
- Disk Drives | Performance — Displays the number of grown defects, date of last new defect, and total Spare Blocks.
- Disk Drives | Inventory — Displays the make and model of disks.

In addition, they monitor alerts for new disk defects discovered, which might indicate that a disk is about to fail.

Implementation

New or missing file systems or disks discovered during a scan might indicate that a disk has failed.

Key Concepts

The administrators use these sections of the Managed Disks Summary Report to generate the information they need to keep track of the health of disks, and predict failures:

- Scans: Computer Group Scan(s). Select Options, Scans, Computer Group
- Alerts: Computer Group Settings. Select Options, Groups, Computer Group

Configuration Steps

Capacity Reporter creates the Managed Disks Summary Report from the data collected during the Disk Scan that is run with the Computer Group Scan. To obtain the appropriate data:

1. They configure Alerts and the Alert methods:

Alert When	Alert Via
☑ Computer could not be contacted for a scan	☐ SNMP Trap (SNMP service needs to be restarted)
☐ Amount of RAM changed between scans	
☑ New or missing partitions or disks discovered during a scan	☑ Windows NT Event Log Messages
☑ New disk defect discovered	☑ E-mail Message to: Hhoncho,SysAdmin
☑ Disk health setting changed outside of SRM	Separate addresses with a comma (,).

2. They then configure Computer groups and the frequency of the scans:

Analyze Results and Take Action

After configuring the Managed Disks Summary report, alerts, and scans, the system administrators take the following actions:

1. They view the Disks Drives | Defect Rate from the Tasks page.

2. If the grown defect rate of a disk is steadily increasing, they drill down to view the individual disk report.

3. From here they can get the required asset information (for example, the disk's serial number), so they can issue a Return Materials Authorization (RMA) to return the disk to the manufacturer.

A disk defect in itself is not necessarily a sign of a bad disk, because the data is usually remapped to a good block. But the administrators know that an increasing trend in disk defects is a bad sign, and they make plans to proactively replace the disk during off-hours, to avoid downtime.

Adjust Configuration

After analyzing the results, the informed administrators can make any necessary adjustments:

- Are the correct people being notified of a potential disk space problem?
- Are the correct alerts set?
- Do any disks need to be replaced?

File Analysis

Objective

The ABC Industries IT department is committed to reducing the amount of storage space consumed by finding and deleting unnecessary files. This is an on-going, closed-loop process: Internet download, e-mail attachments, and multimedia files consume large amounts of space. To identify these file types, they use the following Capacity Reporter tools:

- Largest Files reports, at networkwide and file system levels, in conjunction with filters to find large and unnecessary files
- Stale file analysis
- Directory drilldown
- File Details report - comma-separated values (CSV) files

Largest Files Report

Largest Files reports are available for each domain, single computer, NAS filer, and managed file system.

Key Concepts

The administrators understand and use these Capacity Reporter features:

- Files Report
- Filters
- Scans: File System Group/File Detail Scan(s)

Configuration Steps

The administrators take the following steps to implement their solution to the disk space problem:

1. They apply Capacity Reporter's built-in, preconfigured graphics filter to the file server's file system groups.

2. They create a new filter to find games (for example, doom2.exe), and apply the filter to the file server's file system groups.

3. They create another filter for multimedia files such as *.MP3 and *.AVI.

4. They create a filter to exclude some *.DAT files on particular file systems, because they know that, although these files are very large, they should never be deleted.

5. They apply the filters to the Largest Files report via a file system group's Modify Filters for File System Group page.

6. They schedule scans to run at the time that makes the most sense for their site. File System Group/Detailed File scans must run to collect the data needed for the Largest Files report. Because these scans are the most resource intensive, the administrators typically schedule the scans to run during off-hours.

Note – All new "include" filters must also "exclude" all file types (*.*) in the File Specification Criteria section.

Analyze Results and Take Action

1. Once the scans have run, the administrators analyze the results by viewing the appropriate Largest Files report, from a Domain, Single Computer, or Managed File System report.

2. They identify files to be deleted.

3. They ensure that the files to be deleted are backed up and/or archived, if necessary.

4. After the files have been backed up, they use Capacity Reporter's directory drilldown feature to delete the files by clicking the Windows NT Explorer icon located in the Full Path column of a Largest Files report. A Windows NT Explorer window opens, displaying the directory containing the file of interest. From here they select a file and delete it or move it to a new location.

5. After analyzing the results, the filters might need to be adjusted to perform some additional customization of the Largest Files reports, for example, include or exclude additional files from reports.

Finding Specific File Extensions

The ABC Industries system administrators are particularly interested in finding .JPG files stored in their domains. Historically, these files are large and unnecessary.

Key Concepts

The administrators take advantage of these Capacity Reporter features:

- Largest Files Report
- Filters
- Scans: File System Group Scan(s)

Configuration Steps

First, an administrator creates a filter that excludes all files except .JPG files from the Largest Files reports.

Note that ABC Industries uses the Largest Files reports to solve other business problems. Applying the graphics filter on a permanent basis would be at odds with these solutions. Because of this, the graphics filter is applied only for a short period of time and during off-hours. The system administrators accomplish this by performing the following steps:

1. Remove all filters from file system groups and Largest Files reports.

2. Apply the graphics filter to all file system groups.

3. Apply the graphics filter to the Largest Files report only.

4. After scans have run, review the results in the Largest Files report.

5. Restore the customary filters for the file system groups and Largest Files report.

Note – All new "include" filters must also "exclude" all file types (*.*) in the File Specification Criteria section.

Action Taken

Once the scans have run, and the Largest Files reports have been reviewed, the system administrators can delete unnecessary .JPG files by clicking the Windows NT Explorer icon located in the Full Path column of the Largest Files report. A Windows NT Explorer window is opened, displaying the directory containing the file. From here they can either delete the file, move it to a new location, or identify it as a candidate for archiving.

Adjust Configuration

After analyzing the results, the filter might need to be adjusted to perform some additional customization to the Largest Files report. For example, an administrator might include additional files in, or exclude additional files from, the report.

Modifying a Standard Report

To find the specific kinds of files in the examples above, the system administrators simply modified the Largest Files report. Because the report can be part of multiple business solutions, all administrators who rely on the standard reports must agree to any modifications before they are made. For example, since File System Group scans (which are time consuming) collect the Largest Files Report data, it might not be practical to run these scans during normal business hours. If the administrator needs this information quickly, comma-separated values (CSV) files might be the answer (see below).

Using File Details Report

After reviewing file reports by size, creation date, modification date, access date, and vulnerability, the administrators might choose to find the files that make up a segment from the group by using Capacity Reporter's File Details reports. Once the files are found and analyzed, the administrators can take the appropriate action.

Comma-separated values files, found in Capacity Reporter's Single File System report, can also help administrators analyze the files targeted by filters. Filters do not affect the contents of a File Details report. Every file on the file system is listed in the File Details report. CSV files are file-system-specific; they are not rolled up into a single report.

Key Concepts

The administrators take advantage of these Capacity Reporter features:

- File Details Report (CSV file)
- Scans: File System Group Scan(s)

Configuration Steps

An administrator follows these steps to use CSV files to examine files of interest:

1. Configure File System Groups to collect detailed information by selecting **Collect file details on these file systems**.

Note – File System Group scans must complete before the CSV files are viewed.

---

2. View the CSV files from Capacity Reporter by selecting the **File Details Report** or **Directory Details Report** icon on a Single File System report. By default, Microsoft Excel is opened if it is installed on the machine viewing the Capacity Reporter Web; otherwise, the administrator is prompted for an application with which to open the file.

Note – Capacity Reporter uses Microsoft Excel for viewing CSV files in Capacity Reporter. Excel can view up to 64,000 records. If there are more than 64,000 files on the file system, the administrator can import the data into Microsoft Access for viewing. This also allows the administrator to write queries to perform the analysis.

While Capacity Reporter's CSV files contain the attributes for files located on a specific file system, the File Reporter option can obtain this information across the enterprise. File Prospector software allows you to create detailed custom reports not available using Excel.

Analyze Results and Take Action

As shown in the following section, ABC Industries uses the CSV files to identify stale files and orphan files.

Stale File Analysis

The ABC Industries system administrators want to locate files that are not actively used, so disk space can be reclaimed and unnecessary storage purchases deferred or even avoided. They can also reduce the length of the backup by not including stale or unnecessary files.

Key Concepts

The administrators understand and use these Capacity Reporter features:

- Stale File Analysis Charts, which are available networkwide for all domains and by single computer and managed file system
- File Distribution By Access Date Reports
- File Details Report (CSV file)

Configuration Steps

The administrators take the following steps to identify stales files across the network and reclaim wasted disk space:

1. They configure file system groups to collect detailed information by selecting the **Collect file details on these file systems** option.

Note – File System Group scans must complete before the CSV files are viewed.

---

2. They schedule scans to run at the time that makes the most sense for their site. File System Group/detailed file scans must run to collect the data needed for the Stale File Analysis. Because these scans are the most resource intensive, the administrators typically schedule them to run during off-hours.

Analyze Results and Take Action

1. Once the scans have run, the administrators analyze the results by viewing either the Stale File Analysis Pie Chart from the File Management menu, or the appropriate File Distribution by Access Date report for All Domains, Single Computer, or Managed File System report.

2. From the Stale File Analysis Pie Chart, they identify the computers with the most stale files and drill down on that computer from the pie chart to bring up the Single Computer report.

3. From the Single Computer report they drill down on a file system name to bring up the Single File System report.

4. They identify the files that have not been accessed in a period of time by selecting the File Details report (CSV file) and sorting the Excel spreadsheet by access date.

SAN Planning

Objectives

The ABC Industries IT department decided what critical data and applications warranted the added cost and complexity of implementing a storage area network (SAN). They also decided what storage should remain on less costly server-attached RAID or JBOD (Just a Bunch of Disks). They decided the most obvious elements for SAN migration would be the storage-intensive and mission-critical applications, such as transaction processing, e-mail, GroupWare, ERP, multimedia file serving, and database acceleration. They wanted the following SAN advantages for these applications:

- Greater application availability – Because SAN storage is externalized, it can be accessed through alternate data paths (for example, clusters), eliminating single points of failure.
- Better application performance – While server-attached storage is limited by the server's CPU speed and activity and bus overhead, SAN is server-independent, so is not impacted by its host, and like conventional subnets, adds bandwidth without placing more overhead on the primary LAN.
- Practical data movement – SANs enable cost-effective implementations of high-availability disaster protection configurations such as remote clusters, mirroring, and vaulting.
- Centralized storage – By providing the means to consolidate storage, SANs deliver greater scalability, reliability, flexibility, and serviceability.

The IT managers wanted to determine how to partition the storage arrays that are part of the SAN, as mandated by user needs. They needed to answer the following questions before configuring their SAN:

- What servers and workstations will have access to which SAN file systems?
- What kinds of user activity is expected?
- How much capacity should each SAN file system have?
- Which SAN file systems should be shared by more than one server for failover?
- What should be the ratio of application files to data files?

The managers realized that several servers would be sharing an array, and did not want the servers to go offline if the array went down. For server dependability, the managers decided on a high availability strategy, and to use a fully redundant storage device that utilized their hardware RAID. They decided to take advantage of Capacity Reporter's clustering abilities for even greater availability, and to use remote mirroring to protect the most mission-critical data.

To avoid performance issues, the managers wanted to set up locations where a storage pool could provide capacity to as many servers as possible, keeping the maximum distance between storage pool and server to 500 meters. They matched up the most demanding servers with the highest performance arrays, and used multiple arrays and multiple data paths between the servers and arrays. They also allowed for expansion in arrays where growth was expected. Additionally, they decided on Fibre Channel arrays with features such as LUN masking and load balancing, so that one array could provide storage capacity to multiple servers. This strategy allowed them the capability of adding more capacity by reprogramming the array or the switch rather than buying a new array and cabling it into the SAN.

Available Capacity Reporter Solutions

- Determine what storage to migrate to a SAN.
- Configure the SAN to accommodate user needs after analyzing existing network storage.
- Manage the SAN with tools that provide ongoing monitoring, reporting, and analysis.

Selected Capacity Reporter Solutions

Once all managed resources had been scanned, the IT managers reviewed the following Capacity Reporter reports:

Review these Capacity Reporter Reports ...	To see ...
File Distribution by Size for File Systems	Where the largest files are located. The administrators can then drill down for details and determine if this storage could benefit from migration to a SAN.
Backup Planning Reports	Backup requirements for needed data. How much needs backing up, how often, how long a backup window is needed.
Users Reports	Network consumption rates and historical trends for individual users and groups of users. Identifies user activity needs, consumption needs, peak access times, and high-demand users.
Computers Reports/Directories Reports	File-system capacity requirements.
File Systems Reports	Disk partitions on the SAN, file-system capacity, free space, used space.

Additionally, the File Reporter option provides powerful tools to audit the network storage for planning and migration purposes. Reports apply to either an entire NT-based network, specific file systems, or servers. File Reporter software can provide custom report-writing capabilities on a number of file attributes, including location, owner, size, and time-date stamps, enabling the IT managers to audit storage prior to implementing a SAN.

Analyze Results

The IT managers monitored both logical and physical resources once the SAN had been deployed. They went back to the Capacity Reporter reports and examined line charts to see trend lines. They used Capacity Reporter to provide user consumption, incremental and full backup sizing reports, file access, modification, and creation rates by file system, and historical planning trends. They optimized SAN performance and ensured SAN availability, identified bottlenecks, and forecasted growth. They configured alerts and thresholds for remotely mounted directories (share points) and for each group of file systems, allowing different thresholds on different file systems.

Database Management

Capacity Reporter allows you to drill into databases to see files, log space, data space, free and used data and log space, and more.

Objectives

Janet and Andy compiled the following list of objectives for managing ABC Industries' databases:

- Understand and predict the rate at which databases consume space, so they can plan when to add physical disk space (see Case Study 1: Predict Database Growth Rate).
- Identify databases whose availability could be compromised in the near future (see Case Study 2: Identify Vulnerable Databases).
- Defray the IT costs of maintaining and storing database information by distributing the costs across the business units that use particular databases (see Case Study 3: Chargeback for Database Space).
- Receive notification of database storage-related conditions automatically (see Case Study 4: Manage Database Storage Using Alerts).

Case Study 1: Predict Database Growth Rate

Janet and Andy wanted to identify the fastest-growing databases, so they could be prepared to add more storage as needed.

Product Solutions

Janet and Andy decided to use the graph feature in Capacity Reporter's Summary for Single Database Report to investigate the growth rate of ABC Industries' databases. They then used Capacity Reporter's cross-linking feature to help them plan when to add physical disks.

Implementation

Janet and Andy took the following steps to implement their Capacity Reporter solution:

1. Viewed the growth rates of their databases, by taking the following steps:

   a. From the Capacity Reporter left-hand navigation frame or Resource page, they clicked **Databases**. The Managed Database Summary for All Domains was displayed.

   b. They clicked on the "Sort Descending" (downarrow) button in the **% Used Data Space** column, to sort from most-to-least percentage used data space.

   c. They clicked on the graph button in the **% Used Data Space** column. In the graph, databases with the highest growth rates were obvious.

Note – Databases with high percentage used data space, but low growth rates are usually not a problem. However, databases with high percentage used data space and high growth rates are potential problems.

---

2. From the data provided by Capacity Reporter and from their knowledge of each database's purpose, they compiled a list of databases with potential space problems.

Configuration Steps

After compiling the list of "potential troublemaker" databases, Janet and Andy took the following steps:

1. They drilled down on the "troublemakers" to determine issues involved:

   a. They clicked on the database name to see more detailed information and analyze it.

   b. They reviewed the Database Files Report (on the same page) to see if the database was spread across multiple disk drives.

2. They determined the possible remedies for "troublemaker" databases, including:

a. Increasing the size of the Sybase devices or the Oracle files that make up each database. However, Janet and Andy had to ensure that there was enough disk space for the expansion.

b. Because they had the Capacity Reporter for UNIX agent installed, Janet and Andy were able to click on the file system crosslinks in the Database Files Report to see if there was enough disk space to allow for increased database size.

If there was not enough disk space to allow for expansion, they went to the Computer Report (by clicking on the hyperlink to the computer name at the top of the Database Report). They searched for disk space to use for the expanded database files.

The advantage to this remedy was that Janet and Andy would not have to buy new hardware.

c. They searched for underutilized servers that had a good deal of free disk space. Perhaps storage space could be reallocated from that server to the "troublemaker" database server. Again, Janet and Andy would not have to buy new hardware.

d. If neither of the previous remedies worked, Janet and Andy would have to buy more storage hardware, secure in the knowledge that their existing storage was being used effeciently.

Analyze Results

After analyzing the information in the Database Files Report and hyperlinking to the Computer Report to search for available storage space, Janet and Andy found that some storage hardware was available to be reallocated to their "troublemaker" databases.

Take Action

Janet and Andy reallocated some storage hardware and thereby removed the "troublemaker" status from some of the databases. For the remainder of the "troublemaker" databases, they purchased new storage hardware, secure in the knowledge that there was no other storage hardware available at their site.

Case Study 2:
Identify Vulnerable Databases

Janet and Andy wanted to identify databases whose availability could be compromised in the near future. They decided that a "vulnerable database" meets one or more of the following criteria:

■ Percentage of used data space is high (current free data space is low)
■ Database growth rate is high

Product Solutions

The Managed Database Summary for All Domains report provides information on the criteria that Janet and Andy chose.

Implementation

Janet and Andy took the following steps to implement their Capacity Reporter solution:

1. From the Capacity Reporter left-hand navigation frame or Resources page, they clicked **Databases**. The Managed Database Summary for All Domains was displayed.

2. To check for percentage of used space:

   a. In the % Data Used Space column, they clicked on the down arrow to sort the column in descending order of used data space. The databases with the greatest percentage of used space displayed first in the report.

   b. If the percentage of data space used indicated that a particular database's availability was in danger of being compromised, they took corrective action.

3. To check on the growth rate and/or current free space of a particular database:

   a. They clicked a single database name from the Managed Database Device Summary for All Domains report. The report for the selected database was displayed.

   b. In the Database Report, they clicked on the graph button to the left of **% Used Data Space**. The **History of % Used Data Space** graph depicted the database's growth rate. If the database seemed to be growing at an alarming rate, they took corrective action.

Configuration Steps

Janet composed a memo to the database administrators at corporate headquarters, requesting that they follow the procedure she and Andy devised to ensure that access to mission-critical databases was not endangered. She requested that the database administrators perform this procedure once per week for three months and that they keep a log of downtime of mission-critical databases during the same period.

Analyze Results

After tracking results for three months and comparing those results against the previous three month period, Janet discovered that the downtime for mission-critical databases declined by 5%.

Take Action

After sharing the results with the database administrators who had participated in the experiment and receiving their endorsement for the procedure, Janet and Andy decided to permanently implement the "search for vulnerable databases" procedure at corporate headquarters.

Case Study 3: Chargeback for Database Space

ABC Industries wanted to implement a corporate policy to defray the IT costs of maintaining and storing database information by distributing the costs across the business units that used particular databases. The IT department needed to determine how much to charge each business unit.

Product Solutions

Janet and Andy decided to implement database groups to charge each business unit for the databases it owned. They also decided that billing would be based upon the total space allocated for the database, not just the amount of space being used at any one time.

Implementation

Janet and Andy took the following steps to implement the Capacity Reporter solution:

1. They set up database groups according to business unit or department.

2. They used the Managed Database Groups Summary report's Database Group Description column to verify the business unit to which the database group's costs should be charged.

3. They charged the appropriate business unit for the database space it used. To calculate this charge, Janet multiplied Total Space by cost per MB to determine the amount to bill to the business unit. (See the Database Report at the bottom of the Summary for Database Group to find Total Space for a particular database group.)

Configuration Steps

Andy informed the manager of each business unit that, within 6 months, each business unit would be billed for the IT costs of maintaining and storing its database information. He further informed them that, for the next 3 months, they would receive a "test" bill (no payment required), which they should use to verify that they were being billed for the correct databases. At the end of that 3 month period, corrections would be made to the list of databases owned by each business unit. Then actual billing would begin.

Analyze Results

After some vicious infighting between business unit managers over the ownership of certain databases, Janet, Andy, and the business unit managers were able to come to an agreement about which business units owned which databases. Billing began in earnest. Analysis of IT department costs showed a significant drop.

Take Action

The experiment was so successful that Andy decided to take it a step further. In addition to the cost of hardware, he decided to include the cost of overhead, network infrastructure, and resources to the chargeback costs. This resulted in another significant drop in IT department costs, and a more accurate portrayal of each business unit's costs.

Case Study 4:
Manage Database Storage Using Alerts

ABC Industries' database administrators wanted to be notified when:

- A database could not be accessed
- A database's transaction log free space fell below 10%
- A database's data free space fell below 20%

Product Solutions

The database administrators decided to use Capacity Reporter's database alert feature to automatically monitor database accessibility and storage space.

Implementation

The database administrators created the following plan to implement their Capacity Reporter solution:

1. They created database groups containing databases of approximately the same size and which were accessed at approximately the same rate.

2. They set alerts for the following conditions:

   a. Managed database scan failed

   b. Amount of transaction log free space less than 10%

   c. Amount of data free space less than 20%

3. They configured the alerts so that they were notified automatically by e-mail. They monitored the alerts received by email closely for one week to verify that they were receiving notification of problems in time to take corrective action that would prevent a serious problem from occurring.

Configuration Steps

The database administrators took the following steps to implement their Capacity Reporter solution:

1. Janet and Andy created the following new database groups: SmallDB, MediumDB, LargeDB, using the following steps:

   a. They clicked **Options** in the Capacity Reporter's banner frame. The Options main page was displayed.

b. They clicked **Alerts**. The Select Group page was displayed.

c. They clicked **New** in the Database Group row. The Group Properties for new Database Group page displayed.

d. They entered a name and description for the new database group and clicked **Submit**. The Summary for Database Group page was displayed.

e. They clicked on **membership** in the lefthand navigation. The Modify Group Membership for Database Group page was displayed.

f. They selected the databases to include in the group, then clicked **Submit**.

2. They set alerts for the database group:

a. Andy clicked on **alerts/quotas** in the lefthand navigation. The Modify Alert Settings for Database Group page was displayed.

b. In the **Alert When** column:

i. Andy selected the **Managed database scan failed** check box**.**

ii. Under **Critical Level**, he selected the check boxes **Transaction log free space less than** and **Data free space less than**.

iii. He set the Transaction log free space alert to 10%.

iv. He set the Data free space alert to 20%.

v. He selected a mechanism by which database administrators would be notified of alerts.

vi. He clicked **Submit**.

Analyze Results

During the week that they were closely monitoring the alerts they received, the database administrators decided that the transaction log free space setting was overly cautious. They decided to lower that alert setting to 5%.

Take Action

After lowering the transaction log free space setting, the database administrators were confident that they would be notified of database storage problems in a timely manner. They were also confident that they would be notified if a database scan failed, indicating one of the following possibilities:

- The database's host computer might be down or not connected to the network during a scan
- The database server process might not be running
- Security credentials may be set incorrectly

Solutions to Give You a Competitive Edge

Problem: Unrecoverable Files Threaten Business Continuity

Making sure you can fully recover every file in the event of a system failure is critical. Not knowing if your nightly backups are complete can put the continuity of your business in jeopardy. Backup application logfiles are often scattered across your network, making them impossible to consistently monitor. Furthermore, backup applications fail to report files that they can't "see" (for example, files stored on new file systems or disks, files inadvertently excluded from nightly backups, and so on).

Solution: Capacity Reporter automatically scans the Windows NT File System (NTFS) attributes of every file in your Windows NT enterprise to independently validate recoverability, and creates Vulnerable File reports that list all unrecoverable files (files that have not been backed up since they were last modified) to ensure full data protection.

Problem: Capacity Shortages Create Unwanted Downtime

Network storage capacity shortages occur, resulting in spending precious time reacting to capacity-related downtime when you are needed on other projects and compliance testing.

Solution: Capacity Reporter's networkwide capacity reports, thresholds, and alerts help you to ensure that no file system is close to out-of-space levels, while Capacity Reporter's planning trends enable you to anticipate future capacity needs and avoid capacity shortages. Capacity Reporter's File Access and Stale File reports help you maximize your existing capacity, while its Capacity Planning trends enable you to predict your growing needs in advance so that you are not spending time in a panic paying top dollar for more storage.

Problem: Incomplete Asset Management Can Leave Your Business Exposed

Storage is, arguably, your most critical enterprise computing resource, because it contains all your data. Taking a central inventory of every logical and physical storage resource in your enterprise could occupy your entire IT staff, and general-purpose system and asset management tools do not provide the depth necessary to fully audit and analyze network storage.

Solution: Capacity Reporter automatically discovers, inventories, and monitors every disk, file system, share point, directory, and file on your network, and produces centralized Asset Management reports that can be easily accessed through any web browser to audit your enterprise storage. Firmware revisions for every server and workstation disk, formats for every file system, and business unit dependencies for storage groups are easily and instantly obtained.

Problem: Slow Data Recovery Costs Organizations Time and Money

If you have had to recover deleted, misplaced, or corrupted files from backup tapes, you know it can be a slow process. That means downtime to your end users. The speed with which you can recover your data determines how much downtime your users suffer, and how much productivity and money your organization loses.

Solution: Capacity Reporter automatically scans your enterprise storage and creates Largest File reports that identify space-consuming files, enabling you to reclaim capacity, reduce the amount of data you back up each week, shrink the number of tapes you need for backup rotations, and, ultimately, recover data faster.

Problem: Storage Cleanup Costs Your IT Organization More Time and Money

IT organizations are faced with thousands of redundant files, never-ending backups, unbalanced file servers, and capacity shortages.

Solution: Capacity Reporter automatically scans your enterprise storage and produces web-based reports that alert you to stale files, large files, and duplicate files and shares that can be deleted or archived to reclaim wasted storage capacity.

Capacity Reporter Maintenance

Perform the tasks on these lists regularly.

SQL Server

- Perform tape backups of the Capacity Reporter database.
- Ensure adequate disk space for the Capacity Reporter database installation. For guidelines, see the *Sun StorEdge™ Capacity Reporter Configuration and Installation Guide.*
- Adjust locations of dumps (data and log) as necessary.

Capacity Reporter

- Adjust thresholds.
- Review new resources and move them to the appropriate group.
- Review and adjust membership of local groups.
- Set membership of the Capacity Reporter Users and Capacity Reporter Admin groups.
- Review the unmanaged computers list to determine if you need more licenses.
- Review available licenses.
- Review grayed-out report cells for incomplete scans.
- Review the Event Log (Application) for incomplete scans.

Network and System Impact

This appendix discusses system, network, and security considerations for deploying Capacity Reporter on your heterogeneous network.

Capacity Reporter's Impact on Resources

Area	Impact
Disk	Capacity Reporter Server requires 53 MB.
	Capacity Reporter Agent requires 5 MB.
	Size of Microsoft SQL Server database is a function of the number of resources managed. Resources include servers, disks, file systems, directories, and users. For example, with 50 managed servers, 5000 users, and 5000 directories, the database grows to about 2.5 GB when daily historical data is retained for one year.
Memory Impact	The memory footprint for each Agent when idle is about 3 MB, and when active, reaches about 7 MB of physical memory and between 35–45 MB for virtual memory.
CPU Impact	The CPU usage for the Capacity Reporter Server when idle is 0% of your CPU. When actively collecting data from the Capacity Reporter Agents and entering the data into the Capacity Reporter database, the amount of CPU usage changes, depending on the type of scans performed. Computer Group scans are relatively quick (10 seconds per Capacity Reporter Agent machine) and do not use much CPU.
	Computer Group Scan: When active, a small percentage of your CPU cycles are used to collect, process, and enter the data into the database. This is measured in single seconds.
	File System Group Scan: When active, approximately 40 - 50% of your CPU cycles are consumed while collecting and entering the data into the Capacity Reporter databases. This is for a short period of time while collecting the filtered rollup of the top N files, user data, and directory data. The amount of time is a function of the number of users, managed directories, and size of your top N file lists being sent over from the Capacity Reporter Agents, not the amount of data on the agents. The time of this usage is measured in tenths of a second.
	CPU usage for the Capacity Reporter Agent is about 0% when idle. When actively scanning the computer, the amount of cycles changes depending on the type of scan being performed.
	Computer Group Scan (Capacity Reporter Agent): When active, a small percentage of your CPU cycles are used to scan, collect, and send the data back over to the Capacity Reporter Server.

Area	Impact
	File System Group Scan (Capacity Reporter Agent): When active, approximately 40 - 60% of your CPU cycles are consumed while scanning, collecting, and sending the data back to the Capacity Reporter Server. The Capacity Reporter Agent scans between 250 and 500 files per second. 200,000 files takes between 6–13 minutes. By default, Capacity Reporter Agent runs as a low priority service.
	Plug-Ins: Scans of Plug-In devices are designed to be quick, averaging from 5-10 seconds and to have minimal impact on CPU consumption (5-10%).
Network Impact	Capacity Reporter is designed to minimize network impact. The management server itself has limited impact on network performance. During a computer group scan, there is virtually no impact. During a detailed file system group scan, impact is a function of the number of directories and users being managed on each file system as well as the size of your top-*N* file rollup reports from each file system. Because the data is processed and filtered on each Capacity Reporter Agent and only the rollup is collected on the Capacity Reporter Server, the network traffic is minimal. The exceptions are NAS and NetWare scans, which have a higher impact on the network.
	The web browser component that you use to view Capacity Reporter's storage reports generates the same amount of minimal network traffic as browsing an intranet web site.
	The agents generate a minimal amount of network traffic only after they complete their scans on a managed system. During a scan, the data is processed on the agent (client) and packaged for sending to the management server. Note that the processing of each scan is performed on the managed system, and no network traffic is generated until *after* the agent has completed its work.

Scans

Information is loaded into the Management Server database as a result of scans that are scheduled by you, requested by the management server, and performed by the agent. During the scanning process, the management server sends RPC messages to each agent, the agent performs its scan, and data is sent back to the management server.

Group scans run on schedules that you control through Capacity Reporter's Options page. The types of scans are the following:

- Domain scan
- Computer scan
- File system scan

- Plug-In scan

The Domain scan can be configured to operate in one of two ways. Either contact the domain controller to get a list of known computers and enter into the database, or contact the domain controller to get a list of known computer and then contact each computer. When contacting each computer, about 4 KB is sent back per machine. Although this is a small amount of data, most customers choose to not contact each computer and to get only the list of known computers from the domain controller.

You can group computer and file systems into logical groups, and set specific scanning policies for each group. For example, you may want to place specific servers into a computer group that gets scanned every 15 minutes, because the servers are critical and Computer scans are fast. At the same time, you might want to schedule all your file system scans — which take longer because they are gathering detailed file and user information — to run once each night after your backups complete.

Capacity Reporter scans work as follows:

1. The management server initiates all requests for agent scans, based on the scan settings you define for each computer and file system group inside Capacity Reporter.

2. During a scan, the data is processed on the agent (client) and packaged for sending to the management server. Note that with the exception of NAS and NetWare devices, the processing of each scan is performed on the managed system, and no network traffic is generated until *after* the agent has completed its work.

3. The agent sends its data back to the management server as it collects the data via RPC.

Data Collection Model

The following scan message formats illustrate the kind of information transmitted from the agent to the management server:

TABLE C-1   Domain Group Scan

Computer Name
Domain Name
Total File System Capacity (when configured to scan list of computers)
Operating System (when configured to scan list of computers)
Domain Comment (when configured to scan list of computers)

TABLE C-2   Computer Group Scan

Computer Scan	Disk Scan	File System Scan	Share Point Scan
Processor Type	Disk Name	Disk Name	File System Name
Operating System	Make	File System Name	Share Point Name
Operating System Version	Model	File System Size MB	Share Type
Number of Processors	Firmware Revision	Space Used MB	Directory Name
Processor Speed	Serial Number	Free Space KB	
Domain Comment	Number of Primary Defects	File System Type	
Total Free Space	Number of Grown Defects	Domain Name	
Total Space Used	Signature		
Total Memory MB	Total Size KB		
Total Page File MB	Unused Size KB		
Total Virtual MB	Disk Controller Type		
	Rotational Speed		

TABLE C-3   File Ssytem Group Scan (Detailed File Scan)

Directory statistics (size, owner, and attributes)
Top *N* files
Top *N* Largest Files
Top *N* Largest Directories
Top *N* Most Vulnerable Files
Size Statistics
Creation Statistics
Access Statistics
Modification Statistics
Vulnerability Statistics
SRMFiledata.csv & SRMDirdata.csv file creation when configured

TABLE C-4   Plug-In Scan

NAS	Backup	SAN Switch	RAID
Description	Computer name	Name	Name
Link to management server	IP address	IP address	Redundant controllers
IP address	Vendor name	Manufacturer	Total capacity
DNS name/description	Product name	Model	Supported RAID types
Manufacturer	Product version	Serial number	LUN masking
Model	Link to management server	Firmware level	Performance
Serial number	Vendor scan information string	Performance by port	Enclosure
OS platform		Link to management server	Vendor scan information string
Firmware level		Ports and peer hosts	
Free space		Ports and peer storage	
Total space		Vendor scan information string	
Total active ports			
Number of processors			
Cache size			
RAM			
HGtype			
Vendor scan information string			
List of shares			

Scalability

The management server is responsible for scheduling agent scans, collecting scan information, and storing it in the management database, and publishing the information through the Microsoft IIS web server. You can control the frequency of the scans to accommodate your storage management needs and network schedules. You do not have to install the Management Server on a dedicated server, although it may perform faster if you do. You may also run Microsoft SQL Server on a separate server from the Capacity Reporter Server. Capacity Reporter must be on the same server as IIS.

The number of Agents that a single Management Server can control depends on the following:

- Number of managed systems (Agents)
- Number of users who own files on a single managed system
- Number of managed directories
- CPU speed and system memory of the Management Server
- Number of managed file systems across all managed computers
- Number of days that history records are stored (a user-definable setting)

While there is no hard limit to the number of Agents that can be supported by a single Management Server, typical maximums are:

- 100 managed systems
- 400 managed file systems
- 10,000 managed users

Performance Considerations

The greatest benefits to the performance of Capacity Reporter are achieved by the following:

- Put the SQL Server and the Capacity Reporter Server on the same computer
- Put the SQL database on striped disks
- Add enough memory to the computer and dedicate at least 50% to SQL Server

Security Considerations

Capacity Reporter integrates with and leverages Windows NT Server C2 level security conventions, including file-system access control lists (ACLs), user security groups, and standard authentication dialog boxes. Capacity Reporter also integrates with and leverages security levels available in Microsoft Internet Information Server and standard firewalls to protect access to internal company intranets.