Global Information Assurance Certification Paper

How To Implement an Effective Backup Solution: A Company's True Story

Wanda Jackson, Information Security Analyst
Atlanta Georgia

TABLE OF CONTENTS

Executive Summary

The development, execution, and testing of data backup procedures are one of the most important precautions a corporation can take to protect the integrity of its data. Backing up data is the process of creating duplicate copies of data to protect against data loss, theft, destruction or malicious intent. A network contains many file systems that should be backed up on a regular interval. A network administrator is responsible for developing a backup strategy that is appropriate for a business' infrastructure. This proposal will describe and explain an enhanced backup solution specific to Windows NT and Novell NetWare servers and workstations for Wanda's Web World, Inc.

The facts in this report are based on advanced studies by a team of Wanda's Web World System Administrators. Findings include information on factors considered for a backup plan, types of backup strategies, type of media used and associated costs, that will assist the organization in implementing an effective backup solution.

Introduction

Wanda's Web World, Inc. is moving toward new innovations in technology to stay above in its competitive market. In review of the company's current infrastructure, it was revealed that our backup, recovery and restoration process is in need of modification. As Lead System's Administrator, I formalized a team that was dedicated to the study of several backup plans and procedures for a period of three months. This document reports our findings and illustrates how the new will be implemented.

Many different strategies can be employed for backing up and archiving data. Variables to consider include type of backup (Normal, Incremental, Differential, etc.), frequency (daily, weekly, monthly), types of media used (tape, hard disk, optical media, and floppy disk), backup application (NT Backup utility and other vendor applications), and rotation schedules (onsite vs. offsite). Backups can enable an administrator to quickly and completely recover the most recent data possible, regardless of the severity of the initial failure. Data backups must be viewed as a core business security control rather than an activity that an individual is supposed to perform.

Backup Considerations

There are many factors to consider when devising a backup plan. Some of these factors include:

- ☑ **What needs to be backed up.** Not all files have to be backed up. Eliminating system files or application programs from the backup process saves time and storage space.

- ☑ **Where the files are located that need to be backed up.** As administrator you don't want the job to spend more time searching for files than backing up data.

- ☑ **Who will back up files.** System administrators should be responsible for backing up server files, while users *can* be responsible for their workstations.

- ☑ **The resources used for backing up.** This depends on data size and the tape device's features – speed, capacity, ease of use, etc.

- ☑ **Where and when backups should be performed.** Administrators should not backup files in the middle of the day while users are still accessing/changing them. Backups generally should be performed after normal business hours.

- ☑ **How often files requiring backup change.** Knowing this helps implement a good backup schedule.

Backup Types

A system's administrator must consider the types of backup to be performed when preparing a backup plan. There are five types of backup schemes[1] offered: *Normal, Incremental, Differential, Daily and Copy*. The backup methodology that Wanda's Web World, Inc., will incorporate will include Normal and Differential. Advantages and disadvantages of the backup types are provided in the following sections. Because most backup plans use Normal, Incremental and/or Differential strategies, the Copy and Daily procedures will be briefly explained.

Normal (Full) Backups:

A Normal backup backs up all data, regardless of when *or* if it has been previously backed up. All backup strategies should begin with a Normal backup.

Advantages:

- Files are easy to find since Normal (Full) backups include all data contained on a device, an administrator would not have to search through several tapes to find a file that is needed to restore.
- A current backup of the entire system always exists on one tape or tape set. If a restoration is needed, all of the most recent information can be located on the last full backup.

Disadvantages:

- Redundant backups on files occur. Since most of the files on the file server rarely change, each Normal backup following the initial is merely a copy of what has already been backed up.
- Normal backups take longer to perform. Normal backups can be time consuming, especially when other devices on the network, such as user workstations, need to be backed up.

A Normal (Full) backup should always be performed before adding new applications or before making changes to a server.

Incremental Backup:

An Incremental backup backs up all data that has been created or modified since the last Normal, Incremental, Differential, Copy or Daily backup. The differences between Differential and Incremental backups are that Incremental backups include files that have changed since the last backup and Differential backs up changes from the last Normal backup.

[1] Seagate Backup Exec administrative manual, Backup Strategies (chapter 6).

Advantages:

- Better use of media when backing up files. Only files that have changed since the last backup are included, so there is less data storage space required.
- The Incremental backup process takes less time to complete compared to that of the Normal and Differential processes.

Disadvantages:

- Files are more difficult to find. Files backed up incrementally can be spread across multiple tapes since the last Normal backup.

Incremental backups are generally used for very active site, where many files are changing constantly. Despite their inconvenience when needing to restore an individual file, these sites normally find the Incremental process to be practical.

Differential Backup:

A Differential backup backs up all data that has been created or modified since the last Normal backup. The differences between Differential and Incremental backups are that Incremental backups include files that have changed since the last backup.

Advantages:

- Files are easy to find. Restoring a system backed up with a Differential strategy requires a maximum of two tapes – the latest Normal backup and the latest Differential backup tape. This process is less time-consuming than backup strategies that require the latest Normal backup and all Incremental backup tapes created since the last Normal backup.
- Differential backups take less time to restore than Normal or Incremental backup processes.

Disadvantages:

- Redundant backups. All of the files created or modified since the last Incremental backups are included on each tape.

In most schemes, Differential backups are recommended over Incremental backups. Differential backups allow much easier restoration of an entire device than Incremental backups since only two tapes are required. Fewer tapes also decrease the risk of not being able to restore important data because of media error.

Copy Backup:

A Copy backup copies all files within a set, but does not mark the files as being backed up. Copy backups do not affect the media rotation scheme in any way. Copy backups are useful when a system's administrator need to:

- Backup data for a special purpose (i.e., to send to files to another location).
- Backup specific data.
- Perform an additional backup to transport off-site.

Daily Backup:

A Daily backup backups files that were only changed that day, but does not mark the files as being backed up. Like Copy backups, Daily backups do not affect the media rotation scheme.

Backup Media

There are many different types of media appropriate for storing backed up data, which include: Magnetic tape, digital audio tapes (**DAT** - 4mm & 8mm), digital linear tape (**DLT**), floppy and removable disks, magneto-optical disks and recordable CD-ROM (RCD). The tape medium of choice for Wanda's Web World, Inc. will be the digital audio tapes (DAT – 8mm). "The DAT tape's high capacity – 10 GB or more with hardware compression – makes them ideal for unattended backups" (O'Reilly, pg. 191).

Because of high and constant system utilization, our backup process should be scheduled to run after-hours. The DAT medium will allow Wanda's Web World system administrators to start a backup script to begin between 8:00 P.M. and 9:00 P.M. A single DAT tape holds eight Gigabytes of compressed data and four Gigabytes of uncompressed data (this information should be used to track tape usage).

Backup Strategy

Backup Media Usage

The proposed backup strategy for Wanda's Web World, Inc., uses a minimum of 28 tapes per cycle. System administrators will perform backups on servers and user workstations. Each cycle consists of a six-month period. For server backups, for example, all jobs ran on 1st Mondays of the month (January – June) will be contained on one tape, all 2nd Mondays will share the same tape, and so on. Workstation backups will rotate on six tapes, while the NT and Novell servers will operate on the remaining medium (see illustration below).

Figure 1

Wanda's Web World, Inc. – Backup Proposed Process

	Server	Server	Server	Server	Workstations	Server	Monthly
Week 1	Monday1	Tuesday1	Wednesday1	Thursday1		Friday1	
Week 2	Monday2	Tuesday2	Wednesday2	Thursday2	Thursday2	Friday2	
Week 3	Monday3	Tuesday3	Wednesday3	Thursday3		Friday3	
Week 4	Monday4	Tuesday4	Wednesday4	Thursday4	Thursday4	Friday4	Saturday
*Week 5	Monday5	Tuesday5	Wednesday5	Thursday5		Friday5	

***An additional rotation tape has been provided for months containing five weeks.**

Differential backup
=

Normal backup
=

Backup Methodology

The implementation of both Normal (Full) and Differential backup methodologies will provide Wanda's Web World, Inc. with an efficient process to backup our data. In the event of restoration, system administrators would only need to refer to two tapes – the latest Normal (Full) backup and the last Differential backup. Adopting this method eliminates time used in searching for the right media, the data is restored faster, and users have the capability of quickly returning to their tasks.

Backup Scheduling

A system administrator can schedule a backup job via the server's console or a local workstation containing the backup software's agent application. Scheduling a backup job is completed in three easy steps, with the use of a graphical user interface (GUI) utility, supplied by Veritas please refer to the section on *Backup Software*).

Per the illustrated process (figure 1), a Differential backup should be performed every Monday-Thursday on the file servers. The Network Administrator would be responsible for running the job each evening between 8:00 P.M and 9:00 P.M. Each job runs an average total of 2.5 hours, allocating enough time for NT servers to begin compression at 12 midnight. On Friday nights, a Normal backup is performed on the **NTFS** (NT File System) and **NDS** (Novell Directory Services). The Differential backup tapes created are stored on-site and the previous week's Normal backup is sent to our off-site vendor, Recovery Systems. In addition, a monthly Normal backup should be completed on our Novell context located within the corporate tree.

Every other Thursday, a Differential backup is performed on user workstations. User backups are important as well. In case of errors with server jobs, user workstation backups should be utilized as part of a contingency plan to restore information.

Backup Media Cost

As noted, the proposed rotation scheme uses a minimum of 28 tapes in a six- month cycle (we will include two additional tapes per cycle to replace damaged medium). These tapes will be rotated to backup our two servers (NT and Novell) and fifteen workstations. Backup media is very inexpensive. Access Media, the company's media supplier, charges $6.69 per tape. **Our cost per cycle, $200.70; per year $401.40.**

Backup Software

Wanda's Web World is currently using the Windows NT Backup Facility to perform backups and restorations. "While the Windows NT backup facility works reasonably well for performing basic local system backup and restore operations, it's missing many desirable features of a high-end backup package designed for site-wide use"[2]. Because we operate in a mixed network operating system environment (Windows NT and Novell NetWare), this facility is no longer adequate or appropriate as it relates to our infrastructure.

Veritas Backup Exec[3] is an excellent backup facility that will allow (but not limited to) backup administrators to execute and perform jobs remotely, to automate the backup process, to define and save standard backup settings to initiate for later jobs, etc. While there are several backup utilities on the market today, we chose Veritas for its ease of use and 24-hour technical support capabilities.

[2] O'Reilly's Chapter 7:Backups, page 200
[3] Information about Veritas Backup Exec can be found at the company's web presence: www.Veritas.com

.

Conclusion

In conclusion, data backups are extremely important to the business environment and should be viewed as a necessary element in security standards, policies and practices. The backup scheme proposed will give Wanda's Web World's System Administrators an easy, effective way of backing up, recovering and restoring the company's most valuable asset – its data. By implementing the use of Normal and Differential strategies, the company will save time on restoring data to failed systems and reducing cost for backup media.

For three consecutive months, Wanda's Web World System Administrators compared and tested the new technique against our current antiquated procedures. This method proved successful for our mixed infrastructure and will be adopted corporate wide.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event