That Dreaded Day

Active Directory Disasters and Solutions for Preventing Them

Written by Greg Shields, Founding Partner, MVP, Concentrated Technology

ABSTRACT

Active Directory (AD) disasters can happen, and that dreaded day can arrive if you're lacking protection in key areas. While Active Directory's built-in features will keep IT running after some kinds of failures, there are others from which it cannot bounce back. This paper presents five AD disaster case studies and how they might have been prevented or repaired more quickly with proper planning and tools.

INTRODUCTION

Here's a fun exercise, one that might scare you a bit: Grab a sheet of paper and sketch out your IT infrastructure. Add in servers, applications, users — all the pieces that make up the services you're responsible for managing. Then, start connecting the dependencies. You'll quickly begin seeing a trend:

- Email relies on Microsoft Outlook, which relies on Microsoft Exchange, which relies on Active Directory.
- Users rely on critical business applications, which rely on Oracle, which relies on Active Directory.
- Users' files and folders rely on file servers, which rely on Windows servers, which rely on Active Directory.

It's nearly impossible in any Windows network to stray too far from Active Directory — the source of nearly all authentication and authorization. You'll eventually find every dependency arrow pointing toward Active Directory's services. That's why keeping those services running is absolutely critical for the functionality of every other IT component.

Active Directory's domain controllers (DCs) are designed to be exceptionally resilient. They have to be, considering the responsibilities they're given. With a multi-master model for replication and plenty of built-in redundancy, even losing a couple of DCs isn't necessarily a disaster.

THAT DREADED DAY: ACTIVE DIRECTORY DISASTERS AND SOLUTIONS FOR PREVENTING THEM

Five dreaded disasters, five dreaded days

Disasters can happen, and that dreaded day can arrive if you're lacking protections in a few key areas.

While AD's built-in features will keep IT running after some kinds of failures, there are others from which it cannot bounce back. You must plan for these potential AD disasters.

If you're in the disaster recovery planning process, or can't guarantee the plan you have will actually work, consider the following five use cases as important lessons. Neglecting these situations, or the protections that prevent them, could result in that dreaded day — the day when your entire business grinds to a halt because of some unforeseen Active Directory disaster.

Dreaded day #1: Losing a domain controller

The most obvious of these dreaded day use cases is the loss of an Active Directory domain controller. Losing a DC means losing authentication and authorization services for some portion of your IT environment. It also means taking down one part of your AD infrastructure, leaving those remaining to take over the workload.

While losing a DC is indeed a bad day, almost every Active Directory is constructed with a minimum of two in place. Some environments install DCs into every location, or even pairs into each location. Each and every DC contains an equal copy of the AD database, and any can authenticate users and computers for the entire domain. With AD services typically relegated to single-purpose servers that have plenty of hardware redundancy built in, the chance of a catastrophic loss has diminished steadily over the course of IT history.

Losing a DC is arguably the least painful of all dreaded days. With the right tools, restoring a DC from a good backup doesn't require much time. You can't restore one domain controller's copy of the AD database onto another DC, so these tools are typically installed onto each DC to ensure coverage. It's important, however, to seek tools that complete that restore quickly, returning the server back to operations in short order.

Dreaded day #2: Losing a user, a computer object or a Group Policy

Many disaster recovery plans focus on the big events. Yet, the small ones are the most common cause of pain, even if their impact is only relegated to a single user or computer. Although everyone may not be impacted at the same time, the loss or corruption of a user or computer object is important to the person associated with that object. If someone is under a tight deadline, losing the AD object can be disastrous.

These situations should be familiar. Perhaps a user account was accidentally deleted, or one of its attributes was inadvertently modified. Maybe someone accidentally deleted or changed an Active Directory group or Group Policy. Or the worst-case scenario: What if someone maliciously harmed your AD data?

Any of these circumstances explains why a disaster recovery plan must include the rapid-restore functionality necessary to get a user working again. But, the tools to accomplish this quickly and thoroughly haven't been natively available in Windows until its most-recent version. Even those introduced in Windows Server 2008 R2 are insufficient when speed is important, and every IT pro must be equipped to accomplish the task.

A fully realized disaster recovery plan must spell out the processes and technologies that restore functionality to users or computer objects. The plan must also support the quick restoration of Group Policies and include the necessary interfaces to easily complete the process, while exclusively locking down completion to trusted individuals. Restores themselves must be logged to prevent abuse, protect domain security and ensure that any auditor can verify the process is conducted correctly. The right solution will support all these needs.

While AD's built-in features will keep IT running after some kinds of failures, there are others from which it cannot bounce back. You must plan for these potential AD disasters.

Dreaded day #3: Losing an entire group of users or computer objects

If you don't have access to the Active Directory Users and Computers console or you've never seen it, get someone to show you this powerful tool for managing AD objects. Objects can be created, modified and relocated right within the tool. As fast as objects can be created, they can be deleted.

Here's a scary thought: One needs only three mouse clicks to accidentally or maliciously delete entire groups of objects. At all times, hundreds or even thousands of users and their computers are just three mouse clicks away from complete obliteration. As they go, so also goes the sum total of their information: names, passwords, personal information, mailboxes, permissions — everything gone, simply by a misplaced mouse click.

Even more chilling is the realization that most IT organizations leave AD object administration to team members with the least experience. Managing AD objects is actually mind-numbingly simple. But, it can also be extremely time consuming. The task requires concentration and organization, although little is needed in the way of advanced technology experience. This may explain why many businesses turn the responsibility over to neophyte IT pros.

Inexperienced individuals can wield significant power over your entire AD infrastructure. Without proper security controls, all it takes is one disgruntled person, or someone with slow reactions, or one who means well but doesn't know much to shut down your entire business for an indefinite amount of time. Such disasters waiting to happen must be planned for in order to prevent them. That means implementing good controls over AD data. It also means incorporating solutions that can restore data in seconds, rather than hours or days. The right solution can restore data for large groups as rapidly as individual objects and work across multiple backups, minimizing data loss. That right solution can stop wayward mouse clicks from causing business-impacting incidents.

Dreaded day #4: Losing your entire forest

One of the worst dreaded days that can befall an IT infrastructure is the loss of an entire AD forest. It can take down every single application, service and data access across every desktop and server. This type of nightmare situation keeps many IT pros awake at night.

Painful as it is, losing an entire forest is frighteningly easy. Despite all its marvels, AD's multi-master replication has a key flaw: Any debilitating corruption can quickly spread across every domain controller, causing irreparable harm before anyone recognizes something is amiss.

The recovery process is far from simple. Some argue it's one of the most painful endeavors any Windows environment can undergo. The Microsoft document, Recovering your Active Directory Forest, outlines 15 steps for a multi-domain environment to get the first domain controller operational again. Each additional domain requires another 12 steps just to get the first DC up and running. Eight more post-recovery steps are outlined in the conclusion. And that's just to get each domain's first DC running.

Recovering an AD forest is challenging due to the numerous interconnections DCs require for functionality: AD services must be reconstructed, metadata cleaned up, trusts reestablished, accounts reset and replication restarted among other tasks. All are complex activities that accept no mistakes during the recovery process. Missing a step or performing certain ones out of order can fail the entire process.

That lack of tolerance doesn't bode well with the added stress, finger-pointing and general unease that is common during catastrophic failures. With business leadership and angry users expecting updates on a minute-by-minute basis, the smart IT organization demands detailed planning before the event in combination with solutions that fulfill a forest recovery's process steps with a measure of automation.

No one wants this kind of situation to occur. But if it does, don't leave yourself without simple instructions in hand. The worst kind

A fully realized disaster recovery plan must spell out the processes and technologies that restore functionality to users or computer objects.

> The smart IT organization demands detailed planning before the event in combination with solutions that fulfill a forest recovery's process steps with a measure of automation.

of dreaded day isn't so much the loss of your AD forest — it's realizing you've only got native Windows tools and knowledge base articles in your recovery toolbox.

Lack of experience makes the challenge even more daunting. It's rare to find an IT professional who's been through a forest recovery from start to finish. And with so much at risk, it's rarer still to find outside consultants willing to lend a hand.

You'll want a solution built by experts with years of experience handling this type of activity. The right solution aligns with Microsoft's complex forest-recovery processes, and links backed-up data to recovery operations across each of its numerous steps.

While no AD forest recovery is ever a click-and-go operation, the solution you want at your side automates as much of the process as possible. The key to your business surviving this type of dreaded day is getting back to a semblance of operations quickly.

Dreaded day #5: Any of the above plus losing the backup data

There is one more dreaded day that in many ways eclipses the others. Yes, losing a DC, a user object, a set of users or their computers and watching a forest crumble beneath you can be disastrous. But, these events seem trivial when compared with the worst possible calamity of all: Not having backup data.

This potentially business-destroying and career-ending situation can be remarkably simple in origin. Your data today may not be fully protected without you even knowing it.

The reasons are many: Backup jobs may have not run on domain controllers. Perhaps they failed. They may have been failing for long periods of time, reporting unheeded warnings in long-overlooked logs. Microsoft's native VSS (used to quiet AD's database so backups can be correctly captured) may be failing, with or without warning. The data itself could be backed up, but in a way that's completely unusable for recovery.

All of these situations are entirely possible due to the nature of backups. As a piece of the infrastructure, backups tend to get overlooked by overworked administrators. Incorrectly assuming that no news means good news, these hard-working individuals often neglect taking the time to positively verify backups. Despite daily (if not more frequent) backups, the time-consuming task of validation simply gets lost in the shuffle.

For this reason alone, organizations that value their AD foundation should look for an automated backup tool. Thus, offloading the manual nature of AD backups and backup storage to a third-party product or service can save time and ensure you have backups whenever you need them.

If you choose a software-as-a-service solution, you have the additional benefit of an off-site location. This is recommended and represents an inexpensive insurance policy — both in dollars and network bandwidth — that further protects against any dreaded day scenarios.

Trusting a third party with your data requires finding a reliable provider. The provider must secure your data in transit and at rest, and use industry-standard identity federation for authentication and authorization, plus guaranteed-available platforms to ensure you're never prevented from accessing your data. The ideal provider will alert you when backups have not occurred, as well as when backup data has not been captured in a way that guarantees recovery.

Selecting a backup and recovery service gives you an inexpensive option for further protecting the foundation of your IT infrastructure: its Active Directory data.

AD disaster recovery is business disaster recovery

Disaster recovery for AD comes in many forms. Although the classic use cases for disaster recovery sometimes focus on the biggest events, it's the small ones that cause just as much concern for the people they impact. Ensuring the continued viability of AD means having recovery capabilities that start with individual objects and continue on up through entire domains and forests. Such capabilities are easy to use and quick to restore.

More importantly, ensuring the recovery of AD also means ensuring the recovery of your entire business. With the data and applications that drive your business all residing on top of Active Directory's services, keeping the foundation healthy means keeping the business healthy.

ACTIVE DIRECTORY BACKUP AND RECOVERY SOLUTIONS FROM QUEST

Quest has long been a leader in AD management. More than 3,500 customers rely on AD solutions from Quest to protect 72 million user accounts every day. Quest has the products you need to ensure a complete AD recovery plan.

Recovery Manager for Active Directory

Recovery Manager for Active Directory offers an easy-to-use solution for fast, online recovery. Comparison reports highlight which objects and attributes have been changed or deleted in AD, enabling efficient, focused recovery at the object or attribute level. Accurate backups and a quicker recovery help you reduce the time and costs associated with AD outages and reduce the impact on users throughout your organization.

Recovery Manager for Active Directory Forest Edition

Recovery Manager for Active Directory Forest Edition enables you to restore your entire AD forest from a single console. It eliminates the need for physical interaction at each domain controller that is required when using native tools, speeding recovery time significantly.

By automating the AD domain or forest recovery process, Recovery Manager for Active Directory Forest Edition enables you to recover to a point in time before the directory became corrupt. It selects unaffected backups, quarantines the damaged environment and automates all the manual steps required to facilitate a quick and successful domain or forest recovery.

ABOUT THE AUTHOR

Greg Shields, MVP, vExpert, is an independent author, speaker and IT consultant, as well as a founding partner of Concentrated Technology. With nearly 15 years in information technology, Shields has acquired extensive experience in systems administration, engineering and architecture. He specializes in Windows, remote application and virtualization technologies. A contributing editor and columnist for *TechNet Magazine,* as well as a regular writer for *TechTarget* and other publications, Shields has authored or contributed to 10 books, plus countless white papers and webcasts.

Trusting a third party with your data requires finding a reliable provider. The provider must secure your data in transit and at rest, and use industry-standard identity federation for authentication and authorization, plus guaranteed-available platforms to ensure you're never prevented from accessing your data.