





# Efficient Disaster Recovery for Active Directory: How to Complement Your Existing Processes with Cost-Effective Solutions

There's no question that Microsoft Active Directory has become a mission-critical part of your enterprise, providing authentication and identity management services that help secure your data, provision and configure your computers, and much more. Making Active Directory a part of your overall disaster recovery process is essential, and you've doubtlessly already taken steps to protect this valuable piece of your infrastructure. There is, however, a robust market for third-party Active Directory disaster recovery solutions, which has to make you wonder: What are you missing? In this paper, we'll explore what your existing disaster recovery processes are already addressing, highlight potential weak points, and suggest solutions that help fill those gaps—without requiring you to completely re-do your existing processes or buy monolithic software applications that don't precisely address your needs.

## Categorizing Your Needs for Active Directory Disaster Recovery

A disaster recovery plan for Active Directory actually needs to include provisions for several different types of "disasters," due primarily to the way Active Directory itself works and is used within the enterprise. The easiest of these is the complete failure, perhaps the most severe type of disaster in which your entire directory is somehow lost. This is actually quite rare, as Active Directory itself, with its multi-master storage model, is already quite resistant. Losing the entire directory would entail losing all of your domain controllers for an entire domain or forest. More frequently, "complete failure" comes into play when an entire facility becomes unusable, due to a natural disaster or other occurrence, and you need to bring your entire directory back to life at a backup facility.

Much more common is the individual object loss scenario, in which a single user, group, organizational unit, or other object is lost from the directory, either due to accident or malicious activity. If the object lost is an organizational unit or container, then all of the child objects are also lost, compounding the problem. Tight interrelationships between objects can also make the situation more difficult. For example, if a user is deleted, then their group memberships—often the key to your security architecture—are also lost.

Finally, another common scenario is the ancillary data loss. Much of the data required for the proper functioning of Active Directory isn't actually contained in Active Directory. For example, while Group Policy object (GPO) links are stored in the directory, the GPOs themselves—which contain all the critical settings used to configure your environment—are stored as files on domain controllers, not in the directory.

These disaster scenarios are completely unique in how they occur, what impact they cause, how common they are, and most importantly how you deal with them when they do occur. It's important that your disaster recovery plan uniquely address each of these in order to maintain uptime with as little additional overhead as possible.

## **What Your Existing Disaster Recovery Plan Already Handles**

Nearly every enterprise disaster recovery plan already covers the complete failure scenario with something called a "system state" backup. This is a type of backup so common that it's included right in Windows' own free Backup utility, and it provides insurance against a complete failure of the domain or forest. Most third-party backup applications have built-in support for capturing the "system state," meaning there's little need to buy something specifically designed to capture it.

Unfortunately, the complete failure scenario is also the one that happens the least often, meaning your existing disaster recovery plan may be fully prepared to deal with a situation that won't come up that often. More common are the single object loss and ancillary data loss scenarios, and unfortunately a "system state" backup isn't terribly helpful in those situations. While a "system state" backup can be used to restore a single object, doing so requires that a domain controller be taken completely offline to perform complex, manual, command-line tasks to restore the object—and to manually restore dependent objects or child objects. GPOs aren't included in the "system state" by default, so they're not protected at all.

## **What Your Existing Disaster Recovery Plan is Missing**

Most enterprise disaster recovery plans are missing the means to efficiently restore single directory objects, including the automated restoration of child and dependent objects when needed. The ability to quickly restore GPOs—and in fact to locate the right GPO version to restore—is also something often overlooked in disaster recovery planning.

You should be able to restore single objects and ancillary data without taking a domain controller offline, without learning to use an all-new toolset, without seriously impacting the users who are relying on the directory to get their jobs done, and without resorting to complex, command-line tools and manual procedures.

## **How to Efficiently Complete Your Disaster Recovery Plan**

There's an easy way to provide your disaster recovery plan with the capabilities you need, without having to re-do that plan from scratch or implement costly, complicated software applications. NetPro offers three solutions designed to complement your existing "system state" backups, whether you're capturing those with Microsoft tools or third-party backup software:

- **Simple, Single-Object Restore:** NetPro plugs into the Microsoft Active Directory Users & Computers console—the tool administrators already use to manage the directory—and provides simple, single-object restore without the need to take a domain controller offline. Dependent and child objects can be restored automatically, making disaster recovery for the “single object loss” scenario as easy as dragging an object out of the directory Recycle Bin.
- **GPO Version Control and Restore:** NetPro fills the hole left by “system state” backups by automatically version-controlling all GPOs in your domain. If a GPO is lost or misconfigured, simply retrieve a past version—no need to perform a tedious, full recovery of the directory. GPO versions can be easily compared to find out which one is the one you need, and to instantly spot exactly what settings were changed between versions.
- **Real-Time Change Auditing:** NetPro provides fast troubleshooting capabilities so you can instantly determine “what’s changed.” When the directory malfunctions, the cause is generally due to a configuration change of some kind. Rather than resorting to a full restoration, administrators simply need to “undo” the improper change. NetPro lets you do so by displaying the “who, what, when, and where” for all directory changes, and in many cases by also providing a “before and after” snapshot for each change. Why restore when simply reconfiguring will bring things back to normal much more quickly?

## Extending Microsoft Native Tools

Feature	Native Tools	NetPro
Automatic, scheduled backups	Yes	Yes
Differential Active Directory backups (smaller and faster)	No	Yes
Automatic version control for GPOs	No	Yes
Compare/recover GPOs	No	Yes
Restore single Active Directory objects with no DC downtime	No	Yes
Restore single Active Directory objects using simple GUI	No	Yes
Auto-restore dependent and child objects in Active Directory	No	Yes
Audit Active Directory events in real time	No	Yes
Translate Active Directory events into plain-English messages	No	Yes
“Who, what, when, and where” for Active Directory events	No	Yes
Consolidate Active Directory events into a single database	No	Yes
Active Directory event database is tamper-proof / non-repudiable	No	Yes
Works with your existing disaster recovery plan	Depends	Yes

## The Scalpel vs. the Shotgun: Complementary Solutions vs. the Rip-and-Replace Approach

As stated at the beginning of this paper, a variety of third-party Active Directory disaster recovery solutions are available in the marketplace. These tend to take one of two approaches, which we'll call the scalpel and the shotgun.

The shotgun approach, as the name implies, seeks to provide a complete, monolithic, self-contained disaster recovery solution. These solutions are often expensive, and they often provide a great deal of overlap with your existing disaster recovery solution—specifically, in their ability to perform a “system state” restore to completely restore a domain or forest. In other words, you're paying big bucks for functionality that you already have. In addition, because these solutions are designed to be self-contained, they typically have complex deployment requirements, require additional training for your staff (who will need to “forget” your current processes and learn to work with the new toolset), and often integrate poorly with the rest of your disaster recovery process. You'll need to plan on completely revising your disaster recovery plans, including off-site recovery, staffing requirements, software licensing, and more. Taking this approach seems easy at first—just pull the trigger and hit every need at once—but the actual cost and overhead can actually be quite high.

The scalpel approach differs in that it seeks to leave your existing, fully-functional disaster recovery processes in place, and simply supplement them with additional, highly-integrated functionality that provides for unsatisfied needs. The idea is to minimize the need for additional training and software, keep your existing processes and procedures completely intact, and minimize deployment overhead.

NetPro offers the perfect complement to your existing disaster recovery solution because it:

- Integrates with existing Active Directory tools that you already know how to use, and provides powerful, intuitive single-object restoration. All restores can be performed completely online, increasing uptime and decreasing the impact of the recovery process. NetPro can automatically restore child objects and re-create group membership, ensuring that recovery operations are complete and require less advanced planning. NetPro also knows to grab the ancillary data used by Active Directory, including registry keys and files.
- Provides disaster recovery for Group Policy objects, integrating with the Microsoft Group Policy Management Console (GPMC) that administrators are already using for GPO management. GPOs are automatically version-controlled, and old GPO versions can be retrieved and compared at any time—even across domains. It's easy to find settings that have changed between versions and quickly restore them, without taking a single domain controller offline.

- Provides the missing link for disaster recovery troubleshooting by providing a searchable, plain-English look into the inner workings of Active Directory—including “who, what, when, where” details on every change made to the directory. When things go wrong, NetPro is the first place to look to see what’s been changed so that things can quickly be put right, without having to perform a full recovery.

**You decide:** rip and replace your disaster recovery solution, re-train personnel on expensive monolithic software, and re-design processes to accommodate procedures designed by a software vendor. Or choose the NetPro approach and simply complement your existing tools and processes to fill the gaps in your disaster recovery plan.