SOLUTION BRIEF

6 WAYS TO IMPROVE ACTIVE DIRECTORY RESILIENCE WITH ROLLBACK AND RECOVERY

stealthbits
NOW PART OF netwrix

PROBLEM: THE LOST ATTRIBUTE

What happens when an Active Directory (AD) administrator accidentally changes an important attribute like Department? A global financial services company recently faced this scenario. Its admin inadvertently changed the Accounting Department attribute for thousands of users. Since the Accounting Department attribute was being used to create an AD security group granting users access to financial resources, those affected lost access to critical data and applications they need to do their jobs.

Calls began flooding into the help desk and the problem was soon discovered. Unfortunately, native Active Directory tools don't provide an easy way to restore user attributes. As a result, the admin had to use scripting to simulate and commit attribute restorations. Since the approach wasn't 100% accurate, the admin still had to coordinate with Accounting Department managers and the help desk to make sure every user's Accounting Department attribute was restored.

The cost to the company was significant—a full day of lost work for affected employees and countless hours spent by the help desk, accounting managers, and AD admin fixing the issue.

CHALLENGE: LET ME COUNT THE WAYS

This accidental change to a user attribute is just one scenario indicative of a much larger issue. Many factors can cause unwanted changes in Active Directory:

- Company mergers that necessitate the migration and consolidation of directories
- Disasters or severe outages that bring down Active Directory
- External or internal bad actors that make malicious changes to AD
- Unintended deletion of AD objects (users, groups, computers) or Group Policy Objects (GPOs)
- Inadvertent changes to DNS entries, Organization Unit (OU) or object permissions, GPO settings, and group attributes, including group memberships

While Active Directory does provide some native capabilities for recovering deleted objects and GPOs, they are managed in separate utilities when it would be preferable to recover and restore both in the same solution. Also, object restoration requires dependencies for enabling the features on the specific operating system, e.g., ADAC user interface (2012), Recycle Bin (2008 R2+), and tombstone reanimation (2003, 2008). In addition, none of these native tools were purpose-built to handle scenarios like a disaster or outage requiring the rollback of **all** objects.

SOLUTION: STEALTHRECOVER = YOUR RESET BUTTON

Stealthbits understands that Active Directory is mission-critical, both as the model for a company's organizational structure as well as an authentication and authorization hub for its IT infrastructure. We also understand that Active Directory is not bullet-proof—mistakes happen and bad actors get in and wreak havoc. That's why we created StealthRECOVER, an Active Directory Rollback and Recovery solution that enables organizations to quickly and safely recover deleted items, rollback object and attribute changes, do point-in-time restorations of entire AD domains, and more—with minimal downtime.

With StealthRECOVER, companies can easily restore all or just the information they need to any recorded state by:

- Having full control over when and how Active Directory back-ups are taken

- Leveraging the ability to do on demand directory snapshots before making big changes
- Performing full-text, granular search on multiple directory snapshots
- Seeing a complete history of back-ups with details of added/modified/deleted objects

Having this kind of reset button helps maintain business continuity by minimizing the downtime and damage (e.g., data loss, system malfunctions, etc.) caused by malicious and unintended Active Directory changes. The result is piece of mind that an organization can maintain the security, agility, and operational integrity of Active Directory, no matter what situation arises.

SCENARIOS: STEALTHRECOVER TO THE RESCUE

Here are some common business scenarios where customers are using StealthRECOVER to restore Active Directory from unwanted changes:

1. A Malicious Attacker Strikes

A bad actor (external or internal) adds himself to the Domain Admin group to gain control over the domain. With these elevated privileges, he looks for sensitive data and tries to exfiltrate it. He may also make changes to Default Domain Policy, or Default Domain Controllers Policy, that could affect every user and computer in the domain. Or, he may delete a GPO, causing significant security issues and outages. Once an organization detects and blocks the attacker, it still has to rollback and recover from the changes he made, e.g., rollback Domain Admin group membership, recover GPOs and settings, etc. StealthRECOVER gives the organization the ability to rapidly restore that information.

2. User, Group, or Computer is Deleted

An administrator accidentally deletes an Active Directory object—a user, group, or computer. If it's a user, that user loses all access and can't perform her job. If it's a group, its members lose whatever privileges the group granted them. If it's a computer, all users and groups with rights to it can longer access it. The admin would likely try to restore the object with the AD Recycle Bin; but, it may not work if the Recycle Bin is not enabled properly. With StealthRECOVER, however, the admin can be certain that the user, group, or computer will be restored with all attributes and group memberships reassigned.

3. Members are Removed or Added to Groups

A couple of business users accidentally get added to the local administrators group. These users probably don't even know they've been added. That's a major security risk because an attacker can compromise their access and get on the network undetected. Organizations need a way to detect these inappropriately added members and immediately rollback the changes.

Or the reverse may happen. HR/Payroll employees could get inadvertently removed from a group that gives them access to needed employee information. Business could come to a halt if they lose access during a critical time like benefits enrollment, W-2 distribution, or payroll. AD native tools don't provide an easy way to rollback membership changes. In both these cases, StealthRECOVER can quickly and safely restore the membership of these groups.

4. Attributes on Multiple User Accounts are Changed

Two companies merge and consolidate their Active Directory environments. Somewhere along the way, one of the admins changes the title, manager, phone number, and physical address on multiple user accounts. Without accurate information, these employees cannot be properly placed in the new Active Directory structure. An admin can use scripting to try and restore these attributes but it would be complex, time-consuming, and risky. StealthRECOVER, on the other hand, makes these attribute rollbacks easy so these employees get the right access to the right resources.

5. Domain Name System (DNS) Entries are Modified

A DNS entry could get maliciously changed by an attacker perpetrating DNS spoofing (attacker diverts traffic to his computer) or a man-in-the-middle attack (attacker inserts himself between users or systems communicating with each other). In either case, sensitive data could be immediately compromised. Or, a DNS entry could get mistakenly modified, resulting in users being unable to access a website. If that website is something many employees, partners, or customers use, then it could have a significant business impact.

While the AD Recycle Bin can recover DNS entries, it typically requires more steps than a normal AD Recycle Bin operation. StealthRECOVER, on the other hand, makes rolling back DNS entries easy, fast, and safe.

6. Natural Disaster Occurs

No one thinks it will happen to them. But natural disasters and severe outages do occur and can bring down entire IT infrastructures. If a company has offsite back-ups, then it can restore Active Directory. But the process can take hours or days. Not so with StealthRECOVER. It is designed to allow organizations to rollback all AD objects to the last known good state in minutes.

This capability isn't limited to disasters. Customers also use it when admins make a series of changes that are too complex or time-consuming to manage as individual rollbacks.

NEXT STEPS

Schedule a demo
stealthbits.com/demo

Download a free trial
stealthbits.com/free-trial

Contact us
info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix