Active Directory Recovery: Be More Prepared

By Don Jones

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

Sponsored by DELL

We're all well aware of the need to be prepared for an Active Directory (AD) disaster. But what kind of disaster, exactly, do you need to be prepared for? While the "domain controller hardware completely crashed" scenario is perhaps foremost in our minds (or nightmares), that's hardly the only scenario – and it isn't even the most likely. To ensure the integrity and stability of your directory, you'll need to address a wider range of potential scenarios, include broader recovery capabilities, and generally be more prepared than you may have realized.

What About the AD Recycle Bin?

One of the highly touted features of Windows Server 2008 R2 was the new "Active Directory Recycle Bin," which ironically didn't include any kind of visual "bin" whatsoever. Windows Server 2012 added a much-needed graphical user interface component to this feature, but at the end of the day it offers the same basic functionality: the ability to restore single objects that had been accidentally deleted.

The Recycle Bin won't restore improperly changed attributes of an object. It won't protect against a corrupted domain controller database, against replication failure, or even against deliberate mischief.

That's a pretty big limitation, and it only addresses a fraction of the possible recovery scenarios an AD administrator must be prepared to deal with. The Recycle Bin won't restore improperly changed attributes of an object. It won't work at all in a domain operating below the "Windows Server 2008 R2" functional level. It won't recover external objects, like a Group Policy Object (GPO) file. It won't protect against a corrupted domain controller database, against replication failure, or even against deliberate mischief ("recycled" objects can be deliberately, permanently removed by a malicious operator).

The Recycle Bin is great baseline functionality – but it's not the only thing you'll need to have in your environment in order to be truly prepared.

What You Need to Protect: a Checklist

Let's consider a complete list of what can go wrong – and what you'll need to have in place to mitigate disaster:

- **Attribute recovery.** Someone accidentally changes attributes on a bunch of users, rendering directory information incorrect – which is a problem if you have other applications relying upon it – or potentially even nixing access to critical applications – as in an Exchange environment. The ability to compare an object's current attribute to its past ones, and roll back unwanted change, is perhaps one of the most common day-to-day recovery tasks.

- **Object-Level Recovery.** Objects do get deleted by accident, whether it's users, computers, or something else. The ability to revive them, with all attributes intact, is crucial. And you need that capability even if all of your domain controllers aren't running the latest Windows OS (a requirement of the Recycle Bin feature). You also need easy recovery of entire containers of objects, in the event that an entire organizational unit is wiped out by accident.

- **GPO Recovery.** Group Policy Object links are stored in the directory, but the actual files aren't. The ability to restore those files – and to compare the current version to a known-good backup – is absolutely crucial. A misconfigured – or missing – GPO can wreak havoc on your environment, producing an incredible amount of downtime and lost productivity.

- **DC Recovery.** The failure of an entire domain controller might seem easy to mitigate: simply have another. After all, you can always de-promote and re-promote a failed DC, right? True, although the failure of certain DCs – those hosting FSMO roles – can put your entire domain in jeopardy. And, simply re-promoting a DC can take a long time in a large environment, creating slowdowns and backups throughout the local network. Smart administrators know that they also need regular backups of DCs' System State to ensure quick and effective recoveries in the event of a failure.

- **Forest Recovery.** Yes, it can happen to you – to anyone, in fact, with more than one domain in their environment. And you might be surprised to learn that you have more than one domain in your environment.

Forest Recovery: the Unexpected, Most-Difficult Recovery

Any organization, especially those running more than one domain in their forest, needs to be concerned about forest recovery, and a surprising number of organizations – even relatively small ones – have more than one domain. In the early 2000s, when AD was still new, it was considered a

best practice to create an empty root domain as the first domain in an organization's new directory architecture. This "empty root" would often be implemented on a couple of DCs, with the organization's main production domain (or domains) "hanging" off of, or adjacent to, that root. Those other domains could be more easily renamed or re-architected – something that was appealing in the early days when organizations weren't sure if they wanted to commit to their first-guess domain design. The result is that a large number of organizations actually do have a forest, even though – from an operational perspective – they only deal with a single domain on a day-to-day basis. But the loss of that empty root could spell disaster for the entire environment. Because it isn't used, that root isn't often monitored very well: more than a few forest failure scenarios have occurred because an organization lost one of the empty root's DCs, and were alarmed to find that the other empty root DC had failed months, or years, prior.

A large number of organizations actually do have a forest, even though – from an operational perspective – they only deal with a single domain on a day-to-day basis.

Having to perform a forest recovery is a remarkably easy situation to get yourself into, and it isn't always the result of a "disaster." Many applications, for example, extend the AD schema, a one-way, irreversible operation. Stop using the application, and a forest recovery is the only way to "clean up" the schema. Malicious actions can also make a forest unstable, as can a poorly monitored environment.

Common belief is that Microsoft will only support organizations after a forest recovery if the organization employs Microsoft Product Support to guide the recovery; while Microsoft has no such official policy, a forest recovery is tricky enough that you'll probably want the company's experts on the phone throughout the process. And it can be a time-consuming process – think weeks, in some situations, not hours. And there are no built-in tools to streamline or shorten that process.

The Virtual Consideration

The virtualization of domain controllers has created a whole new twist on AD recovery, thanks to snapshots.

Snapshots seem like an excellent way to provide near-instantaneous recovery. Rather than backing up a server every night, you just snapshot it – a fast operation that results in a set of static files which can be more easily copied off to tape. Server problem? No sweat – just restore the snapshot.

Unless that server is an AD domain controller. Each domain controller assigns a sequential update sequence number (USN) to each change that originates on that DC. As changes replicate to other DCs, the USN tells the rest of the network if the change is new. "Hey, replication partner – here's change #52,667 from DC #4." "Ah, thanks – I've seen that one from another replication partner, so I'll just ignore it this time."

USNs are incredibly fragile. Roll back a DC to a snapshot, and it will immediate start replicating the changes that have happened since the snapshot was made, courtesy of your other DCs. That's a good thing, and one of the strengths of AD. But the rolled-back DC will not update its USN. So the next change it makes won't replicate. "Hey! This is DC #5. I've got change #92,877 for you!" "Um… no offense, but I saw that one months ago. The last one I have for you is #107,422. So I'll ignore this." The result? Instant chaos. Changes that don't get replicated. Domain inconsistency. Disaster.

What's worse is that the affected DC – the one you rolled back – won't even warn you of the problem. It doesn't "see" a problem; AD is working exactly as it should. You're just missing changes throughout your domain. You might as well just demote that DC and start over, pretty much negating the "value" in taking the snapshot in the first place.

The rolled-back DC will not update its USN. So the next change it makes won't replicate. The result? Instant chaos.

This situation is alarming enough that, in Windows Server 2012, Microsoft specifically addressed it. The latest version of Hyper-V, along with VMware vSphere 5.1, support a VM generation ID, which AD can use to determine if it was rolled back to a snapshot. If that happens, the DC will automatically employ a set of safety steps, allowing for proper replication and preventing disaster. Of course, that only works for DCs running on the latest Windows OS, on a compatible virtualization system. Any other virtualized DC must be protected in other ways – ideally by a qualified recovery solution, rather than by simple VM snapshots.

The Solution? Well-Made Tools

Go buy a bunch of lumber and you're ready to built a house, right? Well, no – not quite. You'll need tools, and those don't come bundled with the lumber. So it is with Windows: many of the capabilities you'll need for a successful, reliable environment aren't bundled "in the box." Your organization's concerns, priorities, and tolerance for downtime (and loss) will dictate the specific tools you need.

With Windows, many of the capabilities you'll need for a successful, reliable environment aren't bundled "in the box." Your organization's concerns, priorities, and tolerance for downtime (and loss) will dictate the specific tools you need.

What's important is not that you select AD recovery tools – that's a foregone conclusion. What's important is that you select the right tools. Specifically, you'll want a solution that can, in a single console, address all of the failure scenarios you want to be able to deal with: single object recovery, attribute recovery, GPO recovery, and even forest recovery, if that's a concern.

You'll also want a solution that makes recovery easy. When the chips are down, you don't want to have to run around looking up the syntax for complex command-line tools that enable a recovery. In a failure, you have enough pressure, and enough people breathing down your neck; you need a tool that just does the job. Think graphical wizards instead of inch-thick three-ring binders with recovery instructions. Think point-and-click, drag-and-drop tools that make it easy and intuitive to begin and complete the recovery. Solutions that automatically handle backups, and that you can rely on to be available when disaster eventually does strike.

Also consider the organization behind your recovery solution. Are they available to help you out if – heaven forbid – your entire forest crashes and you need to recover? Will they sit on the phone – perhaps alongside Microsoft Product Support – guiding you through a fix? That kind of backup – especially from experts who do that kind of thing all day, every day – is invaluable. You'll get back online faster, with fewer mistakes and less loss of data.

You'll want a solution that makes recovery easy. When the chips are down, you don't want to have to run around looking up the syntax for complex command-line tools that enable a recovery.

Don't wait until you're neck-deep in an AD recovery to wish you'd had the right tools in place. Recovery preparedness is an insurance policy, just like the one on your car or your house. You might wish you didn't have to think about it in advance, but when something goes wrong that policy is priceless.

Recovery Manager for Active Directory

Recovery Manager for Active Directory enables you to prevent system downtime and lost productivity as the result of human error or hardware and software failures that corrupt Active Directory (AD), system configurations or Group Policy data.

Now you can automate backups, quickly compare a backup to the current value of AD to pinpoint changes and instantly recover the desired data.

Using online, granular restore capabilities, you can recover entire sections of the directory, selected objects or individual attributes—all without taking AD offline. This time-saving solution reduces costs and increases productivity.

Recovery Manager for Active Directory Forest Edition

Recovery Manager for Active Directory Forest Edition quickly restores your entire domain or forest in the event of a major disaster or AD corruption. By selecting unaffected backups, quarantining the damaged environment and automating all the manual steps required to facilitate the recovery, Forest Edition greatly reduces downtime to save your organization lost productivity and lost revenue.

By leveraging the backups from Recovery Manager for Active Directory, the Forest Edition extends the value by simplifying the requirements for recovering a domain or forest in the event of a major disaster. This process is closely aligned with Microsoft's native forest recovery approach and provides the option to restore some DCs from backup and others through demoting and re-promoting them with DCPromo.