Cayosoft®

# Solution Brief

## Instant Forest Recovery with Standby Directories

True Forest-Level Fault Tolerance (FLFT): The Breakthrough Alternative To Legacy Forest Recovery Tools

### BACKGROUND

The two third-party Active Directory (AD) forest recovery software products sold prior to 2021, use a common recovery method that originated at Aelita Software (now Quest Software) in the early 2000s. At the time, Aelita sold an AD data recovery tool called Recovery Manager, which simplified restoring AD data, such as users and groups, making it popular with AD owners. At one point, the Aelita support and development teams assisted a customer with performing a forest recovery manually and inspired their AD forest recovery products. The resulting software, created by Aelita, was a game changer of its time because it automated the complex process of recovery after a forest outage. An almost identical derivative tool is included in a product by Semperis, which has some benefits over the Quest product.

While Microsoft doesn't provide a forest recovery tool, they do supply guidance on their website that explains how forest recovery works in theory. Some believe that Microsoft providing such guidance suggests forest recovery can and should be done with scripting. In reality, building these complicated contraptions simply multiplies the potential for problems and issues. For the purposes of this brief, "legacy tools" refers to off-the-shelf software. This brief will describe how standby directories overcome the shortcomings of legacy tools and illustrate the real benefits to the organization, in terms of simplicity and reliability.

### THE CHALLENGE

The primary problem with legacy tools is that they wait until after an outage has occurred and then attempt to perform a recovery. Arguably, during the outage is the worst possible time to attempt a recovery.

This is because there is an immense amount of pressure from the enterprise directed at IT to "fix it." Also, asking a human to perform a complex recovery process under tremendous stress, when they are only hands on with the tool a couple of times each year, makes the odds of a mistake exponentially higher. In the end, legacy tools leave irrevocable doubts: that each step still works when called upon and whether the recovery itself will work, as no one really knows until the recovery is attempted. The solution to this problem is to go beyond legacy recovery and implement a standby directory solution.

*Note: Standby directory for forest recovery is a patent-pending technology by Cayosoft, Inc.*

### HOW STANDBY DIRECTORIES WORK

The standby directory recovery architecture is a breakthrough in Active Directory forest recovery with numerous benefits, making it a clear choice when deciding between legacy forest recovery or a modern, unified full forest recovery solution.

Standby directories deliver forest-level fault tolerance (FLFT) and resilience in a way that legacy recovery truly can't. There's no comparison in terms of how long it takes to recover because with standby directories there is no time spent performing a post-outage recovery. The standby directory is always ready to take over when needed.

Standby directories are created by performing a backup of the existing production forest's domain controllers (DCs) and configuration details. A pre-outage recovery is then completed in the cloud on an isolated virtual network, where it is instantly available. By scheduling this process periodically, this methodology eliminates possible failures and removes the "will it or won't it work" doubts, because technically it already worked.

## STANDBY DIRECTORY BENEFITS

The additional benefits of standby directories reside in the details of how the solution is implemented. The deployment and backup techniques of a standby directory solution are mostly identical to legacy tools, except the recovery phase, which is where technological advancements reinvent the process and eliminate the legacy problems.

### Isolated Recovery Site(s)

Rather than managing dozens or hundreds of dedicated virtual machines (VMs) or servers to restore the DCs, along with the expense and updates they require, a standby directory model automatically creates an isolated recovery site. This is where the necessary DCs are created as VMs in an isolated network on Azure or AWS. Using an isolated recovery site also ensures naming or addressing conflicts don't arise between the recovery site and the production network, which could possibly interrupt the normal operation of the production AD.

### Continuous Recovery Testing

When a recovery site is created, the DCs are automatically started. Any issues with server configuration are immediately recognized and the IT staff can be alerted to resolve the issue before an outage occurs. This may also be of benefit when answering legal or regulatory questions around business continuity and availability of the organization's computing and IT systems.

### Instant Recovery

If it becomes necessary to switch to an isolated recovery site, the change is made to the network, directing traffic to the site of choice. Not only is this the fastest way to recover, but it's the most resilient method of recovery, should the production directory be down. Instant recovery can also be used as a proactive action against a suspected compromise, such as an advanced persistent threat (APT). If it is suspected that the production directory has become compromised, the compromise can be removed in one of the recovery sites. An instant recovery can then be performed switching to the uncompromised directory before the threat actor can act.

### Low Directory Data Latency

When a new backup is created, scheduling the creation of a recovery site allows for multiple copies of the forest to be created. This minimizes the age of directory data between the site and the original production directory.

### Possible Financial Gains

In some situations, the platform vendor may not charge for VMs that are less than 30 days old. Ultimately, there may be no costs associated with the standby site servers if the site is created then replaced automatically by the solution within that timeframe. If this is the case with the chosen vendor, the cost savings is likely many times the cost of the standby directory solution itself.

### Accuracy Across Dev > Test > Prod Environments

Recovery sites can also be used to create accurate development (Dev) and test environments, because of the ease with which these sites can be created. With an accurate representation of your environment, application testing prior to deployment is more likely to present a more precise picture of how that application will perform in the production directory environment.

### Reduction in Need for Premier Services & Support

Premier services are typically purchased by AD owners to remediate fears that recovery will fail. Legacy recovery tool venders sell these premier services for their products only and don't actually perform the recovery. Effectively, these services are offered at a high premium so if the legacy recovery fails, the vendor is there to troubleshoot their own product's issue. This is not needed with the standby directory model.

---

### ABOUT CAYOSOFT

Cayosoft delivers the only unified solution enabling organizations to securely manage, continuously monitor for threats or suspect changes, and instantly recover their Microsoft platforms, including on-premises Active Directory, hybrid AD, Azure AD, Office 365, and more.

Cayosoft Guardian Forest Recovery is the industry's only solution combining all critical AD recovery scenarios into a single, unified platform. Cayosoft Guardian Forest Recovery's capabilities include: hybrid change monitoring, instant rollback of unwanted changes to objects and attributes, instant rollback of unwanted changes to AD group policies, antivirus-like threat protection for hybrid AD, recovery of domain controllers, partitions, and Instant Forest Recovery, using the standby directory architecture discussed in this solution brief.

To learn more, visit cayosoft.com and be sure to follow @cayosoft on LinkedIn, Twitter, and Facebook.

For more information about Cayosoft Guardian Forest Recovery, visit cayosoft.com/gfr.