WHITEPAPER RESOURCE

Active Directory Disaster Recovery

Written by Russell Smith

Petri IT Knowledgebase

A BWW Media Group Brand

SPONSORED BY

semperis

EXECUTIVE SUMMARY

As the cornerstone of most enterprise IT systems, Active Directory has grown both in importance and complexity in recent years. Enterprise IT environments have evolved with the rise of the mobile workforce and cloud-based applications, and as a result, businesses have become increasingly dependent on Active Directory for authentication and authorization.

The new Active Directory usage landscape has introduced greater complexity to the enterprise IT environment, raising the risk of AD disasters tied to human error and cyberattack. More and more frequently, attackers are using Active Directory as an attack vector to compromise enterprises and, in some severe cases, wiping out the entire IT environment.

Active Directory Disaster Recovery has always been an extremely complicated process, requiring lengthy preparation, planning and testing. Depending on the size of the forest, and source of AD failure, restoring Active Directory can take days or more, rendering businesses non-functional during the recovery process. This white paper examines the complexity of Active Directory recovery, outlines potential Active Directory failures and solutions, and proves the necessity for an Active Directory Disaster Recovery plan.

THE COMPLEXITY OF ACTIVE DIRECTORY RECOVERY

Active Directory is not immune to disasters and recovering AD in the event of a disaster requires in-depth knowledge of how it works. Active Directory is designed for

distributed networks and uses a multi-master replication model to ensure that the directory can be updated and queried efficiently in any location. As a multi-master replicated database, it is subject to replication timing constraints with the potential for different directory views depending on the Domain Controller (DC) to which you are connected.

The key challenge in Active Directory recovery is that you cannot simply restore a single domain controller from a backup and hope the environment is back to normal. DCs work together to form a topology and provide a set of services across an organization - this topology is built into the metadata of an AD forest and that metadata is retained within the AD's backup. When you restore a domain controller, you must ensure that the metadata of the restored environment is consistent with the servers that are available—not those that used to be available. Otherwise, client systems will be unable to correctly leverage your newly restored environment.

In addition, the restoration itself must be carefully orchestrated. Root domain services must be brought up before children, Flexible Single Master Operation (FSMO) roles must be restored and the Global Catalog must be re-built. If you throw DNS into the mix, client systems will not find the right services if DNS, a critical piece of AD health, does not reflect the actual environment as it exists right now (as opposed to reflecting the previous environment).

In order to properly restore the existing environment, at least one domain controller in each domain should be restored from backup in isolation, and then reconnected to recreate the forest. Only once privileged accounts have had their passwords reset and any issues that were present before the restore operation have been corrected, should the remaining domain controllers be redeployed, and the new directory database allowed to replicate.

The bottom line is that the orchestration of the recovery of Active Directory is just as important as having backups of your DCs, and this complexity can greatly prolong the recovery process, if being done manually. The Microsoft Active Directory forest recovery **guide** only provides generic instructions that need to be adapted for each unique restore operation and require a lot of manual effort, meaning that Active Directory could be unavailable for a few days if you need to restore a full forest. The complexity of the recovery process will depend on what caused the disaster, so it's critical to understand the root cause of the failure prior to performing a restore.

WHEN DISASTER STRIKES

Information systems rely on Active Directory for user authentication and security, so any outage can be catastrophic. Some common events that cause Active Directory to fail, or actions that are irreversible, include:

- Database corruption
- Accidental or intentional deletion of objects
- Planned schema changes
- Unplanned or unsanctioned schema changes
- Raising the functional level of the domain or forest
- Permission changes

Disk and memory errors can cause database corruption, which often results in lsass.exe errors in the System event log and the Active Directory Domain Services to halt. If you have two or more domain controllers in each site, the temporary unavailability of a single domain controller shouldn't be critical. But if physical or logical corruption spreads to more than one domain controller, then it might be necessary to perform a complete forest restore.

For example, when a British Hospital Trust suffered a complete Active Directory failure in 2013, it took the IT team days to diagnose and repair the failure. The outage was caused by database corruption which happened over a long holiday weekend and went unnoticed until the following Tuesday morning. Experts from Microsoft and an IT consultancy worked for two days to restore the Trust's Active Directory.

The outage delayed the treatment of 706 patients, and new appointments were recorded on paper for the duration of the outage and then entered manually once systems were back online.

RANSOMWARE & MALICIOUS ACTS

Ransomware, and other types of malware, infect end-user devices, but IT infrastructure is increasingly the target. End-user devices are usually the first target because they are not secured to the same level as domain controllers. Hackers can harvest privileged Active Directory account password hashes and Kerberos tickets from users' PCs to stealthily access domain controllers without needing to know an account password. This so called "pass the hash" attack on privileged Active Directory credentials gives hackers access to domain controllers and any systems that rely on Active Directory for security.

But ransomware isn't the only danger. Insiders can intentionally or accidentally compromise Active Directory. Especially in situations where security best practices are not followed. IT staff are commonly granted privileged access to Active Directory on a permanent basis, which makes a hacker's job easier. Furthermore, separation of administration roles is rarely practiced, and security dependencies are created between highly-trusted systems, like domain controllers, and systems with lower trust, like end-user devices. Automation technologies, like PowerShell scripts, can make large numbers of changes

to Active Directory that quickly propagate. But poorly tested code can result in failures of production systems. Malicious software can also find its way onto domain controllers. But it only takes a single change to cause a failure that prevents domain controllers servicing logon requests, breaks replication, prevents additional domain controllers being added to the domain, or changes being made to the directory.

Because of these threats, organizations need to protect Active Directory and prepare for worst-case scenarios where the only option is to perform a complete forest restore.

PLANNED & MALICIOUS CHANGES

Regardless of how much planning and testing you carry out, applications and systems in your production environment could be affected by changes to Active Directory. Changes sometimes happen accidentally or are the result of malicious activity. Strict change control procedures can prevent unwanted changes, but unsanctioned changes could be carried out by a malicious actor, a disgruntled insider, or accidentally by a system administrator.

Schema changes, and raising the forest and domain function levels, are both irreversible actions. Forest and domain functional levels determine the level of compatibility for the forest and domain respectively with domain controllers running older versions of Windows Server. When the domain and forest functional levels are raised, all domain controllers in the forest and domain must be running a version of Windows Server that is at least the same version as the functional level of the forest and domain.

Raising domain and forest functional levels is a safe operation if all domain controllers are running the required version of Windows Server to support the new functional level. Schema changes can be more problematic and should be tested in a pre-production lab environment before being approved for release in production because there's no supported method for backing out of schema changes. If schema or functional level changes need to be reversed, the only option is to perform a complete forest restore.

OBJECT DELETION

Deleting directory objects, or changes to permissions on objects, can cause Active Directory to fail. Strict change control procedures, and adhering to security best practices, are the best ways to avoid accidental object deletion or modification. Active Directory also includes a flag that can be set on important objects to prevent users deleting them with one click. To enable the flag on every Organizational Unit (OU) in a domain, use the Get-ADOrganizationalUnit and Set-ADObject Powershell cmdlets as shown below.

```
Get-ADOrganizationalUnit
-filter * | Set-ADObject
-ProtectedFromAccidentalDeletion:$true
```

The Active Directory Recycle Bin can be used to restore deleted objects but it isn't enabled by default. The forest functional level must be set to Windows Server 2008 R2 (or higher) and it is an irreversible change. Starting with the administration tools for Windows Server 2012, deleted objects can be restored using Active Directory Administrative Center (ADAC).

Using the Recycle Bin is preferable to restoring objects from backup or reanimating tombstoned objects. Performing an authoritative restore requires booting a domain controller into Directory Services Restore Mode. Note that removed link-valued attributes, such as groups, and cleared non-link-valued attributes, are not restored when you reanimate tombstoned objects.

Some organizations implement lag sites as a recovery solution and for restoring deleted objects. A lag site is an Active Directory site which has delayed replication from other sites in the domain. If objects are deleted from the directory, the lag site can be used to restore them. But lag sites shouldn't be used as a complete recovery solution for several reasons.

Microsoft doesn't support lag sites as a recovery solution. In the event of a malicious attack, AD can be configured so that objects are replicated immediately to the lag site. Additionally, lag sites are a security threat when objects deleted in the main site remain in the lag site. Consider a situation where a user account is deleted but still exists in the lag site. If the Netlogon service is enabled on domain controllers in the lag site, a deleted user might still be able to log on.

BOUNCING BACK

RECOVERING A SINGLE DOMAIN CONTROLLER

Corruption problems can sometimes be repaired in Directory Services Restore Mode (DSRM) using ntdsutil, a built-in command-line tool. DSRM is a safe mode for Active Directory that allows administrators to carry out repairs while the database is offline. In a worst-case scenario, where the database can't be repaired and only one domain controller is affected, the server can be removed from the domain and re-promoted.

If one domain controller needs to be removed from the domain, move or seize (depending upon the state of the domain controller) any FSMO roles it holds and then remove the domain controller from the domain using the **Uninstall-AddsDomainController** PowerShell cmdlet or Server Manager. If the domain controller is Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012, the

demoted domain controller's metadata is automatically removed from the directory providing that during removal, Force the removal of this domain controller is not selected, or the -forceremoval parameter isn't set to $true when using PowerShell.

Reinstall Active Directory on the same or different hardware and then let the directory partitions replicate to it. If you decide to use the same server hardware, it is important to determine the root cause of the failure before reinstating the server.

PERFORMING A FOREST RESTORE

In the event of a complete outage, security breach, or irreversible change to Active Directory, you should perform a forest restore to bring back all the domains in a forest. Restoring a forest is a complicated process that involves restoring Active Directory from full server backups of one domain controller in each domain, connecting the restored domains on an isolated network, and then adding the remaining domain controllers.

Performing a forest restore involves many steps that mean Active Directory could be unavailable for a couple of days. Microsoft only provides generic forest recovery instructions that need to be adapted for each unique restore operation. You can download the white paper here.

One domain controller in each domain must be restored from backup in isolation, and then reconnected to recreate the forest. Only once privileged accounts have had their passwords reset and any issues that were present before the restore operation have been corrected, should the remaining domain controllers be redeployed, and the new directory database allowed to replicate.

SELECTING A TRUSTED BACKUP

Microsoft recommends that you use a trusted backup that is a few days old to avoid restoring a copy of the database that reintroduces the problem that caused the failure, unless you can pinpoint exactly when the problem was introduced into the directory, with the help of the Windows event logs. In the case of a malicious attack, or complete forest melt down, the event logs might not be available unless they are regularly shipped to a server that doesn't rely on Active Directory for its security.

Using a backup that is a few days old will mean that the restored domains won't include changes made to the directory in the days before the outage. But the effort required to reinstate these changes can offset the time lost in restoring domains that don't resolve the issues present before the outage occurred. All group memberships should be reviewed after restoration, and this process will identify a significant number of the changes made post backup.

Starting in Windows Server 2008, the

Active Directory database mounting tool (Dsamain.exe) can be used to mount the Active Directory database from backups made using ntdsutil, Windows Backup, or a backup tool that supports Active Directory. A mounted database can be viewed using ldp.exe or Active Directory Users and Computers (ADUC). The ability to view the database in this way is useful when determining which backup to use for a restore operation. In older versions of Windows Server, it was necessary to restore a domain controller to view the Active Directory database.

FULL SERVER RESTORE

Windows Server 2008 (and later) doesn't support restoring a server using the system state to a new installation of Windows, regardless of whether installed on the same or new hardware. Therefore, you should make full server backups of domain controllers, perform full server restores, and only perform a system state restore after a full server restore to mark SYSVOL as authoritative if the restored server is the first writeable domain controller in the domain. At least two writeable domain controllers should be backed up in each domain.

If you don't want to make two backups for each domain controller, i.e. a full server backup and a system state backup, then SYSVOL can be marked authoritative by editing the msDFSR-Options attribute **(https://support.microsoft.com/en-us/help/2218556/how-to-force-an-authoritative-and-non-authoritative-synchronization-fo)** in Active Directory if SYSVOL is replicated using DFRS. If it is replicated using FRS, then you will need to stop the FRS service, edit the BurFlags registry key **(https://support.microsoft.com/en-us/help/290762/using-the-burflags-registry-key-to-reinitialize-file-replication-servi)**, and restart the service.

A writeable domain controller should be restored in the forest root first to make sure that the Schema Admins and Enterprise Admins groups are present before other domains are restored and to make sure that the trust hierarchy isn't broken during the restore process. Unless the forest consists of a single domain, the domain controller you restore should not be a Global Catalog. If you have no choice but to restore a domain controller that was a Global Catalog, disable the Global Catalog after the restore operation is complete to prevent lingering objects. You should perform a non-authoritative restore of Active Directory 'Directory Services' and an authoritative restore of the SYSVOL share so that when additional domain controllers are added to the domain, they synchronize the contents of SYSVOL from a server that has been set as authoritative. You can perform a restore using the built-in Windows Backup tool or a third-party backup solution that supports Active Directory. Once the forest root domain is in place, you can begin to recover other domains simultaneously, providing that parent

domains are always restored before child domains. The last step is to make the domain controller in the forest root a Global Catalog. Once all the domains are restored, you can check that they are working using the dcdiag, nltest, and repadmin tools on an isolated network.

Before connecting the restored forest back to the production network and redeploying other domain controllers, you should clean up the metadata for all other writeable domain controllers in the domain. This will make sure that NTDS-settings objects are not duplicated, and unnecessary replication links are not created. Furthermore, if restored domain controllers held the RID master FSMO role before recovery, it won't be able to create new relative IDs (RIDs) until the metadata for all other writeable domain controllers is removed. RIDs form part of the unique security identifier (SID) that is assigned to each new Active Directory security principal.

RESTORING THE REMAINING DOMAIN CONTROLLERS

If you are sure that the forest failure wasn't cause by something outside of Active Directory, i.e. a hardware failure or security breach, you can connect the restored forest to the production network and add the remaining domain controllers to each domain without reinstalling Windows Server. Before you add the domain controllers back to the restored forest, forcibly remove them from the failed domain. If forest failure was caused by something outside of Active Directory, like ransomware, then you must reinstall Windows Server.

RISK AND IMPACT ASSESSMENT

Well known for their high-performance graphics cards, NVIDIA has embraced VR Implementing security best practices, and the latest technologies in Windows Server 2016 and Windows 10, helps reduce the likelihood of a successful ransomware attack. But systems can never be one hundred percent secure, so a disaster recovery plan for Active Directory is essential. Performing an impact assessment for Active Directory involves mapping security dependencies to determine which critical business systems rely on Active Directory for security. Once these dependencies have been established, you will be able to identify all the systems that rely on Active Directory. Bringing Active Directory online as quickly as possible after a failure requires a tested disaster recovery plan. The details of the plan will depend on many factors:

- which version of Windows Server each domain controller is running
- whether domain controllers are installed on physical or virtual hosts
- how you will determine which is the latest trusted backup for each domain
- whether domain controllers will be installed to the same or new hardware

Regulatory standards and service level agreements (SLAs) may also impact decisions in how you plan for disaster recovery. The recovery process can be speeded up by using full server restores instead of system state backups. But orchestrating a full forest restore is difficult using the standard tools because they are not designed for automation. As part of designing a recovery plan, you should determine which domain controllers are required to get line-of-business systems back online even if performance is impacted.

A further concern for companies with a hybrid cloud solution is Azure Active Directory, which in larger organizations is almost always synchronized with on-premise Active Directory. Extending on-premise Active Directory to the cloud introduces an additional risk and complexity to the management and the recovery process.

A forest-wide Active Directory failure can cause a complete outage of all business systems, and recovery can be complex and time-consuming. Following best practice advice from Microsoft is an essential step in ensuring that Active Directory is protected. But nothing can replace a proven disaster recovery plan.

SUMMARY

In recent years, businesses have become increasingly dependent on Active Directory, expanding their reliance on AD Directory Services to include authentication and authorization of mobile workforce and cloud-based applications. This increased dependency has led to greater complexity in the enterprise IT environment and raised the risk of Active Directory disasters tied to ransomware, malicious acts or misconfigurations, and human error. While some Active Directory failures can be repaired manually, recovering Active Directory in case of a disaster is a long, cumbersome process that can leave businesses offline for days. The only way to ensure continued business operations is by making sure that Active Directory is truly protected and a solid disaster recovery plan is in place.

Semperis is an enterprise identity protection company that enables organizations to quickly recover from accidental or malicious changes and disasters that compromise Active Directory, on-premises and on cloud. The Semperis Directory Services Protection Platform™ provides enterprises with the capabilities to automatically restore an entire Active Directory forest, quickly recover thousands of objects or a single crucial attribute, and instantly revert to a previous Active Directory state. Semperis customers include Fortune 500 companies and enterprises spanning financial, healthcare, government and other industries worldwide.