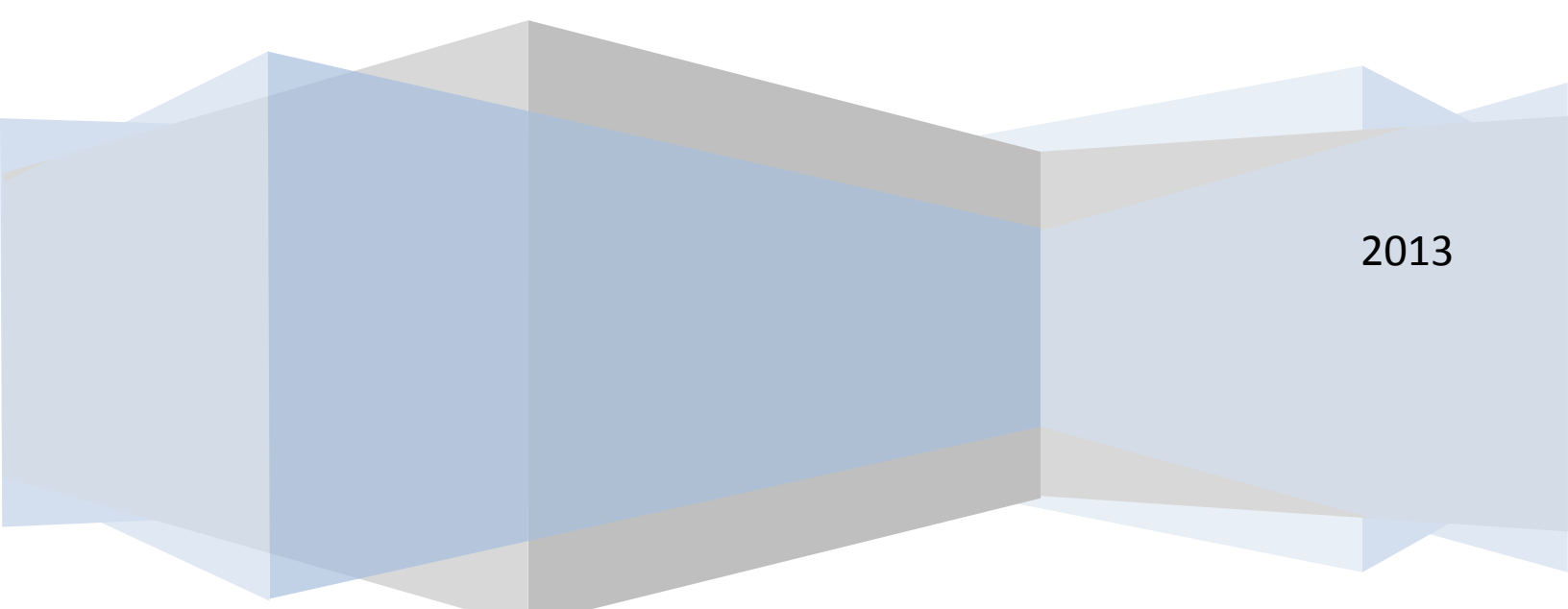


www.lepide.com

Ensuring business continuity after Active Directory disasters

Whitepaper



2013

Introduction

Active Directory is the distributed directory system that contains identification and authentication information of all users, access rights and usage policies of entire Windows network. Active Directory has been designed to cater to all sizes of organizations ranging from small to large ones and the associated resource requirements of implementing and managing Active Directory depends on a number of factors that include size, security level and disaster recovery planning.

Active Directory disaster recovery is an important component of organization's business continuity planning. A well thought-out plan could swiftly restore Active Directory back from disasters thus ensuring smooth flow of business operations without interruptions. Having a robust Active Directory disaster recovery plan ensures a number of benefits for organizations:

- Prevents losses resulting from interruption to normal business operation.
- Ensures adherence to regulatory compliance.
- Keeps the network secure and safe supplementing organizational survival.
- Eliminates risks emerging out of Active Directory disasters.

Active Directory disasters and recovery options

Active Directory disasters may be classified broadly in two categories: Database corruption and Data corruption. Database corruptions could be due to natural disasters or systemic disasters such as disk crash, software failure etc; Data corruption are the result of systemic disasters such as accidental deletion of Active Directory objects, unwanted modifications to Active Directory etc.

This whitepaper focuses on Active Directory disasters caused by Data Corruption and some of the efficient methods (both native and using third-party software) to restore Active Directory to previous stable state.

Data corruption issues of the Active Directory can be solved by any of the following means depending on the type of corruption and viability of solution:

Re-installation: This method is only possible if there is at least one healthy DC present in the domain. Corrupt DC is re-installed and **DCPROMO** operation of Active Directory replicates the data from healthy DC on newly installed DC accurately. Clearly, small organizations running a single DC cannot benefit from this method. Also, considering resource constraints such as bandwidth etc. this method should be tried only if there is no proper backup to restore the DC.

Authoritative backup restoration: Authoritative restore allows you to increment version number of attributes that are being restored from backup so that they are not replaced by attributes of the current state. This method should be used in case some objects have been

deleted and the undesired changes have already been replicated to other DCs. Authoritative restore ensures that restored change is replicated to other DCs and not the other way round. Authoritative backup restoration is performed by a separate tool **NTDSUTIL.exe**.

Non-authoritative backup restoration: Non-authoritative restore does not give you the option of increasing the version number of restored attributes; hence, Object will be updated with the changes that have been affected since the backup was created thus ensuring the latest configuration exists on the restored DC. This type of restoration is preferable when you are performing complete restoration or if accidental deletions (as considered in authoritative restore) have not been affected on replication partners.

Granular Restoration of Active Directory objects

While most of the organizations invest a fortune in devising a complete disaster recovery plan, which rarely happens, they ignore scenarios that are more frequent and cause great pain to Active Directory administrators – accidental deletion or modification to Active Directory objects. A User or Computer object got deleted, an entire group of Users or Computers got deleted; it takes only a few mouse clicks to cause these undesirable changes. However, effect of such changes might not be as innocuous as the cause might seem. It could rattle your business continuity plan leading to severe losses in business operations. Active Directory has provisions to rollback changes at granular level, but it suffers from a number of disadvantages:

- It is very difficult to identify the changes that have led to interruption in business operation. Hit and trial method may take a lot of time before such changes get identified.
- Even after you have identified the changes, restoring objects at granular level might take hours which is unacceptable in normal business scenario.
- Both authoritative and non-authoritative restorations of changes involve a complex set of steps that are difficult to perform.
- Objects that need to be restored might be spread across more than one backup. In such cases dealing with multiple backups using native methods could be difficult.
- Considering the concentration and patience required to perform such tasks, you cannot delegate this task to less experienced users, particularly if that is the cause of the accidental deletion.

Active Directory restoration: Things to consider

Considering Active Directory restoration from data corruption issues such as accidental deletion and modification of Active Directory objects, administrators need to keep in mind a few important points while devising the Active Directory restoration plan apart from the traditional complete backup restoration:

Fast restoration: Dealing with data corruption issues such as accidental deletion or modification requires you to restore the changes as soon as possible. It's quite difficult to bring agility to the restoration process while using NTBACKUP and other native methods of restoration. If there is an alert mechanism that can inform you of the critical changes at the earliest, then damages due to such changes can be eliminated or at least minimized.

Rollback unwanted changes: To rollback unwanted changes granularly, Admins need to have provisions to detect and undo changes to a single object. These are the changes that occur more frequently than complete restoration of Active Directory. Unfortunately, native methods to identify and rollback such changes are complex and time consuming.

Regular Snapshot creation: While restoring Active Directory objects granularly, each of them might be required to be restored to a different point of time a few hours apart. This calls for regular snapshot creation and a mechanism to compare these snapshots with current Active Directory status and rollback changes as required – again a difficult objective to fulfill using native methods.

Restoring from old backups: Backup expiration is another problem that Admins have to deal with while restoring objects to an old state. Generally, Active Directory requires the backup to be not more than 60 days old (180 days in case of Windows Server 2003) for successful restoration and avoiding “Lingering Object” phenomenon. In real world scenario, successful execution of business operations might require you to restore objects to a state well beyond this period.

Tracking multiple domains: Things get messier if you are dealing with more than one domain. Managing regular backups and performing granular restoration become even more complex. Having a centralized pool of Active Directory change logs from all the domains in the network not only ensures security of data but also helps in efficient Active Directory change tracking and control.

It is very difficult to take into consideration all these points while using native Active Directory restoration methods. Specialized software such as LepideAuditor for Active Directory (LAAD) can, however, fulfill these objectives and offer a set of other high value features.

LepideAuditor for Active Directory: Track and Control Active Directory changes

LepideAuditor for Active Directory allows you to track and control Active Directory changes that help in ensuring a highly-secured Active Directory environment. Software ensures business

continuity by ensuring fast recovery from disasters such as data corruption issues. Key features of software are:

Track all domains in the network: LAAD acts as a centralized platform from which you can track all domains in the network. Create a single pool of data and rollback changes for all domains from the same platform.

Long time archiving to support compliance: LAAD creates centralized database of all Active Directory changes that can be archived for as long as you want. This helps in historical change analysis for compliance and forensic investigations.

Quickly identify and restores changes: Restoring Active Directory changes with the help of LAAD is as fast as it can get. Software highlights changes in different colors – deletions in red and modifications in blue. All that is required from you is to perform a few clicks and Objects are restored.

Instant Alert: Instant alerts can be set for critical changes, so that Admins are informed as and when they occur to minimize the response time.

Granular restoration of unwanted changes: Dealing with accidental deletion and modifications is extremely easy with the help of LAAD. It is possible to rollback a single change with just a few clicks.

Create regular snapshots: Software creates regular snapshots of Active Directory that can be as frequent as fifteen minutes to offer you more options while restoring using backups.

LepideAuditor for Active Directory: Major benefits

LAAD helps you to identify undesirable changes made to Active Directory and restore it to a desirable state using any of the snapshots created by software. This tool is a great aid to your disaster recovery plan as you can rollback unwanted changes to bring Active Directory to a previous stable state.

Ensure Business Continuity: Restore Active Directory to a previous stable state thus ensuring business continuity. Create a secure Active Directory environment by eliminating all risk factors such as security breach, compliance violation, fraudulent activities etc.

Uphold Compliance: Uphold regulatory compliance such as SOX, HIPPA, PCI, ITIL etc. by implementing internal and external regulations.

Protect Active Directory from unwanted changes: Get instant alerts on critical changes to minimize the response time and undo undesirable changes to protect AD from unwanted changes.

Minimize downtime: Save time in dealing with data corruption issues to reduce downtime of Active Directory environment.

Track Active Directory changes in real time: Track Active Directory changes in real time to get Who, What, When and Where information for all changes.

Conclusion: Protecting Active Directory is a critical component of your organization's Network security policy. It is important to have well defined plan in place to deal with Active Directory disasters to ensure business continuity. Many a times, Active Directory disasters are caused by seemingly minor incidences such as accidental deletion and modification of Objects.

Ordinary, as these changes might appear, steps to restore Active Directory to a stable state by rolling back cases of deletion and modifications might be incredibly complex and time consuming. LepideAuditor for Active Directory ensures fast restoration of Active Directory Objects to a stable state by granular rollback of unwanted changes.