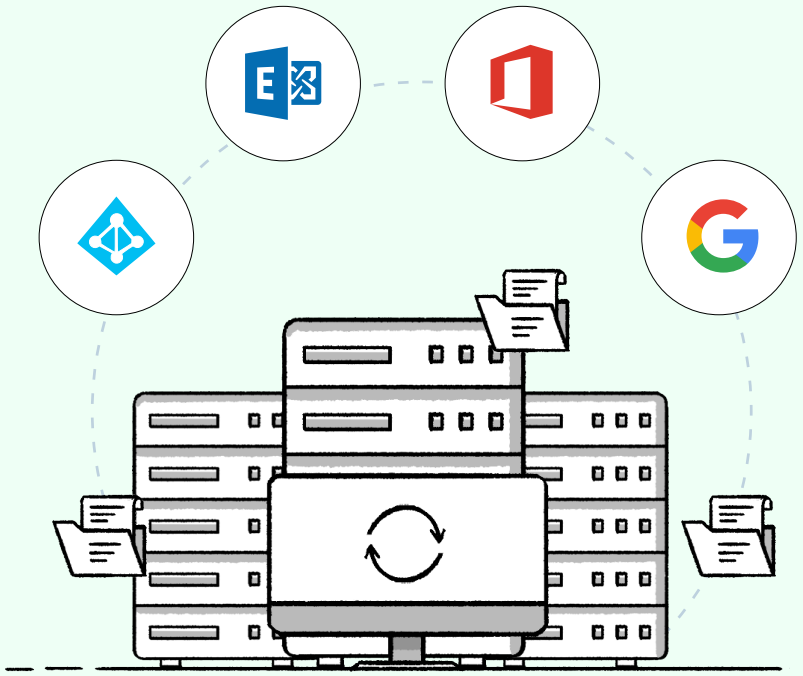
ManageEngine
RecoveryManager Plus

AD DISASTER RECOVERY PLAN: QUESTIONS TO PONDER



Introduction

The intensity, frequency, and extent of damage from floods, fires, and extreme weather are all rising. When you factor in catastrophes like ransomware, server failures, and storage issues, it appears that the future is a quagmire for organizations of all kinds.

Whether the impending disaster is a natural catastrophe, a rat nibbling on power cables, or a deliberate cyberattack, disaster recovery (DR) is a crucial procedure that can help an organization survive and recover. With the help of a DR plan, an organization can zero in on what's most important, rank its risks and assets, create a plan for keeping its data safe, and figure out how to resume normal operations as soon as possible.

What is an IT DR plan?

IT DR is a subset of DR that prioritizes the technological components, like restoring online-critical systems as quickly as possible and minimizing downtime for servers, databases, and employee workstations. The means and steps necessary to recover from a technological disaster are laid out in a DR plan.

What is a business continuity plan (BCP)?

A BCP entails outlining any and all vulnerabilities that can impact the organization's operations, rendering it a vital component of a risk management strategy. After identifying the risks, making a BCP should also involve:

- Understanding the impacts of these risks on operations.
- Implementing precautions and processes to reduce risks.
- Examining procedures to make sure they work.
- Evaluating the DR procedure to ensure that it is updated.

Let's skip to things that matter.

Object-level recovery

What would you do in the event of an administrator with fat finger syndrome deleting five hundred user accounts? Also, to rub salt in the wound, one of them is the CEO's user account.

Questions to ponder

- Can you restore all the user accounts?
- How quickly can you restore the user accounts?
- Can you enable the CEO to carry out their own backup and restoration tasks?

CTRL + Z with RecoveryManager Plus

Deleted user restoration

Restore deleted user accounts to their last known state or to any of their previous versions with ease. Get a preview of the value that you are about to restore before initiating a restoration to prevent restoring unwanted attribute values.

Recovery of users' group memberships

While recovering a deleted user, restore their group memberships along with all the other attributes. Quickly restore users' security permissions so authorized users can access sensitive resources without any delay.

Technicians

Add non-admin users to RecoveryManager Plus so they can carry out certain backup and restoration tasks. Assign each user a role (like auditor, operator, or admin) to provide them with varying levels of administrative access.

Group Policy Object recovery

A junior sysadmin spills hot coffee on their senior admin's clothes and gets fired immediately. While seeking their revenge, they decide to change a critical Group Policy Object (GPO) configuration, such as the one that prevents C-suite executives from accessing folders that contain confidential files or the one that disables the Command Prompt on users' machines.

Questions to ponder

- Is there enough time for you to restore the GPO before a security breach occurs?
- Can you undo any specific modifications made to the GPO?

CTRL + Z with RecoveryManager Plus

AD GPO backup and recovery

RecoveryManager Plus periodically backs up all the changes made to GPOs across your AD environment during each backup cycle. In case of an accidental deletion or modification of GPOs, the backups can be used to restore GPOs to any of their previous versions.

GPO rollbacks

Administrators can roll back GPOs to a previous point in time and void all changes made to the GPOs after that point. This enables administrators to get a GPO back to working condition after accidental modifications.

GPO link backup

This utility can also back up GPO links along with the individual settings. When any GPO link gets disabled accidentally and the GPO in question later gets deleted, restoring the GPO link will also restore the GPO.

Attribute-level recovery

A senior administrator blunders by changing the cab drivers' department from Transport to Support. His company's reputation takes a huge hit since customers are not happy with the new support. All they can hear is, "Where do you want to go?"

Questions to ponder

- Can you automatically restore specific attributes of multiple users?
- Does your organization know how much money it will lose due to downtime?

CTRL + Z with RecoveryManager Plus

Attribute-level restoration

This feature of RecoveryManager Plus lets you restore specific attributes of modified objects. Each change made to an object is stored as an incremental backup, which makes it possible to restore individual attributes.

Linked attribute recovery

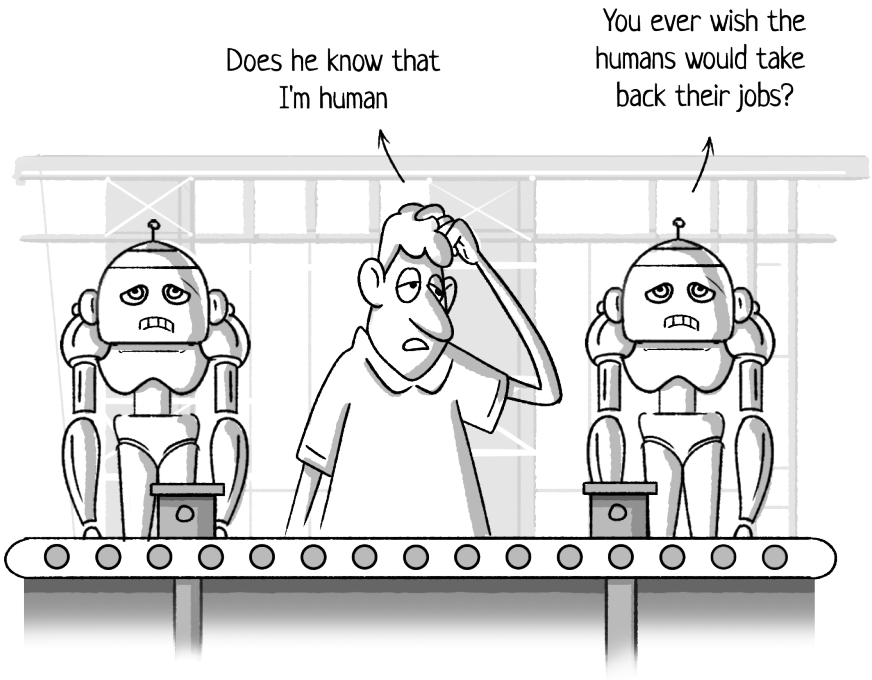
Using this tool, restore the linked attributes of users, such as groups a user was a member of, the list of a user's direct reports and manager, and the list of objects managed by a user (managedObjects attribute).

Security permission restoration

The security permissions and authorizations assigned to users can be restored within a few seconds if any modifications to them are detected. Undeleting users also reinstates all their security permissions along with all other attributes.

Automation of backup processes

There are two types of people: those who create the automation and those who are part of the automation. The last thing we want is a Turing test.



Questions to ponder

- Are you manually backing up your AD environment?
- Can you schedule backups to run during non-business hours and ensure that your AD environment does not undergo any modifications during the backup process?

CTRL + Z with RecoveryManager Plus

Automated AD backups with data integrity

Automate periodic, full backups of your AD environment every week or month, depending on your needs. The backup is updated every time a change is made to AD objects, like the deletion of an object or an attribute-level change. This maintains the backup in a consistent state. Achieve minimal recovery time objectives and recovery point objectives.

Incremental backups

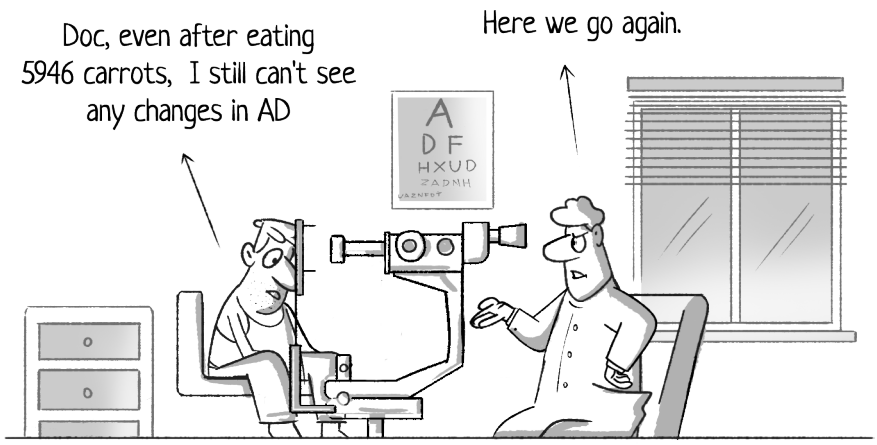
Only incremental backups are created for changes made to AD objects. This ensures that only the changed attributes between two versions are transferred to the backup.

Flexible backup settings

Backup settings can be configured by specifying the OUs, objects, and even specific attributes. The frequency of the backup schedule can also be customized. Rollback Points are created whenever a backup operation is performed.

Visibility and change management

Carrots are amazing vegetables. They are good for your eyes, but unfortunately they can't help admins gain any visibility into changes that take place in their AD environment.



Questions to ponder

- Can you manage the changes in AD data with ease and versatility?
- Do you have a method of readily comparing your live AD environment with your backup?
- Do you have a method of identifying changes that have been made to individual objects since the last backup?

CTRL + Z with RecoveryManager Plus

A bird's-eye view

Gain complete visibility with a user-friendly interface and sleek dashboard view. RecoveryManager Plus provides administrators with comprehensive governance over their AD environment so they can maintain consistency, accessibility, and functionality.

Comparison reports

Generate a comprehensive list of all the versions of backups available from a specified period. This enables you to compare values across every single version and select the best to restore. Administrators can roll back all changes or select individual changes to undo.

Change management

Track the number of changes made to an attribute and the date and time of each so you can choose the right set of changes. This helps you roll back all changes made or a specific set of changes.

A unified backup solution

A school teacher hits the headlines for calling the FBI and the NSA for backup when he lost his students' examination papers in the cloud.

Questions to ponder

- Do you have a solution for backing up and restoring AD, Azure AD, Microsoft 365, Google Workspace, and Exchange?
- Can you back up your Exchange environment, including emails, contacts, and calendars?
- Can you configure long-term retention policies with your solution and store Microsoft 365 backup data for any duration as mandated by compliance regulations?

CTRL + Z with RecoveryManager Plus

Azure AD backup

Back up all Azure AD objects, like users, groups, devices, applications, service principals, directory roles, subscribed stock-keeping units, and domains. Restore entire objects or even specific attributes of individual objects to a backed-up state based on your needs.

Microsoft 365 backup

Back up all mailboxes and sites in your Microsoft 365 environment. Restore entire mailboxes and sites or just specific mailbox items and documents, depending on the situation.

Google Workspace backup

Back up all items in Gmail (emails, contacts, journals, notes, posts, and tasks), Google Calendar, and Google Drive. You can use these backups to restore any data when necessary, regardless of when the data was deleted.

Exchange backup

Back up an restore all mailbox items(emails, calendar entries, contacts, journals, notes, posts, and tasks) in your on premises Exchange and Exchange Online environments.

Conclusion

So, after taking a look at the questions above, is your strategy for handling AD incidents and recovering from disasters up to date? The next incident to impact your organization could happen at any time. Reevaluating your backup and recovery plan to make sure it can save your IT infrastructure and digital assets is a proactive measure that should be taken before a disaster strikes.

With RecoveryManager Plus, a web-based AD backup and restoration tool, administrators can overcome AD disasters caused by undesired changes in their IT environment. RecoveryManager Plus is a holistic enterprise backup and restoration solution that allows you to back up your AD, Microsoft 365, and Exchange environments—all from a single console. In other words, CTRL + Z your AD changes with RecoveryManager Plus.