Averting Disaster:

Preparing Your Organization for an Active Directory Failure

WHITE PAPER

Semperis
Enterprise Identity Protection

Abstract

Since its release in 2000, Active Directory (AD) has become a critical IT infrastructure component that is running in 93% of Fortune 1000 companies[1], and its importance continues to increase with the growth of on-premises/cloud hybrid identity architectures. This changing technological landscape, combined with the recent rash of cyberattacks, has made it necessary for companies to review and update their existing AD Disaster Recovery plan. Active Directory disasters put organizations at risk, with downtime leading to ceased internal and external communications, lost access to line of business applications, lost revenue and damaged brand reputation. This whitepaper reviews the central role Active Directory plays in the enterprise today, examines the real-life threats and impacts of an Active Directory disaster, and helps you ensure that your organization is prepared for any Active Directory failure.

Introduction

Active Directory is one of the most critical enterprise applications, where downtime is not tolerated. In recent years, businesses have become increasingly dependent on Active Directory due to the widespread adoption of new technologies that require AD authentication and authorization.

[1] **Takeshi Numoto**, CVP STB Marketing, May 2013. Fortune 1000 is US businesses, based on revenue.

The rise of SaaS-based applications, which leverage on-premises systems for authentication and access control, has led to the emergence of the hybrid identity model. In this model, the on-premises Active Directory identity store is coupled with a cloud identity service (identity as a service or IDaaS) to authenticate and authorize users to their applications, regardless of where they are located. This means that a hybrid company's field sales team can access salesforce.com using their corporate AD credentials on their notebooks, tablets, or phones, at any given moment. VPN and remote access also often rely on AD authentication, so any disruption in Active Directory services means that employees cannot perform basic business functions or use critical communications applications platforms, like Exchange or Skype for Business.

This increased dependence on Active Directory has led to greater complexity and risk, and any instance of Active Directory failing can severely harm your organization. A major disaster results in ceased operations, lost revenue and, in rare instances, can put a company completely out of business. In order to protect your organization, and ensure your Active Directory services are functioning properly, it is essential to have a robust Disaster Recovery (DR) plan and perform periodic testing.

The Reality of Active Directory Disasters

Active Directory implementations are highly complex, making the system susceptible to human error, hardware failure and software corruption. Over the past two decades, Active Directory has undergone many modifications and these changes, combined with the new usage landscape and heightened security risks, put AD services in a more precarious position than ever. Even Microsoft has acknowledged the complexity and risks tied to Active Directory, publishing the Active Directory Forest Recovery Guide, to help IT organizations navigate Disaster Recovery.

While it might seem rare, Active Directory disasters can and do happen. Since Active Directory underpins every local and wide area network service, even the smallest changes to a system as critical as Active Directory can have catastrophic results.

Examples of Active Directory failures include:

- Schema extension corruption
- Forest functional level raise leading to authentication failure of legacy applications
- Malicious privileged user modifying system permissions
- Ransomware attack encrypting Domain Controllers (DC)
- A single, critical DC failure (e.g. on a site with a single DC)
- Accidental deletion of Group Policies
- Incorrect modifications of critical applications' accounts and groups

These failures interfere with the proper functioning of Active Directory and can be devastating for your business. Recent events expose the vulnerabilities of Active Directory and demonstrate how essential it is to prepare for Disaster Recovery.

How do Active Directory Outages Happen?

1. **Human Error:** An administrator in a large financial institution changed the SQL server service account password, which halted enterprise-wide database replication and backup jobs. Because this was a change, rather than a deletion, and there was no record of the original password, the organization had no way to revert to the previous password.

2. **Cyberattack:** The "NotPetya" malware attack, which was designed to wipe out hard drives entirely, encrypted the drives of every Domain Controller in a large global organization. As a result, the company was faced with the long, tedious process of recovering the DCs from backup and performing manual AD recovery procedures.

3. **AD Configuration Change:** The upgrade of Active Directory authentication from NTLM v1 to NTLM v2 took down an entire production floor in one of the largest manufacturing companies in the world. Unfortunately, IT personnel performing the upgrade were not aware of the fact that the manufacturing machines were authenticating to AD, and that they were running a legacy software that doesn't support NTLM v2.

4. **Rogue Employee:** A telco provider was shut down with no ability to generate invoices after AD became non-responsive. A 24-hour investigation, in partnership with Microsoft, revealed that read permissions were removed from the configuration partition, resulting in a replication failure. The permissions were restored and the company was operational again, only to face the same situation less than a day later. This time, after the restoration was completed, management was required to review all privileged accounts and only a short list left with the administrative permissions.

5. **Software Malfunction:** An Active Directory glitch caused a two-day service outage at the largest health board in Scotland. Information within AD became corrupt and this corruption quickly replicated throughout the organization, crashing the system and resulting in the cancellation of appointments for 700 patients[2].

6. **AD Upgrade:** A large transportation company upgraded their AD Forest functional level from 2003 to 2012. Initially, the upgrade went as planned and the new functional level was set in the organization. However, a few hours later it became clear that one of the mission critical applications in the organization could not operate in the updated AD environment. The functional level change from 2003 to 2012 was irreversible and, as such, the organization had to re-write application code to support operations at the 2012 functional level, causing severe delays in the invoicing process.

7. **Natural Disasters:** Hurricanes, earthquakes and other catastrophes have impacted geographically diverse locations. Domain Controller backups in different geographical locations help, but not as much as having an end to end Disaster Recovery plan in place.

[2] Rare problem blamed for Glasgow health board IT crash, BBC News, November 2013.

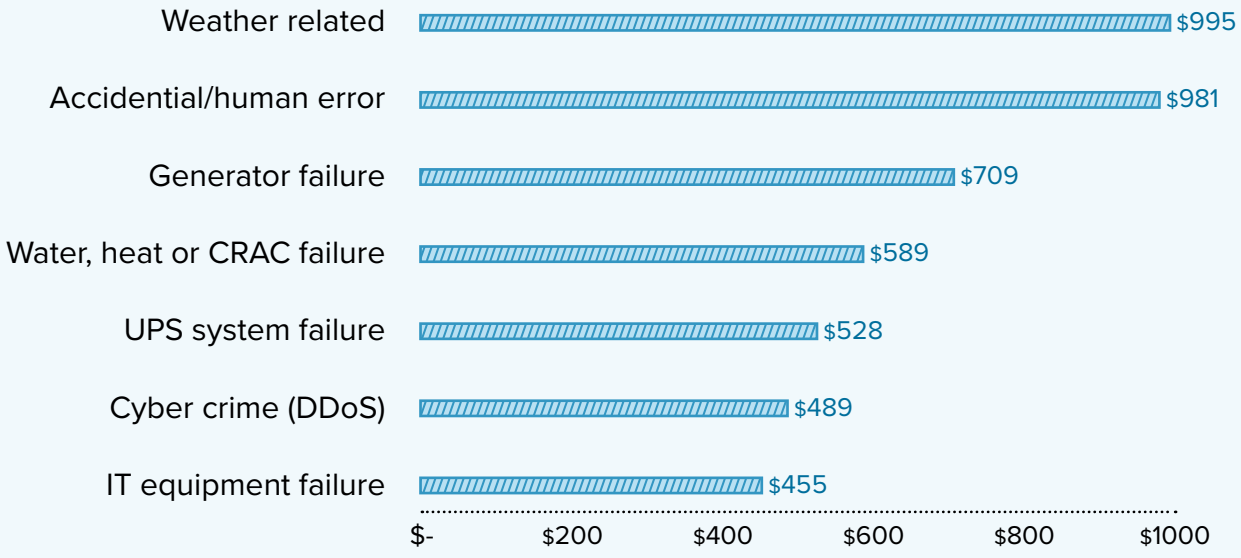
The Consequences of Downtime

In today's modern work environment, shareholders, customers and employees have come to expect constant connectivity, where downtime is not an option. An Active Directory failure could result in a myriad of undesirable consequences ranging in severity from a communications outage to a complete standstill of all business processes. Depending on the severity of the outage, AD-related downtime can lead to:

- **Damaged Brand Reputation:** It takes years to build a brand but only minutes to take it down. Any organization that cannot meet their service level agreements, or even perform basic business functions due to a service outage, is at risk of damaging their brand identity. Damage to your brand can have serious financial ramifications as exhibited in Verizon's acquisition of Yahoo. Once Verizon learned that Yahoo had suffered two massive data breaches, the two companies reconfirmed the terms of the sale and Yahoo's sale price was reduced by $350MM.

- **Lost Revenue:** Time equals money and, in the case of an AD failure, downtime equals lost money. Industry surveys show that companies experiencing downtime lose almost $9K per minute on average, or a total of $531K per hour . The average cost of a data center outage has increased 38% over the last three years to $740K[3].

Cost of Outage by Cause in USD (000)



[3] **Cost of Data Center Outages**, Ponemon Institute, January 2016.

Many businesses are aware of the consequences of an Active Directory disaster, but some still do not have a reliable Disaster Recovery plan in place. With the recent rash of cyberattacks, there's never been a better time to review and update your organization's Disaster Recovery plan.

Revisiting Existing Active Directory Recovery Solutions

The plan for recovering Active Directory after a technical, physical or cybersecurity event should be an ongoing part of an organization's overall business continuity planning, however some IT professionals rely on archaic Disaster Recovery methods. These methods include:

- **Redundancy:** While Active Directory features a strong redundancy capability, this capability does not provide adequate protection against malware attacks, database corruption and human error. Unfortunately, in these instances, the redundancy is working against you because it replicates the problem.

- **Recycle Bin:** The Recycle Bin feature in Active Directory allows users to restore deleted or lost items, but does not enable tracking or undoing any of the changes made to the system - changes that may result in severe impact to the business.

- **Home Grown Solutions:** IT professionals sometimes devise their own Disaster Recovery solutions. These solutions are error-prone and put your business at risk once the developer leaves the company.

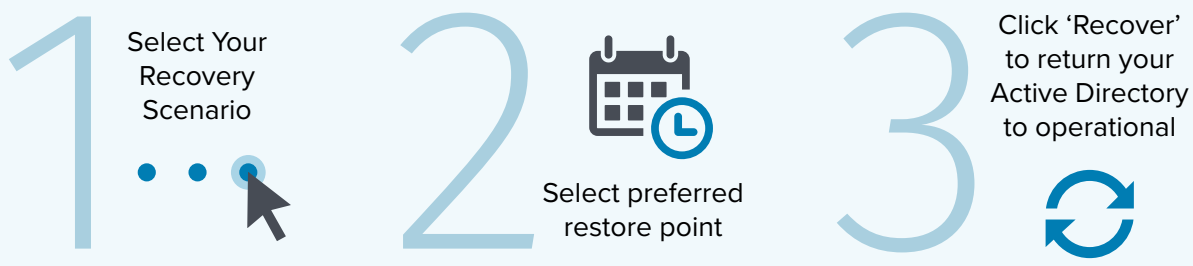
- **Microsoft White Paper for AD DR:** A 47-page detailed guide that is cumbersome, time- consuming and requires a great deal of manual work. Admins are required to study the workflows in the whitepaper and adapt them to the organization's needs, which means that recovery might take days or even weeks.

> 'No one ever wants to be in a position where they have to restore Active Directory, but nevertheless you should prepare for the possibility. Good planning and preparation helps to ensure that you will have a minimal number of surprises in the event of a disaster scenario that requires you to perform a restore.'
>
> Brian Desmond, Active Directory, 5th Edition

Developing Your End to End Disaster Recovery Plan

When faced with an Active Directory failure, it's essential to recover the application as soon as possible. Semperis provides the only 100% fully-automated Active Directory Disaster Recovery solution on the market, enabling you to minimize downtime during a disaster and restore business operations. The Semperis Active Directory Forest Recovery solution automatically backs up your AD environment and dramatically reduces the time to restore with an entire Forest recovery taking, on average, 30 minutes to complete. That's a savings of roughly $531K per hour of downtime, depending on the disaster scenario.

In the unfortunate event of an Active Directory outage, the Semperis solution enables you to get your business back up and running in three quick steps: simply select your scenario, determine the recovery point and restore services.



Granular Object\Attribute Tracking and Recovery

The Semperis solution includes the Active Directory State Manager which features a continuous tracking mechanism and publishes all AD events in real time, so you can pinpoint the exact timing of any potential failure and rollback changes to restore the last trusted backup. Through the State Manager dashboard, you can also gain insight into your organization's Active Directory activities down to the attribute level, compare previous states, revert back when necessary, and eliminate questions on who moved an object or deleted a user. The AD State Manager's real-time auditing capabilities, combined with the fully-automated AD Forest Recovery solution, provide your organization with a robust AD Disaster Recovery capability and allow you to quickly restore normal business operations when disaster strikes.

Conclusion

If designed and deployed correctly, Active Directory can be a stable system. However, the risk of failure is very real and results in downtime and lost revenue. Given the modern work environment, and the increasing dependence on an operating Active Directory, organizations have come to a point where AD downtime is not an option. While existing Active Directory recovery solutions are outdated, and do not address real-life threats to the AD environment, recent innovations in Active Directory management have automated the process in order to provide businesses with a thorough Disaster Recovery plan.

About Semperis

Semperis is an enterprise identity protection company that helps enterprises recover from cyber breaches and identity system failures, on-premises and on cloud. Semperis' leading technology enables organizations to ensure the secure operation of their directory services, allowing IT and Security teams to respond in cases of Active Directory disasters and cyber breaches. Founded in 2013 by experienced IAM professionals, Semperis serves customers in the financial, healthcare, government and other industries worldwide. Semperis' solutions are accredited by Microsoft and are included in the latest Gartner reports.

For more information, please visit www.semperis.com.