semperis

ACTIVE DIRECTORY FOREST RECOVERY

Cyber-first Disaster Recovery for Active Directory.

The requirements for Active Directory recovery have changed. When a ransomware or wiper attack takes out the domain controllers, traditional recovery processes can drag on for days or even weeks. Semperis orchestrates a fully automated forest recovery process—avoiding human errors, reducing downtime from days and weeks to minutes, and eliminating the risk of malware reinfection.

CYBER-FIRST DISASTER RECOVERY
Recover AD even if domain controllers are infected or wiped

ANYWHERE RECOVERY
Restore AD to alternate hardware (virtual or physical)

CLEAN RESTORE
Eliminate reinfection of malware from sytem state backups

ADVANCED AUTOMATION
Automate the entire recovery process and reduce downtime

Confronting the Unthinkable

AD is down: employees sit idle, operations grind to a halt, customers are stranded. The threat is real:

- Ransomware or a wiper attack takes out your domain controllers (DCs)
- A hacker gains access, and the extent of the damage is unknown
- A rogue administrator takes down the directory service
- A schema extension, forest-level upgrade, or other irreversible change renders the directory inoperable

Whatever the cause, you need to restore AD now. On the same or different servers. And without any remnant of the malware or bad actor that wreaked havoc on your network.

Recover (Don't Just Resume) Business Operations Post-Attack

After a cyberattack, businesses often scramble to resume operations. But without a complete, fully tested Active Directory recovery process, your systems will be vulnerable again to the same types of attacks that brought the organization to a standstill in the first place. Semperis ADFR ensures a full, fast, malware-free AD recovery.

Shorten recovery time of the entire Active Directory forest by 90%

In the good old days, Active Directory outages were limited to natural disasters or operational mistakes. Considering that cyberattacks inflict more damage and strike more frequently than natural disasters, it’s time to think “cyber-first.” Does your disaster recovery playbook address this reality? Semperis does.

With Semperis's patented technology, you can recover quickly and confidently from even the most catastrophic AD disaster.

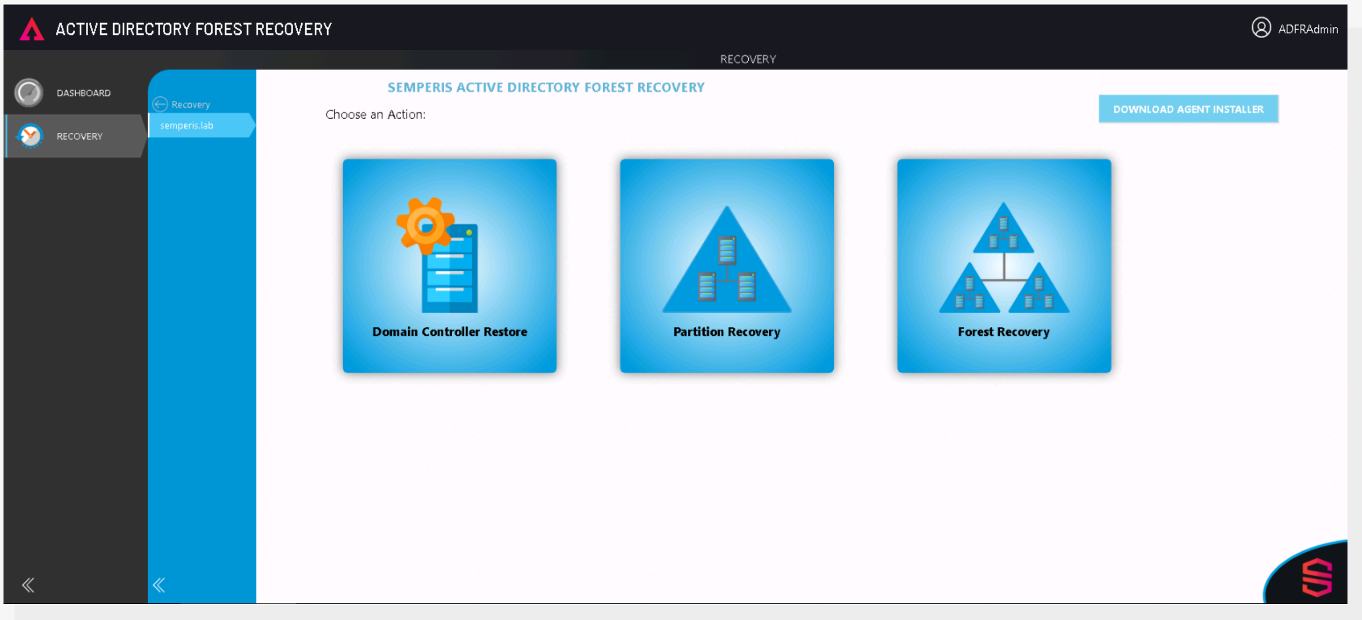

Figure 1.0 - ADFR Recovery Options

The Semperis Advantage

The idea of having to recover AD from scratch is no longer theoretical. It now must be a critical part of incident response planning. Forest recovery is no easy task, and the AD experts at Semperis have taken the challenge head-on. In doing so, Semperis ADFR offers functionality not available anywhere else.

GLOBAL 500 RETAILER

> “Semperis is exactly what I hoped for in an AD recovery tool. Over the years, I’ve had numerous concerns about forest recovery, and Semperis addresses them all.”
>
> **- InfoSec Identity and Directory Lead**

semperis

ANYWHERE RECOVERY

Restore AD to any hardware, virtual or physical – on premises or in the cloud.

CLEAN RESTORE

To prevent re-introduction of rootkits and other malware, ADFR starts with a clean Windows operating system and only restores what's needed for the server's role as a DC, DNS server, etc.

ADVANCED AUTOMATION

Automates the entire recovery process, including restoring DCs, rebuilding the Global Catalog, cleaning up metadata and the DNS namespace, restructuring the site topology, re-promoting DCs, and more.

ZERO MAINTENANCE

Eliminates the need to develop and maintain scripts or manually update configuration information – and the recovery failures that occur when these things don't get done.

BACKUP INTEGRITY

Checks each backup set to verify that it contains all the data necessary to successfully recover your forest, and that this data was successfully written to one or more locations. Also notifies you of any gaps in backup jobs.

SHARE NOTHING ARCHITECTURE

Runs independent of AD – with no reliance on Windows authentication, DNS, or other AD services – so you can recover immediately even if AD is completely down.

LIGHTWEIGHT AD BACKUPS

Backs up only the AD components. This results in smaller backups, which means less data to retrieve, process, and transfer – and less time to perform these operations during restore.

EASY DR TESTING

Spin up an exact replica of the production AD forest, using available servers, in an isolated lab to effortlessly test recovery procedures and document results for compliance with internal and external regulations.

MULTI-FOREST SUPPORT

Manage backup and recovery of multiple AD forests using a single management server and web portal, simplifying setup and ongoing administration.

POWERSHELL SUPPORT

Includes PowerShell commands for automating Semperis ADFR management, providing easier management of backup groups, backup rules, agents, and distribution points.

LAB SETUP

Semperis AD Forest Recovery also makes it easy to spin up a copy of production DCs in the lab, significantly reducing the time to maintain dev/test, staging, training, and support environments.

DISTRIBUTED BACKUP FAILOVER

Leverages distribution point servers to store backups close to domain controllers, reducing network traffic as well as backup and recovery times.

SECURE BACKUP ENCRYPTION

Generates a unique, one-time encryption key for each DC in a backup set—preventing an attacker from decrypting all backups using a single key. Also displays which backup rules have encryption enabled.

SAML AUTHENTICATION

Supports single sign-in (SSO) using SAML to minimize user login frequency—users can log in to the Administration portal using their chosen IdP credentials.

ADVANCED SEARCH

Simplifies operation log record retrieval with advanced search functionality that helps you filter by attributes such as components for a specified date range.

Active Directory is a prime target for cyberattacks. Ensure you can recover quickly and cleanly with Semperis.

Contact us today for a free trial.

semperis

GLOBAL 500 RETAILER

Everything starts with an ID and password. First thing you need to recover is credentials to do any other type of recovery.

- Kerry Kilker, Former CISO, Walmart

AIRLINES

“The Semperis platform helped El Al reach a point where we are sure that we can overcome any Active Directory outage.”

- Deputy Director of Infrastructure, El Al Airlines

Semperis

IT Resilience Orchestration

5 ★★★★★

Source: Gartner Peer Insights

info@semperis.com
www.semperis.com

Semperis Headquarters
221 River Street
9th Floor
Hoboken, NJ 07030
+1-703-918-4884

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing Active Directory, Semperis’ patented technology protects over 40 million identities from cyberattacks, data breaches, and operational errors. The world’s leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning **Hybrid Identity Protection** conference. The company has received the highest level of industry accolades; most recently being named Best Business Continuity / Disaster Recovery Solution by SC Magazine’s 2020 Trust Awards. Semperis is accredited by Microsoft and recognized by Gartner.

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell