semperis

Active Directory Disaster Recovery Planning and Exercise

Active Directory—the primary identity system for 90% of organizations worldwide—is the #1 target for cyberattackers. AD controls authentication and access to applications and services across the organization, so attackers know that if they can disable AD, they can bring the business to its knees.

Although many organizations have built an AD forest recovery plan, these plans have not been fully tested to account for the complexities of a real-life AD compromise, including the lack of a known good AD backup and failure to eradicate malware in the environment, leading to follow-on attacks. Semperis' 2024 Ransomware Risk Report found that 74% of ransomware victims were attacked multiple times—54% on the same day. Organizations that cannot quickly recover AD and resume normal business operations are more likely to pay ransom, yet 35% of those that paid ransom failed to receive decryption keys or were unable to recover their files and assets.

Reduce downtime risk with expert-guided AD disaster recovery planning

The Semperis Active Directory Disaster Recovery Planning and Exercise service helps ADFR customers ensure the ADFR deployment is optimized, aligns their recovery time objective (RTO) and recovery point objective (RPO) parameters, and identifies implicit dependencies that might hinder the plan execution during an incident.

This offering is available with the Semperis Active Directory Forest Recovery (ADFR) solution, with or without the Semperis professional services deployment bundle.

AD recovery plan review

The first step is analyzing your current recovery plan. Semperis AD recovery experts review your existing AD disaster recovery plan to understand the business goals, SLA, disaster scenarios, and methods currently in place to recover AD in the event of a disaster.

"You must make sure your critical infrastructures like Active Directory are completely secure and resilient. That was the main reason we acquired Semperis ADFR: We can guarantee that we recover Active Directory far faster than before."

José Alegria
former Chief Security Officer, Altice Portugal

Planning workshop

Next, Semperis experts work with you to ensure the ADFR deployment aligns with your AD recovery requirements. In the workshop, Semperis experts work with you to analyze your business goals in a disaster (such as recovery point and recovery time objectives), remote sites, number of users requiring initial access, and environment recovery priority in case of a multi-forest disaster. The workshop also aims to thoroughly map the dependencies for the recovery process.

The Semperis team will help you plan different cyber and operational disaster scenarios as part of the workshop, including reviewing offline storage/offsite backups, recovering backups online when required, and similar recovery activities.

The workshop deliverable is a documented AD recovery plan that leverages ADFR and is ready to present to business owners. The plan includes defining the recovery SLA, identifying the mean time to recovery (MTTR), and mapping business applications required to support the core business goals, which informs the AD recovery plan and estimated recovery time.

AD disaster recovery exercise

We recommend conducting a full test of your AD disaster recovery plan at least annually or when a major change occurs. The Active Directory Disaster Recovery Exercise includes a simulated encryption of the entire organization and the process of recovering and regaining control over AD. During this exercise, Semperis experts recover your production backups into an isolated lab environment.

At the end of the exercise, the Semperis team provides a report that describes the test results and documents issues, then revises the DR plan accordingly. You can use this report to help meet governance and compliance requirements.

Key outcomes of AD Disaster Recovery Planning and Exercise

- Expose gaps in roles, responsibilities, and decision-making
- Validate (or rethink) your recovery playbook
- Improve cross-team coordination
- Build confidence at the executive level
- Pressure-test real-world readiness, resilience, and recovery

Unmatched global identity forensics and incident recovery experience

To learn more about the Semperis Entra ID Security Assessment, visit **Semperis.com/solutions/identity-forensics-incident-response**

90+ years' identity-related incident response experience

25+ former Microsoft Premier Field Engineer (PFEs) on staff

170+ combined years of Microsoft MVP experience

30+ years' data analysis for insider threat & risk monitoring

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

Gartner Peer Insights. Customer First

Semperis
IT Resilience Orchestration
5.0
Source: Gartner Peer Insights

Leader SPRING 2024

Semperis
Directory Services Protector
4.7
Source: G2.com

Semperis Headquarters
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030