KuppingerCole Report

EXECUTIVE VIEW

by Dan Blum | August 2018

Semperis Directory Services Protector for Active Directory

Active Directory provides critical identify infrastructure for the enterprise. Semperis offers Active Directory change monitoring and forest recovery products. The Semperis DS-Protector product support change monitoring and rollback for a broad set of AD infrastructure objects.

by **Dan Blum**
db@kuppingercole.com
August 2018

Content

Related Research

Executive View: Microsoft Azure Active Directory - 71550

Executive View: Microsoft ADFS: Active Directory Federation Services - 71126

Product Report: Microsoft FIM 2010 R2 - 70106

1 Introduction

Active Directory is the core IT identity infrastructure system for almost all large global organizations, including those that deploy both Windows and Unix servers. Even organizations using identity-as-a-service (IDaaS) solutions (e.g., Okta, OneLogin, Microsoft's Azure Active Directory) still depend on the ability to populate cloud-based directory accounts and/or to authenticate users from a premise-based AD installation. Should AD be compromised or corrupted, the whole enterprise hybrid cloud is in trouble.

Success attracts cyberattackers like flies to honey. Typically, attackers compromise a single computer or obtain the domain credentials of a single user. From this beachhead, they identify targets via directory reconnaissance. Subsequently, an attacker might obtain the keys to the kingdom by compromising a Domain Administrator's account. Increasingly, automated ransomware programs (such as Samas) are also using AD queries to enumerate computers or accounts, and then spread to those distant systems. Ransomware may also strike domain controllers directly, bringing the network to its knees.

For all these reasons, organizations must enhance AD security, discover breaches faster, and get AD environments back to normal quickly after a breach is detected. With eighteen years in production, many changes, multiple versions, and various production use cases AD implementations tend to be highly complex. Recovery is easier said than done. AD forests are susceptible to human error, hardware failure, and software corruption. According to the Semperis White Paper "Averting Disaster: Preparing Your Organization for an Active Directory Failure," 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) system data
- A single, critical DC failure
- Accidental deletion of Group Policies
- Incorrect modifications of critical applications' accounts and groups

Microsoft does not provide a built-in forest recovery process. Only a lengthy Active Directory Forest Recovery Guide[i] is available, and many of the procedures it recommends are manual in nature. Recovery could take days, even if complete and current backups are available.

To fill the gap, Semperis provides three main capabilities, all focused on Active Directory security:

- Full AD forest recovery
- State management
- Real time activity dashboard

Active Directory Forest Recovery constitutes Semperis' original, and best known, product. It provides an advanced solution for AD Disaster Recovery (DR). It takes regular backups of all domain controllers and preserves all AD attributes, objects, relationships, and other domain structures. The backups are kept on-premise, or in cloud storage enabling full or partial forest recovery scenarios. Semperis provides more information on the AD Forest Recovery solution on its website.[ii]

Semperis also offers AD State Management and a Real Time Activity Dashboard via its DS Protector for Active Directory product. As described in the Service Description below, DS Protector provides more granular solutions to AD infrastructure security issues.

2 Service Description

The Semperis DS Protector for Active Directory (DSP) version 2.5 enables customers to track AD modifications, present them on a dashboard, and roll them back upon command. DSP 2.5 was released in late 2017, and was formerly known as Active Directory State Manager. The product's scope covers all objects in AD, including Domain Name System (DNS) integrated zones data and Group Policy Objects (GPOs).

DSP consolidates logs from disparate AD domain controllers combined with data gathered directly from the AD through replication API's and provides a timeline graphical view of changes that operators can sort or filter. Operators can also roll back individual changes, or roll back groups of changes.

DSP Components

DSP is a premise-based solution consisting of management server, database, and collection agent components.

- **DSP Management Server:** The DSP Management Server provides the GUI for DSP administrators. Capabilities include a real-time dashboard to track changes, change frequency, and the ability to provide filtered views of changes and initiate roll backs. Separate screens are used for change monitoring and recovery of the configuration partition, DNS and GPOs.
- **DSP Database:** The DSP database uses the Microsoft SQL Server, which can be co-located with the DSP Management Server or on a separate server. The database holds DSP configuration settings as well as all change records collected from the AD, enriched with audit data from the domain controller logs. DSP administrators can set the data retention period (weeks, months) for domain change audit information.
- **DSP Agents:** DSP utilizes two types of agents: The core DSP agent installed on two domain controllers per domain, used to initiate local change monitoring and roll back operations; and an Audit Agent that correlate change events with log records and enriches the events.

DSP Functionality

Semperis DSP enables the following functionality:

- Review and revert changes to Active Directory
- Review and revert DNS changes
- Review and revert GPO changes
- Review and revert configuration partition changes
- Role-based access control (RBAC) DSP administration model
- Reporting
- Alerts and notifications
- Security infrastructure integration

Common use cases for strong AD change monitoring and control are to:

- Maintain a small number of domain administrators, and tight control over adding new ones
- Maintain tight control over adding or modifying AD inter-domain trust objects
- Prevent bad practices such as the addition of a nested group as a member of a privileged AD infrastructure group
- Prevent changes to sensitive AD objects (such as the domain controllers organizational unit, or a GPO) or changes to the permissions on those objects in the directory

Review changes to Active Directory

Semperis DSP enables administrators to view changes occurring to AD in real time as well as recent changes and logged changes. These changes can include attribute modifications, object creation or deletion, group membership addition/deletion, changes to GPOs, and changes to DNS. Administrators can zoom in and view individual changes and also search the database for changes by a particular initiator, of a certain type, or with other criteria. Administrators can review or search data from the entire forest or from a single domain.

Administrators can roll back changes to the most recent data, or even to an earlier change. Certain operations, such as new object creation, are not allowed to be reverted through DSP (which by design doesn't delete data from AD) but must be undone through another means. DSP also enables administrators to revert multiple changes at the same time.

Often, enterprises will establish policies and change control procedures to support the use cases noted above. However, AD itself cannot prevent a domain administrator (DA), a privileged user, or a hacker who has obtained the right domain credentials from violating those policies and procedures. DSP enables customers to monitor for events such as unauthorized DA creation, unauthorized trust creation, or a privilege modification on a sensitive object and then revert such changes if appropriate. For

example, an organization might have 10 DAs, of whom only one is allowed to add new DAs to the directory. Even in a large forest with many domains and DAs, using DSP it is relatively easy to flag additions of new DAs by unauthorized persons.

Review and Restore DNS and GPO changes

DSP constantly tracks changes and deletions made in the Active Directory integrated DNS zones. The DSP DNS screen provides an interface to search for, view, and roll back or revert granular changes. It's also possible to view, search in, and restore entire DNS zones that have been deleted.

DSP also tracks the changes and deletions to GPO objects in Active Directory. The DSP GPO screen provides an interface to search for, view, compare, or restore entire GPO objects. Administrators can also back up existing, known good GPOs.

Role-based Access Control (RBAC) Administration Model

DSP provides an RBAC manager screen to control administrative permissions to objects and operations in the DSP management system and agents. Semperis' RBAC model incorporates four components:

- Scope Sets define groups of directory containers, DNS zones, object classes, and domains to which administrative privileges can be applied.
- Permissions define what DSP actions can be performed across a scope set.
- Personas define collections of permissions.
- Delegations map AD groups, or users, to one or more DSP personas and can be customized by restricting privileges within the underlying scope sets a persona points to.

Reports, Alerts, and Notifications

DSP provides pre-defined reports to list inactive user accounts, locked out user accounts, and a number of other user- or security configuration-related AD items. For example, one report lists all the users in the current domain who are members of the Domain Admins, Admins, Enterprise Admins, and Group Policy Create Owner groups. Reports are generated on an ad-hoc, daily or weekly basis. Administrators can also cause a report to be automatically generated.

These reports can be used to validate that policies – such as some of those discussed in the change monitoring and control use cases – haven't been violated. They can also help administrators clean up inactive accounts, another contributor to domain risk.

DSP can be configured to send alerts concerning DSP infrastructure-related events (e.g., installing/uninstalling an agent, or generating a report) to designated email addresses. With the new DSP version 2.6 (due out for general availability in the Q3 2018), the program will also be configurable to generate alerts based on the occurrence of specific change events. For example, customers could request alerts be generated in the event of a change to AD infrastructure objects – such as the OU=Domain Controllers, GPOs, or the AdminSDHolder objects – to get an early, automated warning of unauthorized actions such as the policy violations discussed earlier. No longer will the enterprise depend entirely on careful dashboard monitoring, or log review by an operator to ensure policy violations get flagged.

DSP 2.6 will also be enhanced to transfer DSP's enriched AD log information to security information and event management (SIEM) systems using Syslog messages. In addition, Powershell scripting capabilities will be added, enabling DSP integration with IT service management ticketing systems.

3 Strengths and Challenges

The market for third-party Active Directory administration and protection tools comprises a number of vendors, including AD audit, AD change monitoring, and AD recovery. Semperis' original product - Semperis Active Directory Forest Recovery is virtually alone in the recovery category. Semperis DS Protector is a newer product for Semperis in the change monitoring space. DSP provides some AD audit capabilities as well.

As noted in the list of Strengths from the table below, DSP provides strong AD change notification support. Per the strengths marked with an asterisk, additional functionality will be added in a new DSP Release 2.6. Semperis' challenges are to continue improving the AD change notification and audit functionality, enabling the company to become more of a potential "one stop shop." Additionally, most enterprise customers now have a hybrid AD / Azure AD environment and some of the same issues Semperis addresses in AD exist for customers in Azure AD.

In addition to the changes planned for DSP 2.6, Semperis plans a "DSP 3.0" release for 2019. This release will provide the ability for customers to address some of these challenges. Automated rollback of unauthorized changes to AD is important because it could drastically reduce the time hackers or insider threats have to abuse illicitly-gained privileges.

Strengths	Challenges
• Strong AD change auditing and rollback capability • Coverage of AD DNS changes • Coverage of AD GPO changes • Alerts on administrator selected change events* • Syslog integration with SIEM solutions*	• No automated tools or actions available in DSP 2.5 or 2.6 to handle (potentially) large numbers of alerts • Does not yet support Azure AD change notification, roll back, or alerts

*****To be added in DSP Release 2.6, expected general availability of Q3 2018.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

[i] Active Directory Forest Recovery Guide, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786327(v=ws.10)

[ii] Active Directory Forest Recovery product description, https://www.semperis.com/products/#ADFR

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com