

Become Resilient – Repelling Directory Attacks

Introduction

Welcome to the “Repelling Directory Attacks” section of the workshop, in which you will experience firsthand an attack against Active Directory and recover from it using Sempris ADFR and run a security assessment using Sempris Purple Knight.

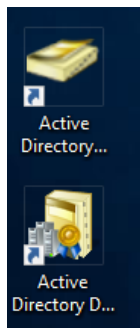
You will gain access to a cloud-hosted lab via RDP and operate from there.

Getting to Know the Lab

Establish an RDP session using the .rdp file provided.

If prompted for credentials, enter the username “SEMPERIS\Administrator” and the password “Ap9^Nh1*rM@3”.

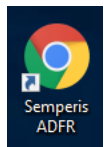
Once the RDP session is established, you can launch Active Directory Domains and Trusts and Active Directory Users and Computers to get familiarized with the environment. For your convenience, shortcuts were placed on the Desktop.



Prepare for a Catastrophe

It is crucial to make sure you have a recent backup before an incident. A scheduled backup should have been taken recently. Visit the Sempris ADFR Administration interface to confirm.

Log into ADFR Administration using the shortcut placed on the Desktop.




Enter “.\Administrator” as username and “Ap9^Nh1*rM@3” as password, and then click SIGN IN on the login page.


Sign in


Administration Recovery

Domain \ Username

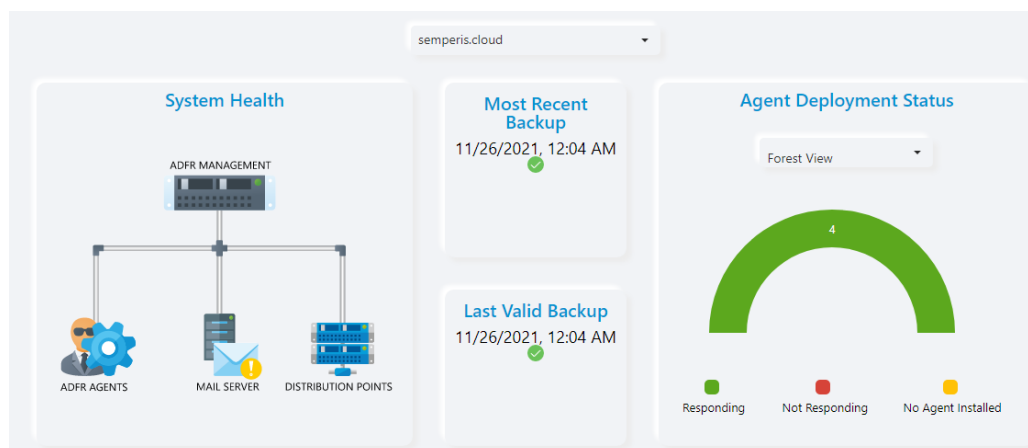
 .\Administrator

Password



 **SIGN IN**

Review the dashboard to ensure you have a valid recent backup,



Feel free to explore ADR and get familiar with it.

Launch a Security Assessment

The Mighty Penguin APT group will attack the environment soon, and you must launch a Purple Knight scan promptly and try to close exposures they might abuse to compromise AD.

Purple Knight is a powerful AD security audit tool that can detect a wide range of Indicators of Exposure/Compromise (IOE/IOC). You will be using the community version, which is free of charge, and you are welcome to download it at home/work.

For your convenience, a shortcut to Purple Knight was placed on the Desktop of your RDP session.





Once Purple Knight finished loading, tick the checkbox next to “I accept the terms in the license agreement” and click Next.

Click SELECT next to “semperis.cloud” to scan the entire forest, and then click Next.

Select forest and domains to assess:

BEST PRACTICE For an accurate assessment, the tool should be run on all domains in the selected forest

 semperis.cloud  **SELECT**

☒ Search...

☒ ▶ semperis.cloud (1)

By default, all the tests are pre-selected except for the “ZeroLogon” test. The ZeroLogon test takes a bit longer to complete, and the domain controllers in the lab are not vulnerable to this attack, so it can be left unchecked.

Click RUN TESTS to initiate a scan.

☒ Search...

<input checked="" type="checkbox"/> ▶ AD Delegation (12)	AD Delegation
<input checked="" type="checkbox"/> ▶ Account Security (23)	Description
<input checked="" type="checkbox"/> ▶ AD Infrastructure Security (24)	AD delegation is a critical part of security and compliance. By delegating control over Active Directory, you can grant users or groups permissions without adding users to privileged groups.
<input checked="" type="checkbox"/> ▶ Group Policy Security (5)	Weight
<input checked="" type="checkbox"/> ▶ Kerberos Security (11)	3

[Check for updates](#) [More information](#)

Available: 75 Selected: 74 **BACK** **RUN TESTS**

The scan should last under a minute, and then you will be presented with a Report Summary. Click VIEW FULL REPORT to dive into the details. The full report will be displayed in a web browser.

Review the scan results and determine whether AD has already been compromised and what can be done to prevent or contain it.

You're Under Attack!

If you were not quick enough to address the exposures, The Mighty Penguin must have escalated their privileges and encrypted AD. In such a case, you would see the following message on the screen:



You may try to launch Active Directory Domains or Trusts or Active Directory Users and Computers to confirm that the Directory Services are down.

Initiate Recovery

Semperis ADFR allows recovering Active Directory forests to the same hosts as the existing domain controllers or new hosts. Following a breach, if the domain controllers were compromised, it is recommended to recover to new hosts to ensure no malware is carried over.


Log into ADFR Recovery using the shortcut placed on the Desktop. If you are already logged into ADFR Administration, you will have to log out first.

In the login page, select Recovery, enter "Administrator" to the Username field and the password "Ap9^Nh1*rM@3". Select "ADFR-MS" as the domain and click SIGN IN.


Sign in

Administration Recovery


Domain

 ADFR-MS


Username

 Administrator

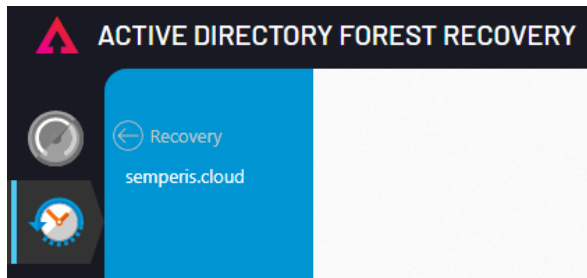
Password



[Reset password](#)

 SIGN IN

Click the Recovery icon on the menu on the left, and select “semperis.cloud”.



Click the Forest Recovery Tile.



Select the most recent backup set and enter a redirected IP address for the primary domain controller in the parent and child domains. You can use the IP addresses 10.192.0.135 and 10.192.0.198 as shown in the screenshot below.

Click Analyze to continue.

HOSTNAME ↑	AD SITE	OS	TYPE	ORIGINAL IP	REDIRECTED IP	AGENT STATUS	RESTORE FROM BACKUP
🔍	🔍	🔍	🔍	🔍	🔍	(All) ▼	(All) ▼
▼ Domain: child.semperis.cloud							
ADFR-CHILD-D...	us-east-1	Windows Server 2019 Datac...	GC (FULL)	10.192.0.1...	10.192.0.135	✓	✓
ADFR-CHILD-D...	us-east-1	Windows Server 2019 Datac...	GC (FULL)	10.192.0.1...		✓	✓
▼ Domain: semperis.cloud							
ADFR-DC1	us-east-1	Windows Server 2019 Datac...	GC (FULL)	10.192.0.1...	10.192.0.198	✓	✓
ADFR-DC2	us-east-1	Windows Server 2019 Datac...	GC (FULL)	10.192.0.1...		✓	✓

BACK
ANALYZE

Click RECOVER and then START RESTORE to commence the recovery process.

FOREST RECOVERY

STEP 1: SETUP AND CONFIRMATION **STEP 2: RESTORING FOREST**

Restoring the Forest to **RETRIEVE RECOVERY CREDENTIALS**

✓ Recovery Topology Analysis **EXPAND**


✓ Restore from Backups **EXPAND**

✓ Post Restore Tasks **EXPAND**

✓ Reinstatement of Forest Functionality **EXPAND**

✓ Generation of IFM **EXPAND**

✓ Repromotion of Domain Controllers **EXPAND**

☒ Show progress log [*all times are displayed in UTC] 

--- The Recovery operation completed successfully. ---
[29-11-2021 20:46:31.350] [Information] [child.semperis.cloud] Substep 'Recreation of Global Catalog' Completed
[29-11-2021 20:46:31.350] [Information] [child.semperis.cloud] Rebuild of the Global Catalog completed successfully
[29-11-2021 20:46:31.350] [Information] [child.semperis.cloud] Step 'Reconnect Domain To Forest' Completed
[29-11-2021 20:46:31.350] [Information] [child.semperis.cloud] Reconnection of the domain to the forest completed
[29-11-2021 20:46:31.350] [Information] [semperis.cloud] RebuildGlobalCatalogs for Domain child.semperis.cloud completed. Result: Success

ABORT **CONFIRM**

The process should take approximately ten minutes. During that time, you should review the Purple Knight report to understand what The Mighty Penguin changed in the environment to install “domain persistence” and what you have to do to eradicate that.

Eradicate the Threat

When the recovery process is finished, you may use Active Directory Users and Computers to see that the Directory Services are once again operational, and, time permitting, you may work through the Purple Knight report to remove any domain persistence that The Mighty Penguin has installed or any exposures that The Mighty Penguin might have exploited to compromise the forest.

Semperis, Inc.

info@semperis.com