

Become Resilient – Recovering from Active Directory Attacks

Reduce AD recovery time after a cyberattack by at least 90% with comprehensive, automated cyber-first DR

Introduction

Welcome to the “Recovering from AD Attacks” section of the workshop, in which you will run a security assessment using Semperis Purple Knight to see some of the vulnerable paths in AD, and then you will simulate catastrophic data loss and denial of service in Active Directory and quickly recover from it using Semperis Active Directory Forest Recovery (ADFR).

You will have access to a cloud-hosted lab via web portal for this lab work.

Getting to Know the Lab

CloudShare is a hosting environment where we create labs for testing and evaluating products. For this session, you will have a fresh AD lab for the Purple Knight and ADFR

The lab servers will auto-login with predefined credentials.

You will be able to select previously saved credentials to log onto the ADFR portal.

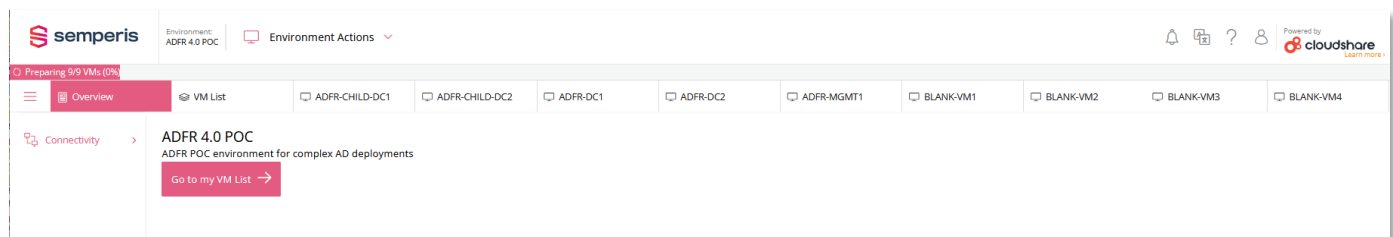
The CloudShare lab for ADFR has a single AD forest with two domains, a root domain and a child domain. Each domain has two domain controllers. The lab also includes additional “blank VMs” which will be briefly discussed in the workshop: these are for scenarios where you would recover to alternate VMs from the original DCs.

Important CloudShare notes:

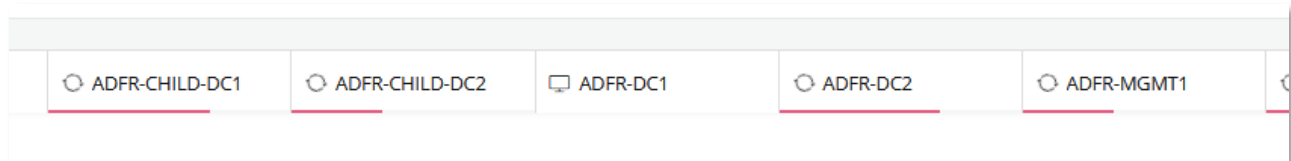
- CloudShare auto-suspends after a period of around 90 minutes of inactivity. This saves costs for allocated resources.
- CloudShare will auto-restart servers that are powered off. This is important to consider when testing the scenarios where ADFR is restoring original DCs to one or more blank VMs. Rather than powering down the original DCs, it would be better to disconnect the network adapter or change the IP address. CloudShare also can connect to the console (CON) rather than use RDP so you can still get to a VM even if you have disconnected/disabled the virtual network adapter.
- You should not test the scenarios for restoring to alternate hardware until we have gone through the scenarios in the workshop.
- CloudShare includes an option to revert all VMs (or individual VMs) to their original state. The only snapshot is the original, so if you revert, all of your changes will be lost. Reverting the entire environment is sometimes useful after you have tested the scenario of restoring all original DCs to the blank VMs.

When logging onto the CloudShare web portal, you will have a view of all VMs, plus some configuration options.

Upon logon, the VMs will all be started automatically, restoring from being suspended automatically.









It takes a few minutes for all VMs to start up, and you should allow a few minutes for the environment to stabilize after being resumed.



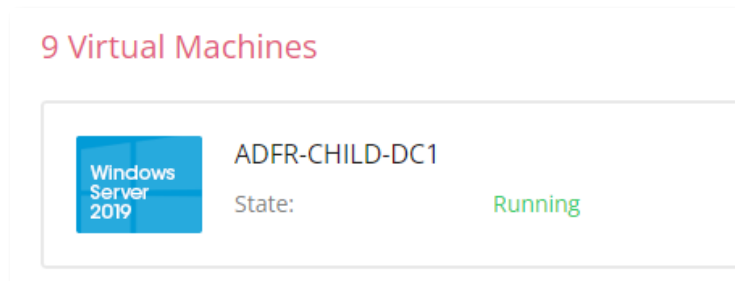
You can also click on the “**VM List**” button to view the percentage status for each VM.

9 Virtual Machines

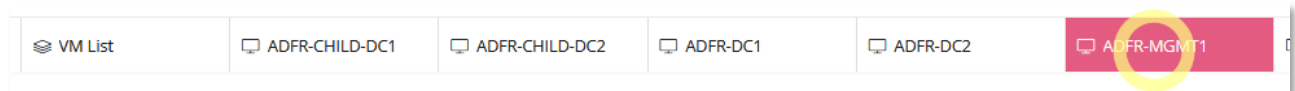
	ADFR-CHILD-DC1 State: Running	 ...
	ADFR-CHILD-DC2 State: Preparing 37 %	 ...
	ADFR-DC1 State: Running	 ...

IMPORTANT NOTE: Generally, you should allow the environment about 5 minutes to stabilize after the initial startup from suspension. This gives the DCs and ADFR server time to settle before testing.

Wait for all VMs to show green “Running” status, like this example:

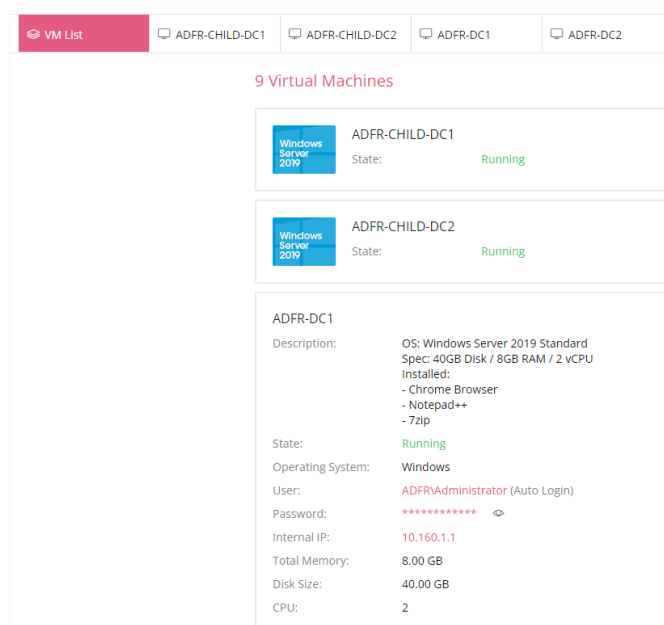


When all VMs are ready and stable, you can click into any VM by selecting the desired tab/button at the top:



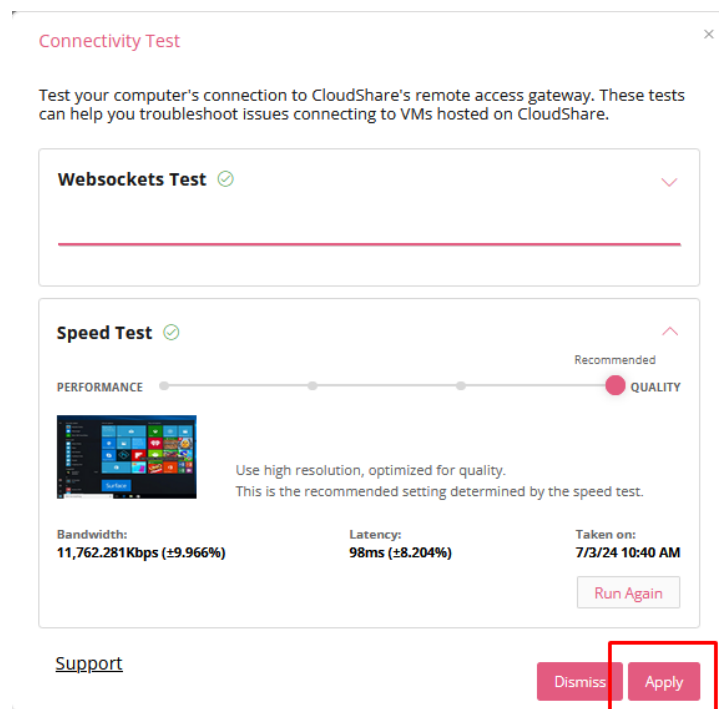
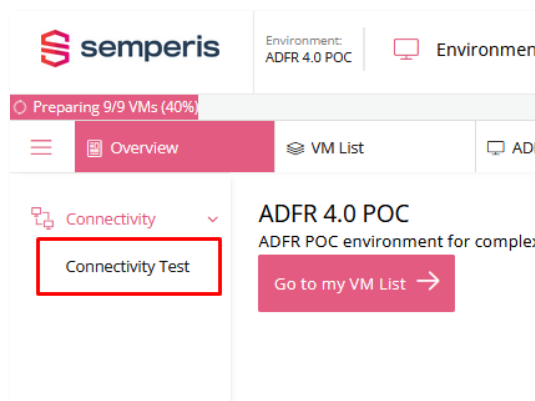
Click any tab, and the VM will auto-login with stored credentials.

VM credentials can also be found on the “**VM List**” tab:



Getting to Know the Lab: Handling Connectivity Issues

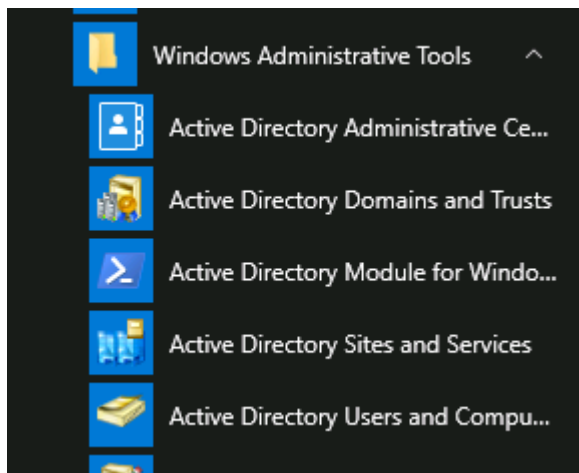
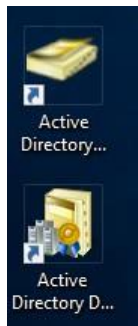
If you have connectivity issues, you can try using the “**Connectivity**” link on the left to perform a connectivity test:



When the test has completed, make sure to click the “Apply” button. That usually corrects connectivity-related issues.

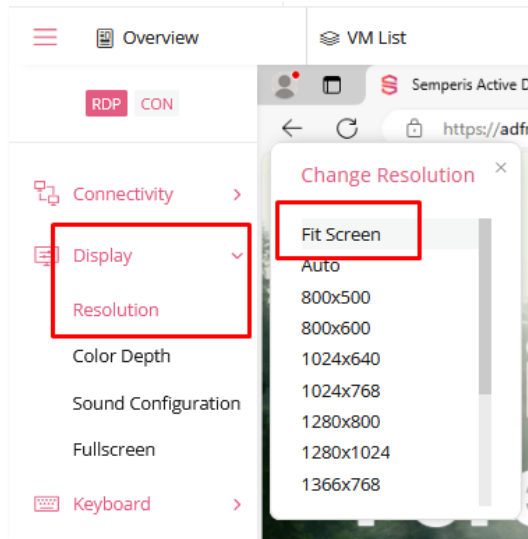
Select the “ADFR-DC1” VM tab to log onto the server.

Once the RDP session is established to the server, you can launch tools such as Active Directory Users and Computers and Active Directory Sites and Services to get familiarized with the environment.

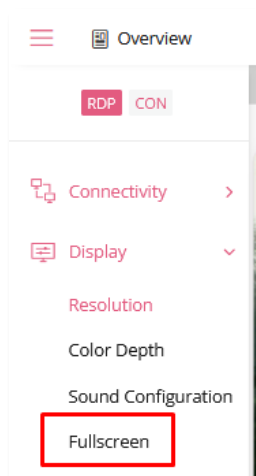


Getting to Know the Lab: Virtual Screen Resolution

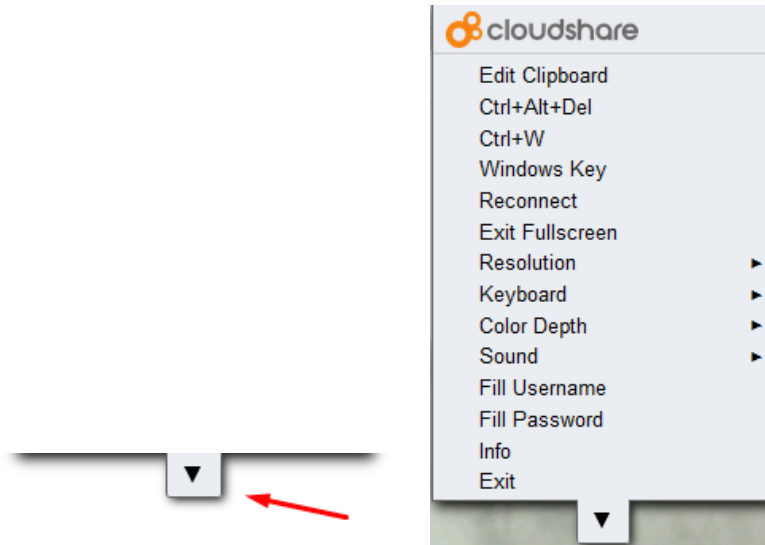
CloudShare is versatile with screen resolution. If you find the browser window is beyond your screen border, you can scroll to the side or you can try adjusting the display resolution in the portal. We find that “Fit Screen” works for most all situations.



If you are working on a smaller screen, you can use the “Fullscreen” option to view more of the VM display.



You can easily exit out of full screen mode at any time with the “ESC” key or the hidden CloudShare menu at the top of your screen:

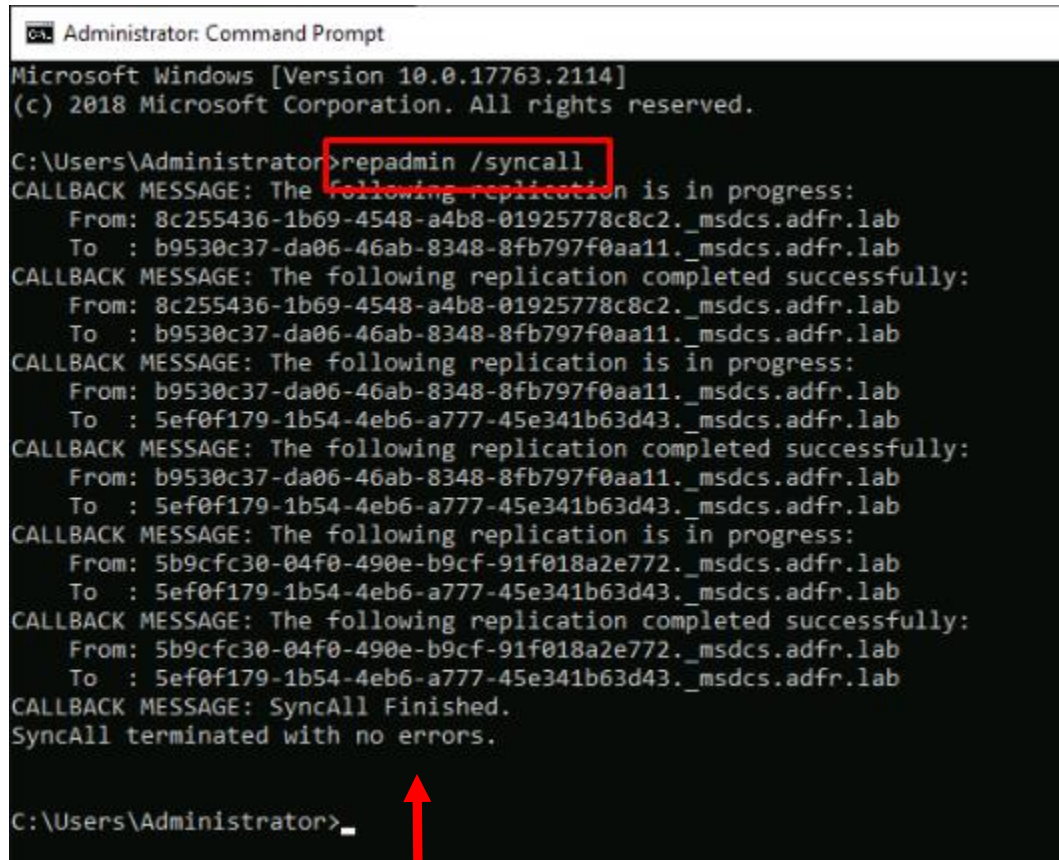


If you are working on a smaller screen, you can use the “Fullscreen” option to view more of the VM display.

Checking the Domain Controllers

Before running through the test scenarios, it is a good idea to perform at least a basic check of Active Directory before starting.

Logon onto one of the root domain controllers, such as ADFR-DC1 and open a command prompt (as Administrator) to run “repadmin /syncall” to make sure replication looks good.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>repadmin /syncall
CALLBACK MESSAGE: The following replication is in progress:
  From: 8c255436-1b69-4548-a4b8-01925778c8c2._msdcs.adfr.lab
  To : b9530c37-da06-46ab-8348-8fb797f0aa11._msdcs.adfr.lab
CALLBACK MESSAGE: The following replication completed successfully:
  From: 8c255436-1b69-4548-a4b8-01925778c8c2._msdcs.adfr.lab
  To : b9530c37-da06-46ab-8348-8fb797f0aa11._msdcs.adfr.lab
CALLBACK MESSAGE: The following replication is in progress:
  From: b9530c37-da06-46ab-8348-8fb797f0aa11._msdcs.adfr.lab
  To : 5ef0f179-1b54-4eb6-a777-45e341b63d43._msdcs.adfr.lab
CALLBACK MESSAGE: The following replication completed successfully:
  From: b9530c37-da06-46ab-8348-8fb797f0aa11._msdcs.adfr.lab
  To : 5ef0f179-1b54-4eb6-a777-45e341b63d43._msdcs.adfr.lab
CALLBACK MESSAGE: The following replication is in progress:
  From: 5b9cfc30-04f0-490e-b9cf-91f018a2e772._msdcs.adfr.lab
  To : 5ef0f179-1b54-4eb6-a777-45e341b63d43._msdcs.adfr.lab
CALLBACK MESSAGE: The following replication completed successfully:
  From: 5b9cfc30-04f0-490e-b9cf-91f018a2e772._msdcs.adfr.lab
  To : 5ef0f179-1b54-4eb6-a777-45e341b63d43._msdcs.adfr.lab
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

C:\Users\Administrator>
```


Prepare for a Catastrophe

For reference and comparison, it is recommended to review the **Microsoft Active Directory Forest Recovery Guide** to see the official Microsoft process and recommendations for a full-forest AD recovery, noting that it is a high-level guide and not a recovery plan. Semperis Active Directory Forest Recovery (ADFR) was built based on this guide and fully automates and orchestrates the steps to fully recover AD in YOUR environment!

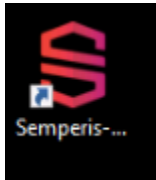
Reference link (or web search “Microsoft Active Directory Forest Recovery Guide”):
<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-guide>

It is crucial to make sure you have a recent backup before an incident. In a normal environment, a scheduled backup should have been taken recently automatically. In the CloudShare labs, the environment will likely have been suspended for the scheduled running of the backup job(s).

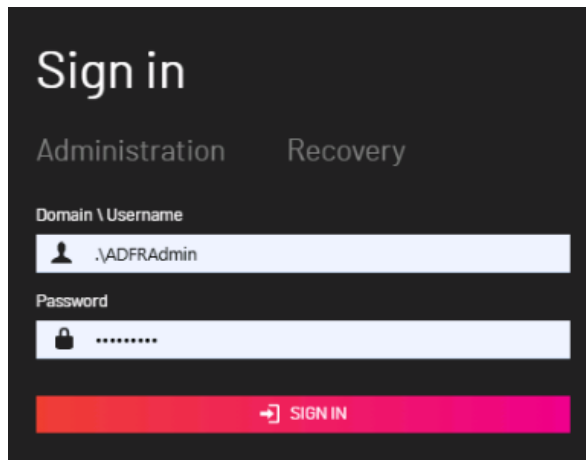
To run a manual backup in the ADFR console, go to the Semperis ADFR Administration interface on the ADFR Management server (ADFR-MGMT1).

Log on to Semperis Active Directory Forest Recovery (ADFR) Console

Log into Semperis ADFR Management console using the shortcut placed on the Desktop (or open the MS Edge browser).

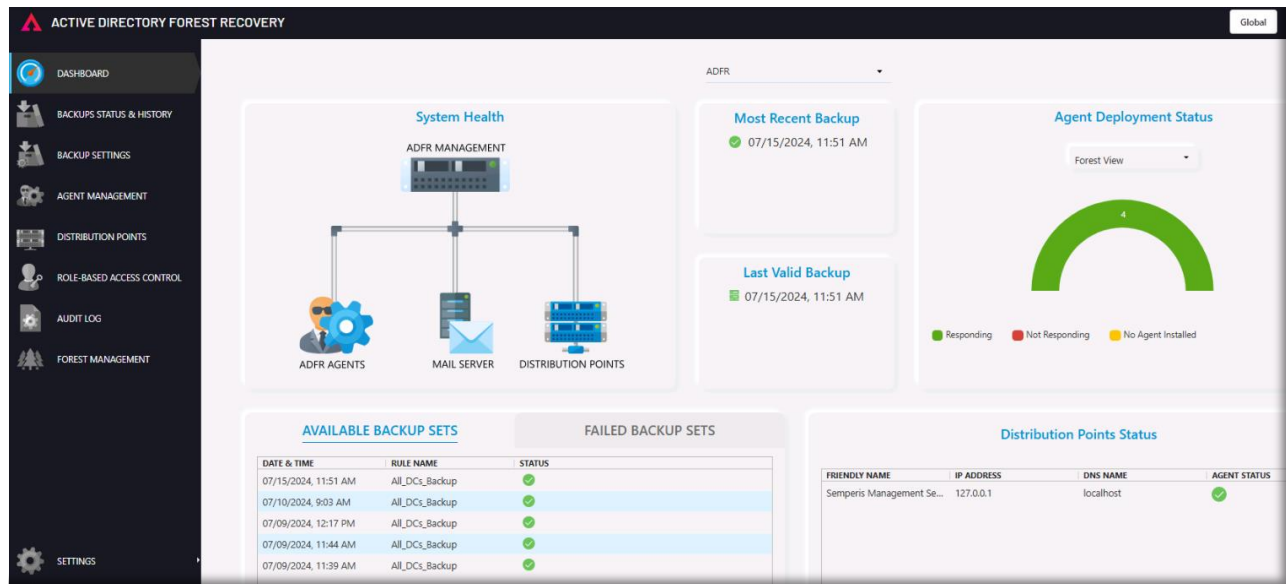


Click on the “**Domain \ Username**” field and select the previously saved “**.ADFRAdmin**” credential, then click **SIGN IN** on the login page. (The credential “**ADFR\Administrator**” also works, which is the initial account used, but we want to demonstrate alternate credentials and role-based access.)

A screenshot of the Semperis ADFR Management console sign-in page. The page has a dark background. At the top, it says 'Sign in'. Below that, there are two tabs: 'Administration' and 'Recovery'. Under 'Administration', there is a 'Domain \ Username' field with a dropdown menu showing '.ADFRAdmin'. Below that is a 'Password' field with a lock icon and a masked password '*****'. At the bottom, there is a red button with a white arrow and the text 'SIGN IN'.

After the logon is completed, the main ADFR dashboard will be displayed.

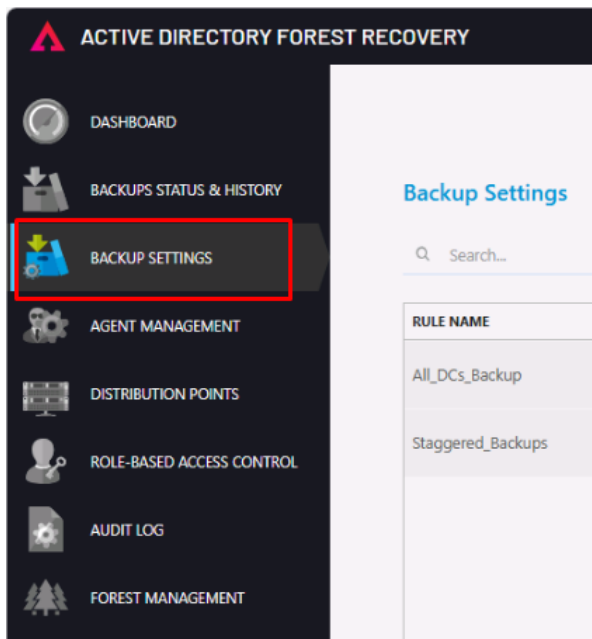
You can review the dashboard to view ADFR management status, agent status and recent backup jobs:



Feel free to explore ADFR and get familiar with it, as well as run an additional backup.

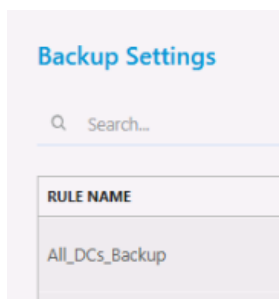
Let's manually run a backup process. There is a backup rule for you to run at any time under **"Backup Settings"**:

Navigate to the **"Backup Settings"** menu option in the left-hand pane.



Under “**Backup Settings**”, you will see one or more backup rules configured in this lab.

We will use the “**All_DCs_Backup**” rule.



On the rightmost side (you may need to scroll due to screen resolution), click the black arrowhead to initiate a backup.

RULE NAME	↑	REPEAT ON	RETENTION	ENABLED	ENCRYPTION	VALID FOR FOREST RECOVERY	STATUS	NEXT BACKUP START TIME (UTC-07:00)	ACTION
All_DCs_Backup		Thu	20 backups	ⓧ Disabled	🔒 Encrypted	✅ Valid	Not running	07/18/2024, 11:00 PM	▶ ⋮

Run Now

All_DCs_Backup

Run groups according to the offsets in the rule or you can configure the run times for each group in the rule down below.

Search...

GROUP NAME	PRIMARY DP	BACKUP START TIME	SECONDARY DP'S
All_DCs	Semperis Management Server	2:37 PM	--

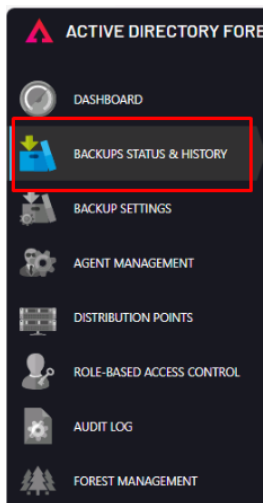
Cancel
RUN

Click “**RUN**” to start the job, which should only require 2 or 3 minutes to complete.

The icon becomes a square shape while running, where you could optionally click the icon and stop the backup job.



To see the **job details**, navigate to the "**BACKUP STATUS & HISTORY**" menu option:



On this page you can view the status of current and previous backup jobs:

Backups Status & History

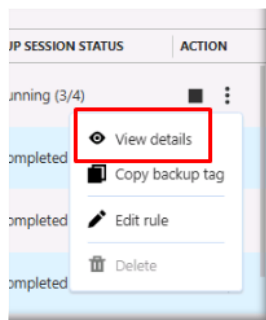
Search... Status All

137 item(s)

RULE NAME	BACKUP TAG	START TIME (UTC-07:00)	END TIME (UTC-07:00)	↓	ENCRYPTION	BACKUP SET VALIDATION	BACKUP SESSION STATUS	ACTION
All_DCs_Backup	{FDF99FC8-9E91-4C55-ACE9-387FF2F01830}	07/15/2024, 2:53 PM	07/15/2024, 2:56 PM		Encrypted	Valid	Completed	
All_DCs_Backup	{27C6107E-CC21-43BF-A53E-D3AFDFC5E437}	07/15/2024, 11:46 AM	07/15/2024, 11:51 AM		Encrypted	Valid	Completed	
All_DCs_Backup	{69A26696-373C-45FC-9A3F-99F3F9A616FD}	07/10/2024, 9:59 AM	07/10/2024, 9:03 AM		Encrypted	Valid	Completed	

View Backup Job Details

If a job is running (or on a completed job), you can use the “**View Details**” option to get more information on the specific domain controller backup jobs for that backup rule, by clicking on the three vertical dots in the **ACTION** field:



Viewing details will provide the status of each job, and when completed, show all DC backup jobs with the start and end times, or any errors that caused the jobs to fail.

DC NAME	DOMAIN NAME	SITE NAME	GROUP NAME	DC BACKUP STATUS	START TIME	END TIME	LOCAL BACKUP	PRIMARY DP	PRIMARY
ADFR-CHILD-DC1.CHILD.AD...	child.adfr.lab	Default-First-Site-Name	All_DCs	Completed	2:53	2:55	2:55	2:55	Semperis
ADFR-CHILD-DC2.CHILD.AD...	child.adfr.lab	Default-First-Site-Name	All_DCs	Completed	2:53	2:56	2:55	2:56	Semperis
ADFR-DC1.ADFR.LAB	adfr.lab	Default-First-Site-Name	All_DCs	Completed	2:53	2:55	2:55	2:55	Semperis
ADFR-DC2.ADFR.LAB	adfr.lab	Default-First-Site-Name	All_DCs	Completed	2:53	2:55	2:55	2:55	Semperis

Once you have a good, current backup, you can respond to Active Directory issues with a safety net for rapid, automated full forest recovery capability.

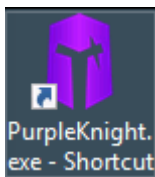
Launch a Purple Knight Security Assessment

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.

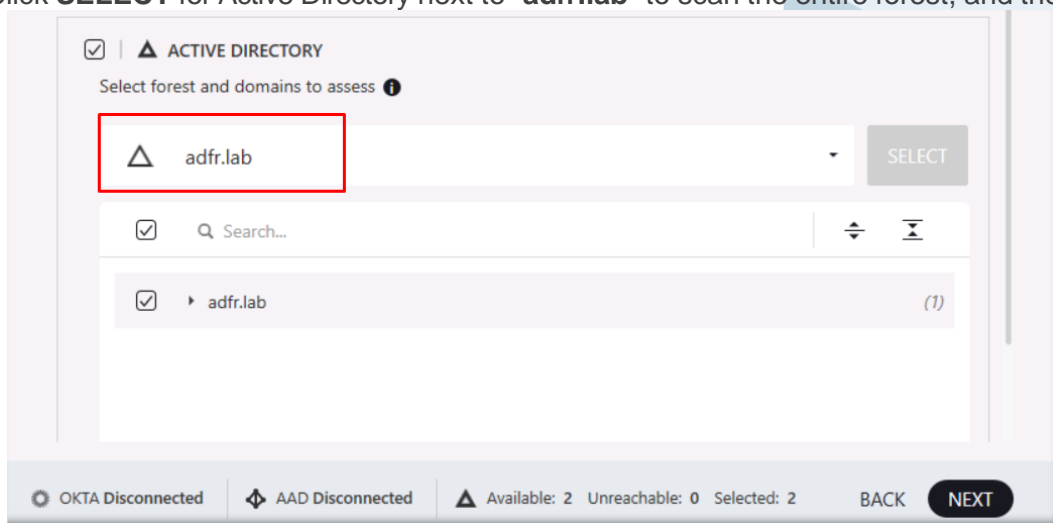
For convenience in this lab exercise, Purple Knight has been set up on **ADFR-DC1** because the ADFR Management server is not a domain-joined computer. (We typically recommend to never run PK on a domain controller, to run it instead on a regular domain-joined computer with non-administrative credentials, do that you get an accurate assessment of what a typical user can get to Active Directory.)



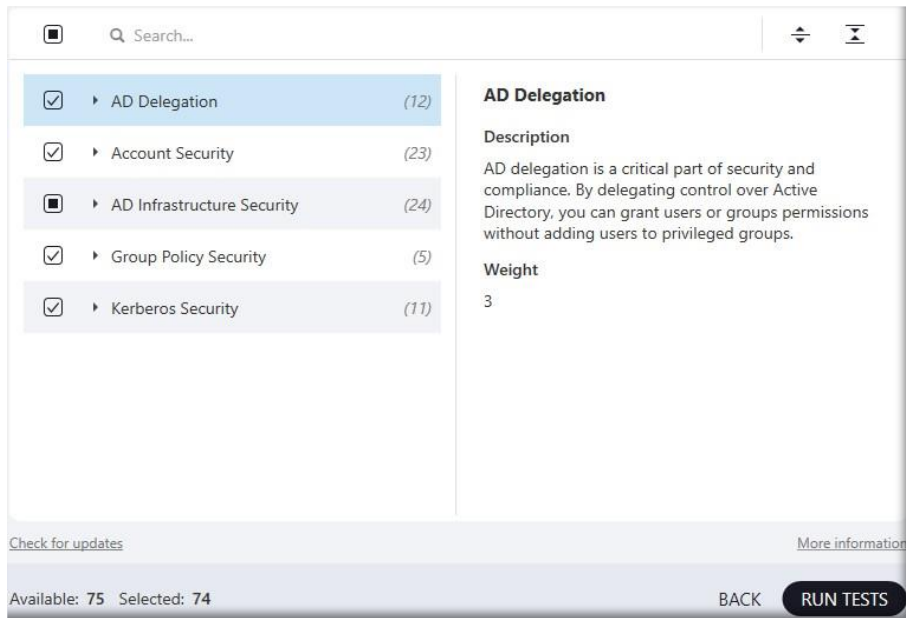
(If you do not see the shortcut, open File Explorer and navigate to the **C:\PK** folder on the domain controller ADFR-DC1.)

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

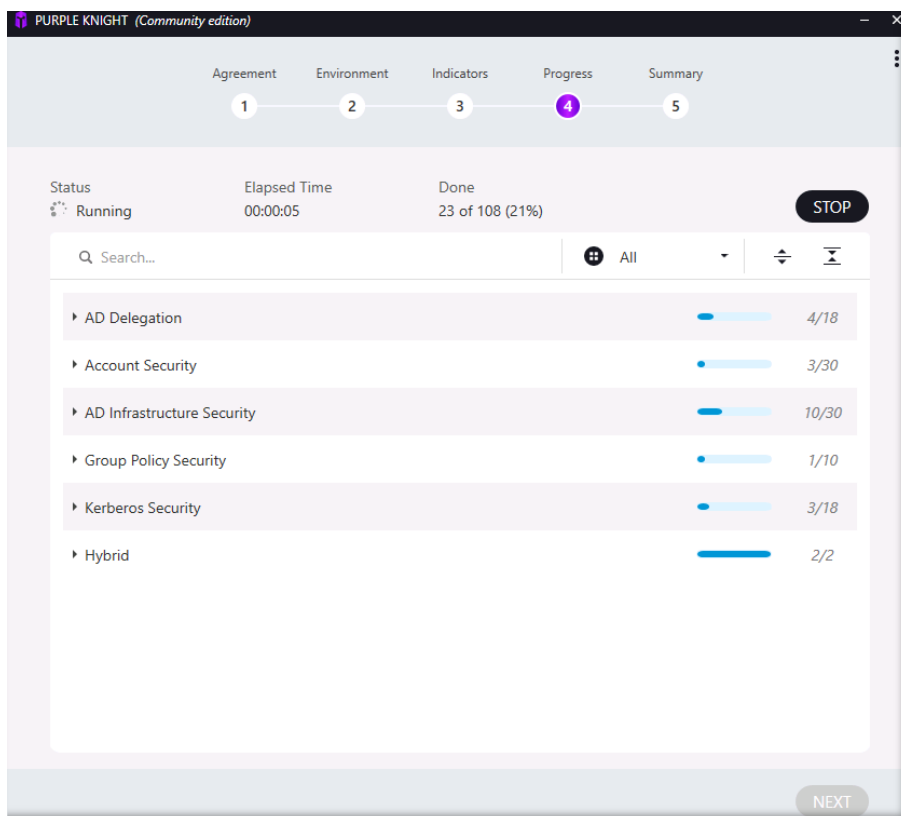
Click **SELECT** for Active Directory next to “**adfr.lab**” to scan the entire forest, and then click Next.

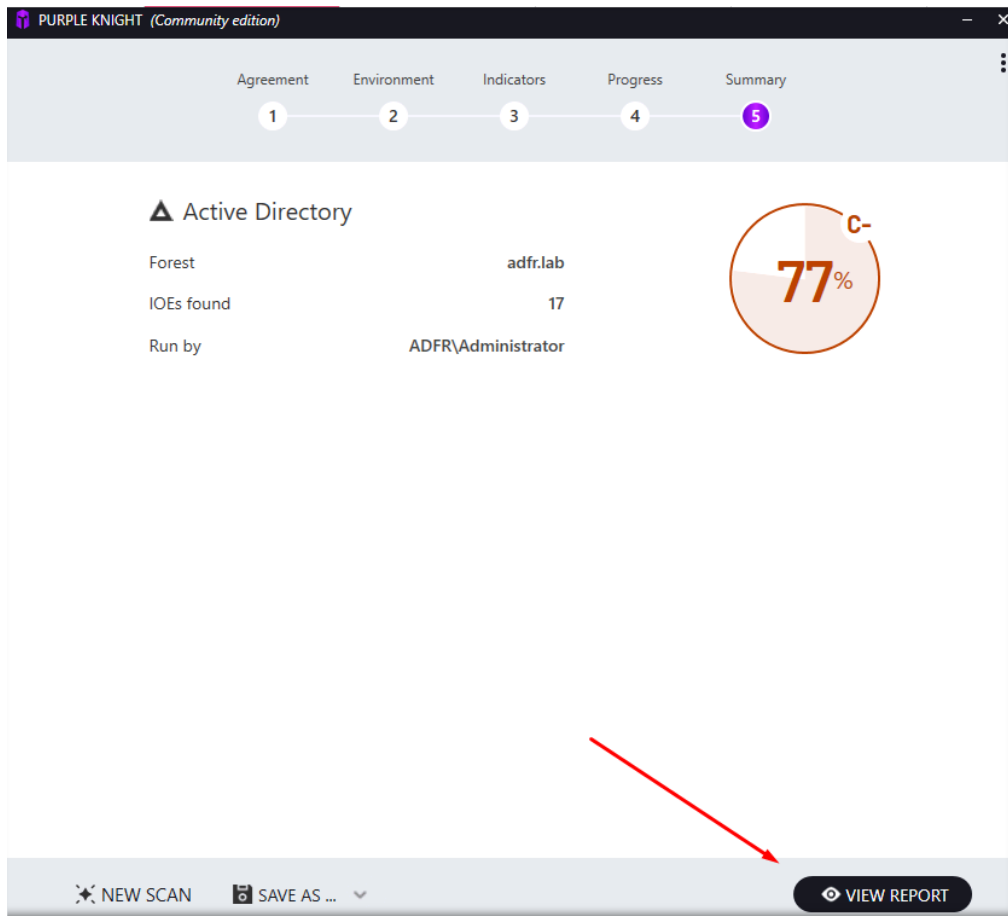


By default, all the tests are pre-selected except for the “ZeroLogon” test. The ZeroLogon test takes a bit longer to complete, and the domain controllers in the lab are not vulnerable to this attack, so it can be left unchecked.



Click **RUN TESTS** to initiate a scan.





The scan should only require about 90 seconds to complete, and then you will be presented with a report summary.

Click **VIEW REPORT** to dive into the details in the HTML output version: 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 something like the following message on the domain controllers:



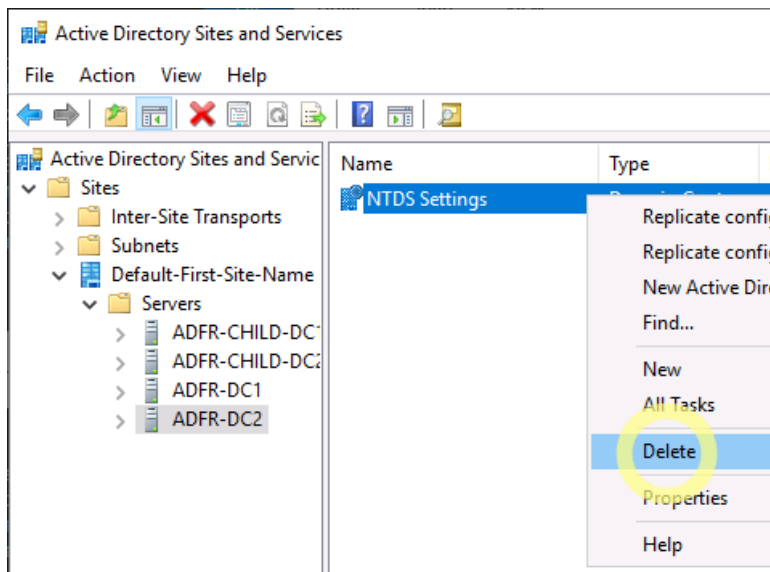
Ransomware, wiperware, etc, running on domain controllers effectively removes Active Directory service functionality.

Active Directory not only needs protection from cyberattacks, but sometimes operational self-inflicted problems can also take AD down.

We will do some damage (manually) to the Active Directory environment, replicating a rudimentary denial-of-service incident, and then fully recover the directory service using Semperis ADFR.

For this lab, we will simulate a denial-of-service style attack with the following steps on our root-level DC's:

- a) Connect to ADFR-DC2.
- b) Connect to ADFR-DC1.
- c) Delete all users in the "TEST" OU. (CTRL-A to select all, and Del - At least 250 users gone!)
- d) Remove all admins: remove all members of "Domain Admins" and "Enterprise Admins". (This change cannot be recovered with the AD Recycle Bin.)
- e) Delete all subnets in AD Sites & Services. (We could modify subnets but for the limited time in this session, we will just delete everything.)
- f) Delete the AD-integrated primary DNS zone. (Removes DNS records critical to AD functionality, not to mention resource records for everything in the enterprise.)
- g) Replicate these changes with the command "repadmin /syncall /force".
- h) Open AD Sites & Services (under "Administrative Tools") and delete the "NTDS Settings" object for the other DC, effectively making it non-functional as an AD domain controller:



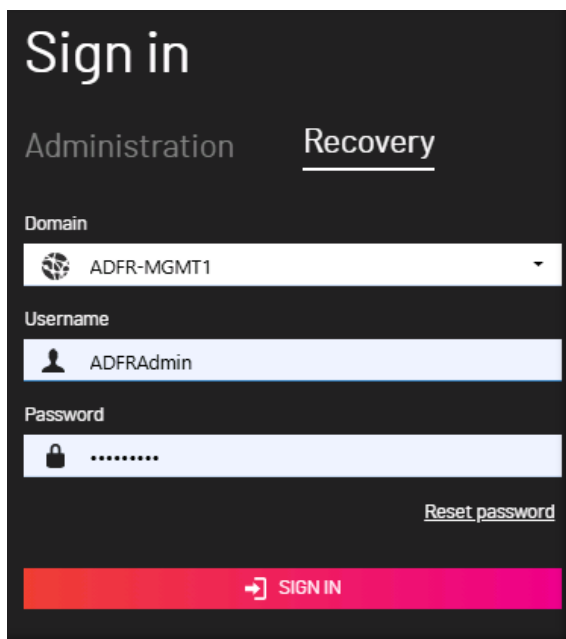
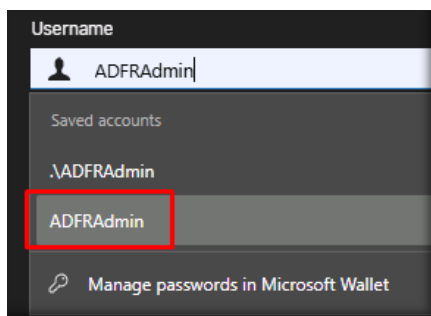
If you want to confirm that Active Directory is trashed, open a Command Prompt and enter the command "repadmin /syncall" on either root-level DC.

Initiate Recovery

Semperis ADFR allows recovering Active Directory forests to the same hosts as the existing domain controllers or it can target to a new host or hosts.

Following a breach, if the domain controllers were compromised, it is recommended to recover to new/clean hosts (i.e., “gold” images) to ensure no malware is dwelling on the DC.

1. Log into ADFR Recovery console using the shortcut placed on the Desktop. If you are already logged into ADFR Administration, you will have to log out first.
2. On the login page, select “Recovery” for the Recovery Console logon page.
3. Select the ADFR Management server for the “domain”.
4. Use the already stored “ADFRAdmin” credentials (the saved credentials without the “.\”) to log onto the Recovery Console.



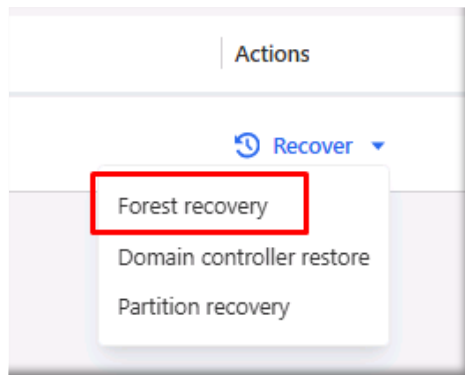
Click the “Recover” icon on the menu on the left for “ADFR” (adfr.lab) Active Directory forest.

Forest List
Select the forest you want to recover

1 item

Friendly name	Forest name	Recovery status	Actions
▶ ADFR	adfr.lab	--	Recover ▼

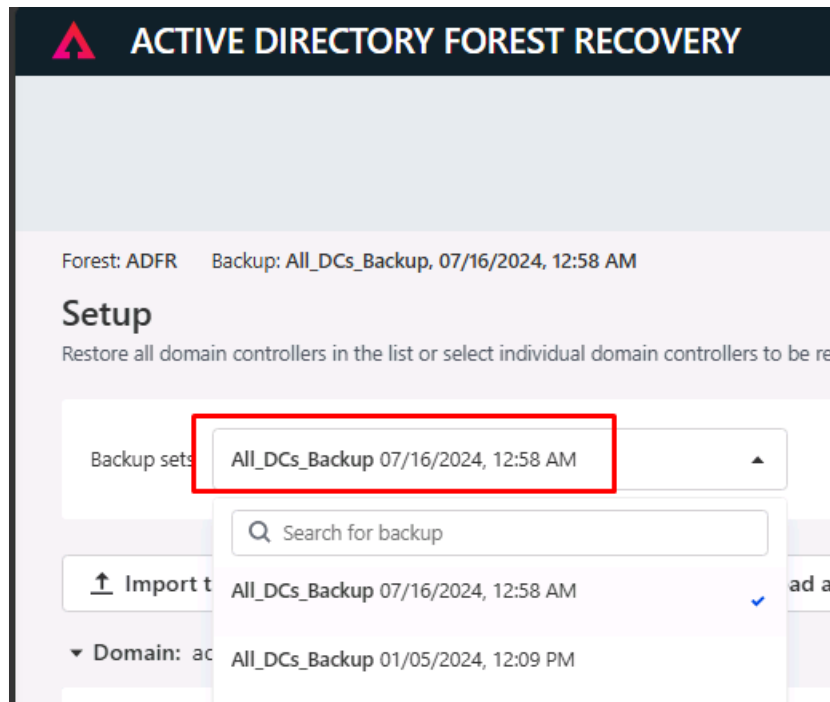
Select “Forest recovery” from the drop-down menu:



Select the latest backup you made for this lab.

Select the most recent backup set.

Example:



You can see the IP addresses of the current active DCs in the screenshot below.

At this point, we could opt to enter different IP addresses to target a different host. (In this lab, there are 4 additional “blank” VM systems ready to be restored to, but for our session, we will just restore over the existing DCs as that is the fastest recovery process.)

Forest: ADFR Backup: All_DCs_Backup, 07/16/2024, 12:58 AM

⬆️ Import target IPs

⬇️ Export target IPs

⬇️ Download agent installer

🔍 Search

☐ Show only issues

📄

🔍

⋮

4 DCs

DC name	AD site	Original IP	Target IP	Agent status	Operating System	Type	Restore from backup or repromote
ADFR-DC1	Default-First-Site-Name	10.160.1.1	Add new IP	Connected	Windows Server 2019 Standard	RWDC & GC	<input checked="" type="radio"/> Restore <input type="radio"/> Repromote
ADFR-DC2	Default-First-Site-Name	10.160.1.2	Add new IP	Connected	Windows Server 2019 Standard	RWDC & GC	<input checked="" type="radio"/> Restore <input type="radio"/> Repromote

▼ Domain: child.adfr.lab

DC name	AD site	Original IP	Target IP	Agent status	Operating System	Type	Restore from backup or repromote
ADFR-CHILD-DC1	Default-First-Site-Name	10.160.2.1	Add new IP	Connected	Windows Server 2019 Standard	RWDC & GC	<input checked="" type="radio"/> Restore <input type="radio"/> Repromote
ADFR-CHILD-DC2	Default-First-Site-Name	10.160.2.2	Add new IP	Connected	Windows Server 2019 Standard	RWDC & GC	<input checked="" type="radio"/> Restore <input type="radio"/> Repromote

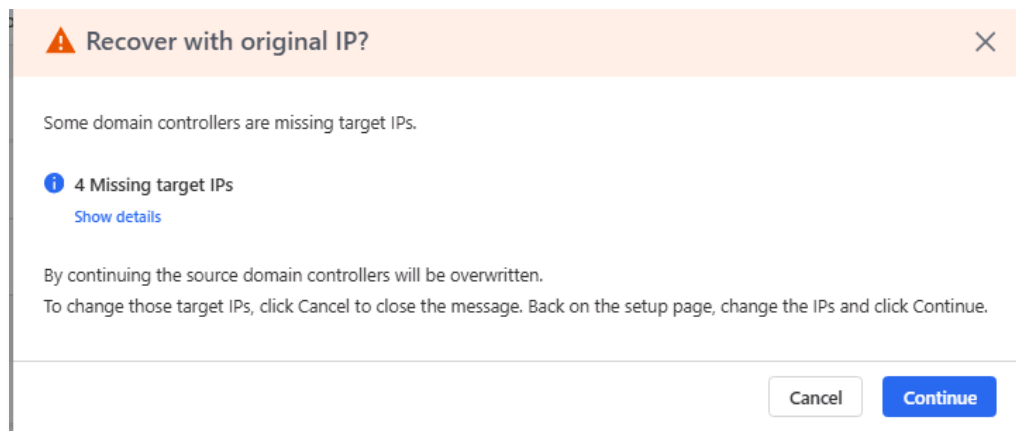
Cancel

Back

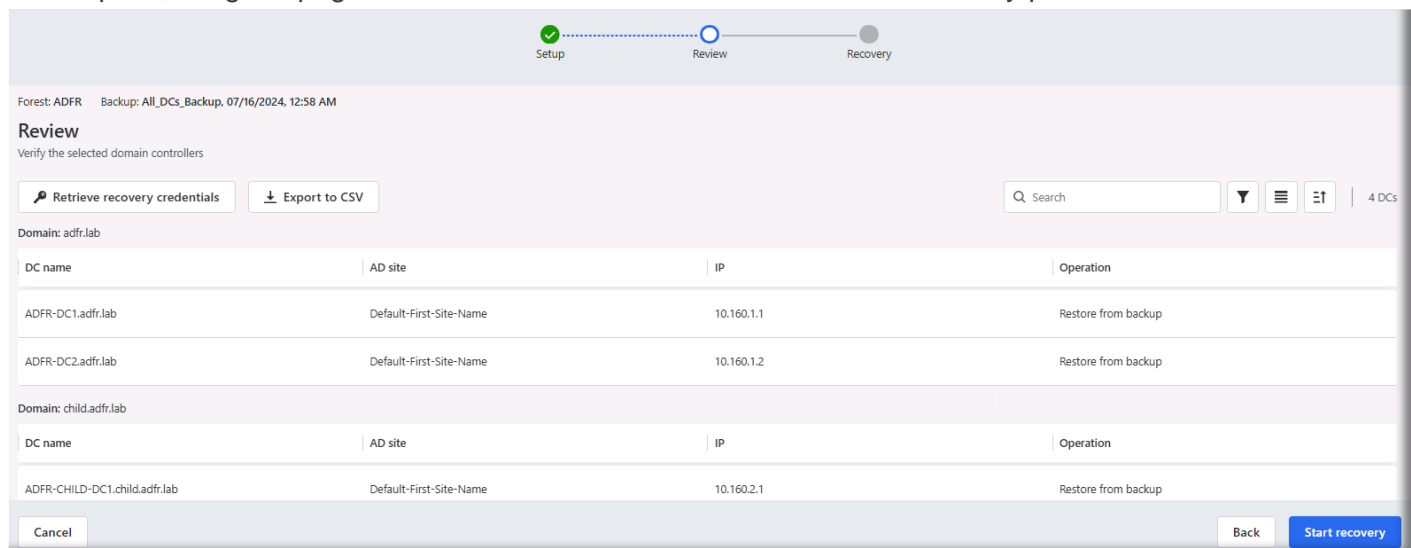
Continue

We will continue with the same servers and IP addresses. Click **Continue** to move to the next page.

Because we are using one or more of the original IP addresses, a warning pops up from which we can continue:

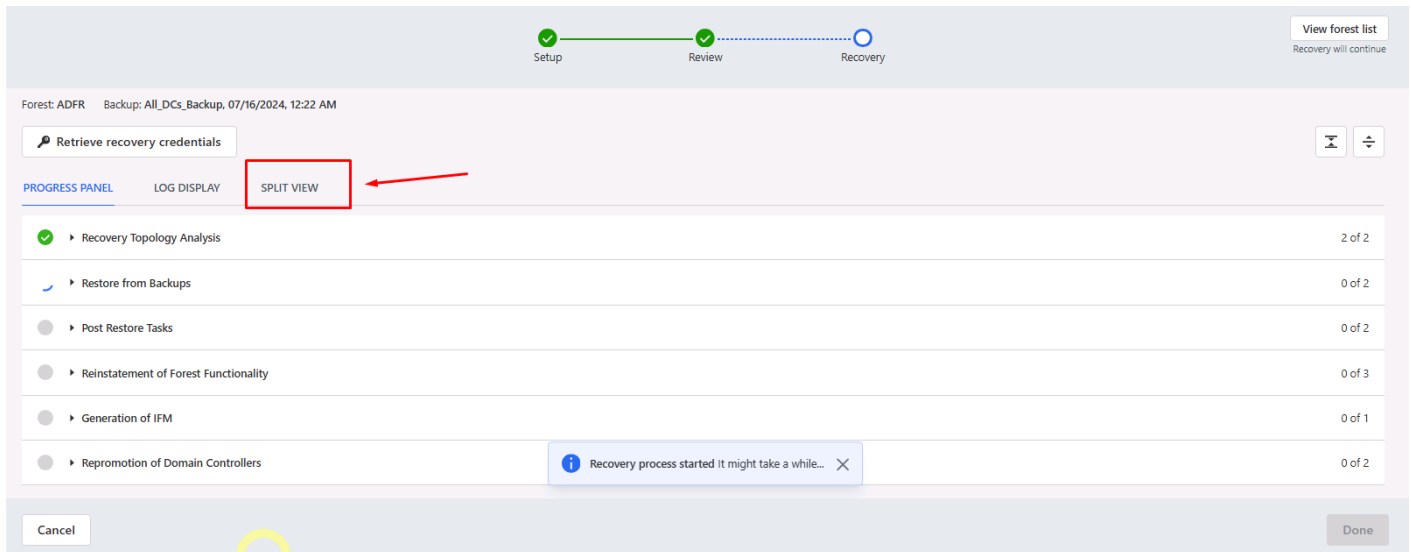


At this point, we get a page to review information and start the actual recovery process:



Click **Start recovery** which will initiate the AD forest recovery process.

When the recovery process is running, you can select the “split view” to see both the high-level steps and the logging at the same time.



Forest: ADFR Backup: All_DCs_Backup, 07/16/2024, 12:22 AM

Retrieve recovery credentials

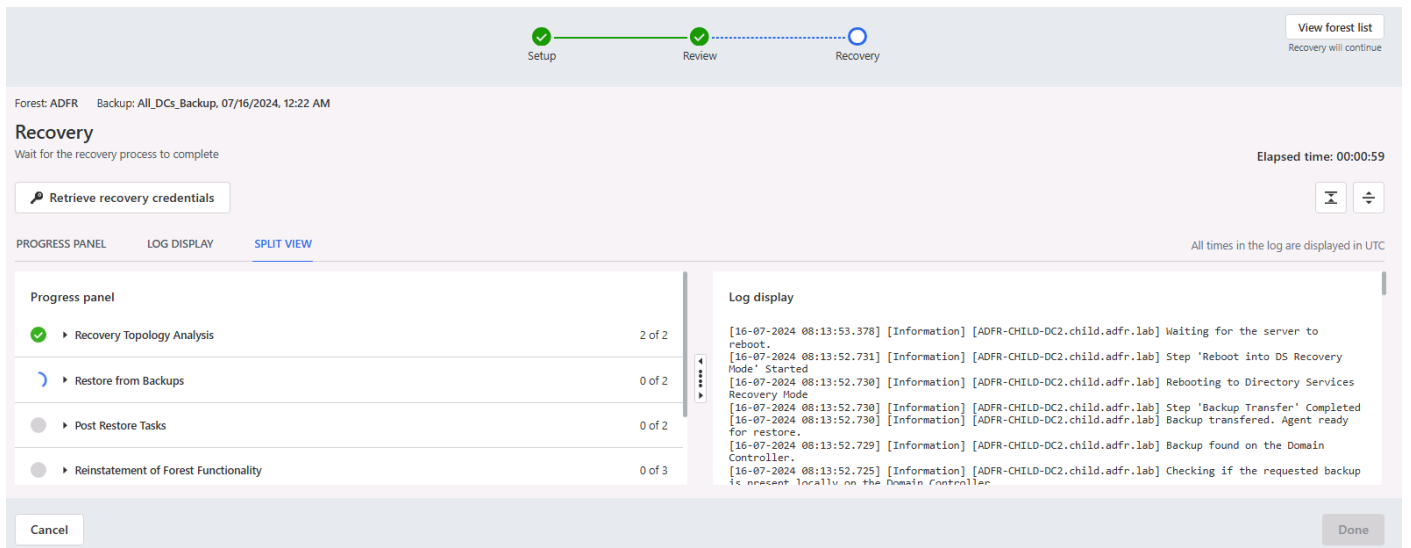
PROGRESS PANEL LOG DISPLAY **SPLIT VIEW**

- Recovery Topology Analysis 2 of 2
- Restore from Backups 0 of 2
- Post Restore Tasks 0 of 2
- Reinstatement of Forest Functionality 0 of 3
- Generation of IFM 0 of 1
- Repromotion of Domain Controllers 0 of 2

Recovery process started It might take a while...

Cancel Done

The logging reflects the steps defined in the Microsoft AD Forest Recovery Guide.



Forest: ADFR Backup: All_DCs_Backup, 07/16/2024, 12:22 AM

Retrieve recovery credentials

PROGRESS PANEL LOG DISPLAY **SPLIT VIEW**

Elapsed time: 00:00:59

All times in the log are displayed in UTC

Progress panel

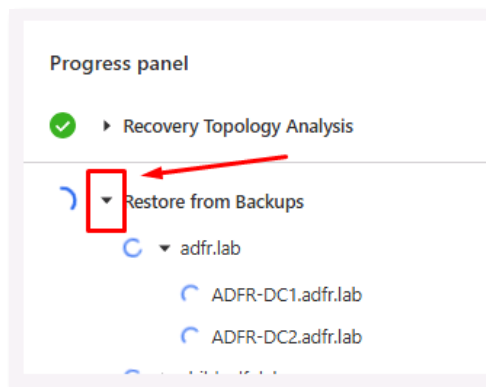
- Recovery Topology Analysis 2 of 2
- Restore from Backups 0 of 2
- Post Restore Tasks 0 of 2
- Reinstatement of Forest Functionality 0 of 3

Log display

```
[16-07-2024 08:13:378] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Waiting for the server to
reboot.
[16-07-2024 08:13:52.731] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Step 'Reboot into DS Recovery
Mode' Started
[16-07-2024 08:13:52.730] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Rebooting to Directory Services
Recovery Mode
[16-07-2024 08:13:52.730] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Step 'Backup Transfer' Completed
[16-07-2024 08:13:52.730] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Backup transferred. Agent ready
for restore.
[16-07-2024 08:13:52.729] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Backup found on the Domain
Controller.
[16-07-2024 08:13:52.725] [Information] [ADFR-CHILD-DC2.child.adfr.lab] Checking if the requested backup
is present locally on the Domain Controller.
```

Cancel Done

You can also click the little “dog ear” icon to expand the view in the left pane:

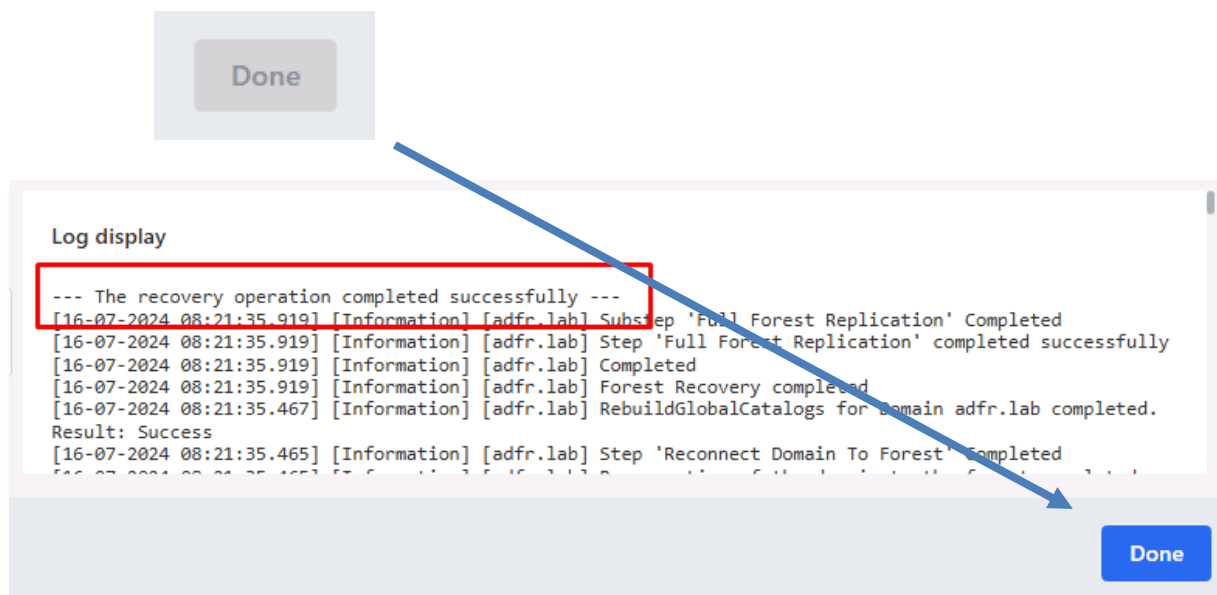


The forest recovery in the lab should normally take about 5 or 6 minutes to complete.

NOTE: The CloudShare lab is using shared resources, so you may experience slower response times due to the shared resources in their hosted infrastructure.

Make sure to click the “**Done**” button when it turns blue, when the recovery process has completed.

This clears the recovery process flag so that backup rules may resume.



Directory Services Restored

When the recovery process is finished, you may use Active Directory Users and Computers to see that the Directory Services are once again operational.

Time permitting, you may work through the Purple Knight report, or Purple Knight Post-Breach Edition (on the ADFR server) to discover any domain persistence or other issues from the “Incident”.

