Lab 13:

Windows   
Active Directory

Windows Server Security  
 2024-2025

© Daan Pareit

## Introduction

# Lab concept

In these exercises we recapitulate some of the basic skills of Windows Active Directory (AD) configuration and usage. We’ll create a new Active Directory domain and add the Windows Server and Windows client machines from the previous lab to it.



# Learning goals

* Configuring a new Active Directory Domain and its Domain Controller (DC)
* AD related Remote server administration
* Basic AD related client configuration

# Practicalities and prerequisites

You’ll need the following:

* The Windows VMs as installed in the previous lab
* Make sure your pfSense is running for Internet connectivity for your new VMs.

## Active Directory Domain services

Before we can use it to control our Active Directory domain, additional software needs to be installed on the King server. In Windows Server terminology, this is called adding the ‘Active Directory Domain Services’ role to the server:

* Start the Windows 11 and King machines
* On your Windows 11 machine, open Windows Admin Center (WAC), connect to the King server and go to the ‘Roles & features’ page

Important note:

To login in WAC, need to use “king\Administrator” format.

* Select the ‘Active Directory Domain Services’ checkbox and click ‘Install’. Select “Reboot the server automatically if required” and accept installing the suggested Roles and features. You can check the progress of this installation in the notifications pane (bell icon on the top right of the window).



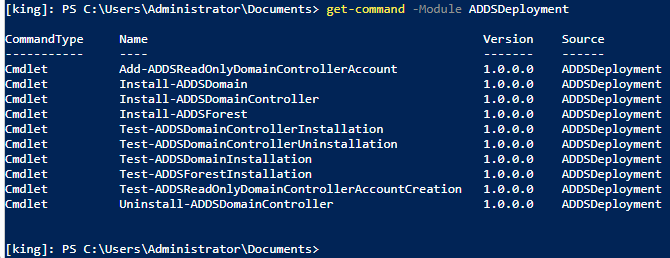
We will now convert our ‘KING’ server from a standalone server to a domain controller (DC). Unfortunately, WAC does not (yet) have support for doing this in the web interface, but we can also do this by using PowerShell:

* Open a remote PowerShell connection to the King Server in the WAC interface (go to the ‘powershell’ page) and log in as the server’s administrator.

A screen shot of a computer

Description automatically generated

* To deploy our new active directory domain, we’ll use cmdlets from the **ADDSDeployment** module. Use the Get-Command cmdlet to find out more information about this module, and read the manual pages for the associated install-\* cmdlets



* Since we are installing our first DC, we also need to make a new AD forest and domain. Do this with the ‘**Install-ADDSForest**’ cmdlet. It will ask interactively for extra information:
  + Choose ‘**COMPANY-<firstname>.serverlabs.be**’ as your domain name
  + Choose a Safe Mode Administrator Password for the ‘Directory Services Restore Mode’. (And don’t forget that password.)

Password: Server2025

* + Accept the promotion to Domain Controller and the necessary reboot.
* Wait until the install finishes, and restart the WAC session to the King server. Logging in as ‘KING\Administrator’ will no longer work. It will have to be ‘company-<firstname>\Administrator’ or ‘administrator@company-<firstname>.serverlabs.be’.

A screenshot of a computer

Description automatically generated

* To manage Active Directory domains, WAC uses a special plugin/extension. In the settings interface for WAC (gear icon on the top right of the window), go to the ‘extensions’ page, and install the ‘Active Directory’ and ‘DNS’ extensions. This will add those as extra pages in the left panel.

A screenshot of a computer

Description automatically generated

But its just not there?...

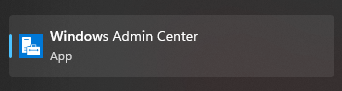
This is apparently an error due to the installation that we have on our machines. I installed v2 of WAC, as it was in the .msi file, from the source from Lab 12.

Here is the Win 11 management (version 24h2)

A close up of a sign

Description automatically generated

Here is my Win 11 host (version 23h2)



And on my host, I do see the extensions I need and can connect my KING server

A screenshot of a computer

Description automatically generated

So I asked my colleagues what the issue can be, and it is apparently due to the newer version of WAC that I could not see it, and even updating the feeds did not help (Microsoft one love)

So I was told to go and install the normal version (v1 or just older) of WAC with chocolatey (so I had to install chocolatey and then windows-admin-center package with it, and voila.

A screenshot of a computer error

Description automatically generated

It allows me to select the certificate as it was asked in the previous lab.

A screenshot of a computer

Description automatically generated

And the extensions are there!

Installed the extensions.

* Because our server was automatically upgraded to the status of Domain Controller in the newly created domain, its local users have now been converted to domain users and can no longer log in as ‘King\<username>’. From now on, these users are known as ‘COMPANY-<firstname>\<username>. Check if you can still log into the console of the ‘King’ virtual machine itself locally with the administrator and John Doe accounts.

A screen shot of a login form

Description automatically generated

Tried to just add it and it did not work.

If added with @COMPANY-serafim.serverlabs.be



Then it works.

* Let’s find out the reason for this. Start a WAC session for the King server and log in as user ‘COMPANY-<firstname>\administrator’. Go to the ‘Local Users and Groups’ page in WAC. You’ll find that it is no longer accessible for the King server since it became a domain controller.

A black text on a white background

Description automatically generated

Now search on the new ‘Active Directory’ page. Can you find the ‘John Doe’ user account? What user groups is he a member of?

A white background with black text

Description automatically generated

Users Domain Users

and Builtin Users.

* In the properties of the ‘John Doe’ account, set user logon name as ‘jdoe@COMPANY-<firstname>.serverlabs.be’ (i.e. the UPN format, Universal Principal Name)

A black and white rectangular object with black text

Description automatically generated

* Create another domain user ‘Donald’. The password needs to conform to the complexity requirements (e.g. Duck123!). Don’t forget to ‘enable’ that user.

A screen shot of a computer

Description automatically generated

Enabled

A white background with black text

Description automatically generated

Password: Duck123!

* Make Donald member of the ‘domain admins’

A close-up of a website

Description automatically generated

Now, as our server is promoted to Domain Controller, it has also become a DNS server. For future domain client computers to be able to successfully resolve names within the domain and on the Internet, we’ll configure the settings of the DNS service on KING:

A screenshot of a computer

Description automatically generated

* Ensure that the DNS server address on KINGs network adapter refers to the DNS service on KING itself, thus 127.0.0.1.

Took me some effort to understand the question.

Here it is correct:

A computer screen shot of a black screen

Description automatically generated

* First, we’ll check the DNS information for the local domain. Go to the ‘DNS’ page for the King server. What information can you find here?

I can get various A (or just plain resolution) of domain names records

A screenshot of a computer

Description automatically generated

* You may get a warning that the remote PowerShell DNS tools are not yet installed, if so, just let WAC install them for you.
* Device names outside our AD range (e.g. on the Internet) are not immediately known by our own DNS. To resolve these ‘outside’ names, requests should be forwarded to pfSense. Unfortunately, the DNS plugin for WAC cannot (yet) tell what ‘DNS forwarder’ our AD DNS is using. Use the PowerShell page (or remote PowerShell to the server) to run the cmdlet ‘Get-DnsServerForwarder’ and check that DNS requests are only forwarded to pfSense. If this is not the case, use PowerShell or Server Manager to correct this setting.

A computer screen with white text

Description automatically generated

## Joining the Windows 11 client to the domain

We will now join our Windows 11 client to the COMPANY-<FIRSTNAME> domain:

* Check if you can resolve ‘king.COMPANY-<firstname>.serverlabs.be’ and ‘COMPANY-<firstname>.serverlabs.be’ on the core server using nslookup. Why will this not work?

A screen shot of a computer

Description automatically generated

But my core can resolve the names and everything is good.

A computer screen shot of a black background

Description automatically generated

However on the Windows 11 client these are related to the pfSense machine. This probably happens due to pfSense being the resolver, and not our ADDC.

A white background with black arrows

Description automatically generated

Hint: have a look at the network settings you previously configured for the Windows client.

* To solve this, change the DNS server in your Windows 11 network settings of Ethernet0 to the IP address of the DC (192.168.11.50). (Alternatively, as in a production site, you could configure the DHCP settings of pfSense to communicate this over DHCP.). Does nslookup work now?

Yes it does

A white background with black numbers

Description automatically generated

A screen shot of a computer

Description automatically generated

To do with DHCP server, go to **http://192.168.11.254 , Services > DHCP Server**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

* Via the Windows graphical configuration ‘Settings – Accounts – Access work or school’ you can click ‘Connect’ and choose ‘Join this device to a local Active Directory domain’.
* Type the ‘company-<firstname>.serverlabs.be’ domain name to join

A screenshot of a computer error

Description automatically generated

Its alright it worked.

* Provide the credentials for John Doe and add him as ‘standard user’. Let the PC restart.

A screenshot of a computer error

Description automatically generated

In the User Account I just said John Doe, without anything else.

* Logon as John Doe on your Windows 11 client. Note that this succeeds flawlessly, even though John Doe is not known as a local user on the system. Open the Local User manager (lusrmgr.msc) to verify that John Doe is indeed not known as local user on the client PC.

A screenshot of a computer

Description automatically generated

* Check that the PC is part of COMPANY-<FIRSTNAME> domain by right-clicking the Windows start button and choosing ‘System’. Or alternatively, via the System Info of the Control Panel via shortcut: Windows key + Break key

A screenshot of a computer

Description automatically generated

* Note: To login as the original local (administrator) user ‘Mickey Mouse’, you have to login as “<PC-NAME>\Mickey Mouse” or even easier as “**.\**Mickey Mouse”. Else, login names are considered as domain users.

Except for the domain administrator “Administrator”. He/she/they explicitly needs to login as “COMPANY-<FIRSTNAME>\Administrator” else it is considered as a local “Administrator” account.

When logging in to your Win11, you can pay attention to the “Sign in to: <xxxxx>” information below the password field. It will show you whether the username is considered a local account (the PC name is shown) or domain account (the domain name is shown).

* Now, log on to your Win11 VM with domain admin user account Donald.

Note: should you receive a ‘your account has been disabled’ message, you’ve forgotten to enable the Donald account when you’ve created it a few steps ago.

COMPANY-serafim\Donald + password.

A screenshot of a computer

Description automatically generated

* Start WAC and add the King server to the list of administered devices. Check if you can find the client PC in the Active Directory domain. Upload a screenshot.



A screenshot of a computer

Description automatically generated

## Active Directory Domain Services extra – User access to domain machines

Earlier, we noticed that all domain users can log in to the Windows 11 client but not all domain users can log in to the King machine. This is the case for John Doe (who could, however, log in to King before we created the AD domain!). Only the domain administrator(s) can log in to all machines. We’ll now find out why this is the case.

* Log in to the Windows 11 machine as a domain administrator
* Use the remote ‘Server Manager’ application on your Windows 11 machine and add the king server if necessary.

A screenshot of a computer

Description automatically generated

Had to add it because the previous steps with Server Manager were done with my host.

* Find the link to the Default Domain Policy via Server Manager > Tools > Group policy manager. If you don’t have that tool yet, you’ll need to install the “RSAT: Group Policy Management Tools” as well as ‘Windows optional feature’ (via Settings – Apps – Optional Features).

Took like 30 minutes to install thanks to windows <3

A screenshot of a computer

Description automatically generated

* Within that Default Domain Policy, go to the policies for User Rights Assignment: Default Domain Policy – Edit – Computer Configuration – Policies – Windows settings – Security Settings – Local policies – User Rights Assignment. Inspect the (Explain tabs) of these policies to explain why John Doe can no longer log in.

A screenshot of a computer security settings

Description automatically generated

I tried to find something relatively suitable for the case, but as far as I understand it, the Administrator account for Core is the default user that is being created. The fact that we created John Doe as a secondary one, does not mean he is supposed to be transferred as well and be part of the thing.

Now however, we created the other user, also being an administrator, and now considering the rule from above – he is supposed to be able to login if and only if he is a domain administrator.