Setting Up Active Directory

Summary

Active Directory configuration and connection on macOS is unfortunately more complex than it should be. This article will show you how to set up AD (Active Directory) on your macOS machine. This article does assume you've already set up Active Directory on a server but assumes nothing beyond that.

Before we do anything though, we need to recognize a few issues with macOS AD. The first point with AD is that it used an encryption method called Kerberos which is time sensitive. What this means is that the time on the server and the client must be within a few seconds of each other in order for the network encryption to work properly. If they're mis-matched, you'll sometimes receive authentication failures when attempting to login, but not always. Windows accounts for this by using NTP (Network Time Protocol) and sets the NTP server as the AD server. macOS unfortunately, doesn't setup the NTP server properly (or at all sometimes). This causes grief for a lot of users who are new to AD on macOS. Next, we need to tackle an issue that seems to be fairly common among MS networks. A lot of networks setup by MS administrators use a domain ending with ".local" (dot local). This does NOT work on macOS due to macOS not performing DNS lookups on .local domains. It instead attempts to lookup locally (internal to the Mac) and if it doesn't resolve locally, it'll then broadcast on the local network for a response regarding the domain. This, from a network administration stand point, is a very bad thing. So, when setting up AD for macOS, you'll need to make sure that the AD domain doesn't end with .local. Next, you'll need to make sure that the Mac is using the AD server as it's DNS server and that the AD server has two very important DNS records setup for the Mac: A and PTR records. Lastly, when using the native AD implementation for macOS, you need to be careful when making queries to the AD service. If you do, you'll end up causing a vital system in Mac to fail.

Pre-Setup: Setting up NTP

Before we do anything, we need to fix our NTP server so AD is properly synchronized. On your Mac, click on the Apple menu and select "System Preferences…"

Should give you a window like this:

From here, select "Date & Time" near the bottom-middle of the window.

From here, you should be presented with this:

Now, you'll need to click on the padlock in the bottom-left corner and enter your administrator password to unlock the options.

Now you can edit the NTP server address by changing the text in the drop-down. Make sure to put the IP or domain of the AD server in there:

Note: This allows both domains (time.apple.com) and IP addresses (192.168.0.1)

Now, you should be setup and as far as NTP is concerned!

Pre-Setup: Changing the DNS Server

Next, we need to alter the DNS server that the Mac uses so AD can properly perform security DNS look-ups. On your Mac, click on the Apple menu and select "System Preferences…"

Should give you a window like this:

Next, click on "Network":

From here, click on "Advanced…"

Now click on the "DNS" tab

Click on the "+" button under the "DNS Servers" section and enter the IP Address of the AD server or a DNS server that is "aware" of the AD server (see below to find the IP).

Finally, click on "OK".

Now your DNS should be good to go!

Pre-Setup: Fixing .local and adding DNS records

Note: if you’re NOT the administrator for the AD server, you’ll need to ask your administrator to do this!

First, we need to make sure that .local isn’t the TLD of the AD domain (meaning it doesn’t end with .local). To do this, login to your AD server and click “Start”, then “All Programs”, then “Administrative Tools”, then finally “Active directory Users and Computers”. Alternatively, you could run this file: C:\Windows\System32\dsa.msc

If needed, update it following this article: https://technet.microsoft.com/en-us/library/cc738208(v=ws.10).aspx

Once this is all done, we need to add some DNS records for the Mac assuming they don’t already exist. With DHCP, they should in theory exist, but it never hurts to make sure that they are there. To do this, Click on “Start”, then “All Programs”, then “Administrative Tools”, then finally “DNS”. Or, you could run this file: C:\Windows\System32\dnsmgmt.msc

Once you have that open, check both the “Foreward Lookup Zones” and “Reverse Lookup Zones” on the DNS server and make sure that the IP address of your Mac is in both locations. Note: Some configurations don’t require a Reverse Lookup Zone.

Setup

Now that you have NTP and DNS setup and have made sure that the AD doesn’t contain .local (dot local), you can begin setting up AD on your Mac. First, you’ll need to open System Preferences from the Apple menu.

Then click on “Users & Groups”

From here, you’ll need to unlock the dialog by clicking on the padlock in the bottom-left corner and enter your administrator password.

Once that is done, you’ll want to click on “Login Options” (1) then click on “Join…” for “Network Account Server:” (2)

From here, you simply need to enter the fully qualified domain of the AD server (something like ad1.ds.aquaconnect.net) in the “Server:” field and hit “OK”.

Note: You ***HAVE*** to enter the AD server name, not your AD domain or an IP address!
Finally, you'll need to enter the administrator credentials for the AD server (not your Mac).

If you’ve setup everything correctly, your Mac should connect up to your AD server without issue and users on the AD server should be able to login without issue on the Mac!

Additional: Finding the IP address of a computer.

Windows - Open a command prompt (Start -> Run…) and type “cmd” and hit Enter. Now type in “ipconfig”. You’re looking for the ipv4 in a block like this:

So your IP in this example, would be: *192.168.1.3*

MacOS / Linux - Open a terminal (on Mac: Command + Space and type “Terminal” and hit Enter) and type "ifconfig" then hit Enter. You’re looking for the "inet" field in a block like this:

So your IP in the example, would be: *162.144.74.35*