# Preparations

There are many ways to configure this. To keep as close as possible to a “real” situation, we will use a separate VM for every task (DC(s), Mendix/SQL, end-user). You can vary this as necessary, for example by adding a separate VM for SQL server, or by installing Mendix on the DC to save resources.

Prerequisites:

* Install VirtualBox (latest): <https://www.virtualbox.org/wiki/Downloads>
* Install vagrant (latest): <https://www.vagrantup.com/downloads.html>
* Start command line (cmd.exe)
  + vagrant plugin install vagrant-windows

# Install Windows domain controller VM

Start command line (cmd.exe)

* Create a folder for vagrant config, CD to it
* vagrant init opentable/win-2008r2-enterprise-amd64-nocm
  + <https://vagrantcloud.com/opentable/win-2008r2-enterprise-amd64-nocm>
* Edit Vagrantfile, use this config:

Vagrant.configure("2") do |config|

config.vm.box = "opentable/win-2008r2-enterprise-amd64-nocm"

config.vm.network "private\_network", ip: "172.28.128.3"

config.vm.provider "virtualbox" do |vb|

vb.gui = true

vb.memory = 1024

end

end

* vagrant up
  + This will take some time while the VM is downloaded

Follow this guide: <https://support.cloudshare.com/hc/en-us/articles/200701095-How-to-setup-and-configure-a-Domain-Controller-on-Windows-Server-2008-R2>

* FQDN for forest root domain: europe.mendix-test.com
* Forest functional level: Windows Server 2008 R2
* Install DNS server, accept all warnings, reboot if necessary

Open Active Directory Users and Computers

* Add a new user in the proper folder. (example: test/M3nd1x!)
* Make sure user is in group “administrators”, otherwise local login won’t work.
* You should now be able to “switch” user to the new user.

Congratulations, you now have a working domain controller!

# Add a second machine to this domain, with Mendix installed

Command line:

* Create folder, CD to it
* vagrant init opentable/win-2008r2-enterprise-amd64-nocm
* Edit Vagrantfile, use this config:

Vagrant.configure("2") do |config|

config.vm.box = "opentable/win-2008r2-enterprise-amd64-nocm"

config.vm.network "private\_network", ip: "172.28.128.4"

config.vm.provider "virtualbox" do |vb|

vb.gui = true

vb.memory = 1024

end

end

* vagrant up

Add the machine to the domain:

* Go to network connections, open intranet LAN, Properties, IPv4 settings
* Set DNS to the DC server (which also has DNS installed) (172.28.128.3 in this config)
* OK, Close etc.
* Open system settings, Change computer name, Change…
* Set computer name, add domain
* Enter domain admin password (example: vagrant/vagrant)
* Restart

After restart login as the domain user you created on the DC to test

Now install Mendix (logged in as vagrant user): <https://world.mendix.com/display/howto40/Mendix+on+Windows+-+Service+Console+4>

* Start by setting up Java: <http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html#JDK7>
* Install SQL server Express: <http://www.microsoft.com/en-us/download/details.aspx?id=30438>
* Enable TCP access to SQL: <http://support.webecs.com/kb/a868/how-do-i-configure-sql-server-express-to-allow-remote.aspx> (Also ENABLE tcp access!)
* Use SQL management tools to create a database, use the vagrant account as owner
* Install Mendix service console
* Set up the app
  + Use localhost\SQLEXPRESS as the database host
  + Use the vagrant account as service user (no, this is not a best practice!)
  + If the DB doesn’t connect, try also starting the SQL server browser service
  + Use port 80, and allow remote access (again, not a best practice, but we don’t need IIS for now)
* Finally, disable windows firewall, to make sure other machines in the domain will also be able to connect to the server.

You should now be able to start the Mendix service and connect to the app using a browser (via http://localhost).

# Add a third machine, to act as the end-user

Repeat the vagrant install for the Mendix server, use this vagrant file:

Vagrant.configure("2") do |config|

config.vm.box = "opentable/win-2008r2-enterprise-amd64-nocm"

config.vm.network "private\_network", ip: "172.28.128.5"

config.vm.provider "virtualbox" do |vb|

vb.gui = true

vb.memory = 1024

end

end

Stop before installing Mendix. You should now have a mostly empty machine, joined to the domain, on which your test domain user can log in.

Install Chrome and access the app running on the Mendix VM.

# Enable Kerberos login on the Mendix server

On the DC

* Create a new user in the AD, note the name (e.g. MendixKerberos), set to never expire PW, cannot change password. The Mx server will authenticate to the DC as this user.
* In a command line, do (replace with actual names):
  + ktpass.exe -princ HTTP/vagrant-mx.europe.mendix-test.com@EUROPE.MENDIX-TEST.COM -mapuser EUROPE\MendixKerberos +rndPass -out vagrant-mx.keytab -ptype KRB5\_NT\_PRINCIPAL
* The keytab file that was generated must be put in the resources folder on the mendix server VM

In the test project model

* Download kerberos module, set startup microflow
* Edit sso.properties file (example values, see comments in file for explanation):
  + domain = europe.mendix-test.com
  + active\_directory\_server = 172.28.128.3
  + kerberos\_servername = vagrant-mx
  + kerberos\_keytab\_file = vagrant-mx.keytab
  + kerberos\_protocol = http
  + debug = true
* Create deployment package.

On the Mendix VM

* Deploy package on server.
* Go to localhost/login-default.html on the mendix machine, and create an account for your test domain user (in a real situation this could be done through LDAP)

On the user VM

* Login with the test domain user
* Set up IE and Chrome for integrated kerberos auth using windows settings:
  + In start menu, go to Internet Options > Security tab, Select local internet > Sites > Advanced and add the url of the application.
  + Go back to the security tab and press custom level. Scroll down to the user authentication section, and select for Logon > Automatic login only in Intranet zone.
  + Close the custom level window and select the advanced tab. Under Security, make sure Enable Integrated Windows Authentication is checked.
* Go to <http://vagrant-client.europe.mendix-test.com/sso> to login

You should now be logged into the application using Kerberos!