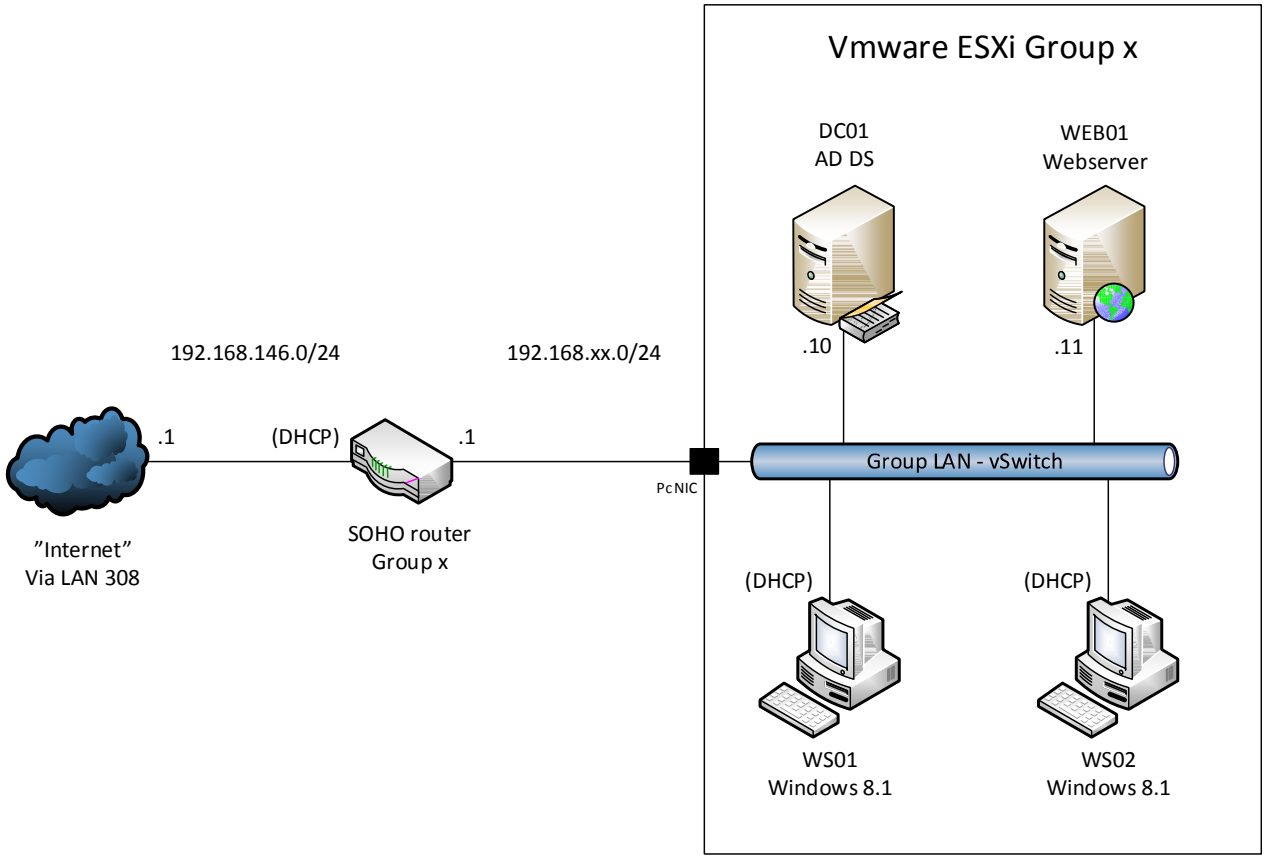
Ascom Server 2012 R2 - Webserver – Case tasks



Task 1

Install the following machines:

DC01	Server2012 R2 Datacenter Edition with GUI
WEB01	Server2012 R2 Datacenter Edition with GUI
WS01	Windows 8.1
WS02	Windows 8.1

Name and configure IP addresses by following the topology drawing.

Task 2

Install Active Directory on DC01. Domain name: domain.local.
Make all machines members of the domain.local domain, except WS02.

Task 3

The company has the following organization. Try to make an efficient OU structure in Active Directory Users and Computers using Microsoft best practice.

Department	No. employees
Management	2
Production	50
Administration	6
IT	3
Sales	10

- Users in every department must be created in their respective OU and must be member of a domain global group in every department. (In practical create one user per department, name the users freely)
- The two client machines must be placed in the management and production OU's respectivly)
- The five servers must also be organized in the OU structure.

Task 4

The company has the following requirements to shared folders and groups that can access them.

	Must have the following level of access to folders:							
Employees in domain global groups	**Administration**	**Management**	**Production**	**Sales**	**Project 1**	**Project 2**	**Project Assignments**	**Common files**
Administration	**Read and write – delete own files**	**Read**	**Read**	**Read**				**Read and write – delete own files**
Management	**Read and write – delete own files**	**Read and write – delete own files**						
Production	**Read**	**Read**	**Read and write – delete own files**					
Sales	**Read**	**Read**	**Read**	**Read and write – delete own files**				
Project 1		**Read**			**Read and write – delete own files**			
Project 2		**Read**				**Read and write – delete own files**		
Any project		**Read**					**Read**	

Furthermore, the domain administrators must have full control of all folders.

(Continued on next page)

You must

- Make a plan of which NTFS permissions needs to be effectuated and from this plan determine:
    - Which domain local groups must be created and their name.
    - Which NTFS permissions the domain local groups must be assigned.
    - Which domain global groups must be member of which domain local groups.
- Follow Microsoft Best Practice for Access Management.

- Create the folders and shares on DC01.

Task 5

Install the WINS feature on DC01 and configure all servers and clients to use the WINS server.

Task 6

- Install IIS 8.5 on WEB01
- Create two new websites: website1 and website2 each with their own application pool and physical path.
- On DC01 configure a DNS record for both www.website1.com and www.website2.com and point to the IP address of WEB01.
- On WEB01 under IIS bindings configure so www.website1.com can be reached on port 80 and www.website2.com can be reached on port 81. Test from CLIENT01.
- On WEB01 under IIS bindings set the port number back to 80 for both websites. Now configure host header so website1 can be reached by the name www.website1.com and website2 can be reached by the name www.website2.com. Test from CLIENT01
- On WEB01 set authentication method for website2 to Windows authentication (Integrated). Add www.website2.com to local intranet zone on Client01. Test access from CLIENT01 and test access from CLIENT02 (Not domain joined)

Task 7

- Create a new service on DC01. (e.g. sc.exe \\localhost create NewService binpath= c:\Windows\System32\calc.exe)
- Configure the service to start automatically when windows starts.
- In case of failure, configure the service to restart the first two times and to run a program the third time.
- Try to stop and start the IIS service on WEB01 with the following commands: **net**, **stop-service/start-service** (PowerShell), **sc.exe (**You must identify the name of the IIS service first)

Task 8

Try to do the following via Group Policy:

- The local administrator and guest account must be disabled on all client machines that are member of your domain.
- User passwords must meet the following requirements:
    - The password must be changed one time every month minimum.
    - The password length must be minimum 9 characters.
    - The password must contain three of the following four categories: special characters, uppercase characters, lowercase characters or numbers.
- If someone tries to brute force a user account, the account must be locked after four attempts. Only an administrator must unlock the account then.