Laboration 4

1DV020 – Serveradministraion

March 4, 2015

1 Introduction

For this module we will work with Active Directory and look at some of the concepts herein. After installing the A.D D.S role we start of by implementing an AGDLP strategy under certain parameters - the exact structure and naming convention will be up to you.

We will then setup group policies on these and assure that we have a proper delegation of control.

2 Deadline

There is only one lab session connected to this module. It is of course okay to present on the following lab.

Accounting   You will show your work and demonstrate your progress at any of these lab session, prepare a small document with an overview of your configuration/setup if needed for overview.

Note: To test the environment I will be using the program **smbclient** from your internal server so make sure that this is installed there. I will also make changes to your groups/add other groups to make sure that the AGDLP is working.

3 Assignment

The following fours sections with subtasks are the assignment:

3.1 A.D DS Installation

Install the Active Directory Domain Services and promote the Windows server to a domain controller.

To be able to have the A.D working properly we need to either delegate the zone corp.mycompany.lab ,so that the linux server instead act as a slave for this zone. Or you can setup a new DNS with forwarders and disable the corp.mycompany.lab on the linux server. This is also a valid workaround. Don't forget to change the DHCP settings.

3.2 A G/U DLP

Adopt a AGDLP strategy for the environment specified in the Work Environment, add the users, and groups necessary to accomplish this. You then apply the AGDLP solution on your shares.

3.3 Join Domain

Make your internal client(win 8.1 Bus) join the A.D Domain. It should be visible under the computers tab in your A.D structure when you have joined.

(If you run into problems during this phase and gets stuck there. A temporary workaround is to: Follow the "Grant members the right to logon locally" guide to enable logon with local users. This is as said only a temporary solution. But you could confirm that delegation and group policies are working.)

3.4 Delegation

Make sure that the following delegations are in effect and make sure you use and AGDLP strategy for this too.

Human Resources:

- Should be able to read user information on all sectors.

Call Center Manager:

- Should be able to add, modify and delete regular Callcenter users, but not managers.
- Should be able to add, modify and delete regular IT Support users.

IT Support: Not the same as administrators!

- Should be able to add, modify, delete and reset password for Callcenter employees, but not Call Center managers.

- Should be able to add, modify and delete regular and reset password for Human resources users.

3.5 Group Policies

Apply group policies. Try at least 4 group policies and confirm that they are working and affecting only the users in the Call Center OU. Apply a group policy that only affects the computers of your domain. Confirm the policies are taking effect.

3.6 Roaming profiles

Create a roaming profile for at least one user.

4 Requirements

The AGDLP strategy should be working.

If you wish to continue using your current DNS solution you can modify the corp.mycompany.lab zone to act as a slave in your bind configuration and specify the the windows computer as the master for that domain. This of course requires the windows server to be set as authoritative over that domain.

It should look something like this:

```
1 zone "corp.mycompany.lab" {
2      type slave;
3      masters {<ip of windows server>};
4 }
```

5 Work Enviroment

We will assume that the primary role of the company is a call center. We will also assume that we have a decent amount of employees 50(but for the lab we don't need to set up all of them!)

5.1 Sections Layout

In the environment there should exist the following sections, with employees:

- IT Support

  – Pelle

- Human Resources

  - Stina
  - John

- Call Center

  - Manager
    * Johan
  - Employees
    * Marcus
    * Calina

5.2 Resources

The following resources should be shared according to your AGDLP solution:

Shares:

- Quick:

  - IT Support have full control
  - Call Center Manager have read and modify Access
  - Call Center Employees have read access
  - Human resources have read access.

- Mirror:

  - Call Center manager have full control
  - Call Center Employees have Read Access.
  - IT support have full control.