AN EXAMPLE OF IMPLEMENTING A DOMAIN AS A CENTRALIZED MANAGEMENT POINT FOR CLIENT COMPUTERS

PRIMJER IMPLEMENTACIJE DOMENA KAO CENTRALIZOVANE MENADŽMENT TAČKE ZA KLIJENT RAČUNARE

Džemal Kulašin
Mahir Zajmović

ABSTRACT

The theme of this paper is based on the implementing the domain as centralized management spot of client computers. Complete implementation of the infrastructure was done using Microsoft solutions, Windows Server 2012 R2 and Windows 10. The virtual company "University", which has 2 servers and 50 client computers, has been created. In the companies in which we work as IT experts, we need to know when we need a work group, and when we need a domain. According to the Microsoft documentation, Workgroup is a network which shares the same network name, is not limited by the number of users, but is recommended for up to 20 users, if there is no need for centralized management, multiple login locations on the network etc. The implementation of the domain provides the ability to create restrictions towards users. All users have to be added into the domain, assigned with privileges and reconfigured per request of the company where AD is being implemented, or per security recommended restrictions.

Keywords: Microsoft Server, Active Directory, policies, server, domain, client

SAŽETAK

Tema ovog rada zasniva se na implementaciji domene kao centraliziranog upravljačkog mjesta klijentskih računara. Kompletna implementacija infrastrukture izvršena je pomoću Microsoftovih rješenja, Windows Server 2012 R2 i Windows 10. Stvorena je virtualna kompanija „University" koja ima 2 servera i 50 klijentskih računara. U kompanijama u kojima radimo kao IT stručnjaci moramo znati kada nam treba radna grupa, a kada domena. Prema Microsoftovoj dokumentaciji, Workgroup je mreža koja dijeli isto mrežno ime, nije ograničena brojem korisnika, ali se preporučuje za najviše 20 korisnika, ako nije potrebno centralizirano upravljanje, više lokacija za prijavu na mrežu itd. Implementacija domene pruža mogućnost stvaranja ograničenja prema korisnicima. Svi korisnici moraju se dodati u domenu, dodijeliti im privilegije i ponovo konfigurirati prema zahtjevu kompanije u kojoj se implementira AD ili prema sigurnosnim ograničenjima.

Ključne riječi: Microsoft Server, Active Directory, politike, server, domena, klijent

INTRODUCTION

Domains, work groups and basic groups are different methods of computer organization in networks. The main difference between them is in the manner of computer management and other resources on the network. Computers which have Windows operative system installed on the network have to be a part of work group or domain. Computers which have Windows operative system installed in home networks can also be a part of primary group, but it is not necessary. Computers in home networks usually belong to a work group or perhaps a primary group and those on the business

networks belong to a domain. In the domain:

- One or more computers are servers. Network administrators use servers in order to control security and permissions of all computers within the domain. This eases changes because they are automatically applied to all computers. Domain users have to insert their password each time they try to log on the domain;
- If you own a user account on the domain, you can log in to any computer on the domain without your user account on the said computer;
- You can probably make only limited changes in the computer settings, because administrators usually want to secure consistency between computers;
- Computers can belong to different local networks.

WHAT IS A SERVER AND WHAT ARE THE TYPES OF SERVERS

The term server is often linked today to the expensive computers with expensive operating systems which almost no one dares to approach because they are very important. The server is a computer in your IT system which is connected to the network and which enables certain services to other computers in the network. A server is not a computer which necessarily needs to have installed server operating system. Therefore, a computer with installed Windows 7 can be a server, if it is adjusted as such in the network and assigned with such role. Nowadays, we can say that there are two groups of servers. The first group consists of servers which, in the event of failure, do not have a key influence onto the performance of jobs, and the second group consists of servers which, in the event of failure, threaten the business, and in this regard have to constantly work. The example for the first group of servers would be, for example, print server which enables computers in the network to use printers connected to it, whereas the example for the second group of servers would be a server which has installed production program, and in the event of failure leads to a total halt in the production line. Depending on their functionality, there are the following types of servers:

1. Server for user identification (Identification server):

The task of such server is to enable the user-controlled network access. This is done so that the user needs to enter their username and password every time (s)he wants to work using a work station. The best known program that operates in this manner is MS Active Directory.

2. Server which enables access to printers (Print server)

Such server enables all work stations the use of printers that are plugged to it. Today, such servers are less and less used because there are printers that can be directly plugged on the network and that already have such function installed. These are the so called network printers.

3. Servers for file sharing (File server)

It is often used server which stores files that are being used by the employees according to their needs. Access to certain documents can be limited in the sense that only specific users can have access or change them.

4. Servers to power web applications (Web server)

If you own a website or a program which requires access by multiple users from different locations, you need a server on which your site or application will be installed, and to which the users will have access when they are connected to the Internet using any of Internet browsers, such as Google Chrome or Mozilla Firefox.

5. Server for file sharing via the Internet (FTP Server)

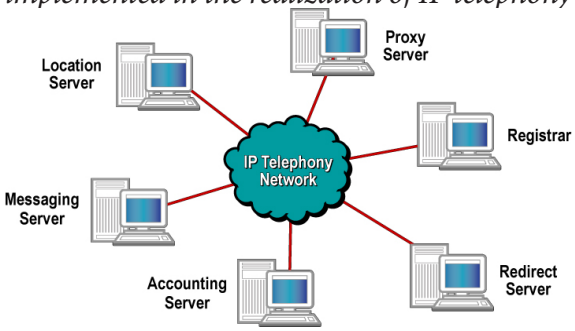
As file sharing server enables file sharing within the local network, such server enables file sharing via the Internet.

6. Electronic mail server (Mail server)
Once the electronic mail server is installed, all electronic mail meant for the employees in the company first arrives to the server, and is later on distributed to them. The same occurs when employees want to send electronic mail to someone. First it arrives on the server, and then the server sends it where it is required.

7. Database server (Database server)
Such servers store data and enable the applications installed on other computers to use such data.

8. Remote access server (VPN server)
Such servers enable the access to your own network from any location where you have the access to the Internet. Simply said, it enables you to use all resources as if you were in the office, and not on some distant location.

Figure 1. Review of multiple servers implemented in the realization of IP telephony



GROUP POLICIES

From the earliest days of usage of active directory, group policies have played one of the major roles in the management of computer environment. Many organizations have realized that the initial purchase or the rental price of computers represents only small piece of the entire ensemble which is connected to the management and maintenance of computers during their life span. The primary cost is an expense of human management of those computers. If all client computers required a manual administration, the price of owning these computers would greatly rise, even to the unacceptable amount. In order to solve this problem, organizations need to move from manual processes and to establish automatic and centralized form of administration of changes and management of user and computer settings within the environment. There are numerous things that we can do with the help of group policies:

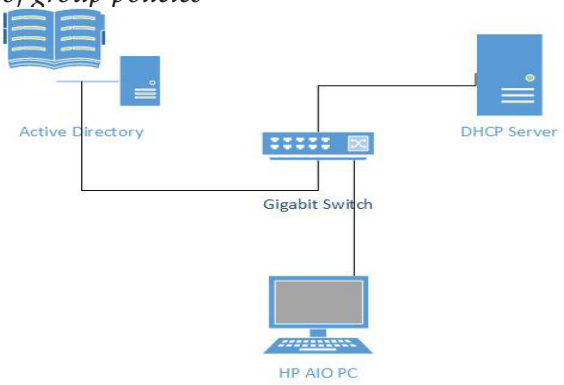
- Installation and software management: For Active Directory-based Group Policy administrator can build software of updates to users and computers. Also, we can remove built-in software based on user location and computer within the structure of active directory;
- Scripting: We can start computer Startup and Shutdown scripts as user Logon and Logoff scripts;
- Security settings: We can configure a large number of security settings for user and computer facilities within AD. Security settings for computers include: Account Policies, Local Policies, Event Log settings and settings that relate to Restricted Groups, System Services, and Windows Firewall & Network Access Protection. Security settings that relate to users include: Public Key Policies & Software Restriction Policies;
- Folder Redirection: We can redirect some parts of user's work environment, such as Documents folder, Start Menu or Desktop into network Share where they will always be available to users and where there will be enabled Backup with the help of standard Backup procedures as arranged by the organization;
- Policy-based Quality of Service (QoS): QoS policy can be assigned to the outgoing traffic network specific Differentiated Services Code Point (DSCP) amount, and we can control which applications, IP addresses or protocols and entry numbers (Port) will have a priority and which ones will be controlled through the network;

- Internet Explorer settings: We can use group policies to manage Browser menu and Toolbars, Connection settings, URL favorites, Security features and default Internet settings. Extensive Internet Explorer settings now can be configured under Administrative Templates-Windows Components-internet Explorer;
- Administrative patterns: We can use administrative patterns for management of large number of GUI elements such as: Control Panel Settings, Desktop settings, Start Menu & Taskbar Settings. These settings configure Registry and the amounts that limit modification which can be made by users on their computers;
- Preferences: Preferences offers the possibility of management of large number of options that relate to Windows settings or Control Panel settings, including: Drive mapping, Environment variables, Network Shares, Local Users & Groups, Services, Devices and many others;
- Printers: Administrators now have the possibility to delegate permissions to users for the installation of Printer Driver (as well as for other Driver applications);
- Blocking of installation of devices: Administrators now can centrally prohibit installation of certain devices on computers in the organization. We can create policy settings which control access to devices such as USB, CD-RW and other media which can be removed from the computer;
- Power Management settings: We can modify specific Power settings through individual settings in group policies, or we can build adjusted Power plan which we can further implement using group policies.

INFRASTRUCTURE

Server on which operates Active Directory roll is HP Proliant DL360 Gen5 Server, with the processor 2x2.5GHz qaud core and 16GB RAM memory, 10K SAS disks. Operative system that was installed on the server is Windows Server 2012 R2. Windows Server 2012 R2 can be downloaded from Microsoft website, on the link: https://www microsoft. com/en-us/evalcenter/evaluate-windows-server-2012-r2. Windows 10 Enterprise can be downloaded from Microsoft website, on the link: https://www. microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise.
From the client's standpoint, we have 50 computers that have been upgraded onto Windows 10, which is from July 29, 2015, available on the market. Windows 10 comes in 7 editions. Our infrastructure of client machines is based on 64 bite architect with computers All In On computers HP Envy Recline 23-k310 23-Inch All-in-One (Intel Core i3-4130T Processor, 8GB PC3-12800 DDR3L RAM, 1TB SATA 6G Solid State Hybrid Drive with 8GB SSD acceleration cache). On the domain server we have implemented a centralized management of anti-virus solutions.
In our example, we have installed ESET NOD32 AV onto Windows Server, and performed deployment of anti-virus applications. Now imagine that we need to install a certain application (in this case anti-virus) on 50 computers – this would take several days. If use the option of automatism, the whole work will be done very quickly, which again depends on the network infrastructure (if it has gigabyte switches, what policies have been implemented, are there any bad network configurations, clients, servers etc.).

Diagram 1. Review of infrastructure that will participate in the example of implementation of group policies

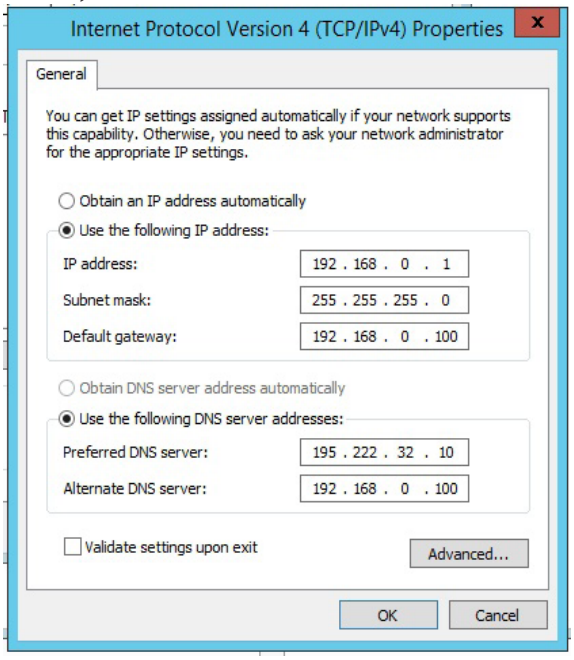


In order to demonstrate the operation of group policies, we will use Windows Server + Windows 10. Precondition for the operation of group policies is the implementation of Active Directory, adding computers into domain and the correct configuration of network settings. We will implement DHCP server onto VM, set address of class C 192.168.0.2 – 192.169.0.52.

IMPLEMENTATION OF INFRASTRUCTURE

In the following chapter we will present realized configuration, in order to get functional environment. Firstly, we will present Windows Server which works as a Domain server, next DHCP server which assigns IP addresses to the clients, and then the example of operation of group policies.
After we have installed Windows Server 2012 R2, we have configured the static IP addresses, as on the following Figure.

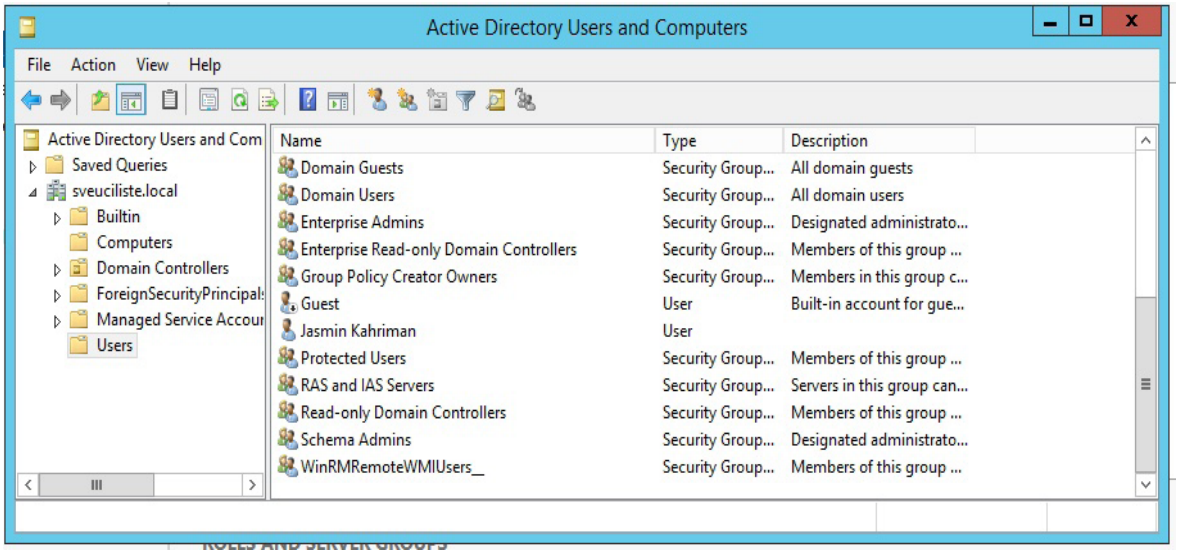
Figure 2. Review of network settings of Win Server, AD DS



Computer name: AD
IP server: 192.168.0.1/24
Added roles: Active Directory Domain Services
Domain name: sveuciliste.local

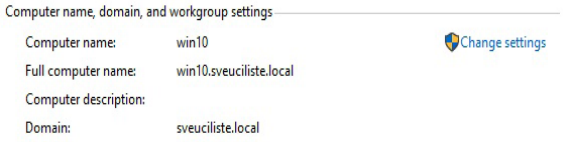
During the installation of Active Directory Domain Services, a global catalogue will be created, within which will be placed all objects we will work with (computers, users, OU, groups...). Necessary service for work of domain server is DNS server, which will be installed automatically, unless we configured it previously. After the installation of AD DS, we will reset the server and create a new domain user, as well as the new computer. Creation and manipulation of objects will be done through ADUC (Active Directory Users and Computers).

Figure 3. The list of users in the domain



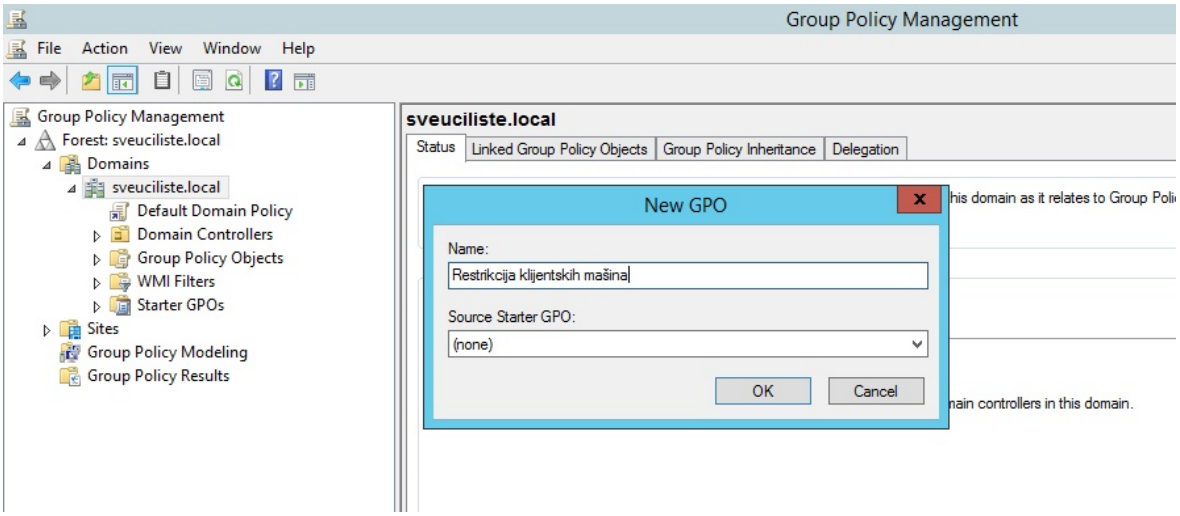
After this, it is necessary to change computer name into "Win10" and Domain name into "sveuciliste.local", reset the computer and log onto it with domain account, which we created in Active Directory, namely "jasmin.kahriman".

Figure 4. Review of settings Windows 10 (computer name, domain)



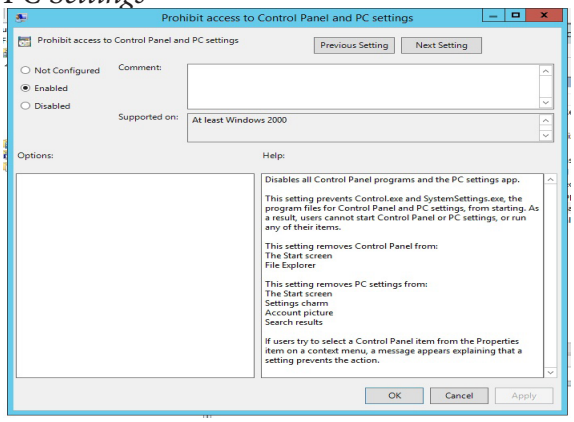
After we have configured everything, we will perform an example of implementation of group policies, which will, let us say, block Control Panel, block Lock taskbar, and block access to the partition C. We will access to GPMO (Group Policy Management Object) on the server where ACDS is installed.

Figure 5. Group Policy Management



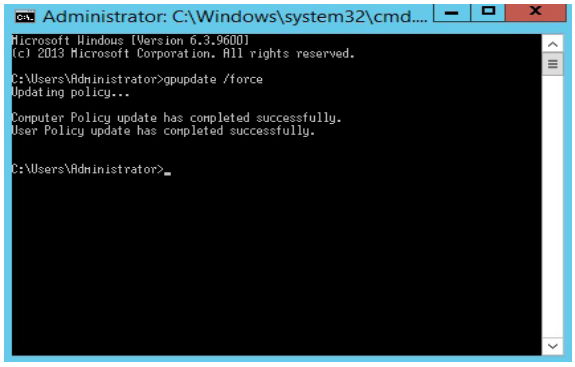
The restrictions which we will implement include: Prohibit access to Control Panel and PC Settings, Lock the taskbar, Prevent access to drives from My Computer.

Figure 6. Prohibit access to Control Panel and PC Settings



After all this, on the server we will open CMD and enter gpupdate /force, in order to forward group policies onto the client devices:

Figure 7. Forced update of group policies through CMD



THE RESULTS

If we click onto Windows logo – Settings, nothing will open, because the Control Panel has been blocked. If we search for "Control Panel" within the Search option, with the intention of opening it, we will receive an error, as shown on the Figure.

Figure 8. Prohibit access to Control Panel and PC Settings

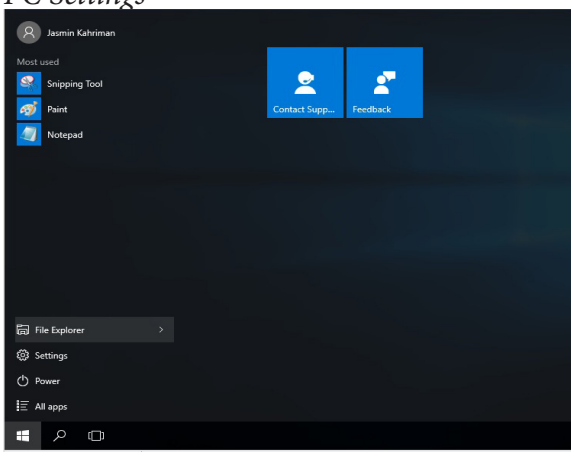
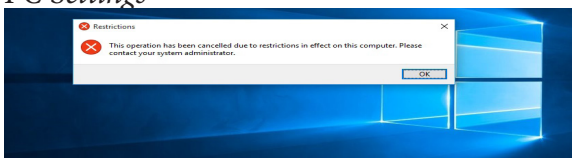
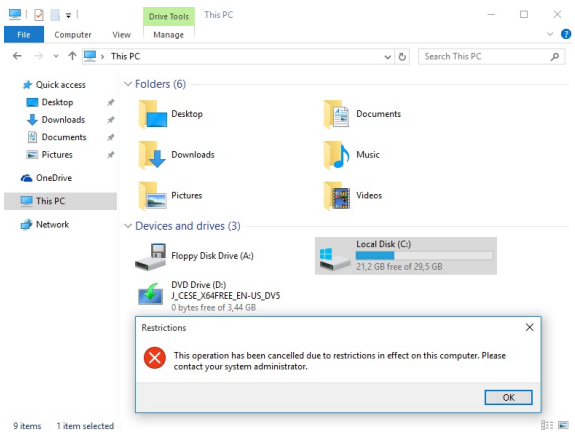


Figure 9. Prohibit access to Control Panel and PC Settings



If we attempt to lock the taskbar, we will not be able to do that, since the Administrator disabled this option. Since we have blocked the access to the partition C, domain user will not be able to access and manipulate the files.

Figure 10. Prevent access to drives from My Computer



CONCLUSION

The concept of server is nowadays often attributed to expensive computers with expensive operating systems which almost no one can access, because they are highly important. The server is a computer in your IT system which is connected to the network, and which enables certain services to other computers within the network. The domain represents centralized management of objects and the possibility of automatism of process and actions over those processes. If all client computers needed to be administered manually, the price of ownership of those computers would increase enormously, even so much that it is completely unacceptable. In order to solve this problem, organizations need to transfer from manual processes and to establish automatic and centralized form of administration of changes and management of user and computer settings within the environment, by using AD and group policies.

This paper was based on the implementation of the domain, as centralized management place of client devices. The total realization of infrastructure was realized through the usage of Microsoft solutions, Windows Server 2012 R2 and Windows 10. We have created a virtual company "University" which has 2 servers and 50 client devices. We have created one domain server, DHCP server and joined Windows 10 to the domain. By using group policies, we have implemented the following restrictions: Prohibit access to Control Panel and PC Settings, Lock the taskbar, Prevent access to drives from My Computer. In the end, we have demonstrated Windows 10 with implemented restrictions.

LITERATURE

[1] http://www.amazon.com/HP-Proliant-Server-2x2-5GHz-Processors/dp/B0096CMENO
[2] http://www.amazon.com/HP-Recline-23-k310-23-Inch-Touchscreen/dp/B00NAWDHGE/ref =sr_1_sc_2?s=electronics&ie=UTF8&qid=1438362878&sr=1-2-spell&keywords=hp+aioc
[3] http://www.hill2dot0.com/wiki/index.php?title=Image:G2003_SIP-Server-Types.jpg (01.03.2017.)
[4] http://www.link-university.com/lekcija/Pogled-na-grupne-polise/3809
[5] https://smist08.wordpress.com/2013/06/01/pulling-my-hair-out-over-gpo/
[6] http://windows.microsoft.com/hr-hr/windows7/what-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup
[7] http://www.2bi.me/blog27.html