STUDY GUIDE FOR MODULE NO. LAB F14

Active Directory

MODULE OVERVIEW

This module provides a comprehensive overview of Active Directory (AD), a core component of Microsoft's Windows Server operating system. Participants will gain a deep understanding of the fundamental concepts, architecture, and functionalities of Active Directory, empowering them to effectively design, deploy, and manage AD infrastructures within organizational environments. Through a combination of theoretical learning and practical demonstrations, learners will explore key topics such as directory services, domain controllers, forests and domains, organizational units (OUs), group policies, user and group management, authentication mechanisms, and integration with other IT services.

MODULE OBJECTIVE

1. Understand the core concepts and principles of Active Directory, including its role as a centralized directory service for managing network resources and user identities.
2. Explore the architecture of Active Directory, including the structure of domains, forests, and trust relationships, and learn how to design an AD infrastructure that aligns with organizational requirements.
3. Learn how to deploy and configure domain controllers, domain services, and related components to establish a robust Active Directory environment.
4. Gain proficiency in user and group management within Active Directory, including account creation, delegation of administrative tasks, and implementation of security policies.
5. Master the use of Group Policy Objects (GPOs) to enforce system configurations, security settings, and software deployment across AD domains and organizational units.
6. Understand various authentication mechanisms supported by Active Directory, such as Kerberos authentication and LDAP queries, and learn how to configure authentication protocols for secure access control.
7. Explore advanced topics such as Active Directory Federation Services (AD FS), Lightweight Directory Access Protocol (LDAP) integration, and Active Directory Certificate Services (AD CS), and understand their roles in enhancing AD functionality and interoperability.
8. Learn best practices for monitoring, troubleshooting, and maintaining an Active Directory infrastructure to ensure optimal performance, reliability, and security.

LEARNING ACTIVITY 1

Name: Cerujano, Erman Ace M. Due date: May 06, 2024

LAB 14

Building an Active Directory Infrastructure for ermancerujano, Corp.

SETTING UP THE LAB

1. Computer Equipment Needed

Item	Minimum	Recommended
Computers	(3) Pentium I 133 MHz	(3) Pentium II 300MHz or greater
Memory	128 MB	256 MB
Hard Drive	2 GB	4 GB or larger
NIC	1/Machine	1/Machine
Hubs	1	1
Network Cable	(3) Category 5 Cables	(3) Category 5 Cables

2. Computer Configuration Overview

Computer Number	1	2	3
Computer Name	Server1	Server11	Client1
IP Address	192.168.1.201/24	192.168.1.211/24	192.168.1.1/24
OS	Windows Server 2003	Windows Server 2003	Windows XP Pro
Additional Configurations	SP1	SP1	SP2

3. Detailed Lab Configuration.

COMPUTER 1

Computer 1 will be named **Server1** and the operating system on this computer will be **Windows Server 2003 Standard or Enterprise**. You should also install **Service Pack 1** to avoid any unforeseen problems. If you do not have a copy of Windows Server 2003 you can obtain an evaluation copy of Windows Server 2003 Enterprise within the Microsoft Press series of books, and Service Pack 1 is available for download on Microsoft's Website.

Server1 will have a Static IP address of **192.168.1.201** with a **255.255.255.0** subnet mask. The default gateway field can be left blank but you should enter this computer's own IP address for the Preferred DNS field (**192.168.1.201**). The alternate DNS Server field can be left blank.

COMPUTER 2

Computer 2 will be named **Server11** and **Windows Server 2003** (either version once again) will be install on this computer with **Service Pack 2**. Server11 will have a static IP address of **192.168.1.211** with a **255.255.255.0** subnet mask. The default gateway field can be left blank but you should configure the preferred DNS server setting to point to Server1, **192.168.1.201** and leave the alternative DNS setting blank.

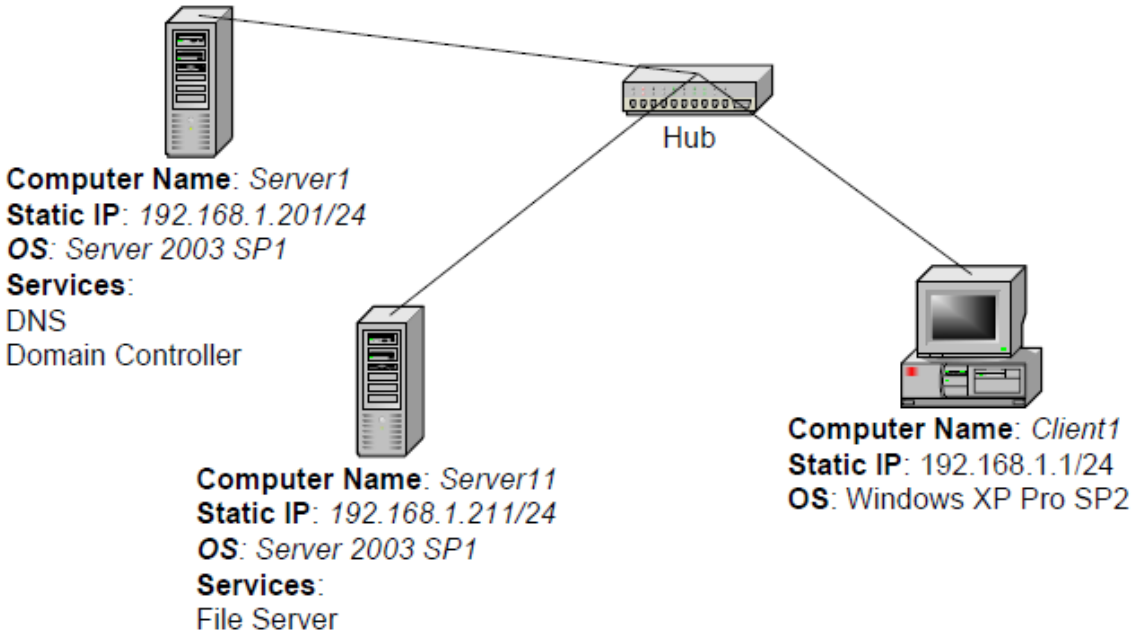
COMPUTER 3

Computer 3 will be named **Client1** and have **Windows XP Professional** insgtalled as the operating system. Client1 will have a static IP address of **192.168.1.1** with a **255.255.255.0** subnet mask. The default gateway field can be left blank but you should configure the preferred DNS server setting to point to Server1, **192.168.1.201** and leave the alternate DNS setting blank.

IMPORTANT

You should test the network connection (using the PING command) between each of these machines to ensure that your network is set up properly. Testing before you get started will save you major time and effort later. To be able to PING computer 3, the Windows XP machine, you will have to either turn off the Windows Firewall or allow incoming echo requests in Windows Firewall. This can be done by **right click the network connect** → **properties** → **Advanced Tab** → **Settings**. This opens the Windows Firewall. Now you much click on the **Advanced Tab** → in the IMCP box you will click **Settings** and make sure the box next to **Allow Incoming Echo Requests** is checked. Click **OK** three times to get back out of the properties.

LABORATORY SETUP



LAB 14.1

Creating an Active Directory

Contents:

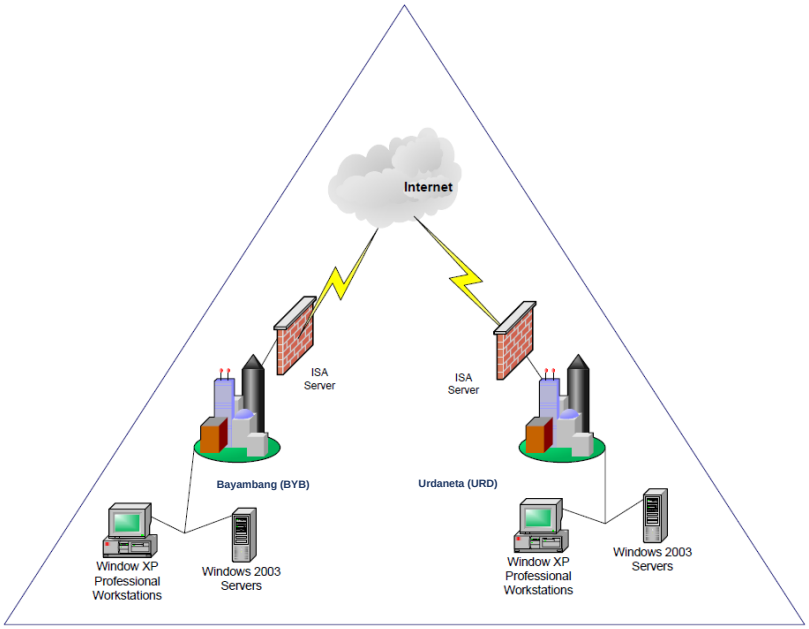
SCENARIO PART ONE

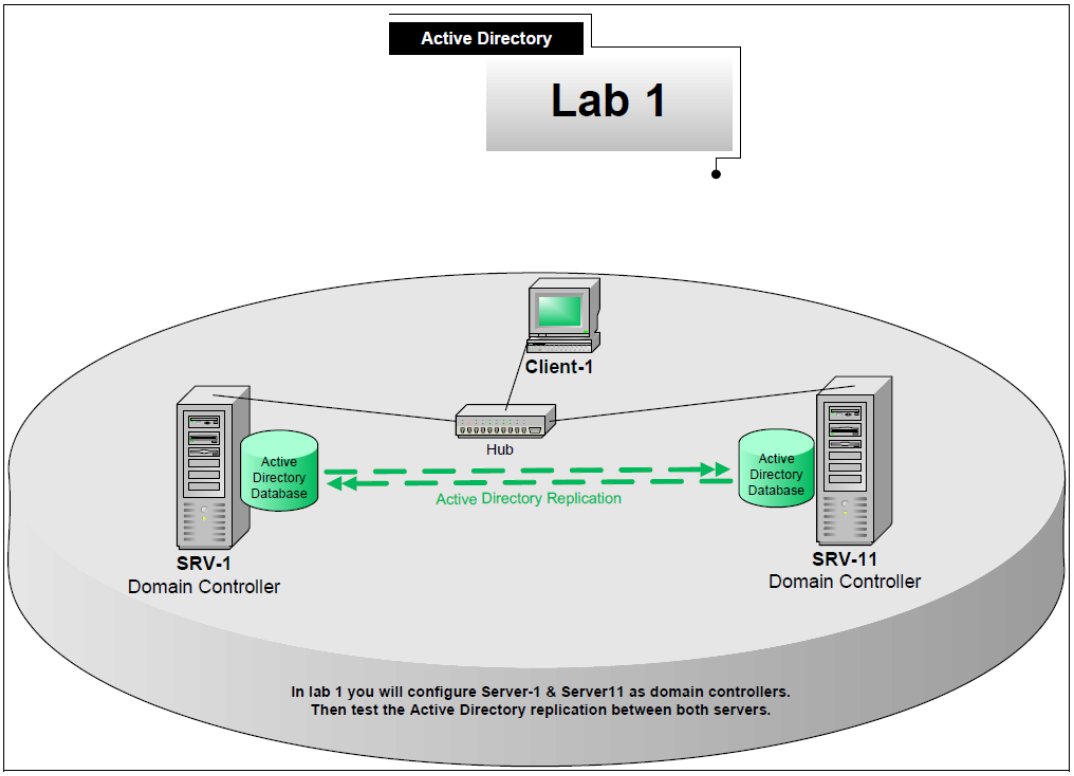
Erman Cerujano., is a manufacturer of gourmet products that are sold internationally. They are in the process of migrating their network from Novell to Windows Server 2003 as well as replacing all of their current servers with new equipment. Their main headquarters is located in Bayambang Pangasinan and they have a manufacturing facility in Urdaneta City Pangasinan. The Bayambang Pangasinan Office is connected to the Internet with a full T1 (1.544 Mbps) and Microsoft's ISA Server (firewall) will protect the internal network. The facility in Urdaneta City is used to manufacture ice cream and ship to Ermancerujano East distributors. The Bayambang Pangasinan office has five servers that have just been purchased; all will be running Windows Server 2003 and also 25 workstations that will be running Windows XP Professional. The Urdaneta City location has five new servers that were recently purchased, all running Windows Server 2003 and 45 workstations, all running Windows XP Professional. Urdaneta City is connected to the Internet with a Fractional T1 (768 Kbps) and they also use ISA Server to protect their internal network. The two locations will be connected together through a VPN that is formed between the two ISA Servers over the Internet.

Ermancerujano has hired you on a contract basis, to help with the implementation of a new pristine Windows Server 2003 domain. You have been given the tasks of installing the first domain controller on the network at the Bayambang Pangasinan office, which will install Active Directory and create a new domain for Ermancerujano. You are also in charge of making sure that all client computers, which have been installed, are able to join the new domain. The Operation Manager, Erman, also mentions that there is an opportunity for you to become a full time administrator with the company, if the project goes well.

In this lab, you will create a new domain for Ermancerujano. Called ermancerujano.com, by building the first domain controller on the network using the Active Directory installation program. You will then configure DNS to work with Active Directory and test that it is working properly on the network using the NSLOOKUP utility. Once your domain controller is working properly, you will join a Windows Server 2003 and a Windows XP Professional machine to the domain. Finally, you will create a second domain controller on your domain and test replication between the two domain controllers.

ermancerujano.com





BUILDING AN ACTIVE DIRECTORY INFRASTRUCTURE

ACTIVE DIRECTORY

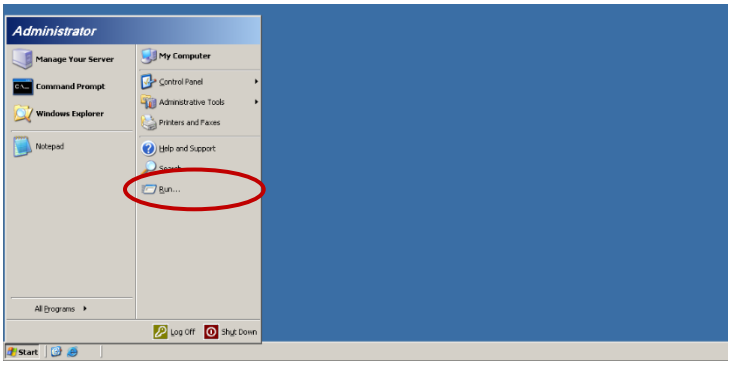
Active Directory is a new feature in Windows 2000 that allows users to logon and access resources from anywhere in the network. It allows administrators to manage the network from a single location and makes network security much easier to manage. Active Directory is really a database that stores information about all objects on the network. Think of Active Directory as a phone book for the network. For example, if you needed to find a resource on the network but you can't remember where it is located, you can do a search in Active Directory to find that resource. Resources include users, groups, computers, printers, and shared folders, to name a few. The Active Directory database is stored on Windows 2000 servers known as Domain Controllers. All of the domain controllers within a domain hold the same copy of the Active Directory database, in a file named NTDS.DIT. Windows 2003 domain controllers are multi-master replication partners, all replicating data back and forth to each other.

LAB 14.1. CREATING AN ACTIVE DIRECTORY

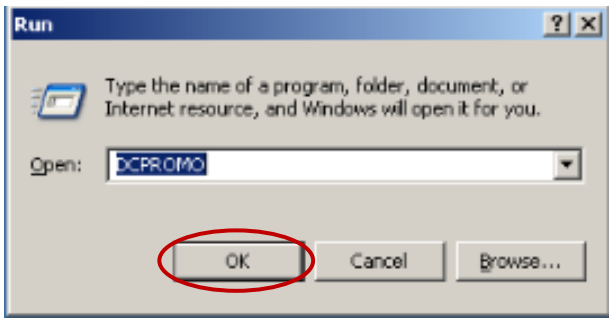
1.1. Install Active Directory

Log on to **Server1.**

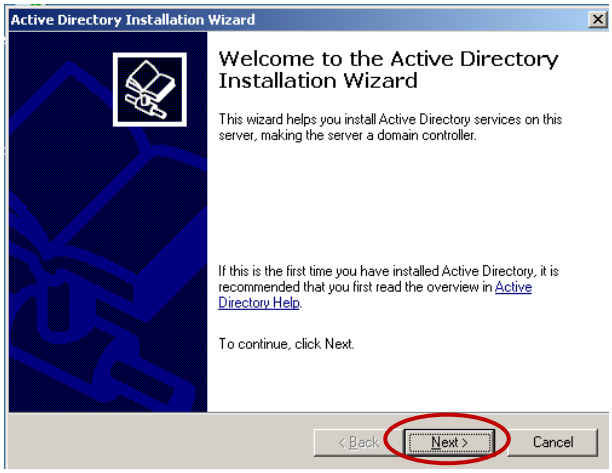
Open the run command. From the desktop click on **Start** then **Run.**



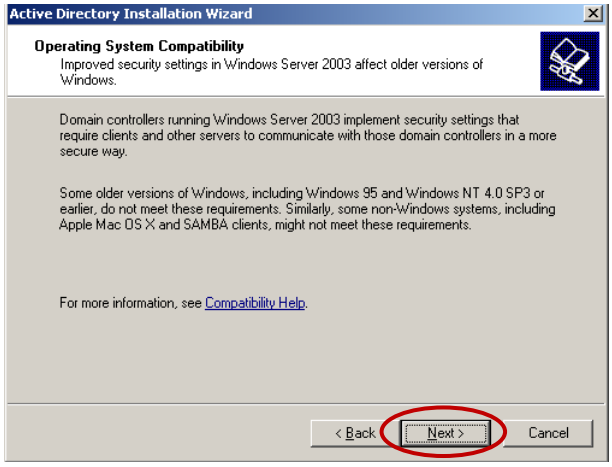
Type in **DCPROMO** in the run command and click **OK**.



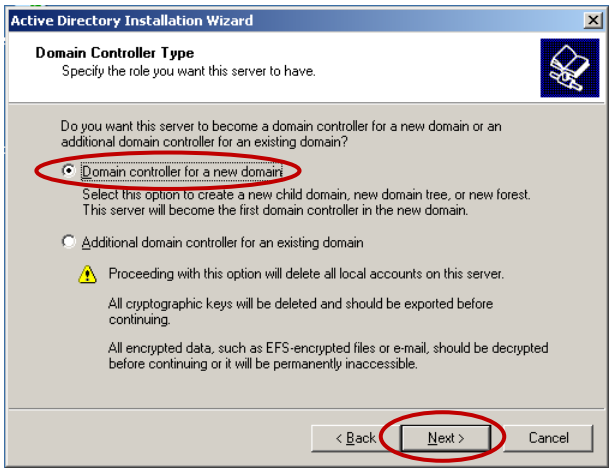
This will begin the Active Directory Installation Wizard. The first screen to appear is the welcome screen, click on **Next** to continue.



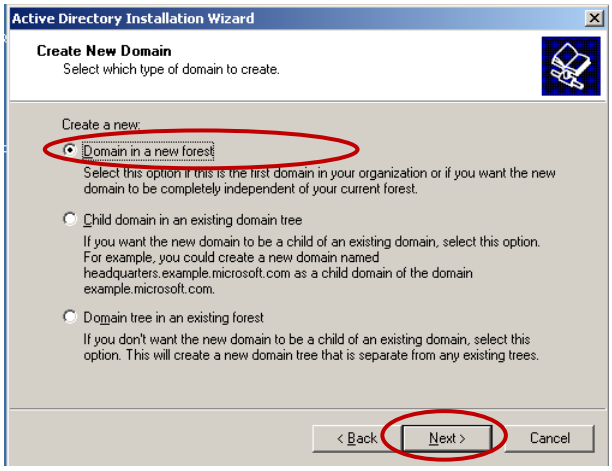
The next screen will inform you about Compatibility issues with older Domain Controllers. Click **Next**.



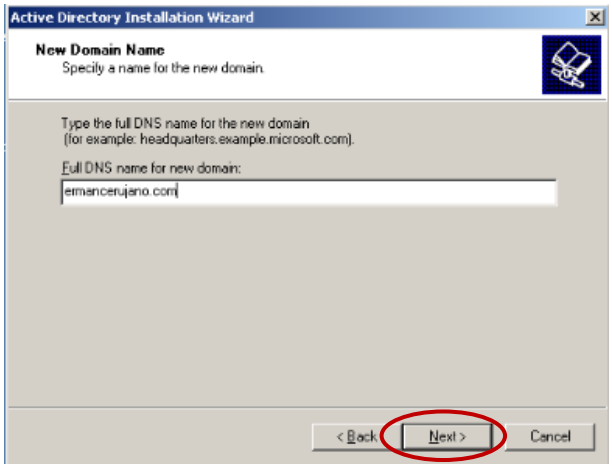
The Domain Controller Type Window will ask you for the type of domain controller you would like to install. You have two options; one is to install this as the first domain controller for a new domain or as a additional domain controller for an already existing domain. This is the first domain controller on the network, select **Domain controller for a new domain** and click **Next**.



The next screen combines two of the screens for Windows 2000. On this screen you will specify whether you want to create a new domain in a new forest, create a new child domain in an existing domain tree, or create a new domain tree in an existing forest. In Windows 2000/Server 2003 you can build domain trees so that the domains are in a hierarchy, for domains to be in a tree they must have a contiguous (continuous) namespace. The first domain in a tree is known as the root domain and any child domains in the tree will have to contain the name of the root domain. for example Cerujano.com may have a child domain for a Chicago office with the name of Erman.cerujano.com and would be considered part of the domain tree because it has the contiguous namespace of the root domain, cerujano.com. Remember, that this is the first domain controller on the network, so it will be the "root" domain of a new tree. Select **Domain in a new forest** click **Next**.

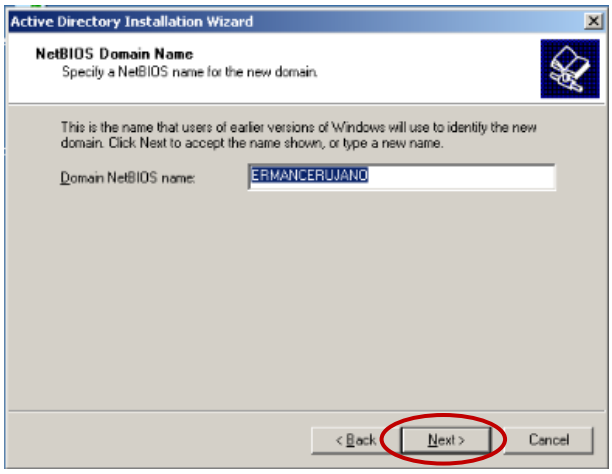


The next screen will ask you to specify the full DNS domain name for your new domain. You do not have to use your company's registered public (Internet) domain name here, but you can if you would like. For this lab, type in **ermancerujano.com** and click **Next**.

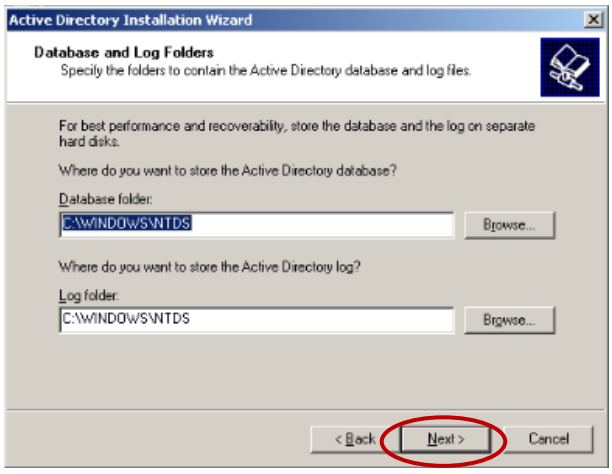


The next screen will ask you to specify the NetBIOS name for the domain. This is the domain name that legacy systems (anything before Windows 2000) and applications that only support NetBIOS will use. The main difference is that NetBIOS domain name can only contain up to 15 characters with no periods. By default the wizard will suggest a name for you, based on the domain name you entered earlier, only now it will use the NetBIOS name rules. In this case, it should come up as **ERMANCERUJANO**. You can modify this name if you would like, but it would most likely lead to

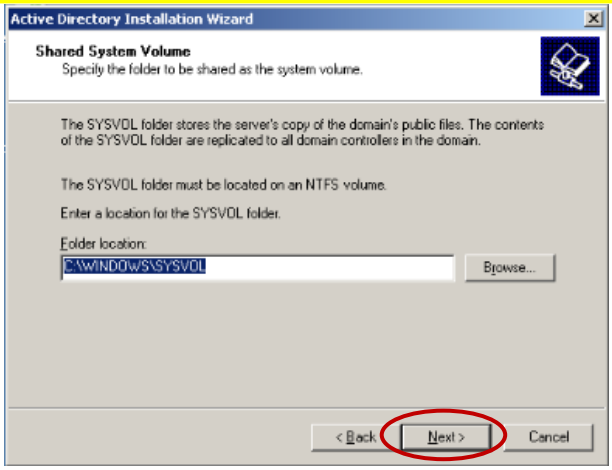
confusion down the road, as you domain will effectively have two names. Leave the default name, **ERMANCERUJANO**. Click as **Next**.



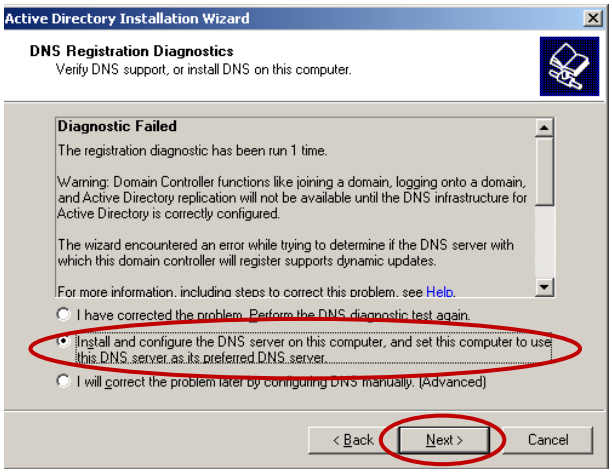
The next screen will ask where you want to place the Active Directory database and log. It's recommended in a production environment, that you place the log file on a separate physical hard drive to increase the performance of Active Directory. This is optional for the lab, if you do not have two physical hard drives you can leave it at the default setting which will be the **%systemroot%\WINNT\NTDS** for both the database and the log, or **c:\WINNT\NTDS**. Click **Next**.



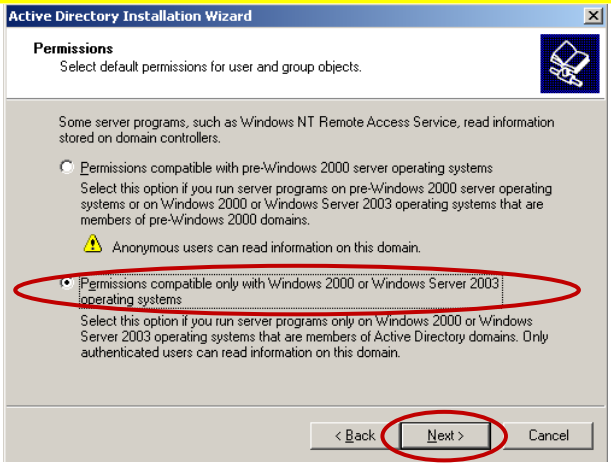
For the Shared System Volume folder stores the server's copy of the domain's public files. The contexts of the SYSVOL folder are replicated to all domain controllers in the domain.



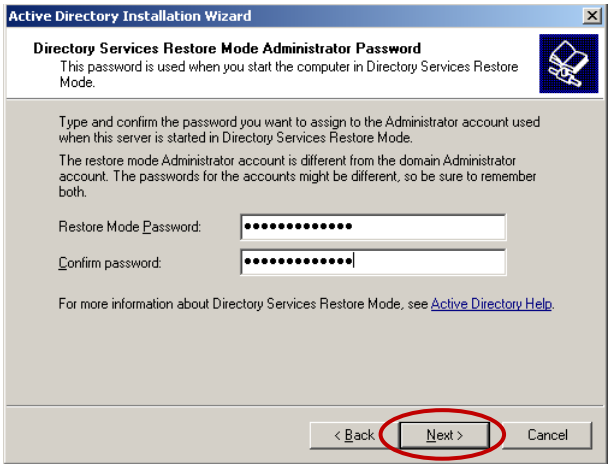
The DNS Registration Diagnostics dialog box will appear and tell you the wizard was unable to find the DNS server that handles the name **ermancerujano.com** and then ask you if you want to run the diagnostic again, install and configure DNS on that server, or correct the problem later. Active directory was designed to work with DNS and will not function without a DNS server that handles name resolution for the domain. Select **Install and Configure the DNS server on this computer…** and click **Next**.



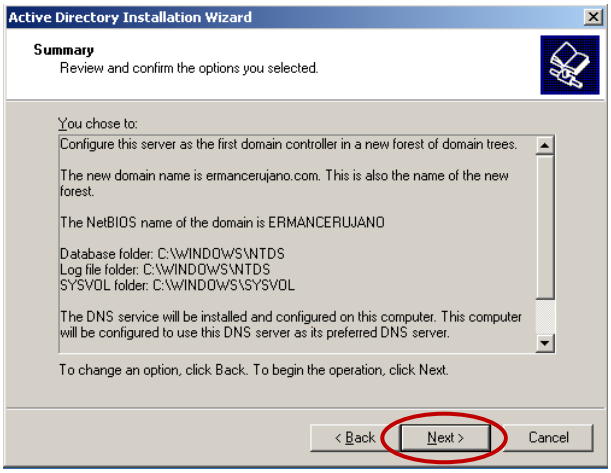
The next screen will ask you what the default permissions should be for users and groups. The first option is for permissions compatible with pre-Windows 2000 servers. This setting will loosen up security a little, but it will allow NT 4.0 RAS servers and other programs to be able to authenticate users. The second option is for permissions compatible only with Windows 2000 or Windows Server 2003 operating systems. This will give you tighter security but will not work with any NT 4.0 RAS servers and can cause problems within NT 4.0 domains. There are no NT 4.0 servers of any kind in the network, nor do you ever plan on having any on the network, so you may choose the second option for **Permissions compatible only with Windows 2000 or Windows Server 2003 operaing systems** and click **Next**.



The next screen will ask you for a directory services restore mode administrator password. This password is used to protect against anyone other than an administrator from rebuilding the Active Directory Database from the directory service restore mode. this password is different from any logon password and should be a different from the administrator's logon password in case the administrators' account gets compromised. Type in **Password1** as the password and click **Next**. Passwords are case sensitive.



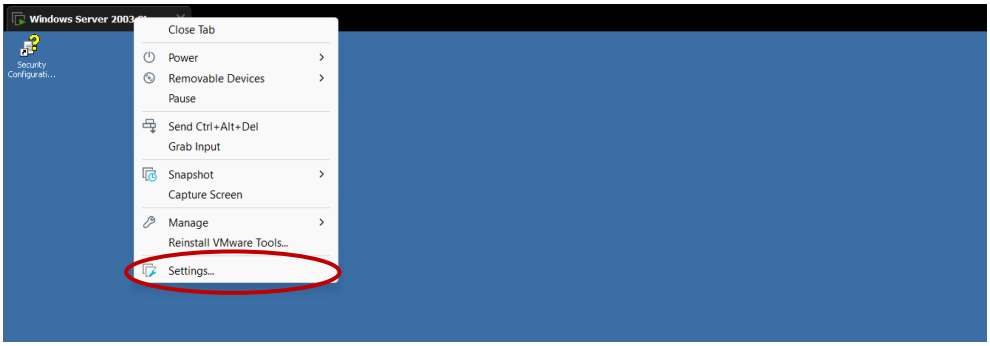
The next screen will give you a summary of all the information you entered in the wizard. Review and confirm that everything is correct and click **Next** to start the Active Directory Installation.



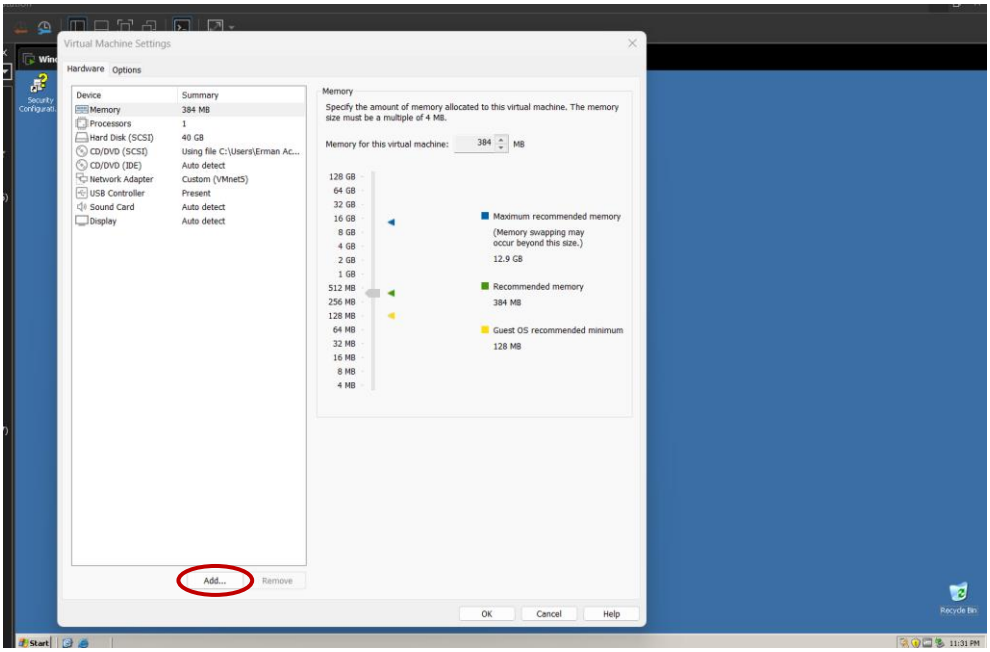
You may be asked for the i386 folder during the installation of DNS, so you should have the Windows Server 2003 Server CD-Rom handy. The installation should take about 15-30 minutes.

To install the CD Drive containing the Windows Server 2003 ISO. Right click on to your Server in the VMware.

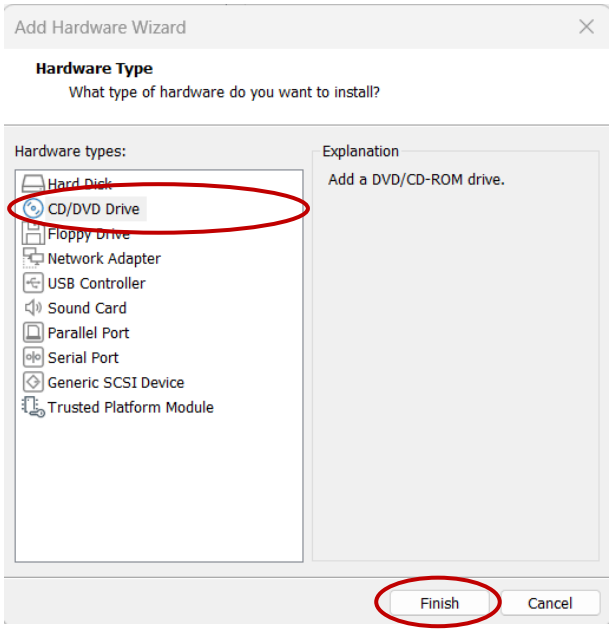
Then select the Settings.



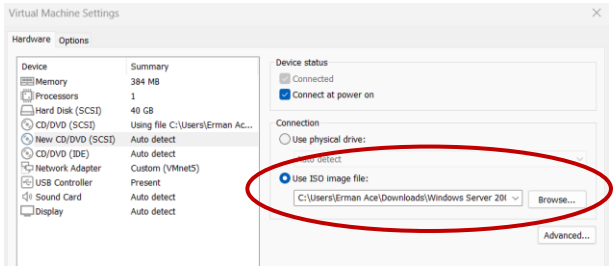
Select the **ADD** button below.



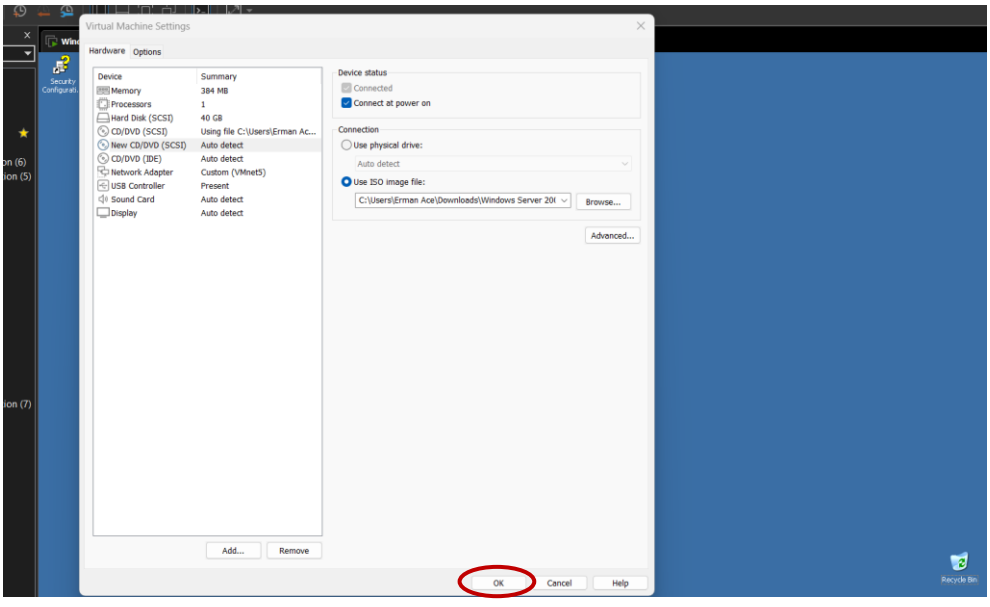
Then select **CD/DVD Drive** and click **Finish**.



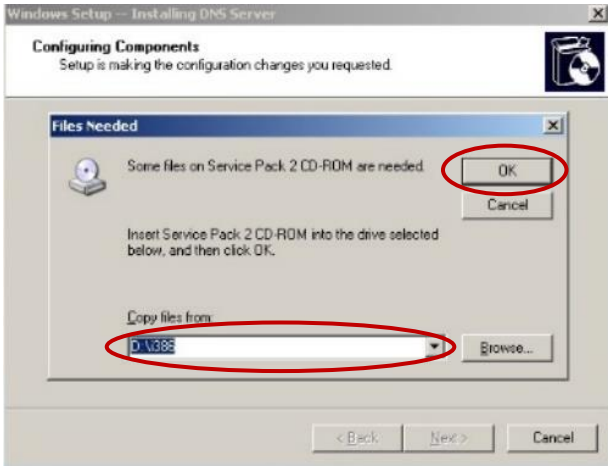
And on the **New CD/DVD**. In the connection section select the **Use ISO image file** and insert the Windows Server 2003 ISO.



Then click **OK**.



Find the directory of the New CD/DVD Drive and click **OK**.



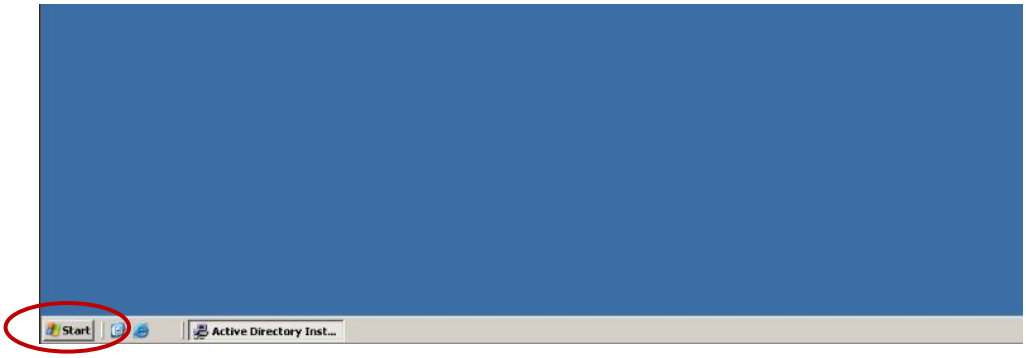
You will eventually get a screen letting you know the installation is done. Click on **Finish**.

You will see a dialog box appear telling you that the server must be restarted before the changes made by the Active Directory installation wizard take effect. Click **Restart Now** for the computer to restart.

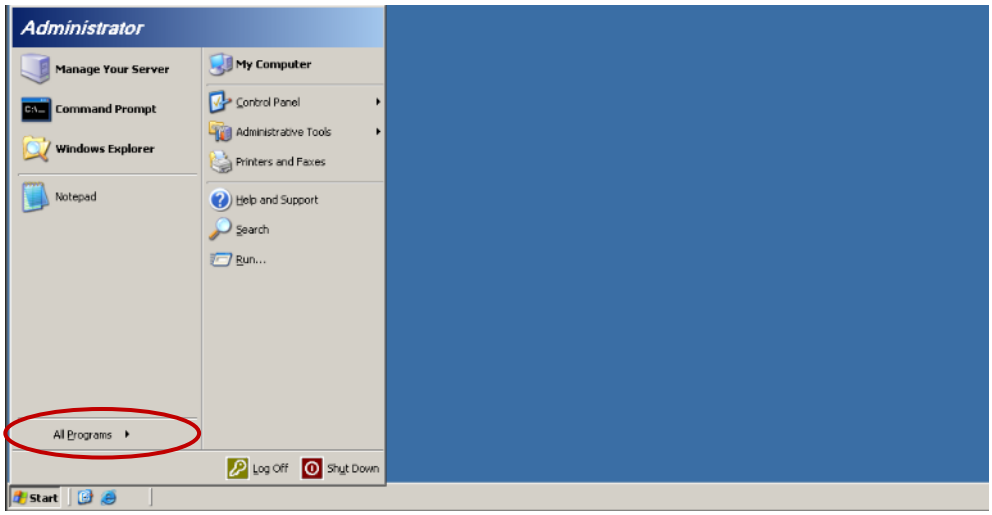
1.2. Configure and test DNS for Active Directory

When the server restarts, log on as administrator and open the DNS management console.

- Go to **Start**

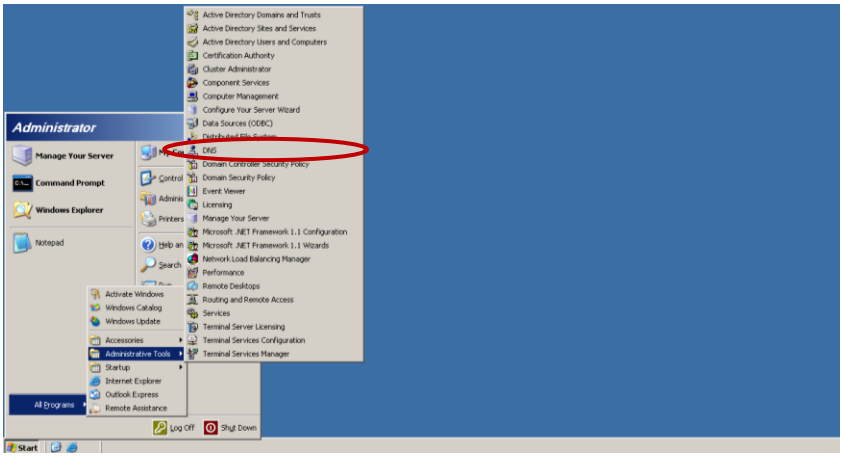


- **All Programs**

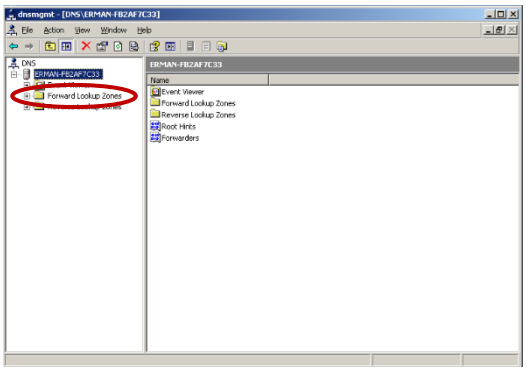


- **Administrative Tools**

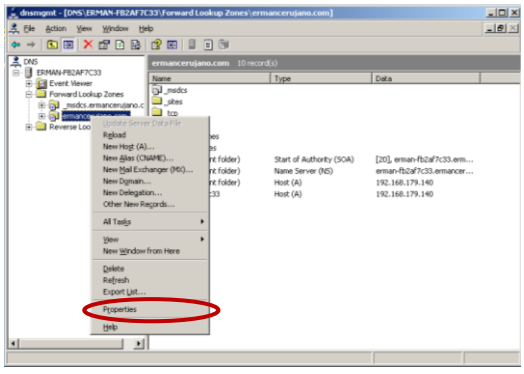
➢ **DNS**



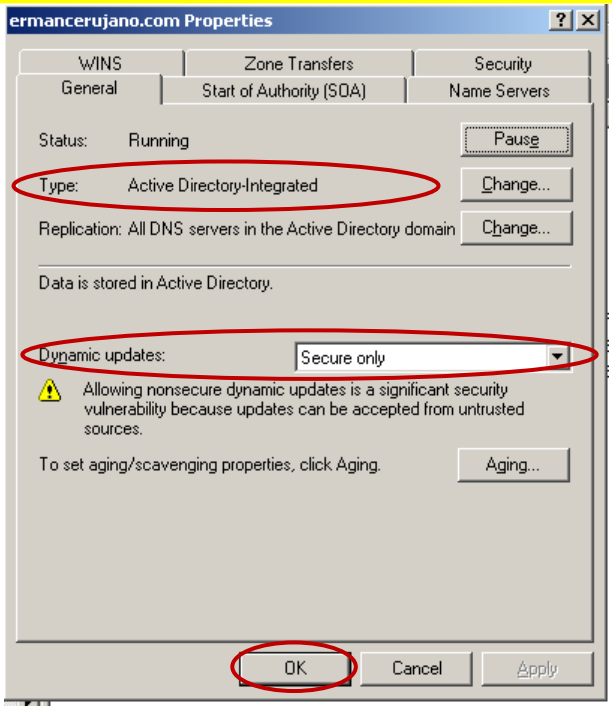
In the left pane open **Server1**, then open **Forward Lookup Zones** folder and find the zone for **ermancerujano.com** check to make sure there is a host entry for Server 1.



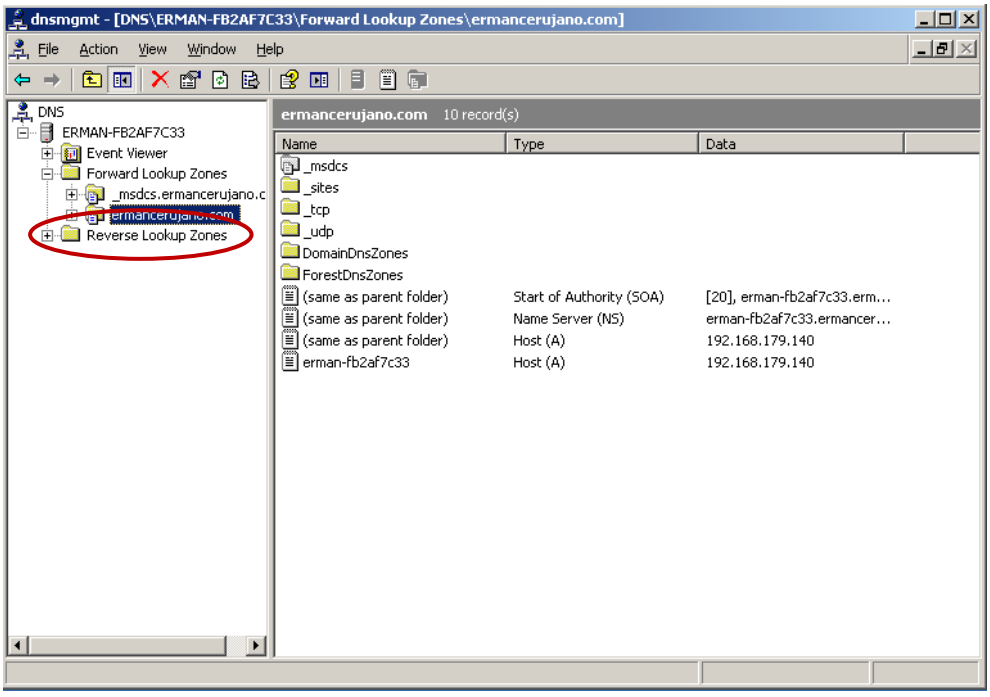
Right click on the **ermancerujano.com** and select **Properties**.



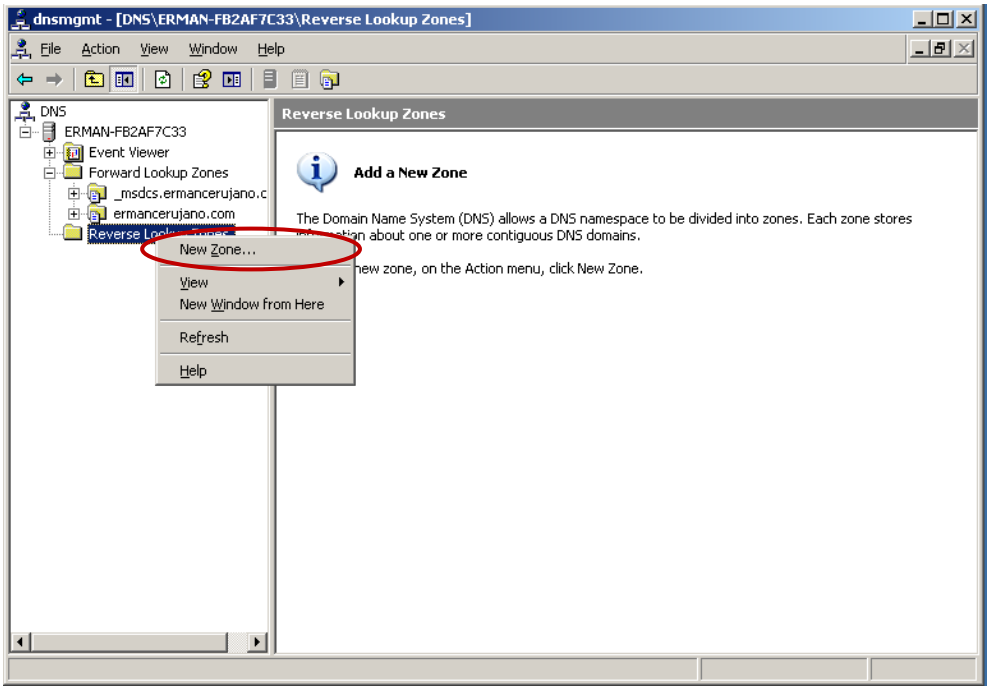
Here you can see that when DNS is installed automatically through the Active Directory installation wizard, the zone type is set to **Active Directory-Integrated** and dynamic updates are set for **Only Secure Updates** by default. Click **OK**.



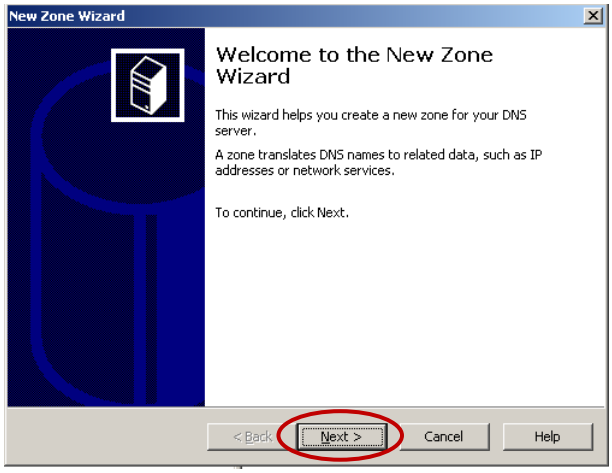
Now you will need to create a reverse lookup zone for the ermancerujano.com network. The reverse lookup zone is needed in order to use the NSLOOKUP utility to test that DNS is working properly and troubleshoot any problems that may arise. Right click on the **Reverse Lookup Zones** folder.



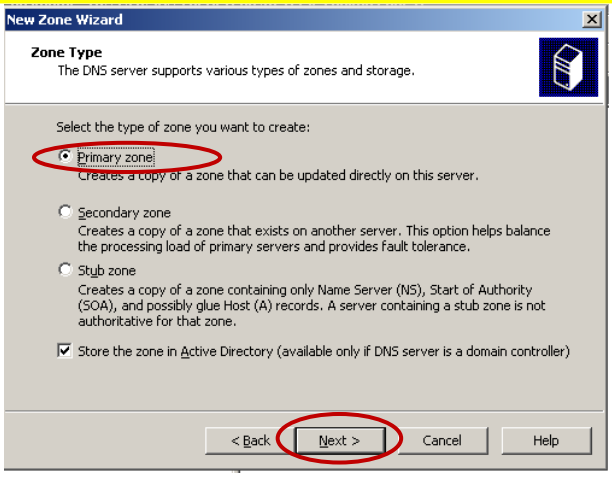
Select **New Zone** and the Reverse lookup zone wizard will start.



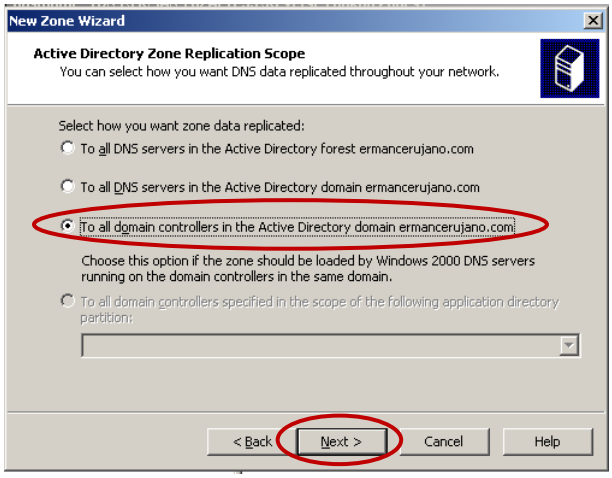
The first screen is the welcome screen, just click on **Next**.



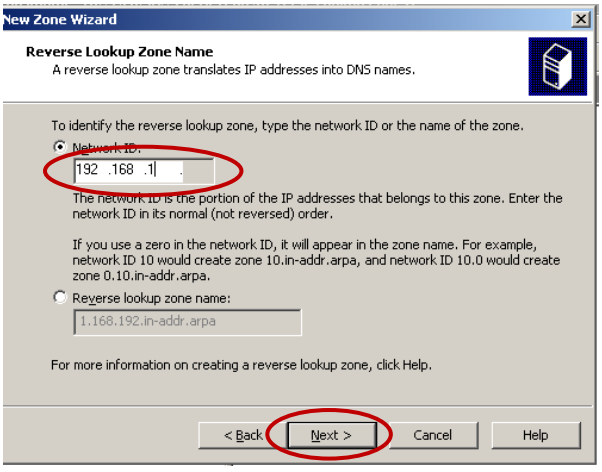
The next screen will ask you to specify the type of zone you want to create. Choose the same type of zone that the forward lookup is set to. Select **Primary Zone** and make sure **Store the zone in Active Directory** is **checked**, click **Next**.



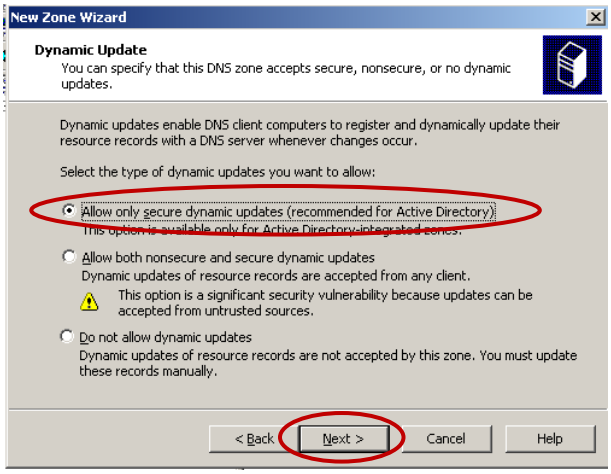
The next window asks how you would like this zone to be replicated. You will select **To all domain controllers in the Active Directory domain ermancerujano.com** and click **Next**.



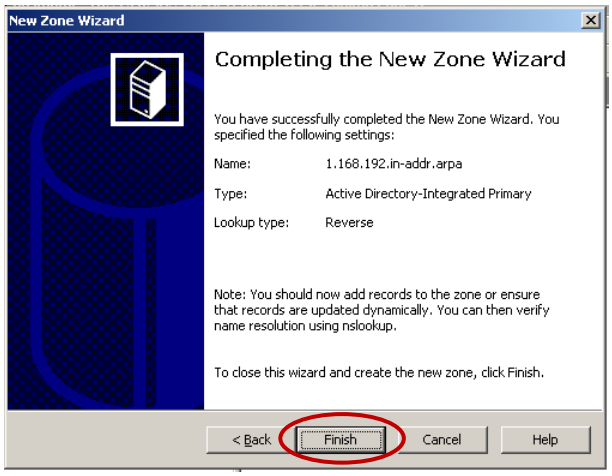
The next screen will ask you to specify the Network ID for the reverse lookup zone. Type in the network **ID 192.168.1.** and click **Next**.



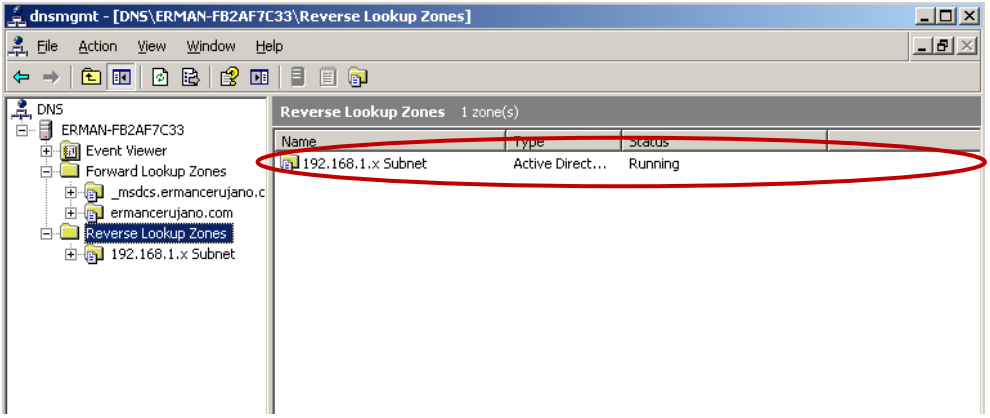
The final thing you are prompted for is Dynamic Updates. You will want to select **Allow only secure dynamic updates** and click **Next**.



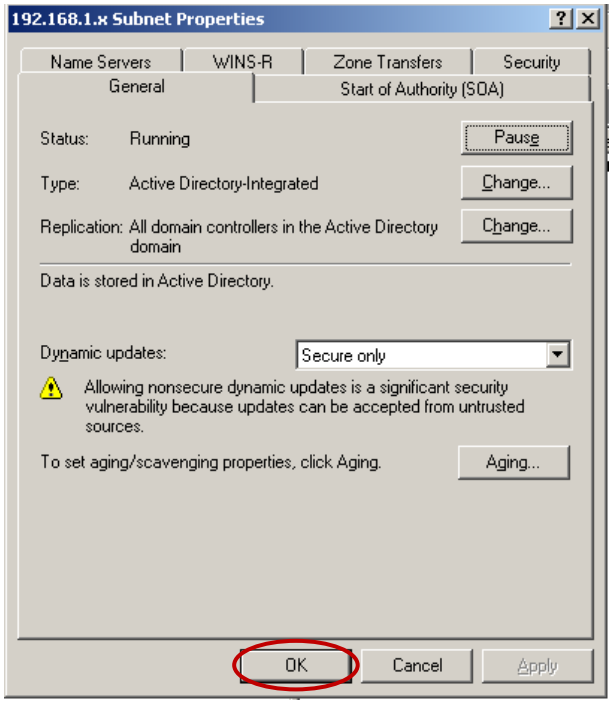
The last screen will show a summary of all the information you entered on the wizard, confirm that it's all correct and click **Finish** to create the reverse lookup zone.



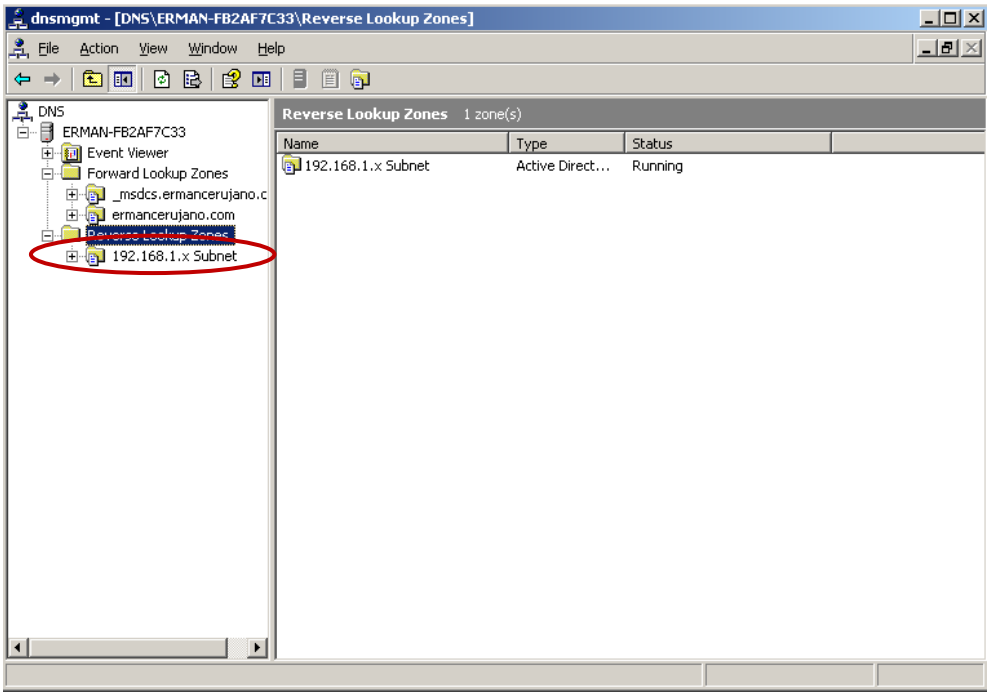
On the DNS console, open the **Reverse Lookup Zones** folder and you should find the zone, **192.168.1.x Subnet**.



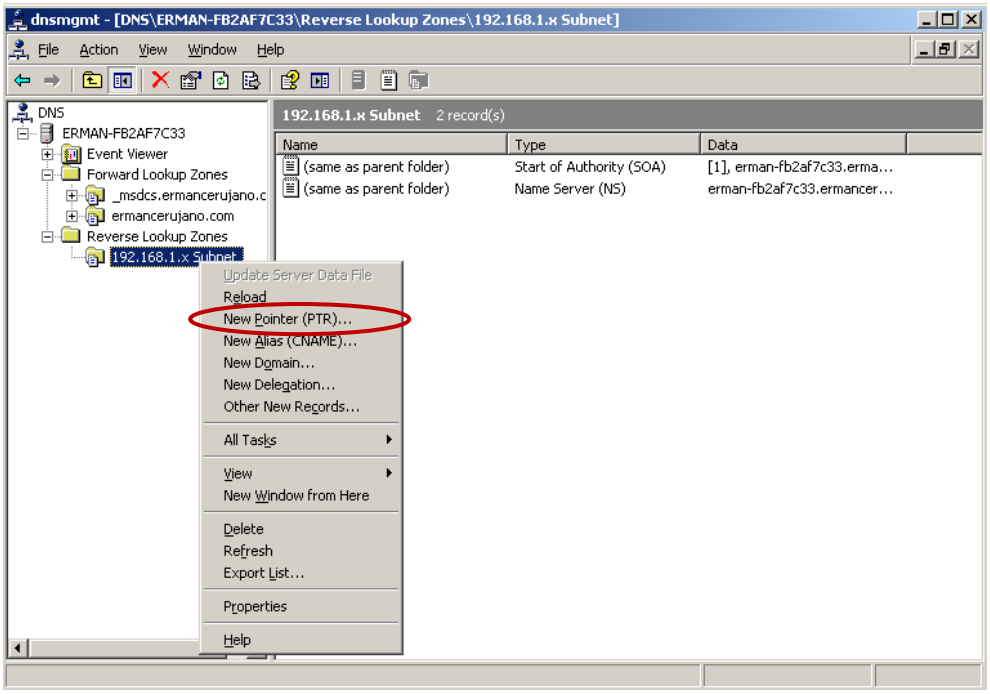
Open the **Properties** of the zone to confirm that the zone type is set to **Active Directory Integrated** and dynamic updates are set to allow **only secure updates**. Close the **Properties**.



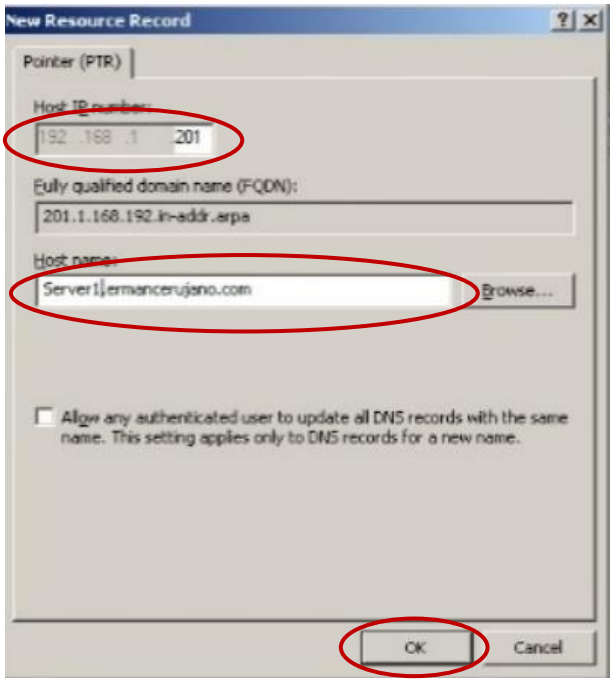
The next step is to create a pointer record for **Server1**, this should be the only pointer record you will have to create manually because any other clients that support dynamic updates will automatically update and create their own host and pointer records. Server1 did not update or create a pointer record automatically because there was no reverse lookup zone available when the host record was originally created. Right click on **192.168.1.x Subnet**.



Select **New Pointer (PTR)**.

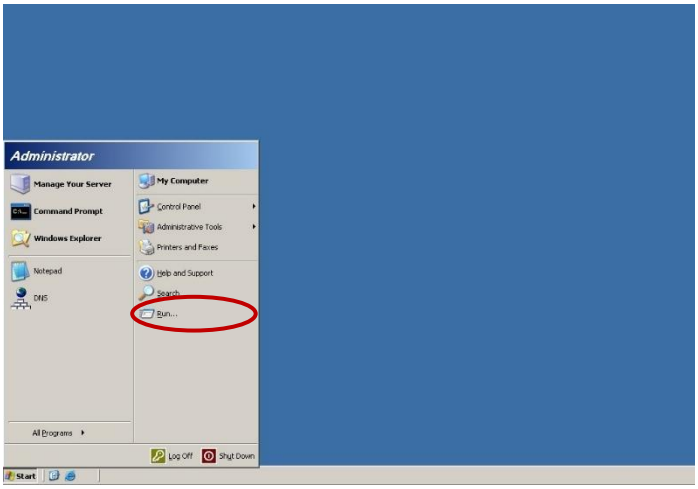


A dialog box will appear asking you for the Host IP address and Host name of the Pointer record. Type in **201** for the host IP number and **Server1.ermancerujano.com** for the host name then click **OK**.

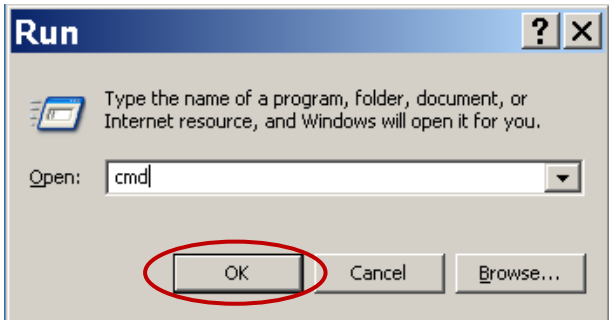


On the DNS console, you should now have a pointer record for **192.168.1.201**. Close the DNS Console.

From the desktop, open the command prompt;
Go to **Start** → **Run**.

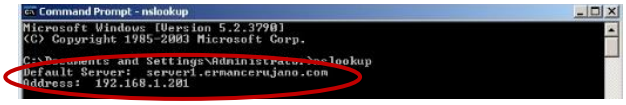


Type in **CMD** and click **OK**.

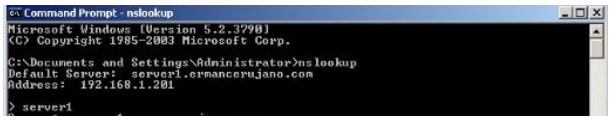


On the command prompt type in **NSLOOKUP** and press **Enter**.

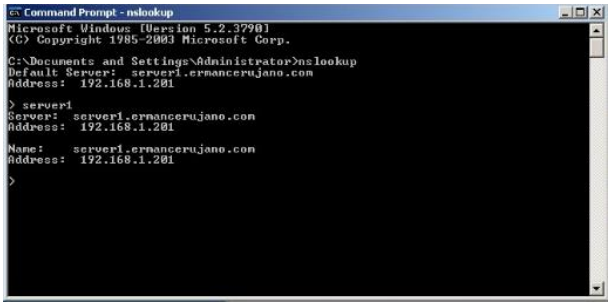
The NSLOOKUP utility will look for the DNS server on the network and return the host name and IP address of the server. You should have the default server **Server1.ermancerujano.com** and an IP address of **192.168.1.201** appear. You may now type in any host name and NSLOOKUP will query the preferred DNS server to resolve it to an IP address. Try resolving the host name for Server1.



Type in **Server1** (name of your server) and press **Enter**.



You should get the full DNS name and IP address of the DNS server and underneath it will appear for the full DNS name and IP address of the DNS server and underneath it will appear the full DNS name and IP address of the queried host.



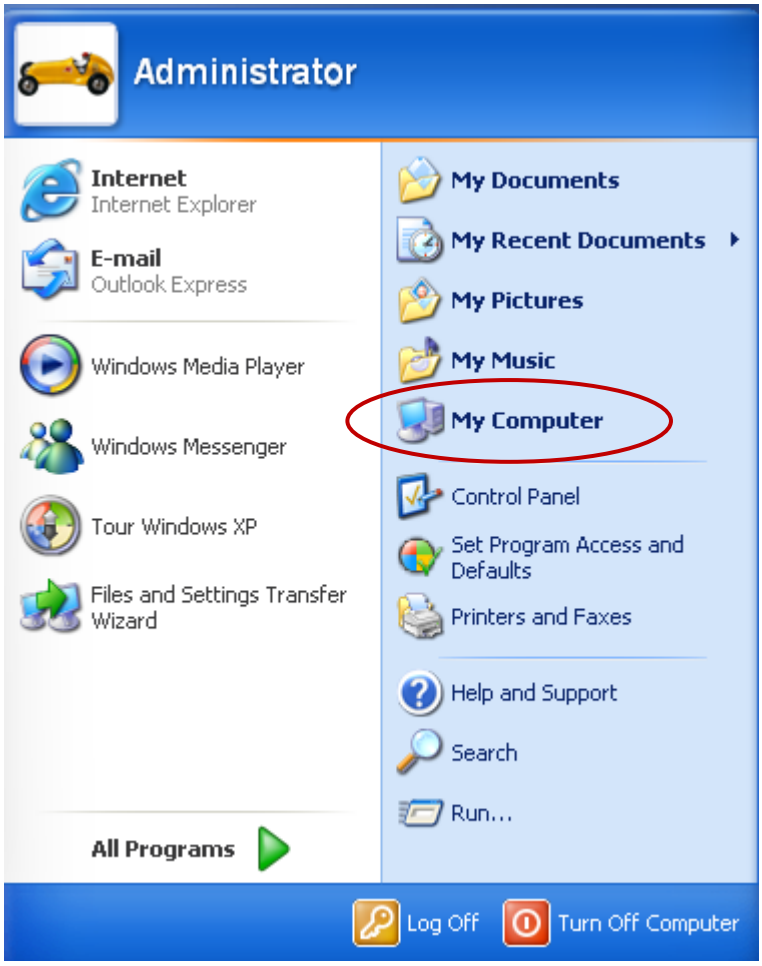
Type in **Exit** and press **Enter** to exit NSLOOKUP. Then type **Exit** and press **Enter** again to close the command prompt.

1.3. Join Clients and Servers to the Domain

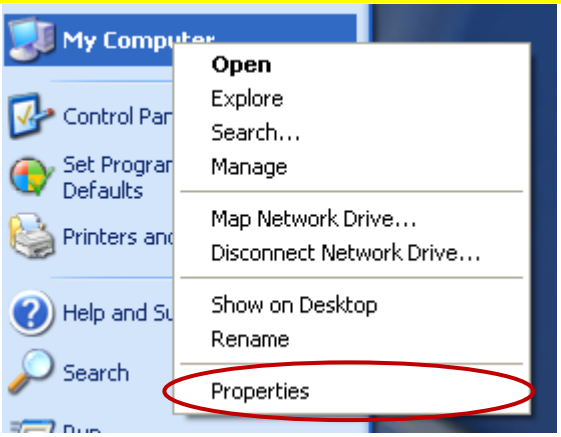
Log on to client1 and open the network identification tab from the System Properties. To do this, just go to the

- start menu.

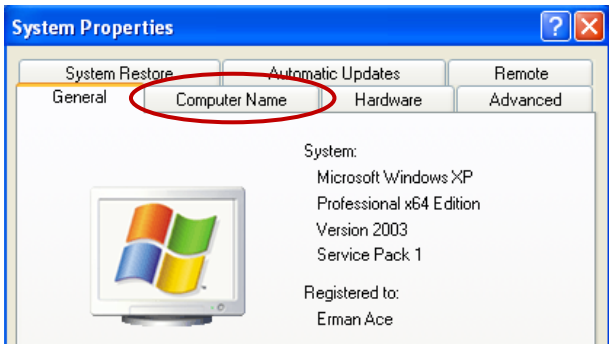
- right click on **My Computer**



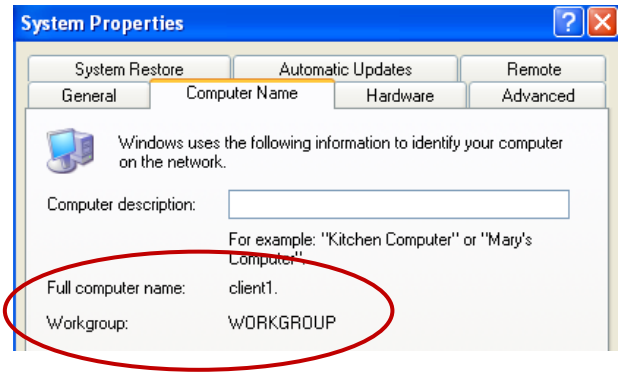
- select **Properties**.



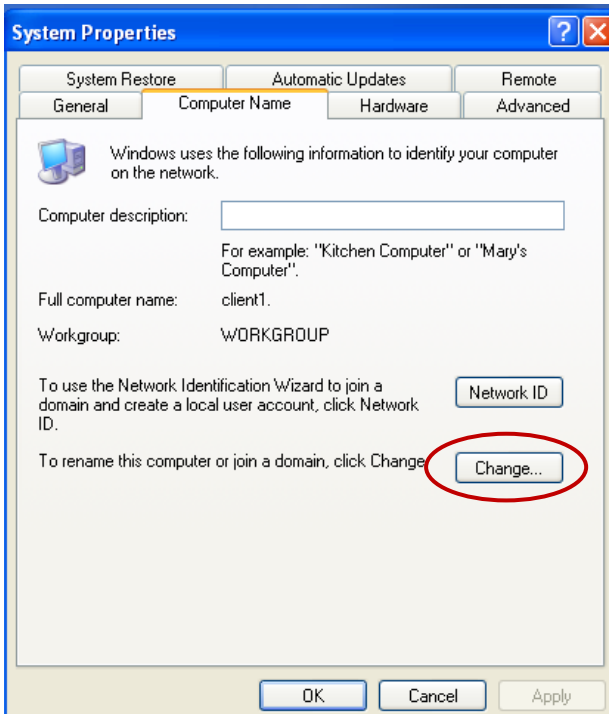
- On properties page select the **Computer Name** Tab.



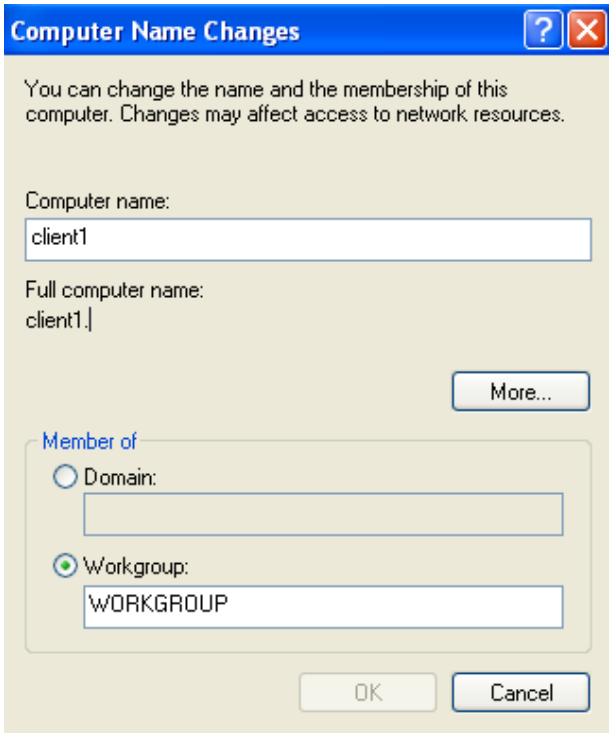
- You will see that the full computer name is **client1** and it is currently a member of the workgroup named **workgroup**, which is the workgroup that **Windows Server 2003** computers join by default unless otherwise specified during the installation.



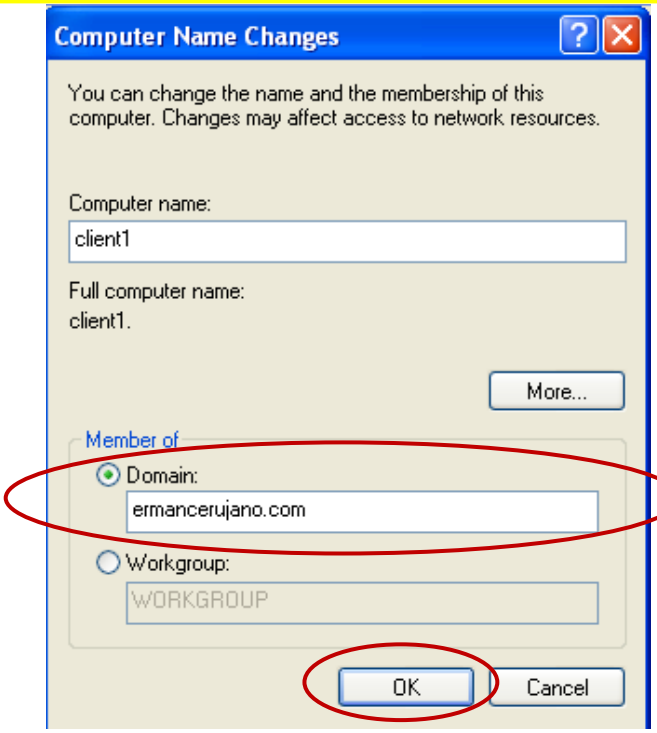
- We need to change the Network ID Information, to do that you just need to click on the **Change Button**.



- On the Computer Name Changes page you can change the computer name and the domain or workgroup that the computer is a member of.

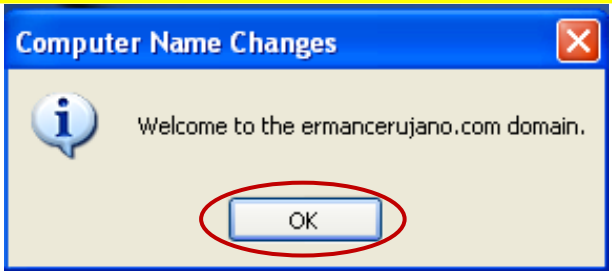


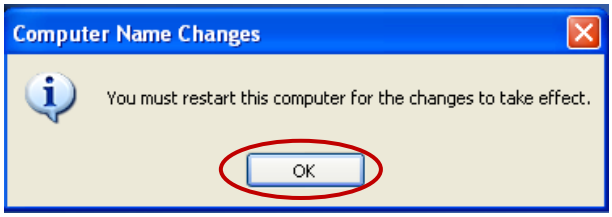
- Leave the computer name as **client1**, for the member of option select **domain** and type in **ermancerujano.com**.

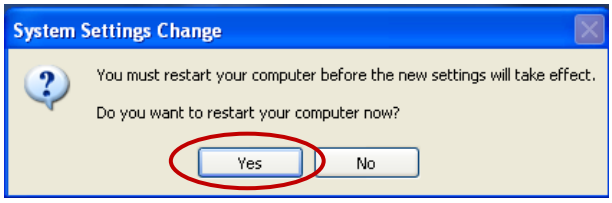


- Click **OK** and you will be prompted to enter a username and password of an account that has permission to join computers to the **ermancerujano.com** domain. Enter the **domain administrator's username** and **password** for the **ermancerujano.com** domain and click ok.

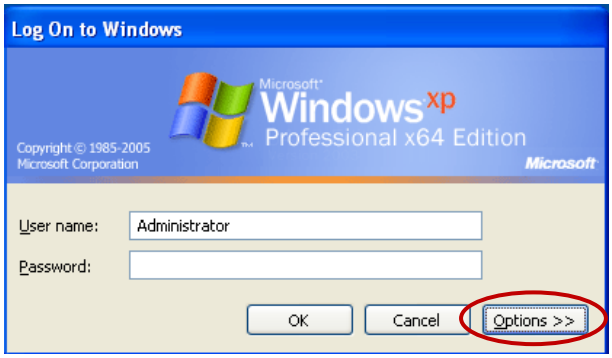
- After you enter the name and password you should get a dialog box welcoming you to the **ermancerujano.com** domain. Click **OK** and you will get a couple more dialog boxes saying that you must reboot the computer for changes to take effect. Click **OK** and **Yes**



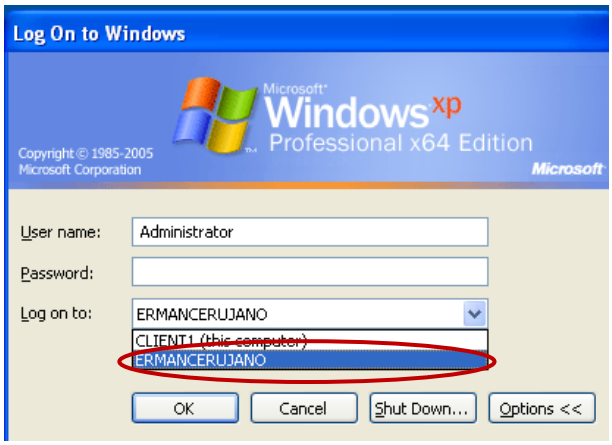




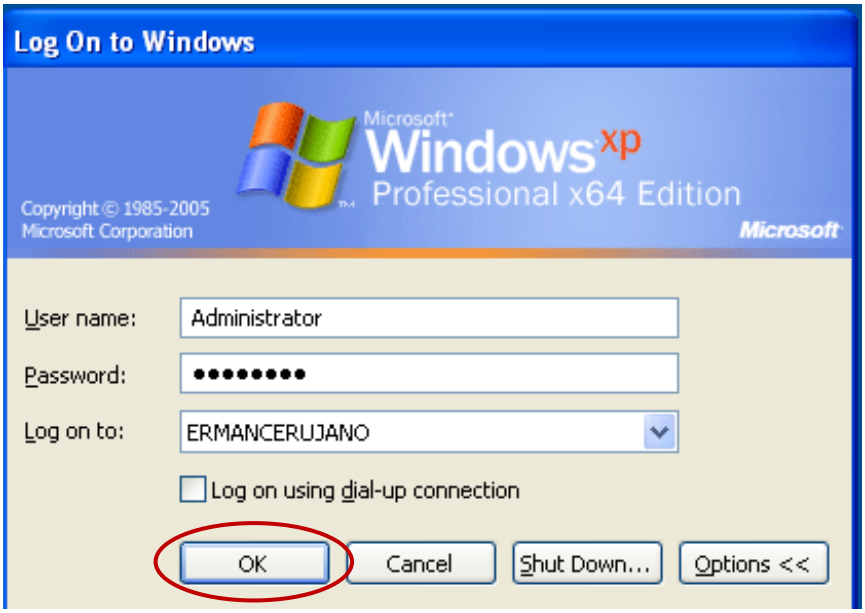
- When the computer restarts make sure, you change the **log on to** dialog box to **ERMANCERUJANO**. To do that, click the options>> button



Then select the **ERMANCERUJANO** in **log on** to:

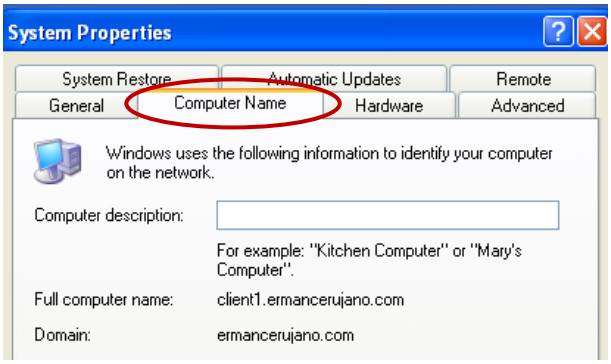


- Use the administrative account from the domain (right now this may be the same username/password as your local administrator account, but it is important to distinguish the two) to logon to the **ermancerujano.com** domain.



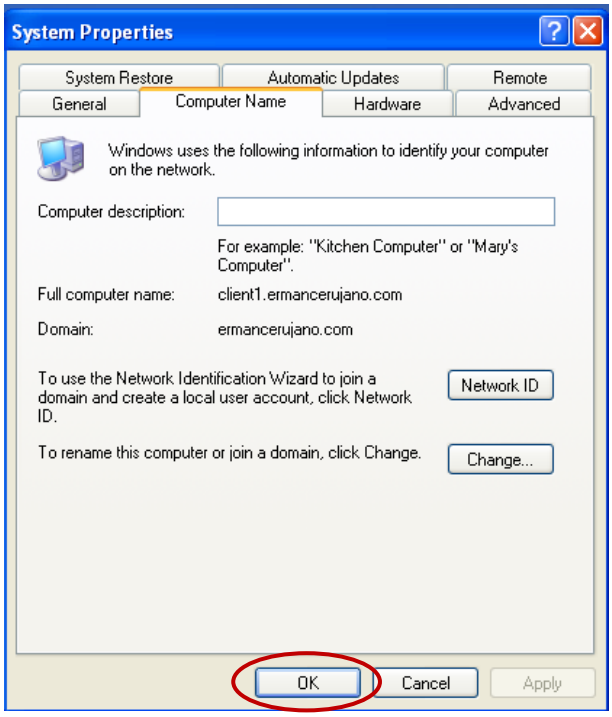
- Once you logon, open the **system properties**.

- Select the **Computer Name**.



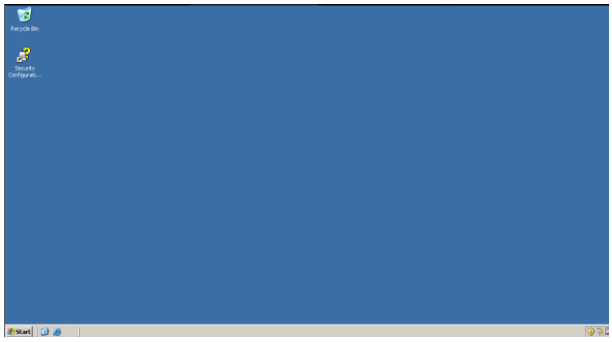
You should now see the full computer name as **client1.ermancerujano.com** and the domain as **ermancerujano.com.**

- Click **OK.**

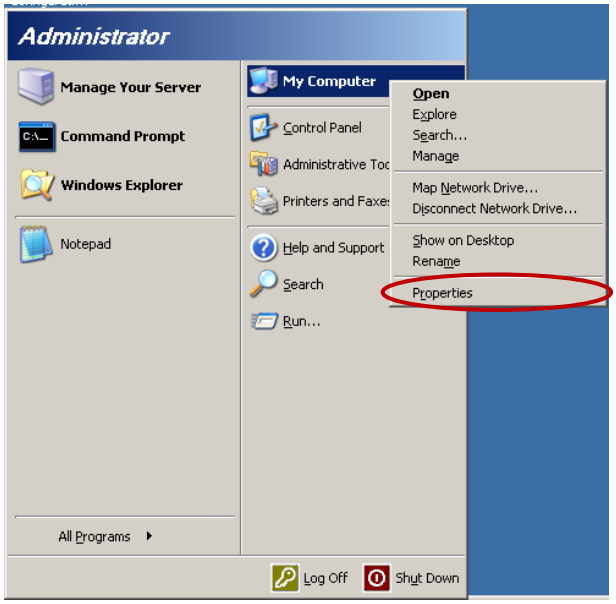


- **Log off client 1**.

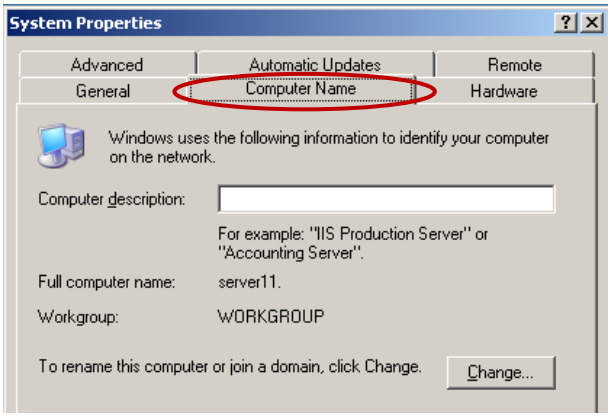
- The process of joining computers to the domain is the same for Windows XP Professional and Server 2003. Now log on to Server11 and make it a member server of the **ermancerujano.com** domain by using the same steps that you used to join the Windows XP Professional computer, client1, to the domain.
  - ➢ Open your Server11.



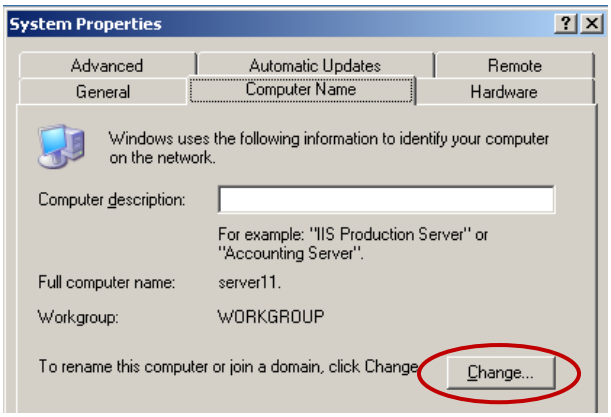
  - ➢ Go to System Properties



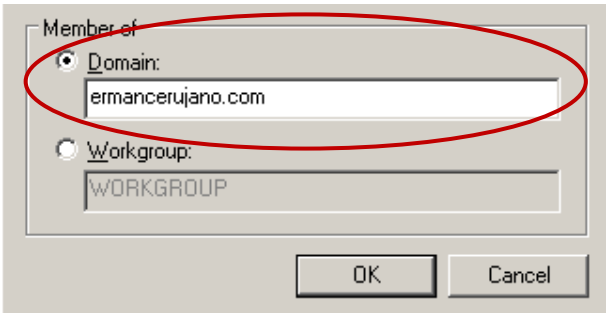
- Go to **computer name tab**.



- Click **change**.

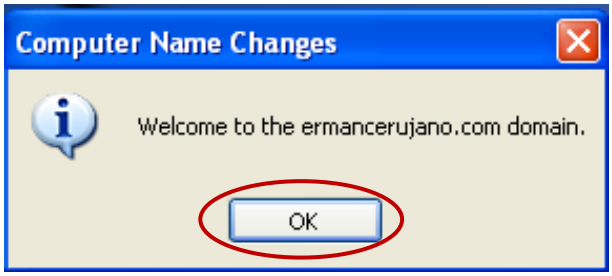


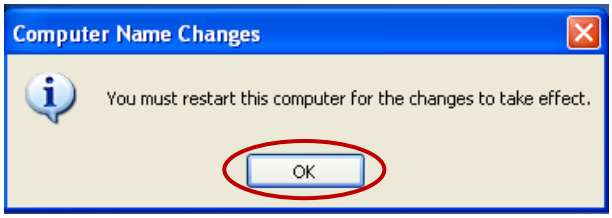
- Select the **domain** and enter **ermancerujano.com**.

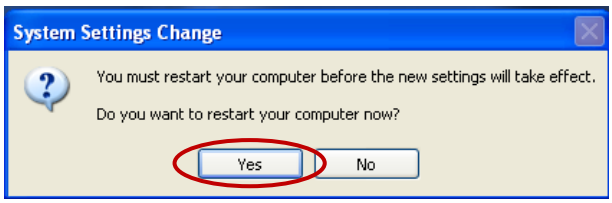


- Enter the domain **administrator's username** and **password** for the **ermancerujano.com** domain and click **OK**.

- After you enter the name and password you should get a dialog box welcoming you to the **ermancerujano.com** domain. Click **OK** and you will get a couple more dialog boxes saying that you must reboot the computer for changes to take effect. Click **OK** and **Yes**







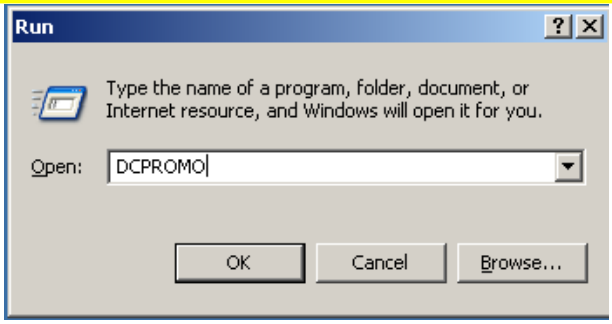
1.4. Add Additional Domain Controllers to the Domain

Log on to the **ermancerujano.com** domain with member server **server11**.

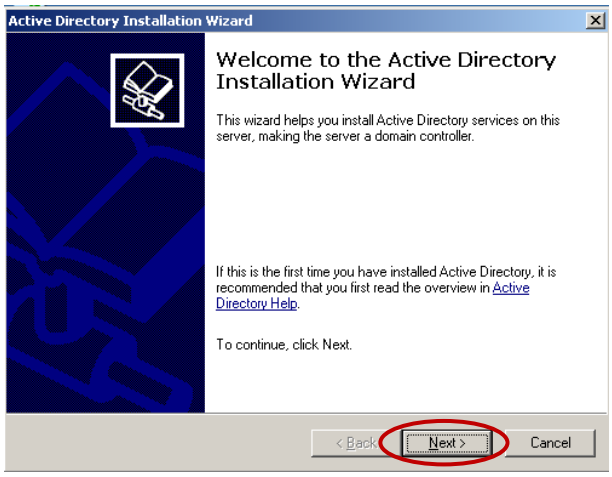
Before attempting to add a second domain controller to the domain, it is very important to verify that DNS is working properly on the server. You can do this by using the **NSLOOKUP** utility from the command prompt and making sure that the default server and address appear without any errors. You should have **server1.ermancerujano.com** appear as the default server with the IP address of **192.168.1.201**.

Exit NSLOOKUP and close the command prompt. If you receive errors at this point, it is very unlikely that the second domain controller will be able to contact the first domain controller and replicate the Active Directory database. You should attempt to fix this problem, which is more than likely related to DNS, before you go on.

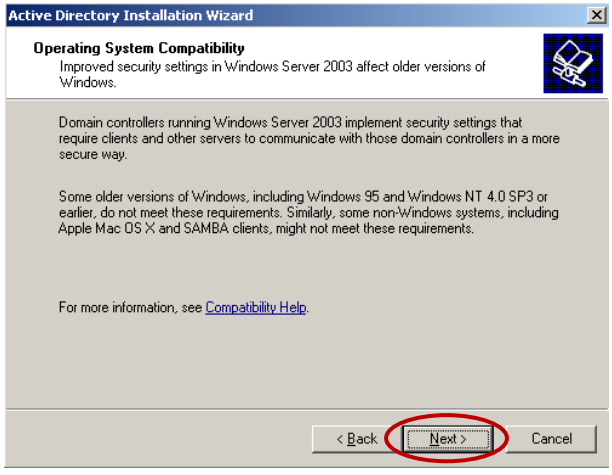
Adding another domain controller to a domain is done the same way as creating the first domain controller, by running DCPROMO and using the Active Directory installation wizard, only this time you will have to select different options in the wizard in order to make **Server11** the second domain controller of **ermancerujano.com**. You can start the Active Directory installation by running **DCPROMO** from the run command prompt.



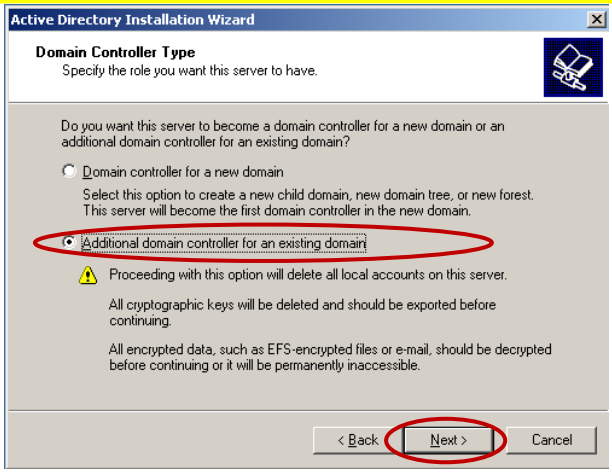
Click on **Next** to move on to the next screen.



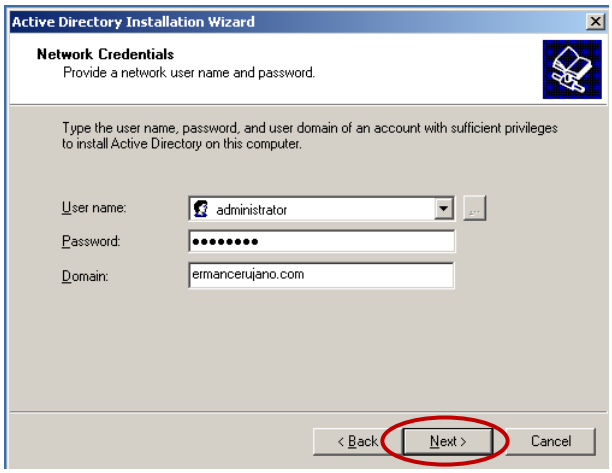
Here, as you can see it will prompt you about the System compatibility, just click **Next**.



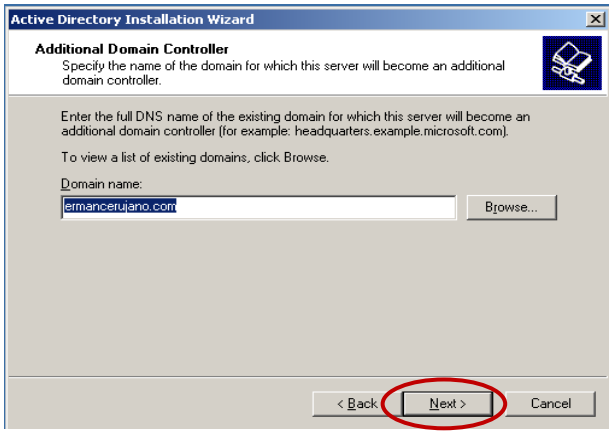
Now you are asked to specify whether this will be a domain controller or a new domain or an additional domain controller for an existing domain. Select "**Additional Domain Controller for an Existing Domain**" and click Next.



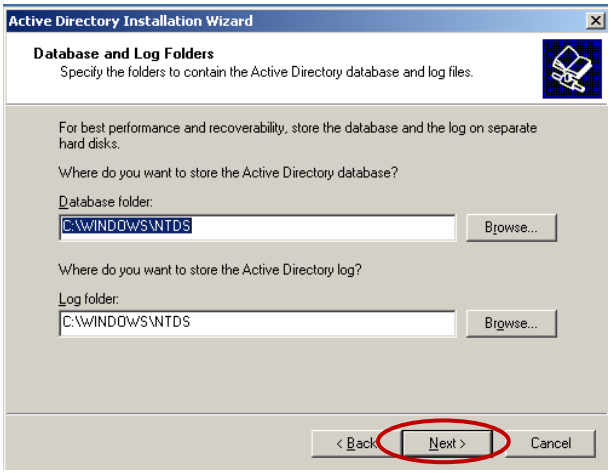
The next screen will ask you to specify a username, password and domain name for the domain it will become a domain controller for. Type in the **administrator's username** and **password** for the **ermancerujano.com** domain. **ermancerujano.com** should appear by default as the domain because this server is a member of the **ermancerujano.com** domain already. Click **Next.**



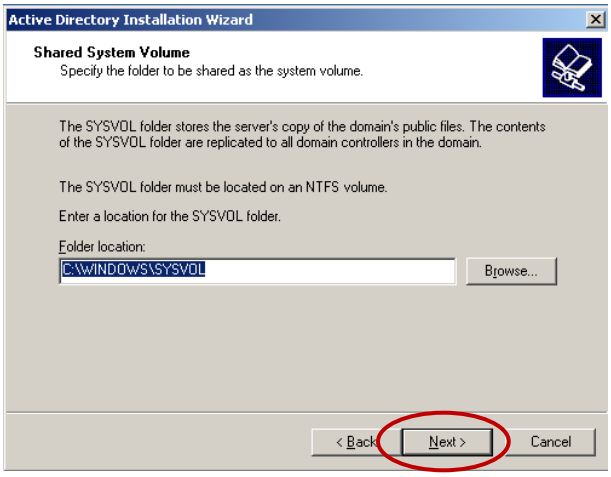
The next screen will as you to enter the full DNS name of the domain for which the server will become a domain controller. By default it should already appear as **ermancerujano.com** because the server is already a member of this domain. leave the DNS name **ermancerujano.com** and click **Next.**



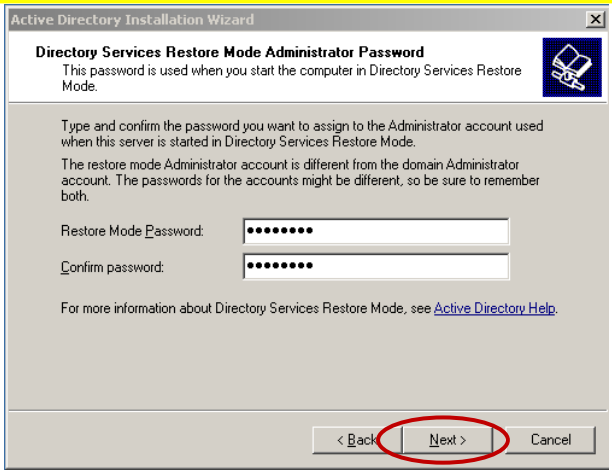
The next screen will as you to specify where to store the **Active Directory Database** and the **Active Directory Log**. By default they are both placed in the **%sysetmroot%**(for this example which is **c:)\WINNT\NTDS** folder. It is recommended that you place the database and the log on separate physical hard drives for better performance, for this lab leave the default location for both the database and the log and then click **Next.**



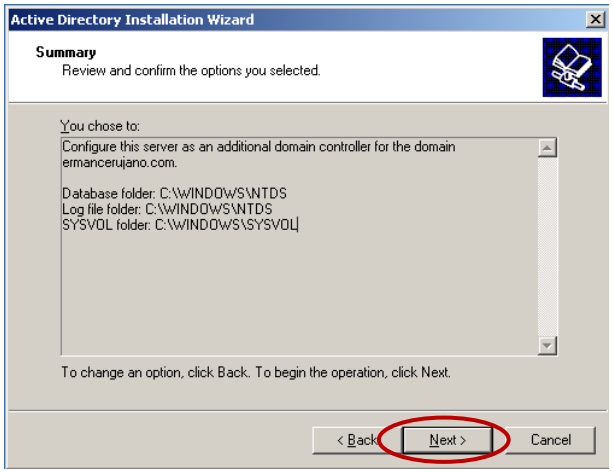
The next screen will ask you to specify the location of the shared system volume. The default location is **%systemroot%\WINNT\SYSVOL.** Keep it simple by leaving the default location for the shared system volume and click **Next**.



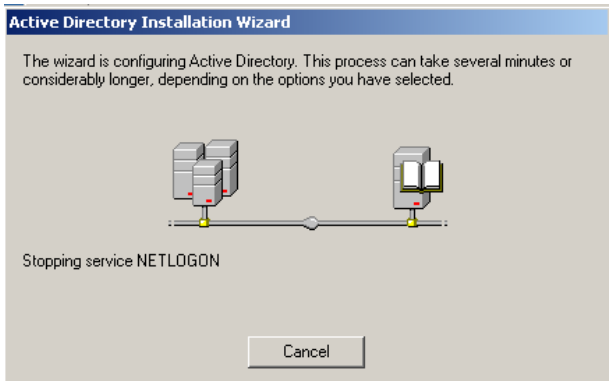
The next screen will ask you for a **directory service restore mode administrator password**. This password will be asked for when starting the computer in directory services restore mode or if the domain controller is being demoted. Use the same password that was used in the first domain controller to be consistent. Type the password and click **Next**.



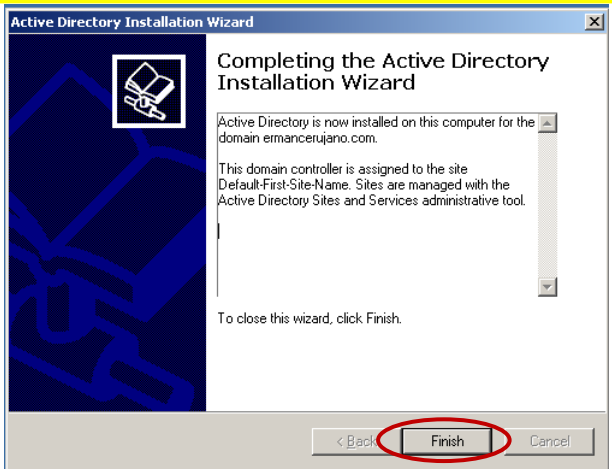
The next screen will be a summary of the information you entered in the wizard. Confirm that the information is correct and click **Next**.



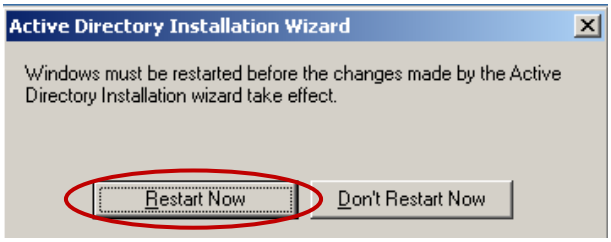
The Active Directory installation will then begin and continue for about 15-30 minutes.



The final screen for the wizard will appear to let you know the installation is complete. Click on **Finish**



A dialog box will appear telling you that the server must be restarted in order for the changes made by the Active Directory wizard to take effect. Click on **Restart Now** for the computer to restart.



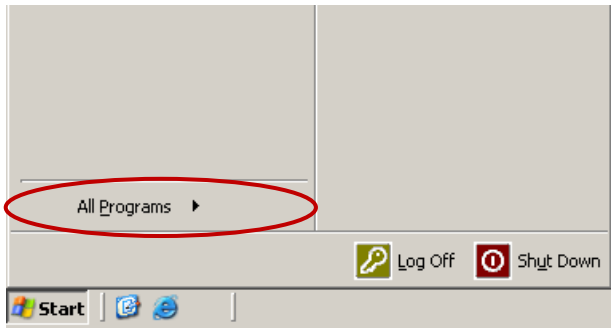
1.5. Test Active Directory Replication between Domain Controllers.

Log on to **Server1**.

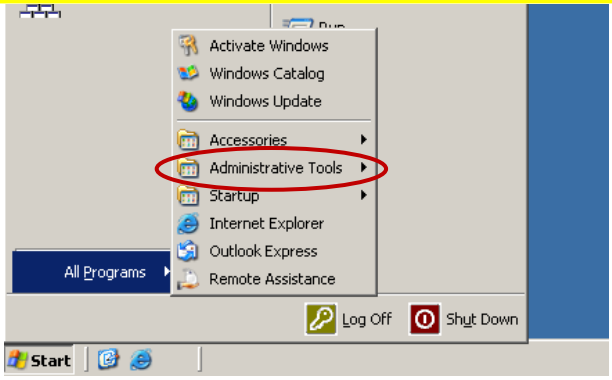
Open the Active Directory Users and Computers console by following the steps below:

- Go to start.

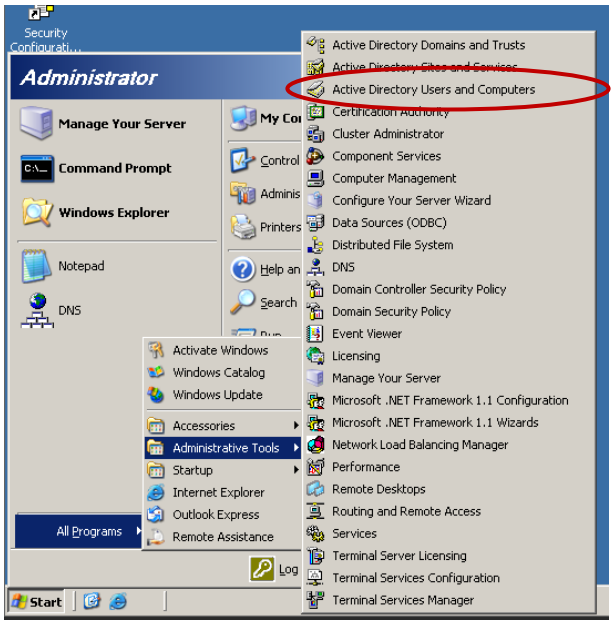
- All programs



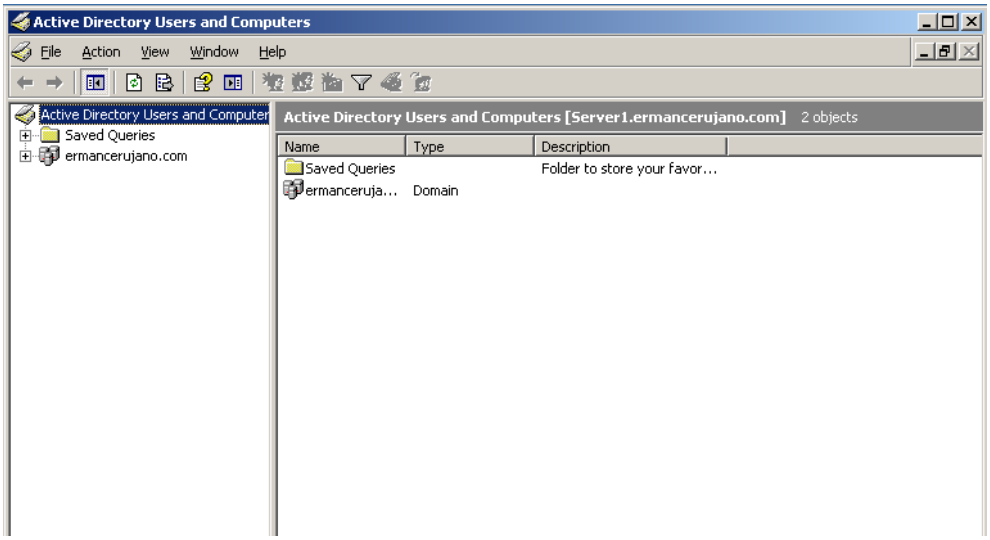
- Administrative Tools



- Active Directory Users and Computers

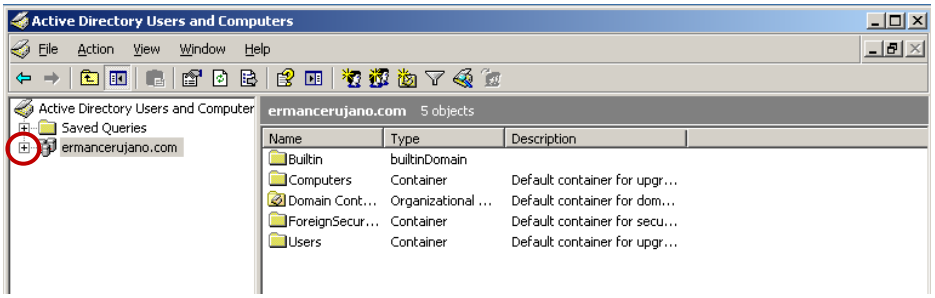


You are now in the Active Directory Users and Computers Console

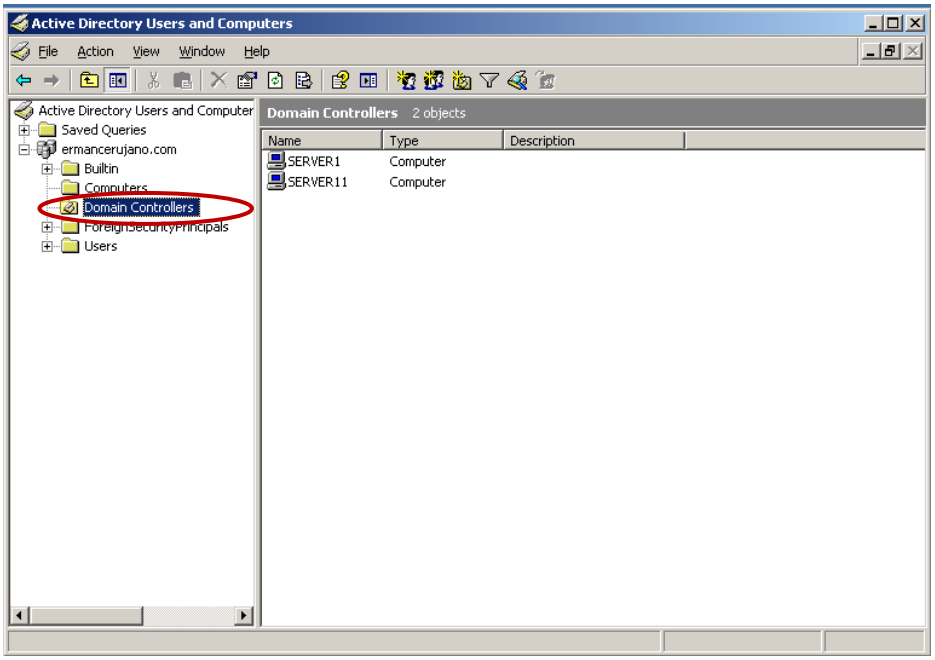


In the left pane of the console open the container named **Domain Controllers.**

- Click the add button in **ermancerujano.com**



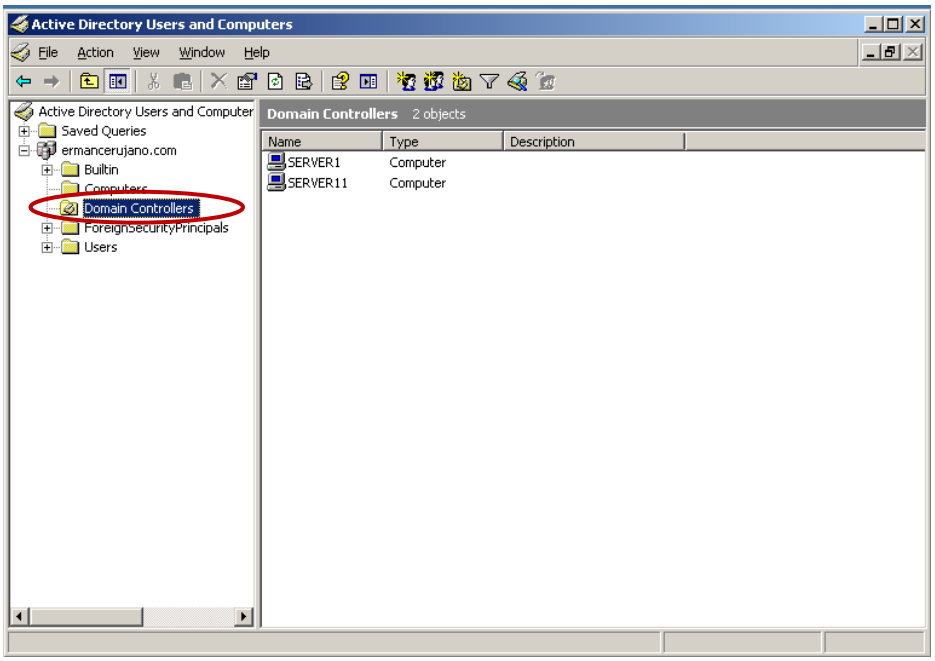
- Select Domain Controllers.



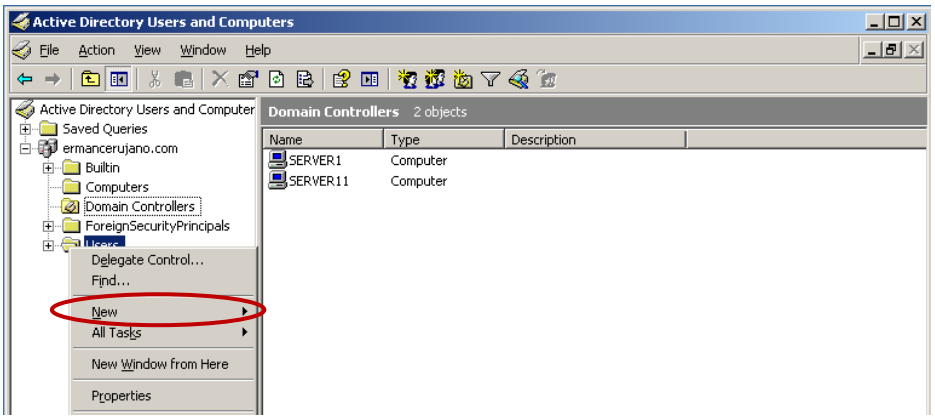
All domain controllers in the **ermancerujano.com** should appear in the details plane on the right. You should see both **server1** and **server11** appear. By default, any domain controllers on the network are placed in this container.

Now create a user account for **Erman Ace Cerujano** to test replication between the two domain controllers. To do that

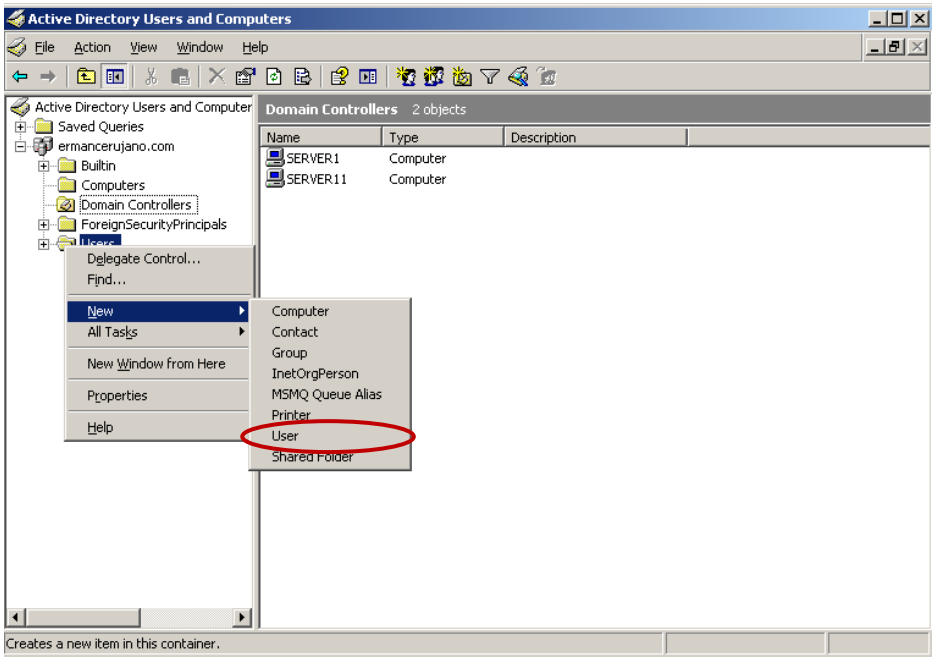
- Right click on the **Users Container** in the left pane.



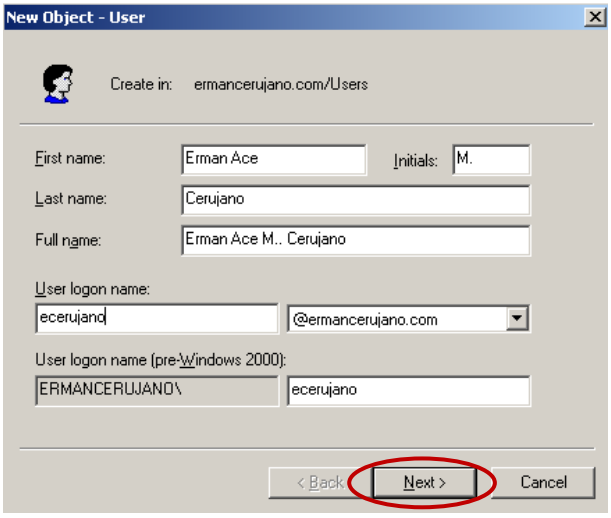
- Select New.



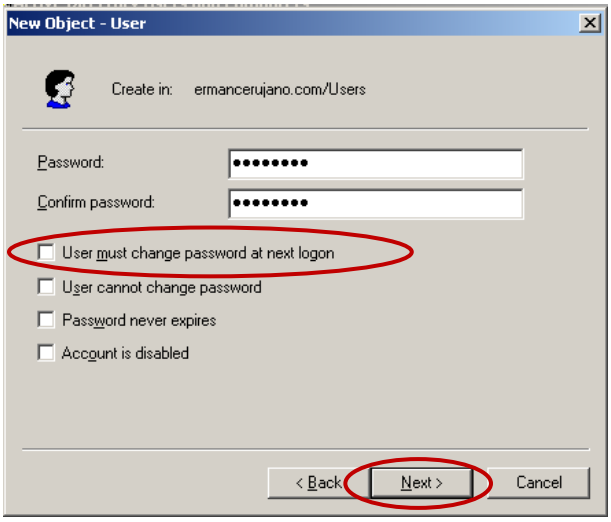
- Select User.



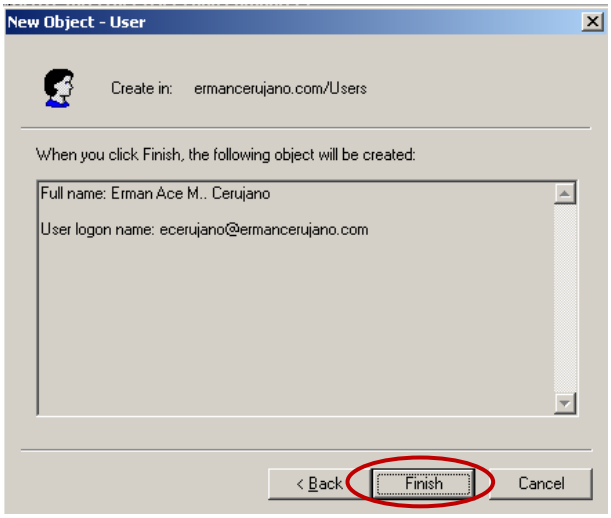
That will bring up a wizard for creating a new user. Type in the first and last name for the user (**Erman Ace Cerujano**) and for the logon name type is the first initial of the first name and the full last name **(ecerujano)** and click **Next**.



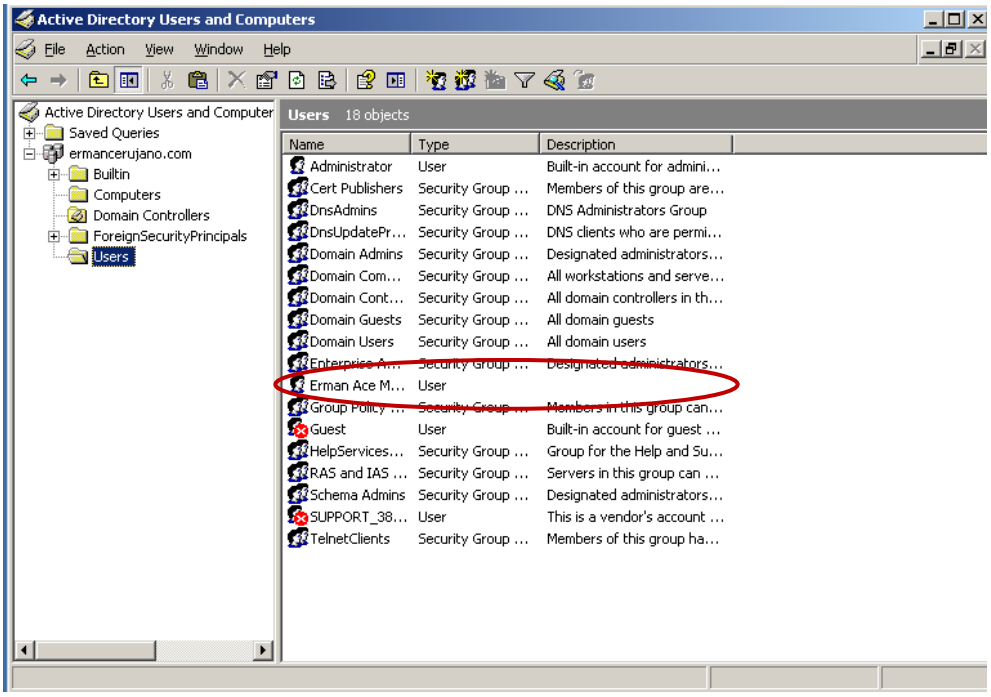
On the next screen you must enter a password for the new user account. Type in **Megalab1** as the password, uncheck **User must change password at next logon** and click Next.



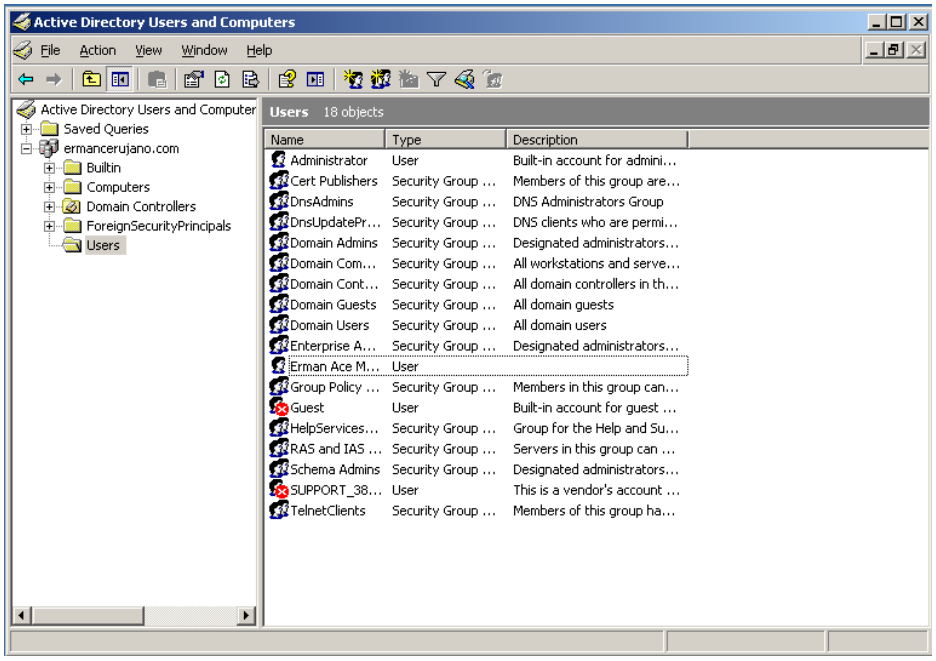
The final screen is just a summary of all the information that you entered I the Wizard. Confirm that the information is correct and click **Finish**.



Then on the Active Directory Users and Computers console there should be a user account named **Erman Ace M. Cerujano** in the User Containers.



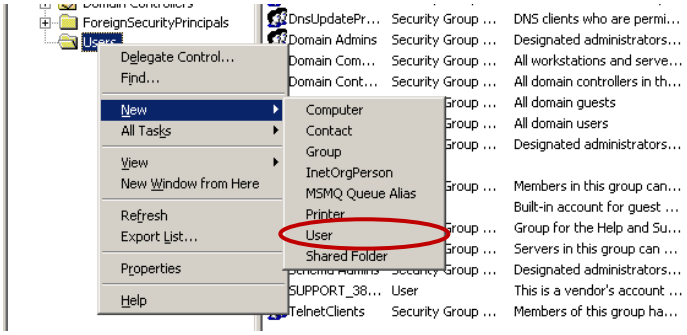
Now log on to **Server11** and open the **Active Directory Users and Computers console** and then click on the **Users** containers in the left pane.



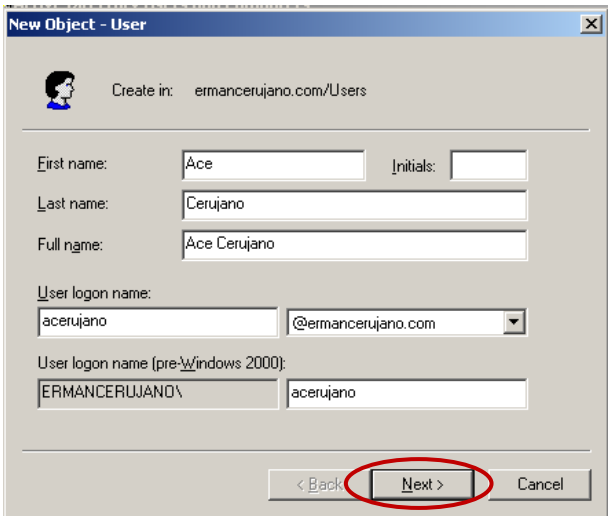
It may or may not appear here. It all depends on whether the domain controller shave replicated the Active Directory database yet or not. There is no absolute time as to how often the domain controller replicate, they may replicate instantly (as you can see above) or it may take up to about 5 minutes after a change is made to the database. For the lab let us assume that the replication has not taken place so your Active Directory Users and Computers console on Server11 will not have the user **Erman Ace M. Cerujano**.

Now create a user account in the **Users** container for **Ace Cerujano** with the password **Megalab1** from within **Server11's Active Directory Users** and **Computers** console. This way you can see how replication will update the Active Directory database on both domain controllers. Close the Active Directory Users and Computers console when finished.

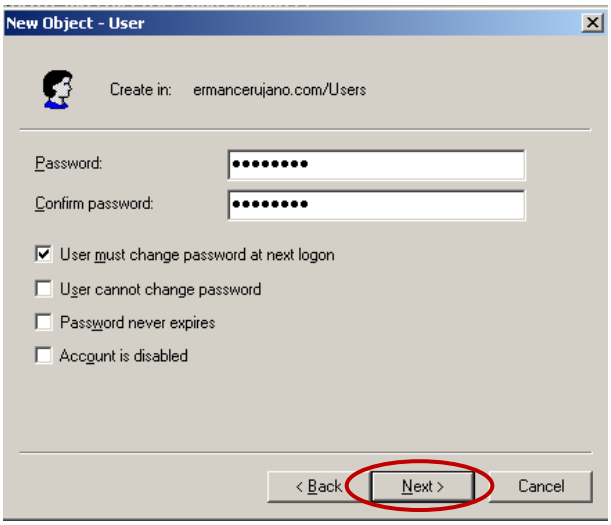
- Right click on users > New > users



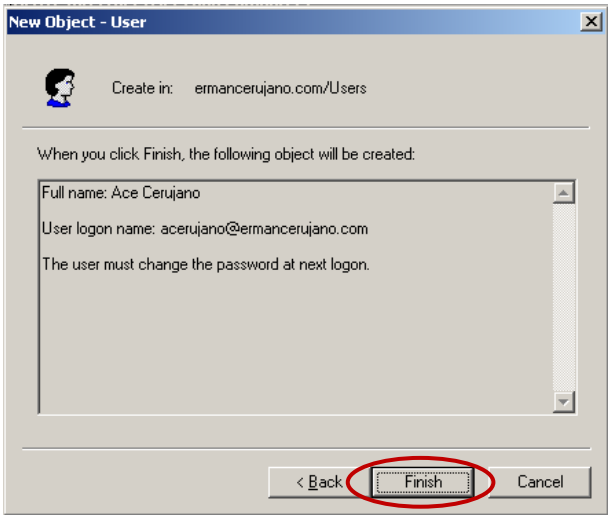
- First name as "ace" and last name as "Cerujano" User logon name should be "acerujano"



- Password should be: "Megalab1."



- Click Finish

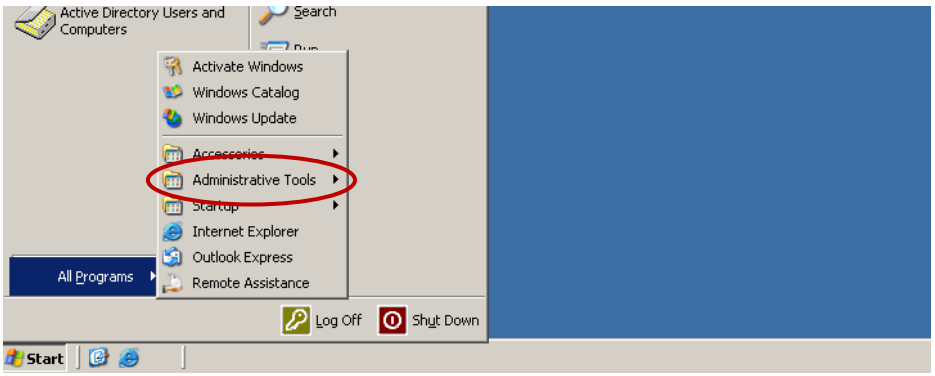


Replication can be forced from any of the domain controllers in the domain from within the Active Directory Sites and Service Console. Use **Server11** since it is the server you were last on and go to

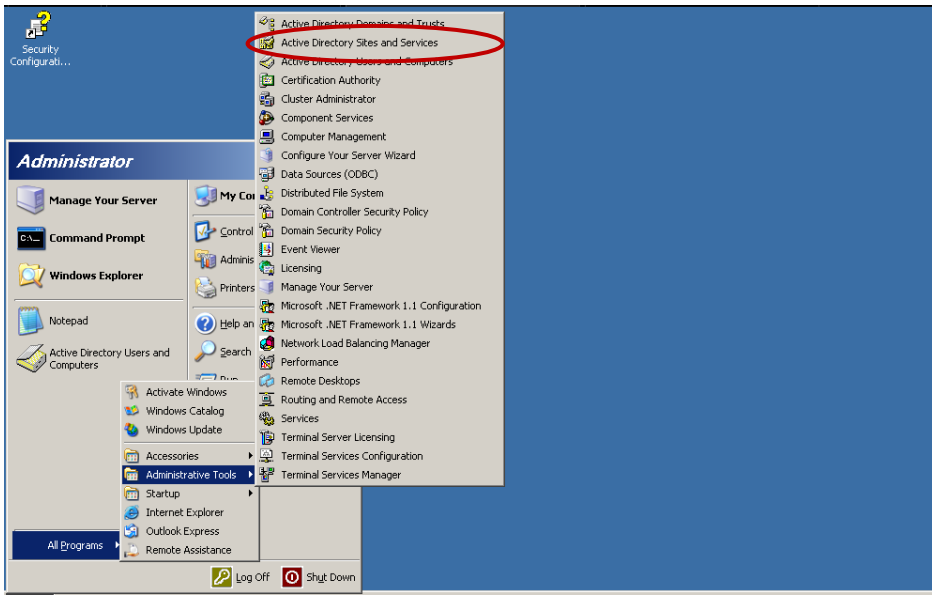
- Start

- All programs

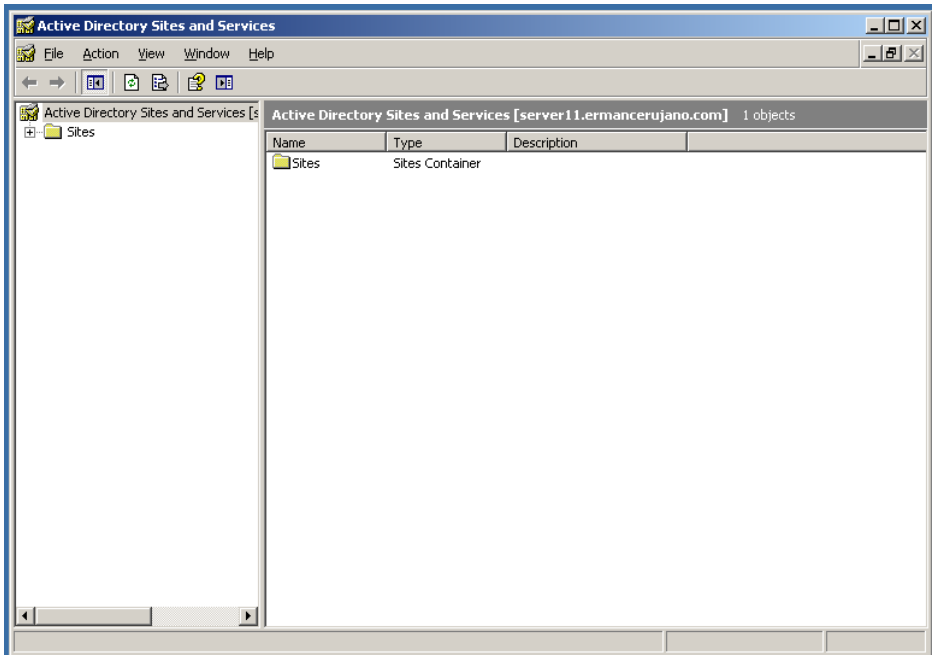
- Administrative Tools



- Active Directory Sites and Services

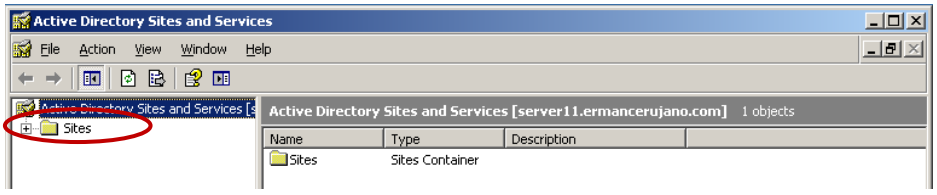


You are now in the Active Directory Sites and Services.

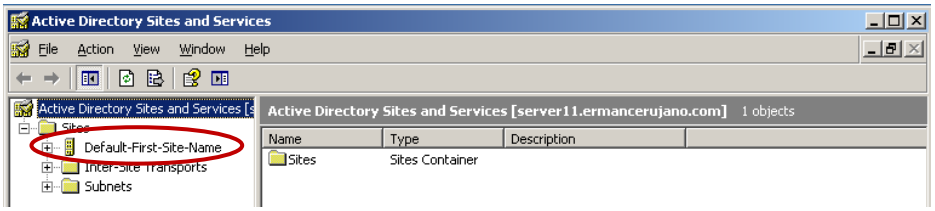


In the left pane go to:

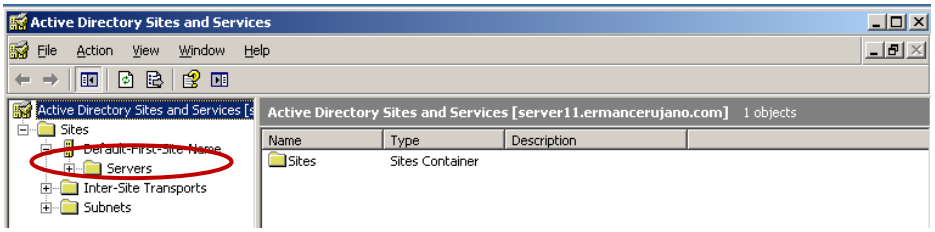
- Sites



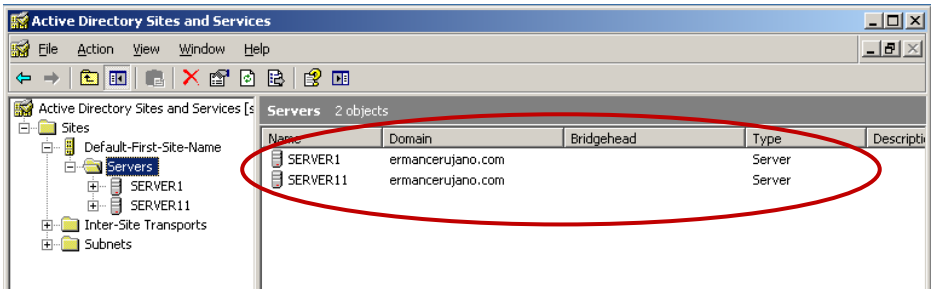
- Default-First-Site-Name



- Servers

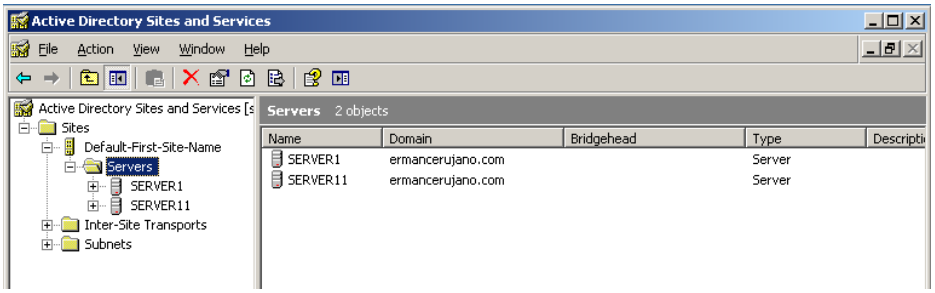


There you should see domain controllers, **Server1** and **Server11**.

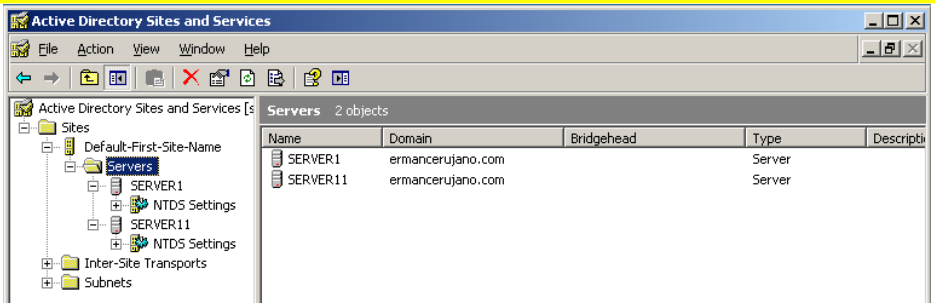


Now within each server are the **NTDS (Active Directory Database)** Settings. Open both servers in the left pane so that you can see the NTDS settings.

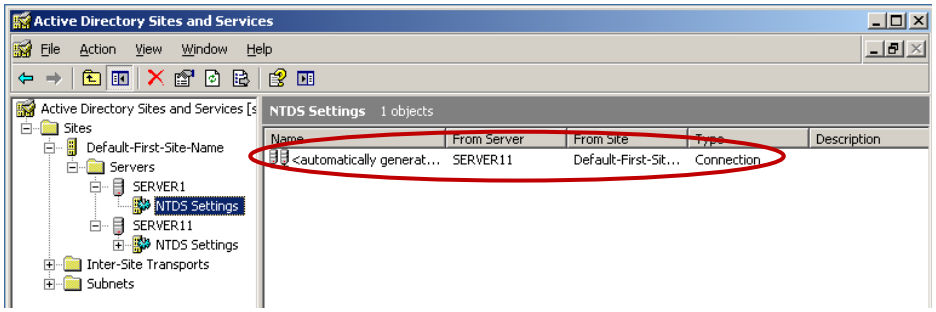
Click the plus button.



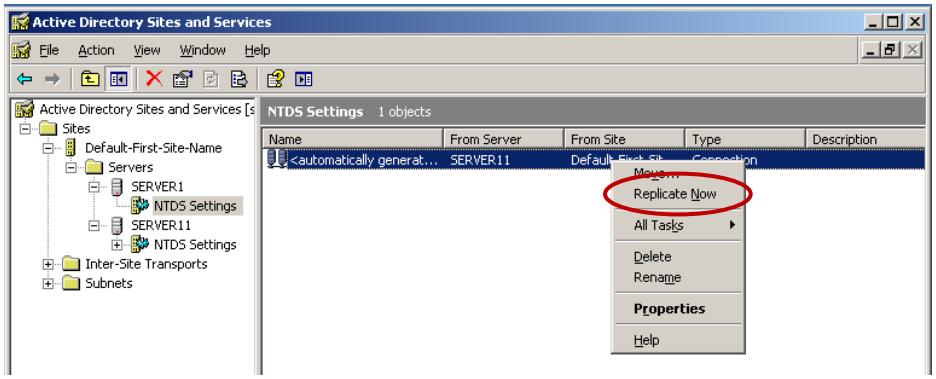
You can see now the NTDS Settings



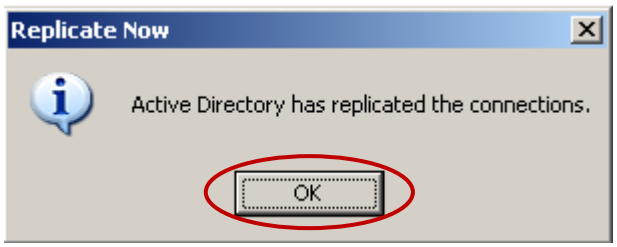
Select the **NTDS settings** for **Server1** and you should see the connection to **Server11** in the detail pane.



Right click on the connection and select **Replicate Now**.

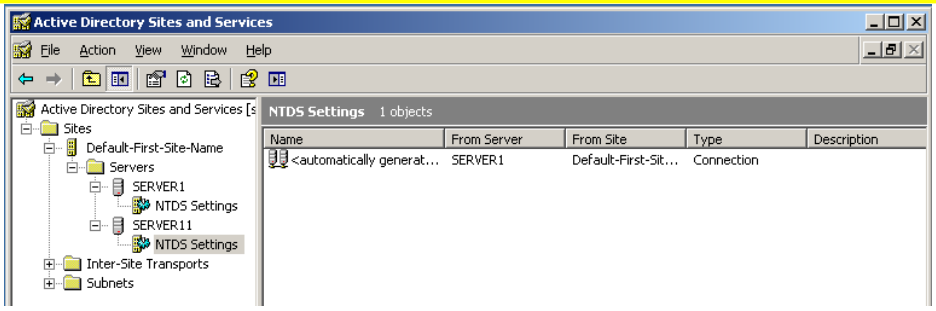


A dialog box will appear telling you that Active Directory replicated.

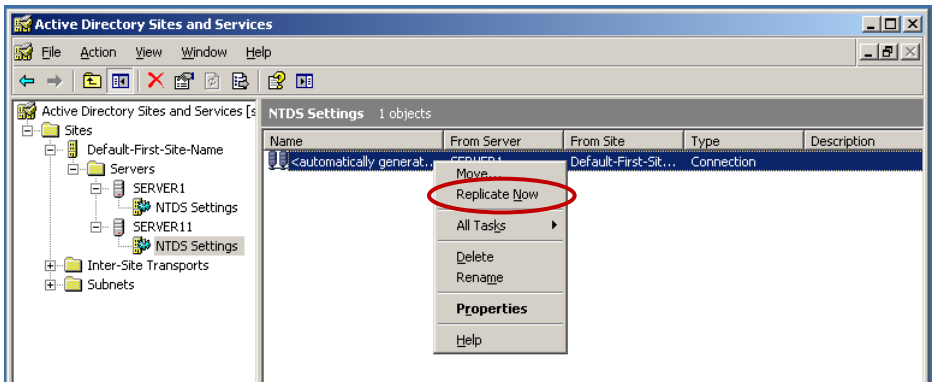


Now do the same for the connection to **Server1** within the **NTDS** settings for **Server11**.

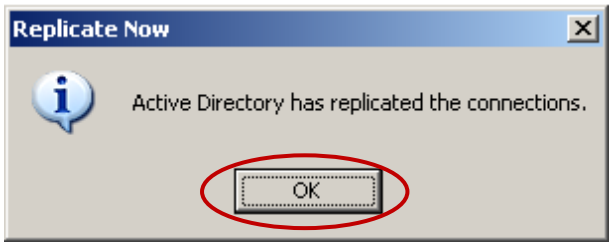
- Open the NTDS of server11.



- Right click on the connection and select Replicate Now.

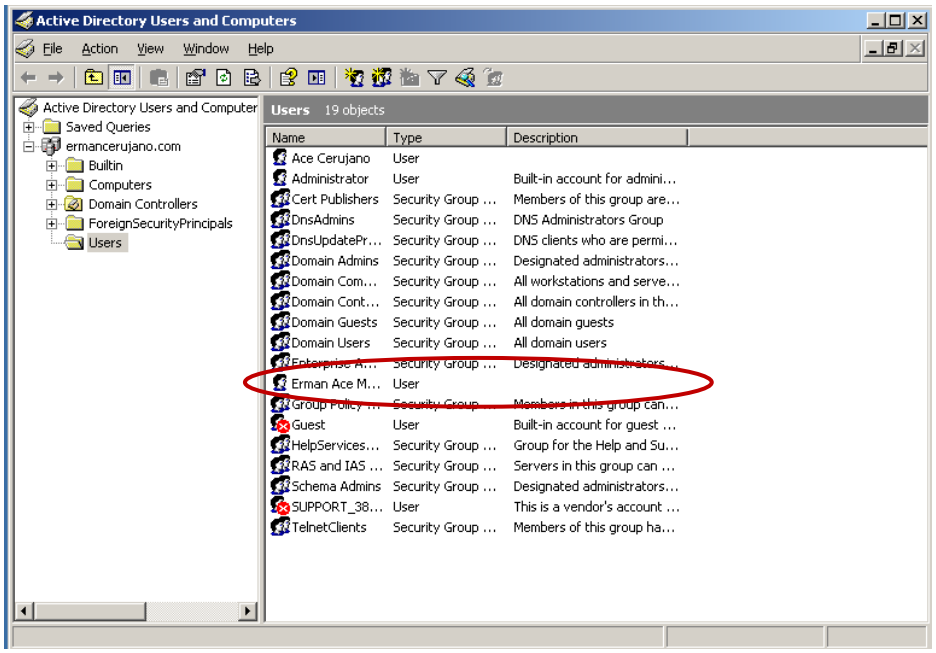


- Click **OK**.

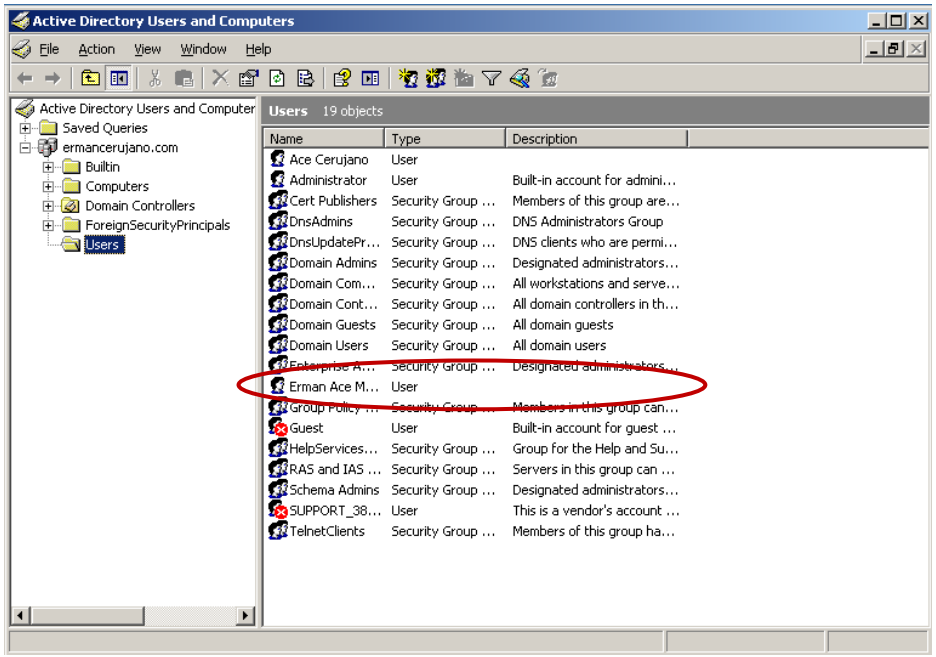


Close the Active Directory Sites and Services console when you are finished.

Now on **Server11** open the **Active Directory Users and Computers** console and try to find the users accounts for **Erman Ace M.. Cerujano** and **Ace Cerujano** in the **Users Containers**. They should both appear in the user's container.



Now try to find them on the **Active Directory Users and Computers** console on **Server1**. If you can see both user accounts on either server, it means that Active Directory replication is working properly.



LAB 14.2

Creating an Organizational Unit (OU) Structure

Contents:

SCENARIO

You finish the installation of the domain controllers way ahead of schedule and everything is working great. You report to Erman, the Operations Manager, that the domain is up and running without any issues. He says, “WOW great job!” He is very impressed, you think to yourself, “that full time administrator job is all mine.” Erman then asks you if you’re ready for the next project. She has designed the Organizational Unit (OU) structure that the company is going to use on the network. She hands the project over to you with all of the necessary information and asks you to see her after you have implemented and tested the OU structure.

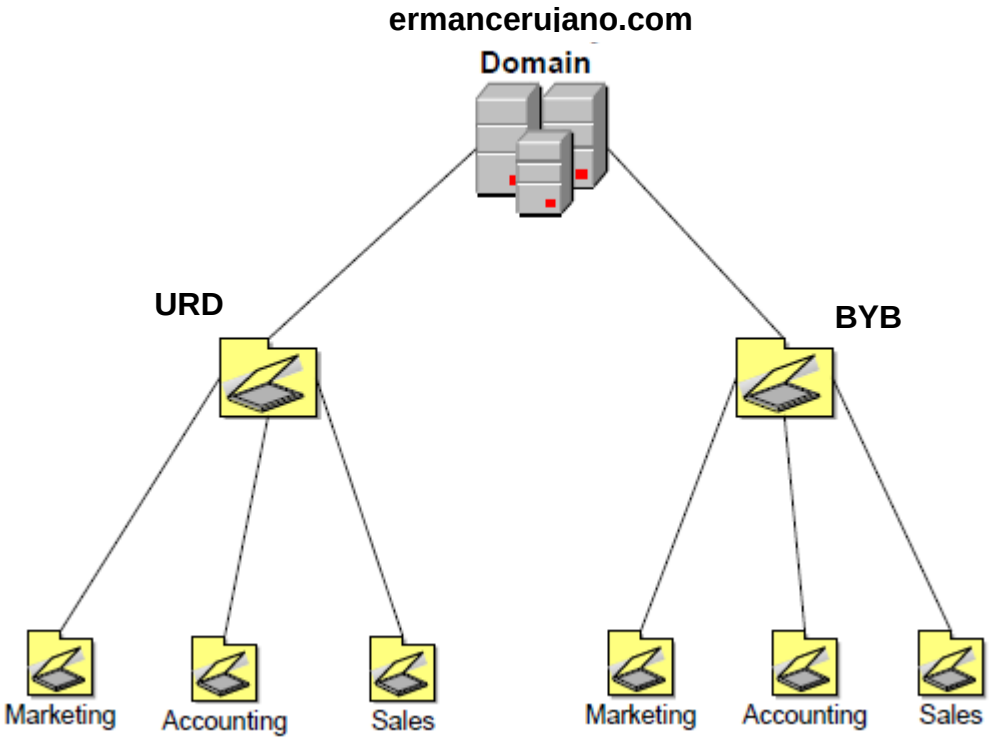
In this lab you will create an Organizational Unit (OU) structure for Ermancerujano. Erman’s design is a “hybrid” approach, based on location first, then on business functions. You will first create OUs for each location and then create child OUs within them for each department in the company. You will also create and move objects within the OU structure. Finally, you will delegate control of some basic administrative functions to a user located in the Urdaneta City location.

ORGANIZATIONAL UNITS

Organizational units were first found in Windows Server 2000’s Active Directory and return in Windows Server 2003. OUs are Active Directory containers that you use to organize objects within a domain. An OU can contain objects like users, groups, computers, printers, other OUs, and shared folders. OUs can be assigned group policies and can be used to delegate administrative tasks to users or groups. The key to building an OU structure is to have a system that is easy to manage and works well of the company. A company may use different strategies for creating their OU structure. The OU structure can be based on different strategies of creating their OU structure. The OU structure can be based on location, business functions, type of objects, or a hybrid of many different strategies. This structure will vary from company to company, depending on what the needs of the individual company are. OUs are a good alternative to creating multiple domains and Microsoft recommends that your company only have one domain if possible.

STRUCTURE

Organizational Unit Structure



LAB 14.2. CREATING AN ORGANIZATIONAL UNIT (OU) STRUCTURE FOR ERMANACE

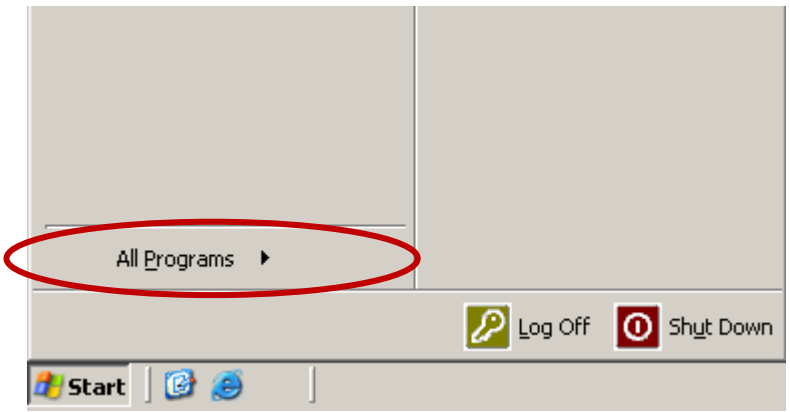
2.1. Create Organizational Unit (OU) Structure

Log on to **Server1** as the domain administrator.

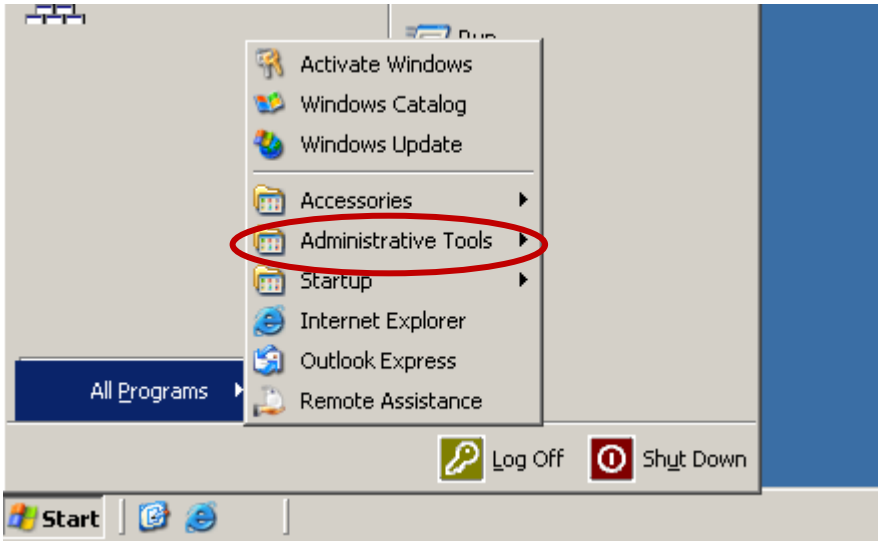
Open the **Active Directory Users and Computer console**.

- Go to start.

- All programs

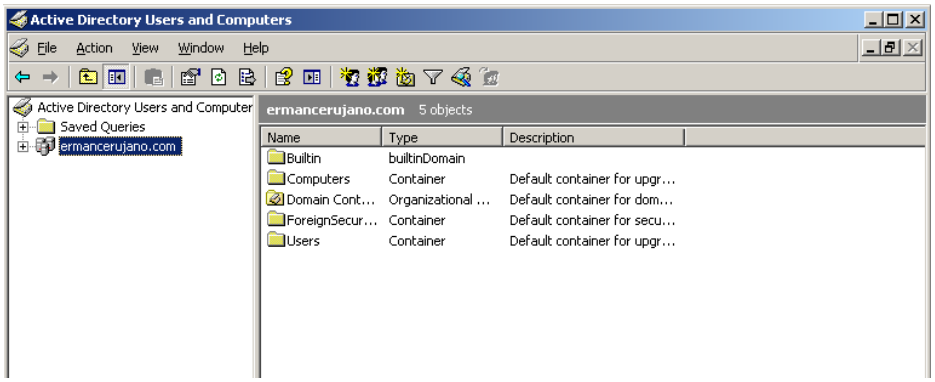


- Administrative Tools

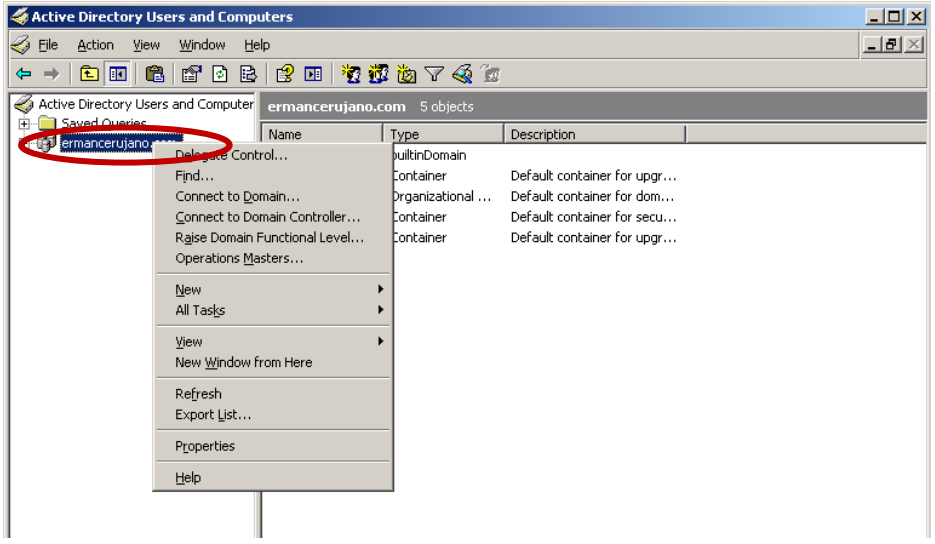


- Active Directory Users and Computers

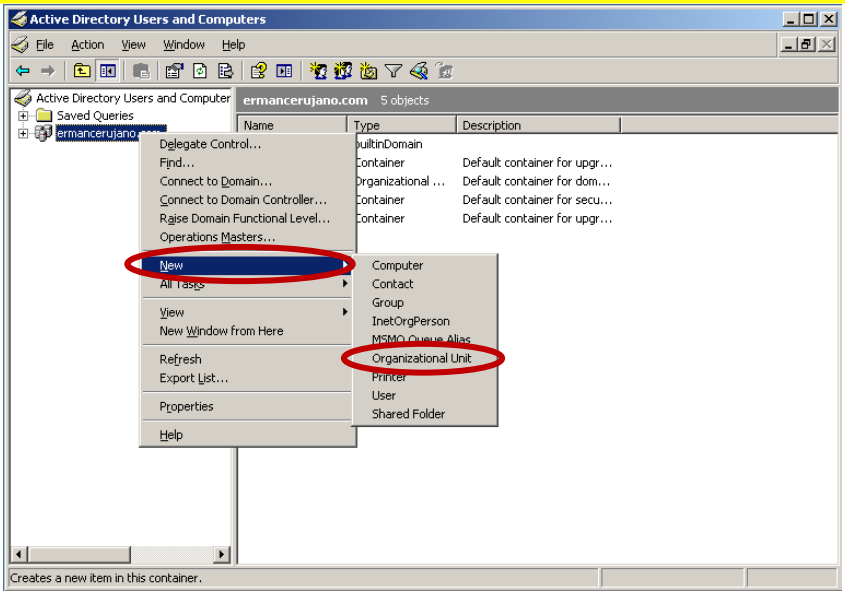
You are now in the Active Directory Users and Computers Console



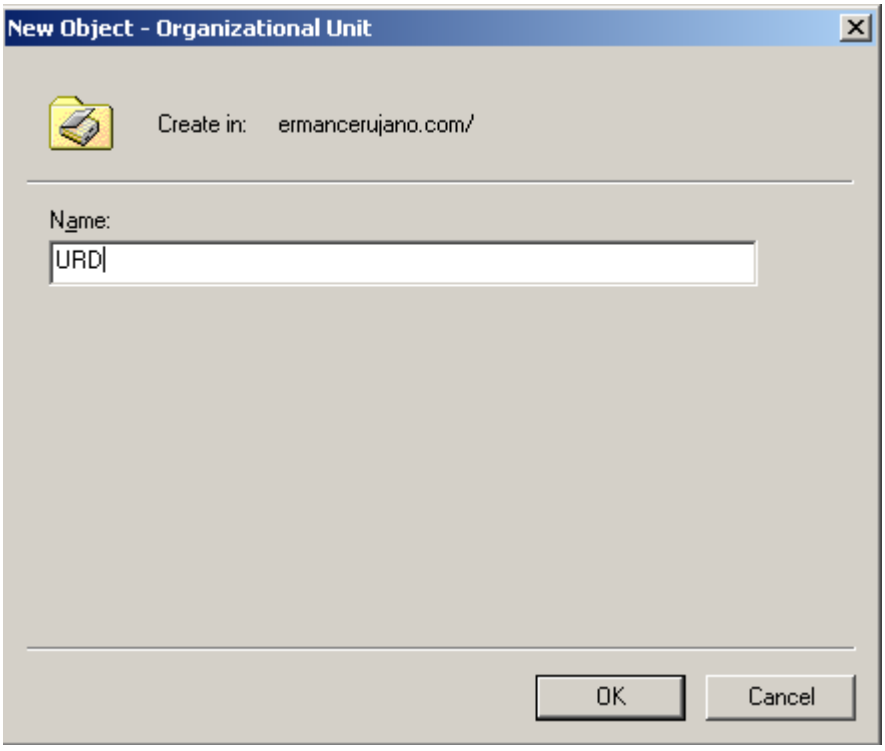
On the left pane, **right click** on **ermancerujano.com**.



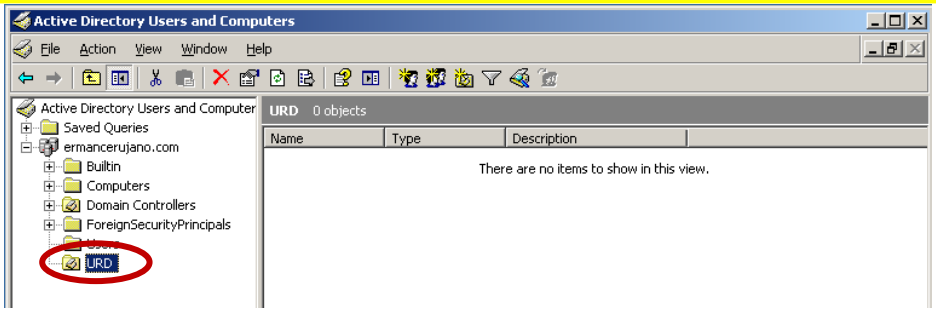
Select **New** then **Organizational Unit**.



A screen will appear asking you to specify a name for the **new OU**. Type in **URD** for **Urdaneta City** and click **OK**.

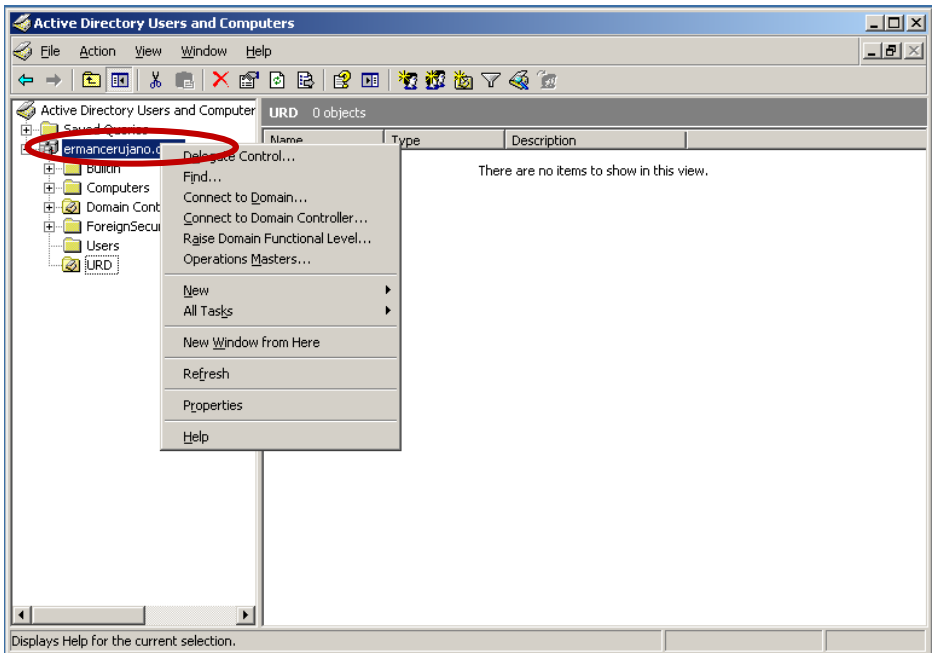


You will now have an OU named **URD** in the left pane of the Active Directory Users and Computers Console.

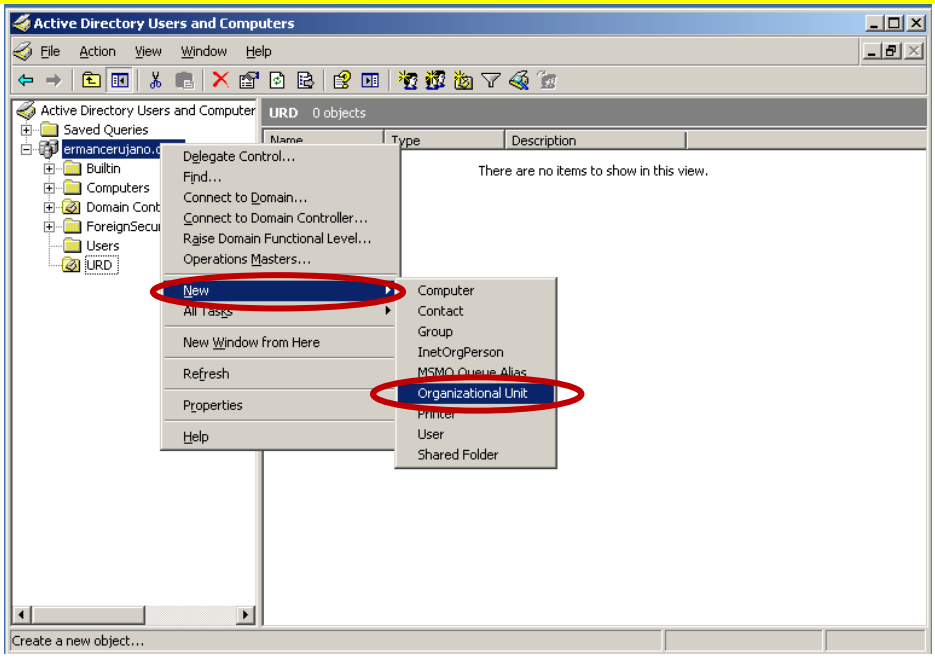


Create another OU in the **ermancerujano.com** domain for Bayambang and name it **BYB**.

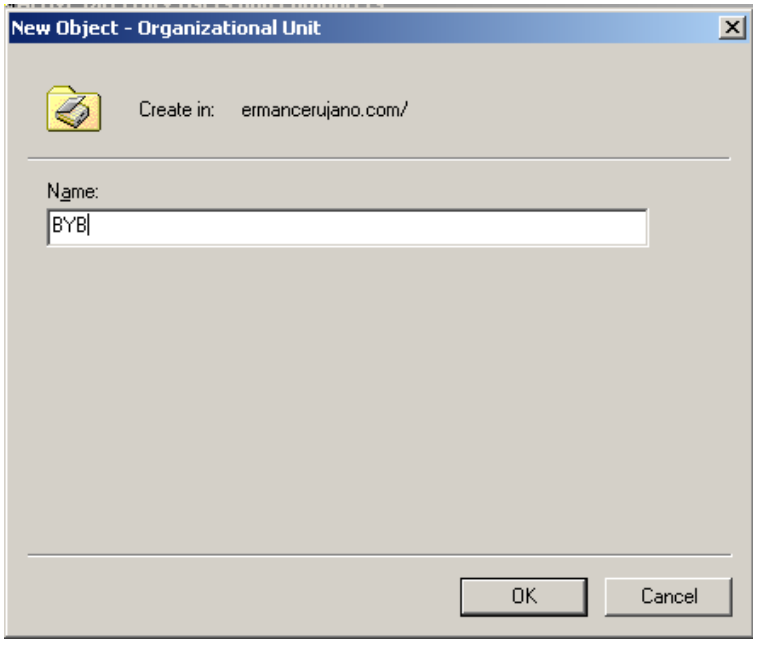
- Right click on **ermancerujano.com.**



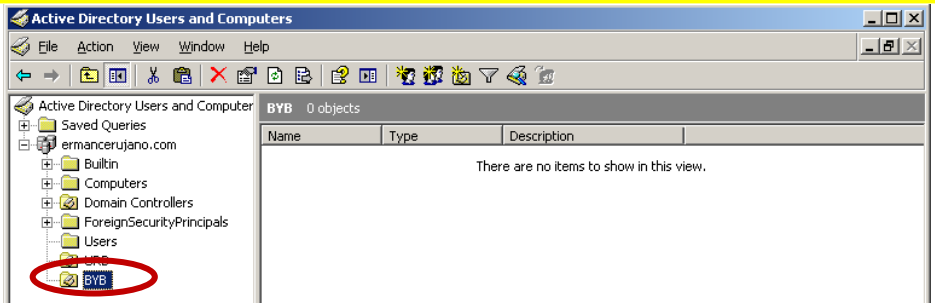
- Then select New and Organizational Unit.



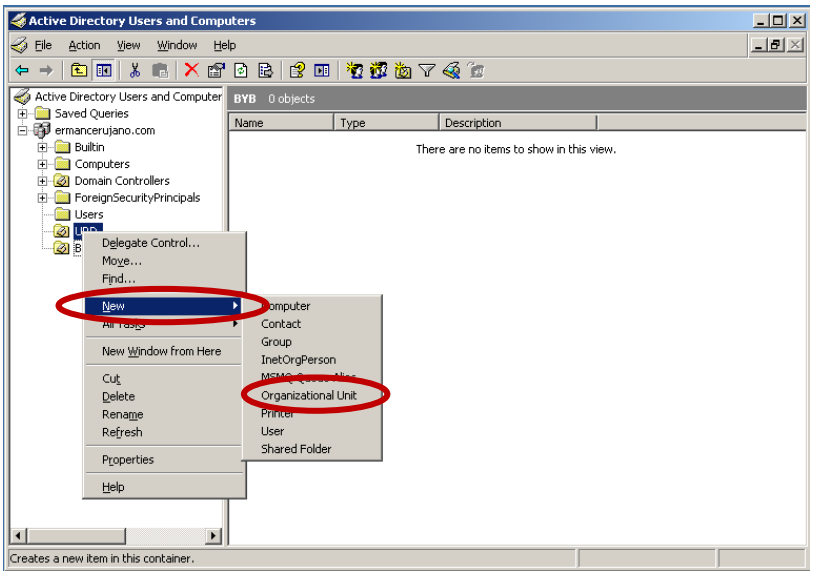
- Enter the **BYB** as the name of your new Organizational Unit and click **OK**.



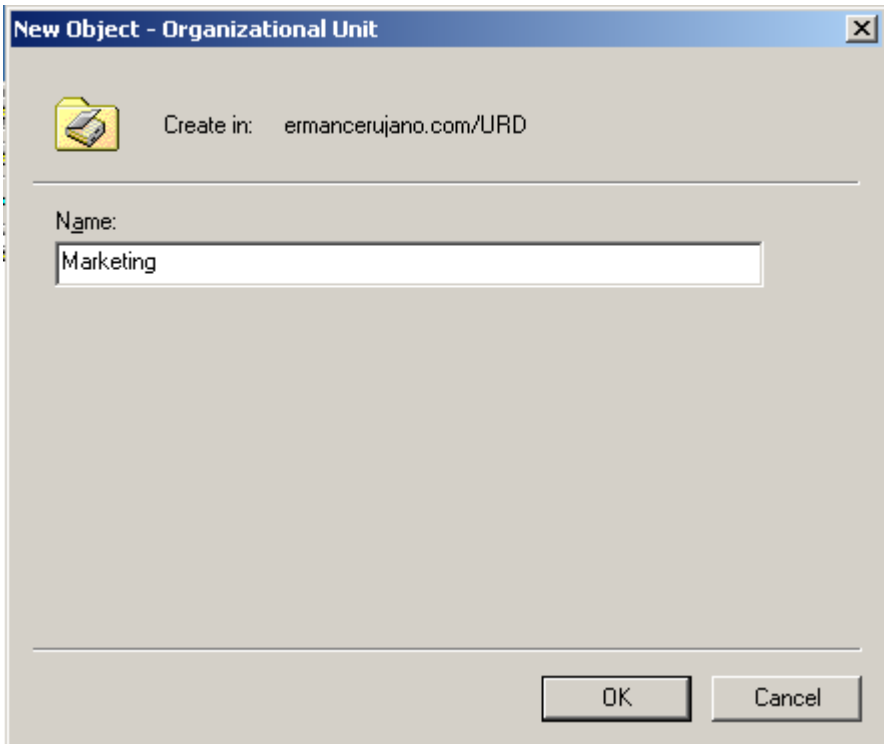
You should now have two OUs appear in the left pane of the Active Directory Users and Computers console. One named **URD** for the **Urdaneta City** and location and one named **BYB** for the **Bayambang**.



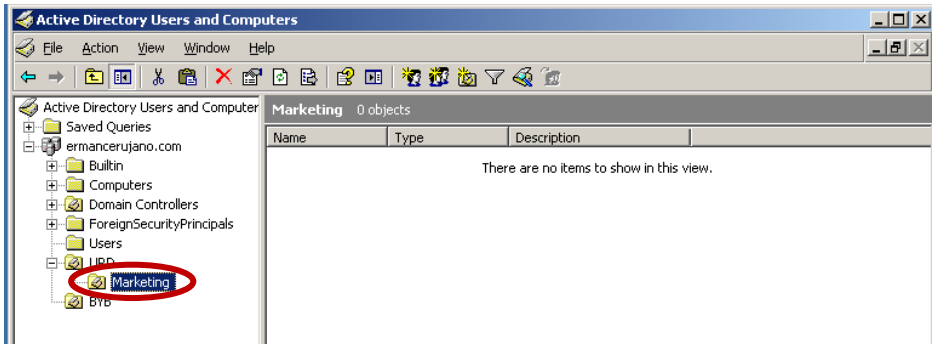
Right click on the **URD** organizational unit and select **New** then **Organizational Unit**.



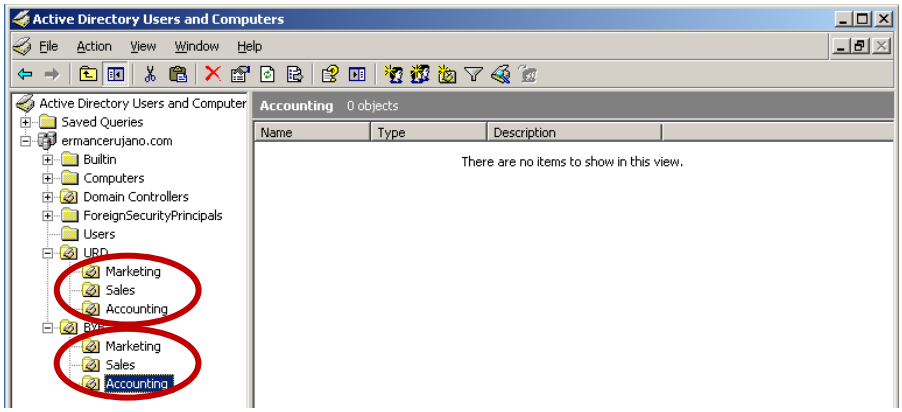
Type in **Marketing** for the name of the new organization unit and lick **OK**.



You have now created an organizational unit for the marketing department within the **URD** (Urdaneta) organization unit.



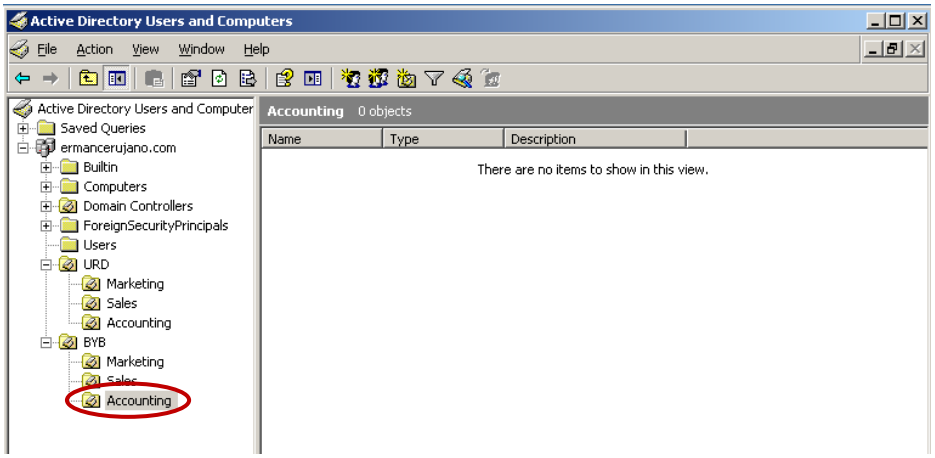
Next, create additional organizational units for the **Sales** and **Accounting** departments within the **URD** OU. Then create the same three organizational units for the different departments within the **BYB** (Bayambang) organizational unit. Your final structure should look like the figure below.



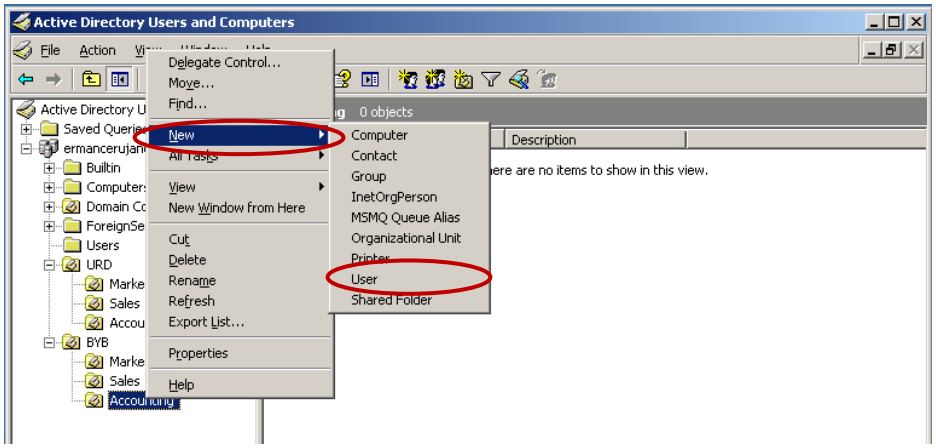
2.2. Creating Objects Within the Organizational Units

Create a user account for **Jeff Morales** in the **Accounting OU** within the **BYB OU**. To do that:

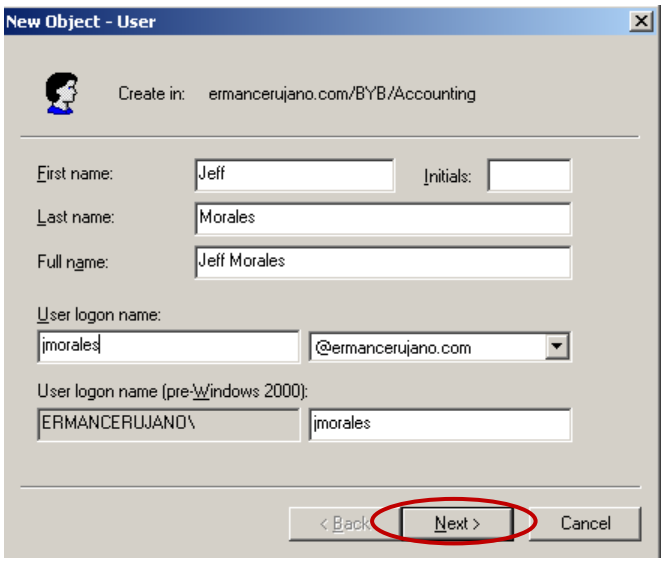
- Right click on the **Accounting OU** within the **BYB**.



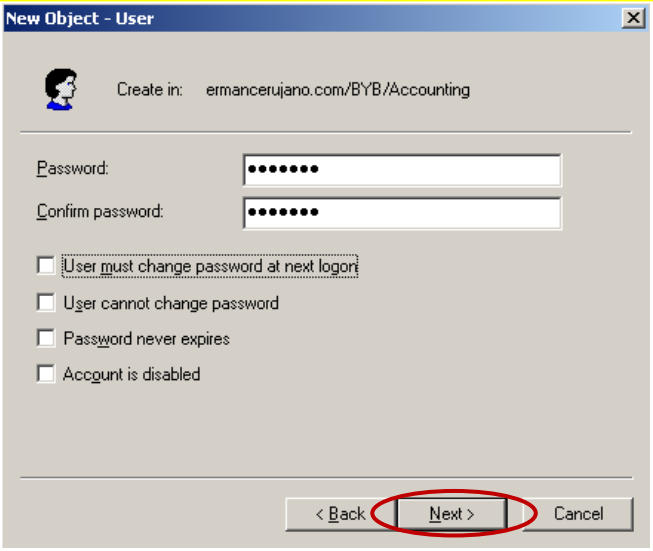
- Select New then user.



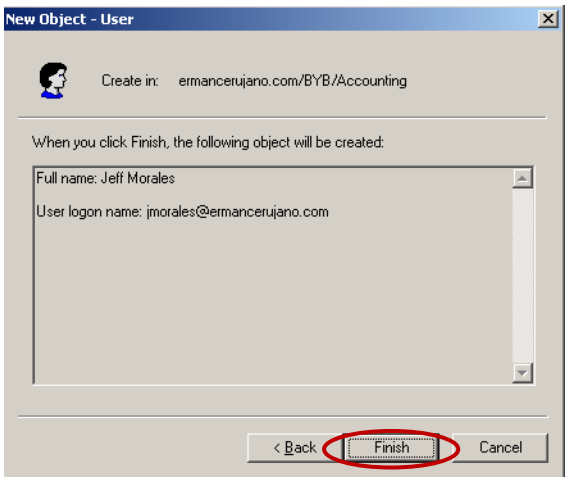
The new user wizard will appear. Type in the full name of **Jeff Morales** with the user logon of **jmorales** and click **Next**.



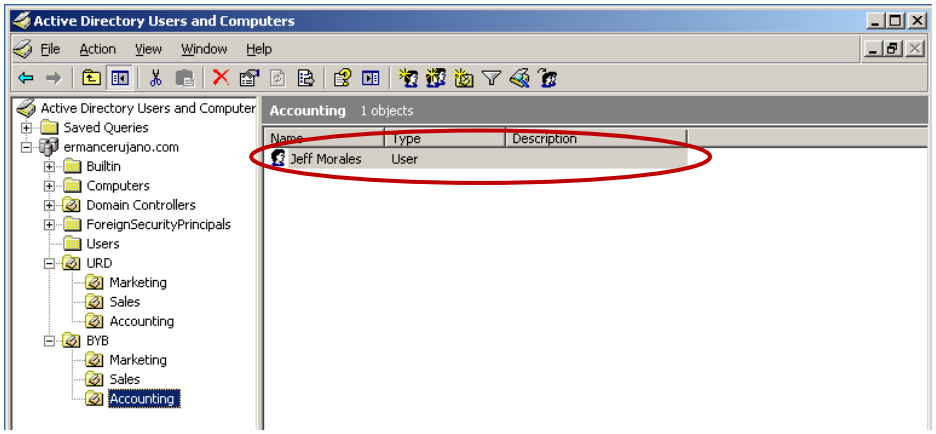
Type in **Tester1** as the password, uncheck **User must change password at next logon** then click **Next**.



Click Finish.



You should now have a user account for Jeff Morales appear in the details pane on the right side when you select **Accounting OU** within the **BYB OU**.

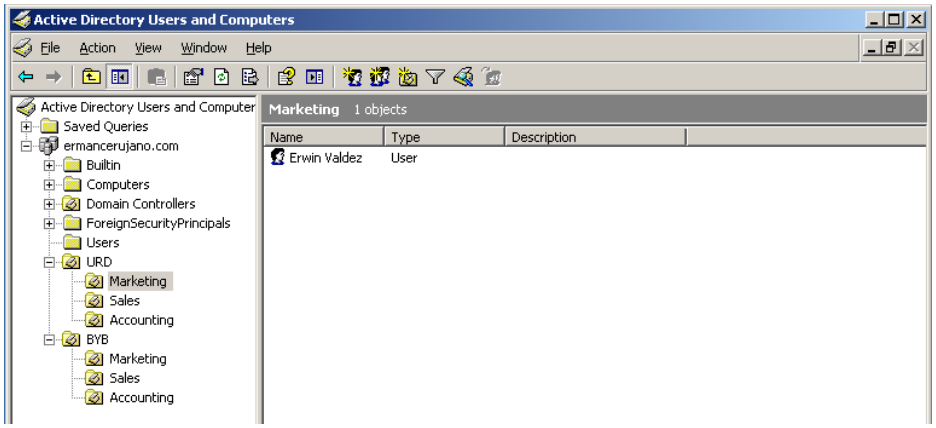


Now create the following users from within the table below. Make sure that they are created within the correct OUs.

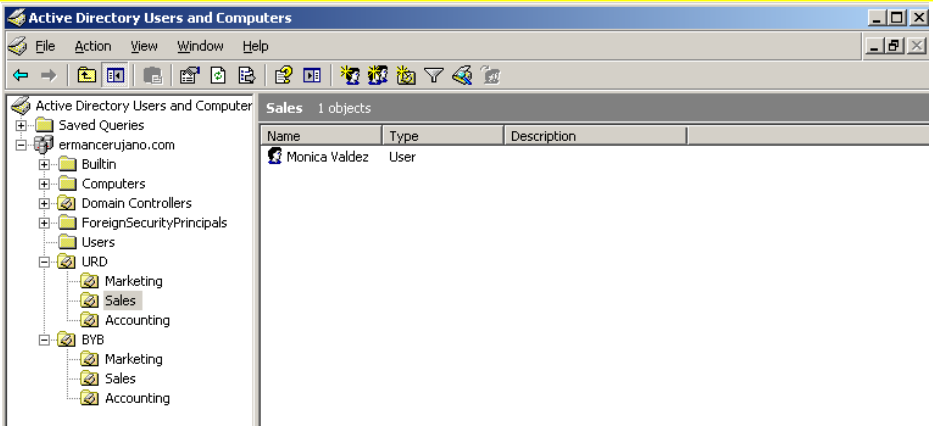
First Name	Last Name	Username	Password	OU
Erwin	Valdez	evaldez	test	URD - Marketing
Monica	Nimer	mnimer	test	URD – Sales
Elle	Cerujano	elcerujano	test	URD – Accounting
Patrick	Luzon	pluzon	test	URD – Accounting
Sherry	Perez	sperez	test	BYB – Marketing
Mark	Ancheta	mancheta	test	BYB – Sales
Paul	Ramirez	pramirez	test	BYB - Accounting

The details pane should look like this:

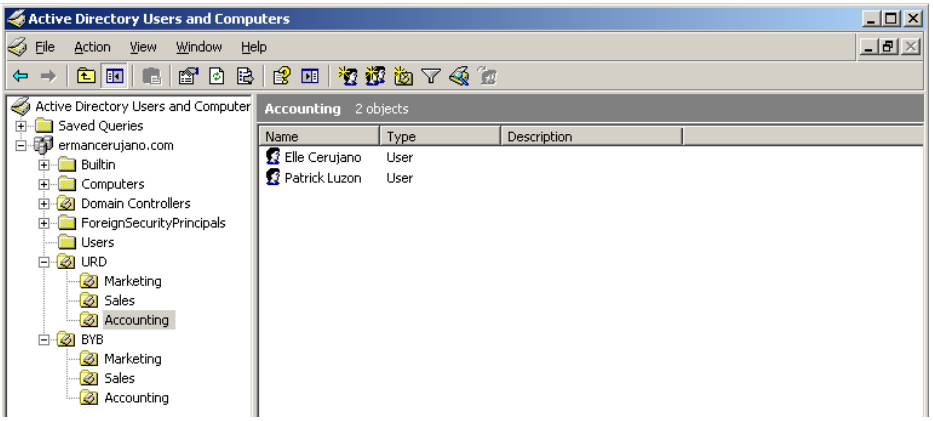
URD – Marketing



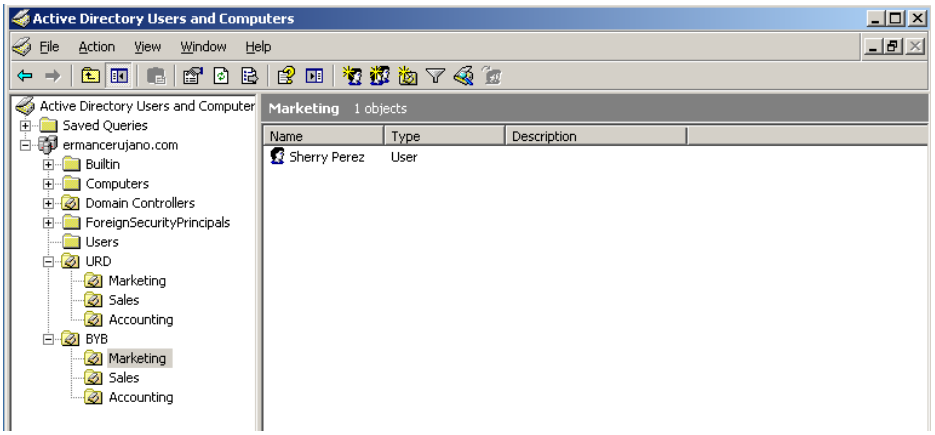
URD – Sales



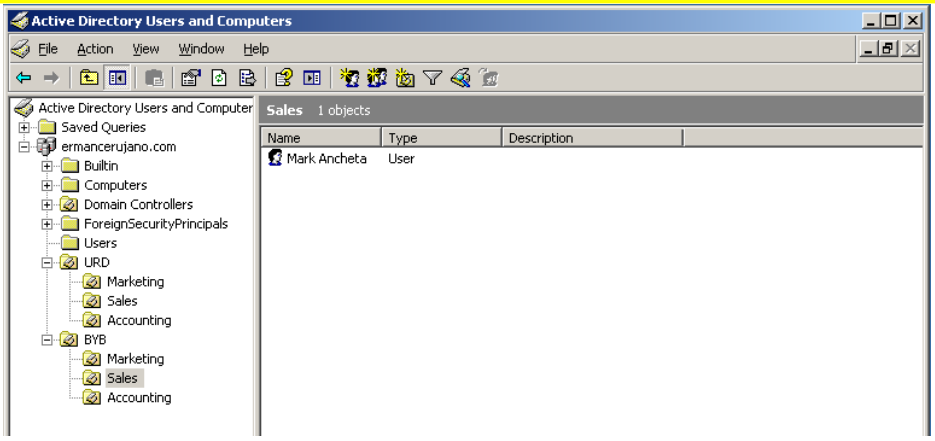
URD – Accounting



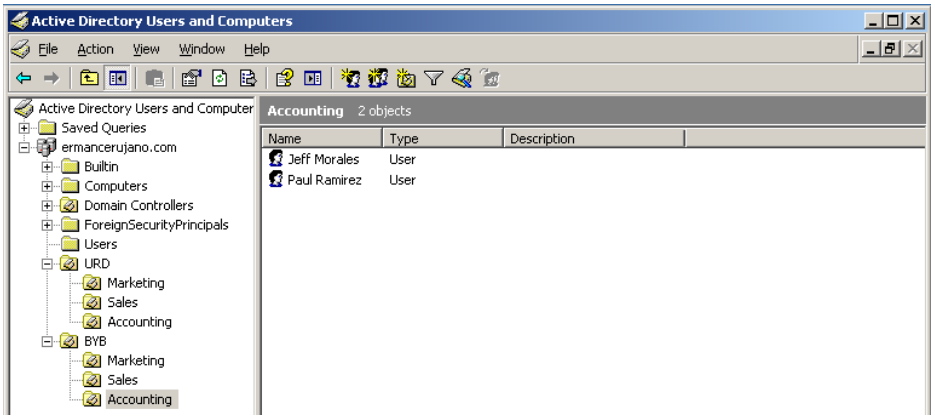
BYB – Marketing



BYB – Sales

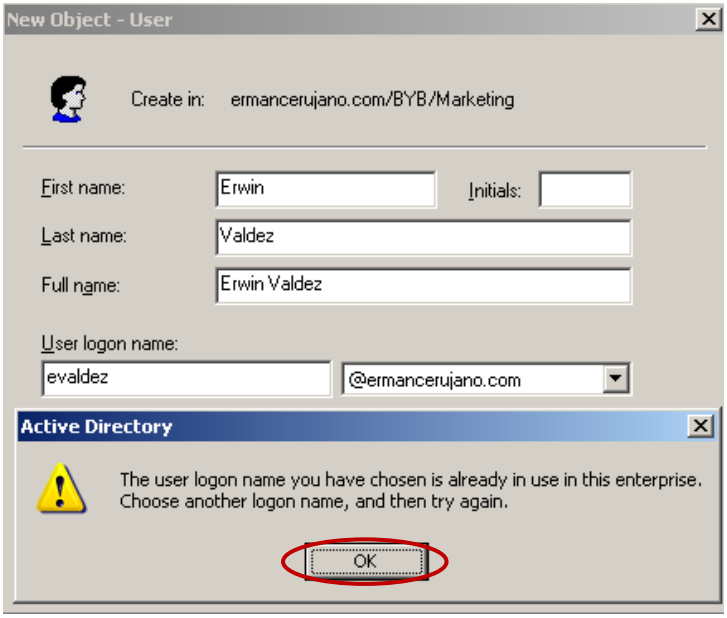


BYB – Accounting



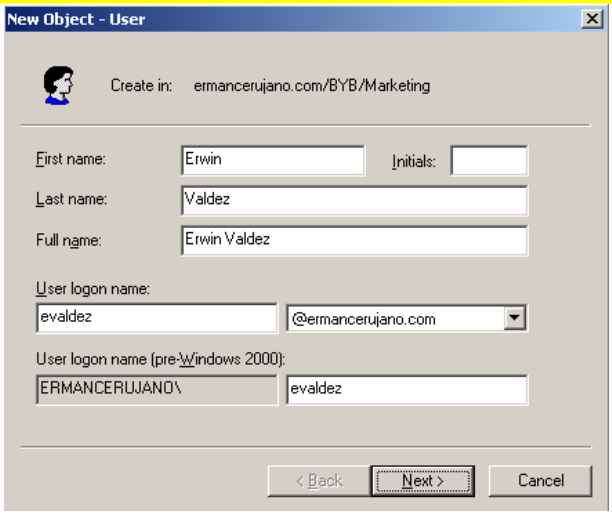
2.3. Moving Objects Between Organizational Units

You cannot have two objects with the same username in your domain; regardless of what organizational unit they are in (technically you can make this work, but it is not worth the hassle and is beyond the scope of this lesson). For example, let's say that the user **Erwin Valdez** is being relocated from the Urdaneta location to the Bayambang Location. If you try to create a user account for **Erwin Valdez** in the **Marketing OU** within the **BYB OU**, you will get an error message when you try to advance to the next screen of the new user wizard.

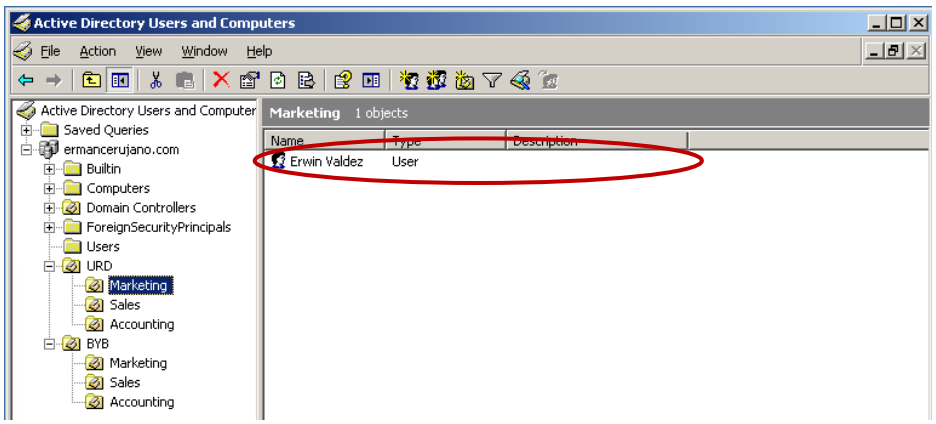


If you follow along, Click **OK**.

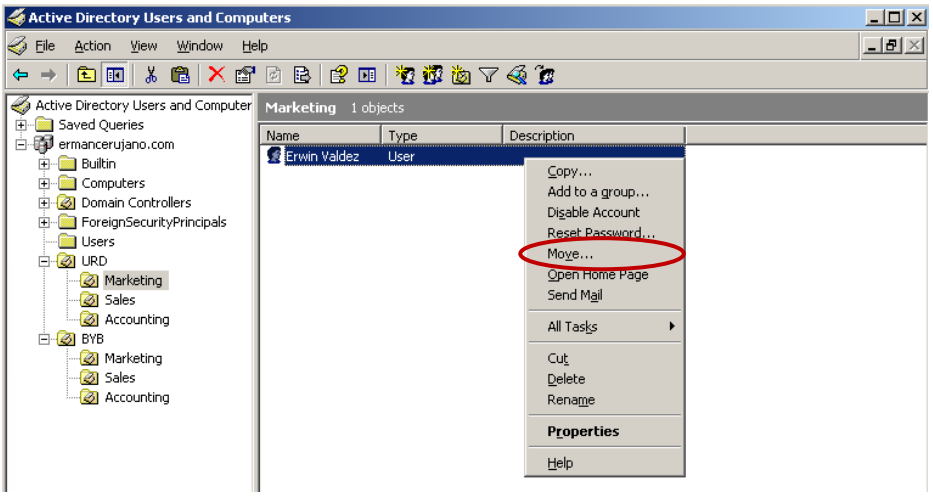
Then click **Cancel** to close the new user wizard.



Instead of deleting a re-creating the user account in the Bayambang-Marketing OU, try moving the user account. Find the user account **Erwin Valdez**, which is located in the **Urdaneta – Marketing OU**.

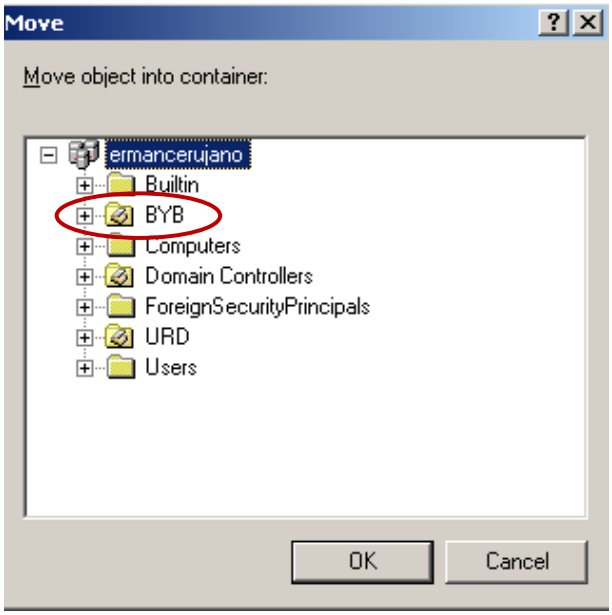


Next, **right click** on the user account and select **Move**.

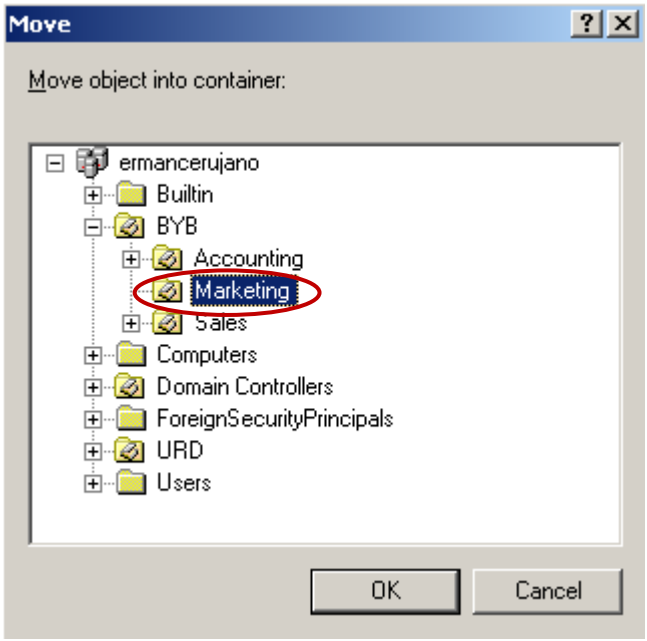


That will bring up a small explorer window where you can browse through all the containers that are available within the domain.

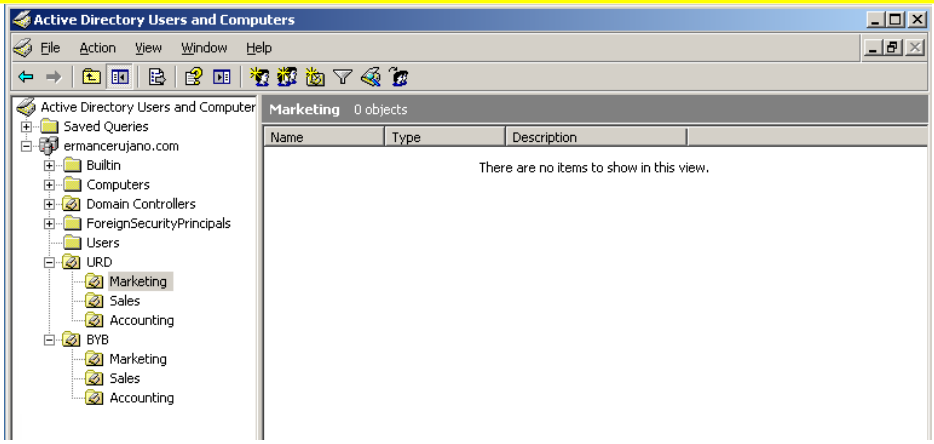
- Open the **BYB OU**



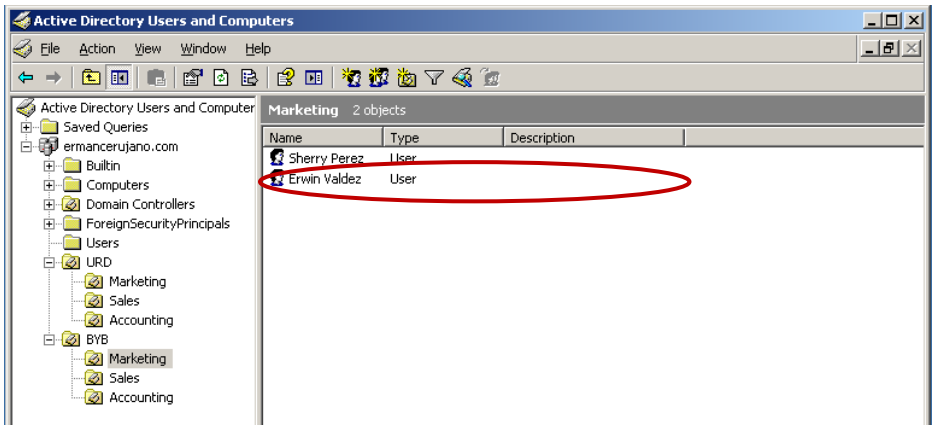
- select **Marketing OU** and click **OK.**



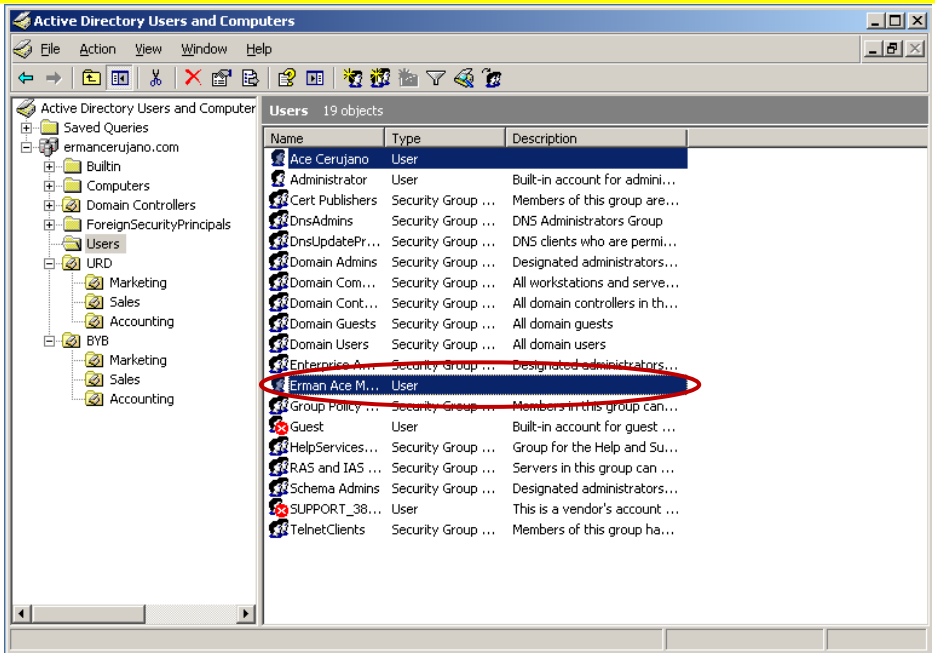
The user account for **Erwin Valdez** should no longer appear in the details pane on the right of the console for **Urdaneta – Marketing OU**.



Now open the **Bayambang – Marketing OU** and you should find the user account for **Erwin Ferrer** located in the details pane of the console.

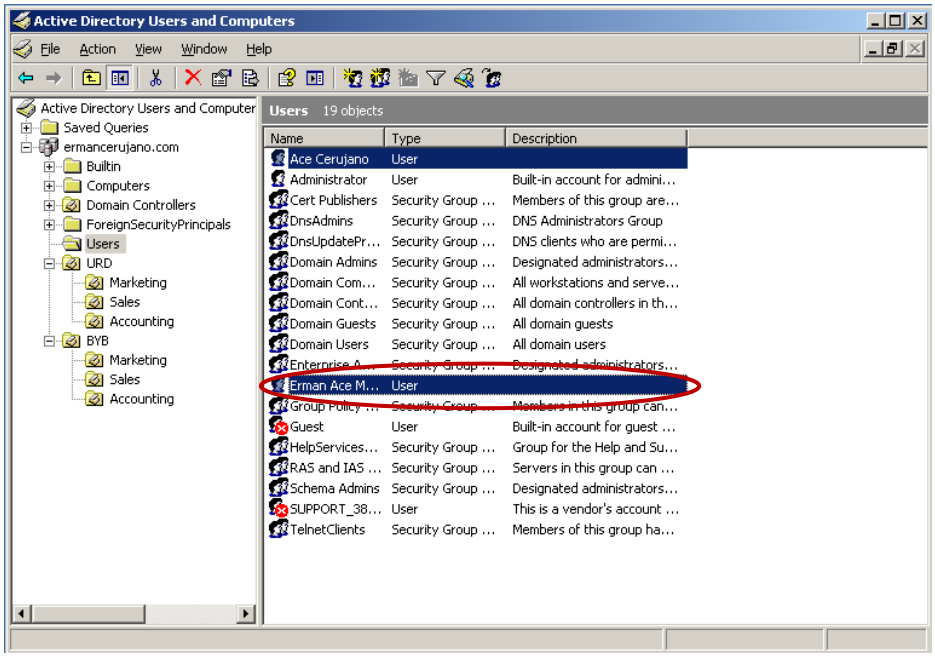


Next, you will move the user account for **Erman Ace M. Cerujano** and **Ace Cerujano** from the Users container to the departments they are a part of. Open the **users** container and find the user account for **Erman Ace M. Cerujano** and **Ace Cerujano**.

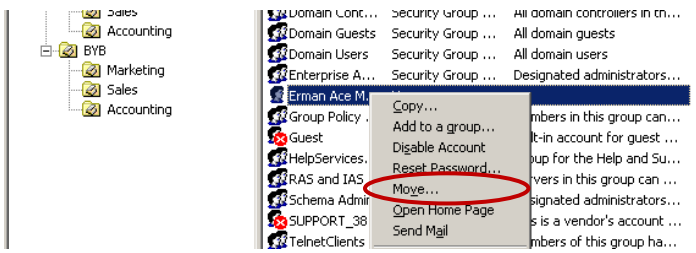


The user account for **Erman Ace M. Cerujano** needs to be place din the **Urdaneta – Marketing OU**.

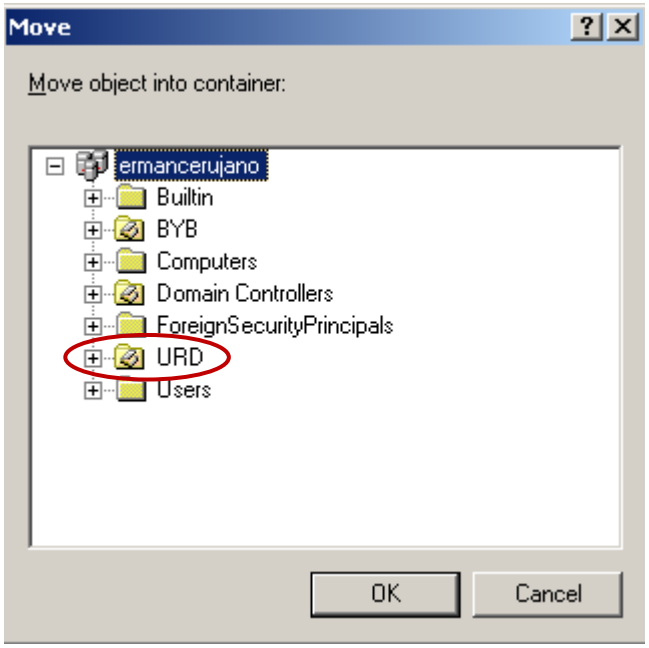
- Right click on the user **Erman Ace M. Cerujano**



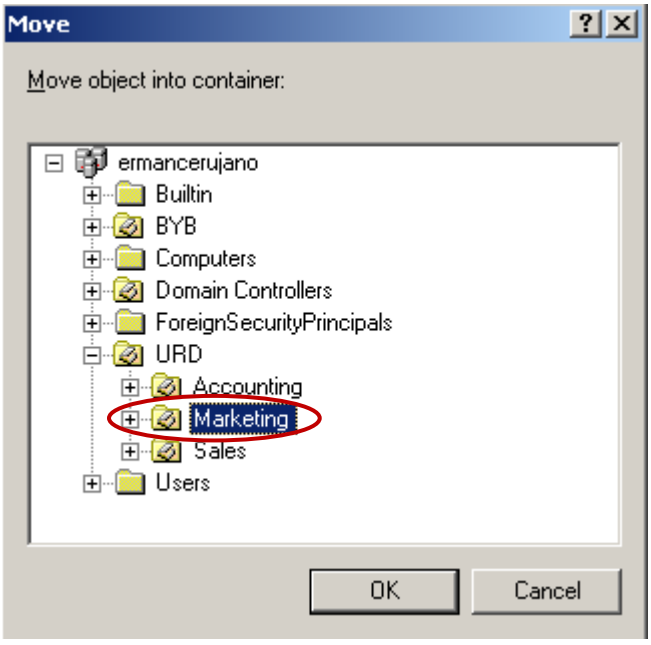
- Click Move



- Select the URD.

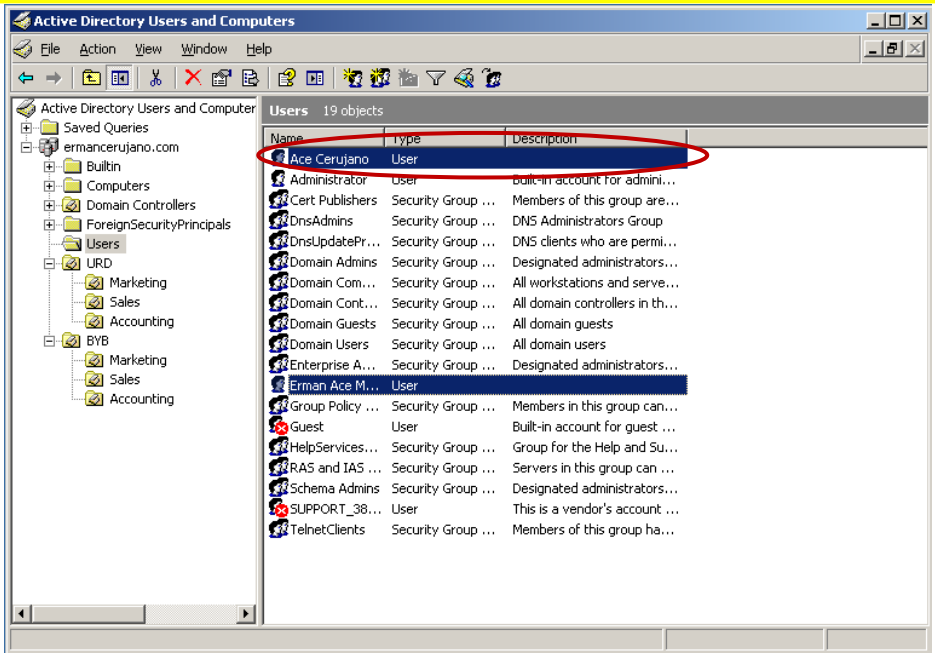


- Select Marketing and click OK.

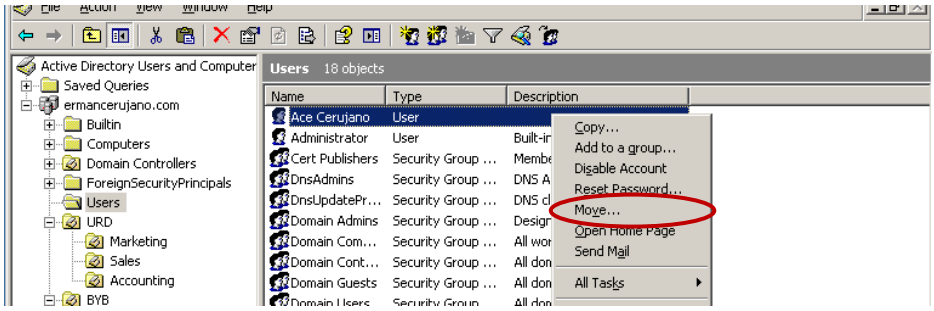


The user account for **Ace Cerujano** needs to be placed in **Bayambang – Marketing OU**.

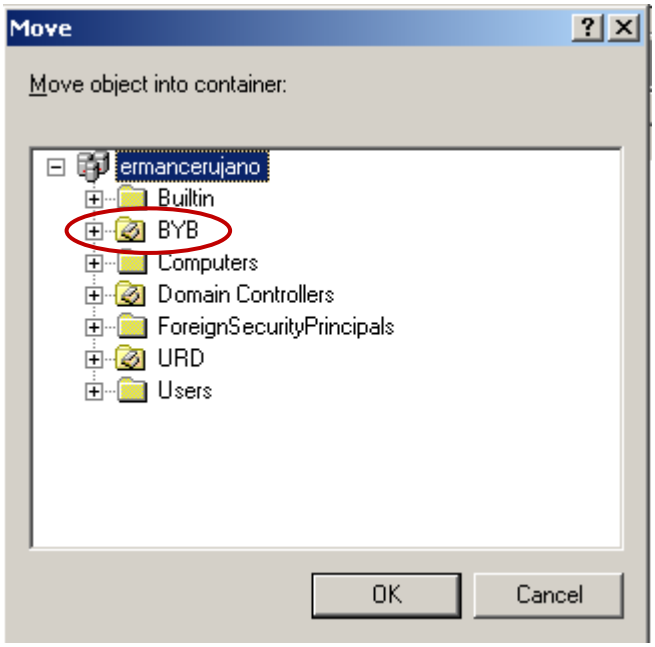
- Right click on the user **Ace Cerujano**



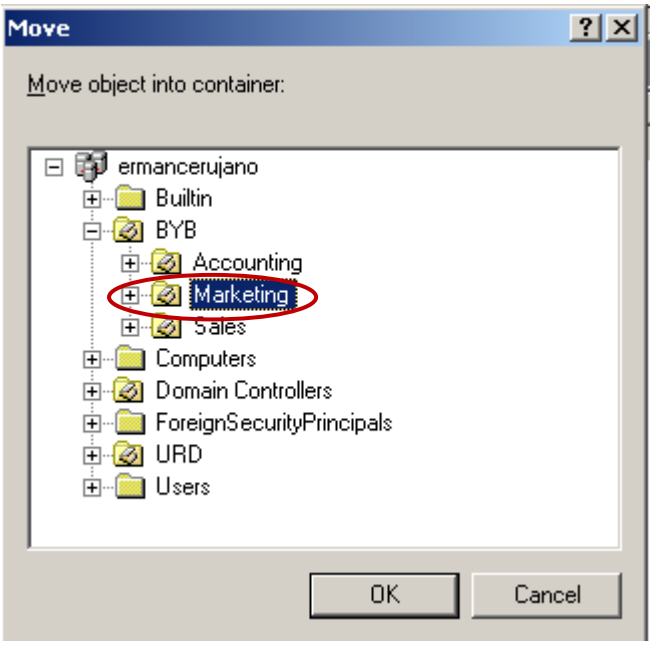
- Click Move.



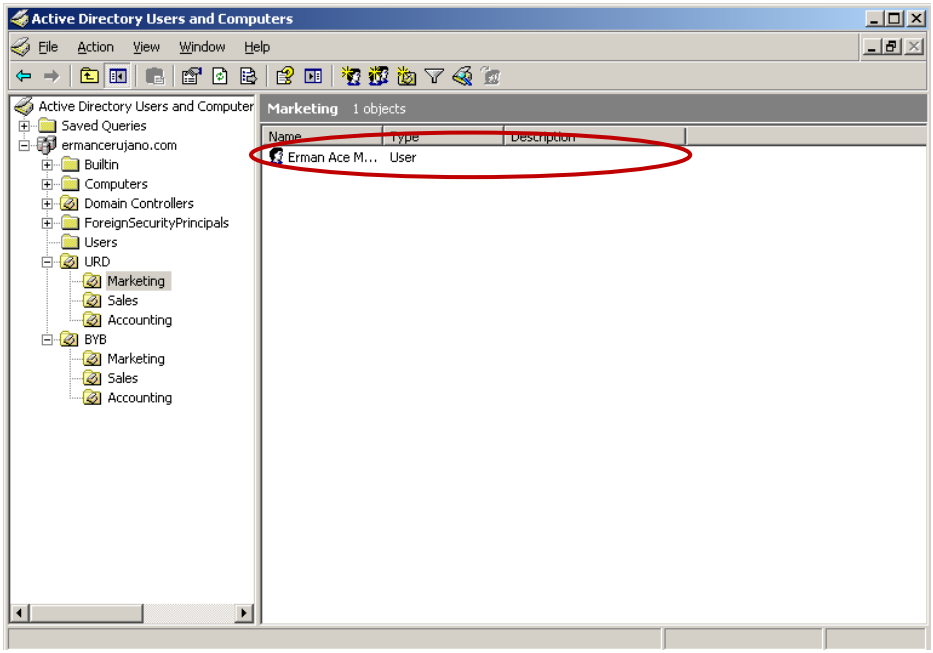
- Select the BYB.



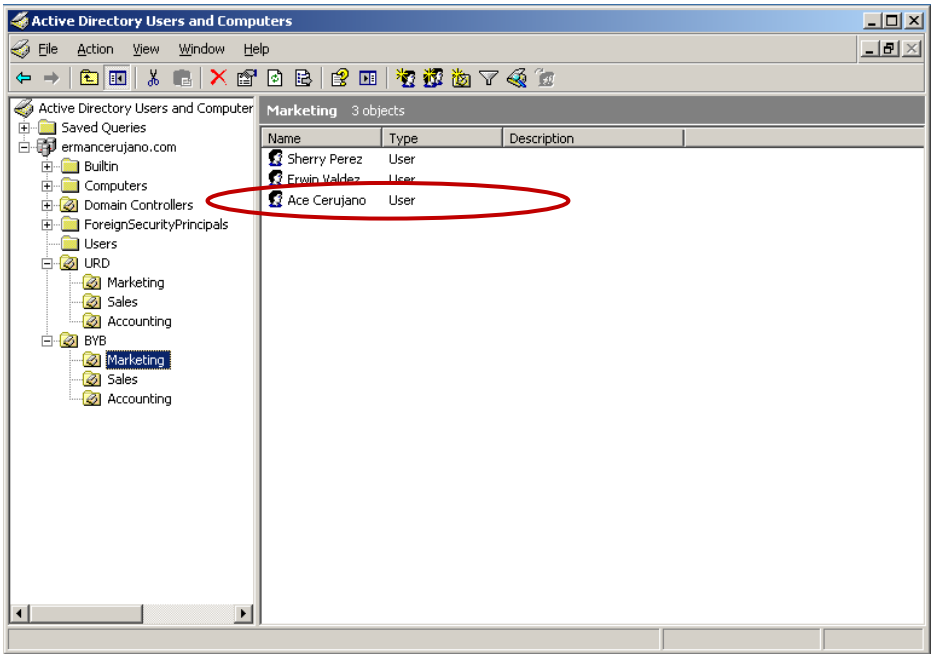
- Select Marketing and click OK.



Now we successfully move **Erman Ace M. Cerujano** and **Ace Cerujano**. We need to recheck it first, go to **URD – Marketing OU** and we need to make sure that **Erman Ace M. Cerujano** is the user in this OU.



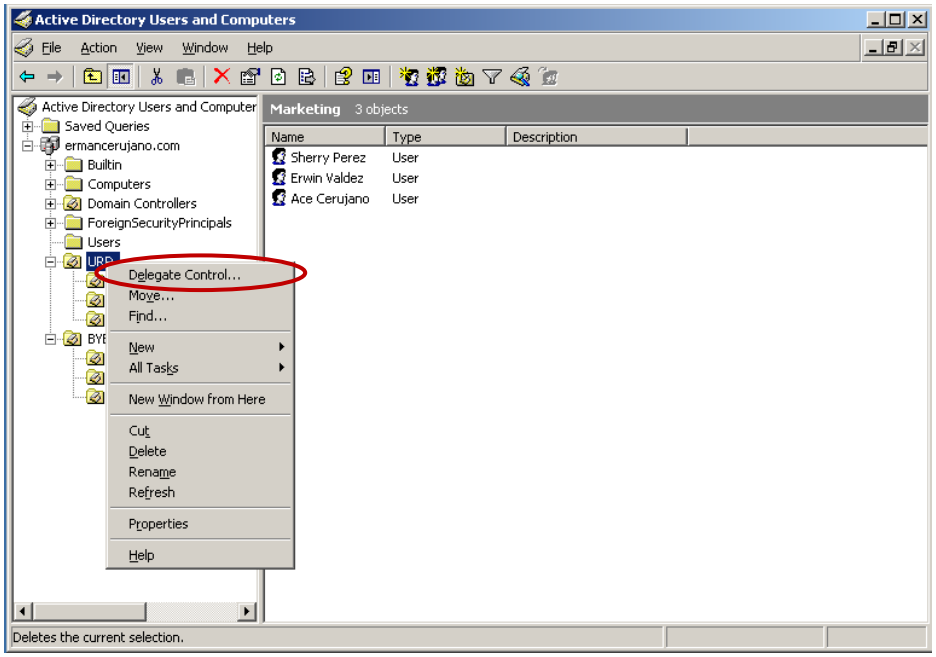
Ace Cerujano should be a user in the **BYB – Marketing OU**.


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
ermancerujano.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
URD
Marketing
Sales
Accounting
BYB
Marketing
Sales
Accounting
Marketing 3 objects
Name Type Description
Sherry Perez User
Erwin Valdez User
Ace Cerujano User

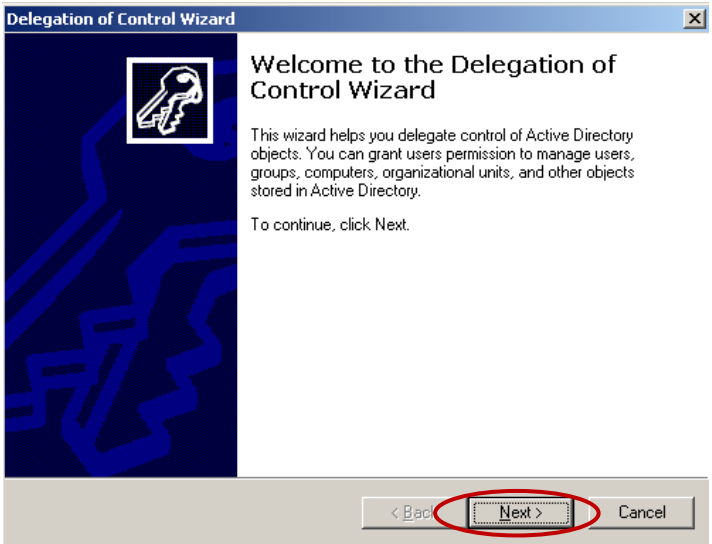
2.4. Delegate control of Organizational Units

By using Organizational Units (OUs), you can delegate control of tasks for an OU to a particular user or group that may not have any administrative privileges to perform these tasks. That user or group can then administer the tasks and only those tasks that were delegated to them. For example if a user in accounting is delegated control of resetting passwords for the Accounting OU in California, they will only be able to reset passwords for that OU. If the user tried to reset a password anywhere else in the domain they will be denied.

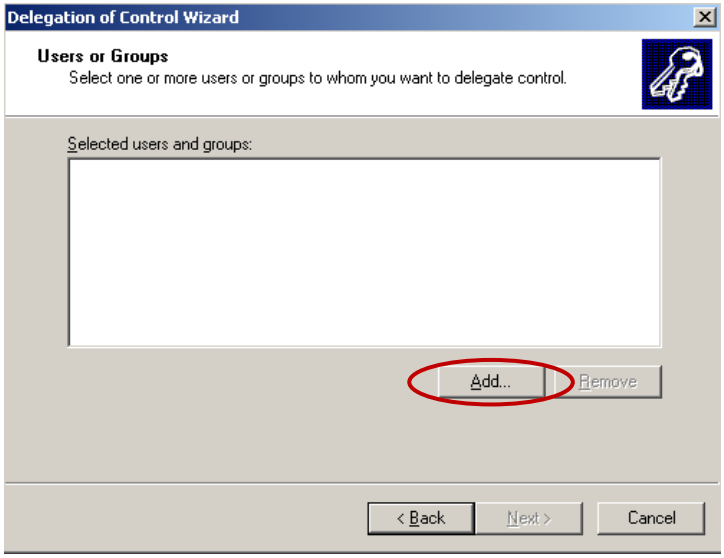
On the Active Directory Users and Computers Console, right click on the **URD OU** and select **Delegate Control.**



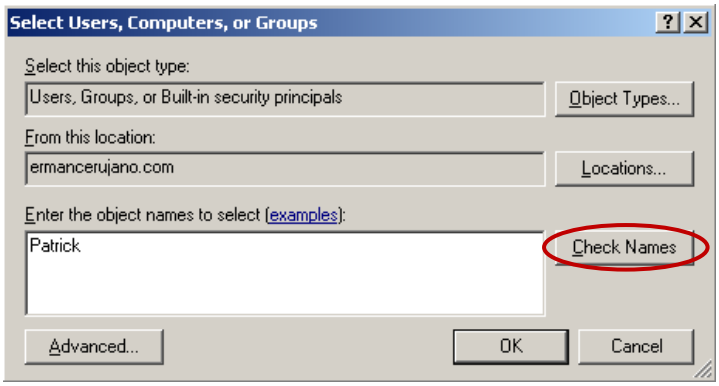
This will start the delegation of control wizard, click **Next**.



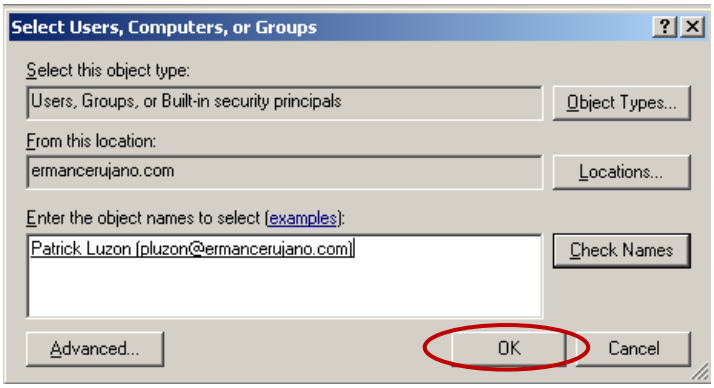
You will have to select the users or groups that you want to delegate control to. Click on **Add** and you will have another screen appear.



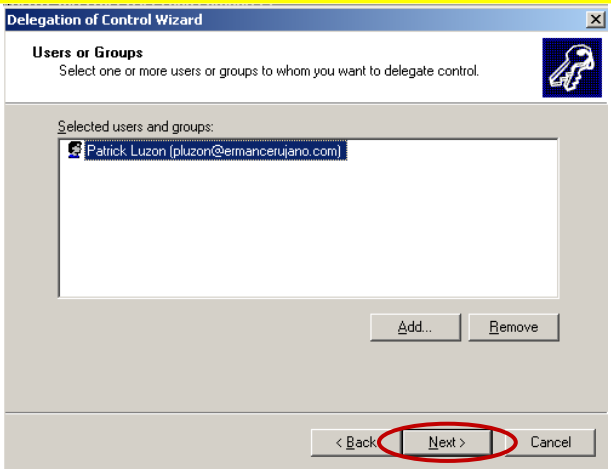
Type **Patrick** and click **Check Names**.



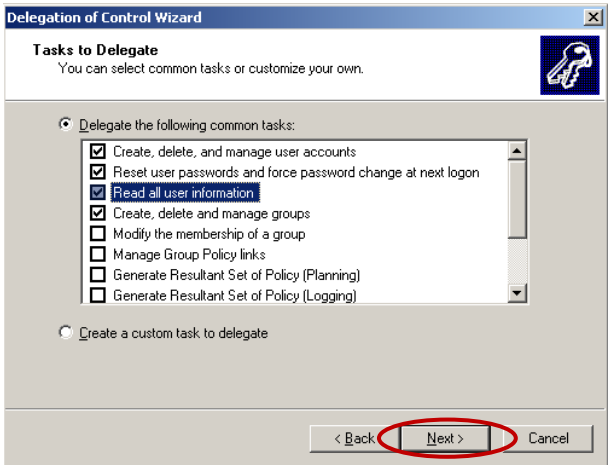
As you can see, it will display the information of the name that you enter. Click **OK**.



You should now have the user named **Patrick Luzon** appear as the selected user that you want to delegate control to. Click **Next**.



The next screen will show you some of the possible tasks that can be delegated to this user. Microsoft selected six of the most common tasks that administrators may want to delegate. If none of these tasks are what you want, you can also choose to create a custom task to delegate. Creating a custom task to delegate is a lot more complex, especially if you are not very familiar with Active Directory Security. Use the tasks that are supplied by Microsoft until you become a Windows Server expert or have excellent documentation to guide you. Select the first four **common tasks** that are supplied, which will give **Patrick Luzon** all of the control he needs without giving him too much control and then click **Next**.



The final screen of the wizard will give you a summary of the selection you made. Confirm that all of the information is correct and click **Finish**.


Delegation of Control Wizard
Completing the Delegation of Control Wizard
You have successfully completed the Delegation of Control wizard.
You chose to delegate control of objects in the following Active Directory folder:
ermancerujano.com/URD
The groups, users, or computers to which you have given control are:
Patrick Luzon (pluzon@ermancerujano.com)
You chose to delegate the following tasks:
To close this wizard, click Finish.
< Back
Finish
Cancel

2.5. Test Delegated Organizational Units

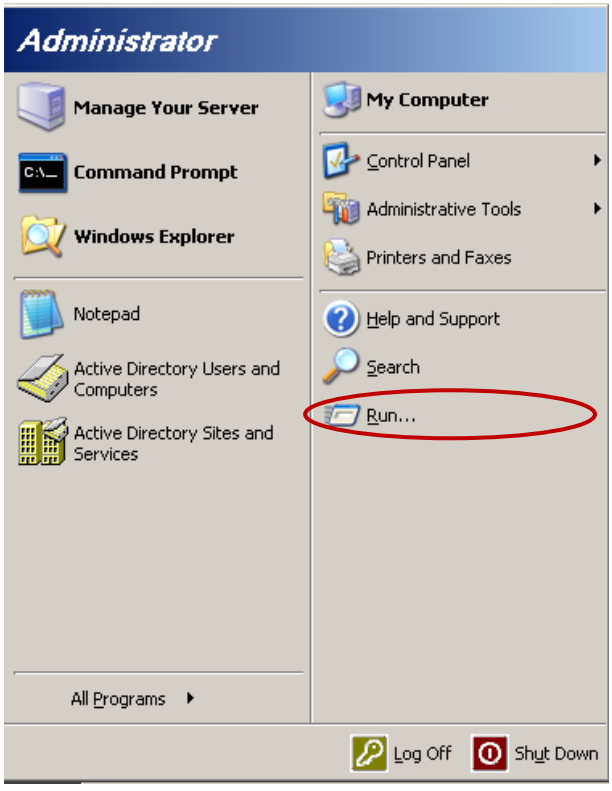
In order for the user to access the **Active Directory Users and Computers** console, you will need to remotely configure his computer (the Windows XP professional machine at his desk) to make him **a local administrator**. This will give him administrative privileges to his local computer only, **not the domain**. the user will then be able to install the **adminpak.msi** file that is located on the **i386** folder of the **Windows Sever 2003 CD-ROM**.

The adminpak.msi file will install the administrative tools for the domain on the computer because Windows XP does not include the Active Directory administrative tools. You will then need to create a management console for Active Directory Users and Computers so that the user can easily access the tools he will need without giving him access to all the administrative tools. Then you will have to create a share for this user to be able to access the files he needs over the network.

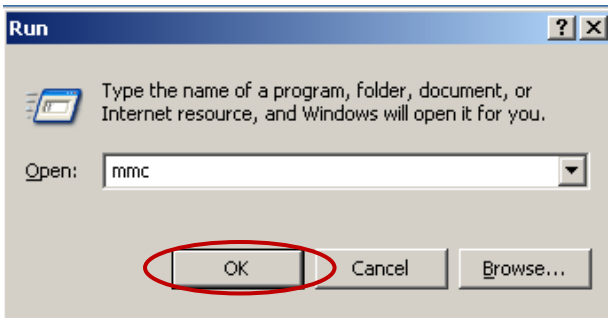
Log on to **Server11** as the domain administrator. Now create a management console to connect to **client1's** local users and group snap-in tool. To do that

- Start

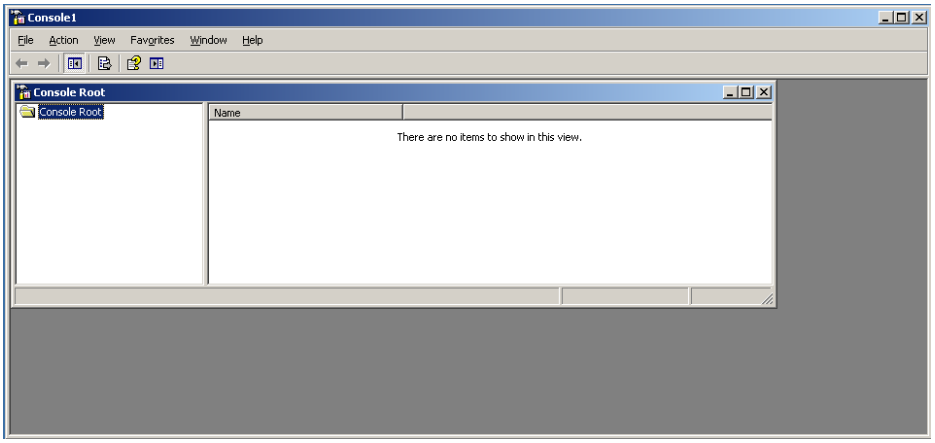
- Run



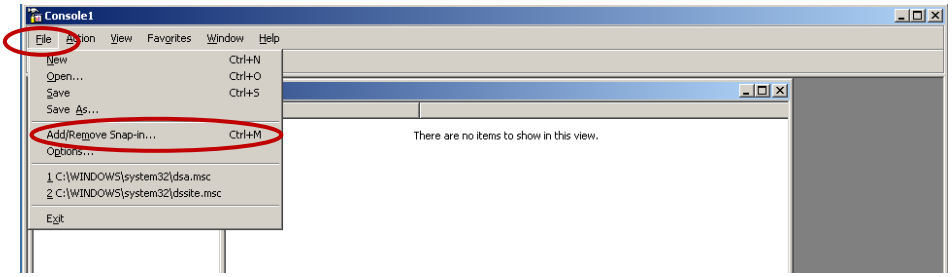
- Type **mmc** and click **OK**.



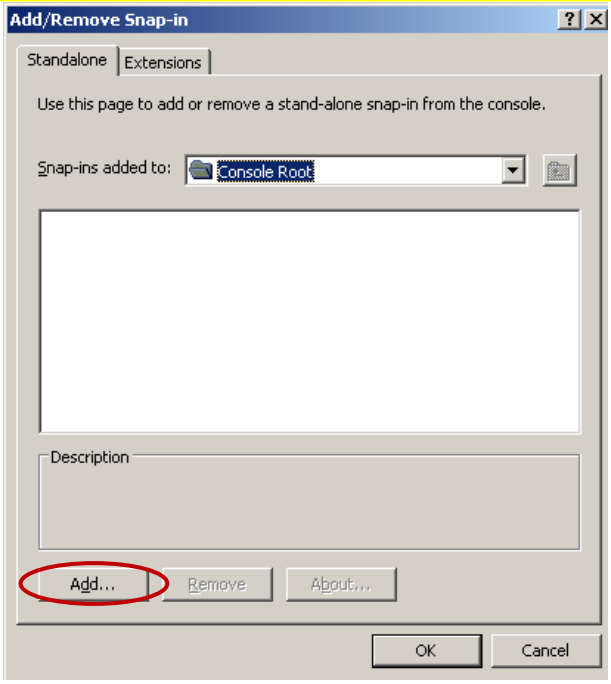
That will bring up an empty management console.



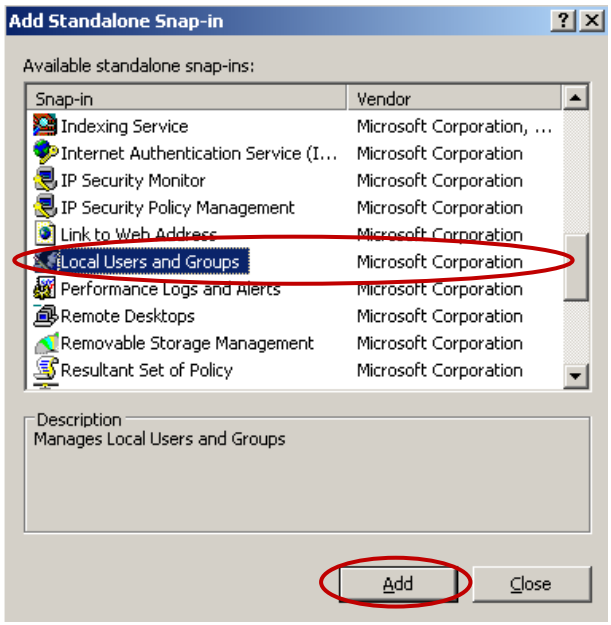
On the top menu select File then Add/Remove snap-in.



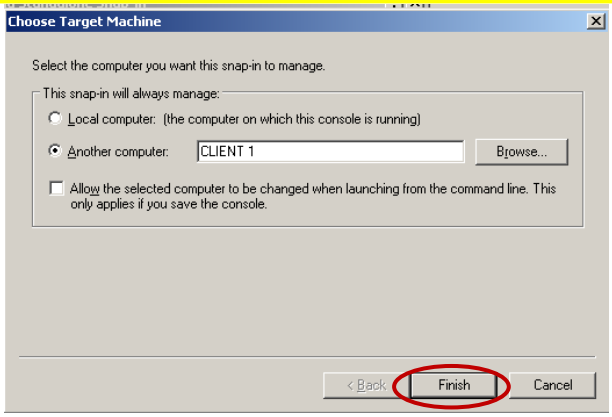
That will bring up another empty screen, which is where you add the snap-in tools that you want to use. Click on **Add** to bring up a list of available tools that can be added.



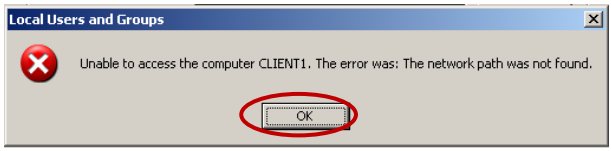
Select **Local Users and Groups** then click **Add**.



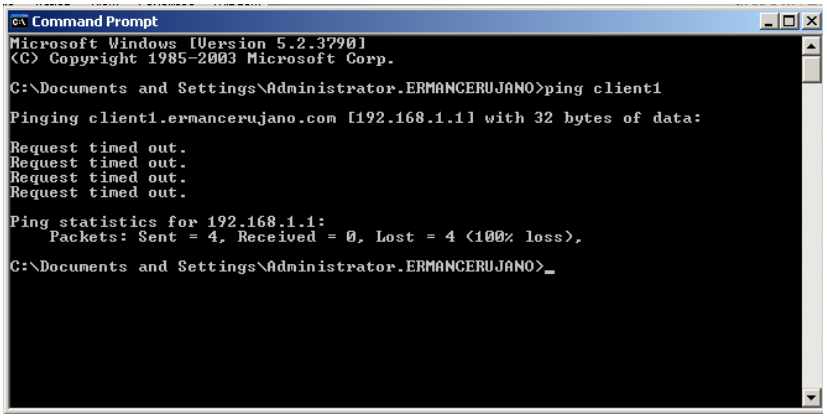
You will be asked to select the computer you want to manage with this snap-in tool. By default, it will have the local computer you are on selected, but you want to manage the computer **client1**. Select the option for **Another computer** then click **Browse** the ermancerujano.com domain for **Client1** or simply type in **client1** and click **Finish**.



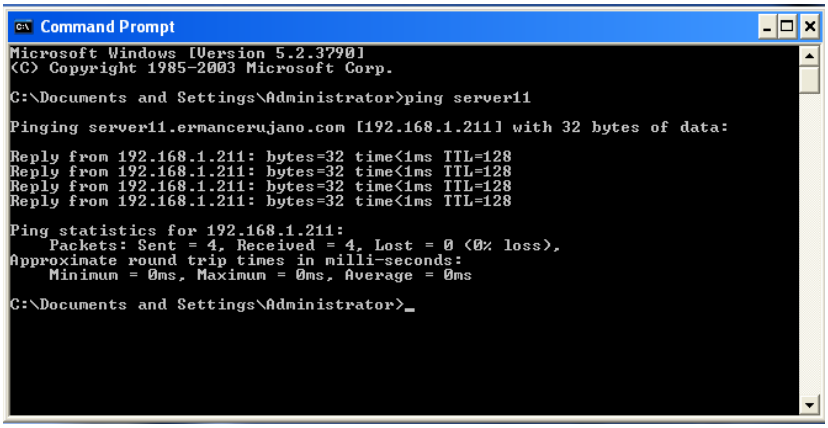
You might encounter some problem like this.



The first thing that you need to do is to ping client1 from the Server11.

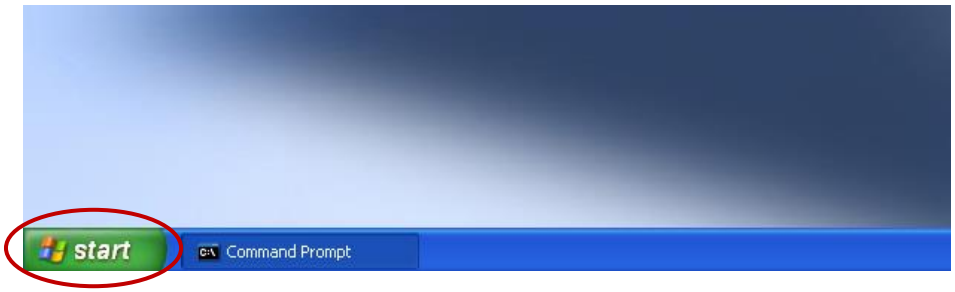


We need to check first if we can ping the server from client1. Go to client1 and ping the server11.

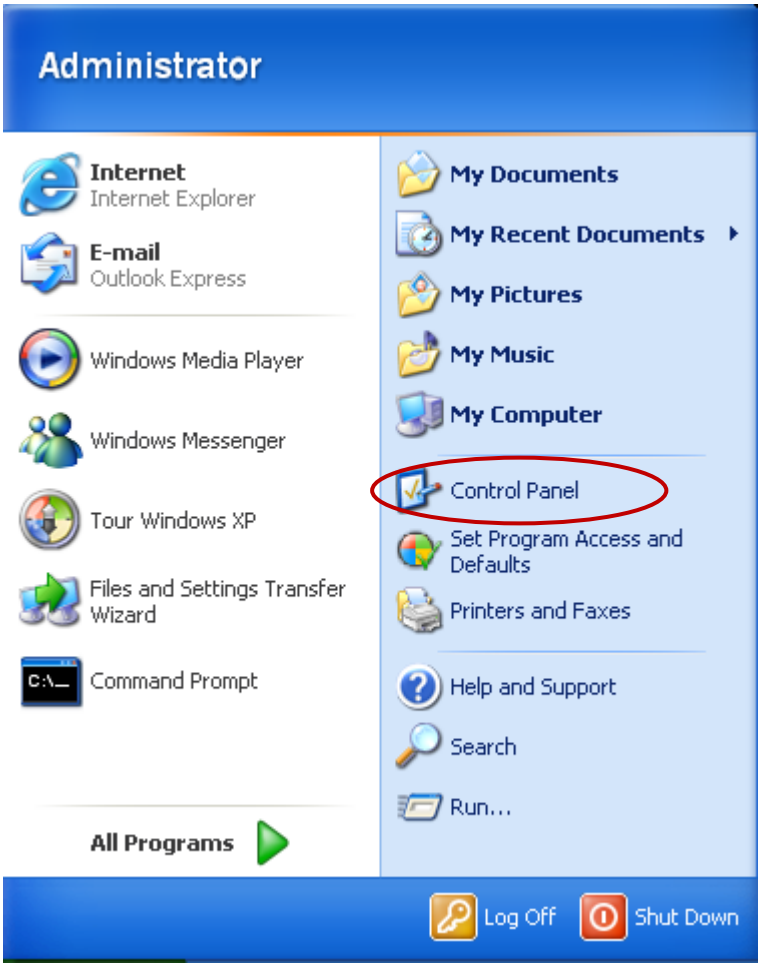


As you can see, we can ping the Server11 from client1. We need some configuration into our client1 so that we can ping it from the server side. One factor that blocking the server from pinging the client1 is because of the firewall. We need to turn off first the firewall of our client1. To do that go to client 1:

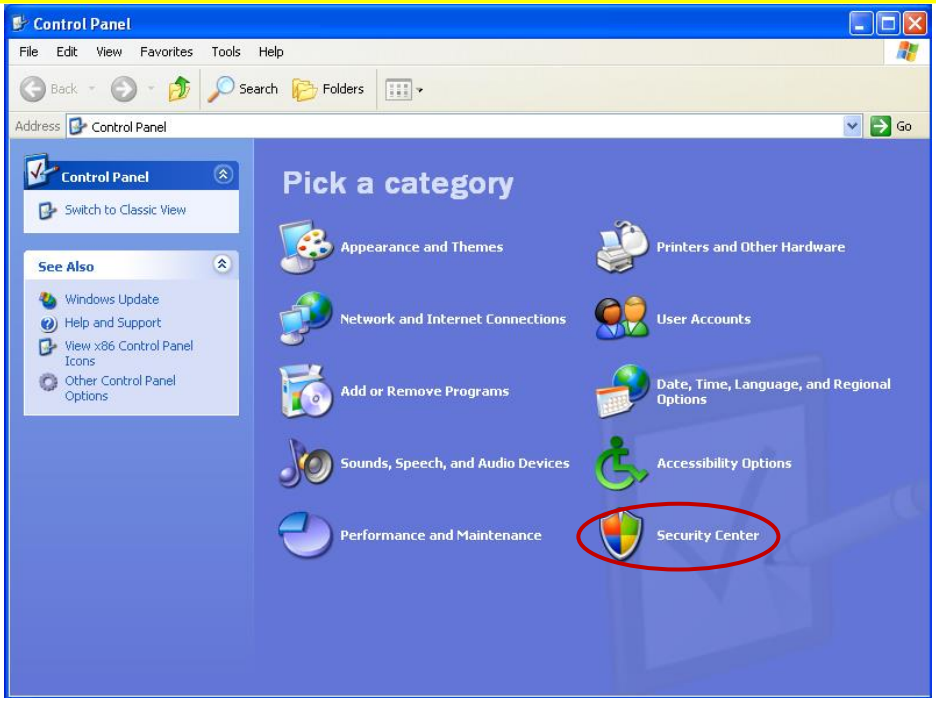
- Start



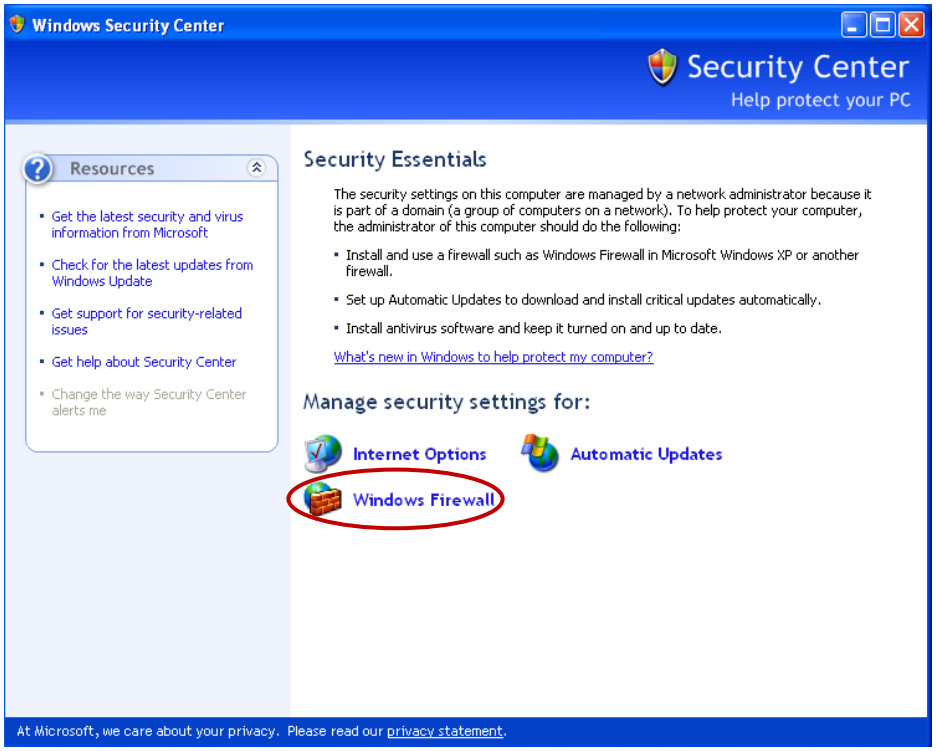
- Control panel.



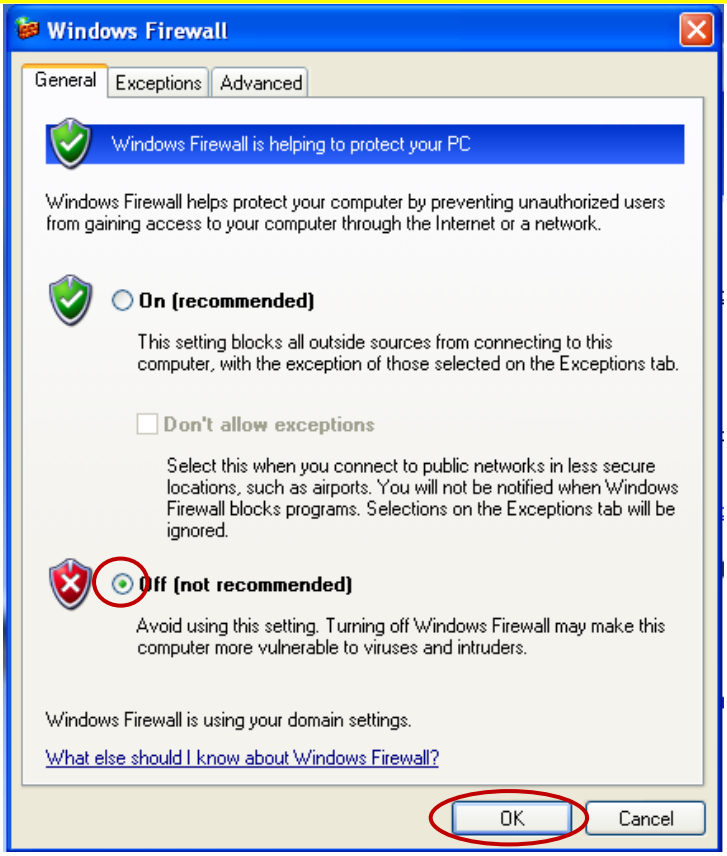
- Security Center



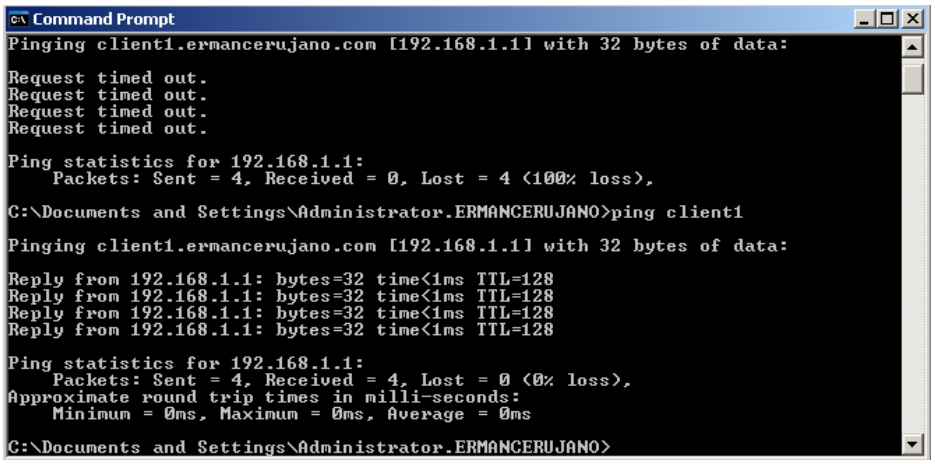
- Select the Windows Firewall.



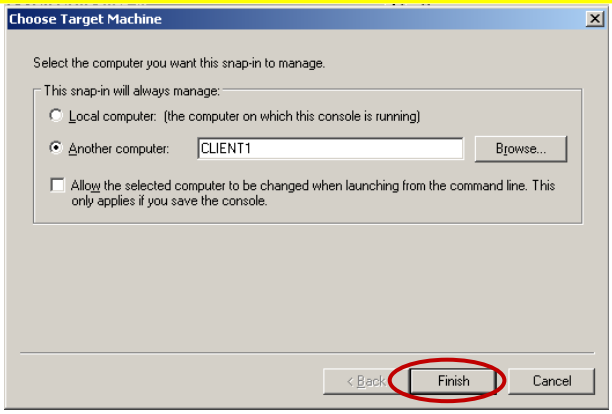
Select the **Off(not recommended)** and click **OK**.



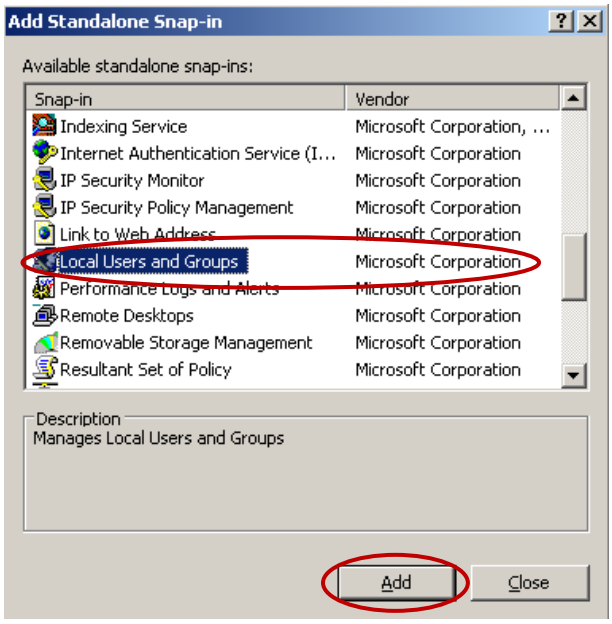
Go to our server11 and try to ping client1.



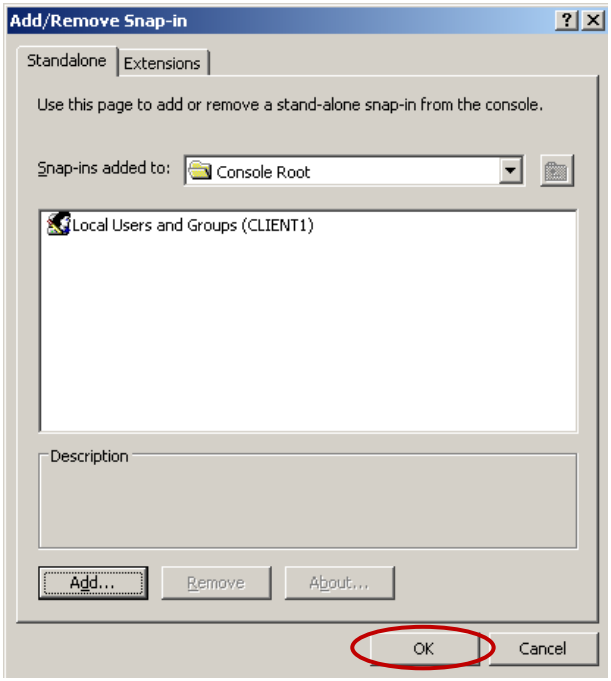
As you can see now, we can now ping client1 from our Server. We can now continue configuring our Active Directory. Browse again the computer then click Finish.


Choose Target Machine
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer on which this console is running)
Another computer:
CLIENT1
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel

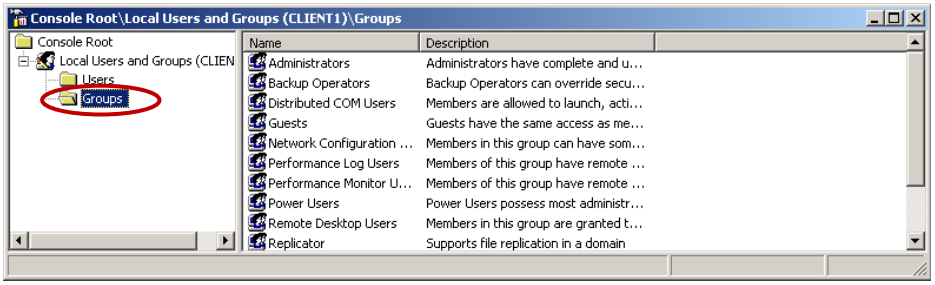
Click **Close.**


Add Standalone Snap-in
Available standalone snap-ins:
Snap-in
Vendor
Indexing Service
Microsoft Corporation, ...
Internet Authentication Service (I...
Microsoft Corporation
IP Security Monitor
Microsoft Corporation
IP Security Policy Management
Microsoft Corporation
Link to Web Address
Microsoft Corporation
Local Users and Groups
Microsoft Corporation
Performance Logs and Alerts
Microsoft Corporation
Remote Desktops
Microsoft Corporation
Removable Storage Management
Microsoft Corporation
Resultant Set of Policy
Microsoft Corporation
Description
Manages Local Users and Groups
Add
Close

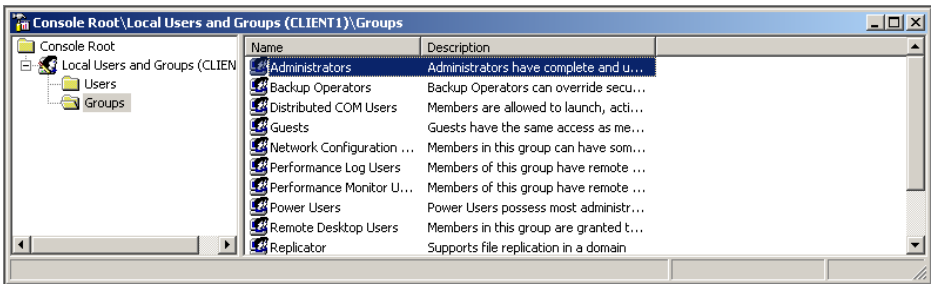
Click **OK**.



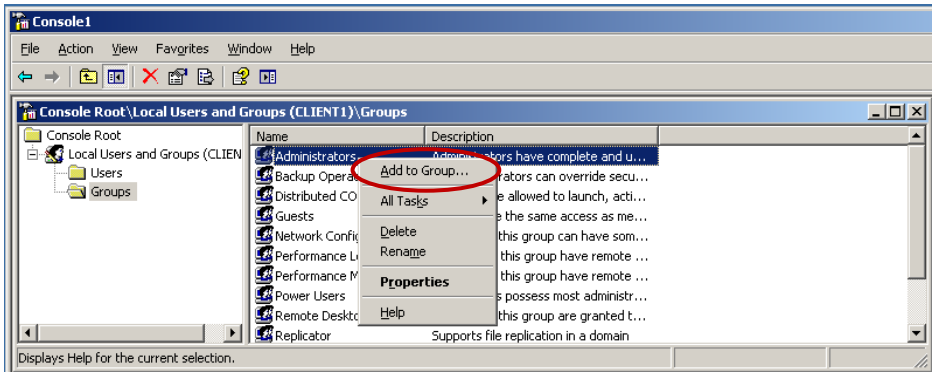
This will bring you back to the management console within the local users and groups snap-in tool for client1. You want to add the **domain** username **pluzon** to client1's local **Administrators** group. In the left pane open the **Groups** folder,



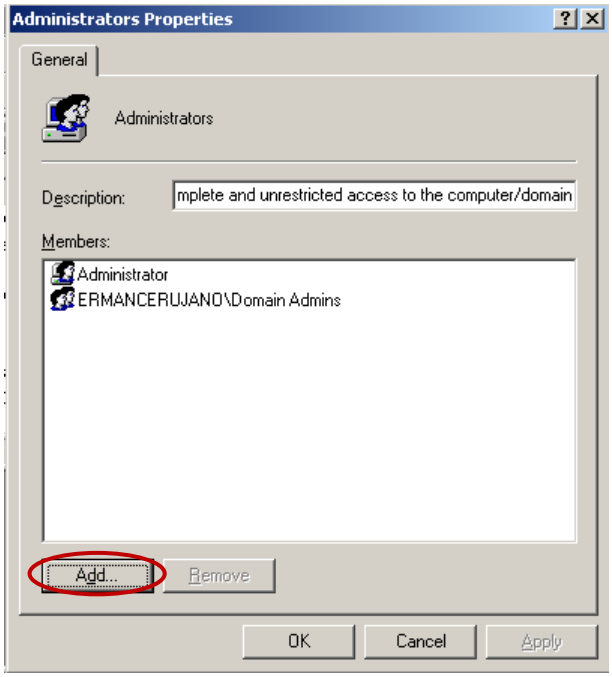
Then in the detail pane, right click on the **Administrators** group.



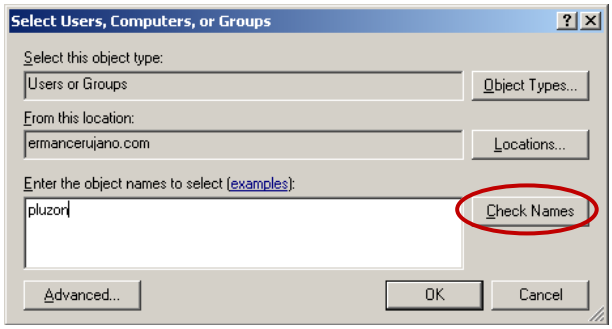
Select **Add to Group**.



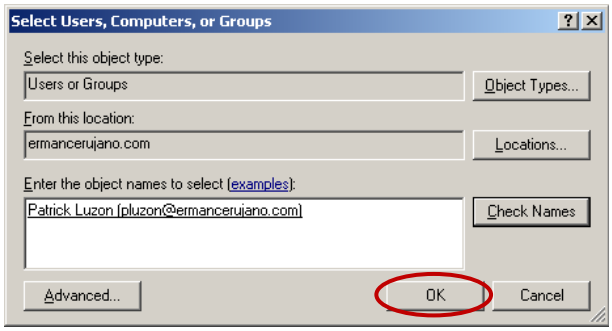
Click the **Add** button.



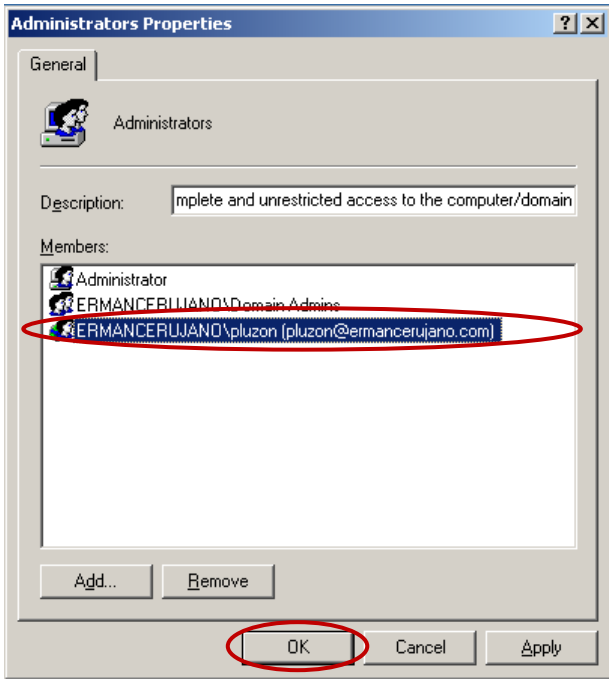
Type in **pluzon** and Click **Check Names**.



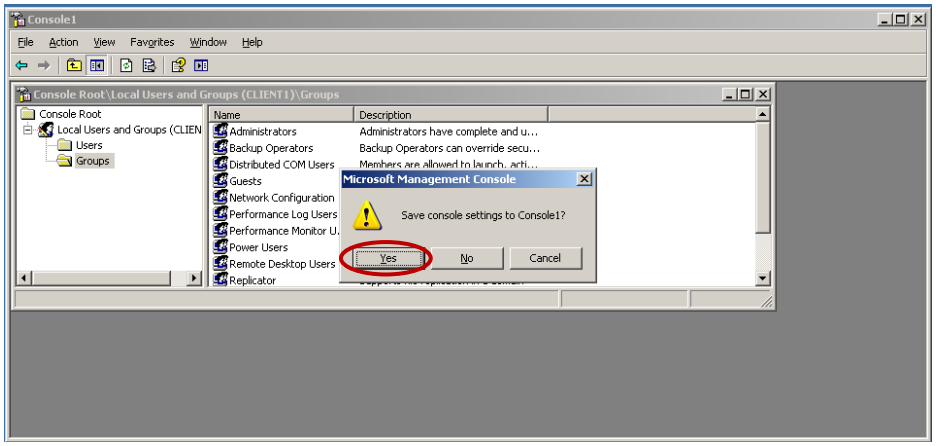
Click **OK**.



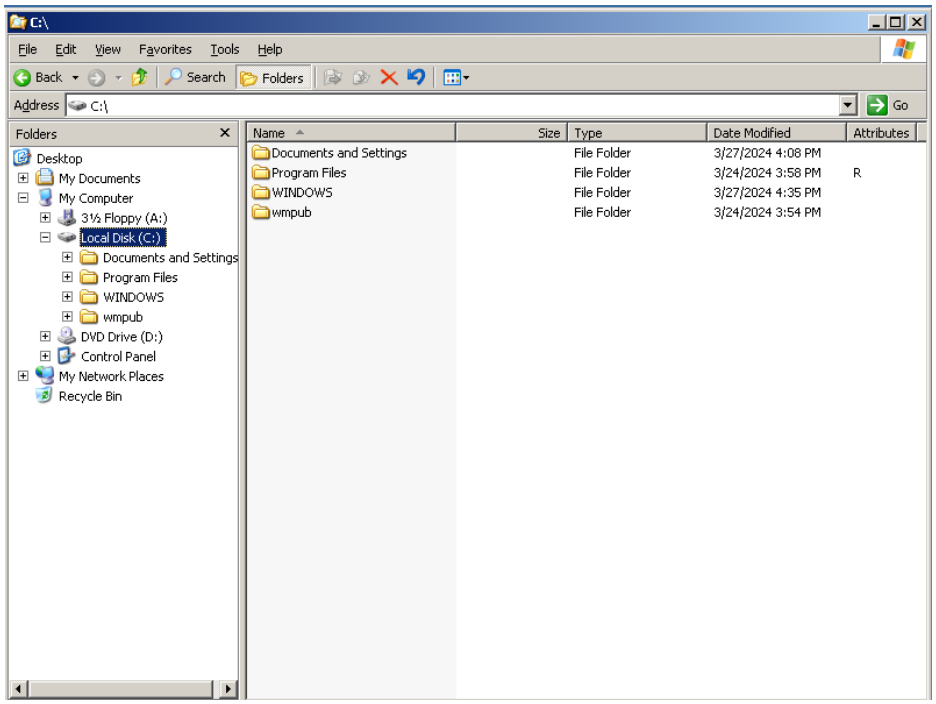
That will bring you back to the list of members in this local administrators group. Look to make sure that the user **ERMANCERUJANO/pluzon** appears on the list and click **OK**.



The user **Patrick Luzon** is now a member of the local administrators group for the computer **client1** only. He will not have any administrator privileges for the domain or any other computer in the domain, except for **client1**. Now close the management console without saving it. This is not a tool you will be using very often and it's easily accessible if it's ever needed again.

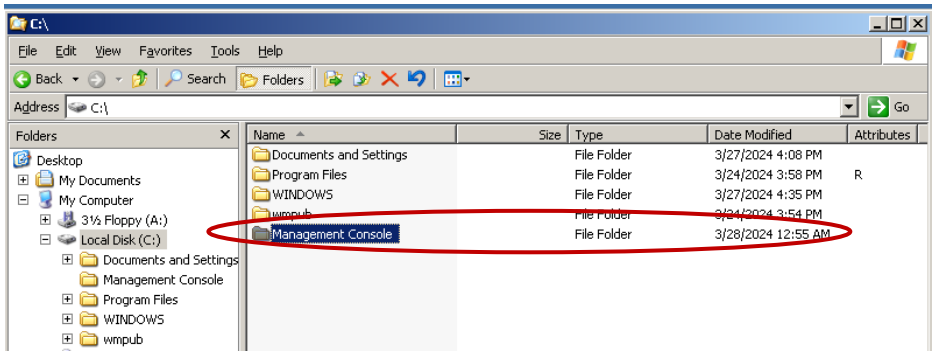


Now open the **C: drive**, using **Windows Explorer**.

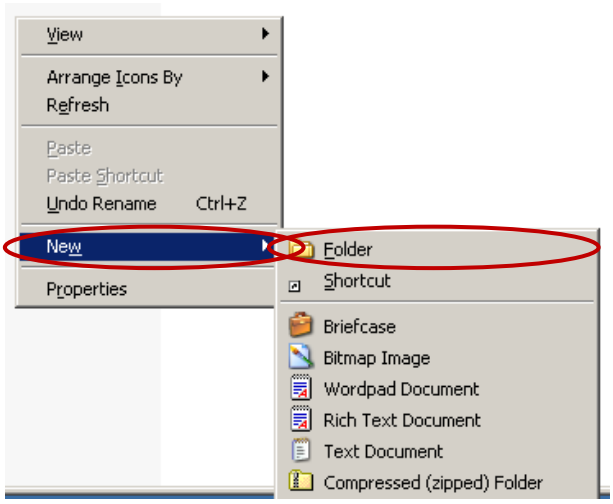


Create a new folder named **Management Console** to place the files the user will need.

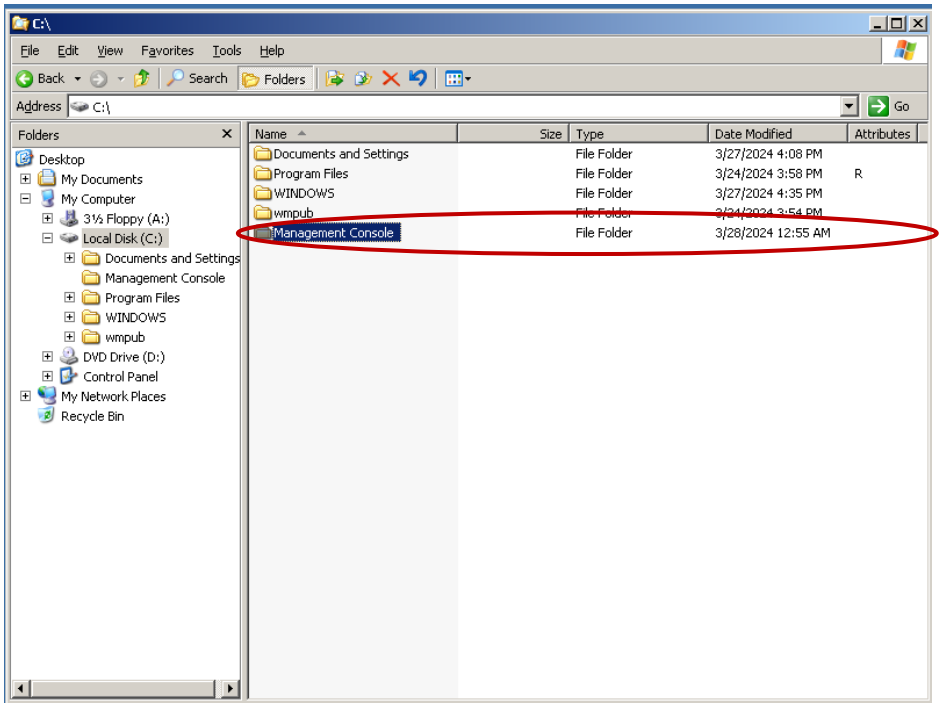
- Right click on the empty space.



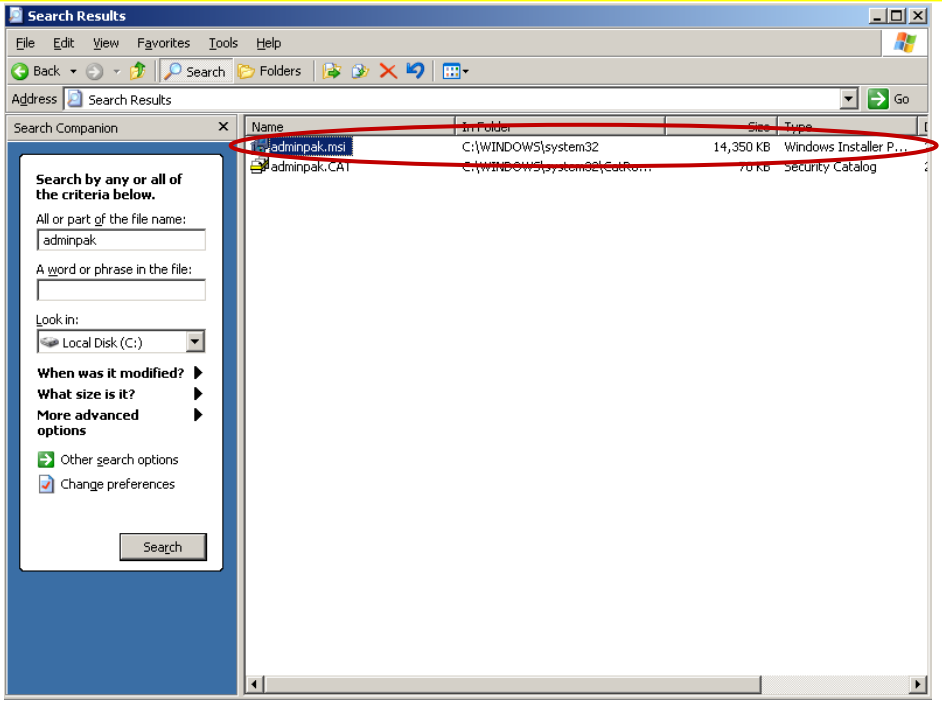
- Select **New** then **Folder**.

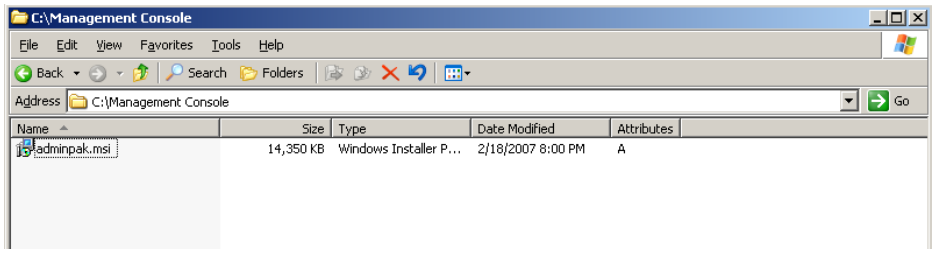


Name the folder to **Management Console**.



Next, insert the **Windows Server 2003 CD ROM** and copy the **ADMINPAK.msi** file located in the **i386** folder to the folder you just created named **Management Console** on the **C: Drive**.



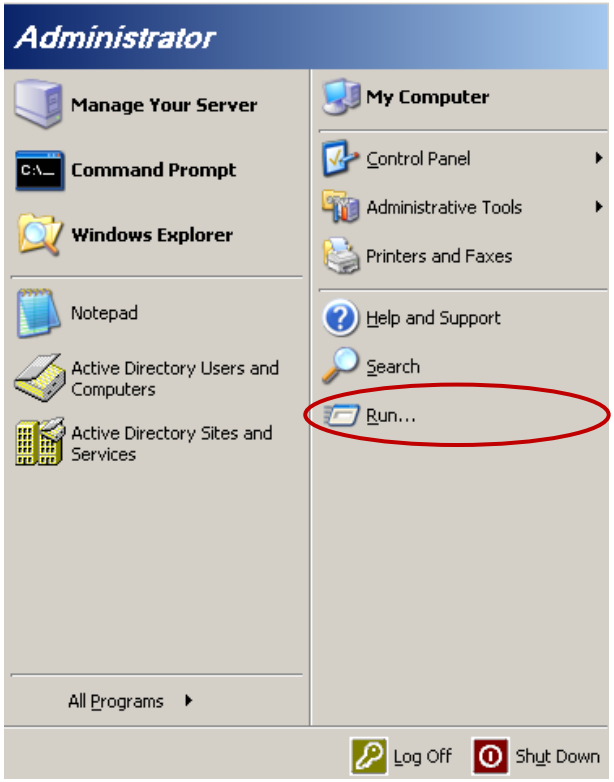


Now you need to create a management console with the Active Directory users and computers snap-in tool and save it in the management console folder. This will make it easier for the user to manage the OU and it will keep all the other administrative snap-in tools out of site.

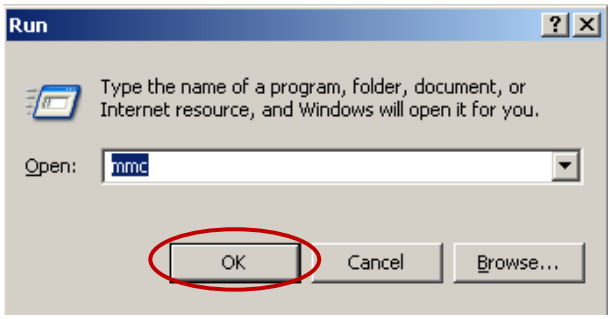
Go to

- Start

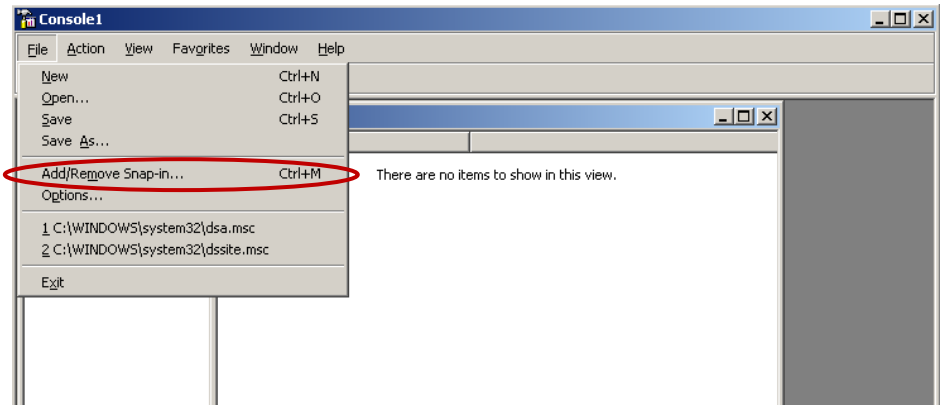
- Run



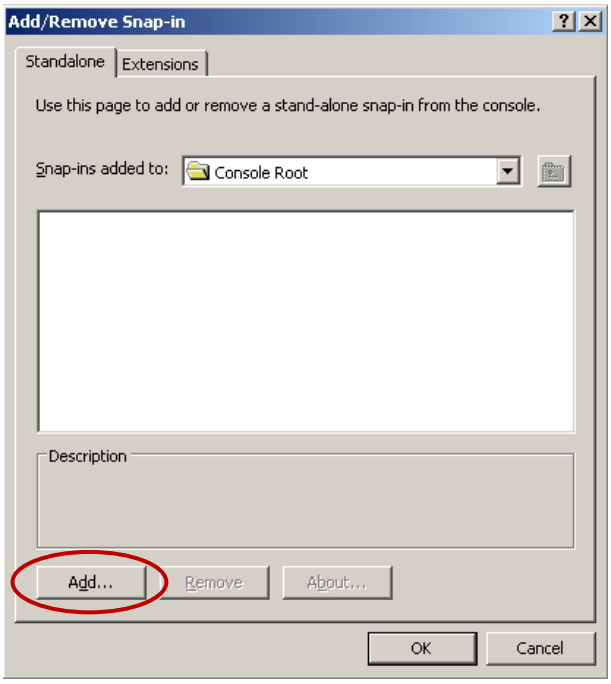
- Type mmc in the command prompt and click **OK**.



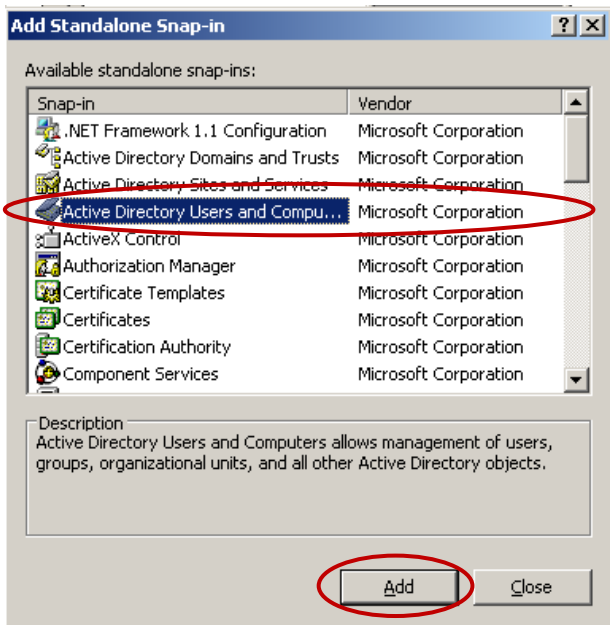
This will open an empty console. On the menu select **File** then **Add/Remove Snap-in**.



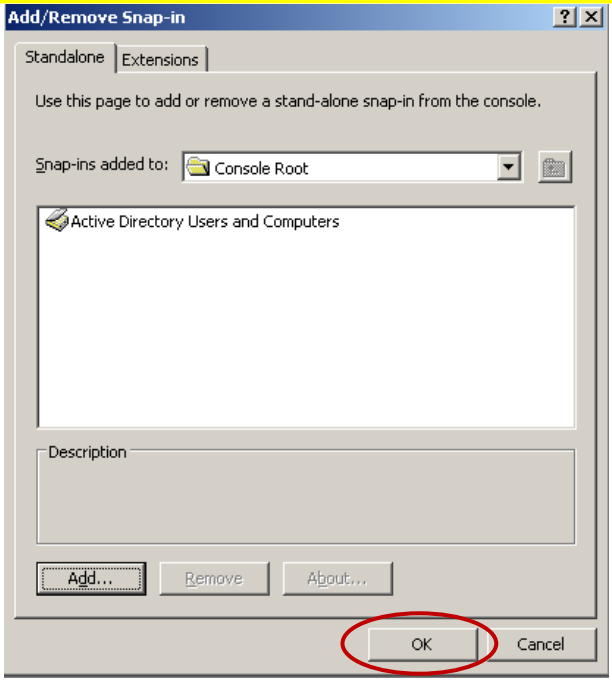
On the next screen click **Add** to see a list of available snap-in tools.



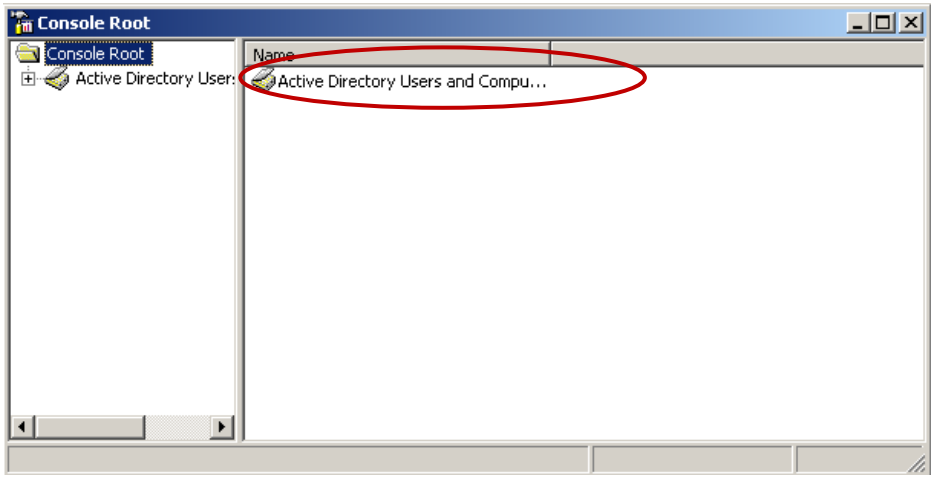
Select **Active Directory Users and Computers** then click **Add** and **Close**.



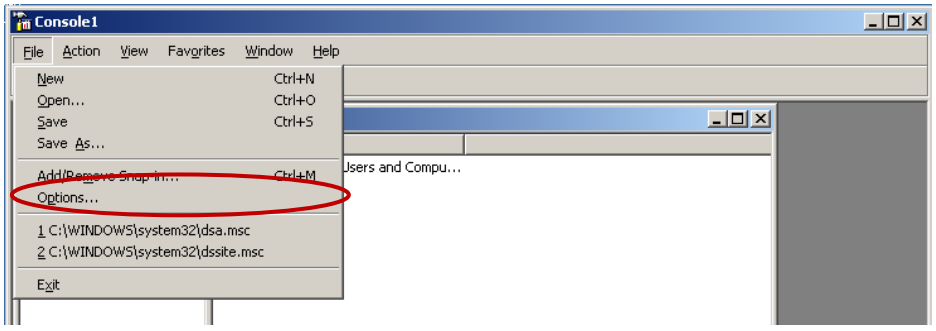
Then, click **OK** on the next screen**.**



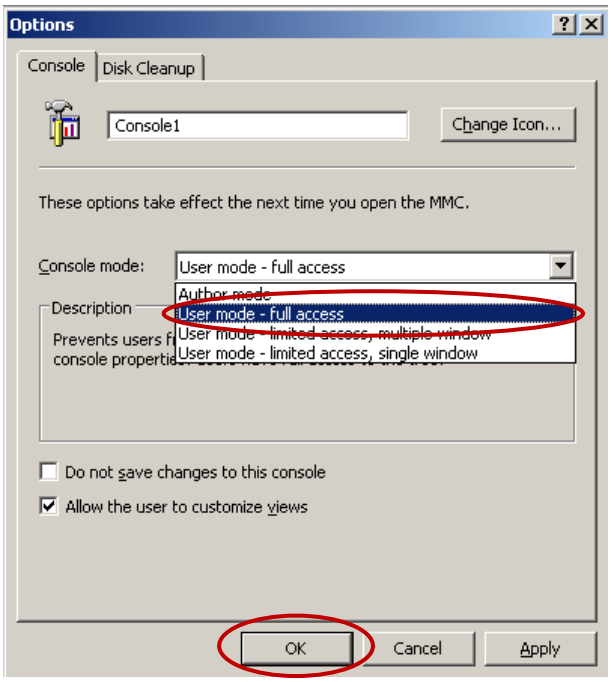
You should have the **Active Directory Users and Computers** snap in tool appear in the management console.



Before saving the management console, make sure to set the options on the console so that it is set to user mode. this way the user will not be able to add or remove any other snap-in tools to this console. To do that, from the top menu select **File** then **Options**.

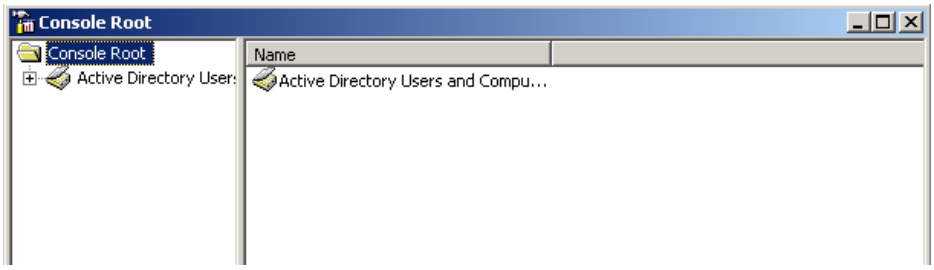


Change the **console mode** option to **user-mode – full access**. This will allow the user to have access to all the management commands, but will prevent the user from adding or removing any snap-in tools and keep him from changing the console properties. Then click **OK**.

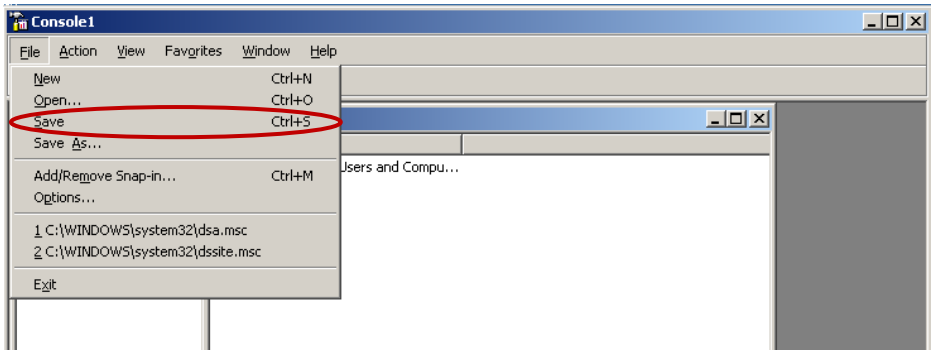


Now save the console with the name **AD Console** in the **Management Console Folder** on the **C: drive**. To do that

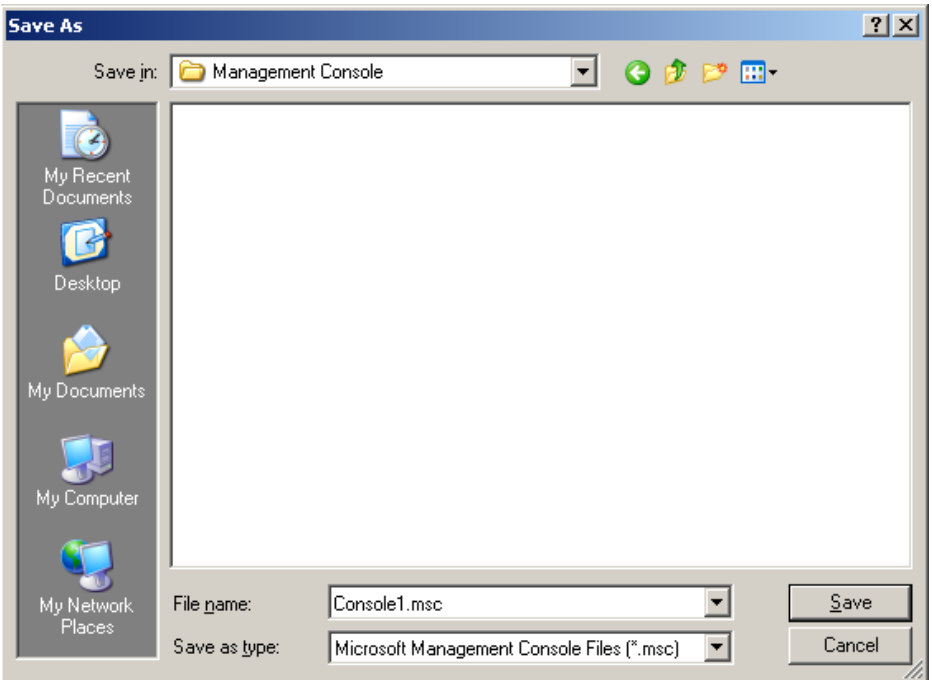
- Click file.



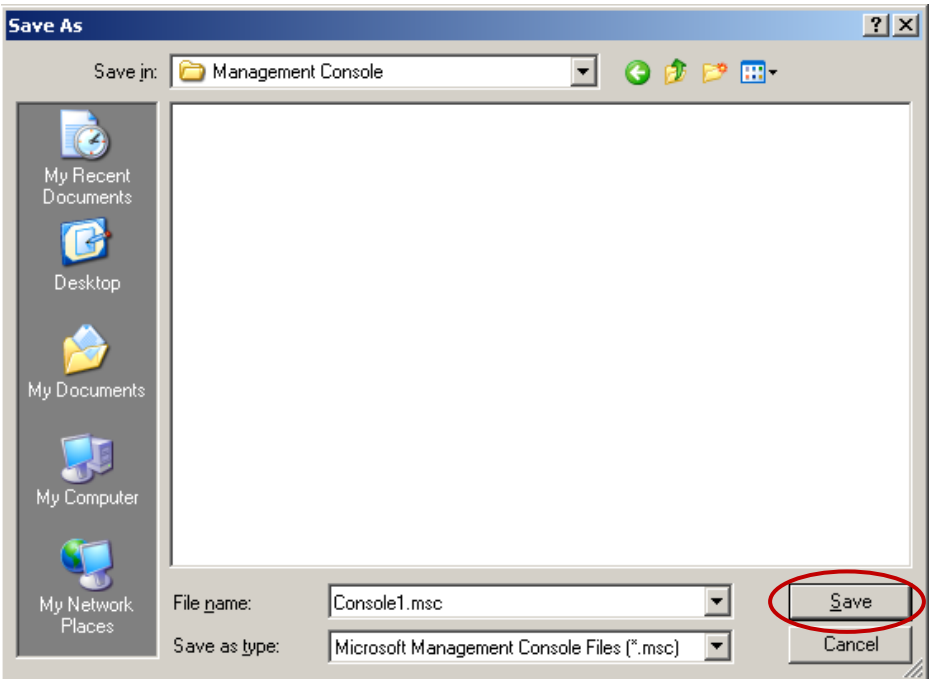
- Click Save.



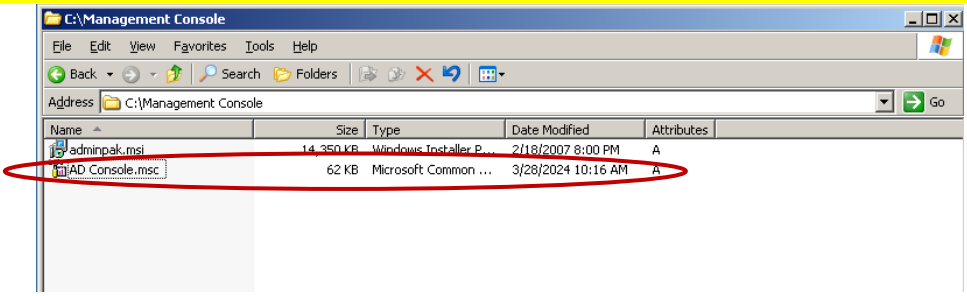
- Locate the **Management Console Folder** on the **C: drive**.



- Click save.

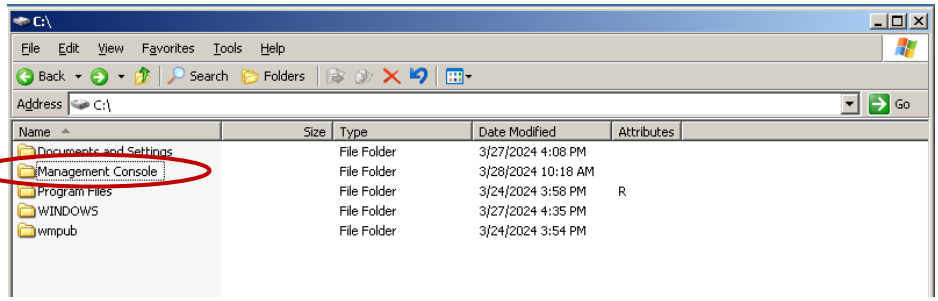


Close the console and open the **C:\Management Console** to confirm that the file was saved**.**

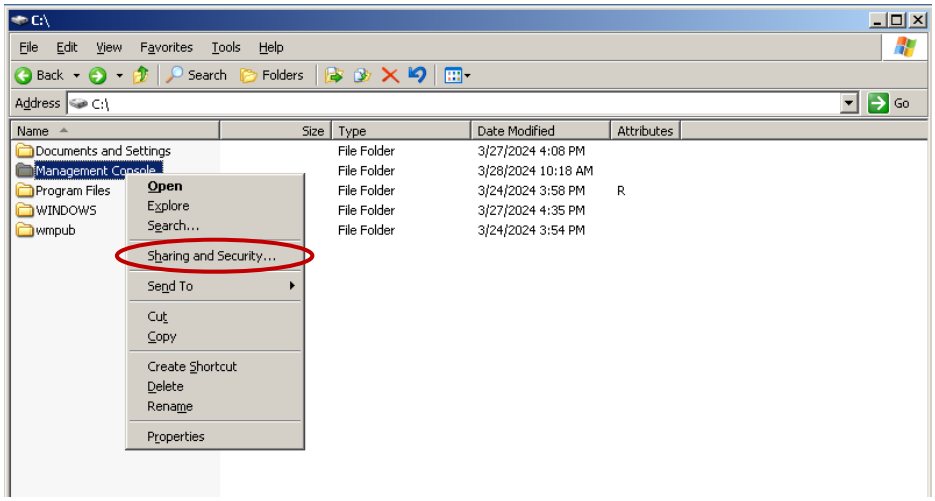


Now you will need to share the folder so that the user will be able to access the folder from his computer.

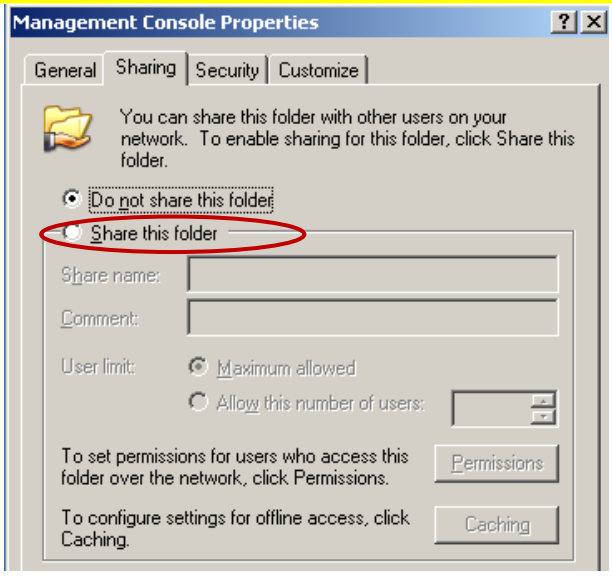
- On the **C: drive**, right click on the **Management Console Folder**.



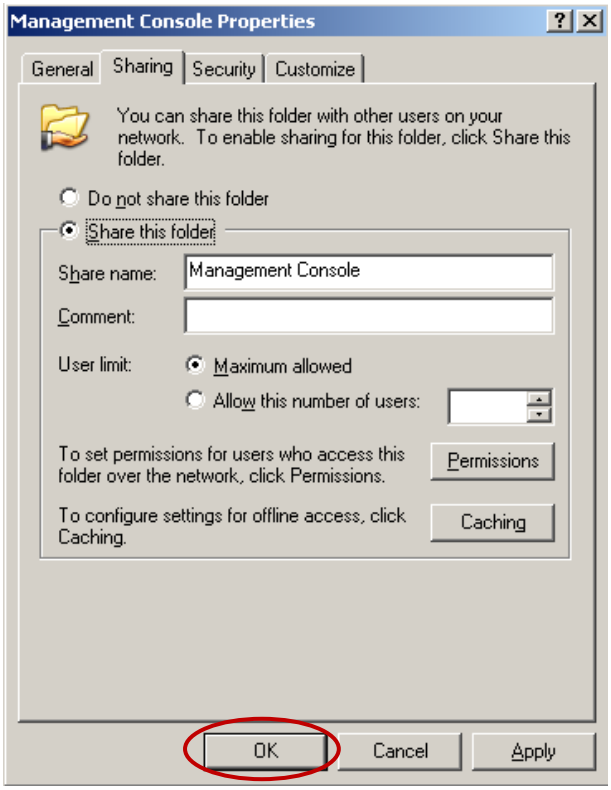
- Select **sharing and security**.



- Select the **Share this folder** option.



- Leave the default share name **Management Console** and click **OK**.



- Now close windows explorer and log off the server.

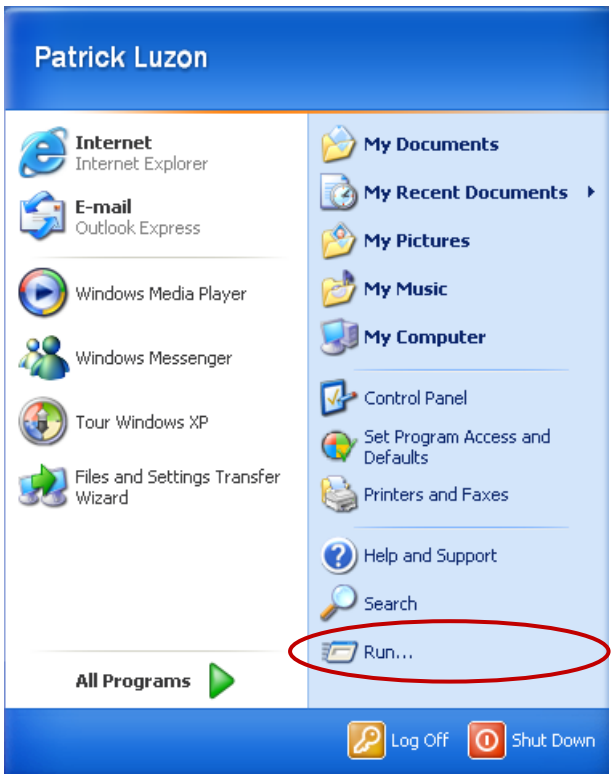
Now you will need to share the folder so that the user will be able to access the folder.

- Log on to **client1** with the username **pluzon**.

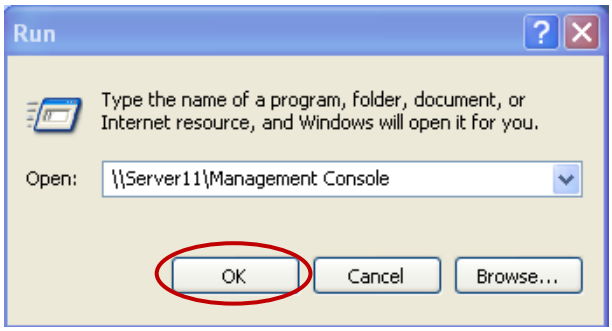
Install **ADMINPAK.msi** onto his computer and copy the **AD Console** over to the desktop. Open the shared folder by using the **UNC** (Universal Naming Convention) path in the run command prompt.

- Start

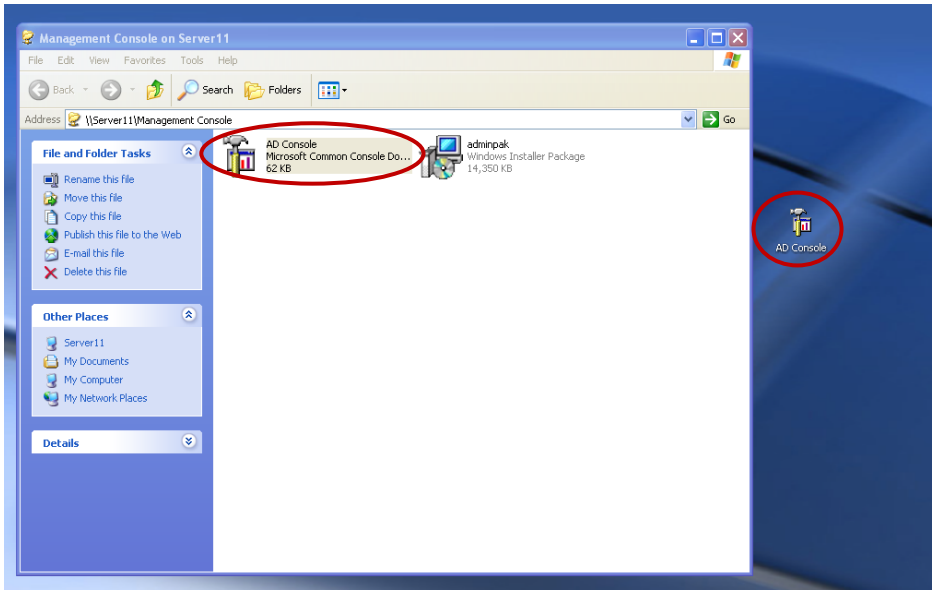
- Run



- Type in **\\Server11\Management Console** then click **OK**. (The UNC path is **\\<Computer_Name>\<share_Name>**, which in this case is **\\Server11\Management Console**).

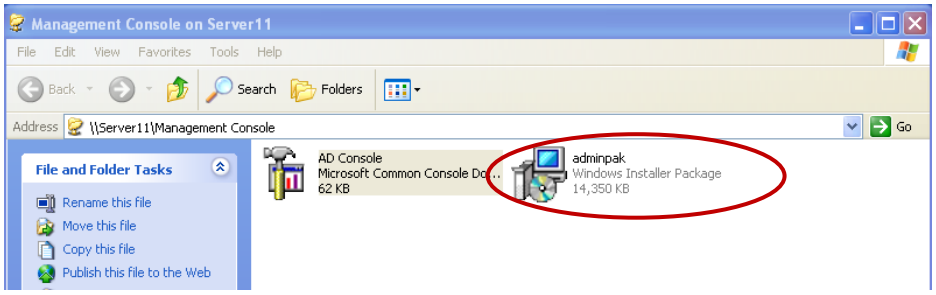


This will directly open the shared folder, **Management Console** on **Server11**. Copy the **AD Console** over to the desktop.

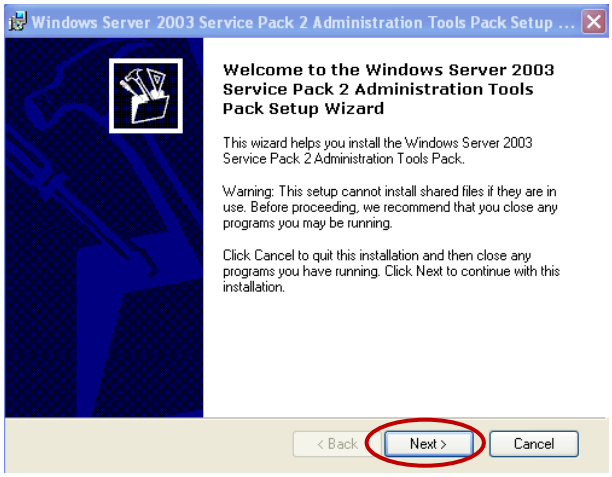


Open the **adminpak.msi** file to install the administrator tools on to the Windows XP Professional Computer.

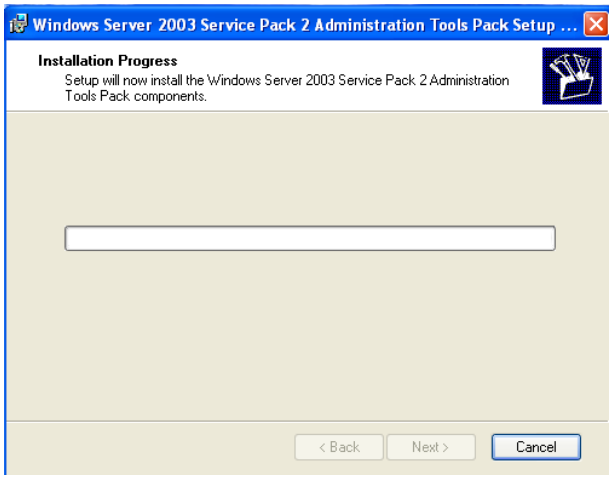
- Double click the adminpak.msi



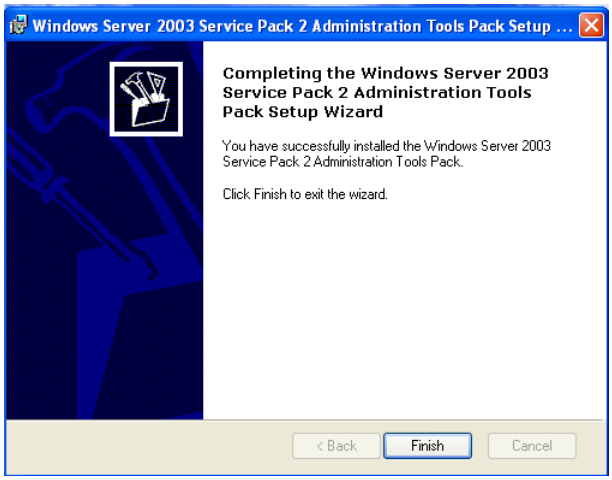
- The next screen will display the Welcome to the Windows Server 2003 Service Pack 2 Administration Tools Pack Setup Wizard. Just click **Next**.



- Wait for it to download.

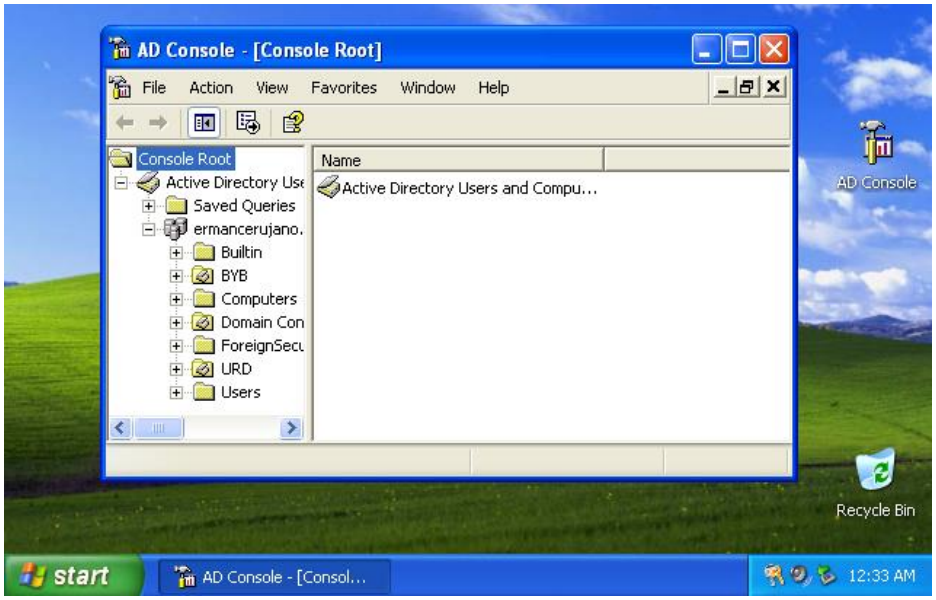


- You are now done completing installing the adminpak.msi. Click Finish.

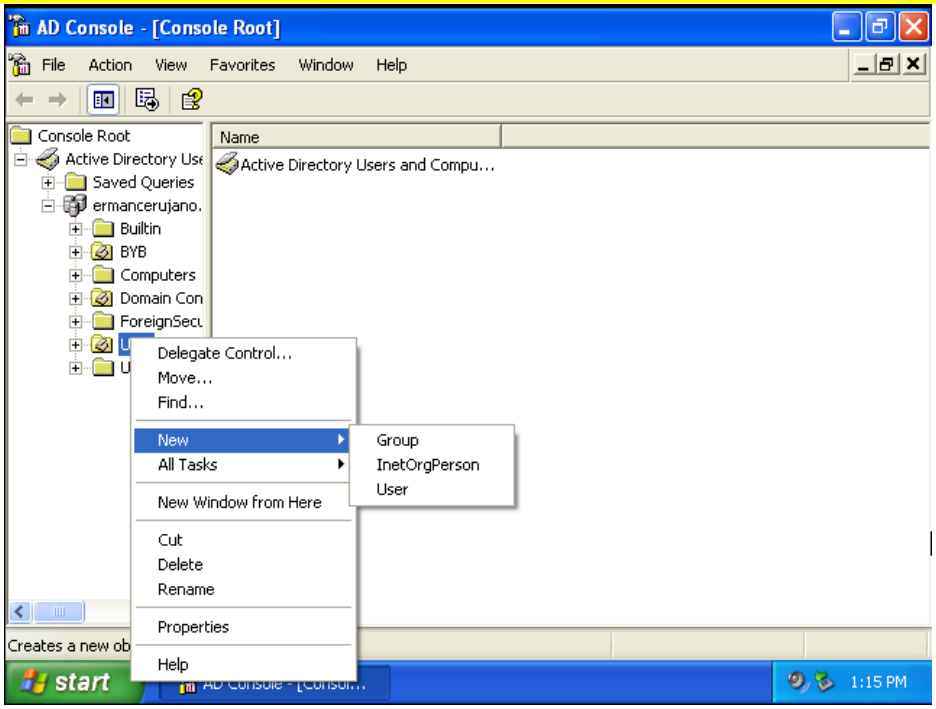


When the installation of the administrator tools is finished, close the **Management Console** folder and open the **AD Console** located on the desktop.

It should open up to the **Active Directory Users and Computers** snap-in tool.

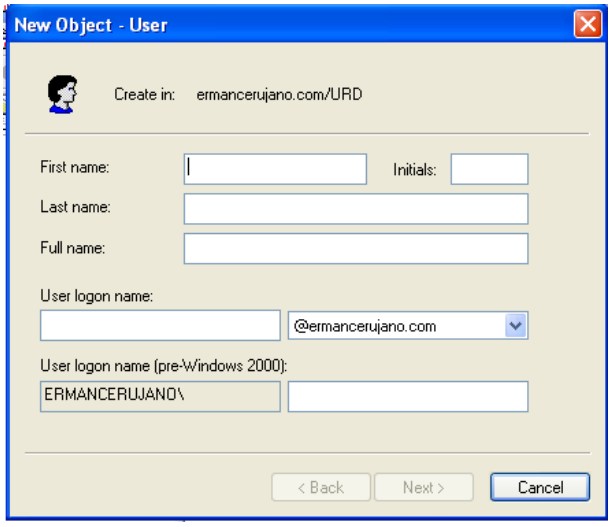


Now, to test if the delegation worked, try to create a new user in the **Urdaneta OU**. Right click on the **URD OU** and select New.

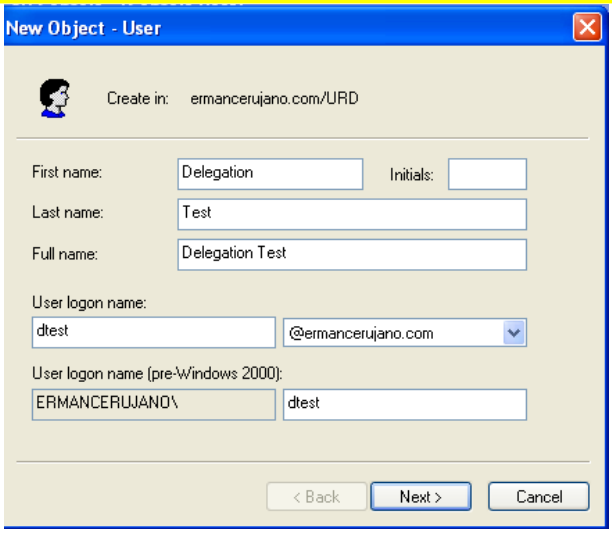


Notice that you only have three options to choose under new, they are **Group, InetOrgPerson** and **User**.

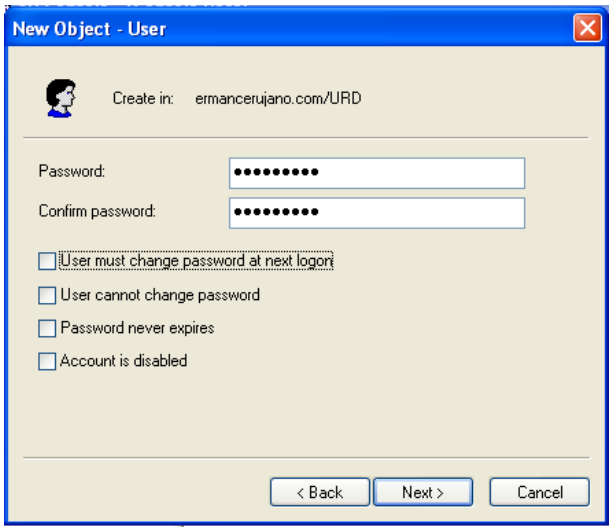
Select **User**, to open the new user wizard.



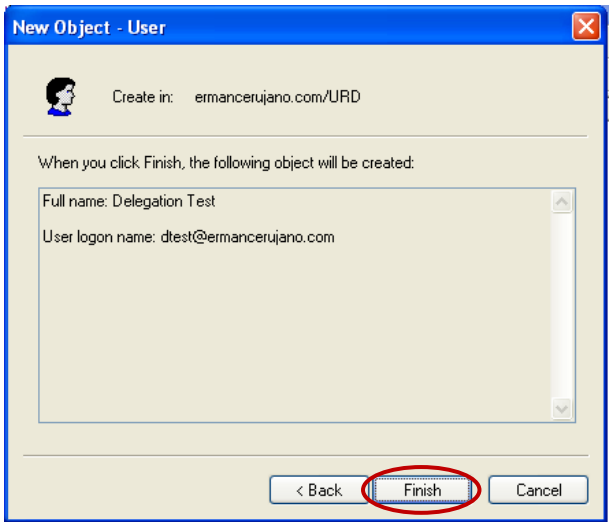
Create a user named **Delegation Test**, username **dtest** then click **Next**.



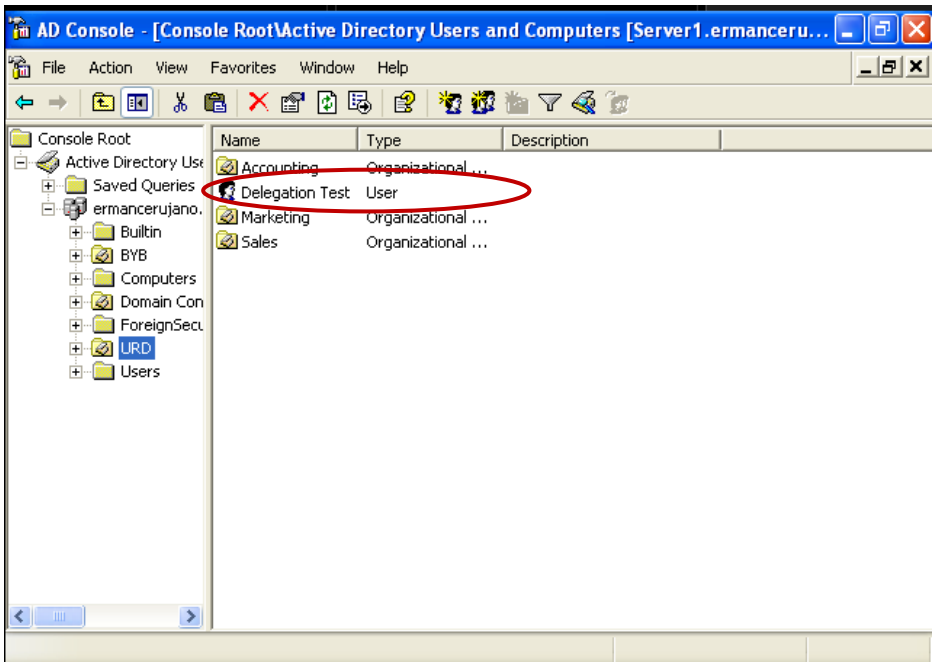
password **Delegate1** and click **Next**.



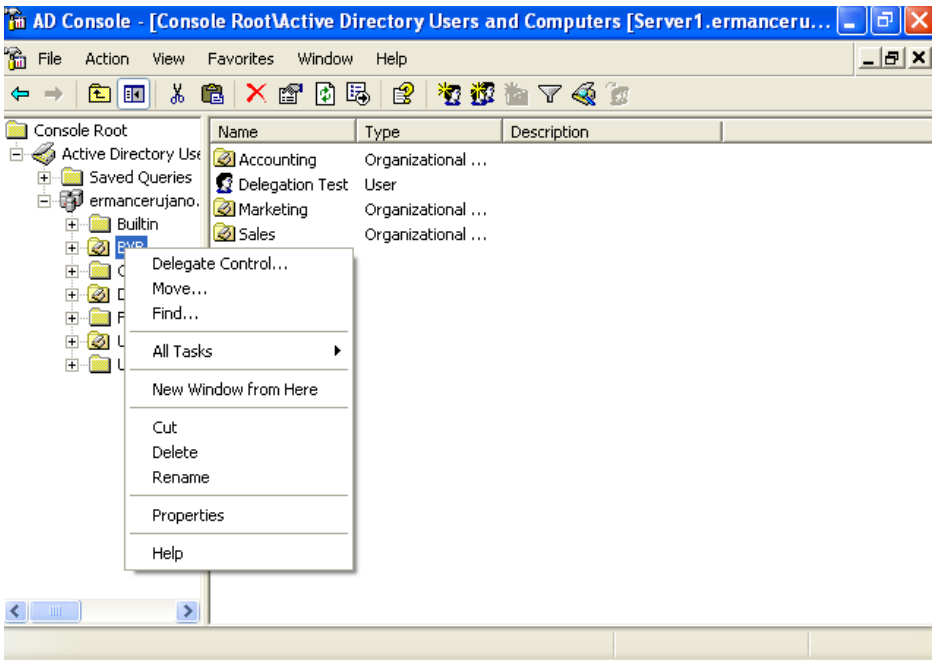
Click **Finish**.



When you finish the new user wizard, you should see the new user you created in the **URD-OU**.

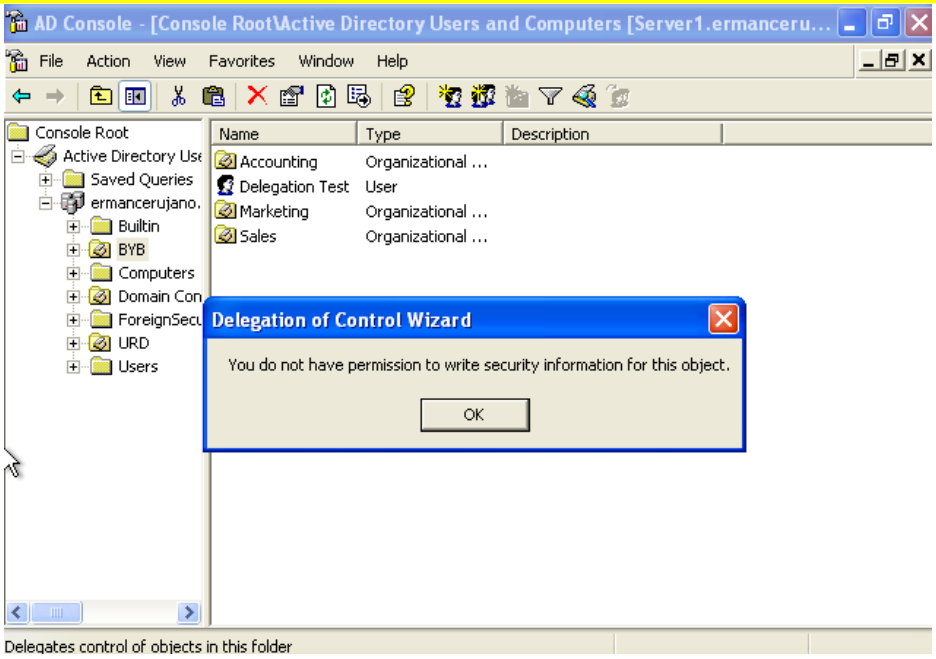


Now try to create a new user from the **Bayambang OU**. Right click on the **BYB** OU**.**



Notice that there is no **New** option available on the shortcut menu because this user was only given permission to manage the **URD** OU and therefore, cannot create any new users or groups in the **BYB** OU. Although there are other options still available, the user will get an error message stating that access is denied if they try to use any other option.

For example, we want to use delegate **control**.



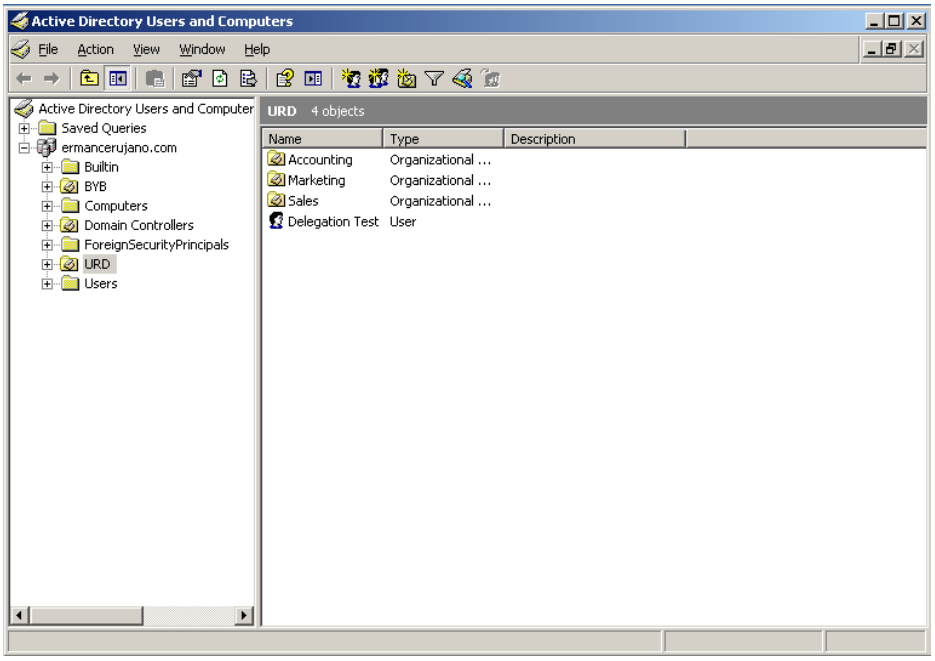
As you can see, we received an error message.

Close the **AD tools console** and log off **client1**.

2.6. Remove Delegated control of an Organizational unit.

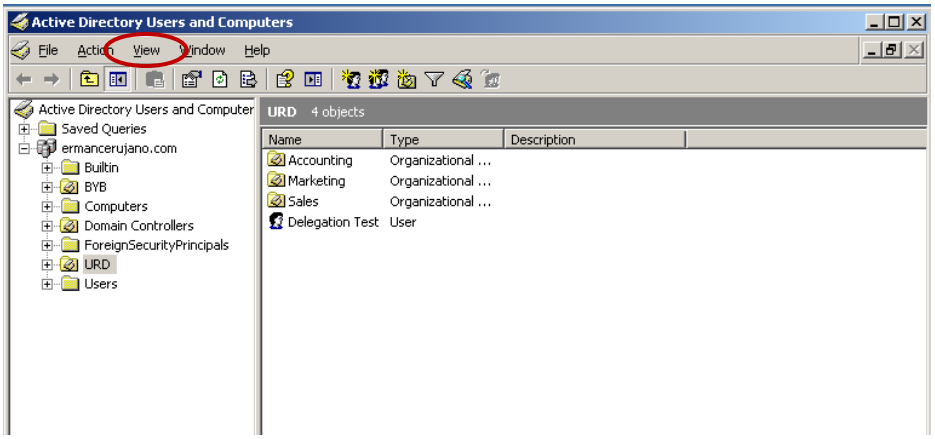
Removing the delegated control is slightly more difficult than delegating the control because there is no wizard that will "**un-delegate**" permissions. The only way to remove any delegated permissions is to go to the security tab of the container and remove the permissions that were granted through the delegation wizard. This can be a touch complex for anyone not familiar with **Windows Server 2003**. Another point to keep in mind is that you should always document any permissions that you have delegated. It will make it easier on you and anyone who may come in after you when trying to figure out who has permission to do what in the domain.

Log on to **Server1** as the domain administrator and open the **Active Directory Users and Computer Console**.

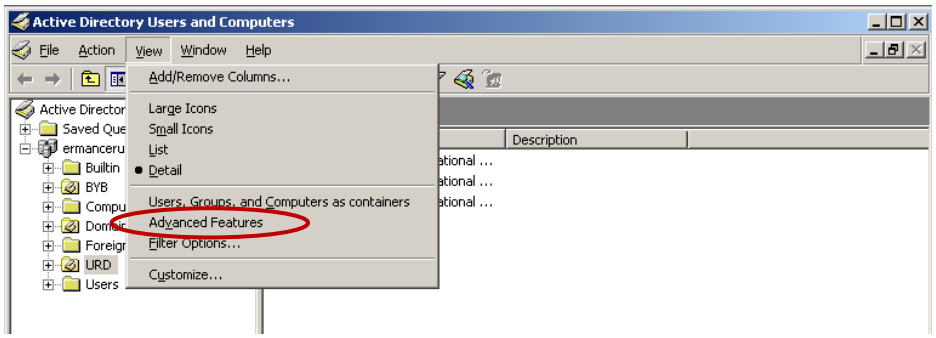


The first thing you need to do is change the view of the console to **advanced features** so that you can access the security tab for the containers.

- Click view.

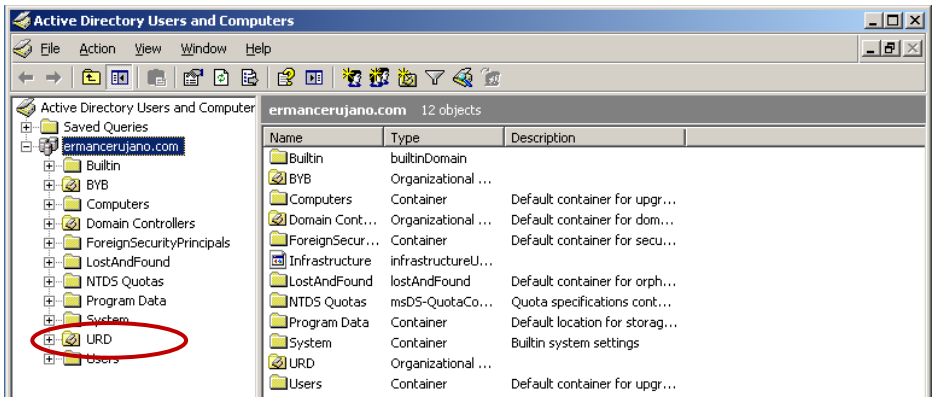


- Select Advance Features

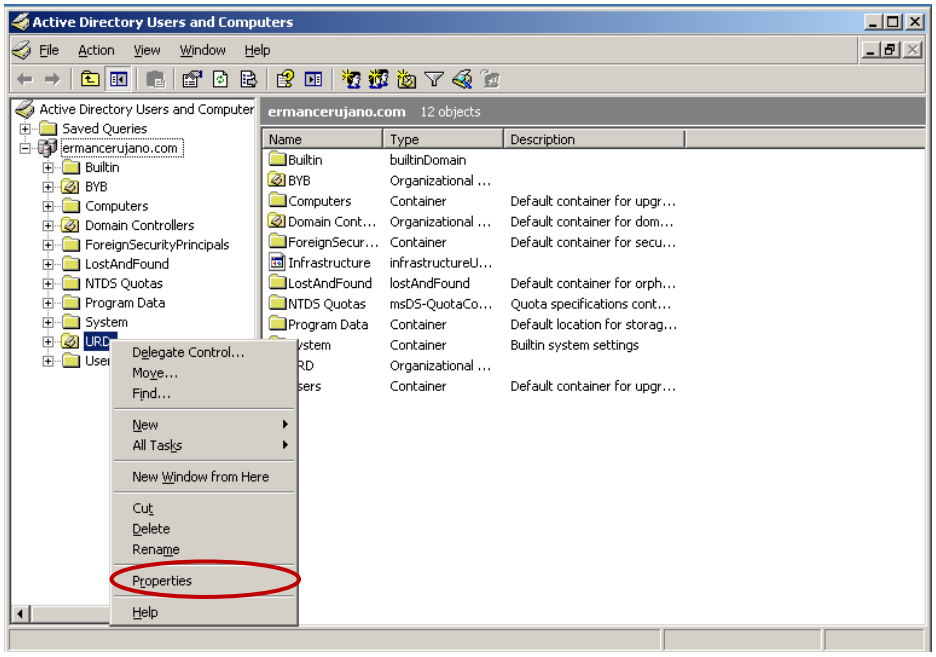


Try to open the security tab in the properties of the **Urdaneta** OU .

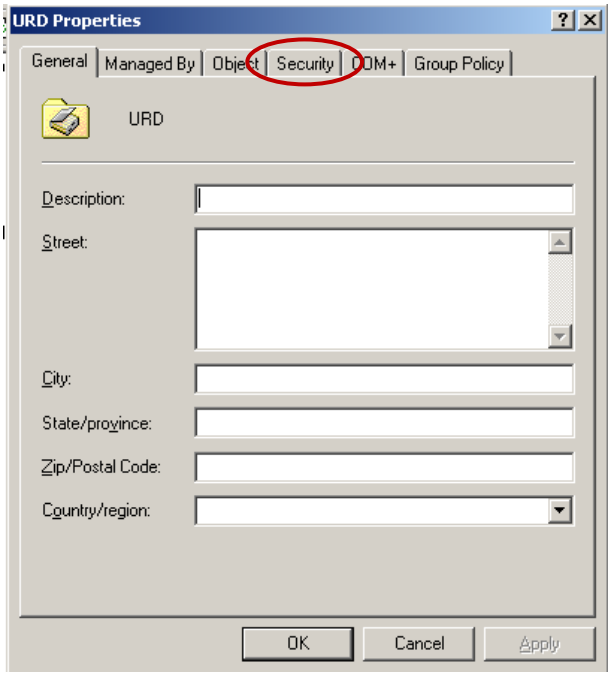
- Right click on the **URD OU**.



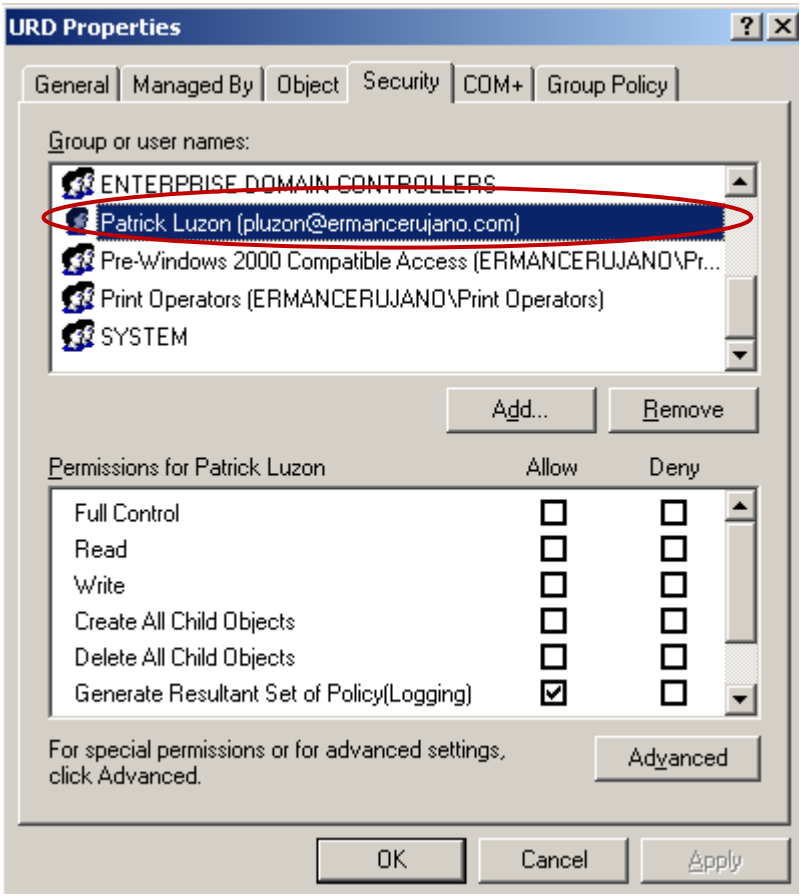
- Select Properties



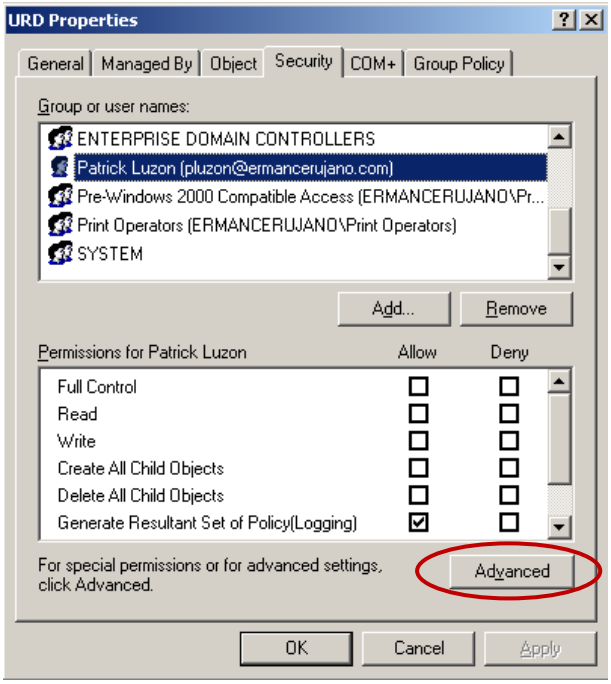
- Select Security Tab.



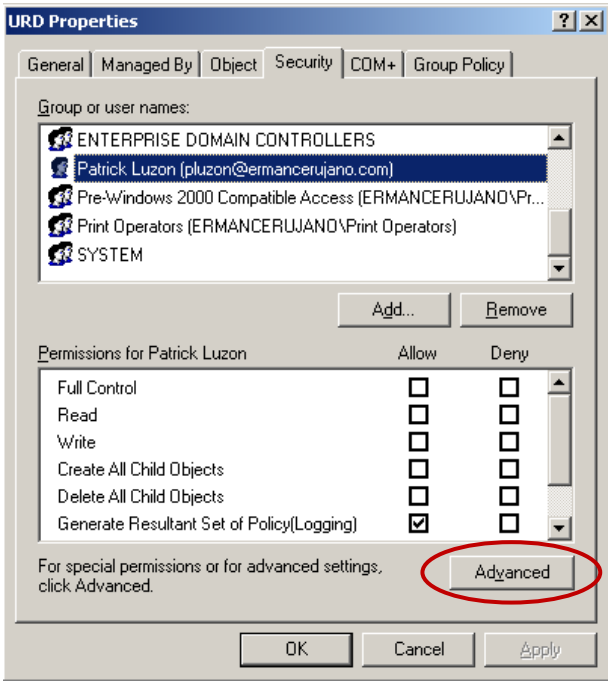
- Find the name for the user **Patrick Luzon** in the security list.



Notice that that all the permission for the user are blank. It doesn't mean that the user has no permissions for this OU though. if you look at the bottom of the screen, next to the advance button, you will see that the user has **additional permission set**.

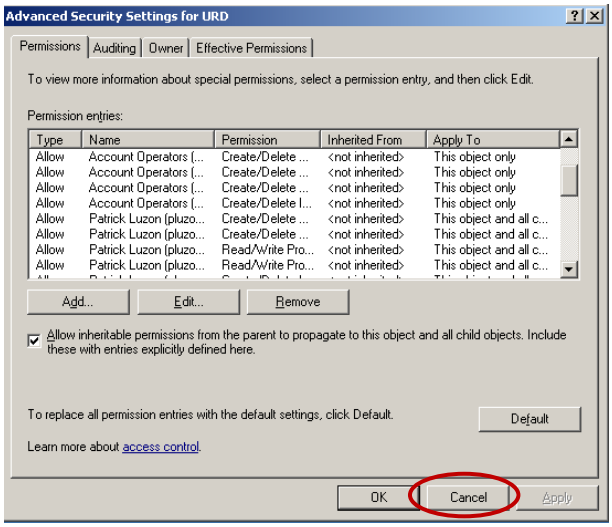


Click on the **Advanced** button to view the advance permission.

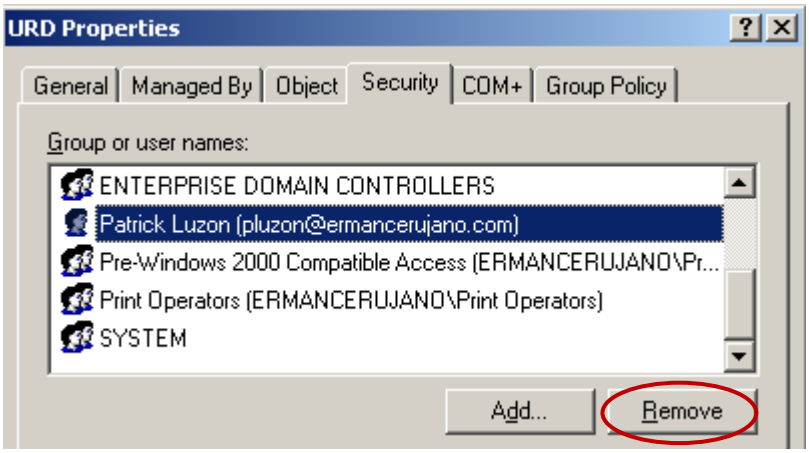


You should see that there are four permissions for the user **Patrick Luzon**. You can either remove specific permissions from the user or remove them all. You can also add specific permissions that may not have been included on the wizard from here. If you plan on removing all the permissions from

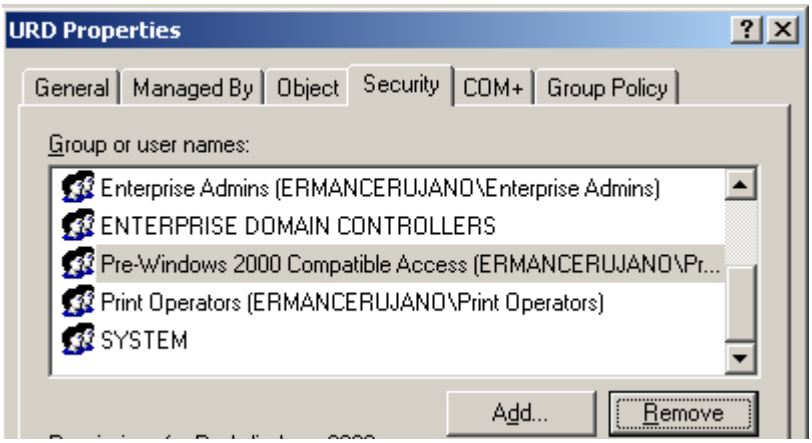
the user, then you would be better off just removing the user from the security list on the security tab. Click **Cancel** to return to the security tab.



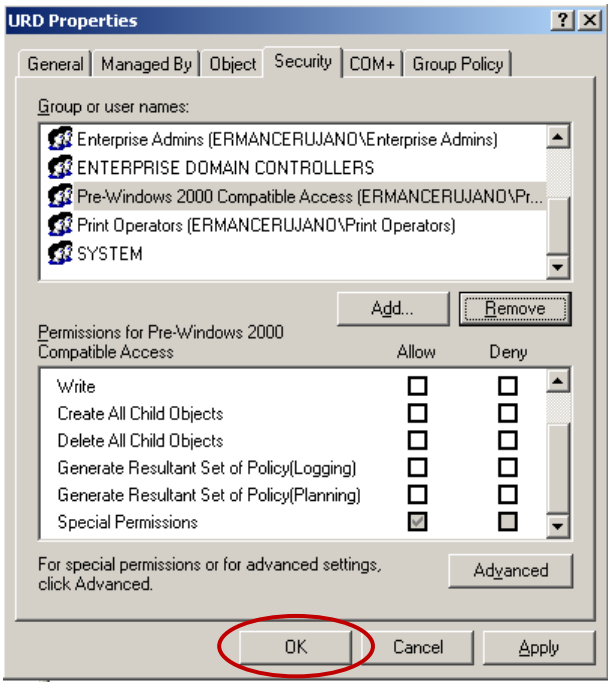
Select the user **Patrick Luzon** from the security list. Click the **remove** button.



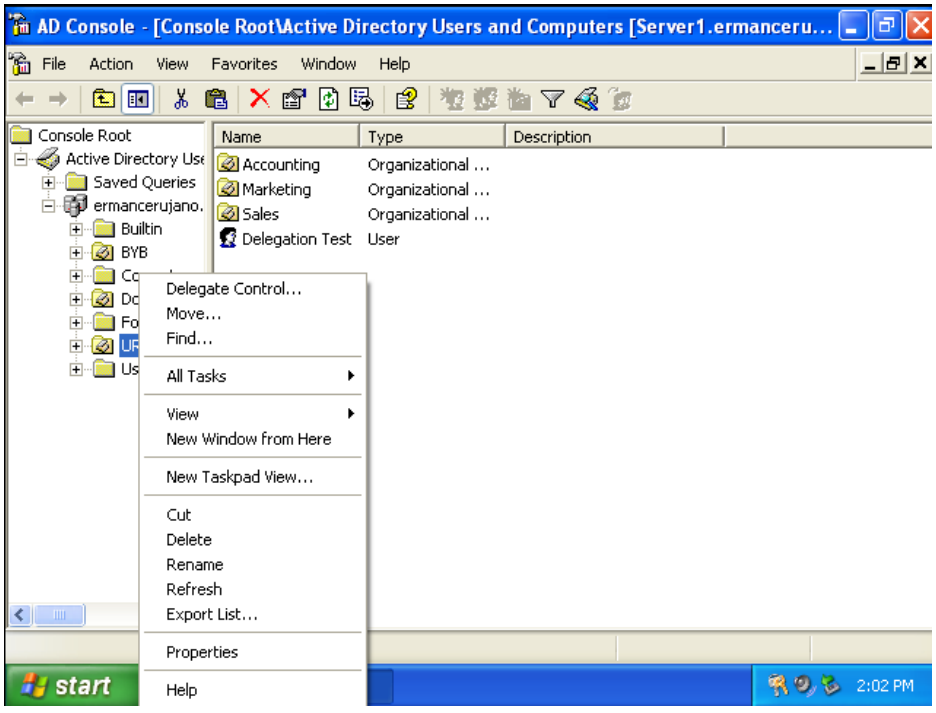
As you can see the user will now disappear from the security list.



Click **OK** to close the properties page.



Now log on to **cleint1** with the username **pluzon**. Open the console **AD Tools** located on the desktop and try to create a new user or group for the **URD-OU**.



Notice how the **New** option on the shortcut menu is no longer available.

Note:

If the New option is still appearing on the menu, it may be that the domain controllers have not replicated and therefore, the user still has permission to the **OU**. You can wait a few minutes for them

to replicate or you can log on to one of the domain controllers to force replication. Either way, you will have to log off and log back on the **client1** for the changes to take place.

LAB 14.3

Creating and Assigning a Group Policies

Contents:

SCENARIO – PART ONE

Up until now, users in both Officers of Ermancerujnao, Corp. have been able to change their display settings and install their own screen savers and backgrounds. But in your weekly meeting with Erman, the Operations Manager, she feels that there are some users who have taken it to far by either placing inappropriate pictures on their screens or spending way too much time installing and looking for new screen savers to install on their systems.

In some cases, they have even damages their computers by changing the display settings, “How can we stop users from accessing parts of the operating system that they shouldn’t access? Erman asks. “Group Policy is the easiest way,” you respond, “and we won’t have to police the users either. It just works!” After discussing the matter in great detail, you and Jill reach the conclusion that there is really no reason that the users of the domain need to access the control panel either. You decide to create a group policy on the domain to restrict all users (except the administrators) from the control panel. You also decide to disable the My Network Places icon on the desktop to keep the users from browsing the network and instead, just allowing them to use their mapped network drives that are pre-assigned.

Erman agrees to all of your propositions but reminds you that marketing department in both locations will need to access their display settings because of a custom piece of software that requires them to adjust their screen resolution. This means that the group policy you discussed previously will not be enforced on users in the marketing department.

In this lab, you will create group policies, configure policy settings, and link them to the domain and an OU. You will also see how one group policy can override another group policy based on where in the Active Directory it is linked. Finally, you will see difference between removing a group policy from a container and deleting a group policy from Active Directory.

GROUP POLICIES

Group Policy is a new feature in Windows 2003 that allows that9 administrator to set user and computer configuration across the network in an efficient manner. Some of the settings that can be specified include scripts, security, folder redirection, software installation, and registry-based options. Group policies are similar to system policies used in NT 4, except that group policies are easier to work with.

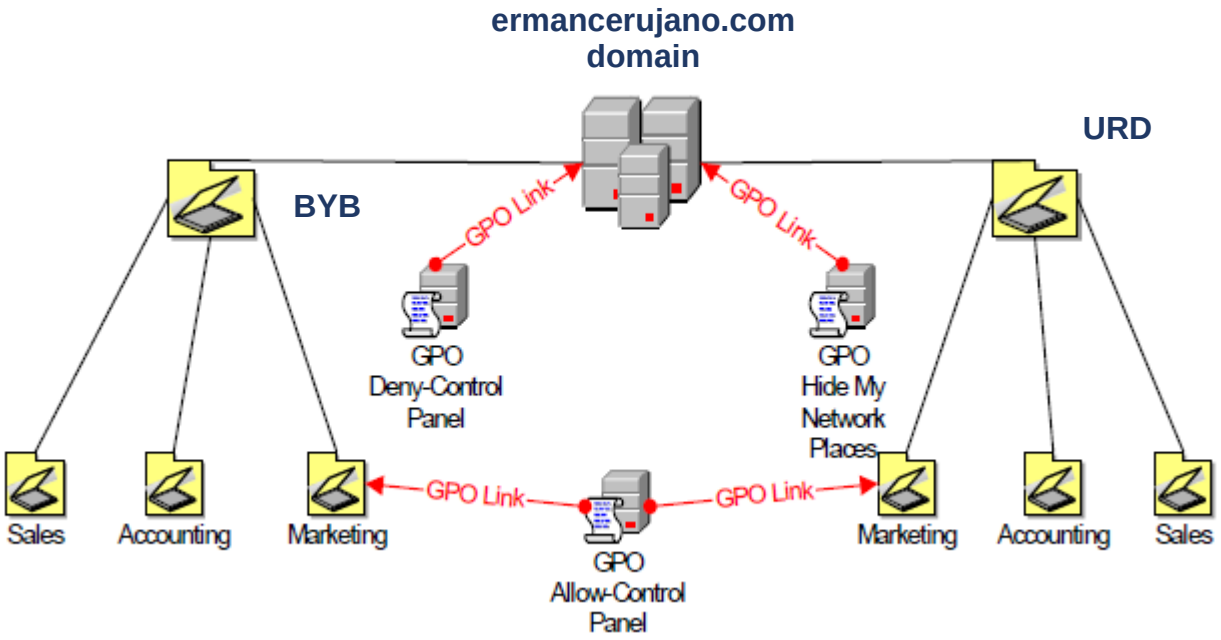
Group Policy settings that you can create are stores in a **GPO (Group Policy Object)** and are replicated to other domain controllers via Active Directory. With NT 4.0 system policies, you have to make sure that the file, which contains the settings, is replicated to all domian controllers in the domain and whenever you delete that system policy you have to remove the setting from every compute that is was applied to.

The Group Policy Object (GPO) is assigned to an Active Directory container (Sites, OUs, or Domain) and the settings are then applied to all user and computer objects that reside within the container. Any group policy setting that is removed does not need to be changed in the register on each computer. It is automatically removed from each system.

There are two general types of group policies in Windows 2000:

1. Local Based Policy – will just apply to a local computer or a local user on the computer.
2. Domain Based Policy – works with Active Directory and is applied to computers or users in the domain.

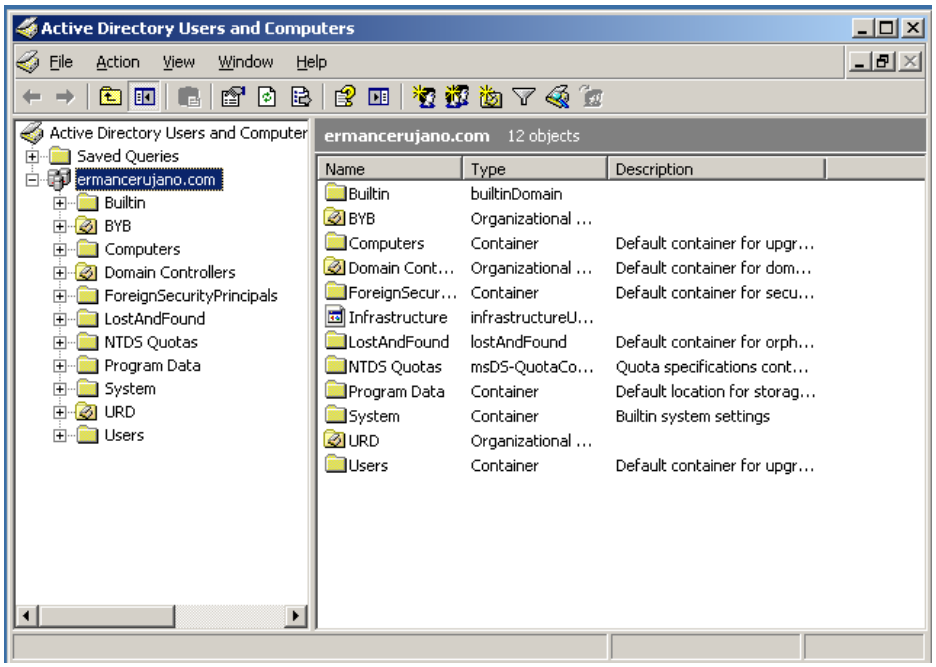
STRUCTURE



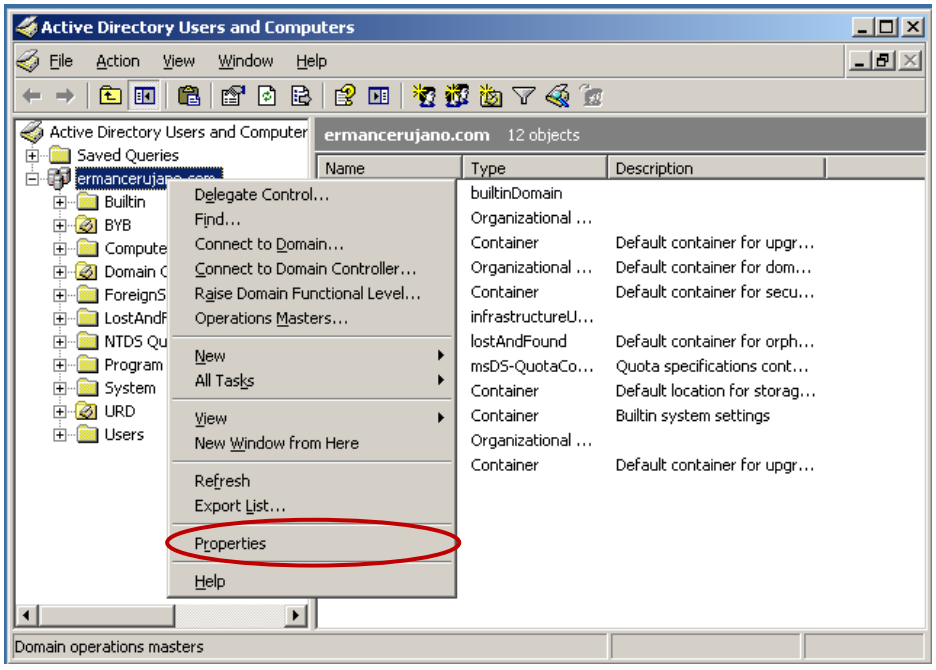
LAB 14.3. CREATING AND ASSIGNING GROUP POLICIES.

3.1. Creating and Assigning a Group Policy to the Domain

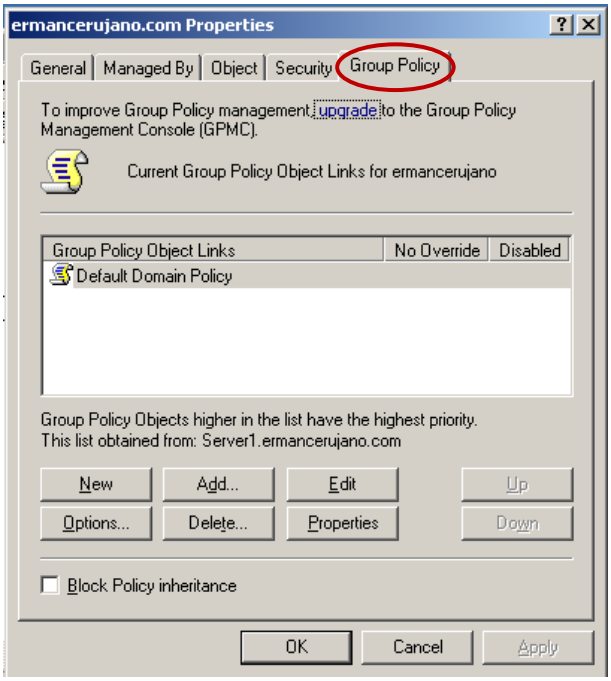
Log on to **Server1** as the domain administrator and open the **Active Directory Users and Computer Console**.



Right click on the domain **ermancerujano.com** and select **properties.**

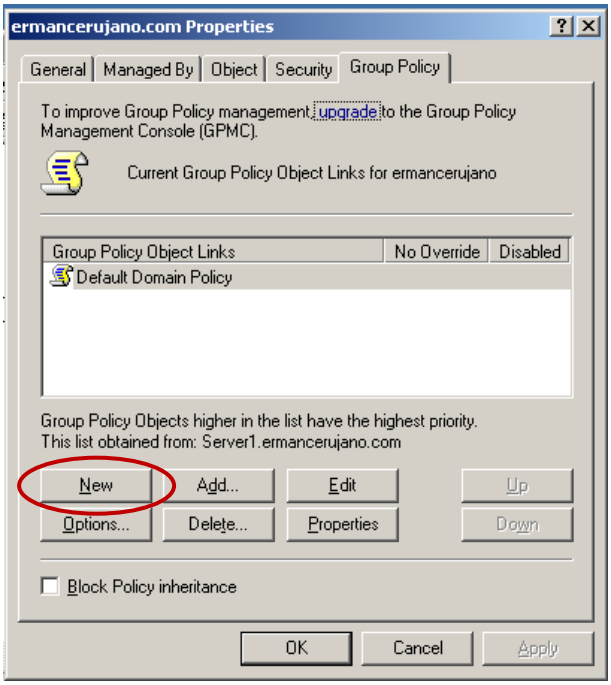


On the properties page select the **Group Policy** tab to view a list of **GPO's** that are linked to the domain.

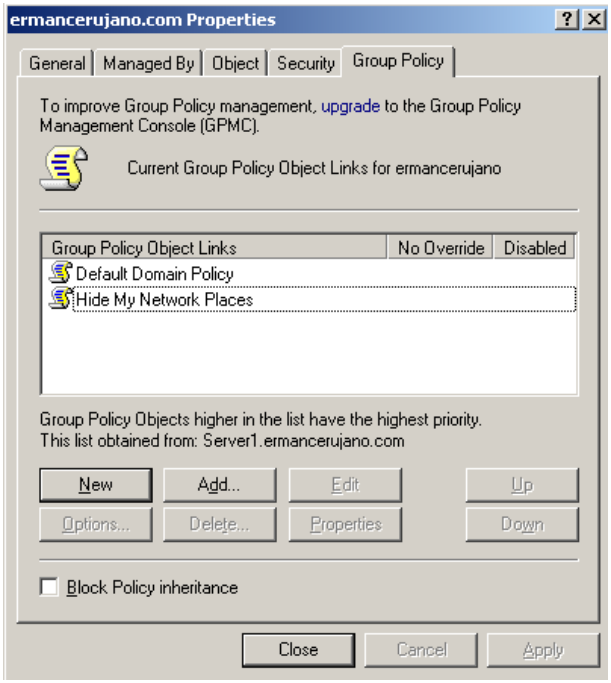


By default, you will see the Default Domain Policy on the list. This GPO will have some basic settings in place, but in order to lock down client computer you will have to create additional settings within the GPO or another GPO that is linked to the domain.

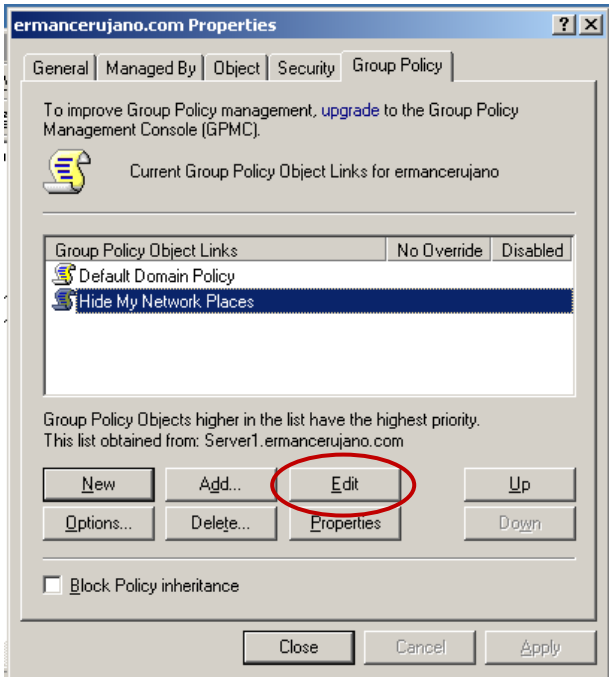
Click on the **New** button to create a new **GPO**.



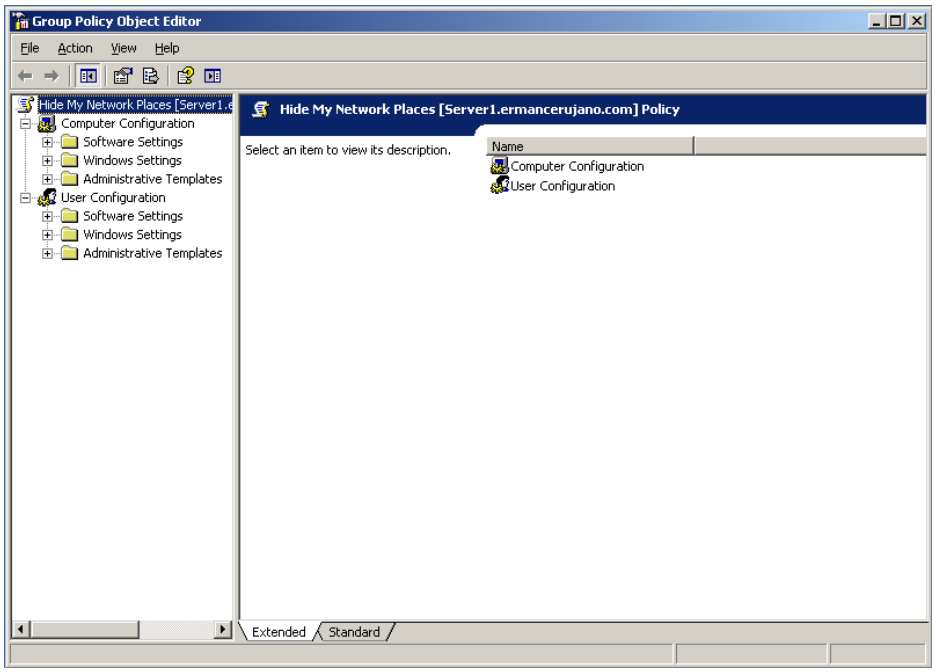
Name the GPO, **Hide My Network Places**.



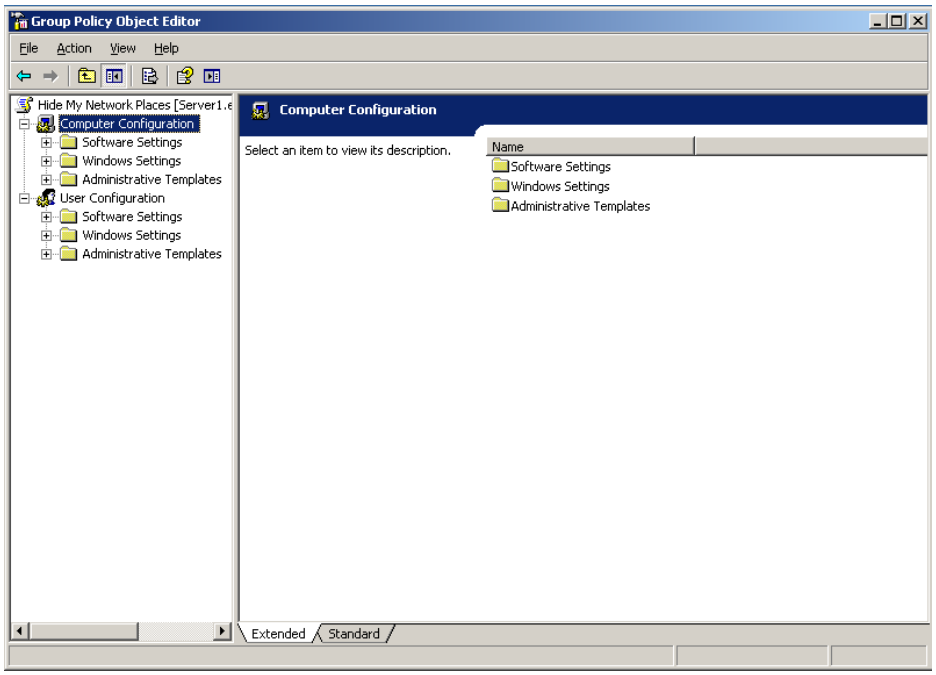
Highlight the new **GPO** and select the **Edit Button**.



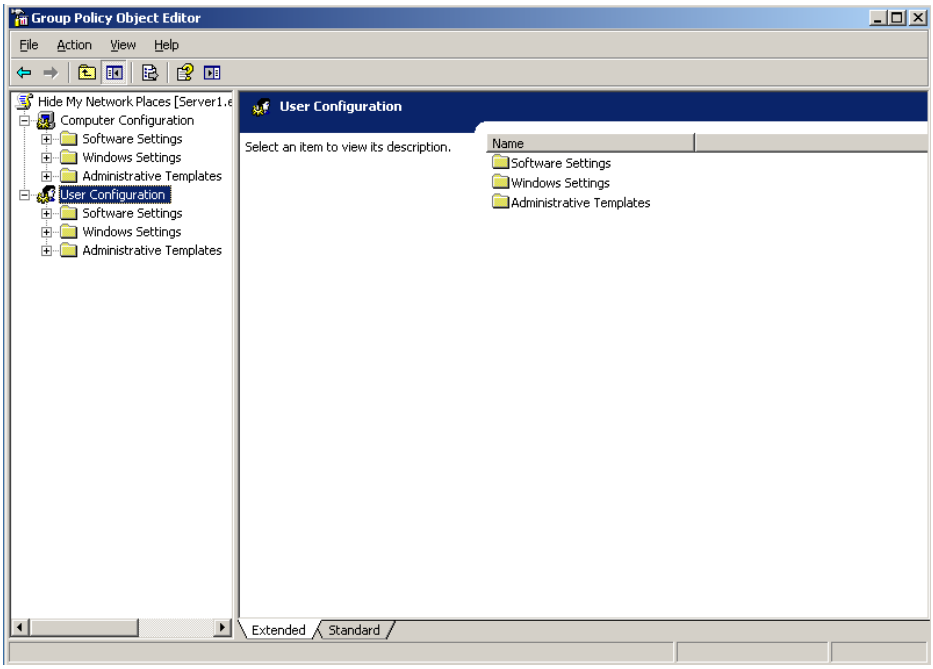
This will open the group policy snap-in tool.



From here, you can see the two different types of settings. The first one is the computer configuration settings that are applied to the computers when they start up.



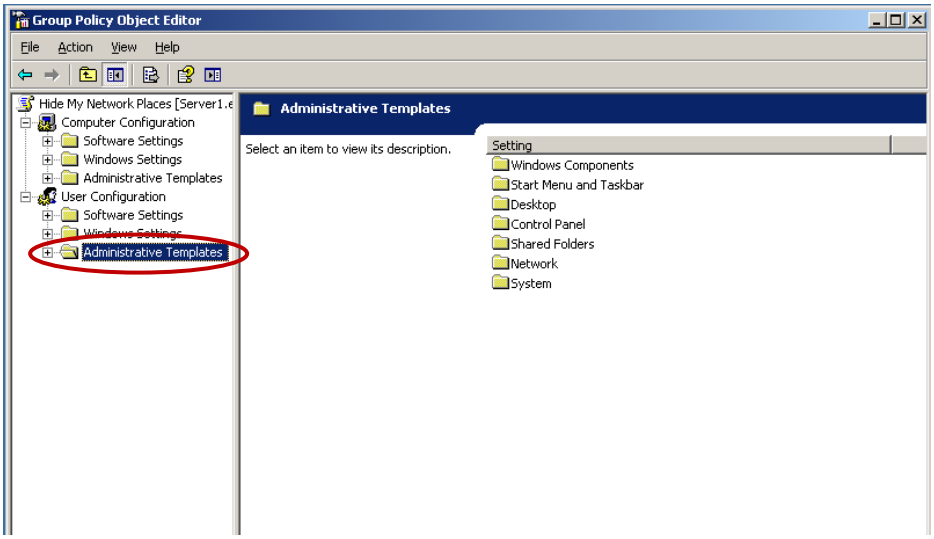
The second one is the user configuration settings that are applied to users when they logon.



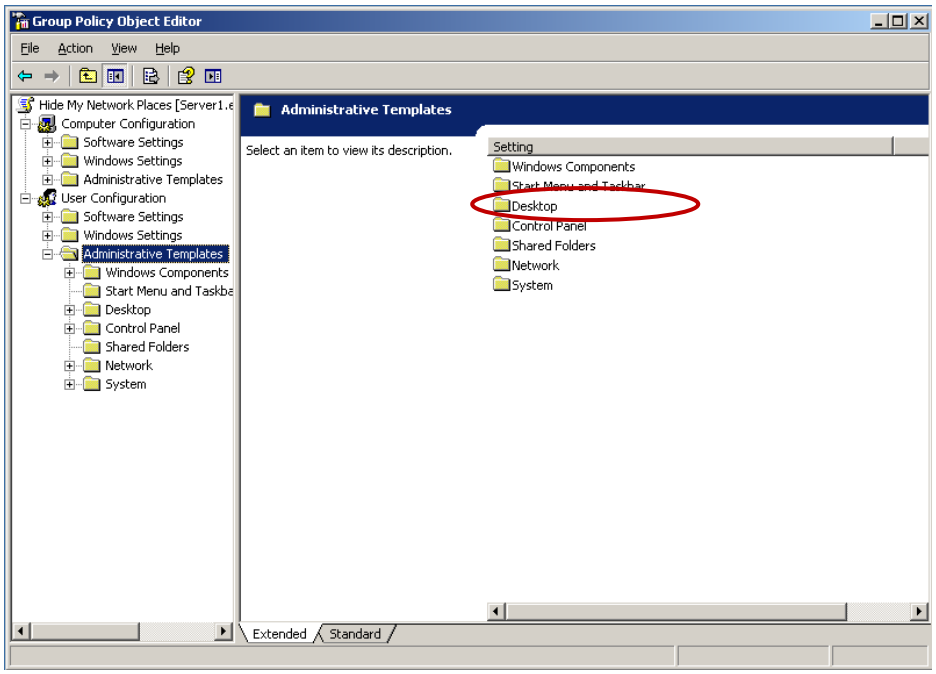
Note:

In this lab we will create one Group Policy Object (GPO) for every policy setting, so that you can see how each GPO works. It does not mean that you are limited to just one policy setting for every GPO. You can configure as many policies as you want in a GPO, but you must have a plan on how you will be implementing group policies on the network, so that you know what policy settings can be placed in the same **GPO** and what policy settings require a separate GPO.

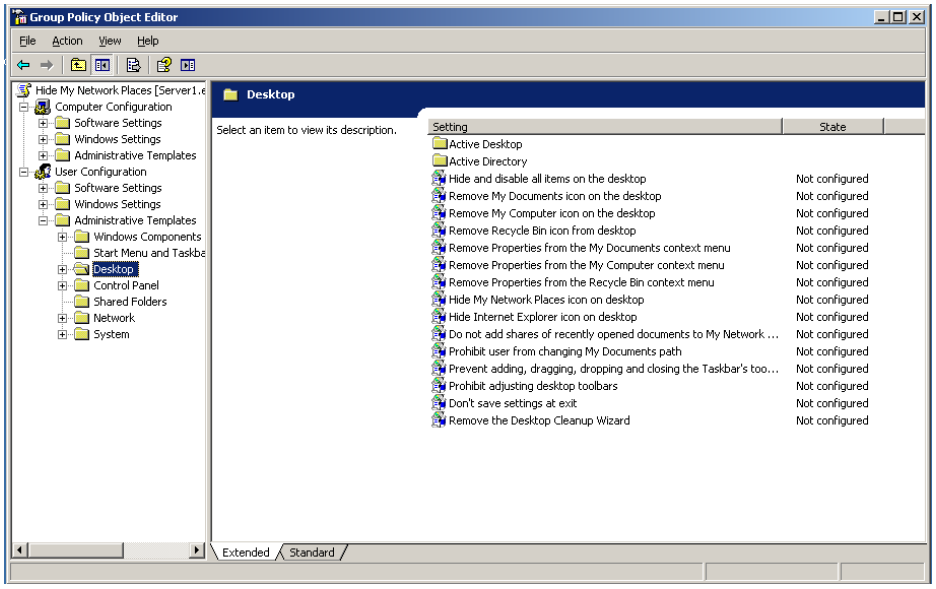
You want to create a GPO that will hide the **My Network Place** icon from the desktop and apply it to users on the entire domain. You also don't want it to affect any of the administrators. On the left pane select **Administrative Templates** under **User Configuration**.



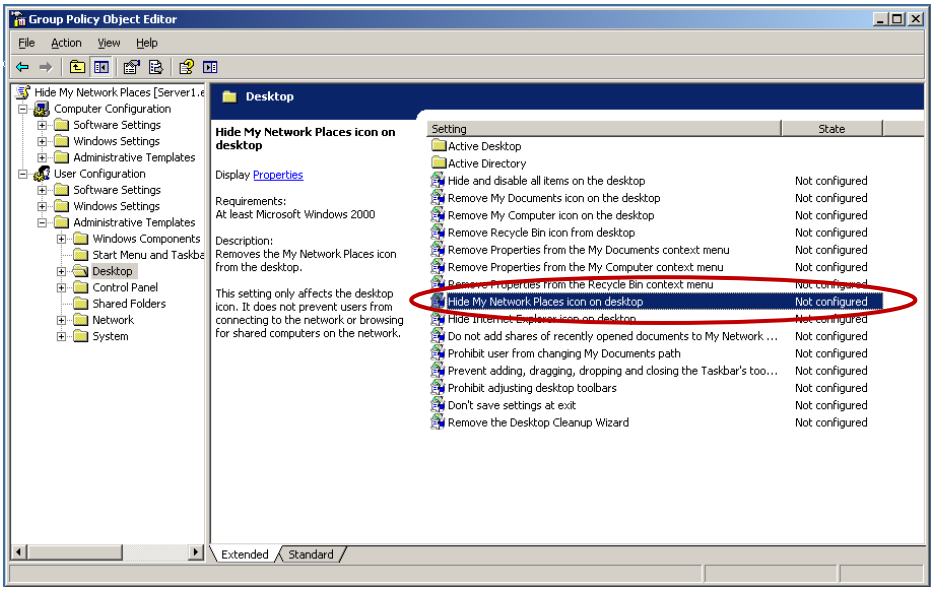
Under the administrator template folder, select the **Desktop** folder.



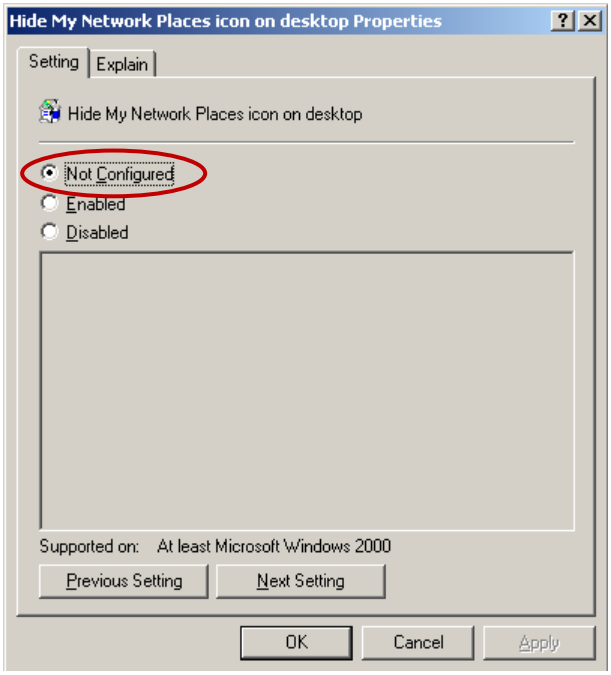
You will see all of the available settings on the right pane. You should also see that all of the settings on a new GPO are not configured by default.



In order to enable the policy find the policy settings that says **Hide My Network Places icon on desktop** and double click on it.

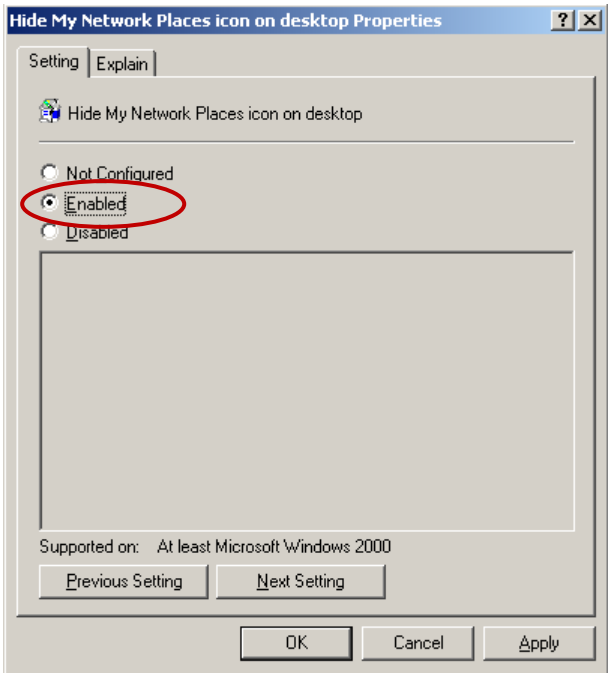


This will open the properties of that setting and show you the options available on it.

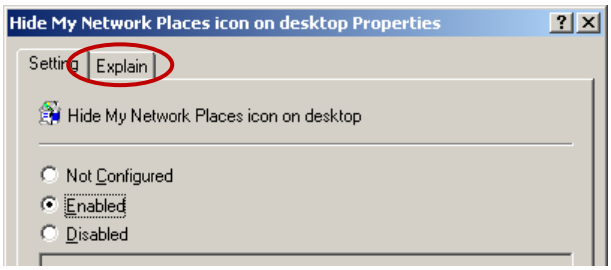


As you can see above, there are three options. The default option that is selected is **Not Configured**. There are also options to **enable** or to **disable** the policy.

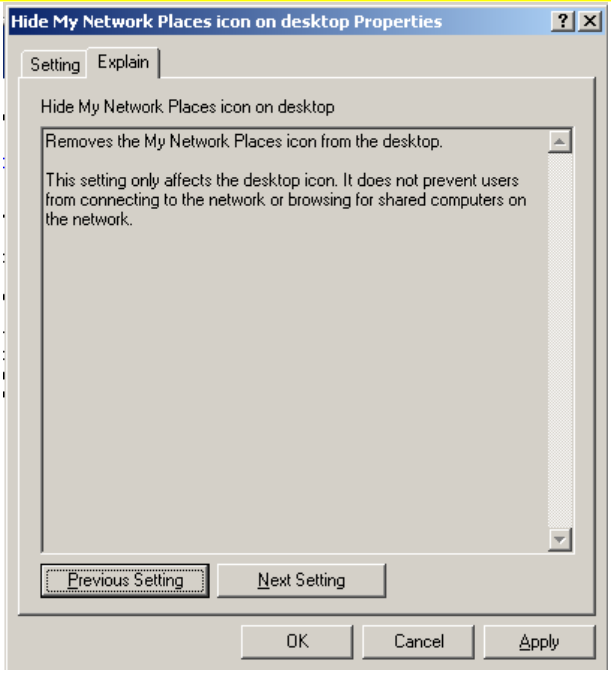
Select the **Enable Option**.



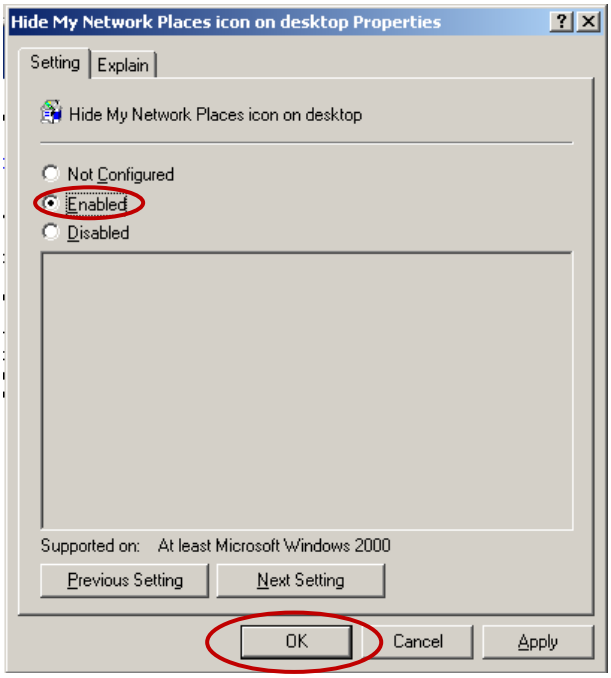
For every setting, you also have a tab called **Explain**. Select the **Explain** tab.



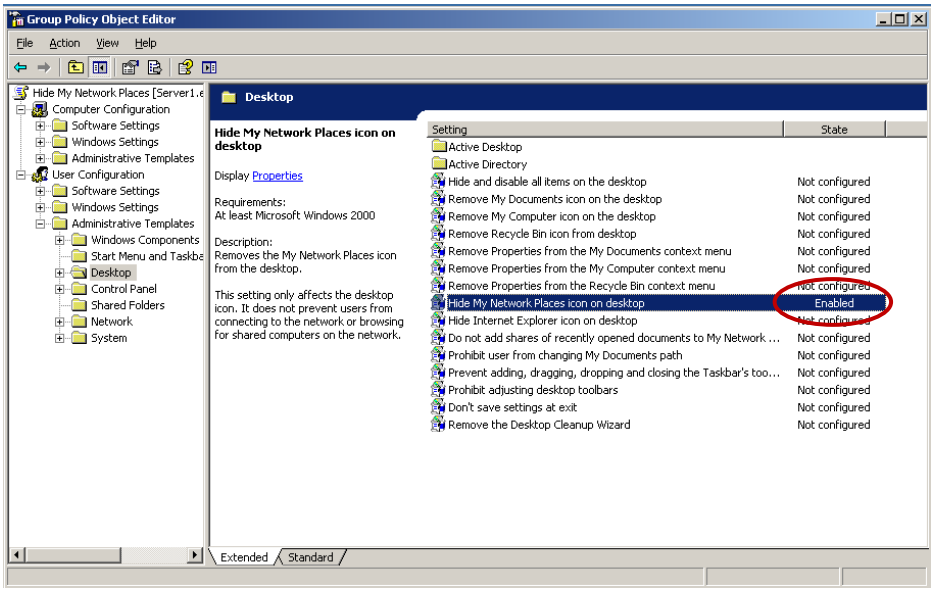
You can read what affect this setting will have if it is **enabled** or **disabled**.



Go back to the **Policy** tab and make sure that the setting is **Enabled** and click **OK**.

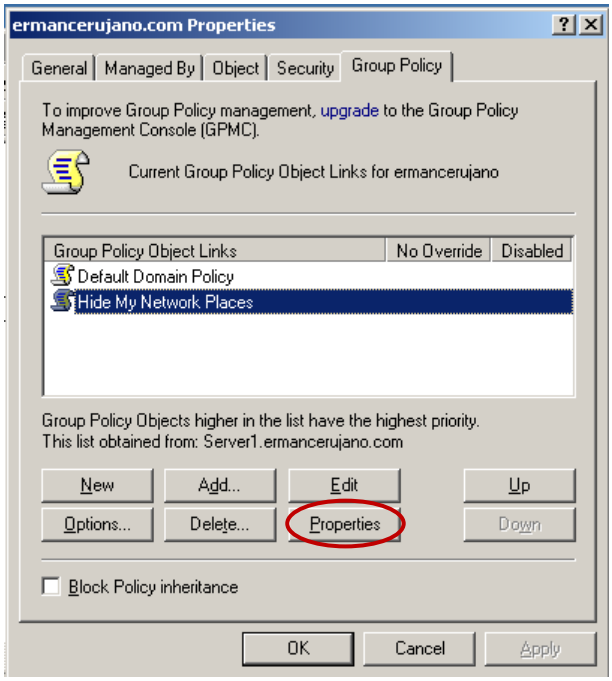


This will bring you back to the Group Policy snap-in tool. Now if you look at the **Hide My Network Places icon on Desktop** setting you will see that it shows that it is enabled.



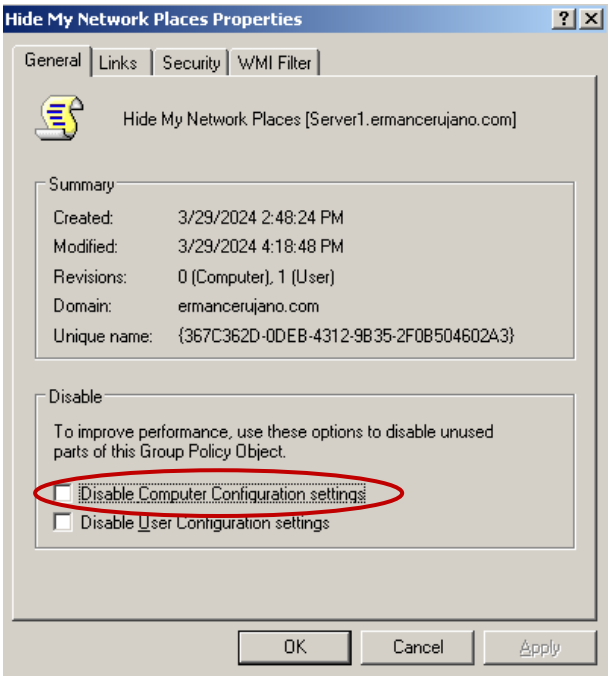
Close the **Group Policy** snap-in tool.

This will bring you back to the **Group Policy** tab for the **ermancerujano.com** domain. Highlight the **Hide My Network Places** GPO and click on the **Properties** button.

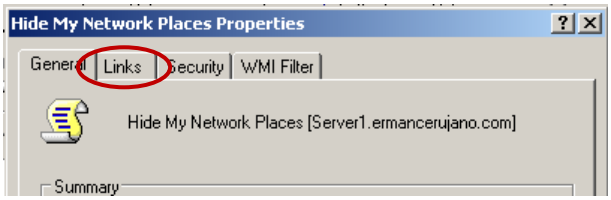


On the properties page of the GPO you will see a summary of the GPO. It shows the date and time it was created and the last time it was modified. Then you will see how many revisions have been made to the GPO. This just tells you how many settings have been changed since the GPO was created. In this case, there one was done for the user configuration. Underneath the summary are

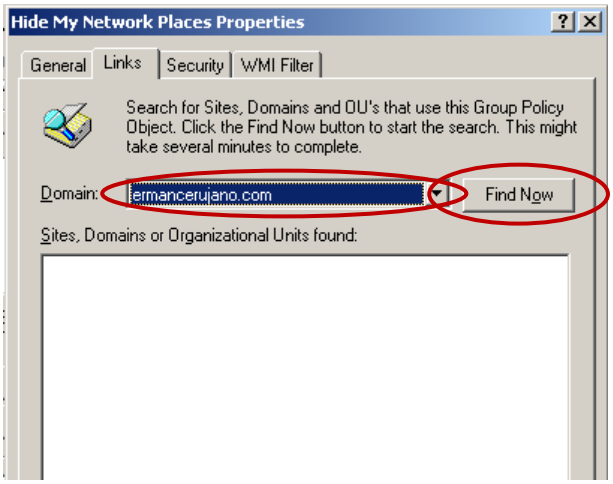
options to disable unused parts of the GPO. For example in this GPO, since only a user setting has been enabled, selecting the **Disable Computer Configuration Settings** will speed up the computer start-up and logon time.



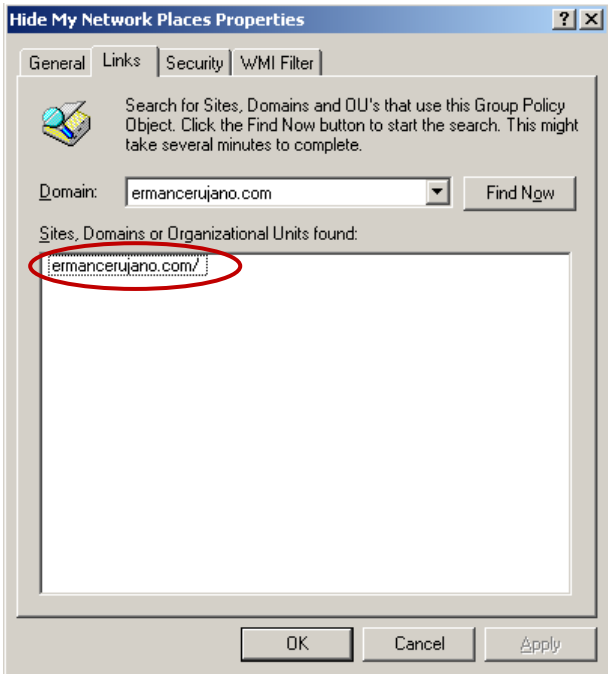
Select the **Links** tab.



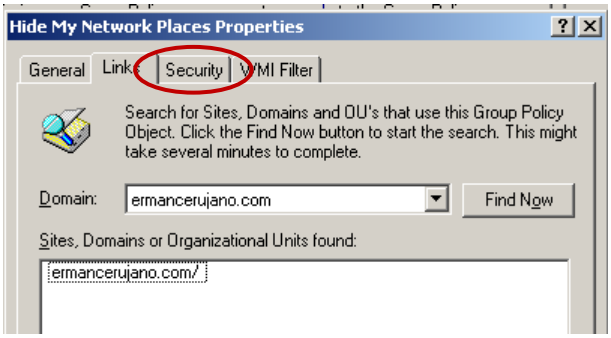
This is where you can do a search to see what containers on the domain have this GPO linked to them as well. Select **ermancerujano.com** domain and click on **Find Now**.



The search should only find the **ermancerujano.com** domain.

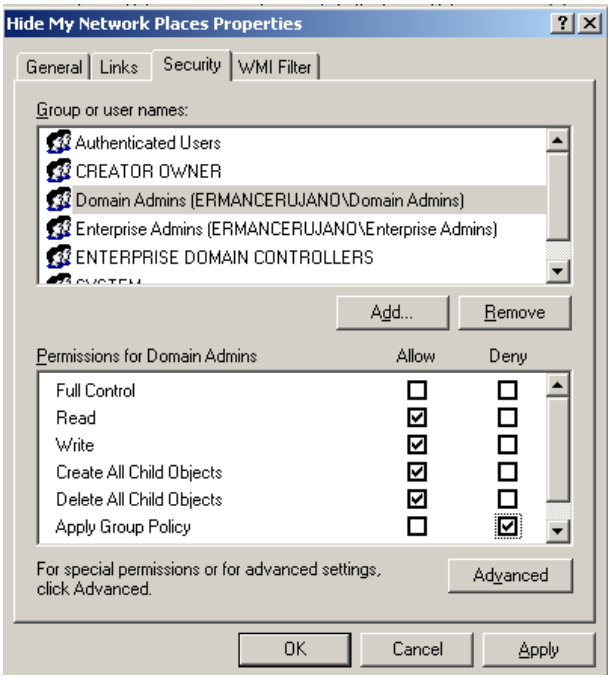


Select the **Security Tab**.

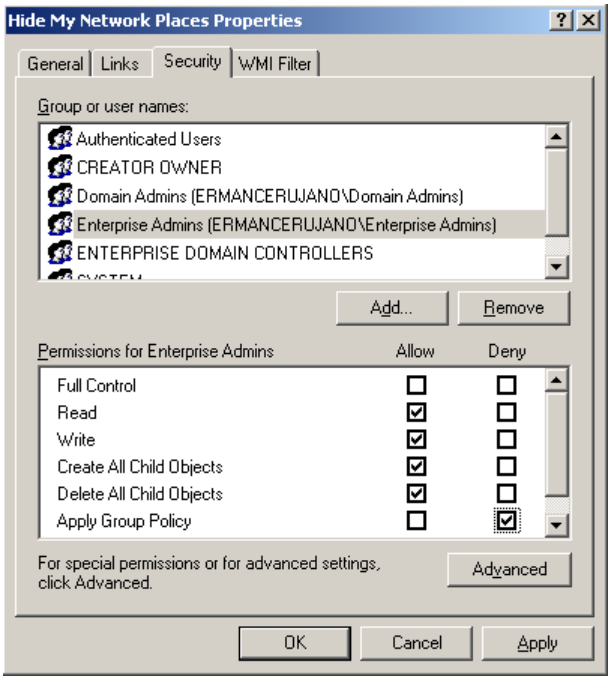


This is where you assign permissions to users or groups for the Active Directory Object that you are working on. You set permissions on an Active Directory Object in a similar fashion to files and folders. Permissions on an Active Directory Object determine what a user or group can “do” to that object (i.e. see it, change it, delete it, etc). In this case, you do not want this policy to apply to any administrator on the domain. So, find the **Domain Admins** group and the **Enterprise Admins** group, and select **Deny** for the **Apply Group Policy** option.

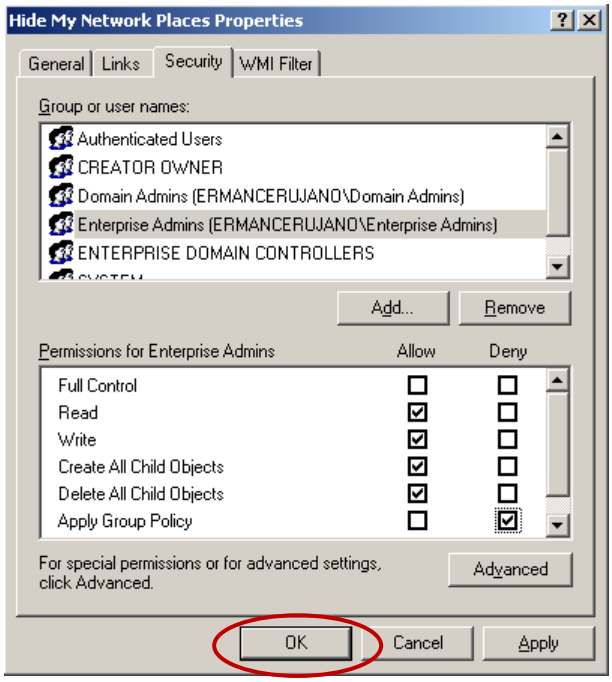
Domain Admins



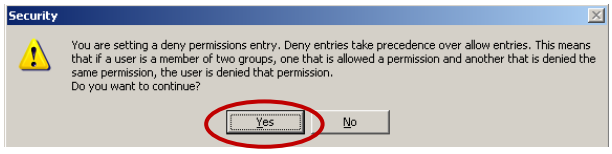
Enterprise Admin



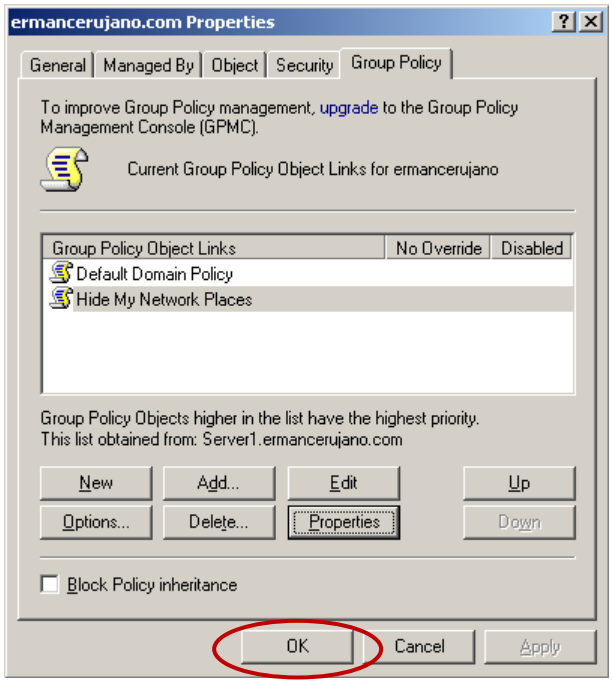
Click **OK**.



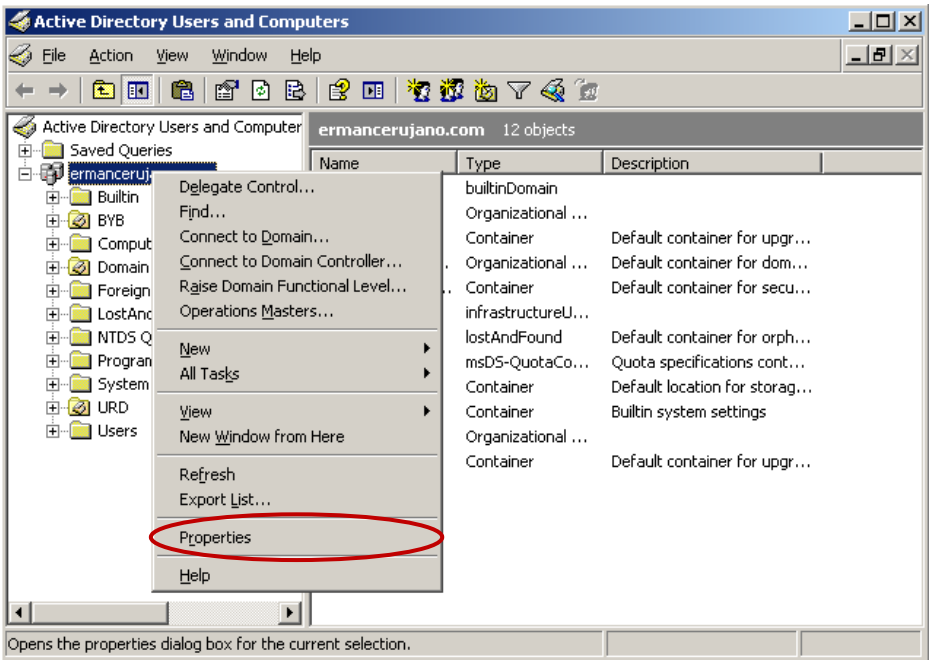
You will get a warning message about setting Deny permissions because the deny permission always take priority over any Allow Permission. Click on **Yes**, that you wish to continue.



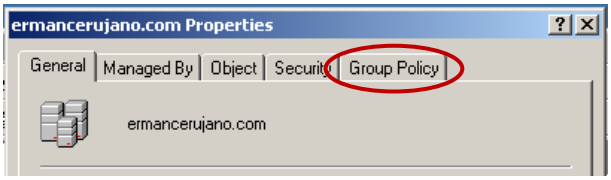
Then click **OK** until you get back to the Active Directory Users and Computers snap-in tool.



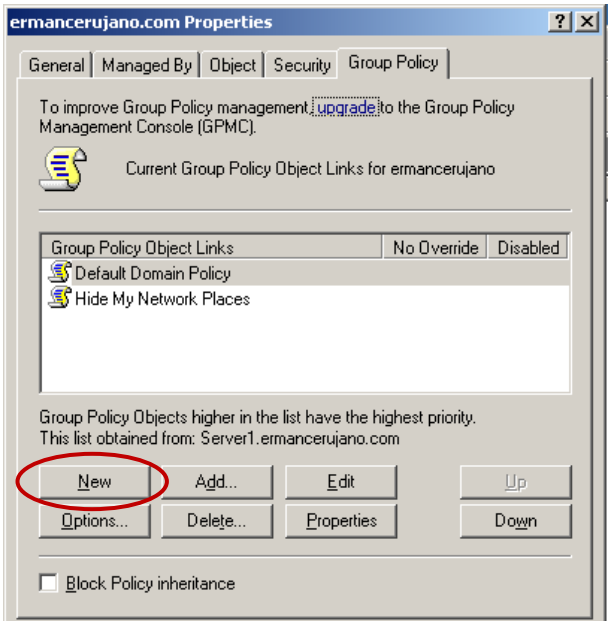
Now, Create a new domain **GPO** that will disable for **Control Panel** for all users except for administrator. Right click on the **ermancerujano.com** domain and select **Properties**.



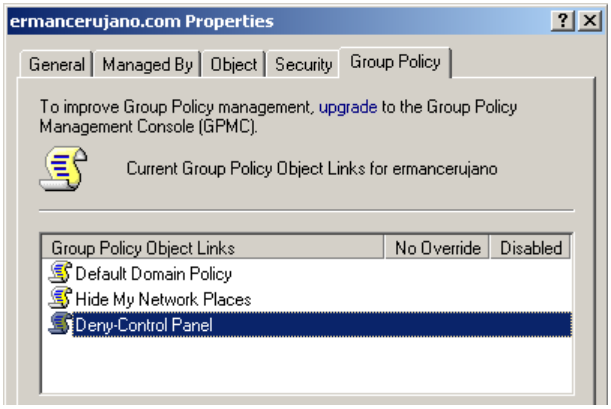
Go to the **Group Policy** tab.



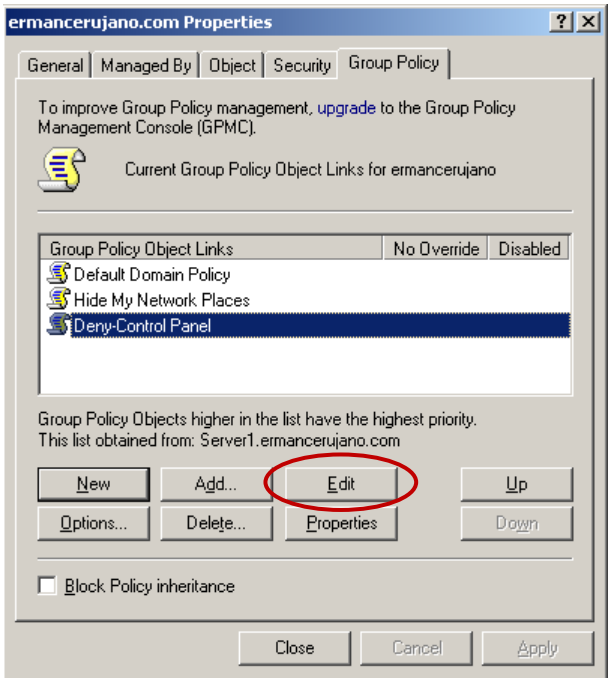
Click on **New.**



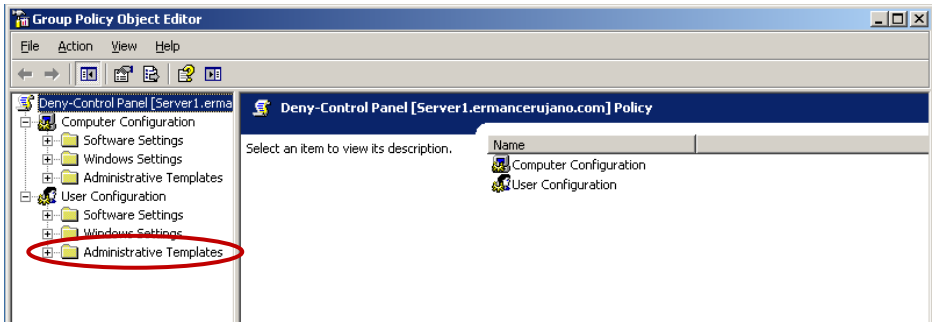
Name the new GPO **Deny-Control Panel**.



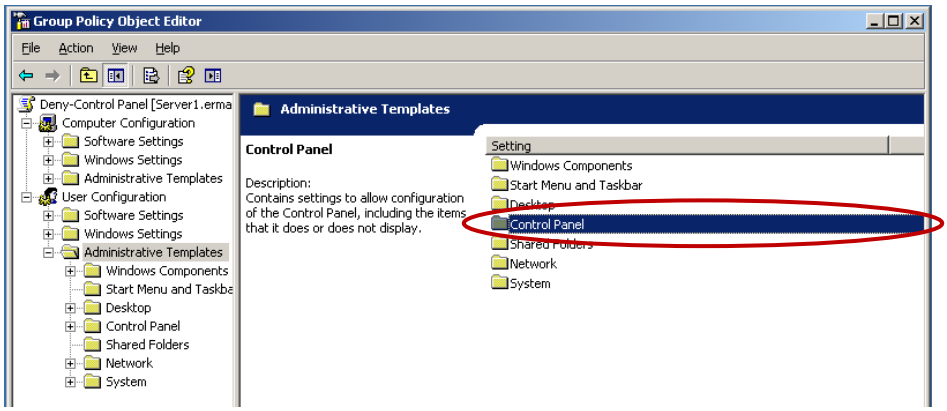
Then click on **Edit** to open the group policy span-in tool for the GPO.



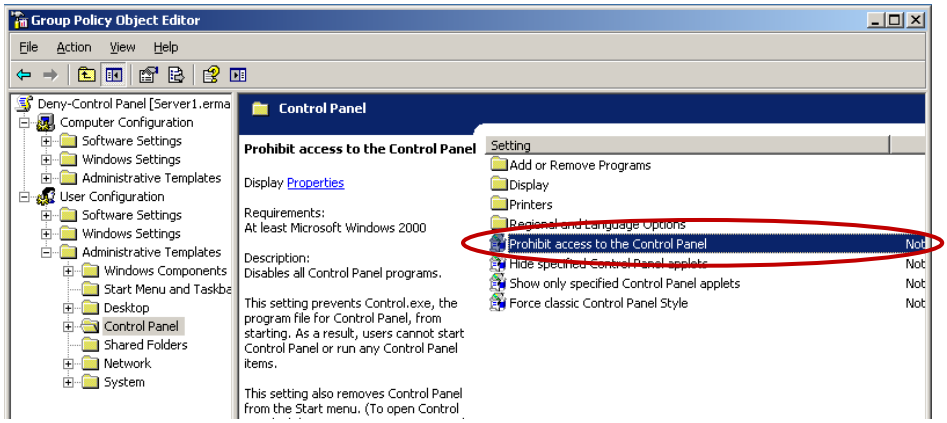
On the snap-in tool, select **Administrative Templates** under **User Configuration**



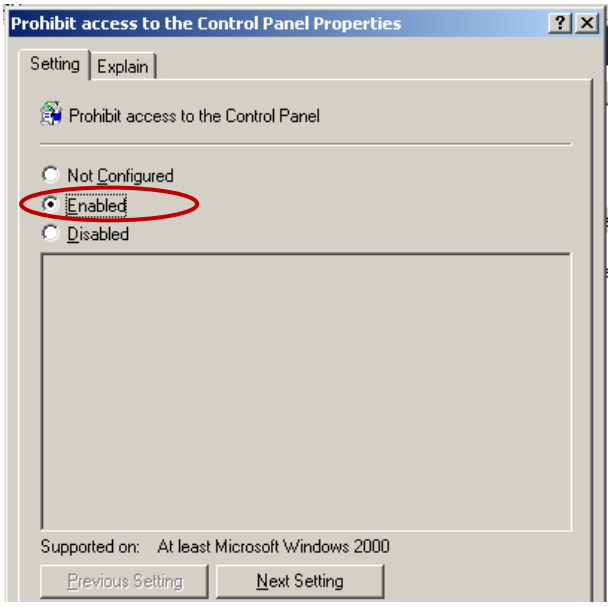
Select **Control Panel**.



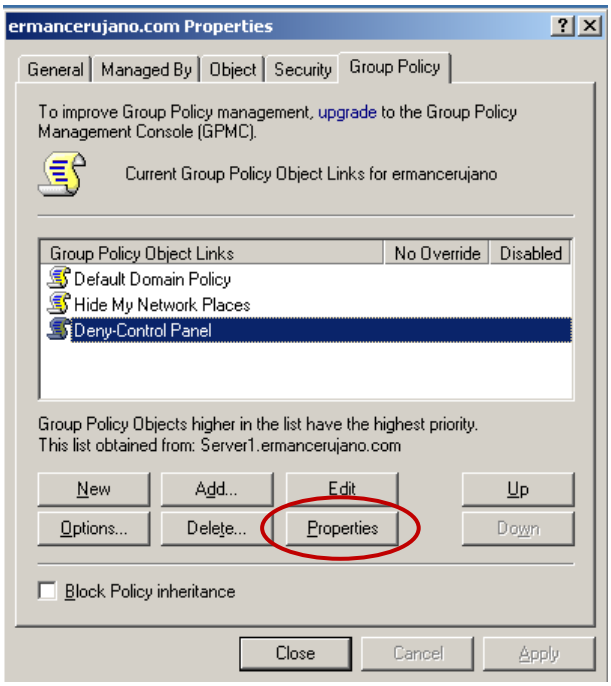
On the right pane double click on the **Prohibit Access to the Control Panel** setting to open the properties.



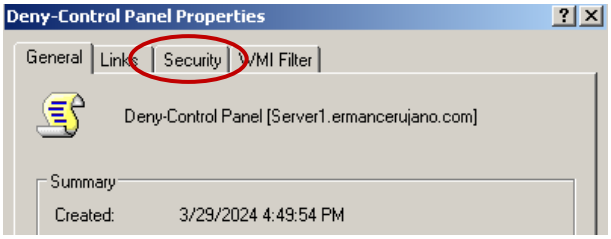
Select **Enable** on the properties page. Click **OK** and you should see that the setting is now enabled.



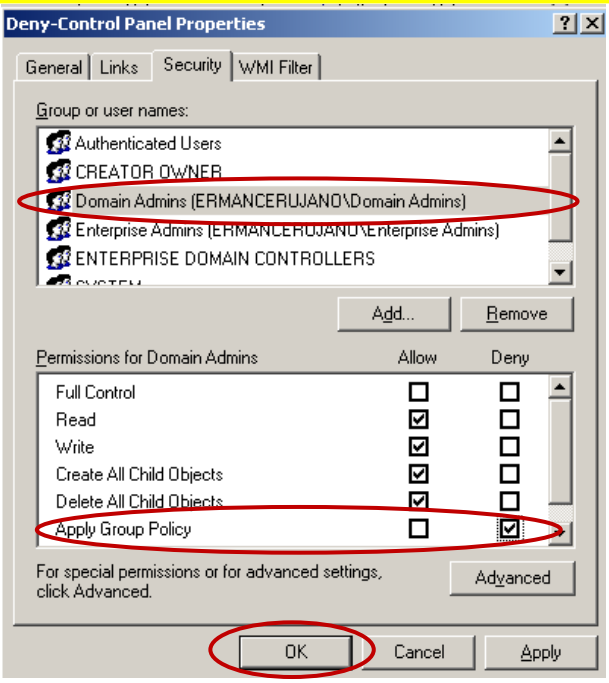
Close the snap-in tool and open the **Deny-Control Panel** GPO **Properties**.



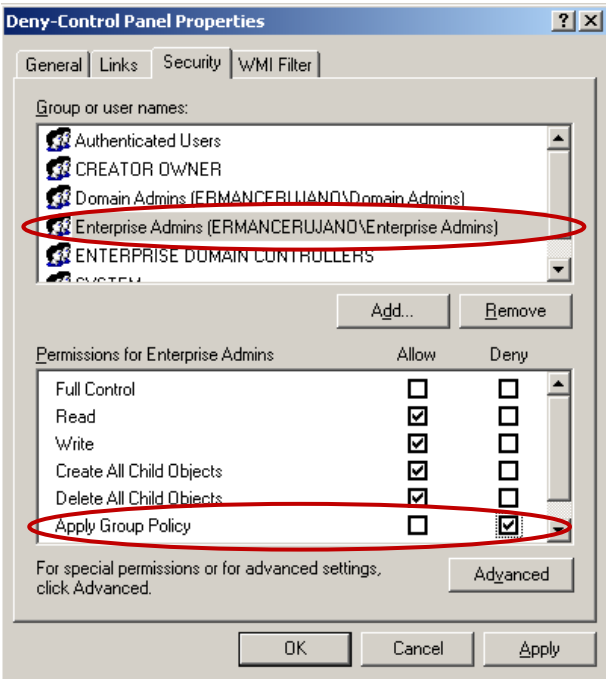
Select the **Security** tab and make sure the GPO does not apply to any **administrators**.



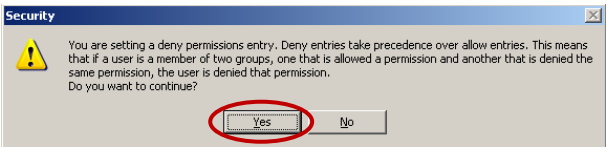
- Select **Domain Admins** and Deny the **Appy Group Policy**.



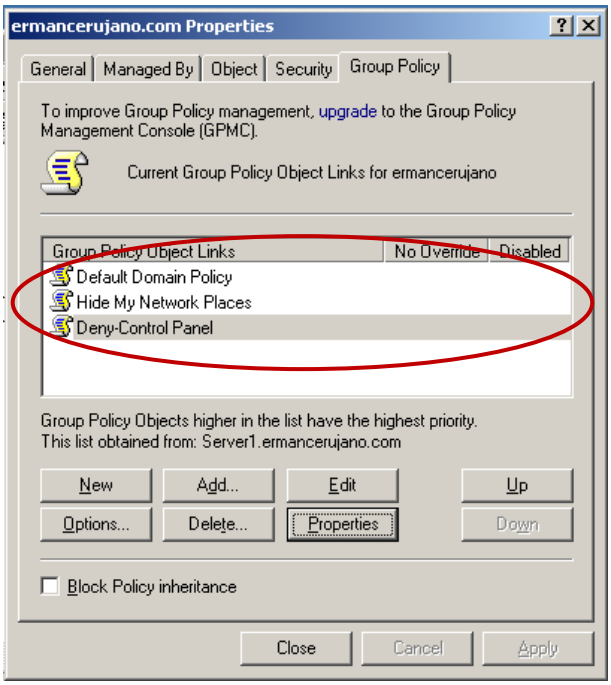
- **Enterprise Admins** and Deny the **Appy Group Policy**.



Click **OK.** You will get a warning message about setting Deny permissions because the deny permission always take priority over any Allow Permission. Click on **Yes**, that you wish to continue.

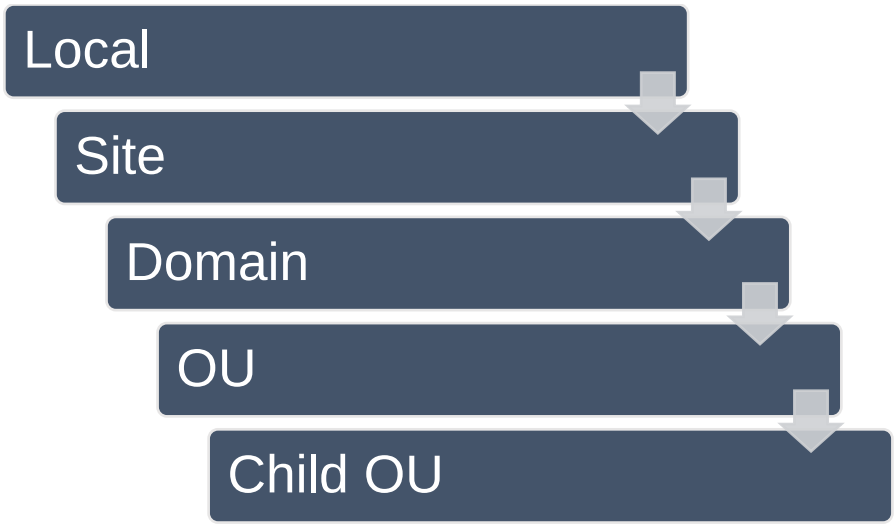


The **ermancerujano.com** domain should now have three GPO's assigned to it.



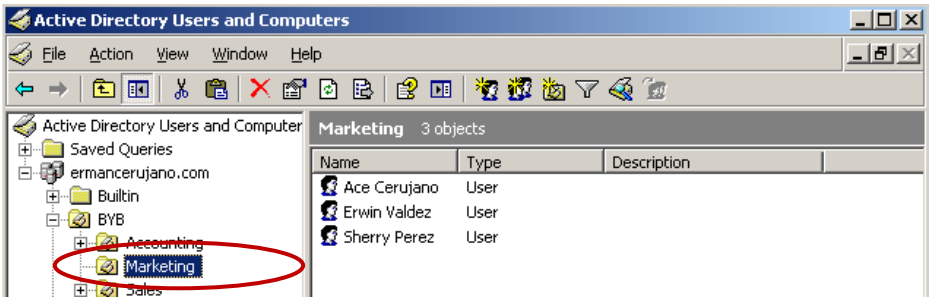
3.2. Create and Assign a Group Policy to Organizational Units

Next, you must allow the users in the Marketing Department access to the control panel so they are able to change the display settings on their desktop. This is necessary because the Marketing Department runs a piece of software that works best at lower resolutions. Instead of editing the security list for the GPO, you should create a GPO that will apply only to the Marketing OU, which contains all of the users in the Marketing Department. This can be done by creating and assigning the GPO at the OU level so that it overrides the GPO set at the domain level. The order in which the policies are applied is:

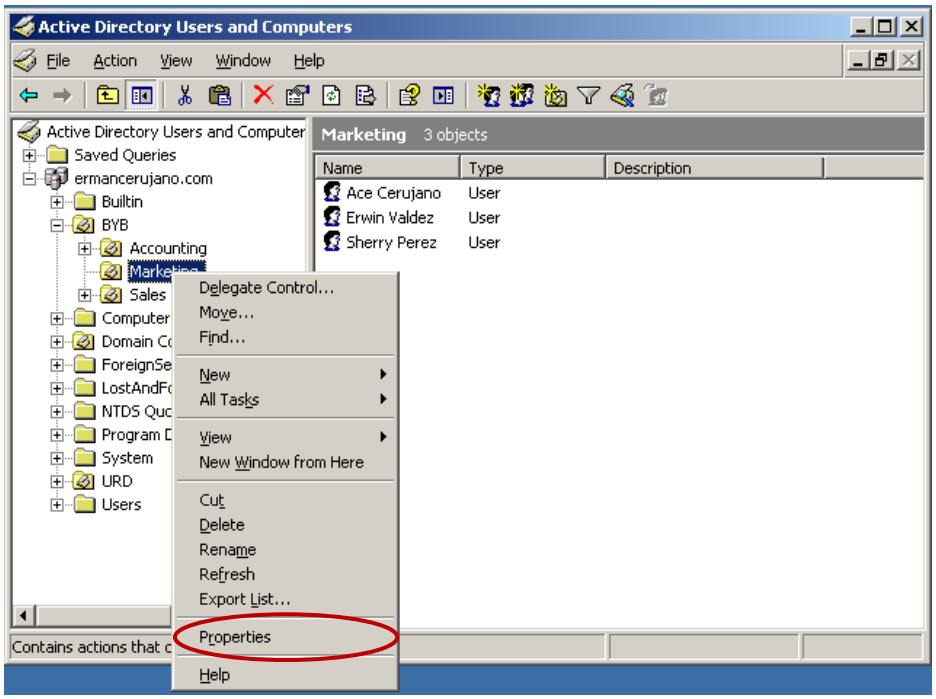


In other words, any OU policy will override a domain policy, a domain policy will override a site policy, a domain policy will override a site policy, and a site policy will override a local policy. Keep in mind that this order of precedence only applies to contradicting policy settings. For example, a policy to install software that is applied at the site level will not be overridden by a policy at the OU level to determine the background color of the desktop. But, if you set a policy for a green desktop background at the site level and set a policy for a blue desktop background at the OU level, users or computers within the OU will receive the blue desktop background.

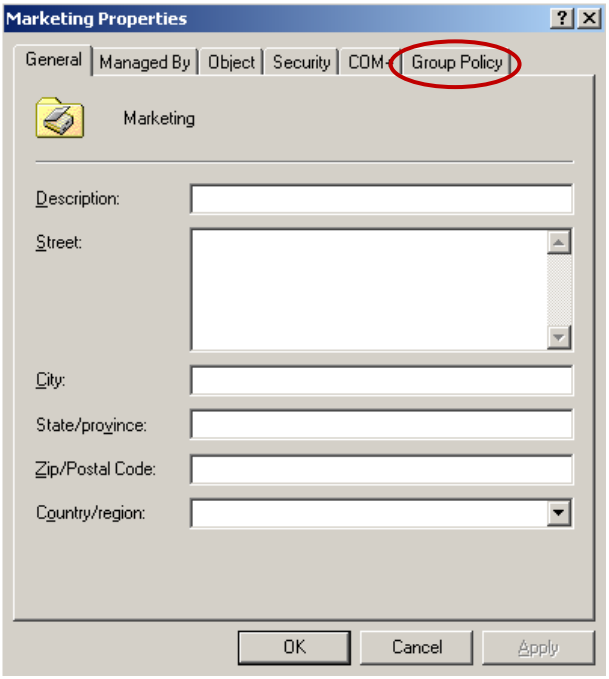
Within the Active Directory Users and Computers console, find the **Marketing OU** located within the **BYB (Bayambang)** OU.



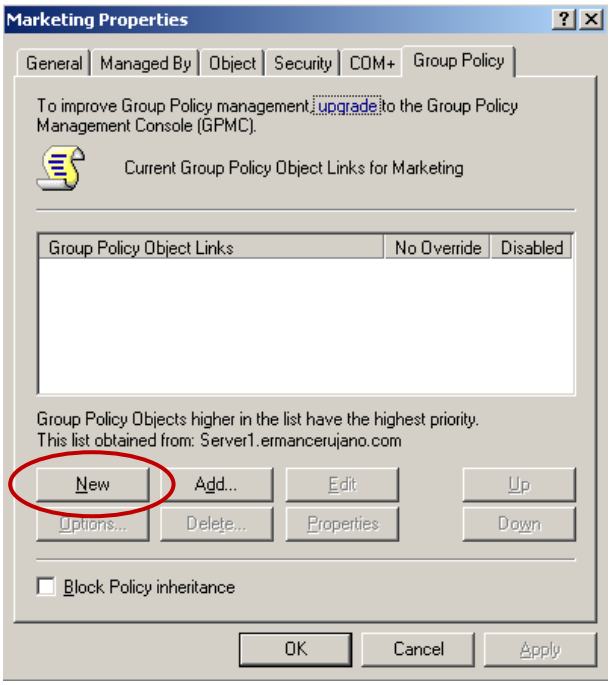
Right click on the **OU**, select **Properties**.



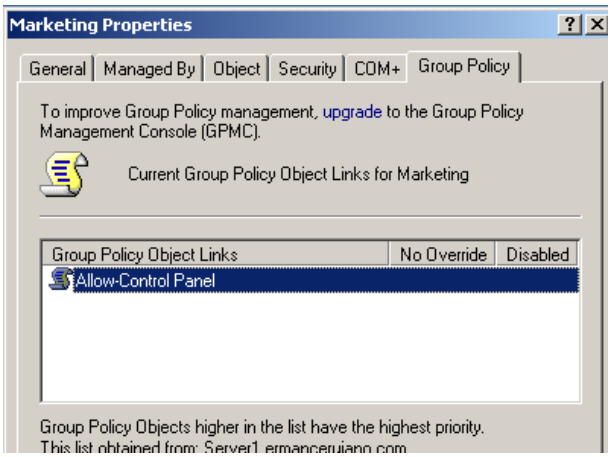
On the properties page select the **Gorup Policy** tab.



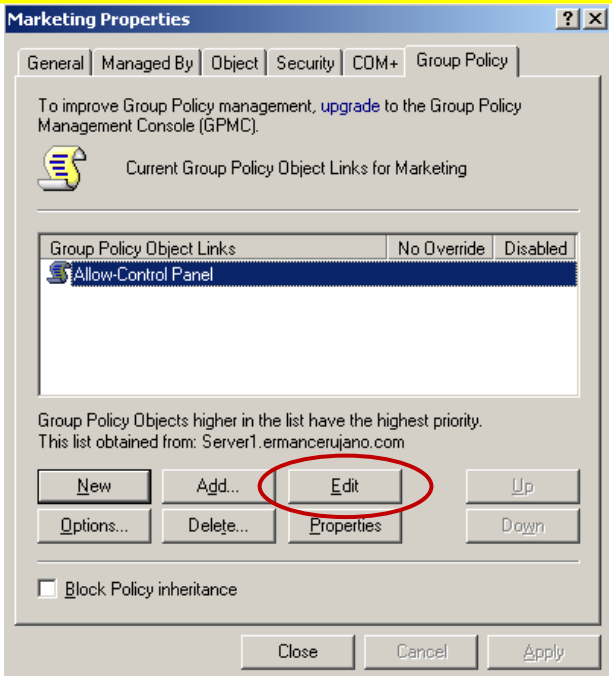
Click on **New** to create a new **GPO** that will be assigned to this OU.



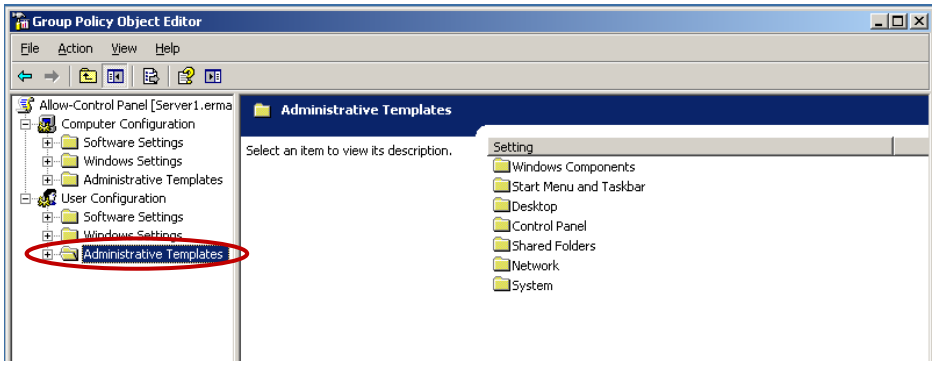
Name the new GPO **Allow-Control Panel**.



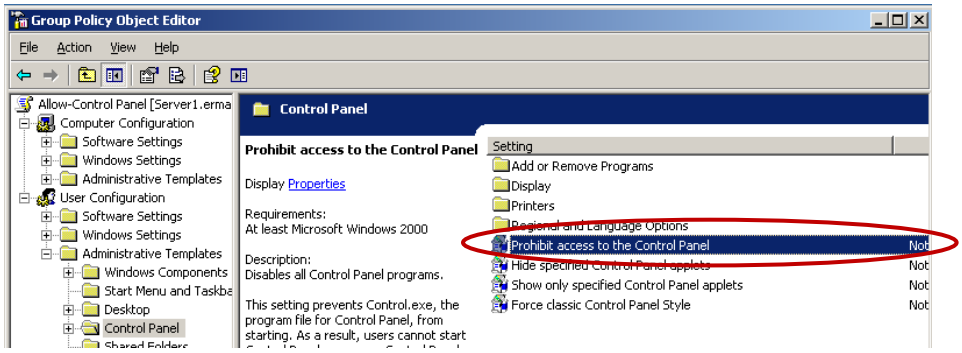
Highlight the new GPO and click **Edit** to open the policy settings snap-in tool.



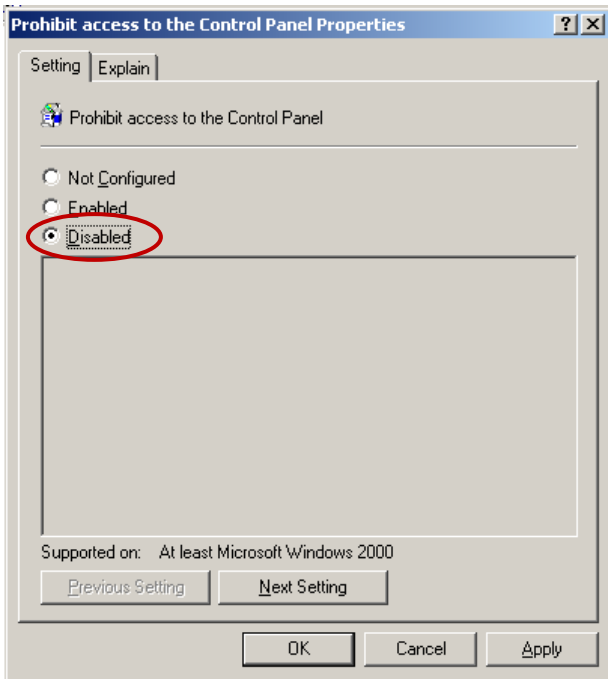
Open the **Control Panel** settings, which are located under **User Configuration** and **Administrative Templates**.



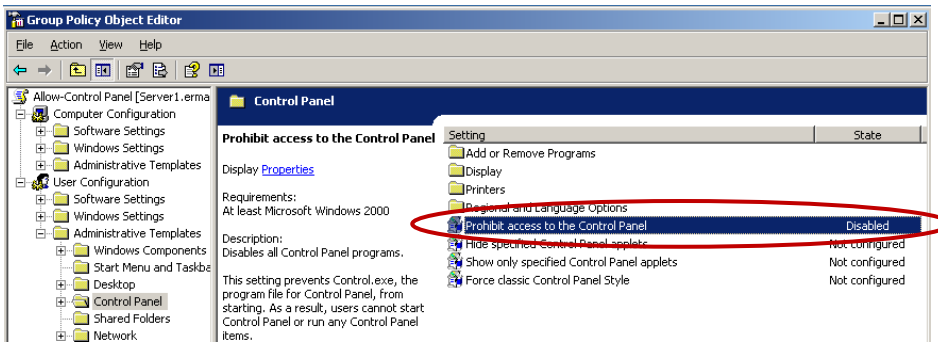
Find the setting **Prohibit Access to the Control Panel** in the right pane and double click on it.



On the setting properties select the **Disable** option and click **OK**.



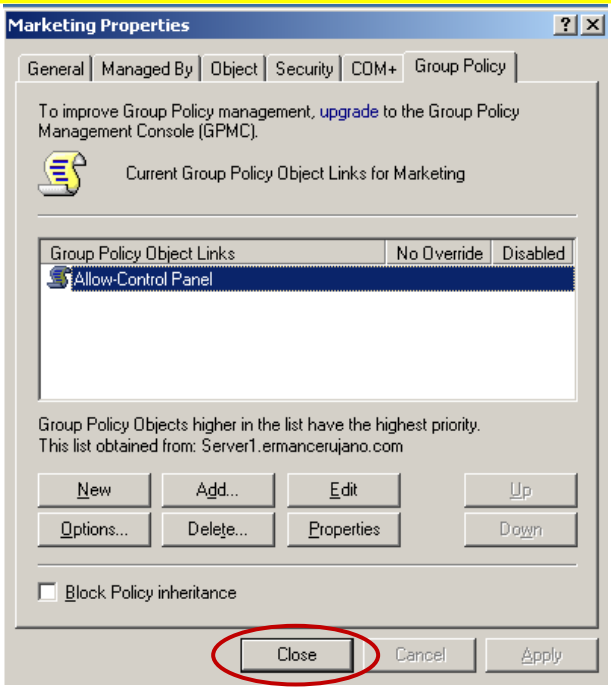
You should now see that the **Prohibit Access to the Control Panel setting** show that it is **Disabled**.



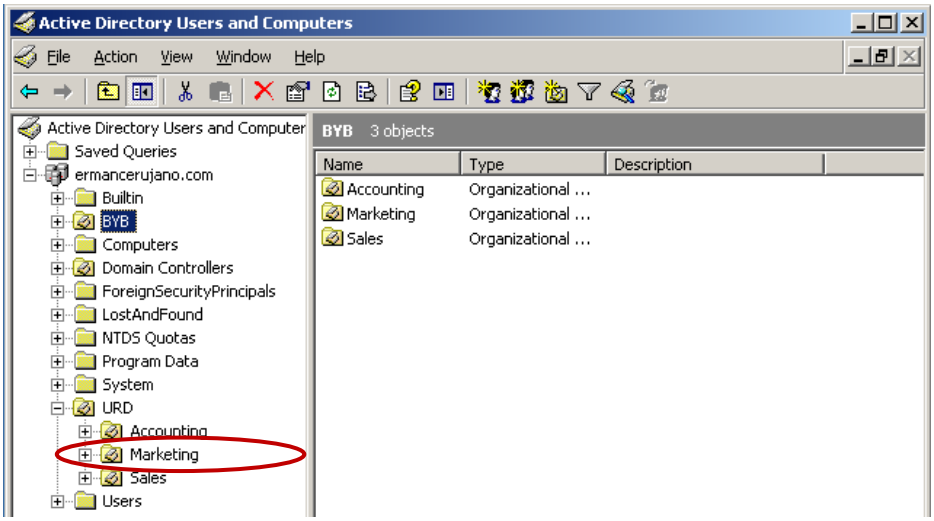
Note:

You must carefully read what the policy setting does, before configuring it, because some of the policy settings can sound confusing and you may have to read it twice. For example you just disabled the disable control panel setting. Do you know exactly what this will accomplish? By configuring the setting to disable, it will allow all users with this GPO to access the control panel. When you enabled this setting on the GPO at the domain level you enabled it so that all domain users will not be able to access the control panel.

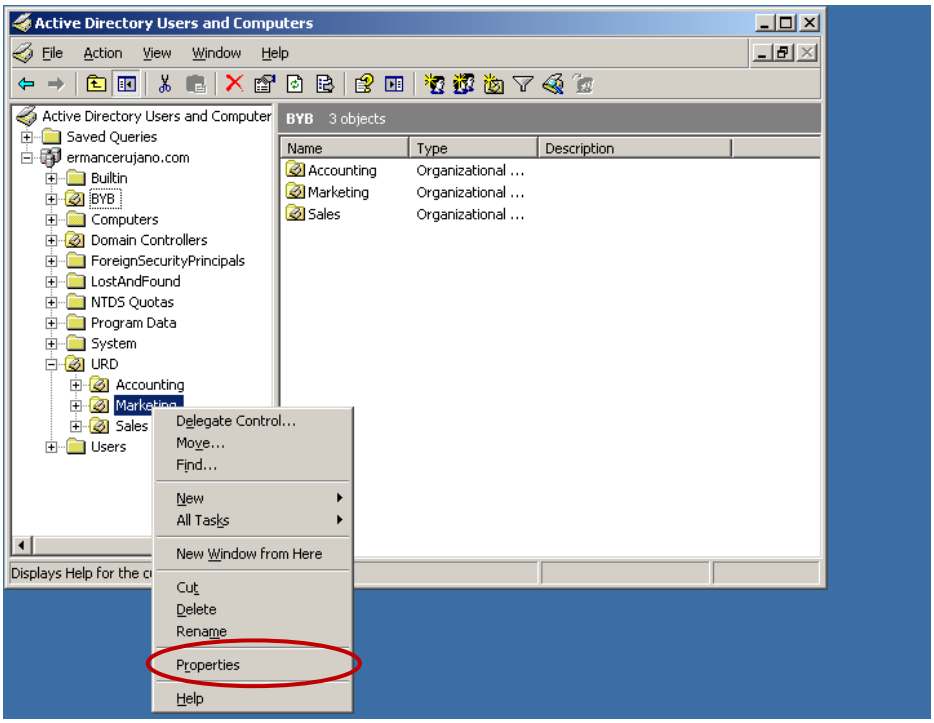
Close the **Group Policy** snap-in tool and make sure the **Allow-Control Panel GPO** appears on GPO links list, then click **Close**.



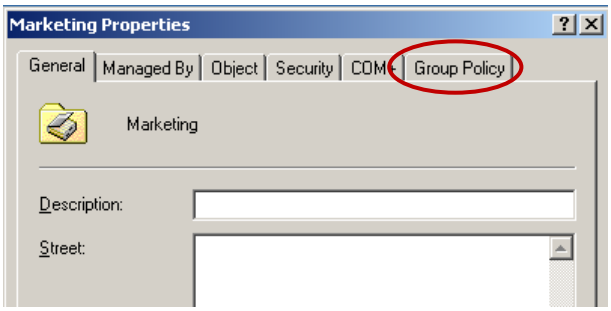
Now you will need to add the same policy to the **Urdaneta – Marketing OU**. Open the **Active Directory Users and Computers** console, find the **Marketing OU** located within the **URD (Urdaneta) OU**.



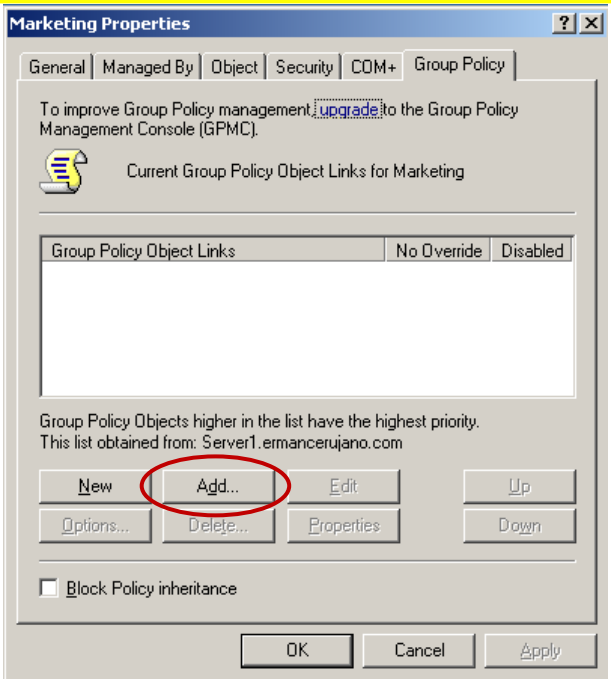
Right click on the **OU**, select **Properties**.



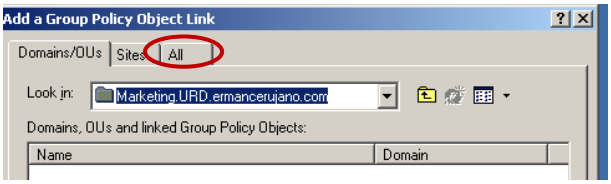
On the properties page select the **Group Policy** tab.



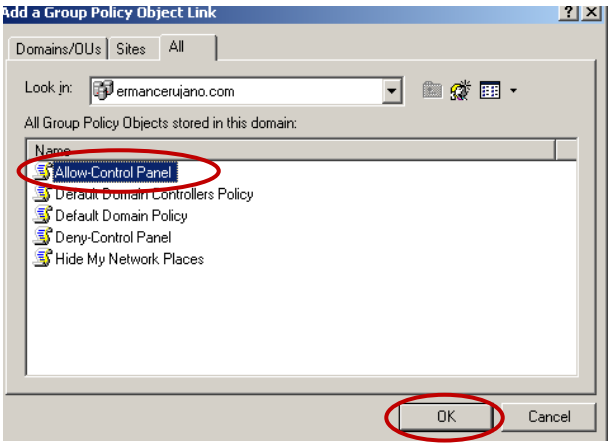
This time instead of creating a new GPO for the same policy setting, you will use the same GPO that you created for the **Bayambang – Marketing OU**. To link the GPO that you created previously to this **OU**, click on **Add**.



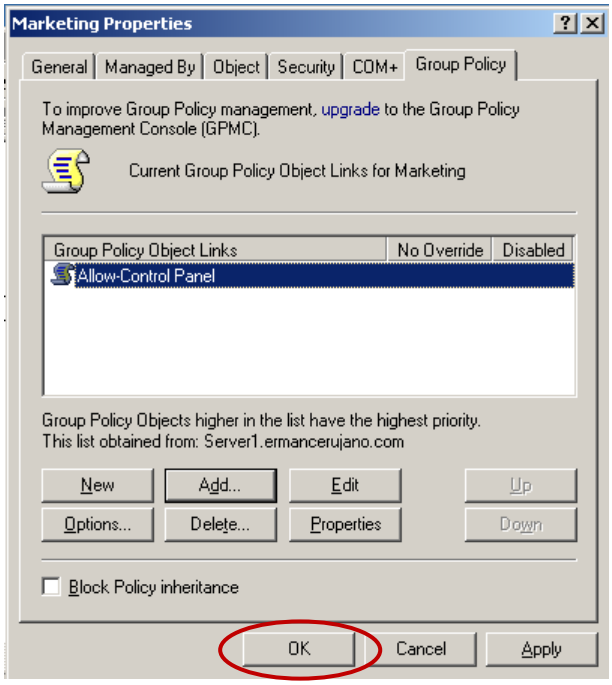
This will bring you up a list of GPO's that are stored within Active Directory. You can search for a GPO by domain, OU, or site. The last tab, **All**, will show you all of the domains within Active Directory and is generally the easiest to work with. Select the **All** tab.



Then select the **Allow-Control Panel** GPO and click **OK**.



You should now see the **Allow-Control Panel** GPO appears on the group policy links list for the **Urdaneta – Marketing OU**. Anytime there is a change made to the **Allow-Control Panel** GPO it will now affect both **OU**'s. This makes it easier to manage the GPO from just one location and then have the policy settings apply to all of the containers that are linked to it. Click **OK** and close the **Active Directory Users and Computers** snap-in tool.


Marketing Properties
General
Managed By
Object
Security
COM+
Group Policy
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).
Current Group Policy Object Links for Marketing
Group Policy Object Links
No Override
Disabled
Allow-Control Panel
Group Policy Objects higher in the list have the highest priority.
This list obtained from: Server1.ermancerujano.com
New
Add...
Edit
Up
Options...
Delete...
Properties
Down
Block Policy inheritance
OK
Cancel
Apply

3.3. Test the GPO's from a Client

Log on to **client1** as the user **Jeff Morales** (jmorales). Remember that this user works in the accounting department in Bayambang. Therefore, she is a member of the **Accounting OU** located within the **Bayambang OU** (**BYB**) and should now have access to the **My Network Places icon**, the **control panel** or the **display settings from the desktop**.

		YES	NO
1	Can the User view **My Network Places** icon on the desktop?		X
2	Can the User access the **Control Panel** from the start menu?		X
3	Can the User access the **Display Settings** from the desktop?		X

1. Can the User view **My Network Places** icon on the desktop? (NO)

   On the desktop, look for the **My Network Places** icon. If you cannot see it on the desktop then the **Hide My Network Places** GPO is working.

2. Can the User access the **Control Panel** from the start menu? (NO)

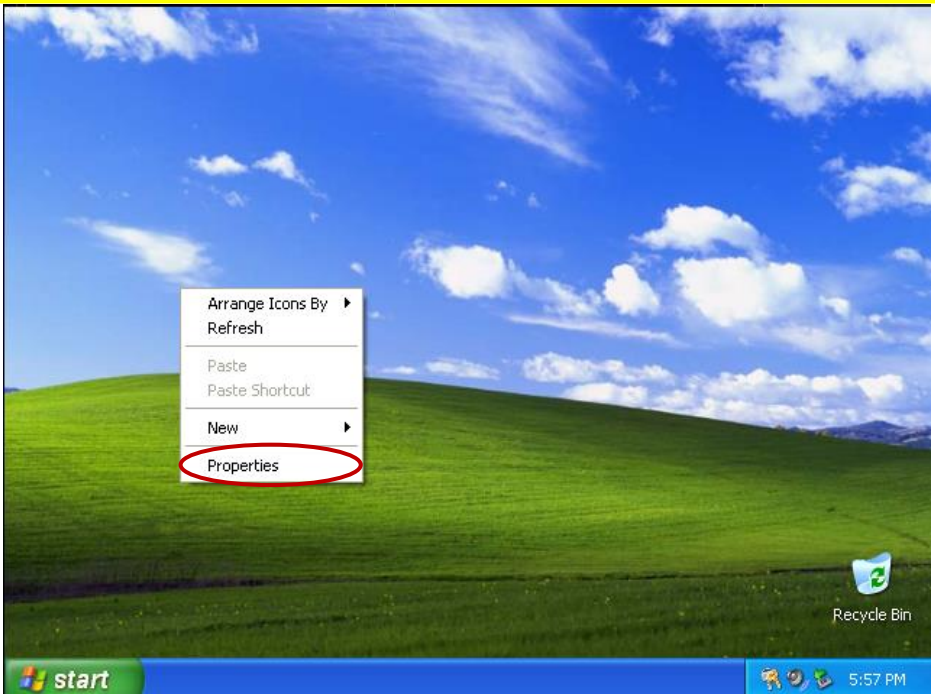
   Now look in the Start menu to see if the Control Panel is available.

   ➢ Go to start then settings.

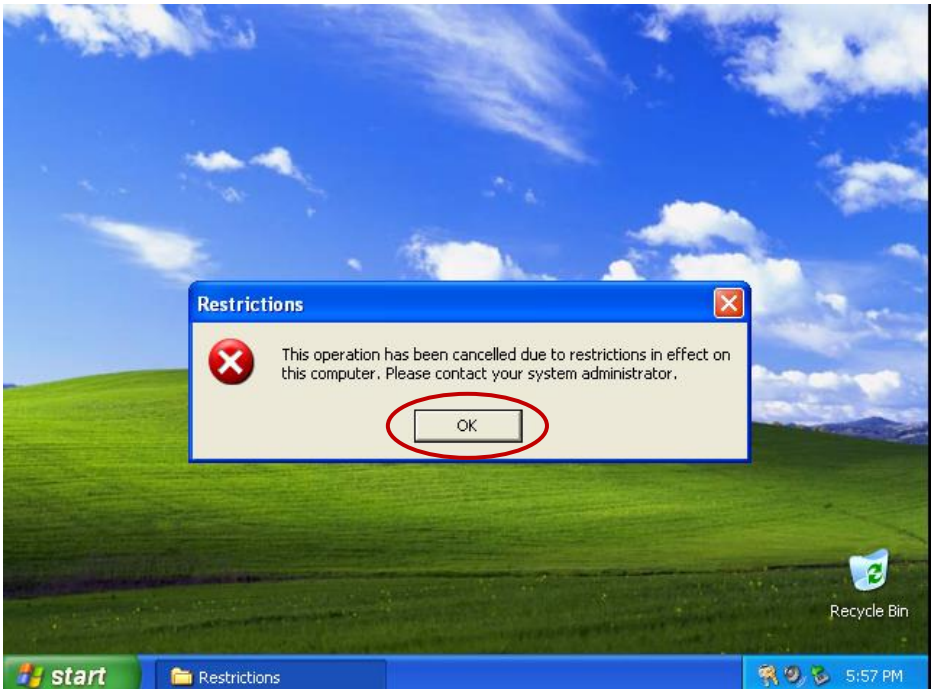
If you do not have the Control Panel option available then the **Deny-Control Panel** GPO is working.

3. Can the User access the **Display Settings** from the desktop? (NO)

Now try to access the display setting by right clicking on any **free space** on the **desktop** and selecting **Properties**.



You should get an error message appear saying that the operation has been cancelled due to restriction on the computer which means that the **Deny-Control Panel** GPO is working. Click **OK**.



Log off the user **Jeff Morales (jmorales)** and log back on with the user **Erwin Valdez (evaldez)**. Remember the user **Erwin Valdez** works in the marketing department in Bayambang. Therefore he is a member of the **Marketing OU** located within the **Bayambang OU** (**BYB**) and should now have access to the My Network Places icon but he should have access to the control panel and the display settings from the desktop.

		YES	NO
1	Can the User view **My Network Places** icon on the desktop?		X
2	Can the User access the **Control Panel** from the start menu?	X	
3	Can the User access the **Display Settings** from the desktop?	X	

1. Can the User view **My Network Places** icon on the desktop? (NO)

   On the desktop, look for the **My Network Places** icon. If you cannot see it on the desktop then the **Hide My Network Places** GPO is working.

2. Can the User access the **Control Panel** from the start menu? (YES)

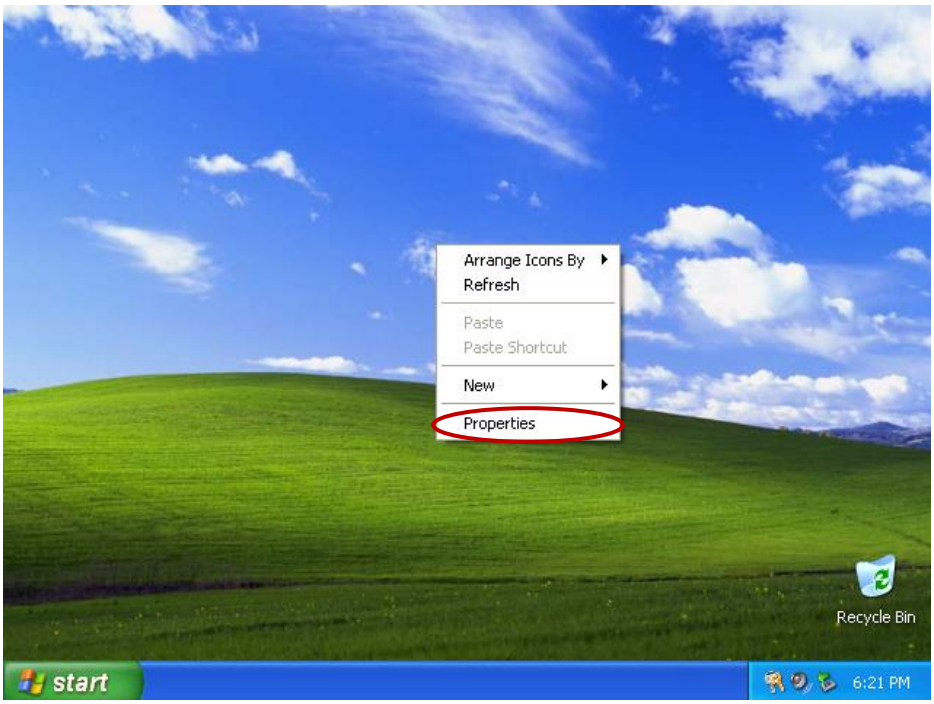
   Now look in the Start menu to see if the Control Panel is available.

   ➢ Go to start then settings.

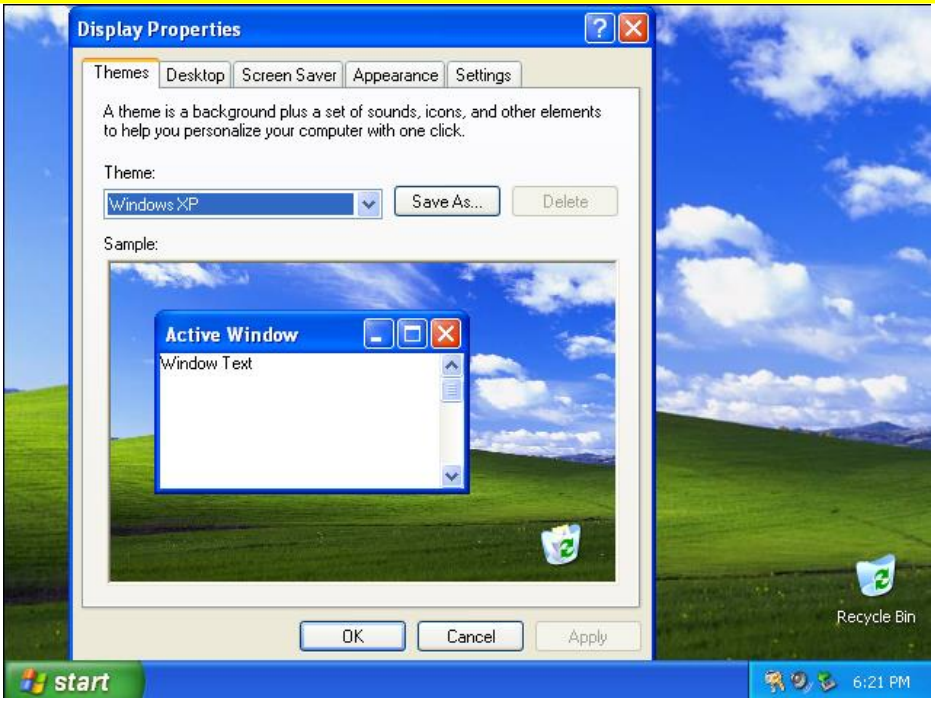
   As you can see, Erwin Valdez has a control panel.

3. Can the User access the **Display Settings** from the desktop? (YES)

Now try to access the display setting by right clicking on any **free space** on the **desktop** and selecting **Properties**.



As you can see, we can access the display settings from the desktop.



Test the group policy settings with the User **Ace Cerujano (acerujano**) who is located in the **Marketing OU** within the **Urdaneta OU (URD)**. This user should have the same policy settings as the user **Erwin Valdez (evaldez)** from the **Marketing OU** in **Bayambang**.

		YES	NO
1	Can the User view **My Network Places** icon on the desktop?		X
2	Can the User access the **Control Panel** from the start menu?	X	
3	Can the User access the **Display Settings** from the desktop?	X	

1. Can the User view **My Network Places** icon on the desktop? (NO)

   On the desktop, look for the **My Network Places** icon. If you cannot see it on the desktop then the **Hide My Network Places** GPO is working.

2. Can the User access the **Control Panel** from the start menu? (YES)

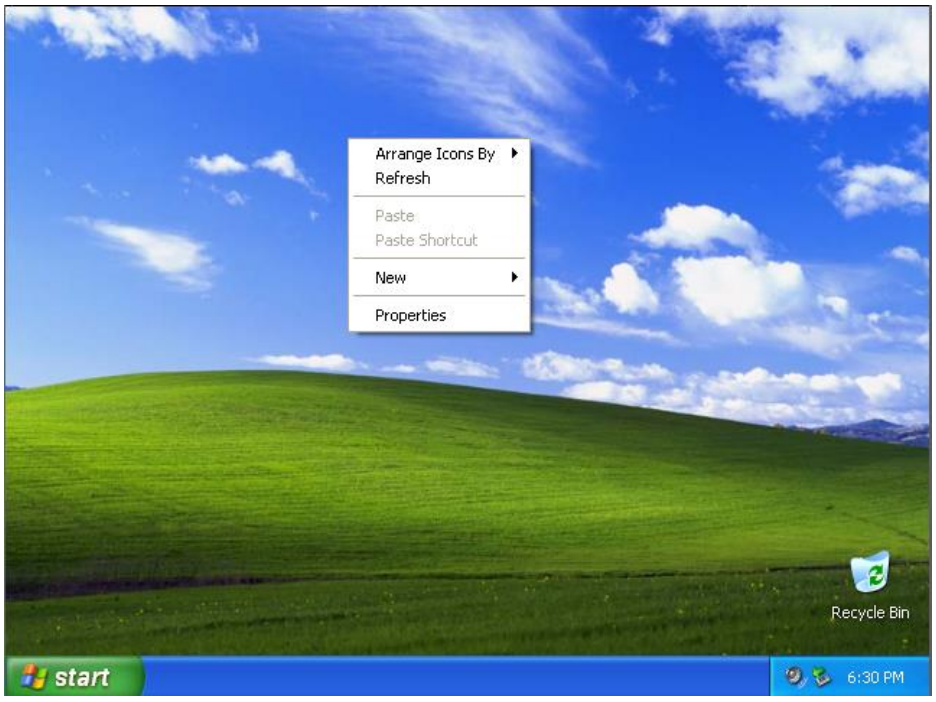
Now look in the Start menu to see if the Control Panel is available.

- Go to start then settings.

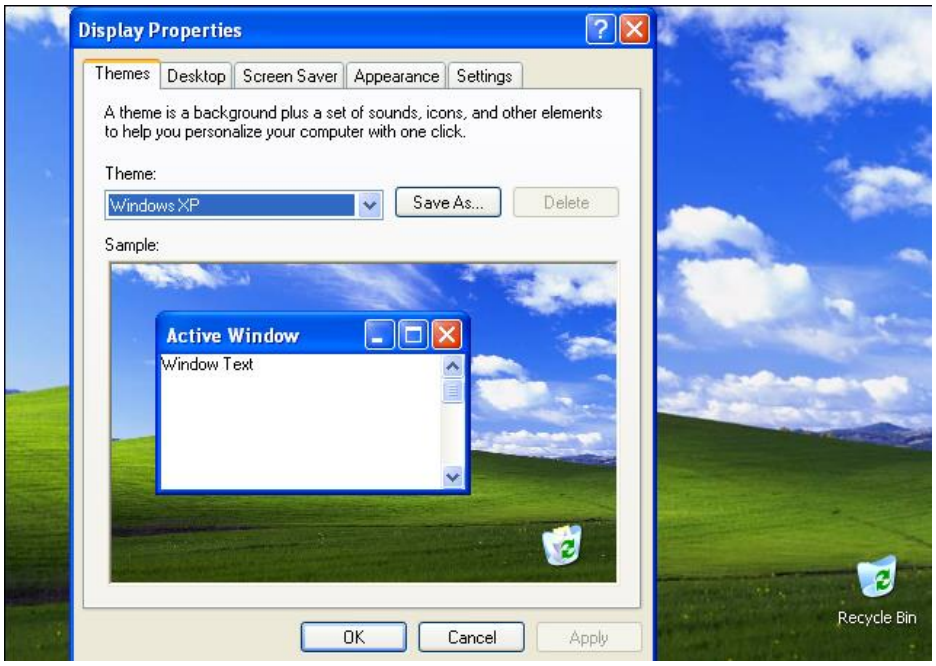
As you can see, Ace Cerujano has a control panel.

3. Can the User access the **Display Settings** from the desktop? (YES)

Now try to access the display setting by right clicking on any **free space** on the **desktop** and selecting **Properties**.



As you can see, we can access the display settings from the desktop.



Log off the user and log back on as the **domain administrator**. You should be able to access everything because none of the GPO's applies to any of the administrators.

		YES	NO
1	Can the User view **My Network Places** icon on the desktop?	X	
2	Can the User access the **Control Panel** from the start menu?	X	
3	Can the User access the **Display Settings** from the desktop?	X	

1. Can the User view **My Network Places** icon on the desktop? (YES)

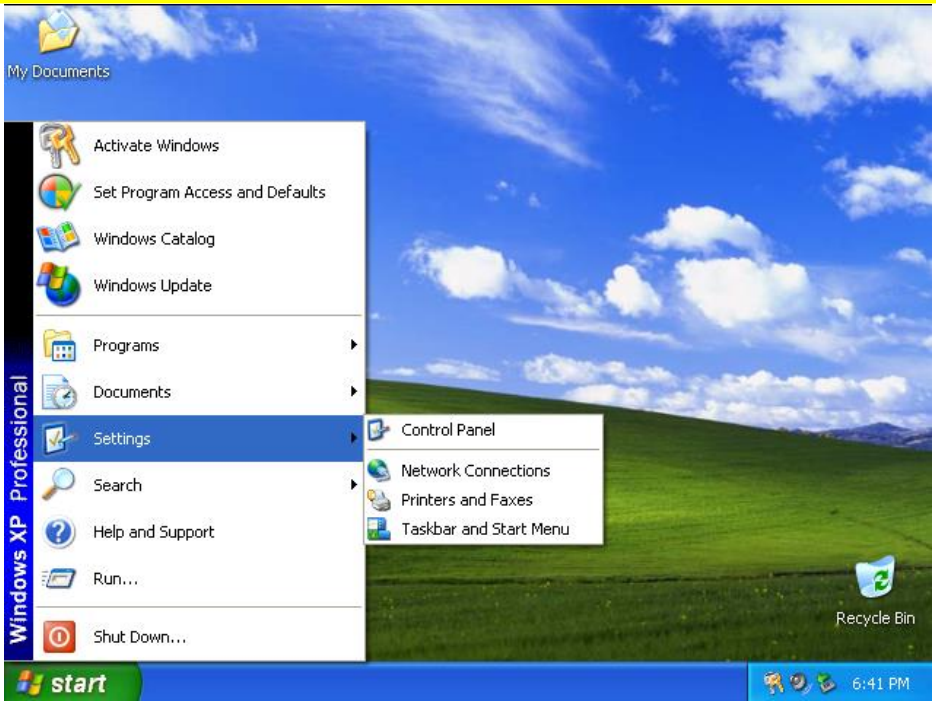
   On the desktop, look for the **My Network Places** icon. As you can see, we have **My Network Places** icon in our desktop.

2. Can the User access the **Control Panel** from the start menu? (YES)

   Now look in the Start menu to see if the Control Panel is available.

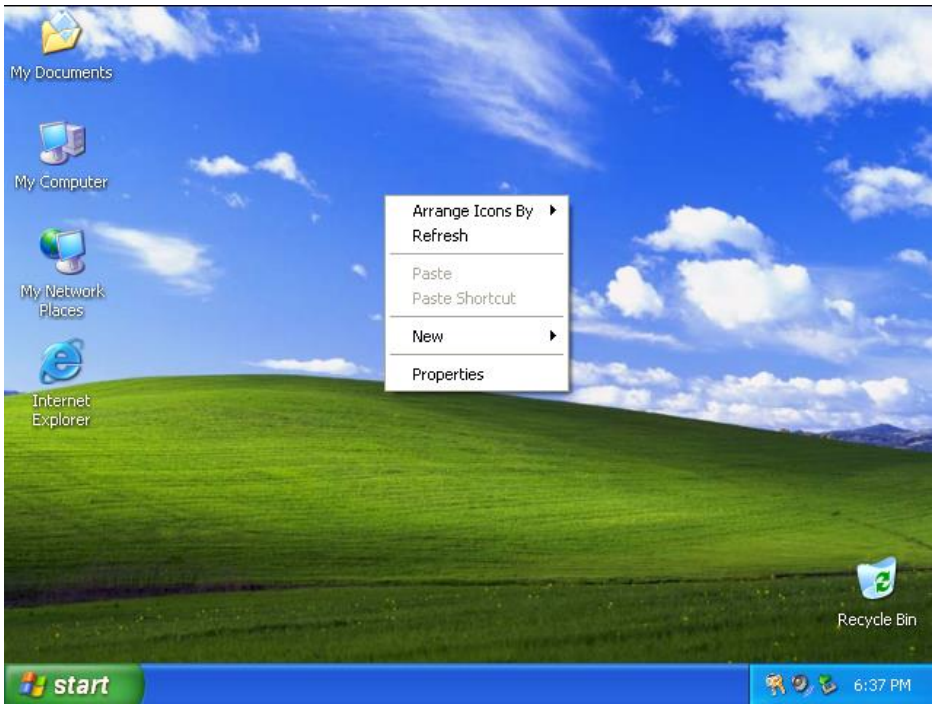
   ➢ Go to start then settings.

   As you can see, administrator has a control panel.

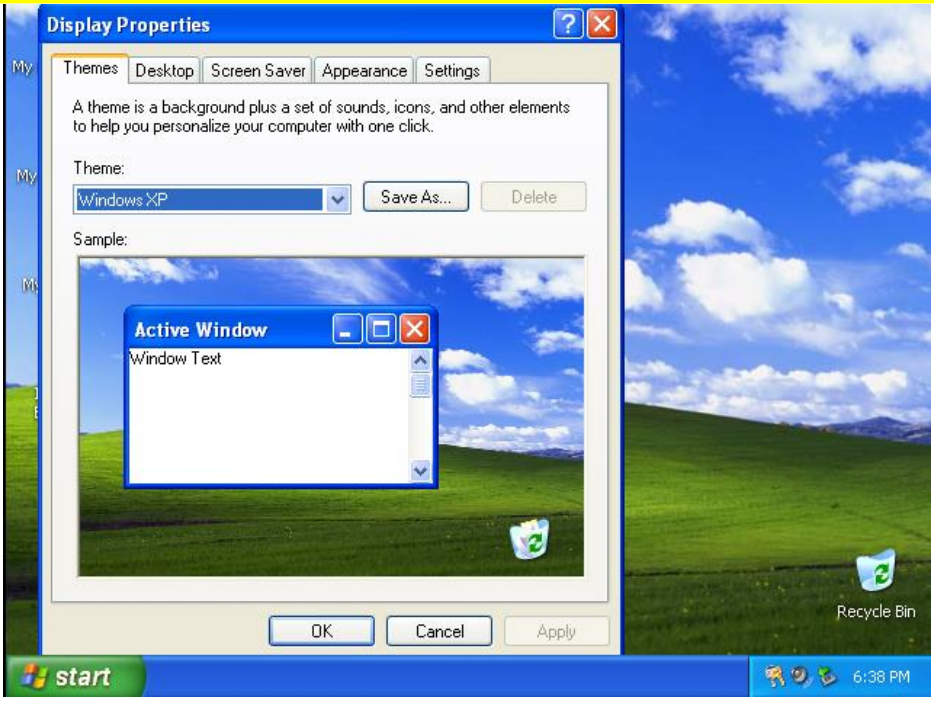


3. Can the User access the **Display Settings** from the desktop? (YES)

   Now try to access the display setting by right clicking on any **free space** on the **desktop** and selecting **Properties**.

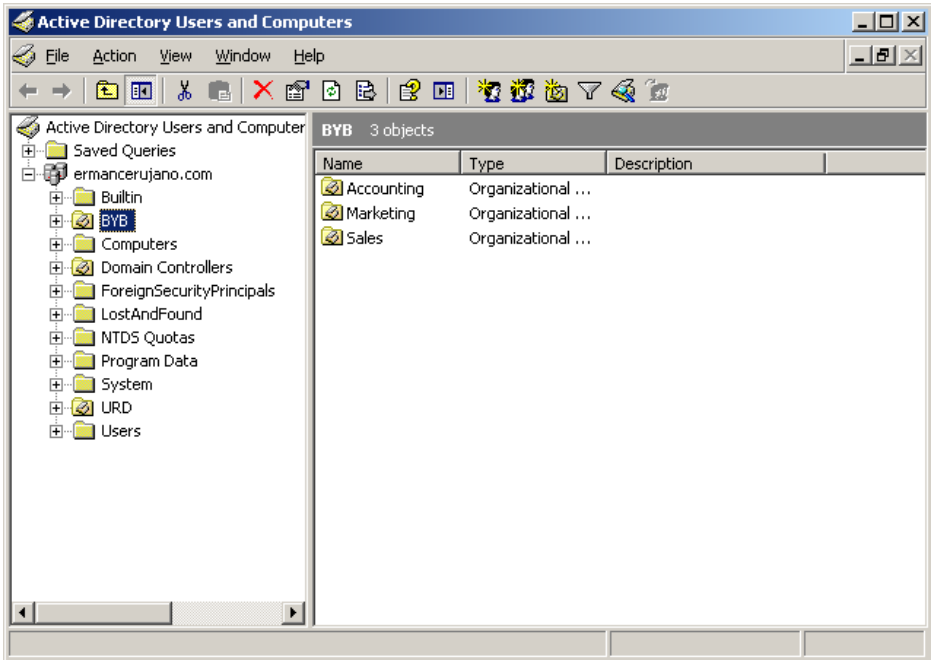


As you can see, we can access the display settings from the desktop.

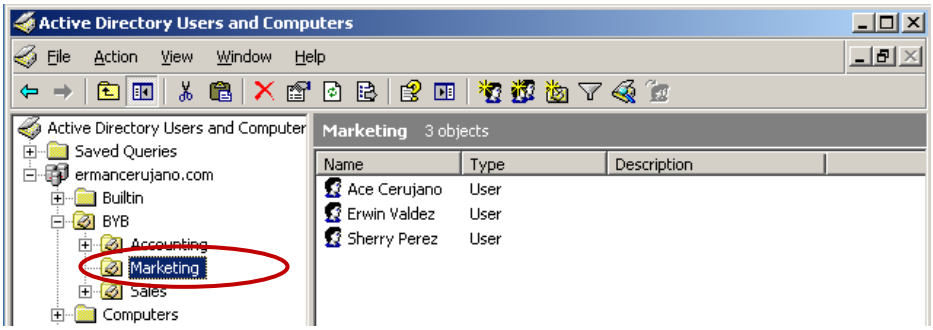

Display Properties
Themes
Desktop
Screen Saver
Appearance
Settings
A theme is a background plus a set of sounds, icons, and other elements to help you personalize your computer with one click.
Theme:
Windows XP
Save As...
Delete
Sample:
Active Window
Window Text
OK
Cancel
Apply
Recycle Bin
start
6:38 PM

3.4. Removing a GPO

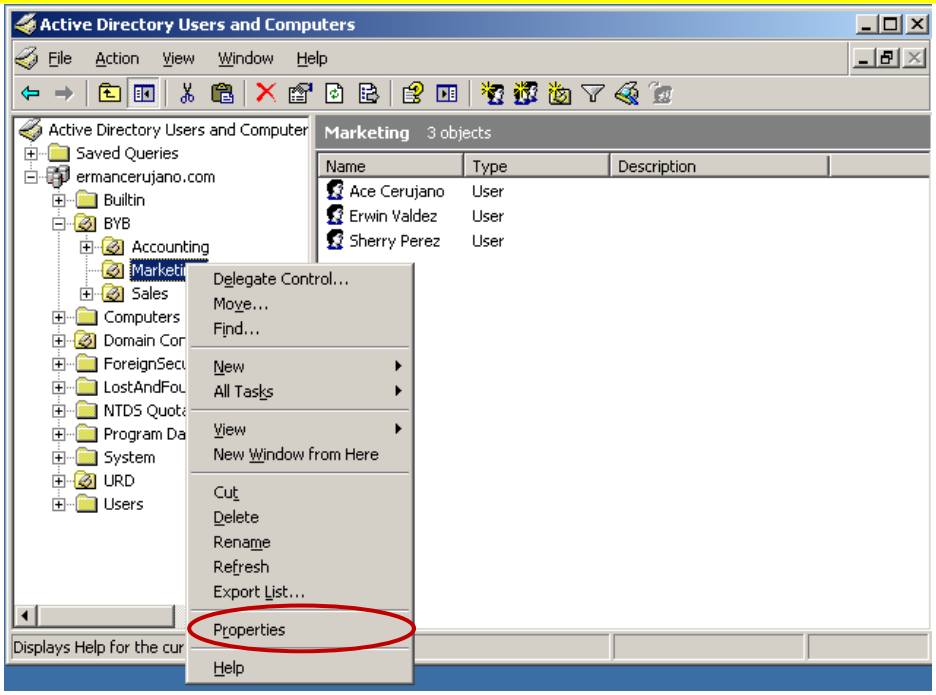
Log on to **Server1** as the domain administrator and open the **Active Directory Users and Computer** console.



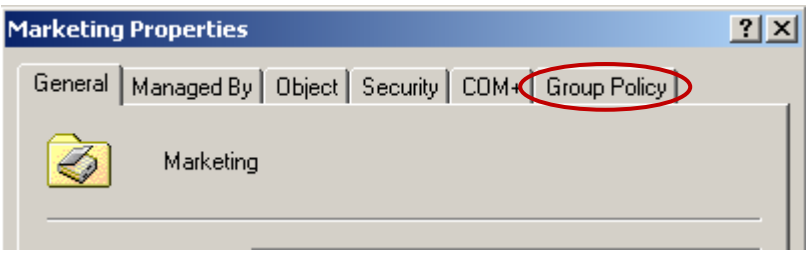
Find the **Marketing** OU located within the **BYB** OU.



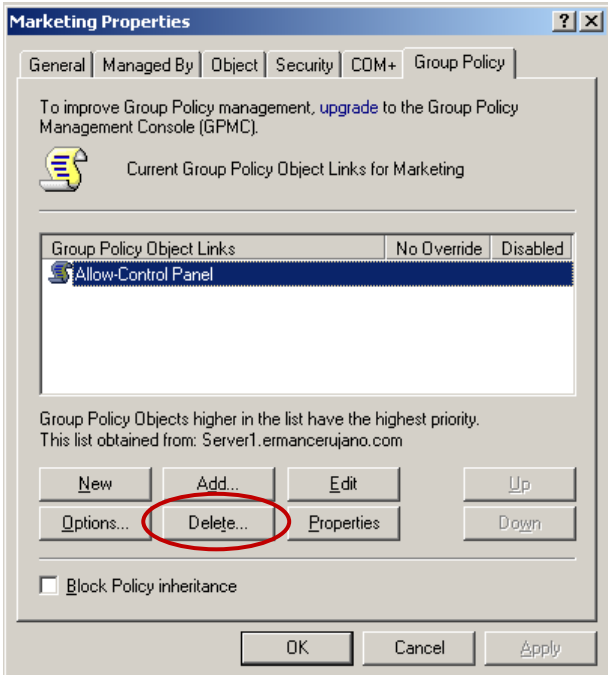
Right click on the **OU**, select **Properties**.



Then select the **Group Policy** tab.



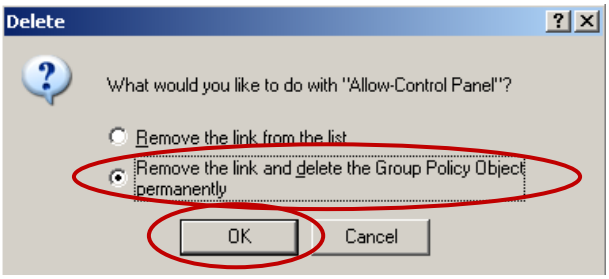
On the group policy tab find and select the **Allow-Control Panel** GPO link then click on **Delete**.



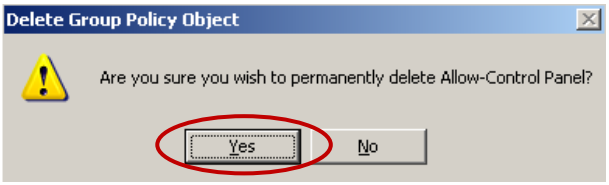
This will bring up a screen asking you whether you want to remove the link from this OU or if you want to remove the link and the GPO permanently.

- **By removing the link**, the GPO will still exist in Active Directory and will still apply to the Urdaneta-Marketing OU. The GPO will still be available to use on other containers on the network.
- **By removing the link and deleting the GPO permanently**, it will no longer apply to the Urdaneta – Marketing OU and it will no longer exist in Active Directory to use again.

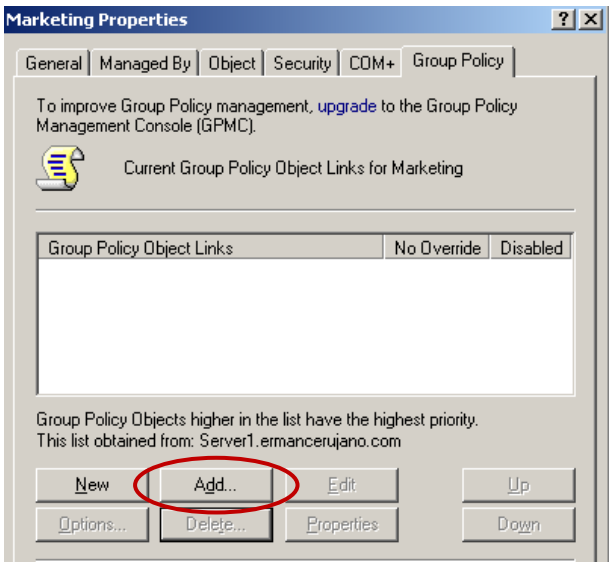
Select **Remove the link and delete the Group Policy Object Permanently** and click **OK**.



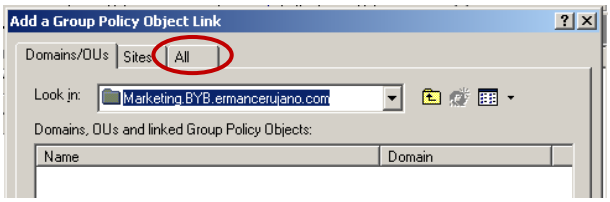
You will then get a warning asking you if you're sure you want to permanently delete the GPO. Click **Yes**.



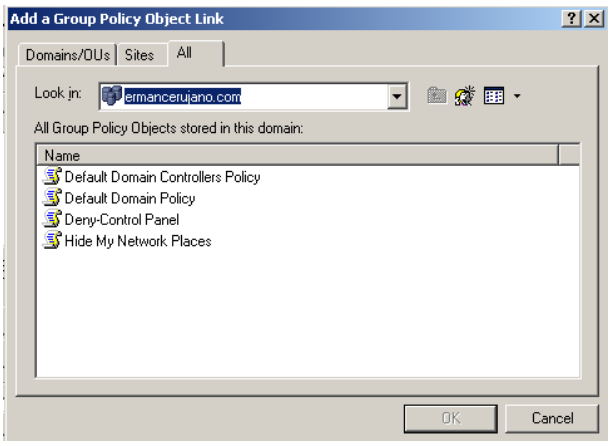
This will bring you back to the Group Policy Tab for the **Marketing OU** in **Bayambang** then click on **Add**.



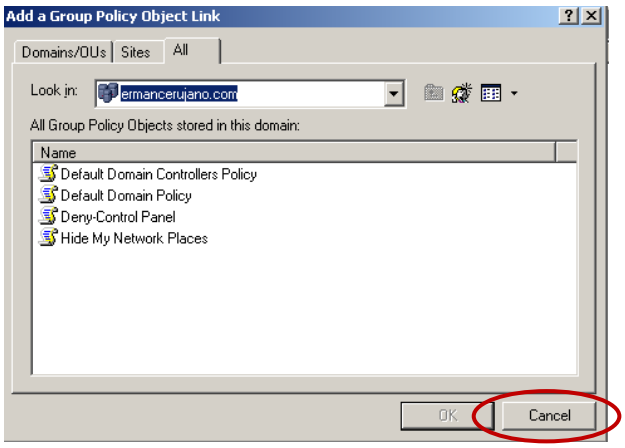
Select the **All** tab on the GPO list.



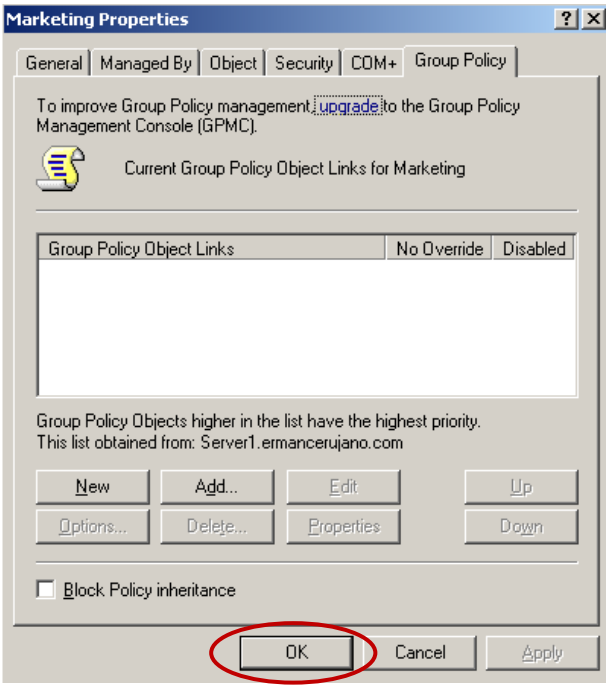
Notice that the **Allow-Control Panel** GPO is no longer on the list of available GPO's for ermancerujano.com



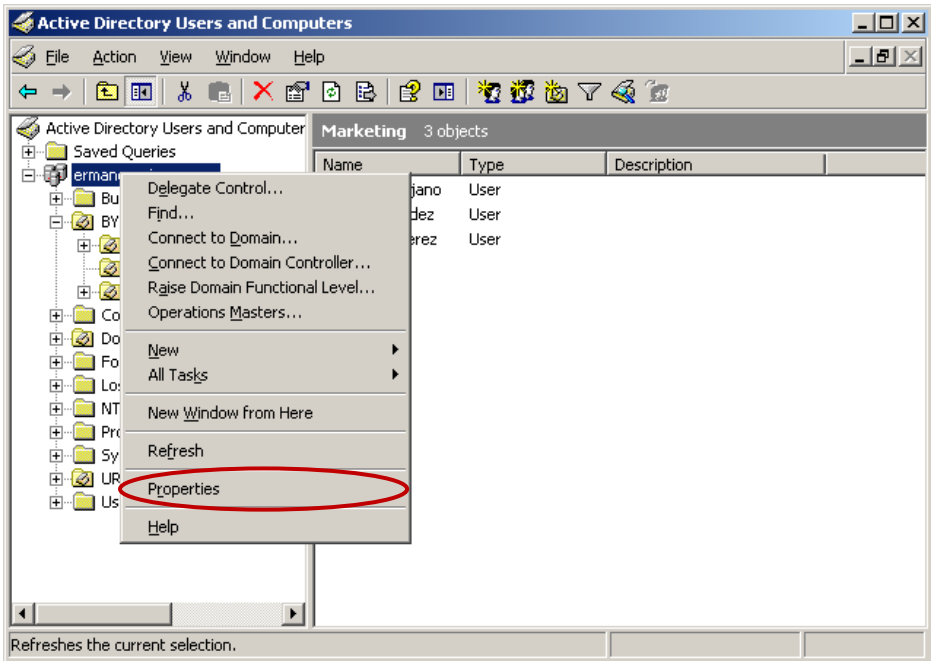
Click on **Cancel**.



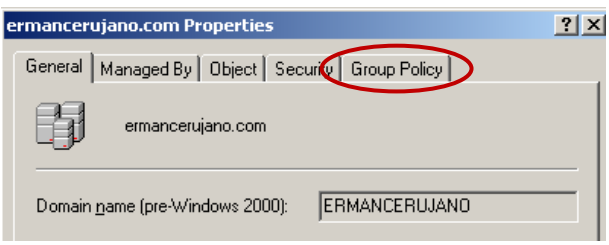
Then click on **OK** to return to the Active Directory Users and Computers console.



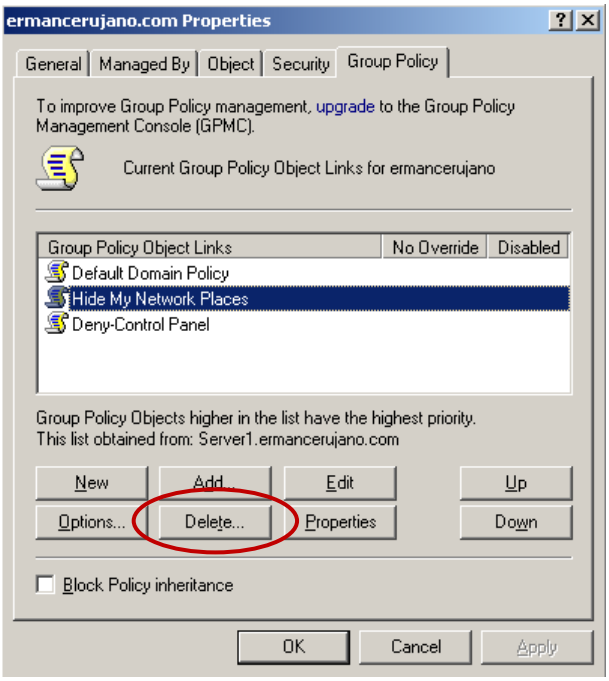
Open the **ermancerujano.com** domain **Properties**.



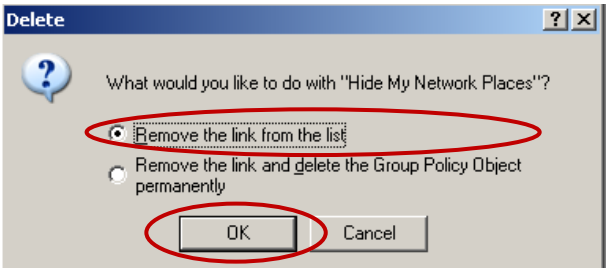
Select the **Group Policy** tab.



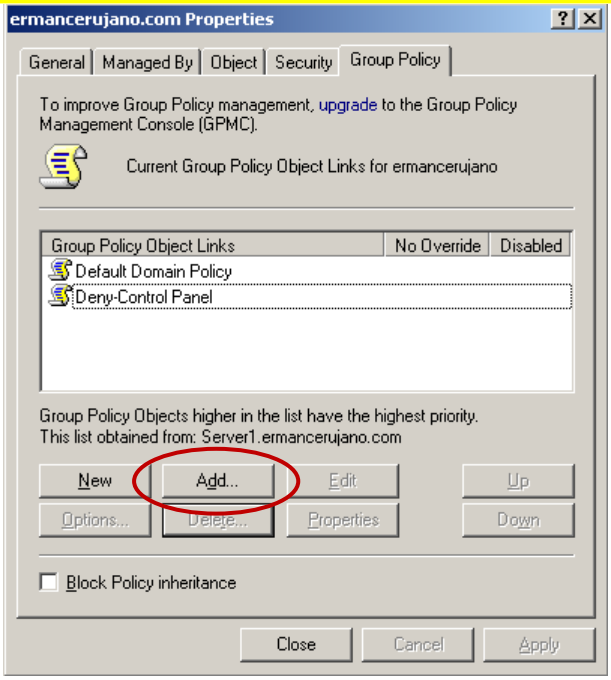
On the group policy tab find and select the **Hide My Network Places** GPO link then click on **Delete**.



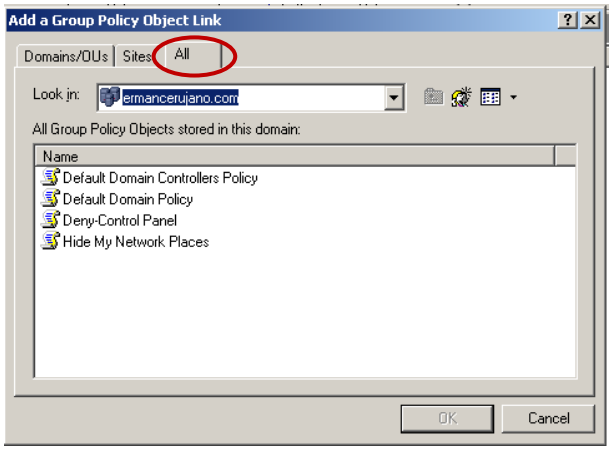
That will bring up a screen asking you whether you want to remove the link from this OU to the GPO or if you want to remove the link and the GPO permanently. Select **Remove this link from the list** and click **OK**.



On the group policy tab for the **ermancerujano.com** domain, you will see that the GPO **Hide My Network Places** no longer appears on the GPO links list. Click on **Add**.



Select **All** tab, on the GPO list.



Here, notice that the **Hide My Network Places** GPO does still appear on the list of available GPO's for ermancerujano.com and can be used in other Active Directory containers for the domain.

LAB 14.4

Administrating Resources

Contents:

SCENARIO PART ONE

Everything seems to be working out pretty good for you at Ermancerujano Corp. All of your major projects are done and you finally have time to kick back and take it easy for once. For your next project, Erman wants you to work on optimizing Active Directory so the users will be able to search through it more efficiently.

In this lab you will create and publish shared folders, printers, and contacts in Active Directory. Then, you will log on to the client computer as regular users to try and access those resources to make sure they are available.

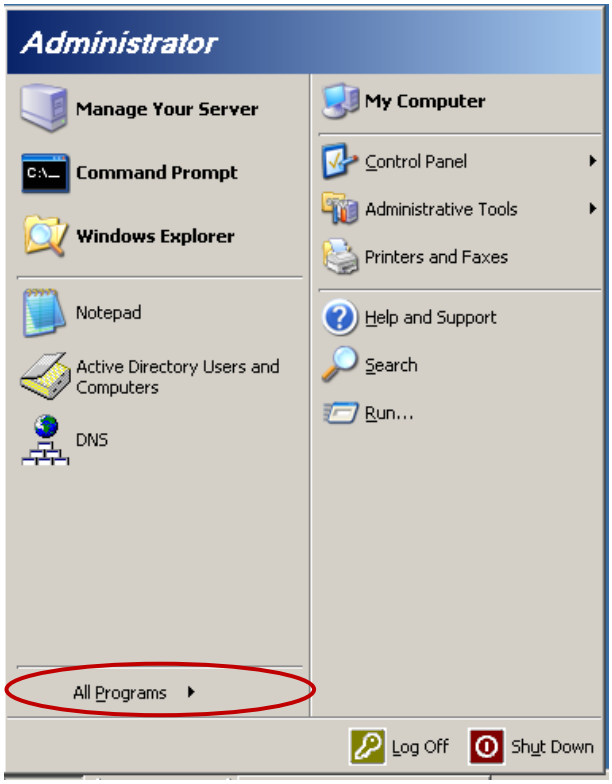
LAB 14.4. ADMINISTRATING RESOURCES.

4.1. Create and Share a Folder

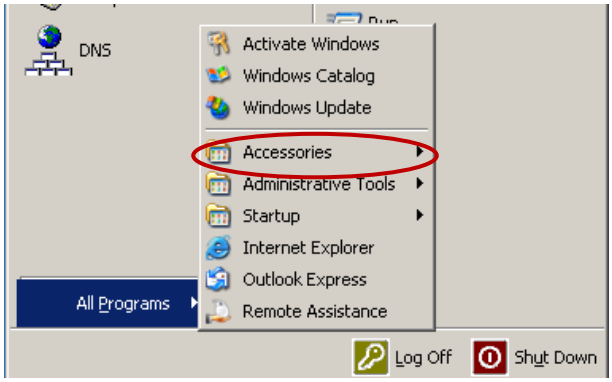
Log on to **Server1** as the domain administrator and open **windows explorer**.

- Go to Start.

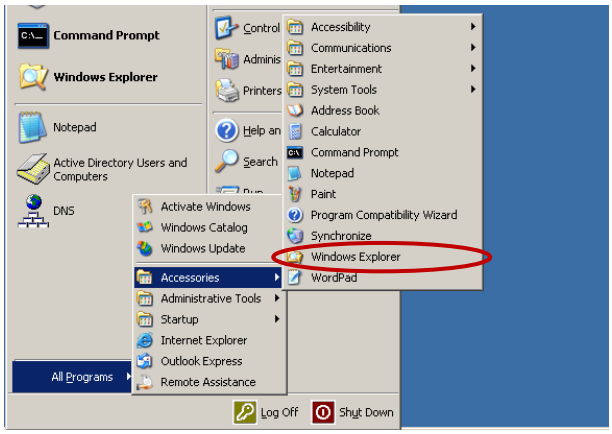
- Select All programs.



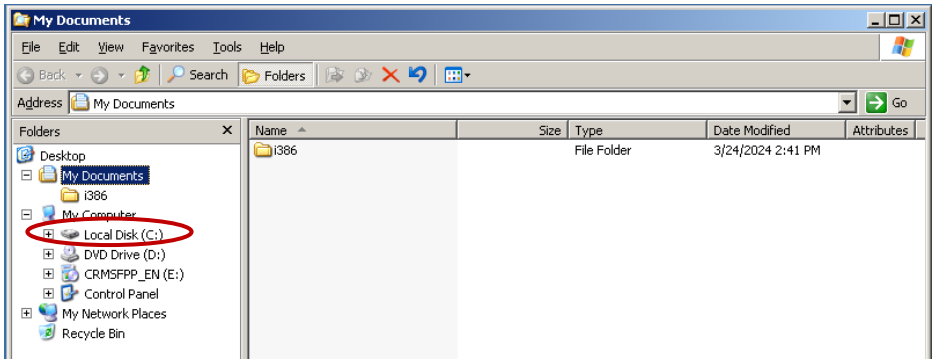
- Accessories.



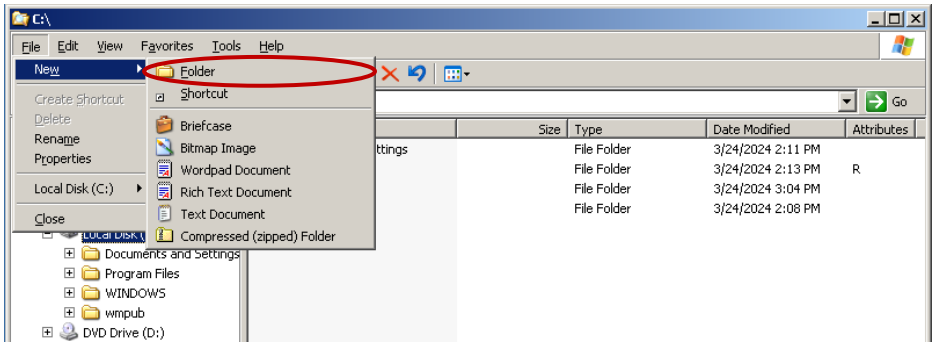
- Windows Explorer.



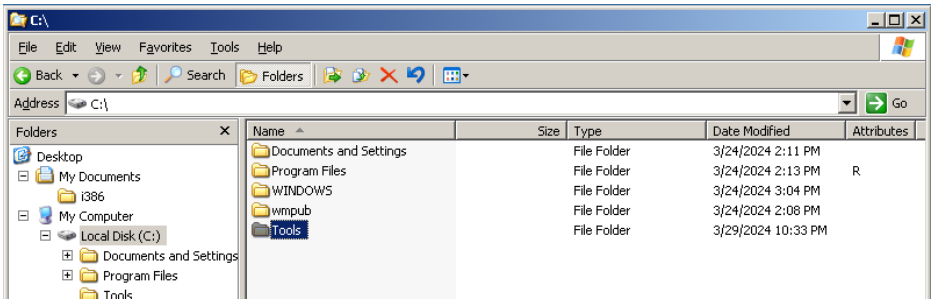
Double click on the **C:** Drive.



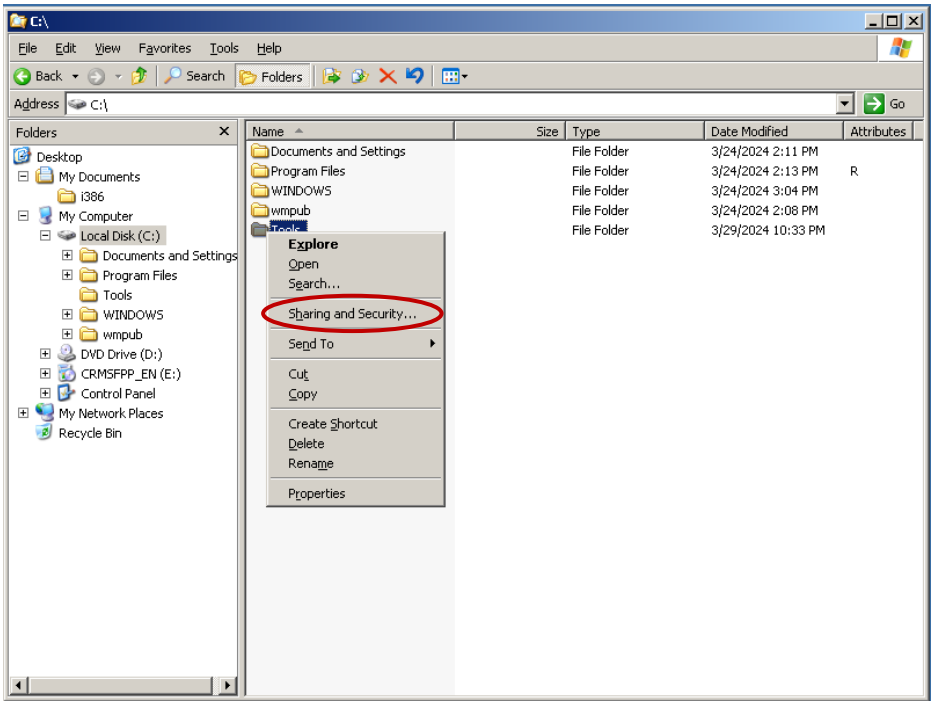
Then from the **File menu** select **New** then folder.



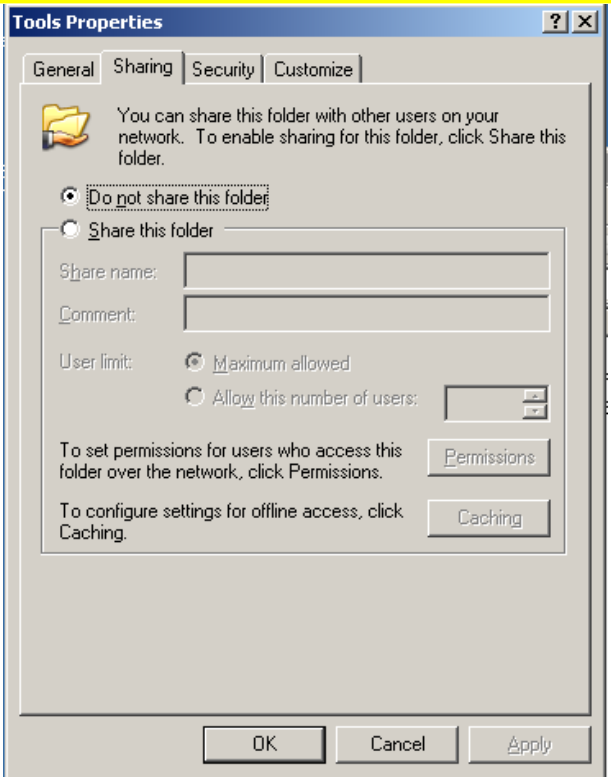
Name the new folder **Tools**.



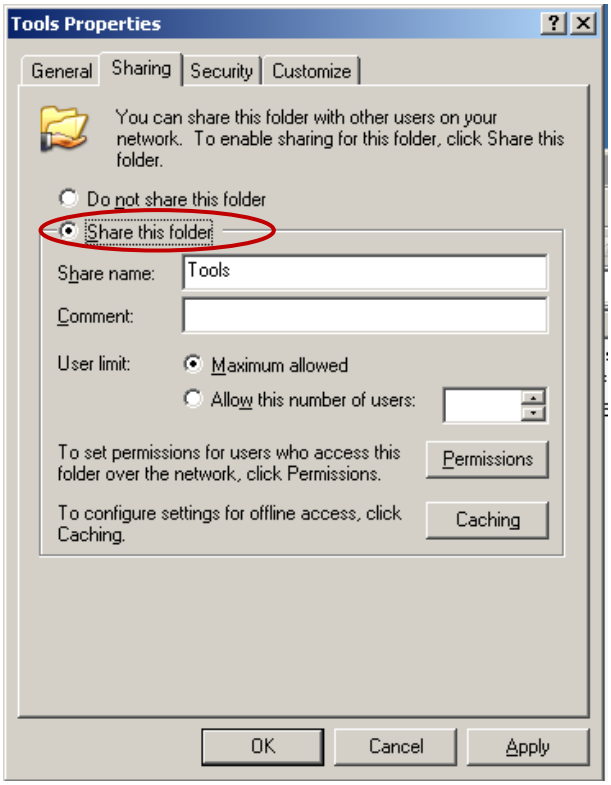
Then right click on the folder and select **Sharing and Security**.



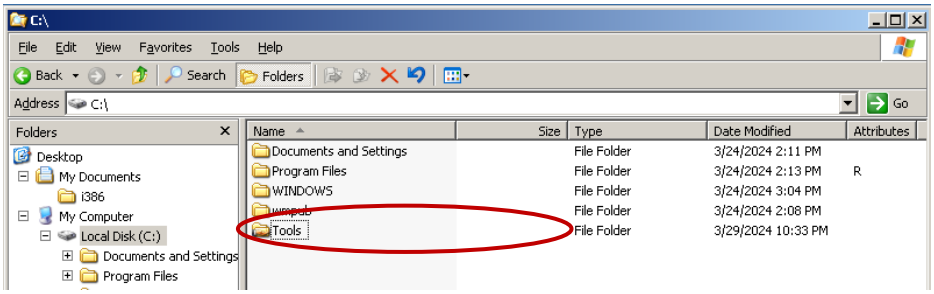
This will open the **Sharing** tab on the properties page of the folder.



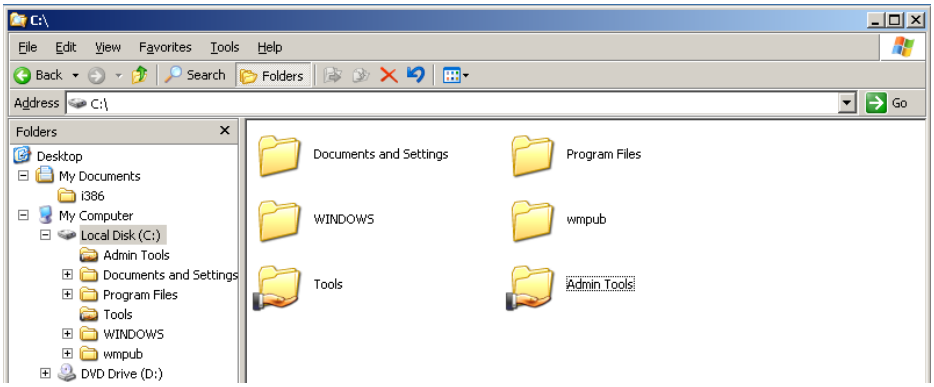
To share the folder, select the **Share this folder** option, leave the default share name **Tools** and click **OK**.



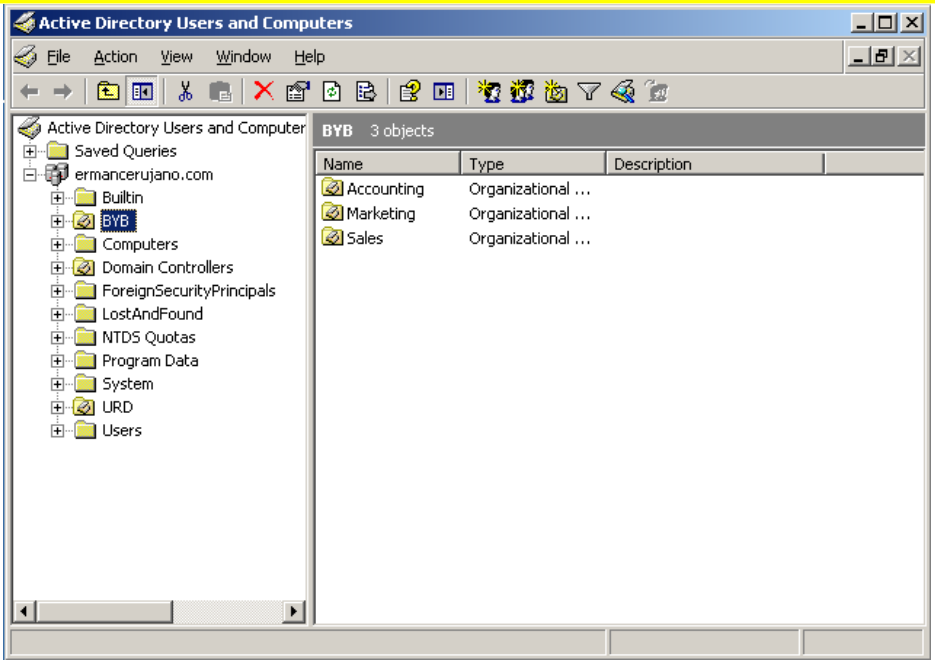
There should now be a hand underneath the folder showing that the folder is being shared.



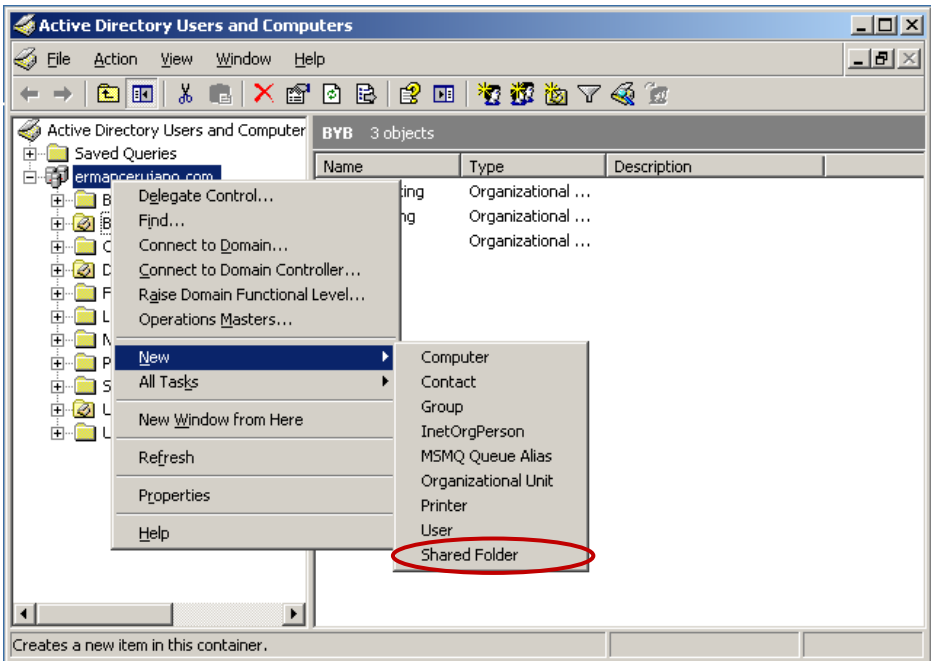
Now create another shared folder and name it **Admin Tools** on the **C:** drive. This folder will be used to store support tools for administrators only and will not be published in Active Directory.



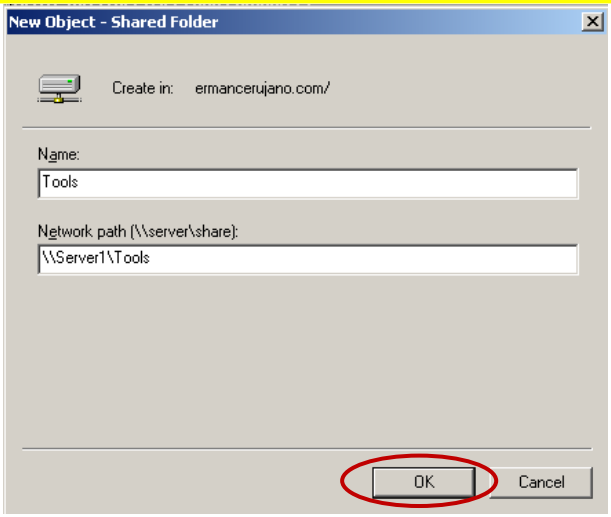
In order for users to search the Active Directory database for this shared folder it will have to be published manually. Shared folders are not published into Active Directory automatically. You can publish a shared folder into Active Directory and place it into any container you want for organizational purposes. When you publish the shared folder all you are doing is creating an object for it in the Active Directory database. Close **Windows Explorer** and open the **Active Directory Users and Computers** Console.



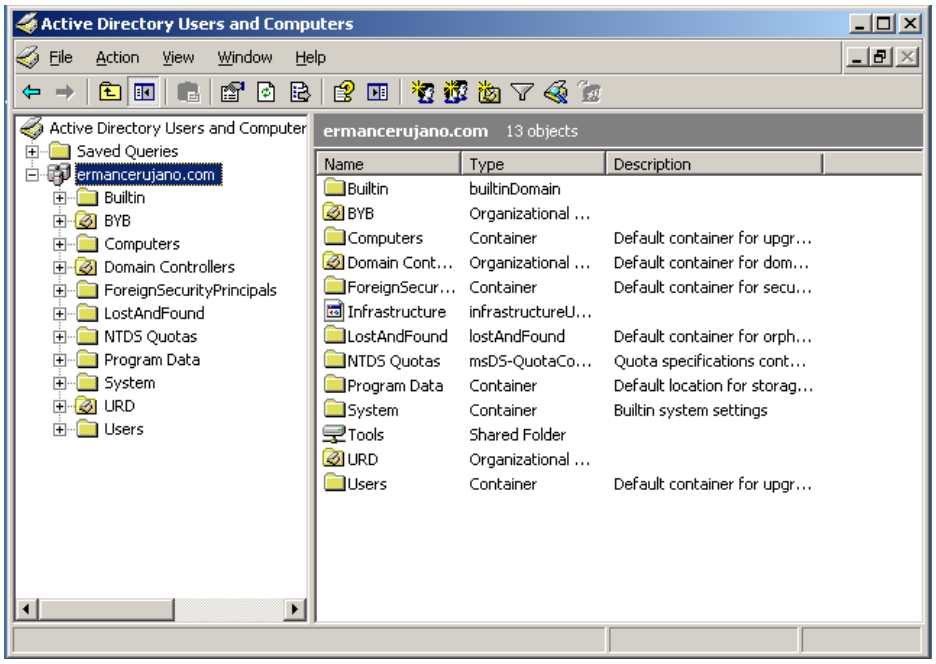
Right click on **ermancerujano.com** domain located in the left pane and select **New** then **Shared Folder**.



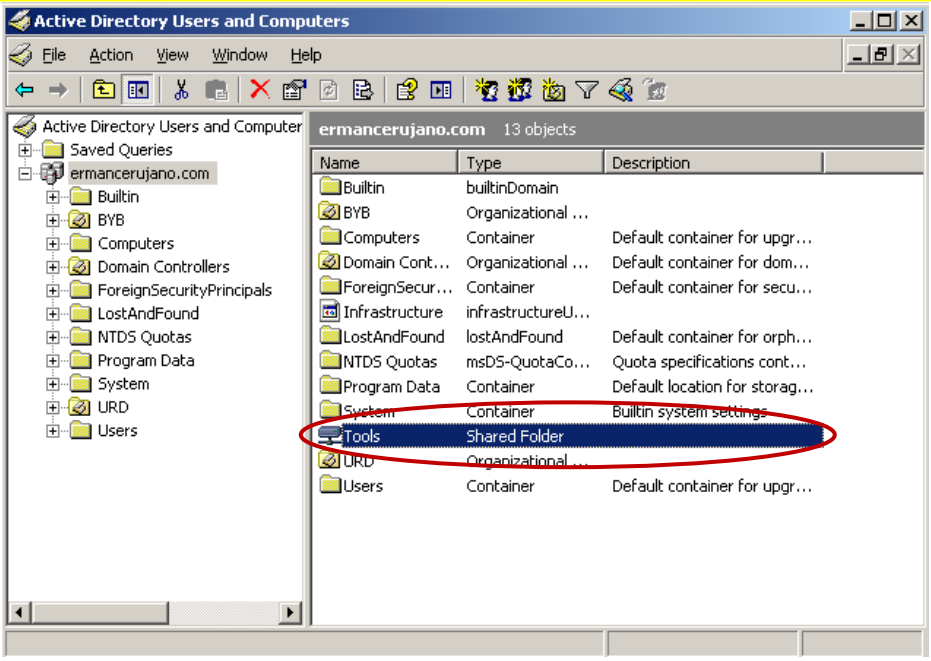
This will bring up a screen when you enter the name and the network path (UNIC) of the new-shared folder. Type in **Tools** for the name of the share and then the network path (UNC) to the shared folder. This is the name of the computer the shared folder resides on, followed by the actual name of the share. Type in **\\Server1\tools** for the network path of the shared folder and click **OK**.



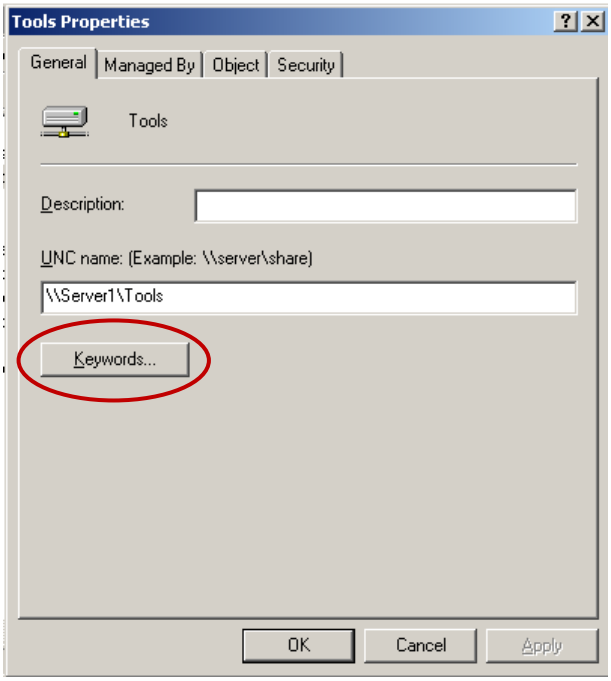
You will now have a shared folder object named **Tools** located in the domain. it can be moved into other containers just like any other object in Active Directory.



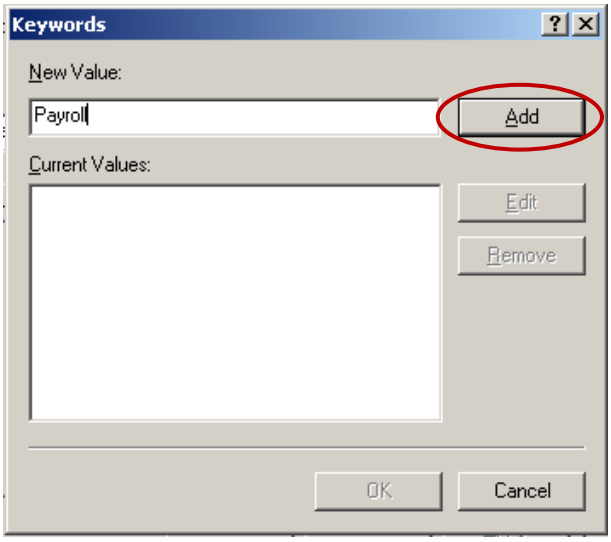
The next thing you need to do is create keywords for the shared folder. This way, users who don't know the exact name or path to the share can use keywords to find it in Active Directory. Open the **Properties** of the **Tools** shared folder in the Active Directory Users and Computers console by doubling clicking on it.



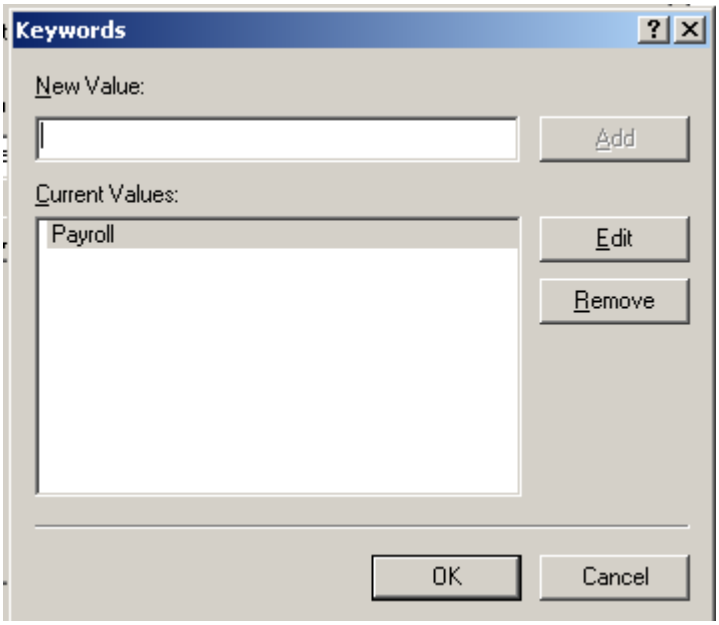
On the **General** tab of the **Properties** page click on the **Keywords** button.



A screen will appear where you can enter the keywords to associate with the shared folder. Employees must have access to this folder because it will contain forms they need to use for benefits, payroll and requesting time off. Therefore you must enter keywords that relate to any of those topics. Type in **Payroll** and click **Add**.

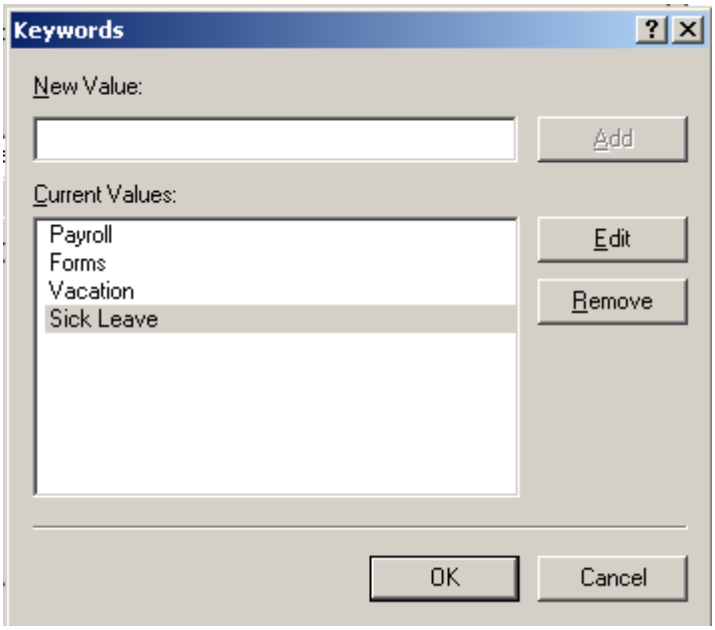


That keyword is now associated with the shared folder in Active Directory.

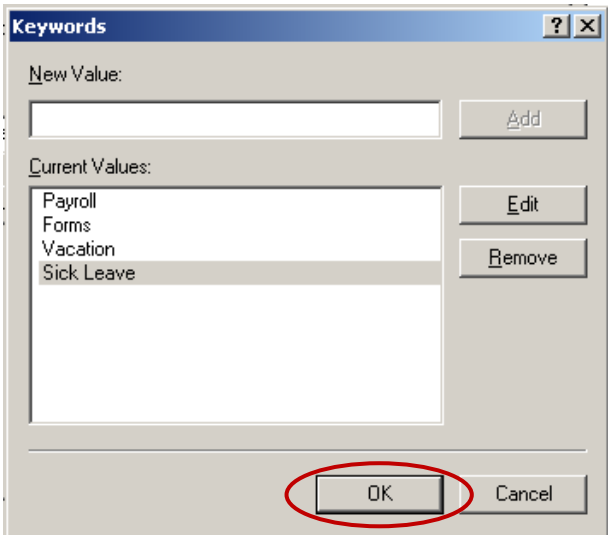


Now add the following keywords and any other words you feel may be associated with this folder.

Keywords: Payroll, Forms, Vacation, and Sick Leave.



Click **OK** when you are done.



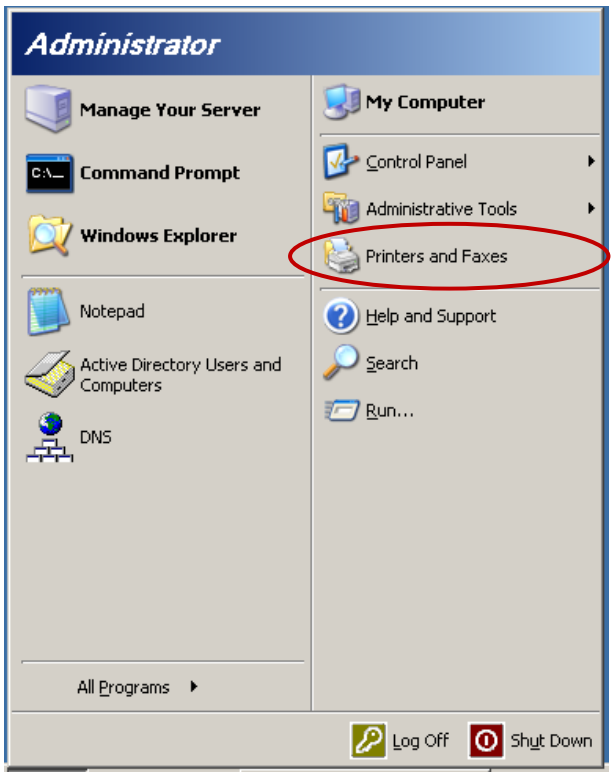
4.2. Add, Share, and Publish a Network Printer.

In order to add a printer to the network you must first install the printer locally on the server and then share the printer similar to the way you would share a folder.

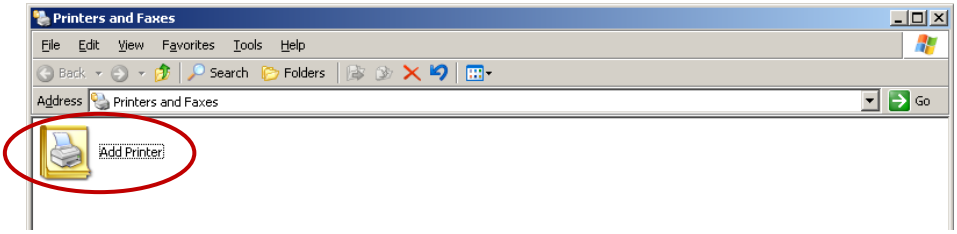
Add a printer to the server, **Server1**.

- Go to start.

- Printers and Faxes.

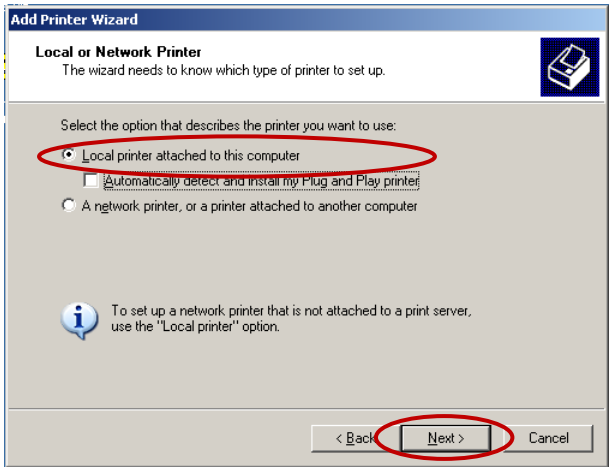


- Double click on the **Add Printer** icon to start the Add Printer Wizard.

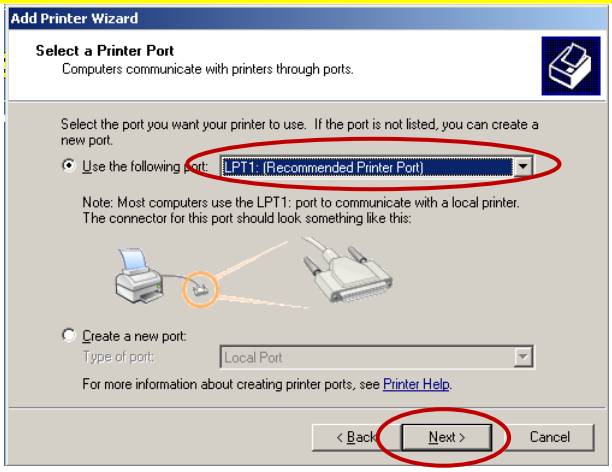


The first screen on the wizard is just a welcome screen, click on **Next**.

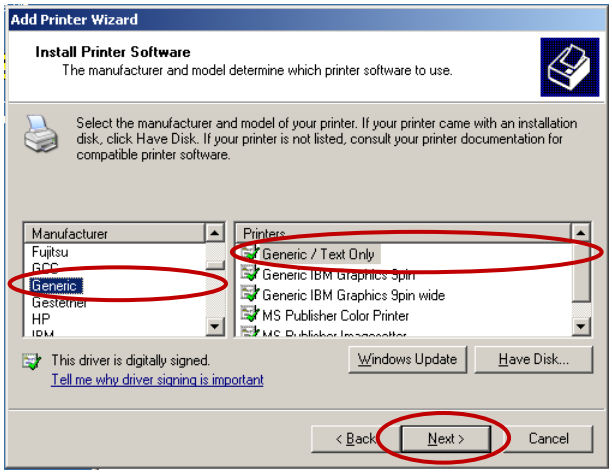
The next screen will ask you where the printer is attached. You can select the local printer option if the printer is directly attached to the computer or the network printer option if you are trying to add a printer that is already on the network. Select **Local Printer** and uncheck the box underneath that says **Automatically Detect and Install my Plug and Play Printer** because you are not installing an actual printer. By leaving the box checked, the wizard would try to find and install the printer, but you will get an error stating that the printer can't be found. Click **Next**.



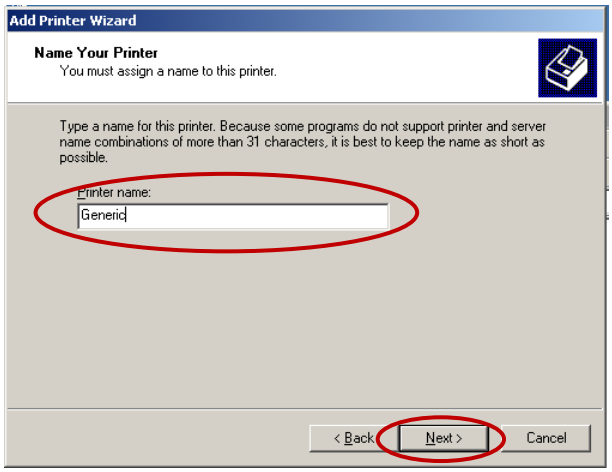
Now the wizard will ask you to choose a port the printer will use. Select the **LPT1 Printer Port** and click **Next**.



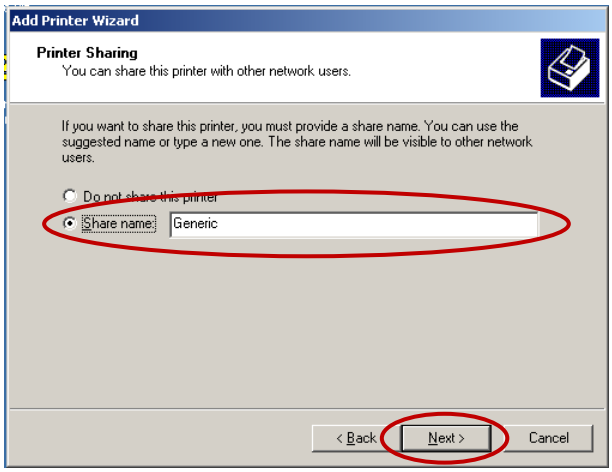
The next screen will ask you to specify the **Manufacturer and Model** of the printer. This will install the drivers necessary for the printer to work on the Windows 2000 operating system. Select the manufacturer **Generic** and the model **Generic/Text Only**. Click **Next.**



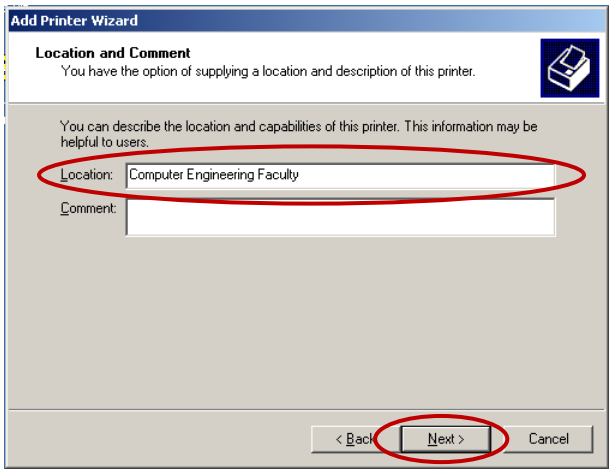
The next screen will ask you to assign a name to the printer and to specify if you want this to be your default printer for Windows-based programs. Type in **Generic** as the **Printer name** and select **Yes** to make this the **default Windows Printer**.



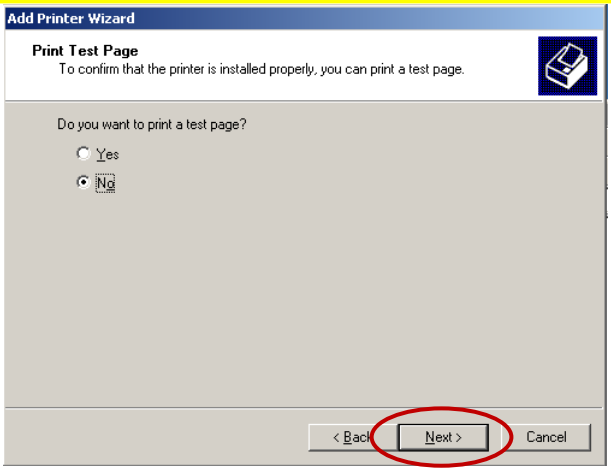
The following screen will ask you to specify whether you want to share this printer or not. Select **Share name:** to share this printer and leave the default name of **Generic** as the share name.



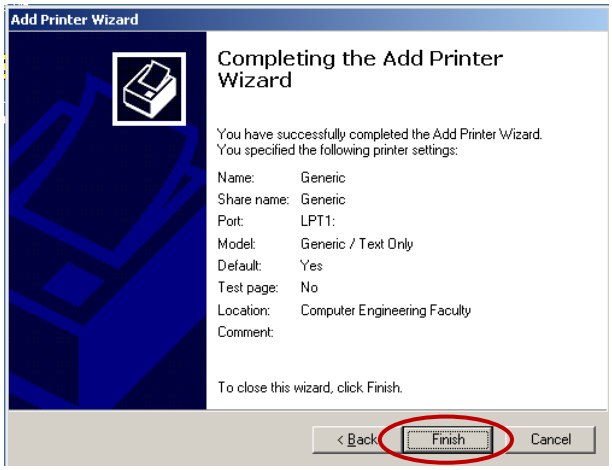
The next screen of the wizard allows you to place information about where the printer is located and any other comments you may want to add to this printer. This is optional and can be left blank, but it is a good idea to at least give it a location if you ever need to know where it's located in a big building. For the location type in: **Computer Engineering Faculty** and you can leave the Comment section blank or enter any comment you want. Then click **Next**.



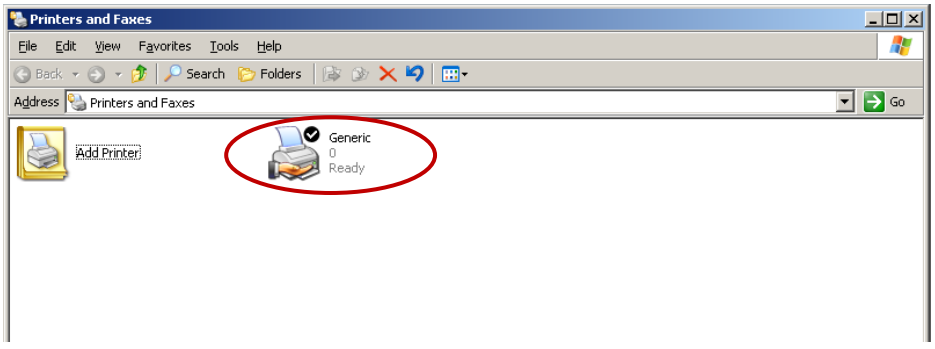
The next screen will ask you if you would to print out a test page to confirm that the printer is working. Select **No**, because there is no actual printer to print out to, but it is a good idea to print out a test page if you are installing an actual printer. Click **Next**.



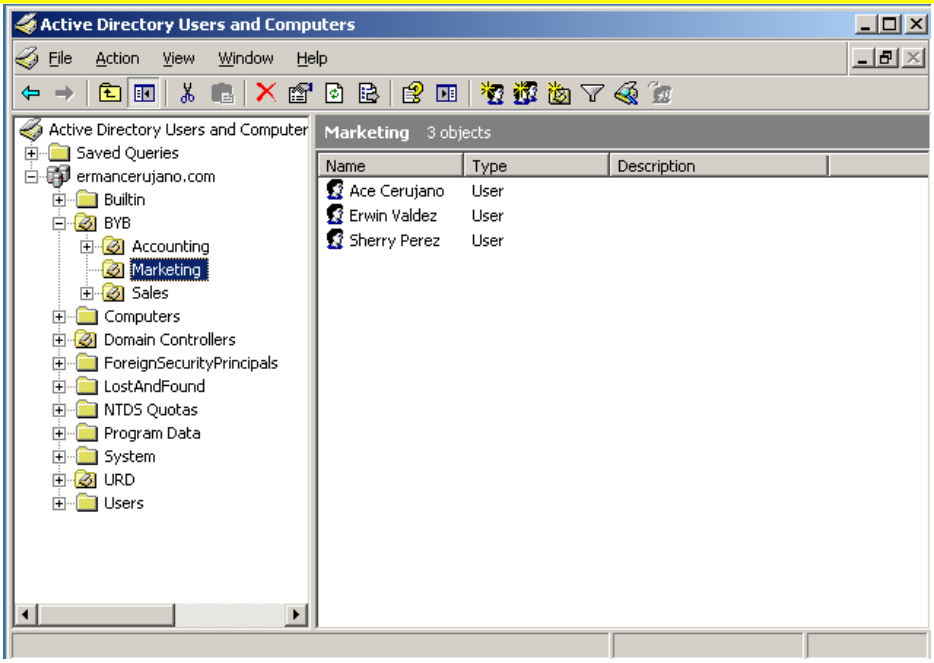
The final screen will just be a summary of all information you entered into the add printer wizard. Confirm that all the information is correct and click on **Finish**.



You should now have a printer icon appear in the printers folder named **Generic** and a hand underneath it including that the printer is being shared.

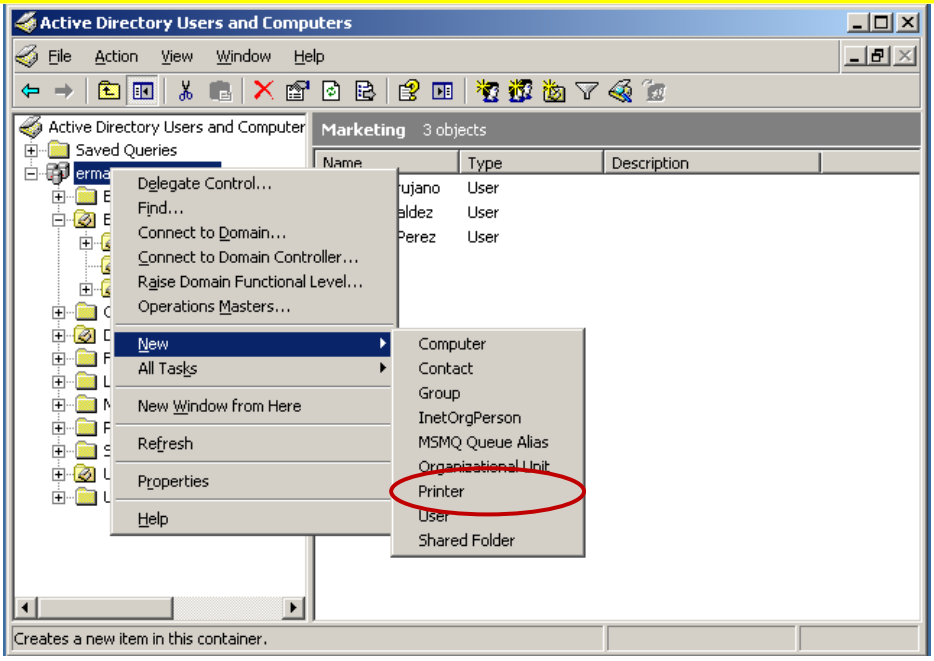


Printers are published in Active Directory automatically. The only time a printer will need to be published is if the printer is installed on a pre-Windows 2000 computer. Try to publish that printer anyway to see if it will work. Open the **Active Directory Users and Computers** console.

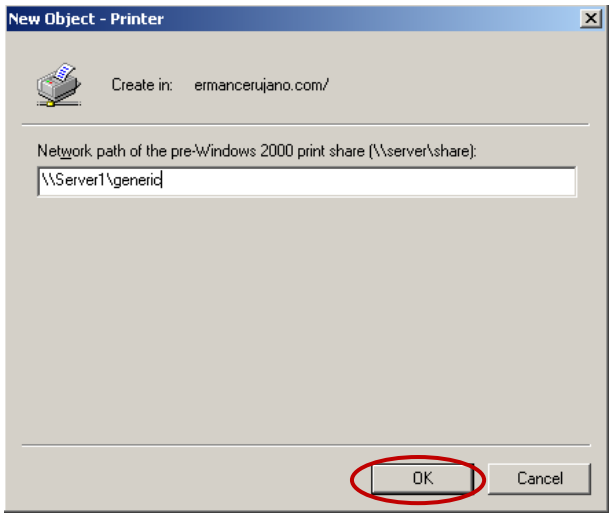


Right click on the **ermancerujano.com** domain.

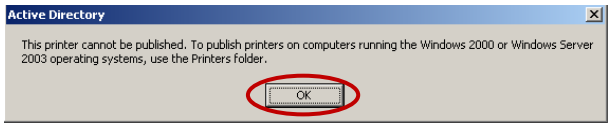
Select **New** then **Printer**.



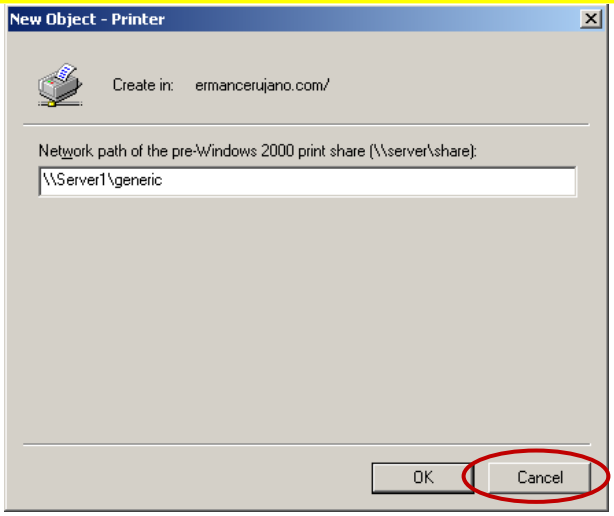
This will bring up a screen where you enter the network path of the shared printer. Type in the path to the generic printer on **Server1** (\\Server1\generic) anyway and click **OK**.



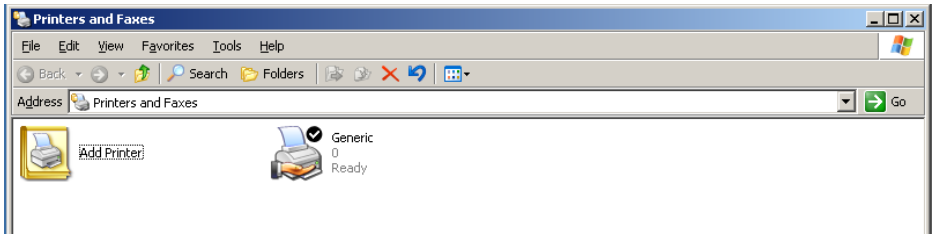
You will get an error telling you that the printer cannot be published and to use the printer folder to publish printers on Windows 2000 or Windows Server 2003 Operating Systems. Click **OK** on the error message.



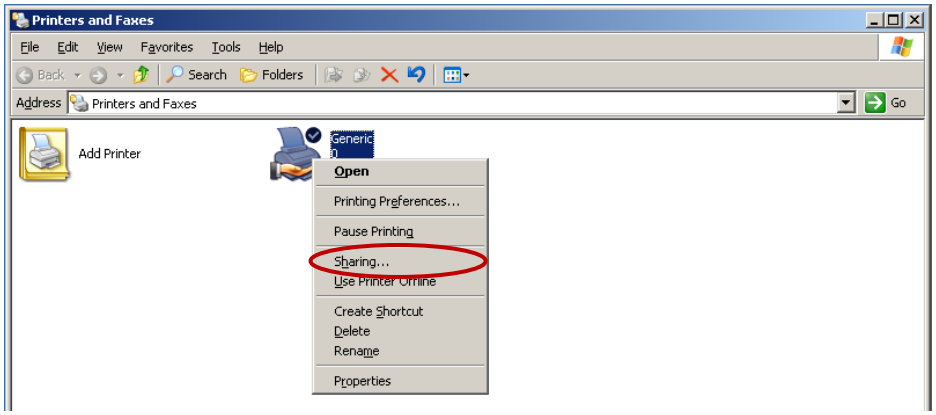
Then **Cancel** on the new printer object screen.



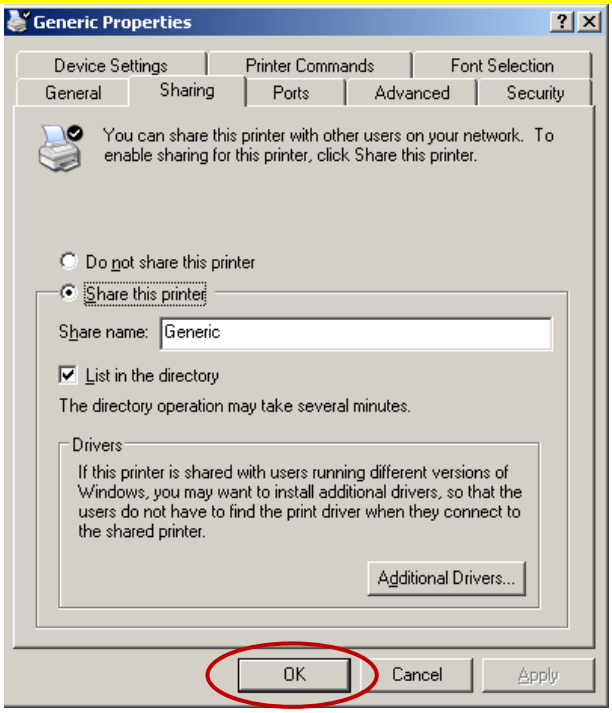
Close the **Active Directory Users and Computers** console and open the **Printers folder**.



Right click on **Generic** printer icon and select **Sharing**.



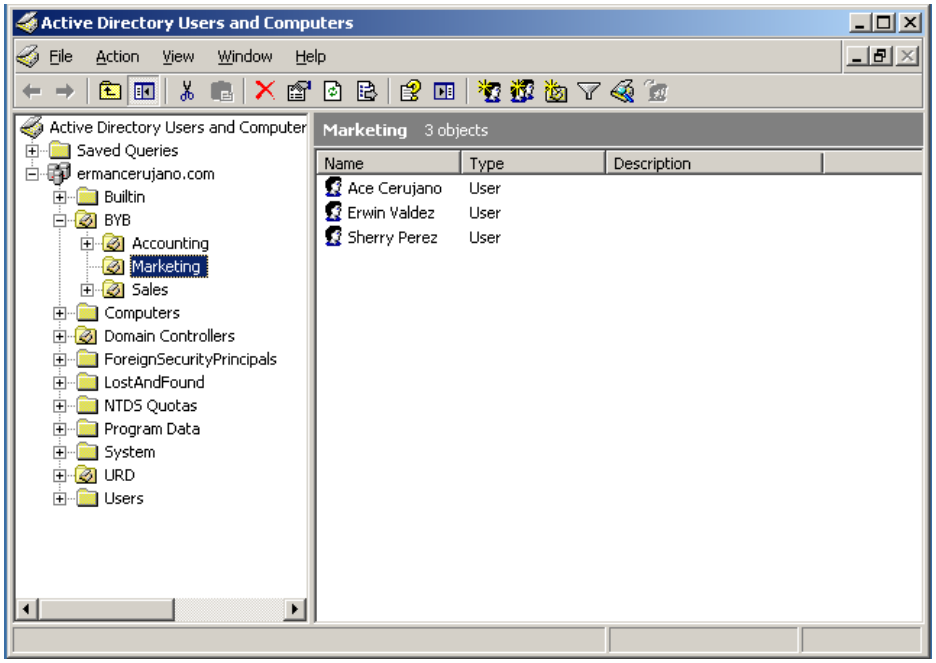
This will open to the **Sharing** tab on the **Properties** of the printer. Here you can un-share or share the printer if you did not share it in the wizard and add any additional drivers that may be needed. Remember that printers are automatically published in Active Directory when they are installed on a Windows 2000 or Windows Server 2003 computer. If you need to remove the printer from Active Directory all you must do is uncheck the box that says **List in Directory** and vice versa if you need to add it back to the Active Directory. Leave the printer published in Active Directory, click **OK** and close the **printers folder**.


Generic Properties
Device Settings
Printer Commands
Font Selection
General
Sharing
Ports
Advanced
Security
You can share this printer with other users on your network. To enable sharing for this printer, click Share this printer.
Do not share this printer
Share this printer
Share name:
Generic
List in the directory
The directory operation may take several minutes.
Drivers
If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.
Additional Drivers...
OK
Cancel
Apply

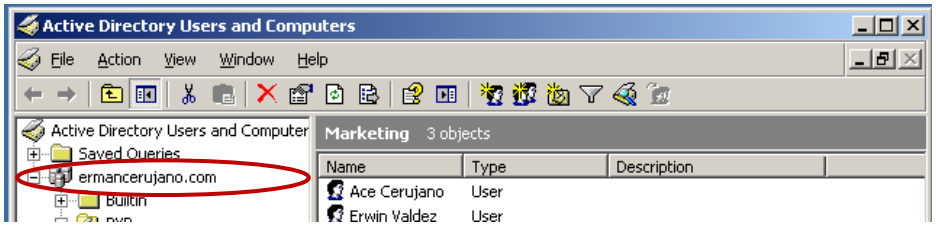
4.3. Create a Contact in Active Directory.

A contact may be created in Active Directory to list information for someone without having to create an actual user account. Contacts are used to store information for people that are outside of your company. For example, business partners, vendors, and possibly customers. Contacts are most useful if you are running Microsoft's Exchange Server (Microsoft's Mail Server Product) because they allow you to integrate your mailing lists with your Active Directory structure.

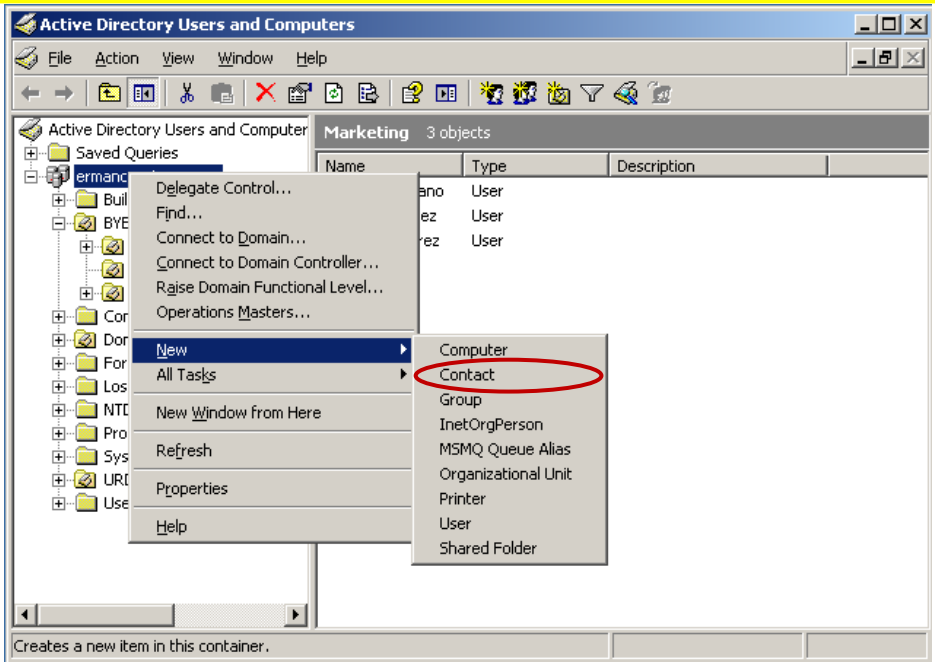
Open the **Active Directory Users and Computer** console.



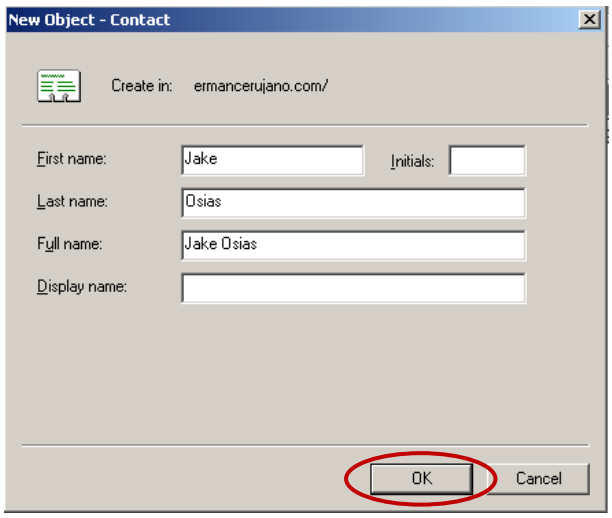
Right click on the **ermancerujano.com** domain.



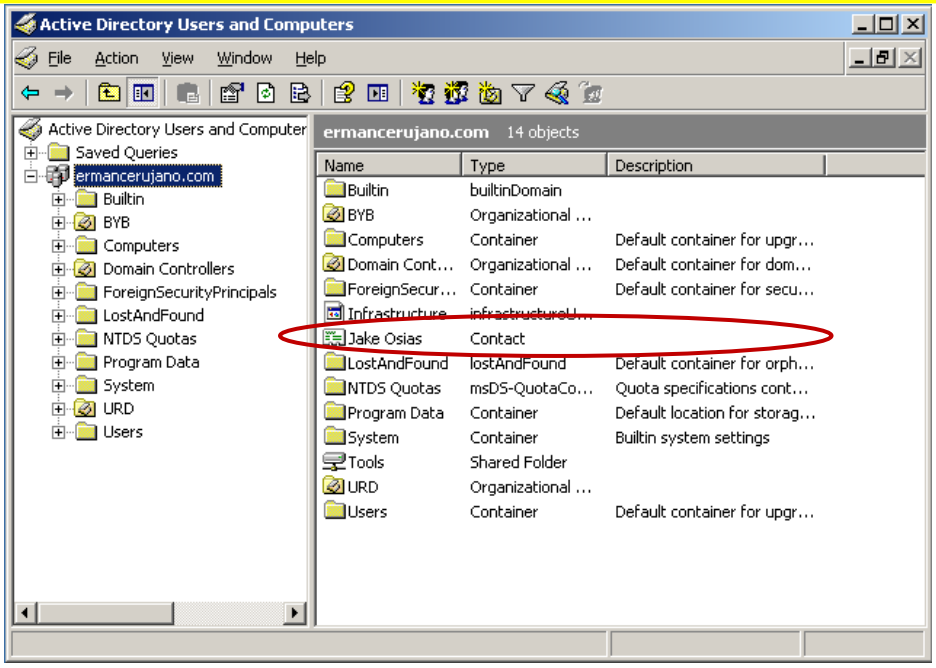
Select **New** then **Contact**.



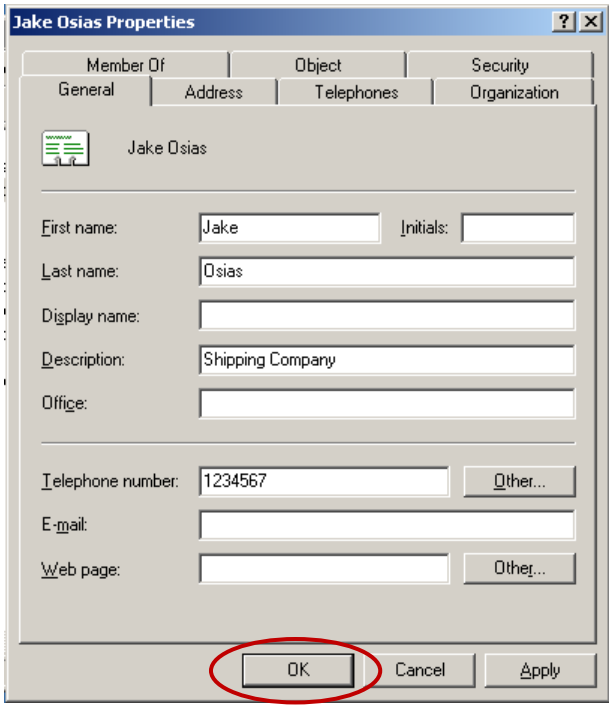
This will bring up a screen for you to enter the new contact name. type in **Jake** for the first name, **Osias** for the last name and the full name should appear as **Jake Osias**. Click **OK** when finished.



Now double click on the contact **Jake Osias** in the right pane to open the **Properties**.



On the properties of the contact you can add more detailed information like telephone numbers, email addresses, etc. Type in **Shipping Company** for the **Description** of this contact and enter any seven-digit telephone number in the **Telephone Number** field. You can view the other tabs to see what additional information you can add about this contact. Now users on the ermancerujano.com domain can do a search within Active Directory to find the information they need for this contact. Click **OK** when finished and close the Active Directory Users and Computer console.

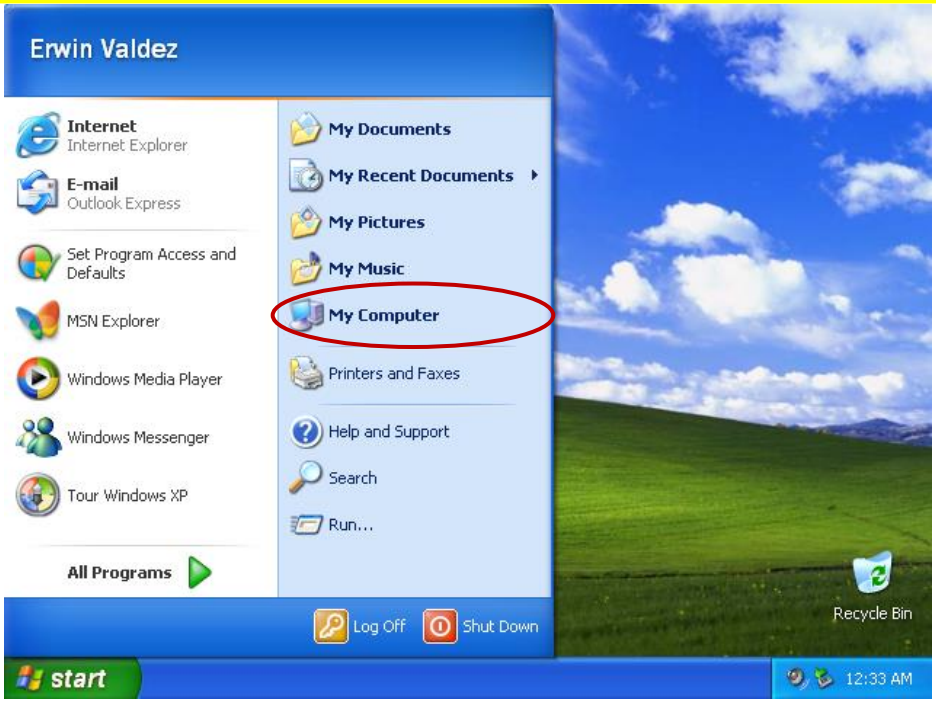


4.4. Perform Active Directory Searched for Published Resources: Shared Folder-Scenario.

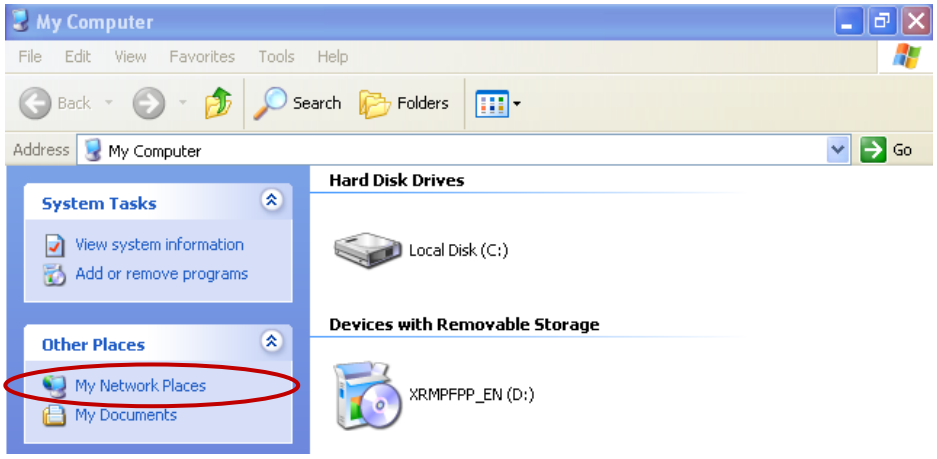
Erwin Valdez needs to fill out a form requesting vacation time. They told her where the forms were located on the network the first day she started but now almost a year has gone by and he can't remember where it is. He does know how to search the Active Directory for resources though. Maybe he can find it by doing a search with the keyboard vacation.

Log on to **client1** as the user **Erwin Valdez (evaldez)**.

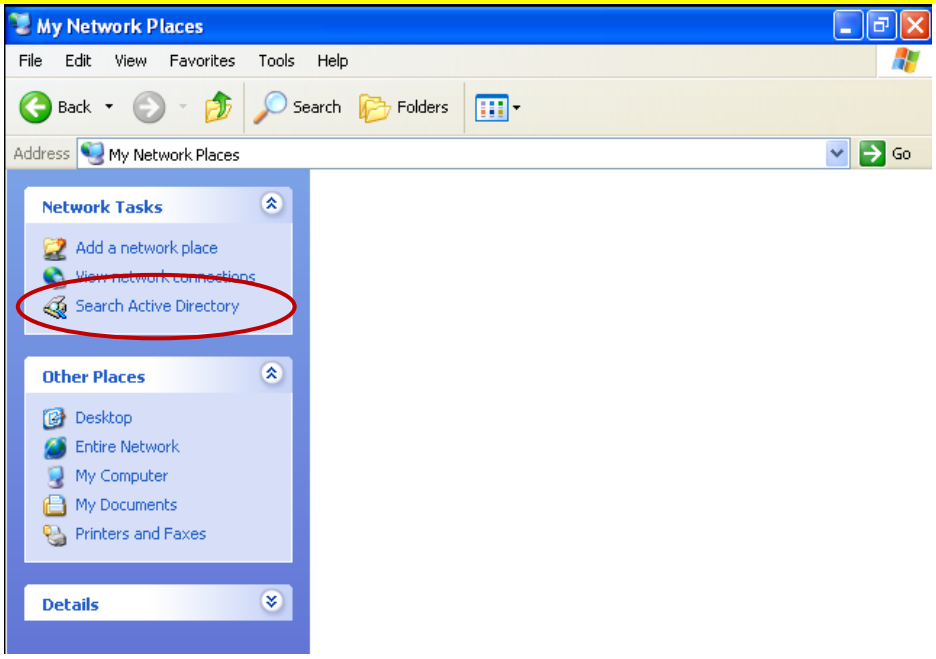
Click **My Computer**.



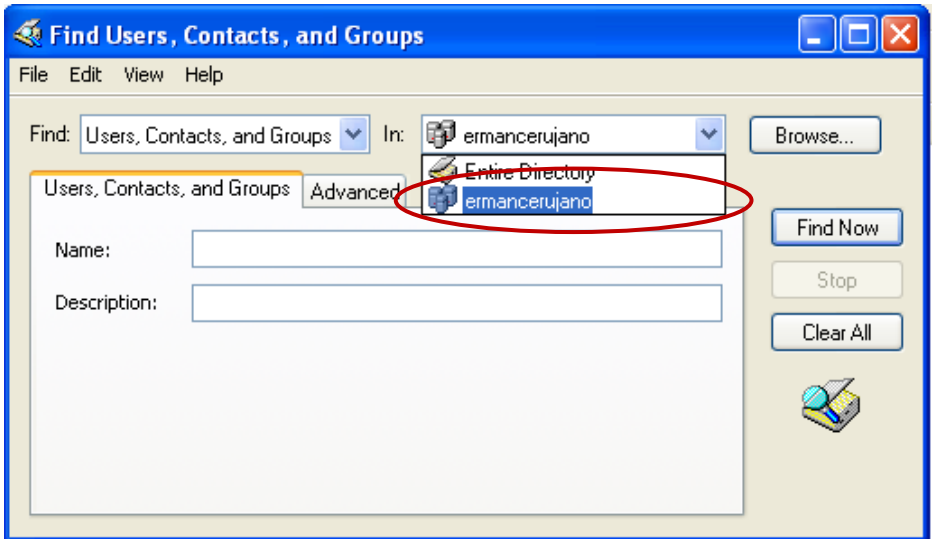
Select **"My Network Places"**



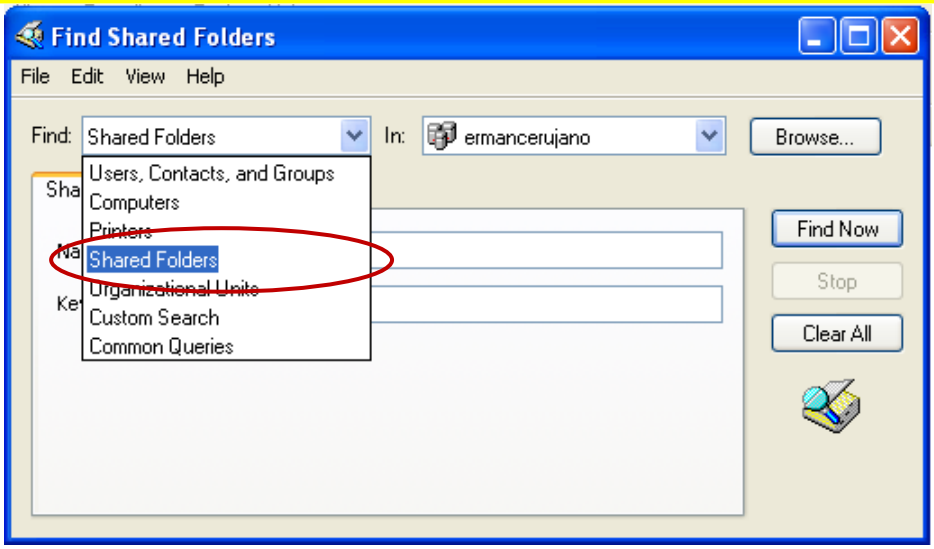
In the My Network Places folder click **Search Active Directory** on the left column.



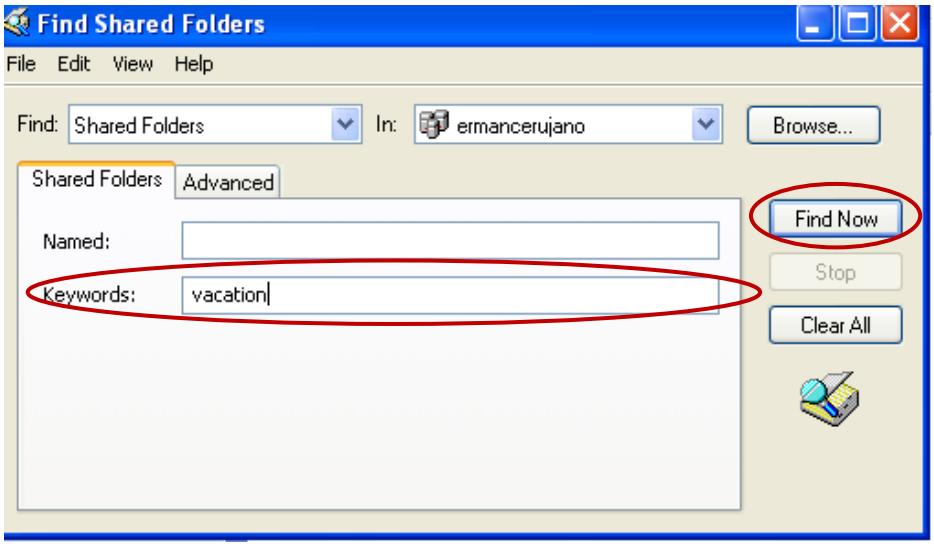
Then select search in **ermancerujano.com** from the pull down.



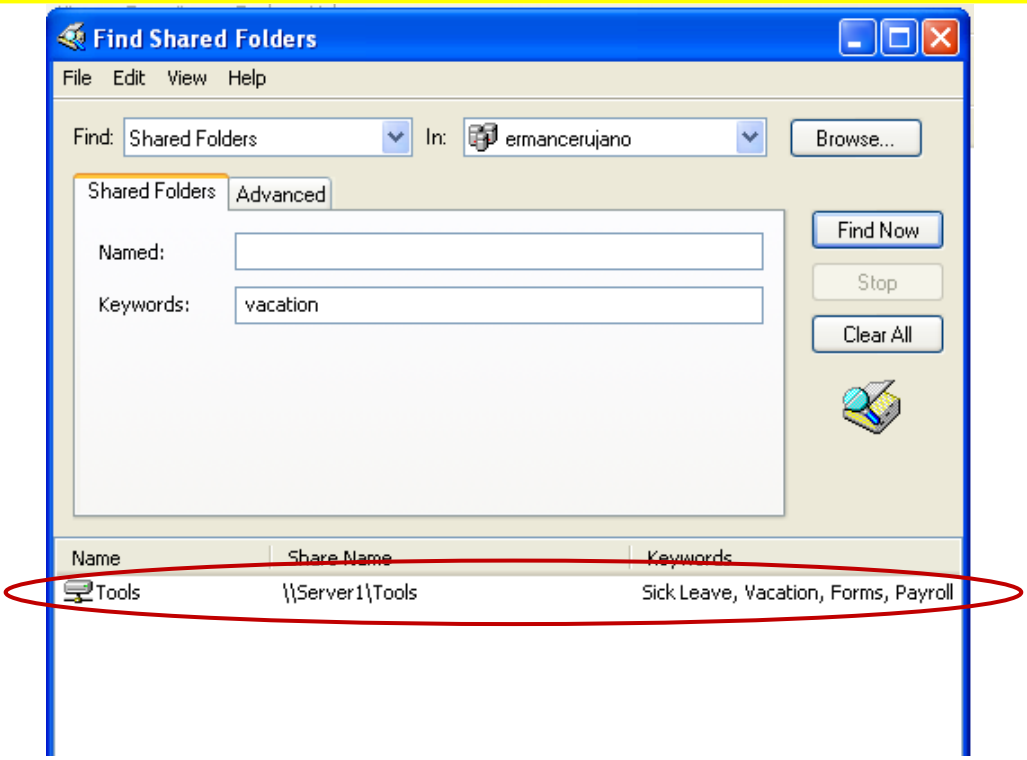
Click on the **Find** drop down menu and select **Shared Folders**.



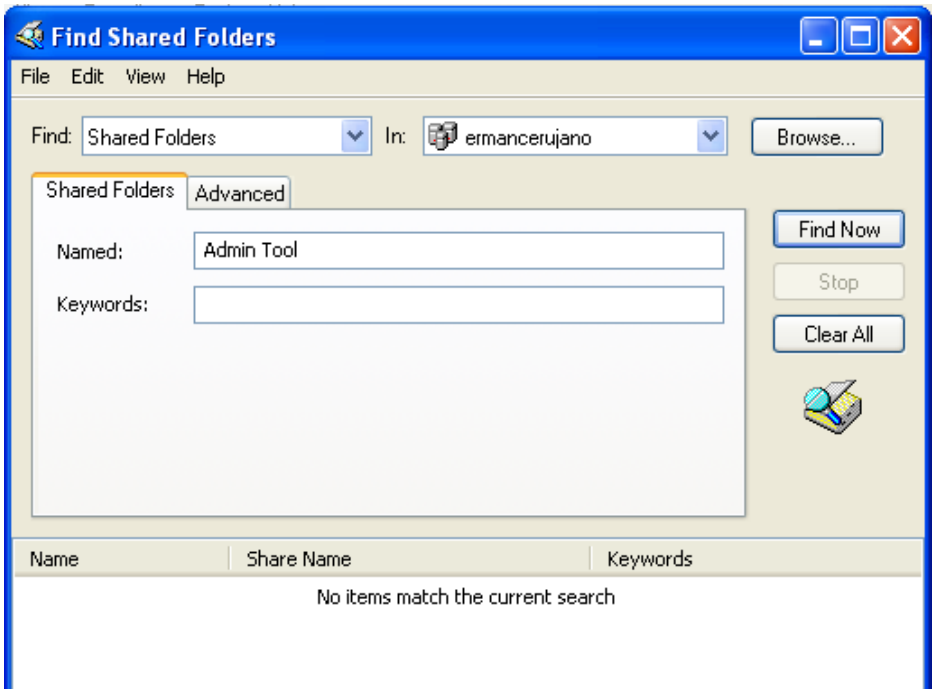
This will give you option of searching by name or by keyword for the shared folder. Type in the keyword **vacation** and click on the **Find Now** button.



This should list all of the shared folders that have the keyword vacation associated with them. In this case there is only one, which is the folder that contains the necessary forms. This folder can be opened by double clicking on the share.



Now try to do a search for the **Admin Tool** folder. Even though the share does exist on the network it will not be found in Active Directory because it was not published.



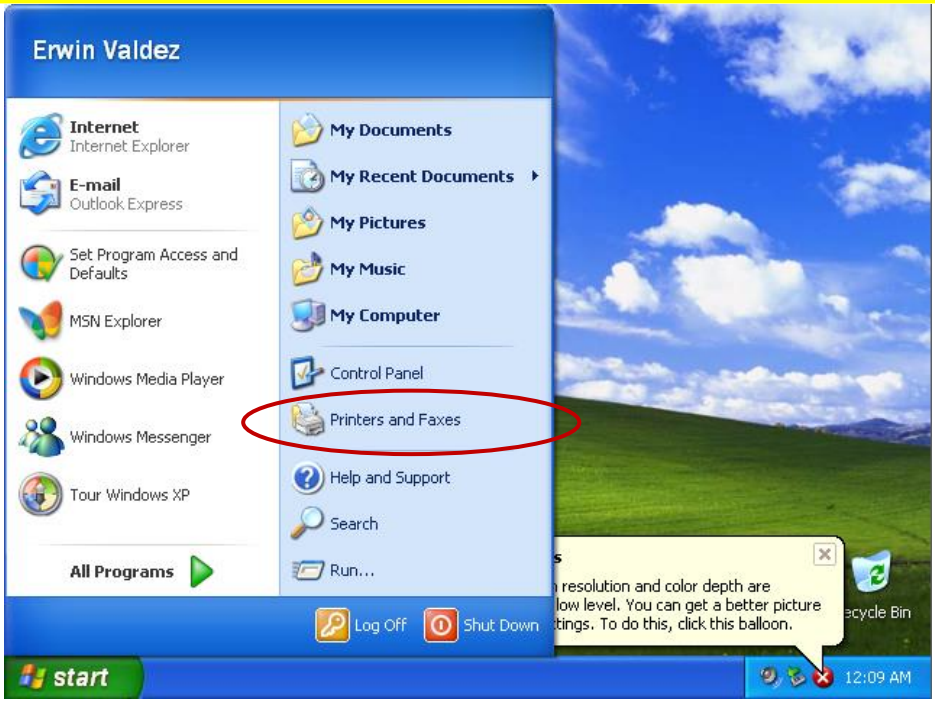
Now close all windows and **log off** the user **Erwin Ferrer**.

4.5. Perform Active Directory Searched for Published Resources: Shared Printer-Scenario

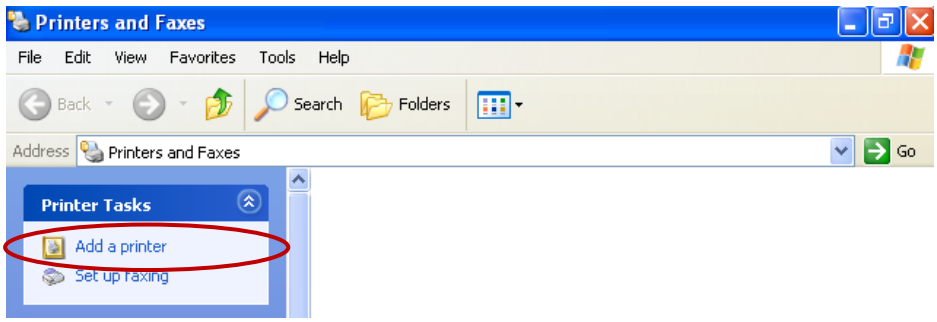
Erwin Valdez needs to connect to the new printer that was installed right behind his cubicle. Unfortunately, he doesn't know what the printer share name is. He is going to try to add it to his computer anyway.

Log on to **client1** as the user **Erwin Valdez** (**evaldez**).

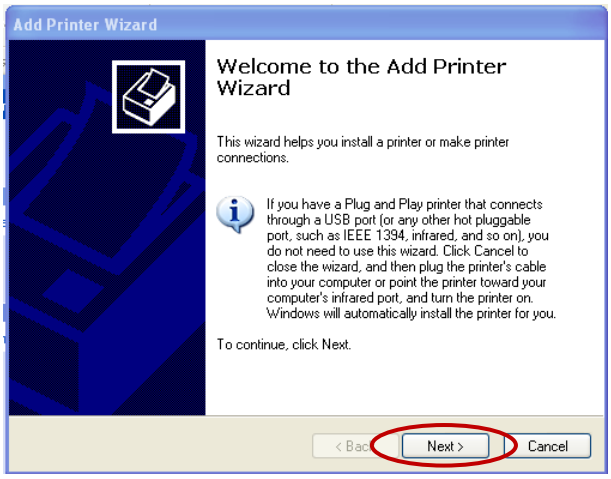
Open the **Printers and Faxes**.



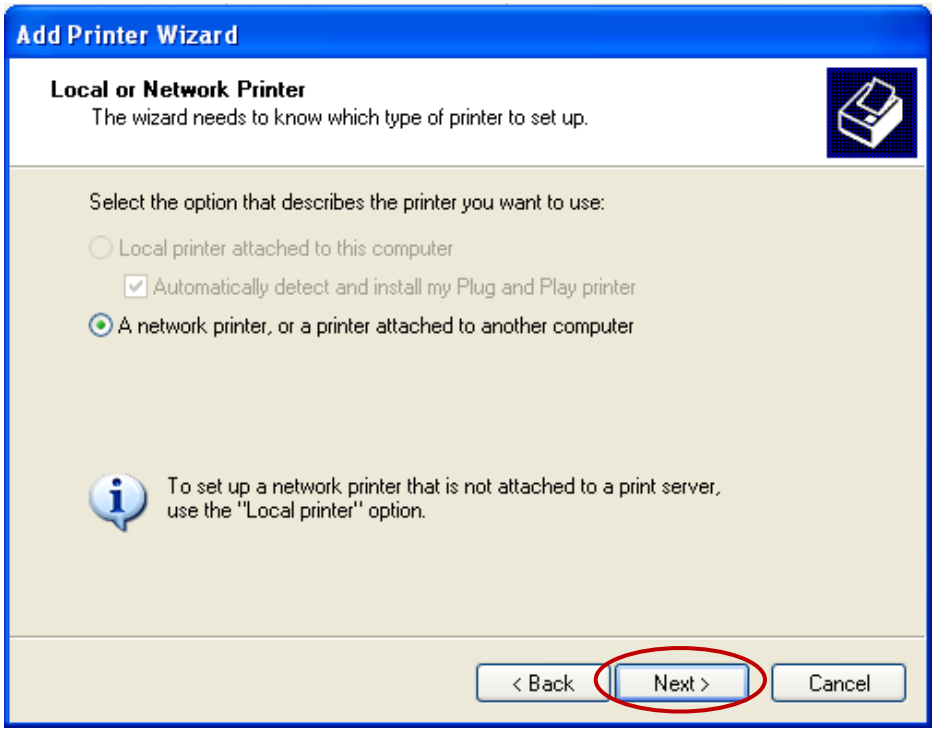
Double click on the **Add Printers** icon.



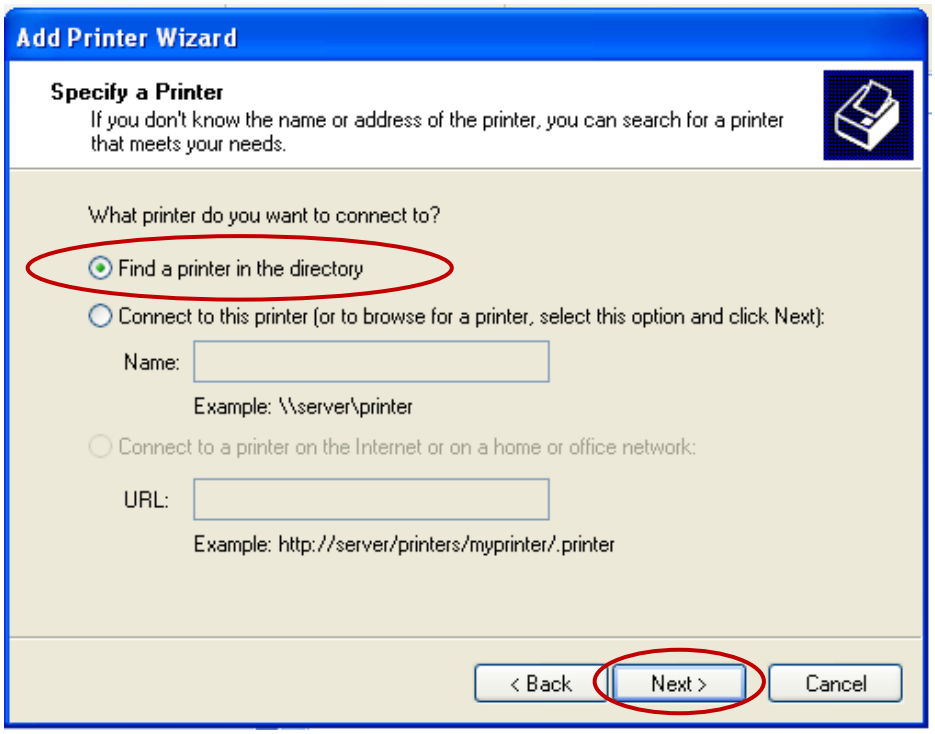
This will start the Add Printer Wizard. The first screen is just a welcome screen, click **Next**.



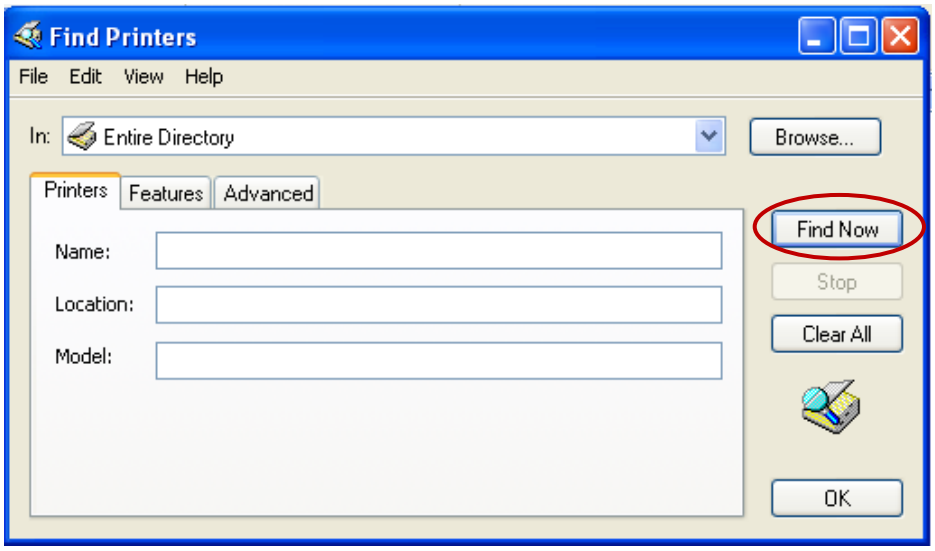
The next screen will ask you what type of printer you want to install. The **Network printer** is the only one that will be available because the user does not have permission to install a printer locally. Click **Next**.



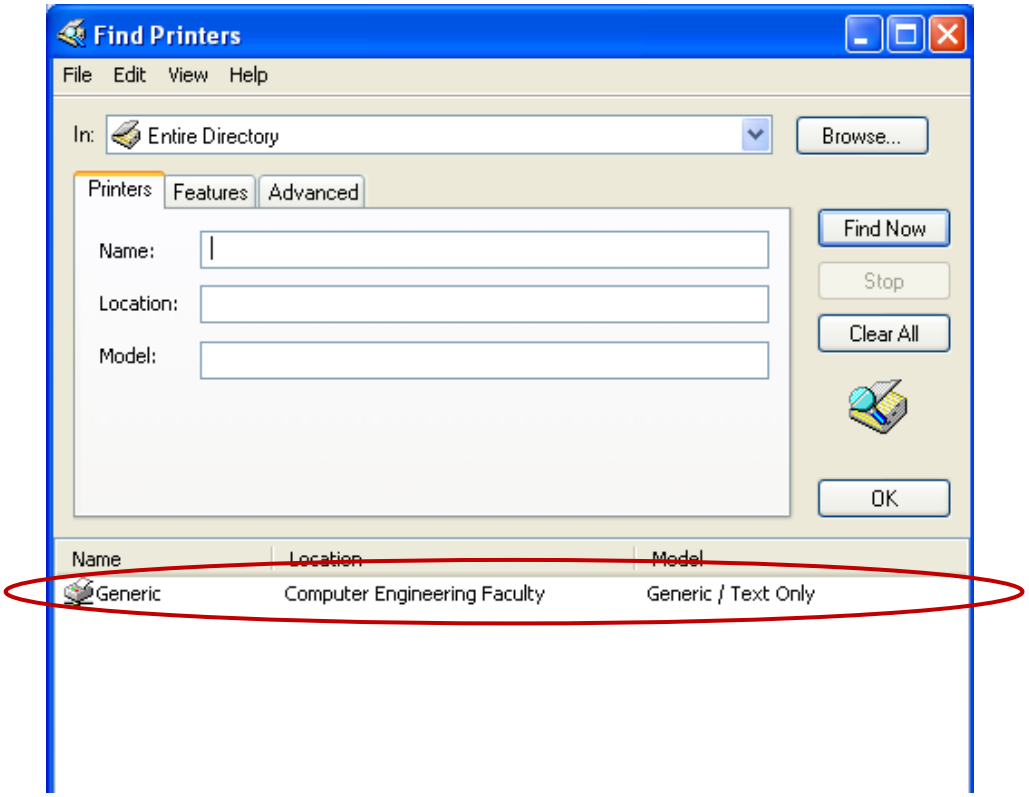
The next screen gives you different options to find the printer. Select the **Find a Printer in the Directory** option and click **Next**.



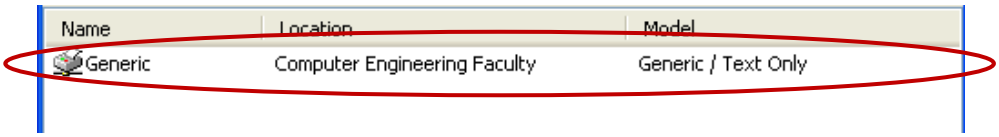
This will bring up a search screen for printers. Leave the entries blank and it will give you all of the shared printers available in the directory. Click on **Find Now**.



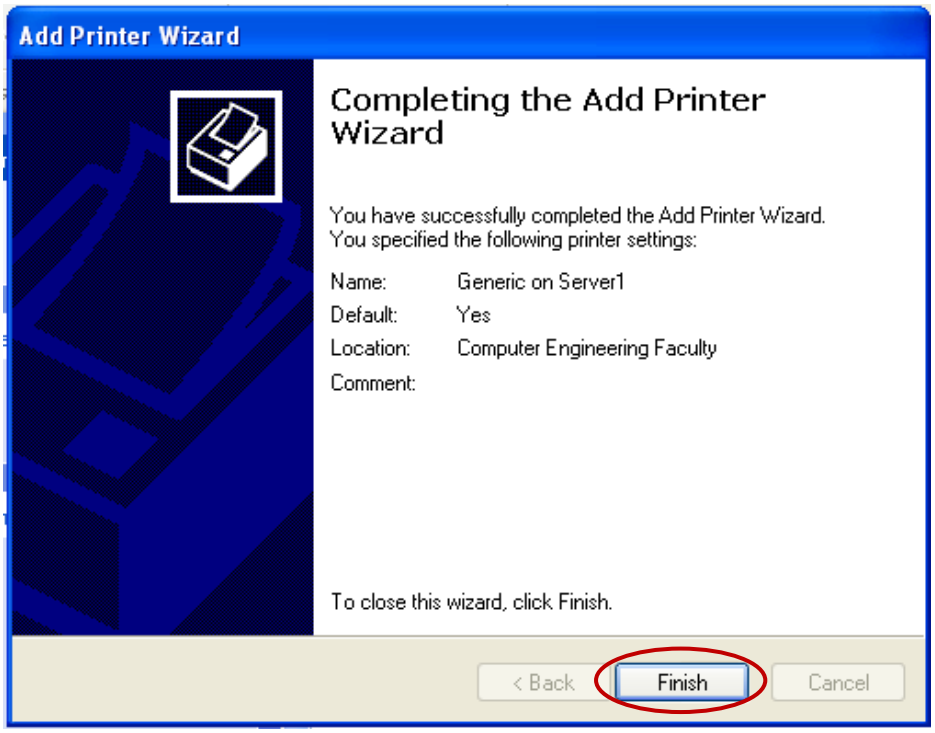
You will get the printer named **Generic** to appear because it is the only printer in the domain. You can see that the location of the printer is the correct one for this user.



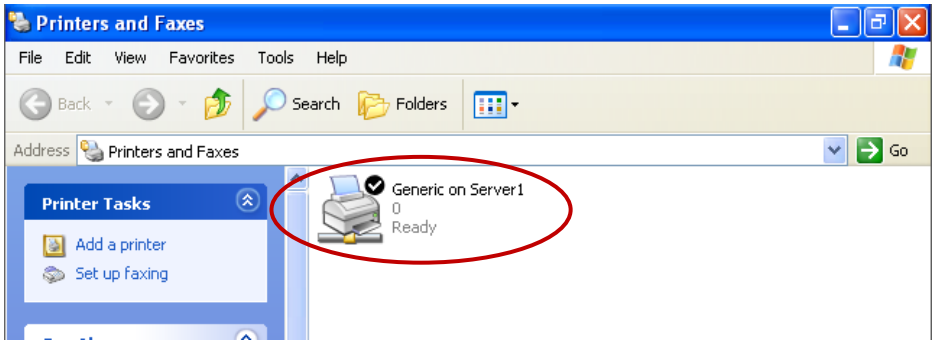
Double click on the **Generic** printer.



The final screen will show the information you placed in the wizard. Confirm that it's all correct and click **Finish**.



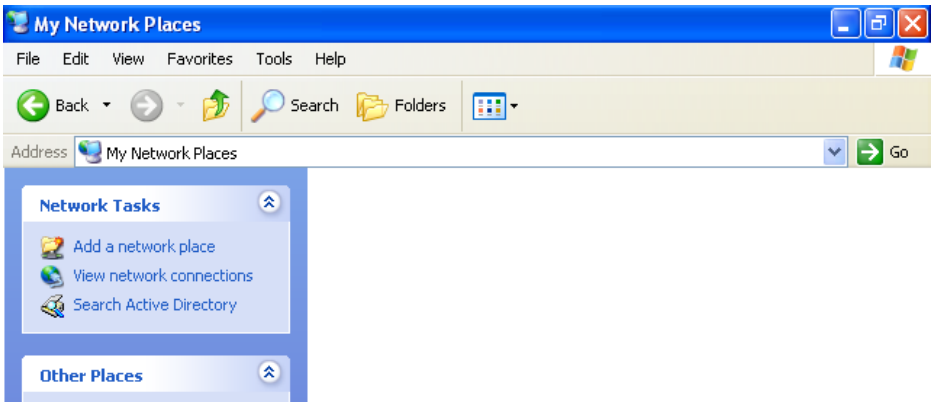
You now have the Generic printer icon appear in your printers folder as the default printer. Close the **printers folder**.



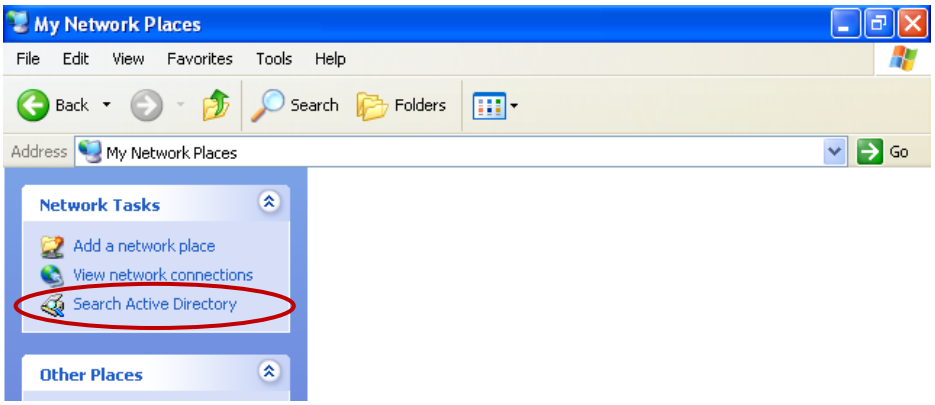
4.6. Perform Active Directory Searched for Published Resources: Contact Scenario

Erwin's boos told him to call the representative from the shipping company and ask him why he billed the marketing department for a shipment. He gave Erwin the phone number but Erwin has lost the number in his mess of an office. He remembers that his boss got the number from Active Directory in the first place, so now he is going to try and do a search in Active Directory for the contact.

Open **My Network Places**.

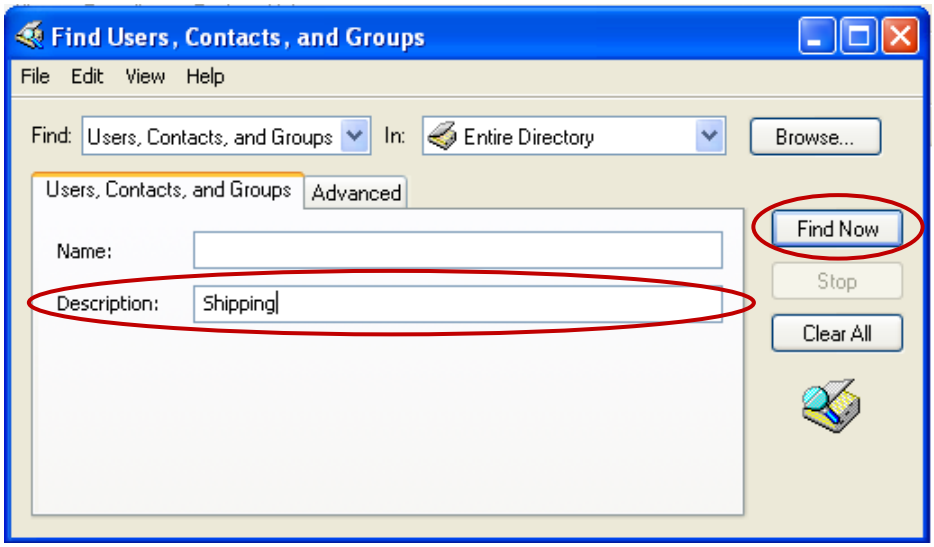


Click on **Search Active Directory**.

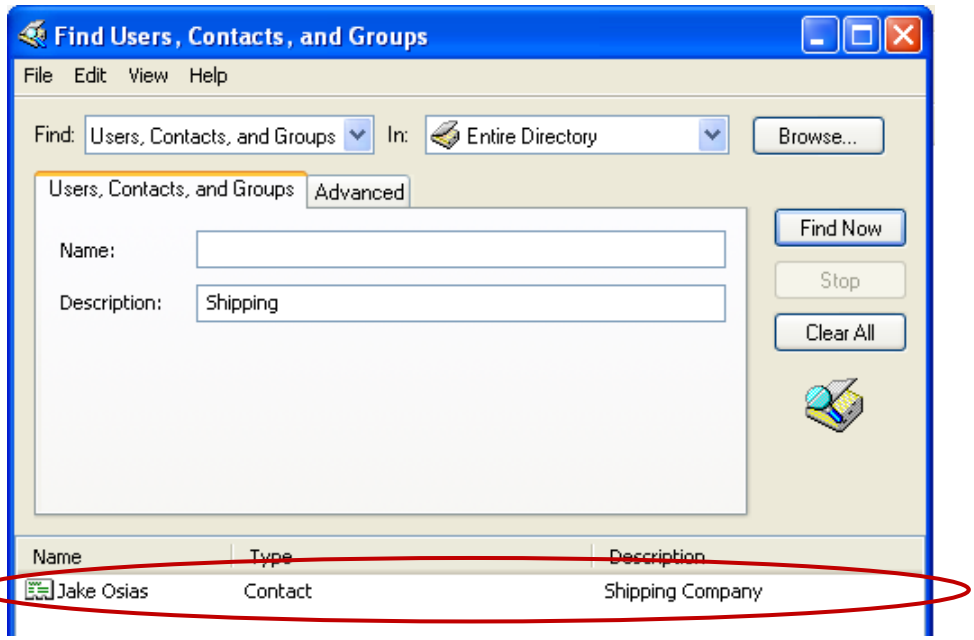


You will do a search for **Shipping** in the Description box in hopes of finding the contact for the shipping company.

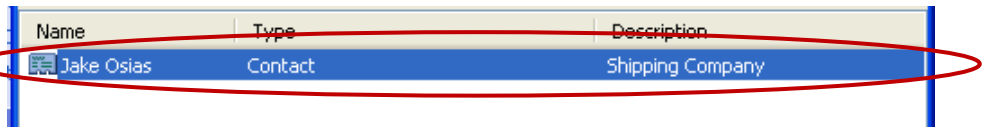
Enter in the Description box the **Shipping** and click **Find Now** Button.



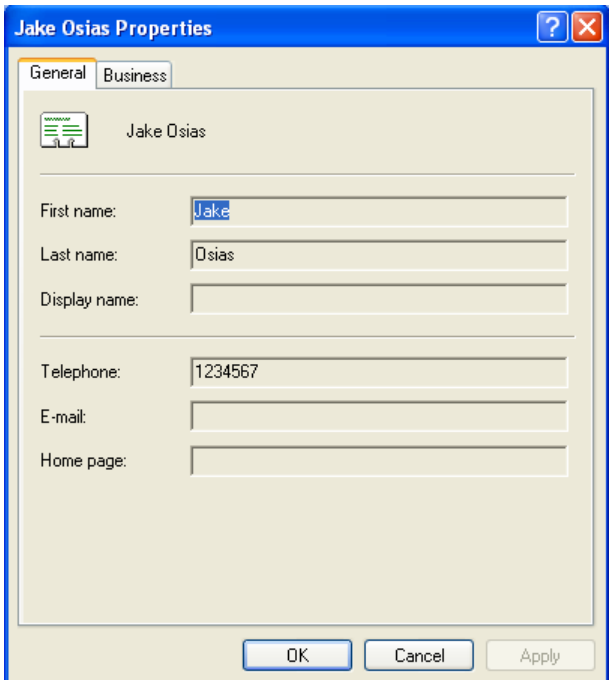
You should get a result for **Jack Osias**.



Double click on the contact.



You will be able to get all the information you need to contact him.



SUMMARY / CONCLUSION

Establishing an Active Directory presents both challenges and opportunities, forming the cornerstone of streamlined IT governance within any organization. Through consolidating user authentication, regulating resource access, and enforcing policies, Active Directory alleviates administrative burdens and fortifies network security. Nonetheless, its effective deployment demands methodical planning, strict adherence to industry standards, and continuous upkeep to sustain peak performance and resilience against potential vulnerabilities.

REFERENCES

How to install Windows XP on VMware? Step by step guide. (n.d.). Tutorials Freak. https://www.tutorialsfreak.com/nmap-tutorial/windows-xp-installation-on-vmware

Scott Skinger. (2002). *Building an Active Directory Infrastructure for Ben & Brady's Ice Cream, Corp.* Train Signal, Inc.,.

Example: Installing Windows Server 2003 as a guest operating system. (n.d.-b). https://web.mit.edu/asedeno/Favorites/sipb%20homedir/vmware/vmware-console-distrib/lib/help-manual/new_guest_example_gsx.htm