Intro to Active Directory Domains - Anthony Adams

Module Objectives

Install a new Windows 2019 Server in a Virtual Machine

• Identify differences between a domain controller, a member server and a standalone server
• Install Active Directory thereby promoting the system to a domain controller and creating a subdomain (child domain)
• Obtain an overview of Active Directory administrative tools
• Demote a domain controller and removing a subdomain (child domain)
• Create a member server

Activity: Prepare the Environment

1. Boot the computer at your seat – this is your local host
2. Login
3. Navigate to D:\Courses\COMP-10041\
4. Open the folder AcmeCoreDC2019
5. Double Click on AcmeCoreDC2019.vbox (the blue

icon) to open your domain controller
6. Open the folder Client10-PC.vbox
7. Double Click on Client10-PC.vbox (the blue icon) to open your client machine
8. Start the AcmeCoreDC2019, and then start the Client10-PC
9. Login to the workstation as Anthony.Green@acme using the password AdminP@ss Anthony Green is the Domain Administrator
• Perform this procedure immediately at the start of every class unless told otherwise

Note: This environment differs from our standard preparation
10. Create a second Windows virtual server
– Create the virtual machine using:
• Name: Windows
• OS Type: Windows 2016 (64 bit)
• Hard Disk: Create new hard disk – Windows2019
• CD\DVD-ROM: Mount using ISO Image File
D:
\Courses\ISO\en_windows_server_2019_updated_march_2019_x64_dvd_2ae967ab
• Network: Host Only Network

Activity: Install Windows Server 2016
• The virtual machine just created represents the

hardware of a brand new computer without a previously installed operating system
• The virtual CD\DVD ROM drive is configured to use the Windows Server 2019 Installation ISO image
• When booted, the Setup program will run automatically
1. Start the new Windows Server virtual machine
– The Oracle VirtualBox startup screen appears for a few seconds
– The Setup program will start
2. Click Next to accept default language, time and currency format values
3. Click Install now to start the installation
4. Enter the Product key. This is a trial install. Chose "I don't have a product key"
5. On the Select the operating system you want to install page, choose the Windows Server 2019 Standard (Desktop Experience) (GUI)
option and click Next
6. Accept the license terms and then click Next

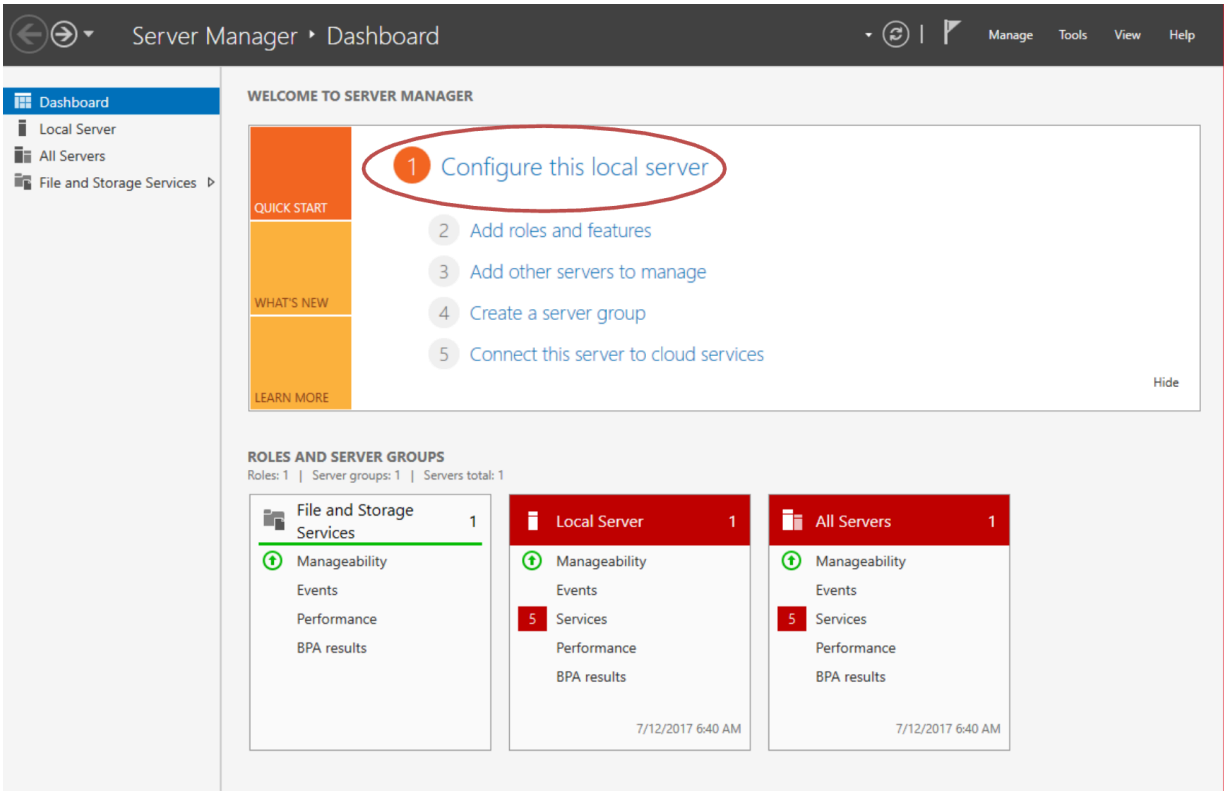
Activity: Install Windows Server 2019
7. On the Which type of installation do you want page, choose the Custom: Install Windows only (advanced) option
8. On the Where do you want to install Windows page, the default hard drive is already selected, so

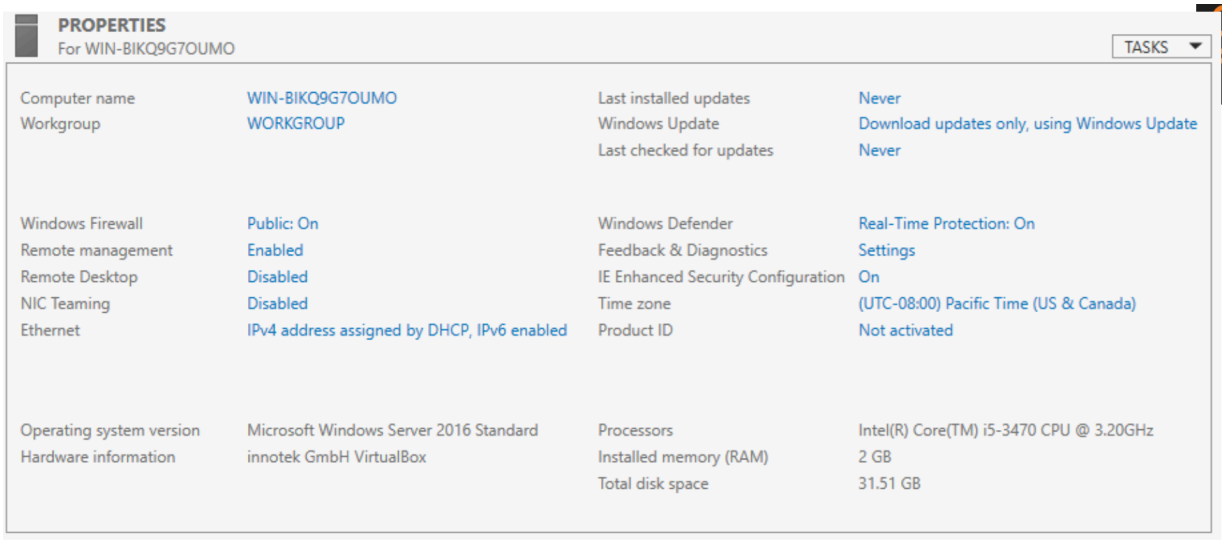
click Next
– You do not need to partition or format the drive as the virtual machine was created using the Windows 2019 (64-bit) option
9. Installation of the operating system will now start
– Setup copies the full disk image to the hard drive and expands it
– Setup then installs features based on the computer's configuration and detected hardware
10.Set the Administrator's password to AdminP@ss, click Finish
11. Log on to your new Windows Server 2019 as: User: Administrator Password: AdminP@ss

Server Manager

• This virtual image is the result of a typical Windows Server 2019 installation and is known as a stand-alone server
• Server Manager is Automatically displayed at logon after new installation
• Command center for performing many administrative tasks
• Interface to many Server Role configuration utilities
• Functionality similar to Add/Remove Programs option in the Control Panel
• Screen doesn't provide all available options for the configuration and management of some server roles

– We will NOT use this interface very often in this course

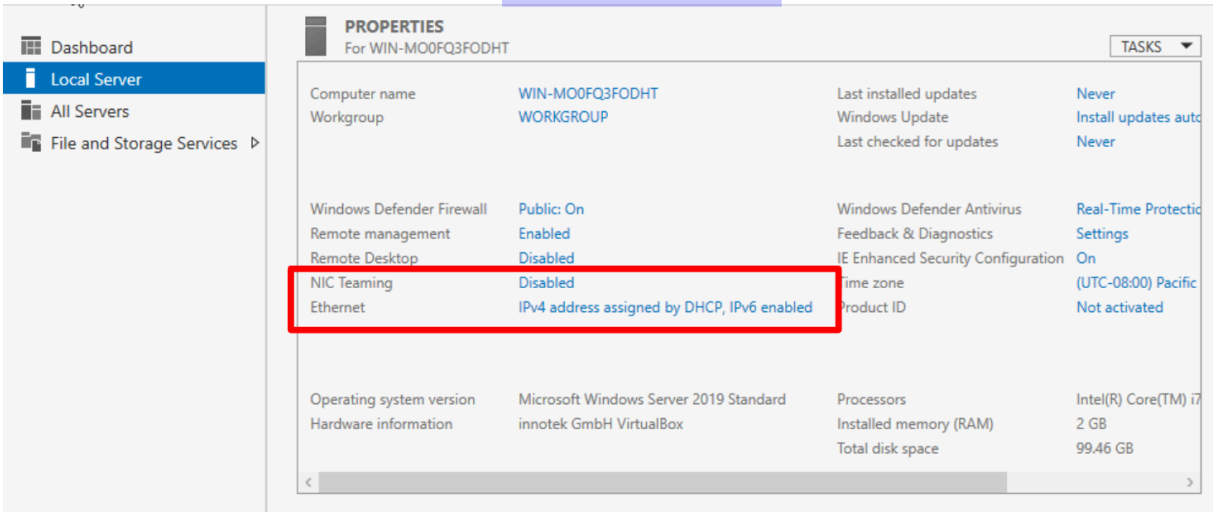




Activity: Viewing Server Roles and Features

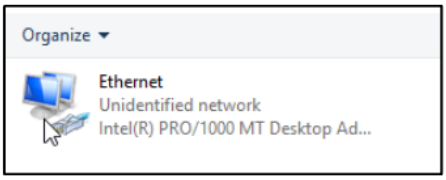
1. On the Dashboard, under the Configure this Local Server section, select Add roles and features
– Read the section, Before You Begin
2. Select Server Roles
– Examine the list of possible server roles
3. Select Features
– Examine the list of possible server features
4. Click Cancel to close the Add Features Wizard
5. Select menu item Manage
6. Select Server Manager Properties
7. Check the Do not start Server Manager automatically at logon box
8. Click OK

Activity: Configuring your Network IP Address



1. Choose the ethernet setting:

2. Double click ethernet:

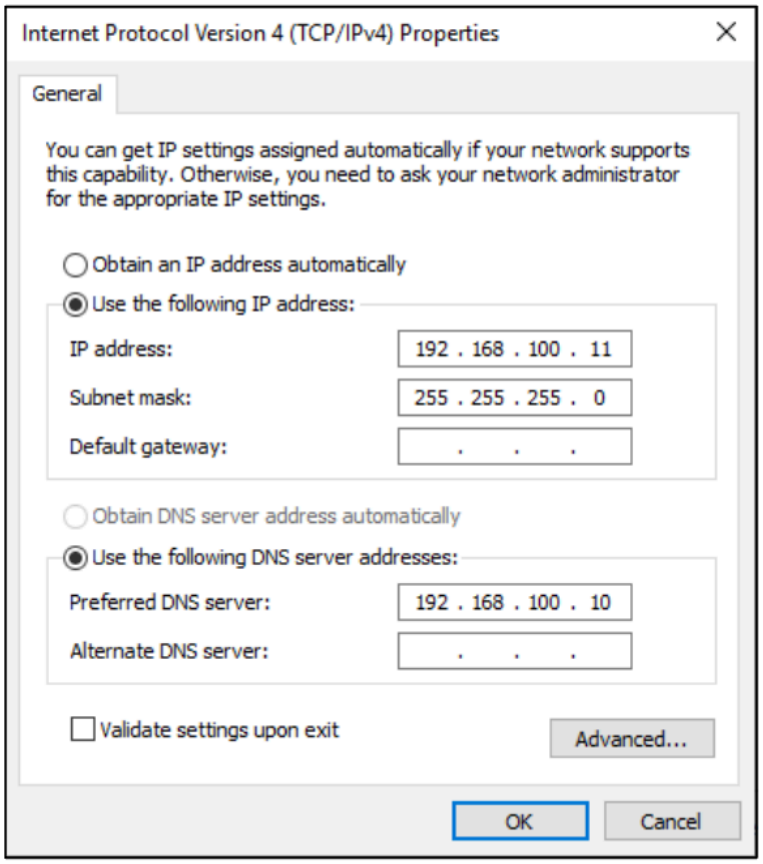


Activity: Configuring your Computer's Name Settings

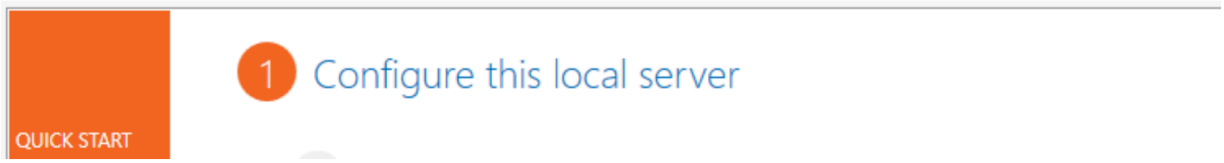
3. Choose Properties
4. Select Internet Protocol Version 4 (TCP/IPv4) and chose properties
5. Configure the system's TCP/IP (Ethernet) settings as follows:

– IP Address: 192.168.100.11
– Subnet Mask: 255.255.255.0
– Default Gateway:
– Preferred DNS Server: 192.168.100.10

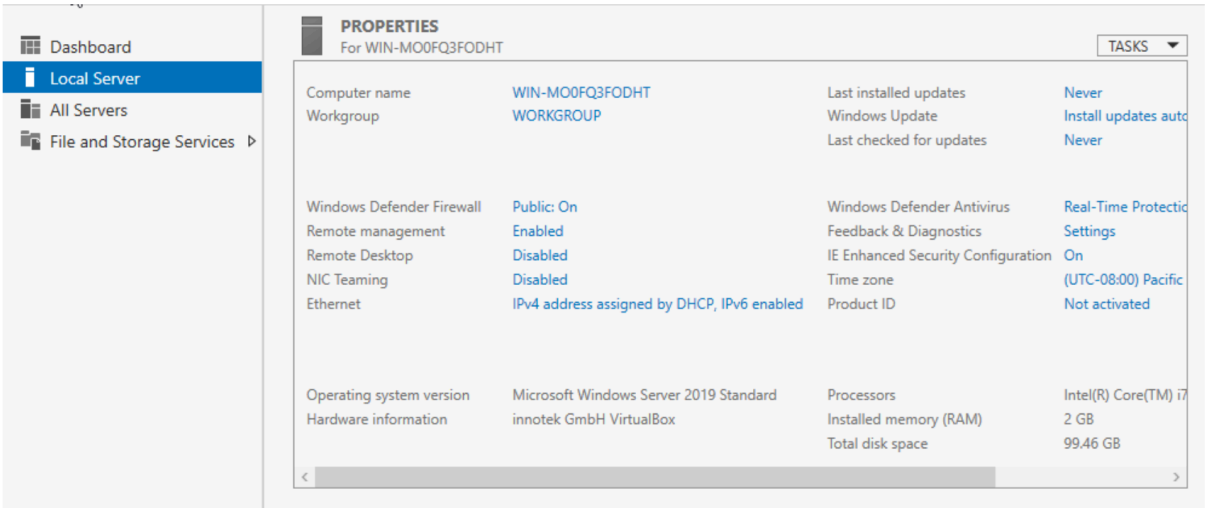
6. Click OK to exit TCP/IPv4 Properties
7. Click Close to exit Ethernet Status
8. Exit out of the Network Connections

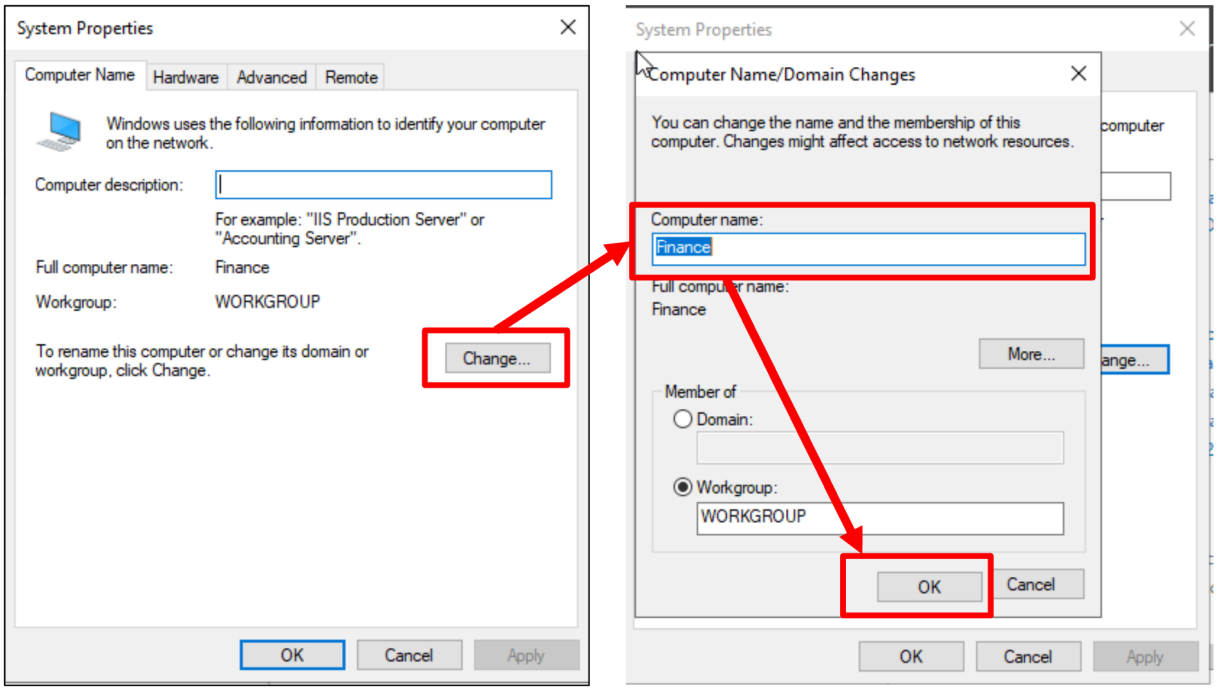


Activity: Configuring your Computer's Name Settings



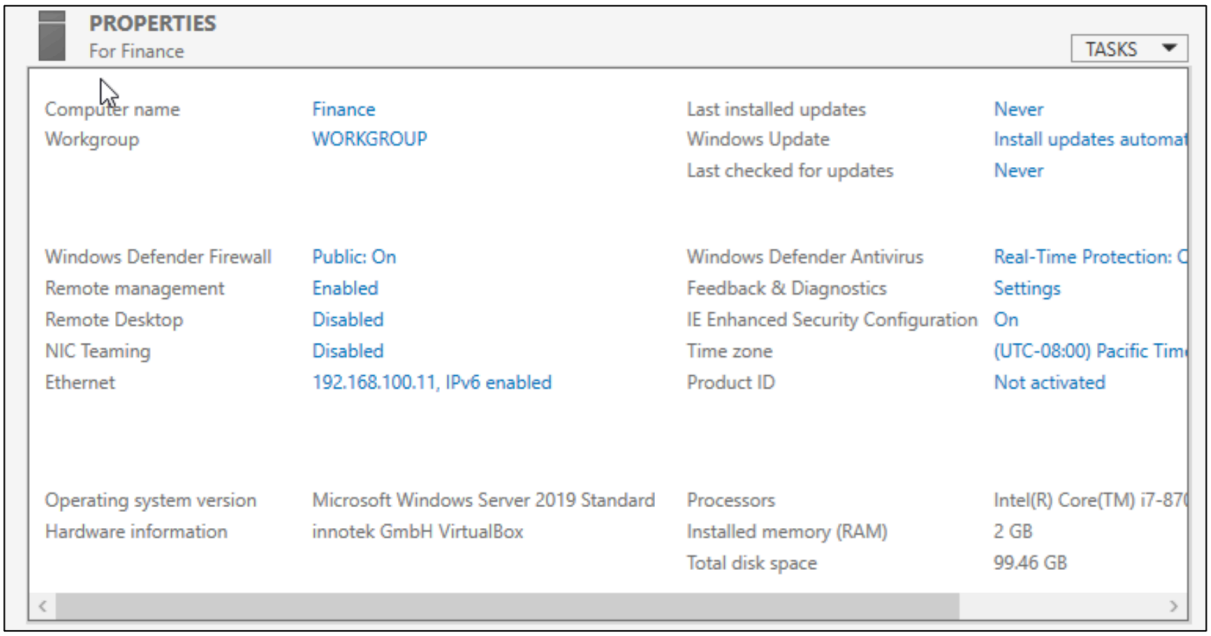
Change the computer name to Finance





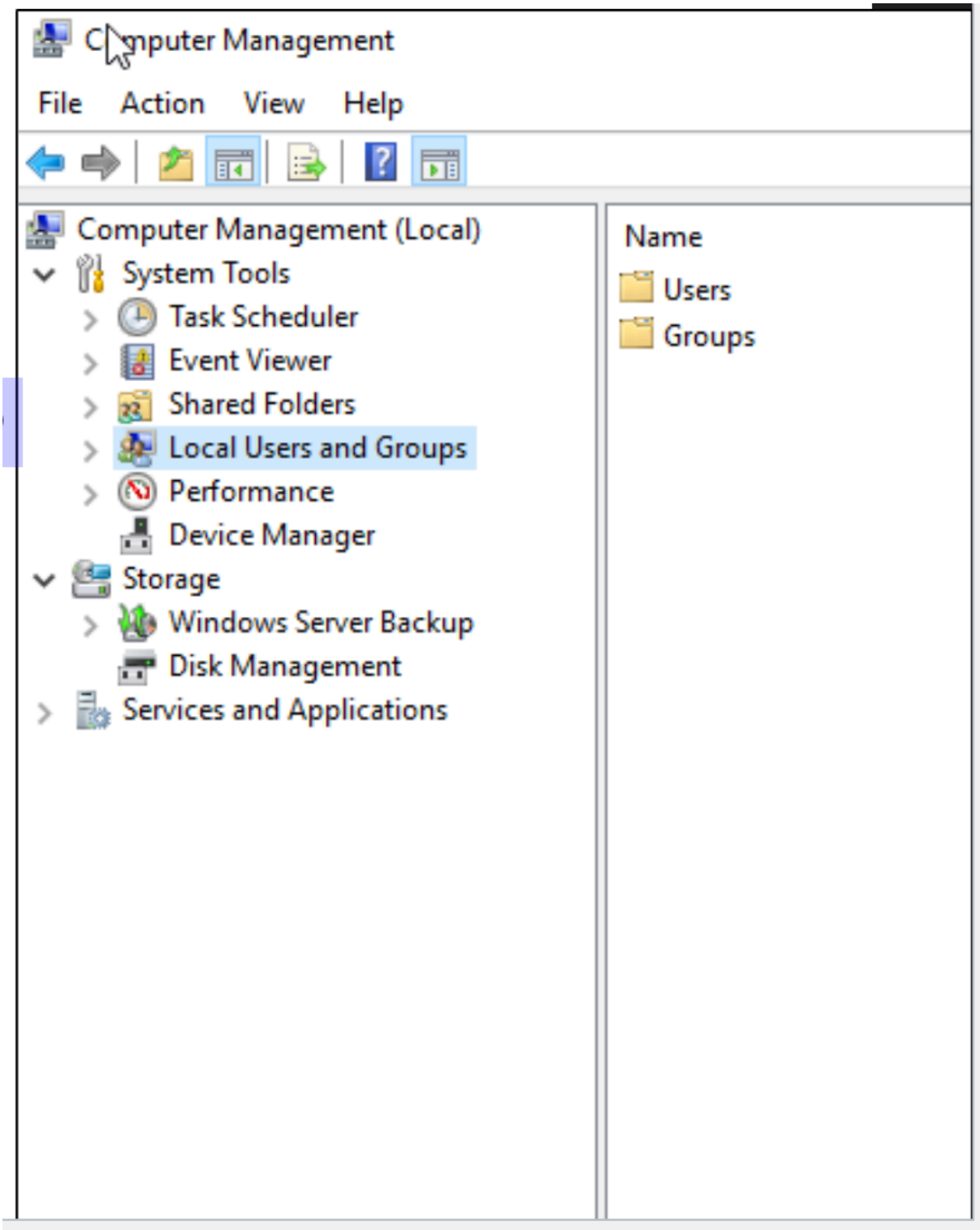
Restart your computer to complete the renaming process

We now have our standalone server configured and ready to join the Acme Domain



Activity: Identifying a Standalone Server's Default User and Group Accounts

1. Right click on the Start Menu and choose Computer Management or click on the start menu and type Computer Management
2. Expand the Local Users and Groups folder which is located under System Tools
3. Select the Users folder and note the default user accounts
4. Select the Groups folder and note the default group accounts
5. Close all open windows



Standalone Server Accounts

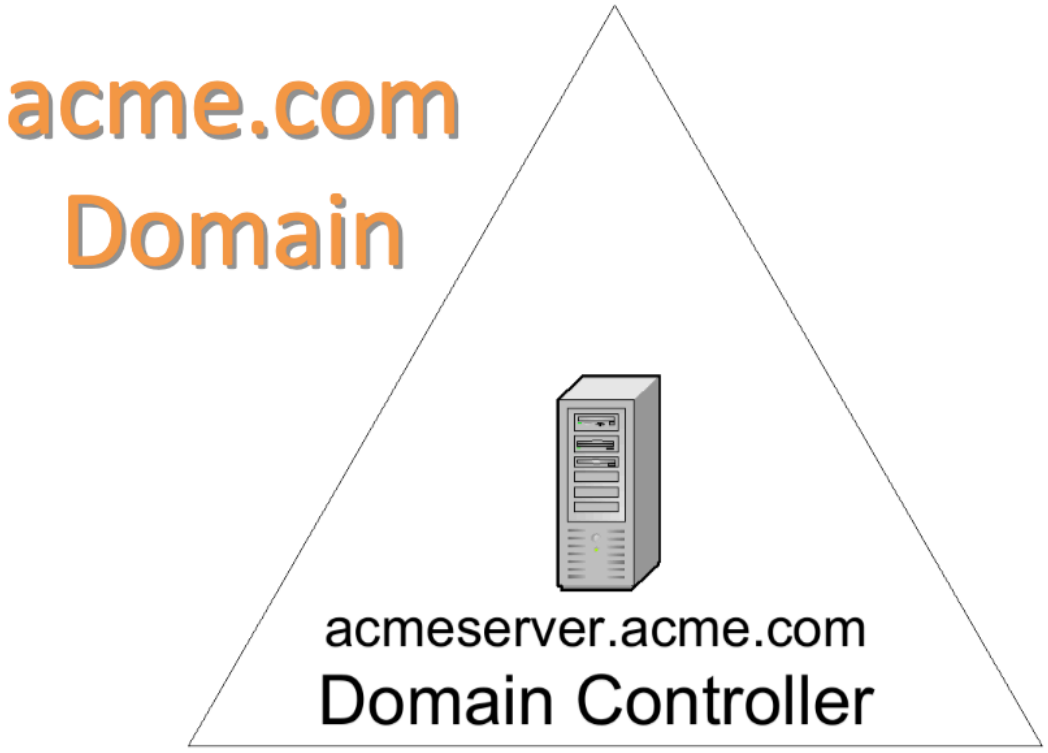
• User and group accounts on a standalone server are stored in the computer's Security Accounts Manager (SAM) database
• These are NOT domain accounts
– Cannot be used to access domain resources
• SAM accounts are deleted when Active Directory is installed on the standalone server

Installing Active Directory

• Installing Active Directory onto a standalone server or member server makes the server a Domain Controller
• Active Directory installation causes the server to be "Promoted" to a Domain Controller
• A new set of built-in group and user accounts are created
– SAM accounts are deleted

Domain Controllers and Domains

• Every domain must have at least one domain controller
• A domain requires an Active Directory database which is only stored on a Domain Controller

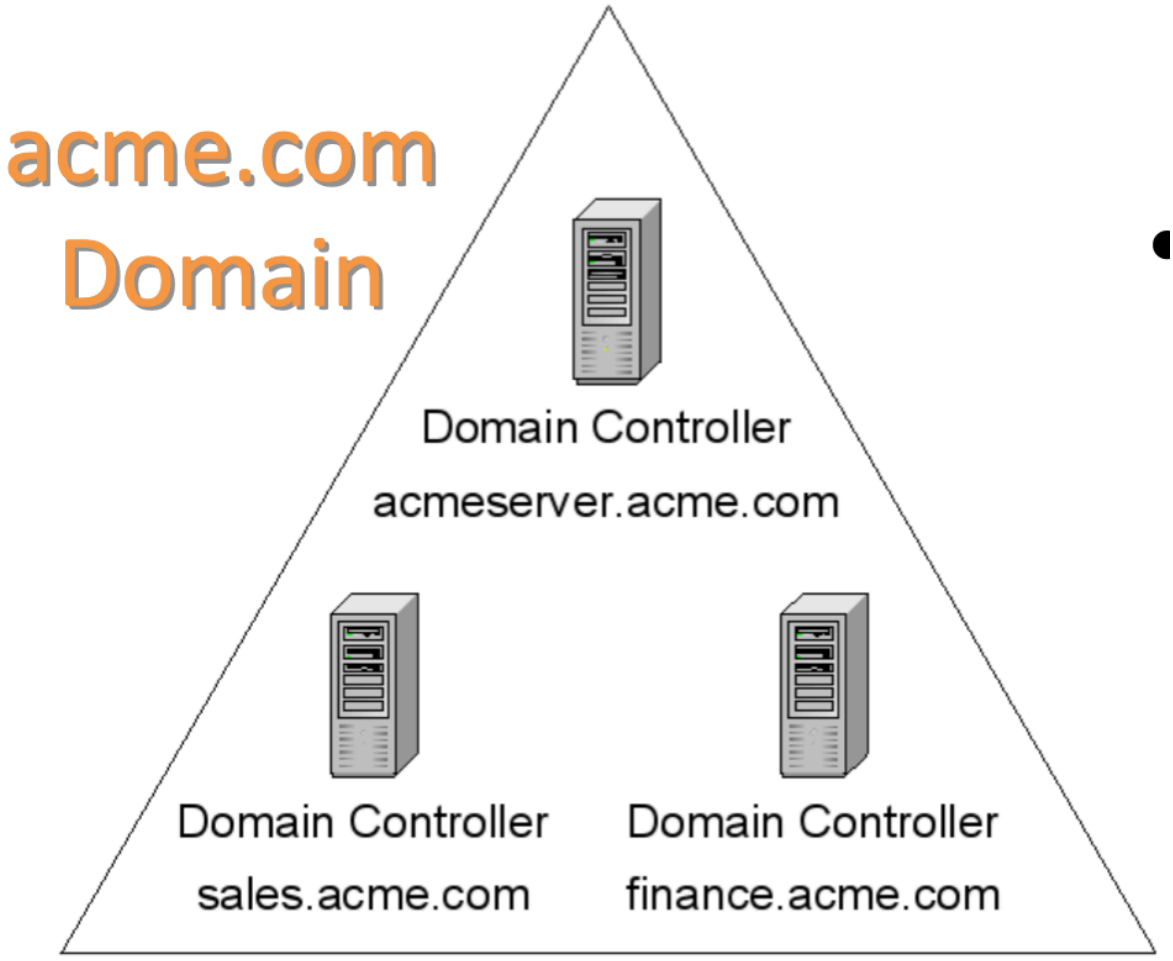


Domain with Multiple Domain Controllers

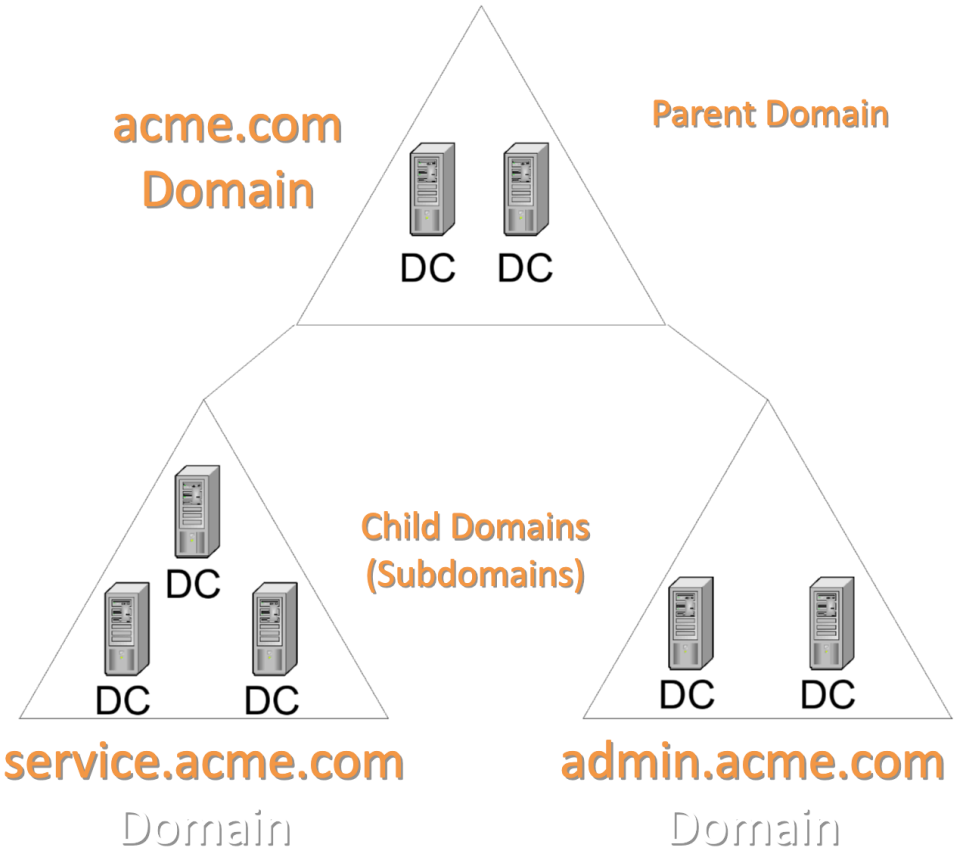
- A domain can have multiple domain controllers
- Recommended

– DC stores the all important Active Directory

– Multiple DCs means duplicate copies of the Active Directory reside on each DC



Parent Domains and Child Domains



Promotion and Sub-domain Creation

• The next activity will have the following results:

a) Active Directory will be installed on the standalone server

b) Standalone server will be promoted to a domain controller

c) Sub-domain (child domain) below acme.com domain will be created

• One wizard will do all of these procedures

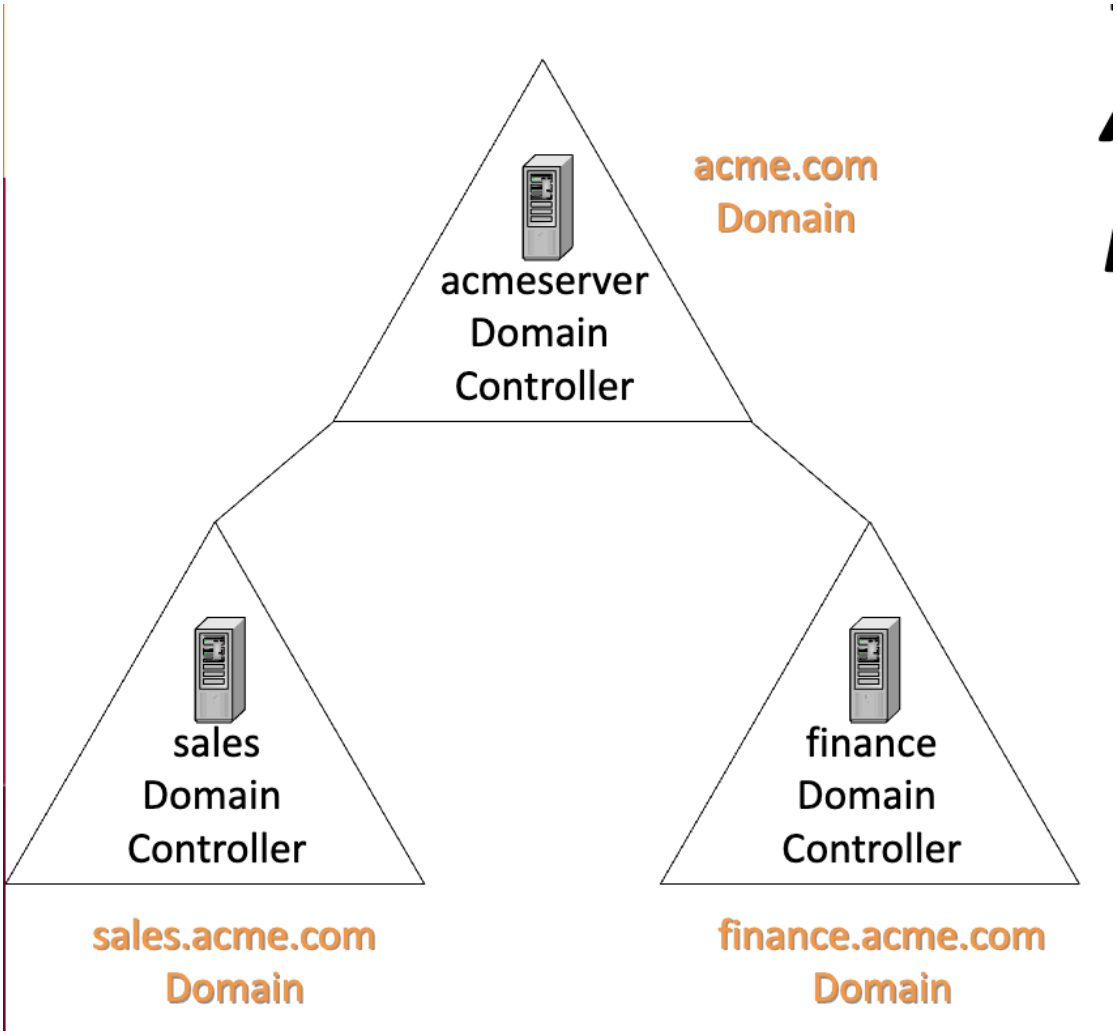
• Steps a) and b) are linked in that you cannot perform one without the other also occurring

Target Domain Structure

• Next you will use the Active Directory Installation Wizard to:

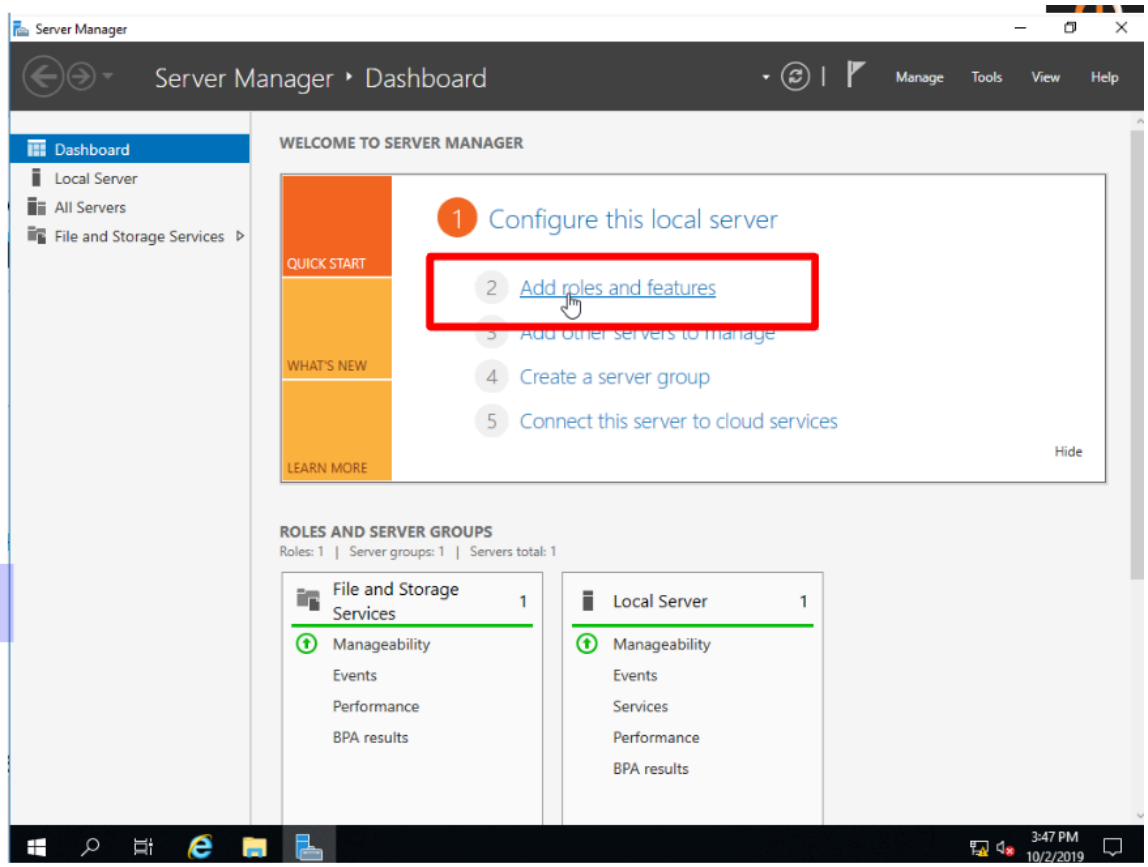
a) Promote your server to a domain controller

b) Create a subdomain called Finance



Activity: Promotion and Subdomain Creation

1. Start Server Manager
2. Under Configure this Local Server choose Add roles and features
3. Click Next 3 times accepting the defaults on each screen to advance to the Server Roles screen
4. Click Active Directory Domain Services
5. Click Add Features, click Next
6. On Features, Click Next
7. On AD DS, Click Next
8. On Confirm Installation selections, click Install
9. On Results, Click Close Active Directory tools will be installed on this server

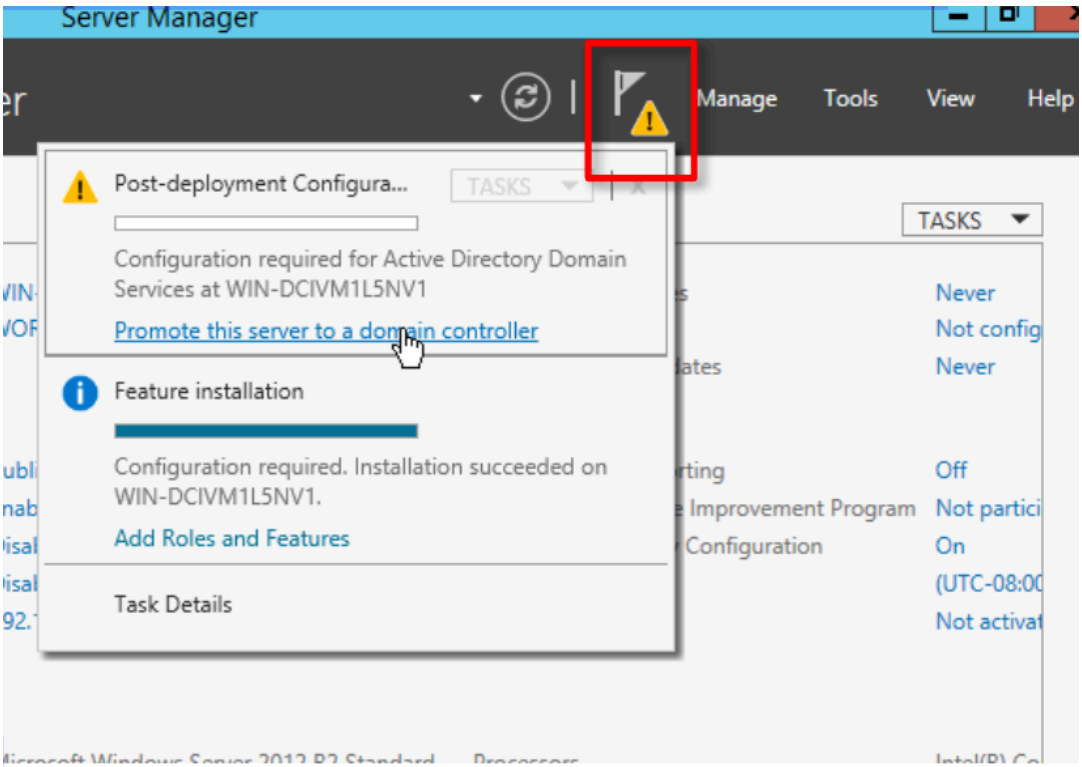


Activity: Promotion and Subdomain Creation

• The next series of slides contain detailed instructions you are to follow for this procedure and also lists questions about information you are to obtain from the wizard screens The answers to these questions should be recorded on the Supplemental Content document that you were suppose to bring to this class

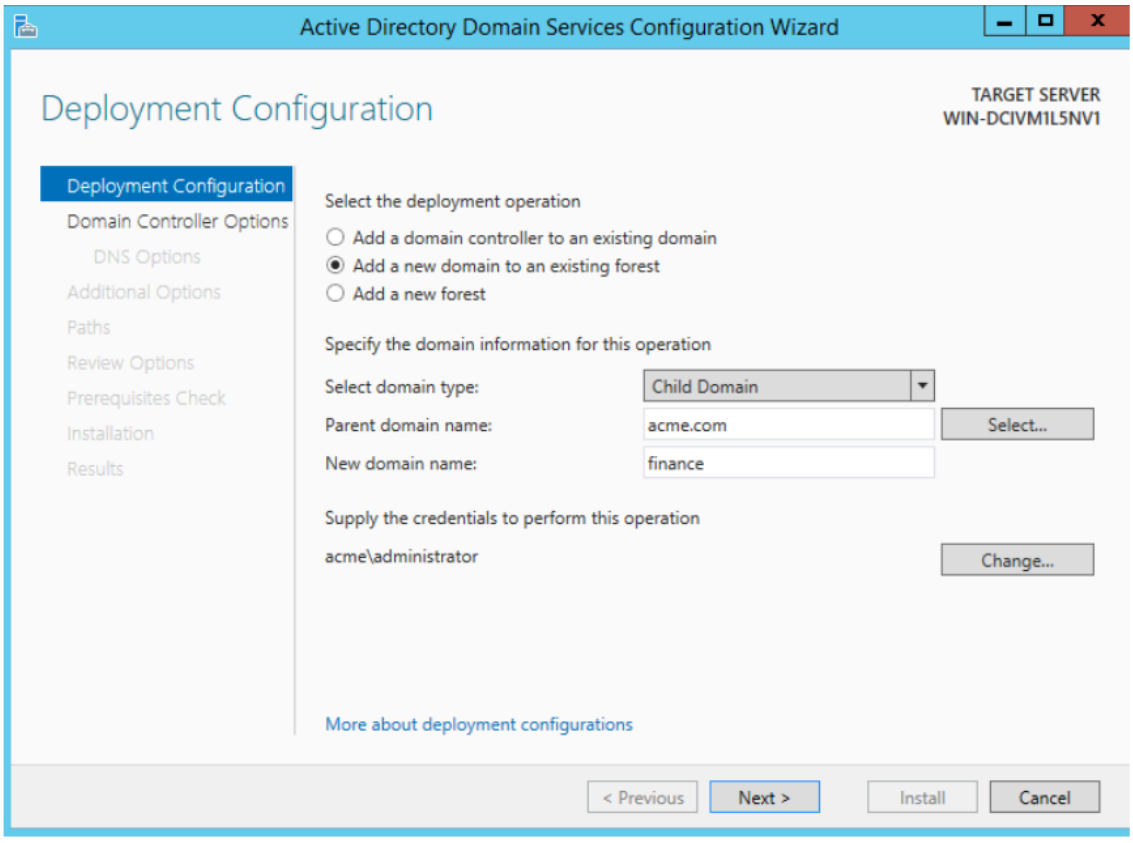
Activity: Promotion and Subdomain Creation

1. Click on the Notifications emblem (the flag)
2. Under Post-deployment Configuration choose Promote this server to a domain controller
3. Ensure you select the options that will create a Add a new domain to an existing forest
4. Select domain type: Child Domain
5. Parent Domain name: Acme.com
6. New domain name: Finance



7. Click Change under “Supply the Credentials to preform this operation” and supply:
– User Name Anthony.Green@acme (Acme Domain Administrator)

– Password AdminP@ss
This account has the privileges necessary to install Active Directory onto this computer, as a Sub-Domain Controller
8. Click Next
9. Set the domain functional level at Windows Server 2016
• What operating systems can be used as domain controllers at this level?



10. On Domain Controller Options Use Adminf1nance as the Directory Services Restore Mode Administrator password click Next

11. On DNS Options accept defaults click Next
12. On Additional Options verify the NetBIOS domain name accept the default click Next
13. On Paths Use the default Active Directory folder locations click Next (make note of this information in your notes)
14. On Review Options click Next
15. Review Prerequisites Check click Install

• What is the recommended storage drive configuration with regard to the Active Directory database and Active Directory log files?
• What is the default path to the folder where the Active Directory database will be stored?
• What is the default path to the folder where the Active Directory log file will be stored?
• What is the default location of the SYSVOL folder?
• What is stored in the SYSVOL folder? Activity: Promotion and Subdomain Creation
• Is the restore mode Administrator account the same as the domain Administrator account?
• On the Summary page, note that the password for the administrator of this new domain will be the same as the password for the administrator of this local computer
• What is the NETBIOS name of the new domain?

• Note that the Active Directory configuration may take a few minutes to complete

16. When prompted, restart the computer
17. When prompted, log on using the administrator account for the Finance subdomain you just created – The password for this administrator account is still AdminP@ss as it was for
the administrator account on this computer before it was promoted to a
domain controller

Active Directory Administrative Tools

• Domain Controller promotion includes automatic installation of several Active Directory management console tools including:
a) Active Directory Domains and Trusts For managing domains, domain trees and domain forests
b) Active Directory Sites and Services For managing sites and subnets
c) Active Directory Users and Computers For managing domain users, groups, organizational units and computers

d) Active Directory Administrative Center
e) Active Directory Module for Windows PowerShell
Additional tools and functions

Activity: Quick look at Active Directory

Domains and Trusts

1. Open Active Directory Domains and Trusts
   -From the Start Menu select Administrative Tools
   -Select Active Directory Users and Computers
2. Expand acme.com domain
3. Right click your finance.acme.com subdomain and select Properties
4. Record the following default settings:
   –Domain functional level:
   –Forest functional level:
5. Close this console

Domain and Forest Functional Level Settings

• “Windows 2000 mixed mode” supports DCs running Windows NT 4.0, Windows 2000 and Windows Server 2003
– Downside 1: Reduced AD management functionality
– Downside 2: Not able to use domain controllers running Windows Server 2016 and computers running Windows Server 2016 may have issues when working with Windows NT DCs

• “Windows 2000 native mode” supports DCs running Windows 2000, Windows Server 2003 and Windows Server 2008
– Upside: More AD management functionality than “mixed”
– Downside: Windows NT DCs are not supported

Description of a Site
• A site is made up of one or more reliable and fast TCP/IP subnets
• Creating sites allows AD access and AD replication frequency to be optimized in relation to network performance capabilities
– E.g. If two areas of a domain are geographically distant from each other and are connected by a relatively slow WAN link then each area could be placed in a different site
– AD replication frequency between sites can be reduced to minimize bottlenecks on the WAN link
• See the section under “Understanding Sites and Subnets” in the text for more details

Activity: Quick Look at Active Directory Users and Computers
1. Open Active Directory Users and Computers
2. Expand your finance.acme.com icon

3. Select the Users folder
– Note the new set of predefined user and group accounts have been created (SAM accounts have been deleted)
– Note there is a Users folder but no Groups folder – recall prior to the promotion, Computer Management showed a
Local Users and Groups folder that contained a Groups folder
4. Close the ADUC consoles

NTDS.dit
• Domain accounts are stored in the Active Directory database on the domain controller
• NTDS.dit is the name of the Active Directory database file
– To remember this file name, think NT Directory Services.Directory Information Tree

Activity: Verifying SAM Accounts have been Deleted
1. Open Computer Management
2. Attempt to locate the Local Users and Groups folder
– Formerly under System Tools
– You should NOT be able to locate this folder
3. Close the Computer Management console

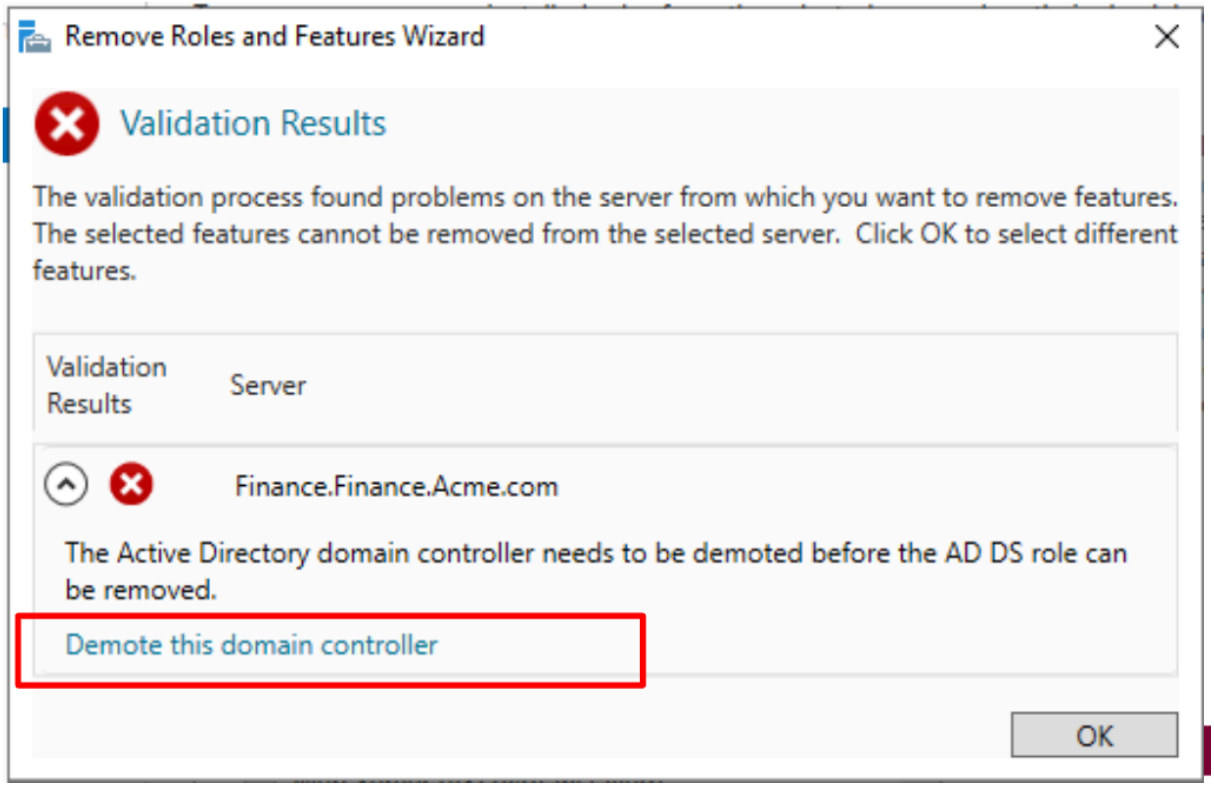
Activity: Demoting a Domain Controller

1. Server Manager is used to Demote a Domain controller to Standalone Server Status
2. Choose Manage
3. Remove Roles and Features
    -Before You Begin Click Next
    -Server Selection select the server you want to demote Click Next
    -Server Role – Uncheck Active Directory Domain Services Click Remove Features
4. Before the process can be completed you must Demote this Domain Controller

• The next series of slides contain detailed instructions you are to follow for this procedure and also lists questions about information you are to obtain from the wizard screens

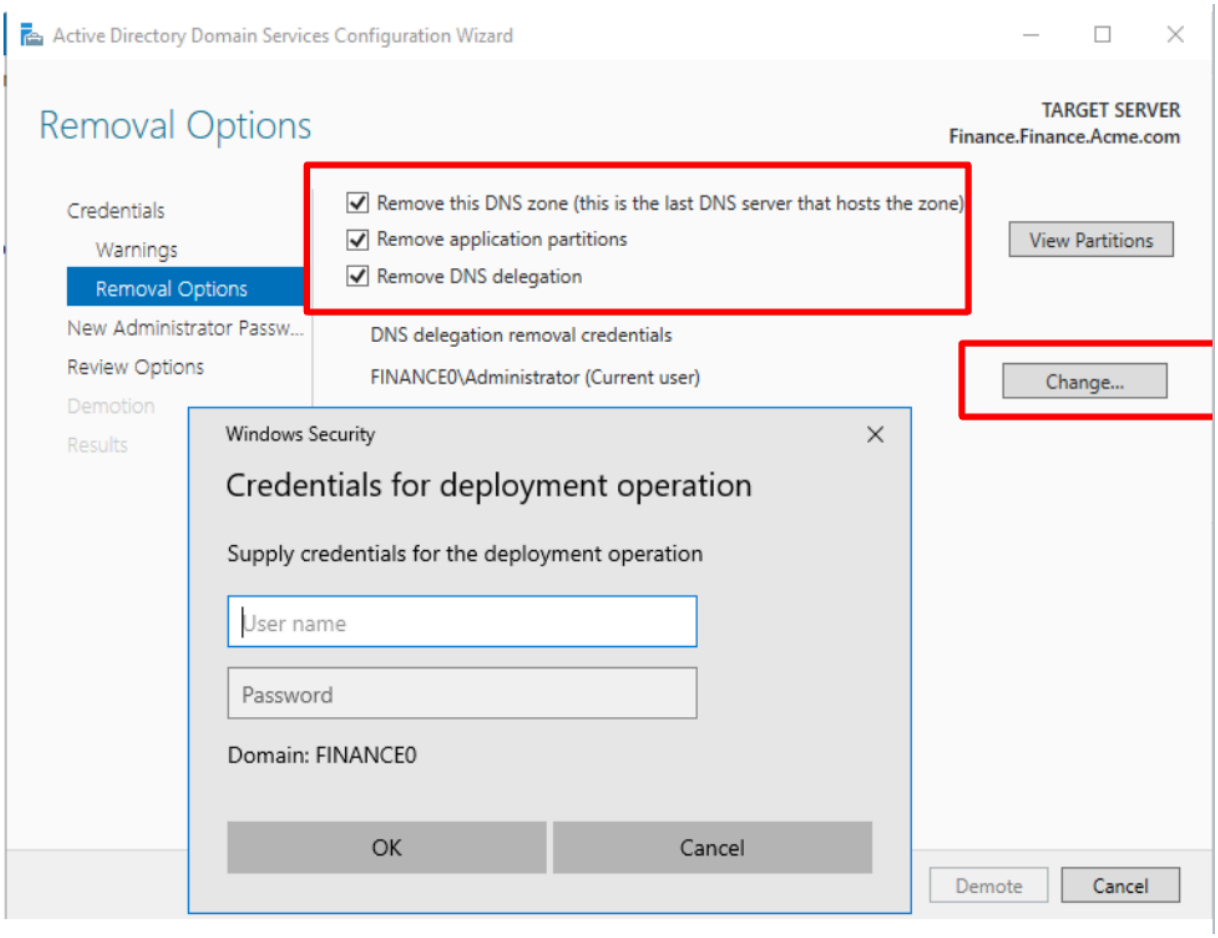
Activity: Demoting a Domain Controller

1. Deselect Active Directory Domain Services (Remove the checkmark) Click Next
2. Click Remove Features
3. The following warning message advises you that your credentials will not allow this demotion
4. Click Demote this domain controller to continue



5. Verify Proceed with removal
– Once Active Directory has been removed, the finance child domain will no longer exist because there is no other DC in the finance subdomain to support this domain
6. What determines whether a demoted domain controller becomes a member server or a standalone server?
7. Remove this DNS zone (this is the last DNS that hosts this zone)
8. Remove Application Partition
9. <No credentials Provided> Click on Change. When requested, use the acme.com domain administrator username and password

(acme\Anthony.green, AdminP@ss), click Next



Activity: Demoting a Domain Controller

1. Supply New Administrator Password (Use P@ssw0rd)
2. Click Demote
3. The server will restart
4. Log on to the Stand Alone Server as Administrator, P@ssw0rd

Activity: Demoting a Domain Controller

1. In Server Manager Choose Manage
2. Select Remove Roles And Features
3. Click Next until Server Roles
4. Uncheck Active Directory Domain Services, click Remove Features, click Next until Confirmation
5. Click Remove
6. When the process is complete, click Close
7. Restart the Server

• Because AD has been deleted, a new SAM database is created so your Administrative password is reset to P@ssw0rd
• This server is now a stand alone server ready to be used in other capacities

Standalone Server Status

• Now that AD has been removed, your computer is a standalone Windows Server again
• Standalone servers are NOT part of the domain
• Standalone servers maintain their own set of local accounts in SAM
– Check Computer Management and verify the SAM Accounts and Groups
• The system is back to the same status as it had at the very beginning of this module when you first installed the OS

Standalone Server Accounts

• In the upcoming section, this server will be converted to a member server
• To identify some of the key differences between a member server and a standalone server, we will look at the membership of the Administrators group and the Users group for both the standalone server configuration and the member server configuration
• First let's look at the standalone server membership

Activity: Active Directory Administrative Tools

1. Select Start / Administrative Tools
• Note that the three Active Directory Administrative Tools (Active Directory Domains and Trusts, Active Directory Sites and Services, Active Directory Users and Computers) are not present
• During the DC demotion procedure, these tools were removed from the system as they would provide no functionality without being part of a domain

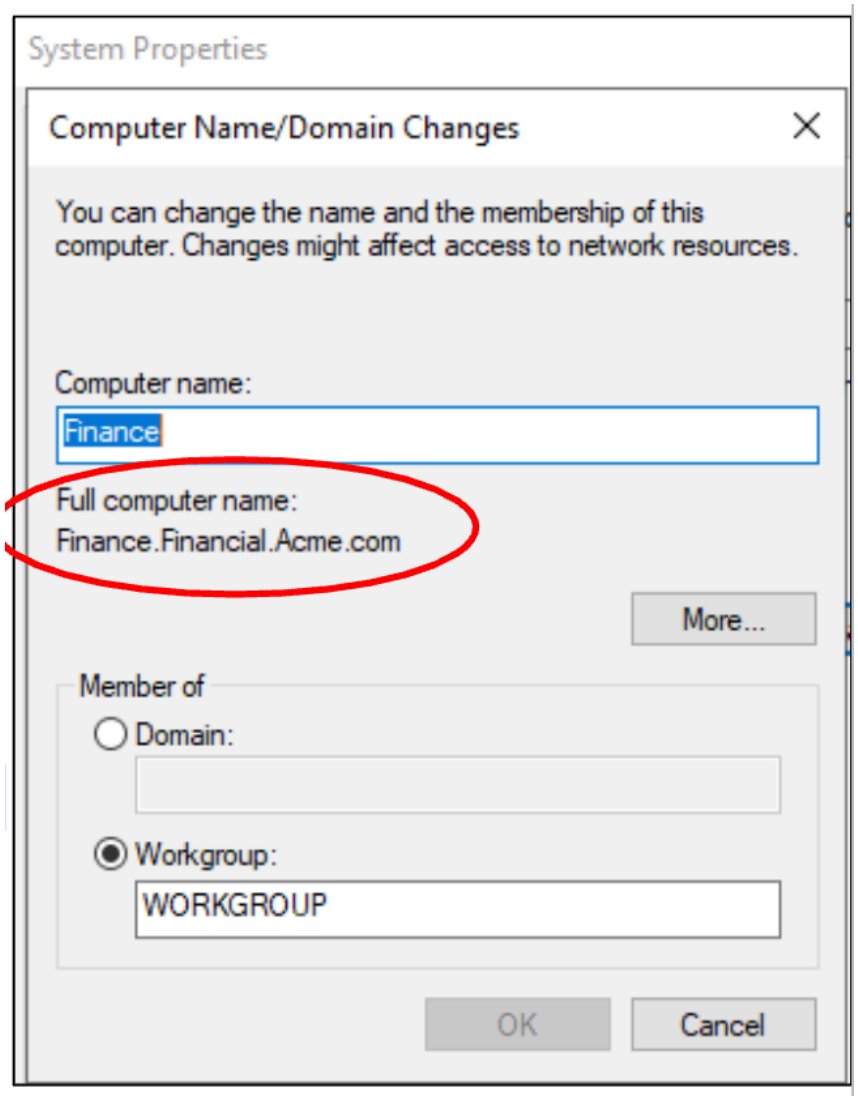
Activity: Standalone Server Users and Administrators Group Membership

1. Open Computer Management

2. Select the Groups folder under System Tools / Local Users and Groups
3. Right click Administrators and select Properties
4. Record the group member(s)
5. Right click Users and select Properties
6. Record the group member(s)
• In a few slides, the standalone server will be converted to a
member server and you will check these memberships again

Activity: Determining the Computer's Name
1. Open File Manager
2. Right-click on ThisPC and choose Properties
3. Under the Computer name, domain, and workgroup settings section you can see the computer name
4. Record the entry beside Full computer name:
-Click Change settings and then select Change
5. Notice that although not in a domain, the full computer name still includes the name of the finance subdomain
6. Click the More button, remove the entry for the Primary DNS suffix and click OK
7. You will need to restart for the name change to

take effect
8. Log back in as Administrator, AdminP@ss and close the Server Manager console



Activity: Trying to Add Domain Accounts to Standalone Servers

Now we will try to add a domain user account to the standalone server's SAM
1. Open in Computer Management, expand Local

Users and Groups and select the Groups folder
2. Right click Administrators and select Properties
3. Click the Add button
4. Look at the locations available in the From this location field
– You should only have access to this local computer (name matches the Full computer name you recorded on the previous page)
– You have no access to domain accounts so they cannot be added
5. Close the console

Converting a Standalone Server to a Member Server

• Domain accounts cannot be added to the SAM account list for a standalone server
• In order to give a domain account access to the standalone server, this system must be converted to a member server
• By joining the domain, a standalone server becomes a member server
• Procedures for joining a domain are identical for both a Windows 10 workstation and a Windows Server 2016 standalone server

Activity: Converting a Standalone Server to a Member Server

1. Right-click the Start menu select Settings

2. Under Related settings select System info (This is an alternate method to see System Properties)
3. Under the Computer name, domain, and workgroup settings section select the Change settings
4. Click the Change button
5. Enter Finance in the Computer name field if the computer name is not already Finance
6. Select the Domain radio button and enter acme.com as the domain name
7. Click OK
7. When prompted, enter the Anthony.Green user name (password is AdminP@ss)
8. Click OK at the “Welcome to the acme.com domain” window
9. You must restart the compute Click Close and the Restart Now
• This system is now configured to be a member server

Determining Membership Changes

• Earlier you identified the default membership for the Administrators and Users groups on a standalone server
• Now that this system is a member server, we want to see if there are changes to these group memberships

• Earlier you identified the default membership for the Administrators and Users groups on a standalone server
• Now that this system is a member server, we want to see if there are changes to these group memberships

Activity: Determine Which Domain Accounts are added to Member Servers

1. At the logon window, use the local Administrator account with the P@ssw0rd password
2. Open Computer Management and select the Groups folder located under
System Tools / Local Users and Groups
5. Right click Administrators and select Properties
6. Record the group members not listed before
7. Right click Users and select Properties
8. Record the group members not listed before

Activity: Add Domain Accounts to Member Servers

• Earlier we tried to add a domain user account to the standalone server's SAM but it was NOT allowed
• Now we will repeat this on a member server
1. While in Computer Management, select Local Users and Groups then select Groups
2. Right click Administrators and select Properties
3. Click the Add button

4. Look at the locations available in the From this location field

– Now that this computer is part of the domain, you can give domain accounts access to this computer by adding them

5. Because you are now logged on using a local account that doesn't have domain permissions, you will be prompted to enter a user name and password with this authority – enter the acme.com administrator name and password (Anthony.Green, Adminp@ss)

6. Set the From this location: to acme.com

– If you had been logged on with the acme domain administrator account when attempting this last activity, you would NOT have been prompted for a user name and password when adding an account

7. Enter tony.green in the Enter the object names to select field

8. Click on Check Names

9. Click OK then Apply to save the changes

10.Close the console

Tony.Green Account Status

• The tony.green account is an existing account on the acme.com domain

– You will use this account in many of the subsequent labs

• tony.green now has the same authority on this member server as that of the local administrator and the domain administrator account

– A member of the Administrators group for this local computer

– NOT a member of the domain Administrators group

Activity: Confirming Tony.Green has Authority on the Member Server

1. Log off and log back on using Other User as Anthony.green@acme with the AdminP@ss password. (make sure that the acme domain is used)

• Because this is the initial logon to this computer for the Anthony.green account it will have a new user profile which includes a fresh Desktop, My Documents folder and other default startup policy settings

• Because of this new policy, the Server Manager console will also start

2. Close the Server Manager console

Activity: Confirming Tony.Green has Authority on the Member Server

• To verify the domain account Anthony.Green has administrative control of this member server, we will

use it to create a user account
1. Start Computer Management
2. Expand the Local Users and Groups folder
3. Right click the Users folder
4. Select New User and enter a user name and password of your choice
    – Password must meet the password complexity rules
    – You should be successful in creating this account
5. Close the New User dialog box
    – The New User dialog box remains open for adding more users
6. Close the console

Account Database Storage

Server Type

Domain Controller
Member Server
Standalone Server

Account Storage Location

Active Directory database
SAM database
SAM database

• SAM accounts only provide access to the computer

on which the SAM is stored
• Active Directory accounts provide access to resources across the domain system

Supplemental Content

• The Supplemental Content document for this module (located on the course web page) includes the following:
– Questions that can be answered by performing the Activities in this module
– Questions related to the theory covered in this module
– Questions from the reading assignments
– A list of hands on tasks covered in the module
• You are responsible for knowing all of this information