

Installation and Configuration of a Windows Server 2016 Domain Controller

**MOREnet Annual Conference
October 2017**

Presented By:

Stephanie Hanson
hansonsj@more.net

&

Jim Long
long@more.net

Contents

CONTENTS	2
INTRODUCTION	4
SECTION I: INSTALLING WINDOWS 2016 SERVER SOFTWARE	5
MUST-READ LINKS!	5
BEST PRACTICES	5
SECTION II: WINDOWS SERVER 2016 INITIALIZATION	16
SECTION III: WELCOME TO SERVER MANAGER	20
NAVIGATING SERVER MANAGER	21
Server Manager Console Header:	21
The Notifications Area:	21
Manage:	22
Tools:	23
View:	24
Help:	24
MANDATORY CONFIGURATIONS	25
Set the Time Zone	25
Setup the Network Card(s)	28
Change the Computer Name	31
Windows Update	33
Enable Remote Desktop	37
SECTION IV: BUILDING A DOMAIN CONTROLLER	39
DEFINITIONS	39
MUST-READ LINKS!	39
INSTALLING ACTIVE DIRECTORY DOMAIN SERVICES	40
The Wizard	41
PROMOTING YOUR SERVER TO A DOMAIN CONTROLLER	47
Naming Considerations for Your Domain	47
The Wizard	48
SECTION V: CUSTOMIZING YOUR DOMAIN CONTROLLER	57
MUST-READ LINKS!	57
ADMINISTRATOR ACCOUNTS	57
Create a New Administrator Account	59
Add Your New Administrator Account to the Built-In Administrators Security Group	61
Secure the Built-in Administrator Account	62
ADDRESSING ERRORS	65
Troubleshooting Tools	70
DNS SERVER CONFIGURATION	71
Definitions	71
Must-Read Links!	73
Navigating DNS Server Properties	74
Interfaces Tab	75
Forwarders Tab	75
Advanced Tab	76

<u>Root Hints Tab</u>	<u>77</u>
<u>Debug Logging Tab</u>	<u>78</u>
<u>Event Logging Tab</u>	<u>78</u>
<u>Monitoring Tab</u>	<u>79</u>
<u>Security Tab</u>	<u>79</u>
<u><i>Navigating Forward Lookup Zones</i></u>	<u>80</u>
<u>General Tab</u>	<u>81</u>
<u>Start of Authority Tab</u>	<u>83</u>
<u>Name Servers Tab</u>	<u>84</u>
<u>WINS Tab</u>	<u>84</u>
<u>Zone Transfers Tab</u>	<u>85</u>
<u>Security Tab</u>	<u>85</u>
<u><i>Creating Reverse Lookup Zones</i></u>	<u>86</u>
<u>The Wizard</u>	<u>87</u>
<u><i>Creating Conditional Forwarders</i></u>	<u>91</u>
<u>SECTION VI: SECURITY POLICIES FOR WINDOWS SERVER 2016</u>	<u>93</u>
<u>MUST-READ LINKS!</u>	<u>93</u>
<u>GROUP POLICY MANAGEMENT</u>	<u>95</u>
<u>PASSWORD POLICIES</u>	<u>97</u>
<u>AUDIT POLICY CONFIGURATION</u>	<u>104</u>
<u>USER RIGHTS ASSIGNMENT</u>	<u>109</u>
<u>SECURITY OPTIONS</u>	<u>112</u>
<u>EVENT LOG POLICIES</u>	<u>116</u>
<u>RESTRICTED GROUPS</u>	<u>118</u>
<u><i>Create a New Security Group to Manage Workstations & Member Servers</i></u>	<u>118</u>
<u><i>Add Administrative Users to the New Security Group</i></u>	<u>119</u>
<u><i>Create Your Local Administrator Group Policy</i></u>	<u>120</u>
<u>SYSTEM SERVICES</u>	<u>124</u>
<u><i>System Services Example Configuration</i></u>	<u>126</u>
<u>REGISTRY POLICIES</u>	<u>132</u>
<u>FILE SYSTEM PERMISSIONS</u>	<u>138</u>
<u>WIRELESS NETWORK POLICIES</u>	<u>139</u>
<u>SECTION VII: HOSTS FILE GPO</u>	<u>140</u>
<u>MUST READ LINKS!</u>	<u>140</u>
<u>CREATE A SHARE</u>	<u>141</u>
<u>The Wizard</u>	<u>142</u>
<u>DOWNLOAD THE CURRENT MVP HOSTS FILE</u>	<u>156</u>
<u>CREATE THE GPO</u>	<u>158</u>
<u><i>Disable the DNS Client Services</i></u>	<u>159</u>
<u><i>Deploy the Hosts File GPO with Group Policy Preferences</i></u>	<u>161</u>
<u>TEST, TEST, TEST!!</u>	<u>163</u>

Introduction

This document is intended as a step-by-step guide for installing and setting basic security settings for a Domain Controller.

We will walkthrough basic settings and configurations, giving you a starting point to create and maintain a secure Windows 2016 Domain Controller. We advise you use this guide in addition to other available guides, supplementing this information with strategies outlined on the Microsoft Security site as well as SANS, NSA and NIST. This will improve the security of your domain.

Do not consider your domain, or computers in your domain invincible from hacking, viruses or worms because you set certain policies discussed in this guide. You must also keep current service packs, updates, hot-fixes and security patches applied to the all systems on your network. Not merely Servers, but also Workstations and any other network devices.

Following Microsoft best practices for security will reduce the chances of security breaches, but maintaining good practices, end-user communication, and thorough documentation for your own environment is an absolute necessity!

We hope you enjoy this document!

Section I: Installing Windows 2016 Server Software

MUST-READ LINKS!

Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/windows-server-2016>

System Requirements for Windows 2016 Server

<https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements>

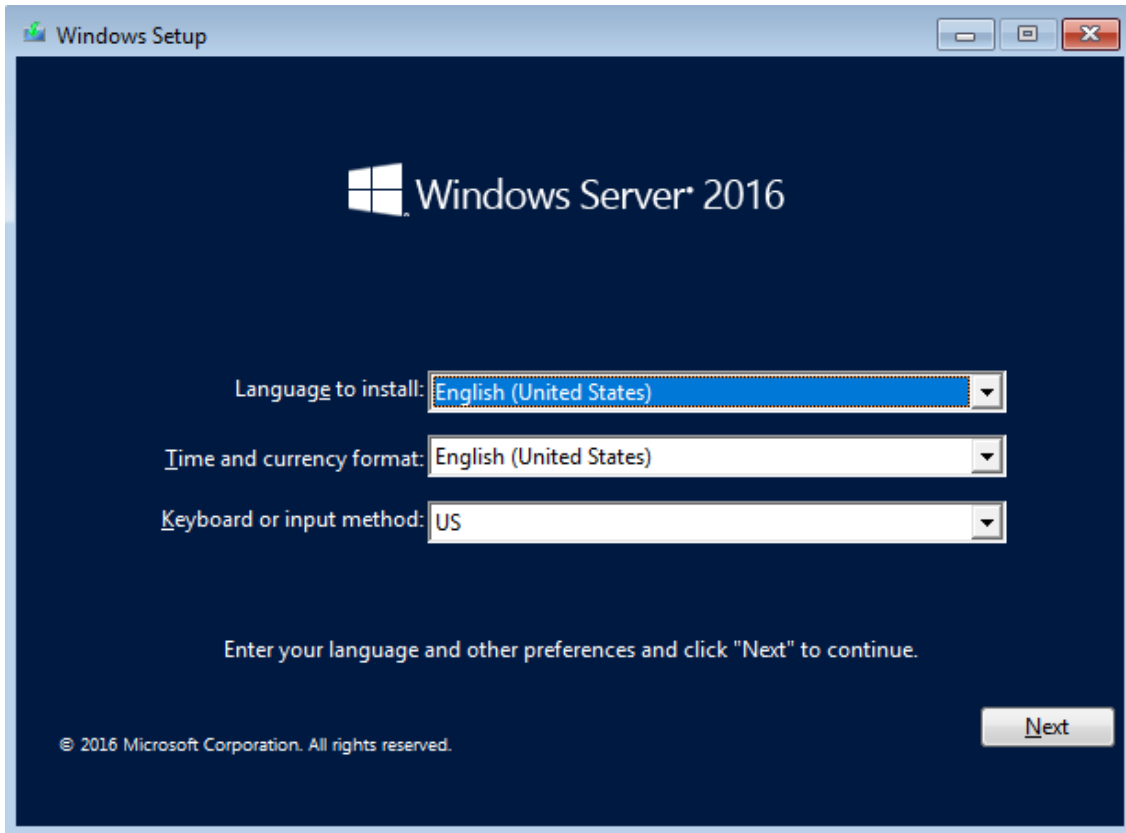
Important Issues in Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/get-started/windows-server-2016-ga-release-notes>

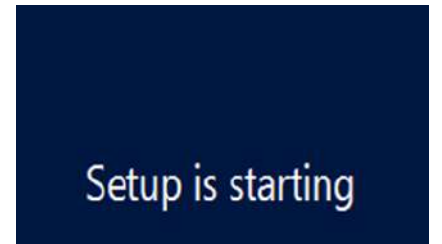
BEST PRACTICES

- Never install a new system on the public network.
- Start system in a development environment then move system to your production network.
- Patch system immediately after installation.
- Apply all security settings to system.
- Configure Host Based Firewall.
- Install and update Anti-Virus software.
- Verify all settings.
- When upgrading or reloading a system, perform a full backup prior to installation.

1. Turn on system and insert installation disk
 - a. If the Startup Sequence in the BIOS hasn't been set to boot from the CD/DVD drive, you will want to change these settings prior to starting your installation

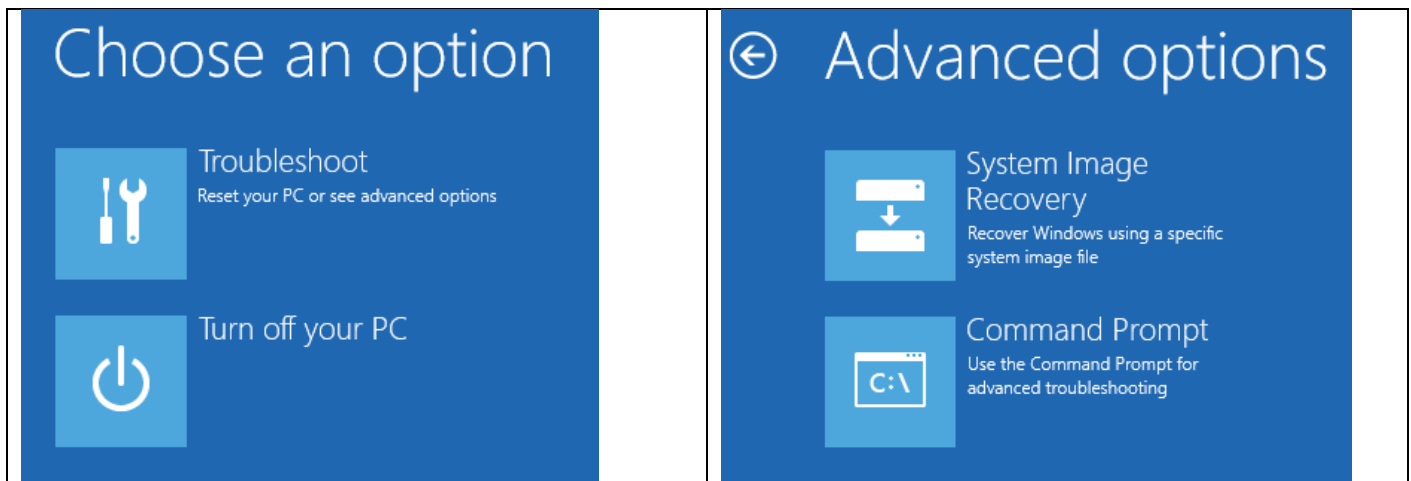


2. Choose Language, Time and currency format and Keyboard input method.
3. Click Next.



a. You will receive a message “Setup is starting”.

4. Click Install now.



b. The installation iso can also be used to Repair Your Computer.

i. If you select Repair your computer from the Windows Setup screen above, you will be asked to Troubleshoot or Turn off your PC.

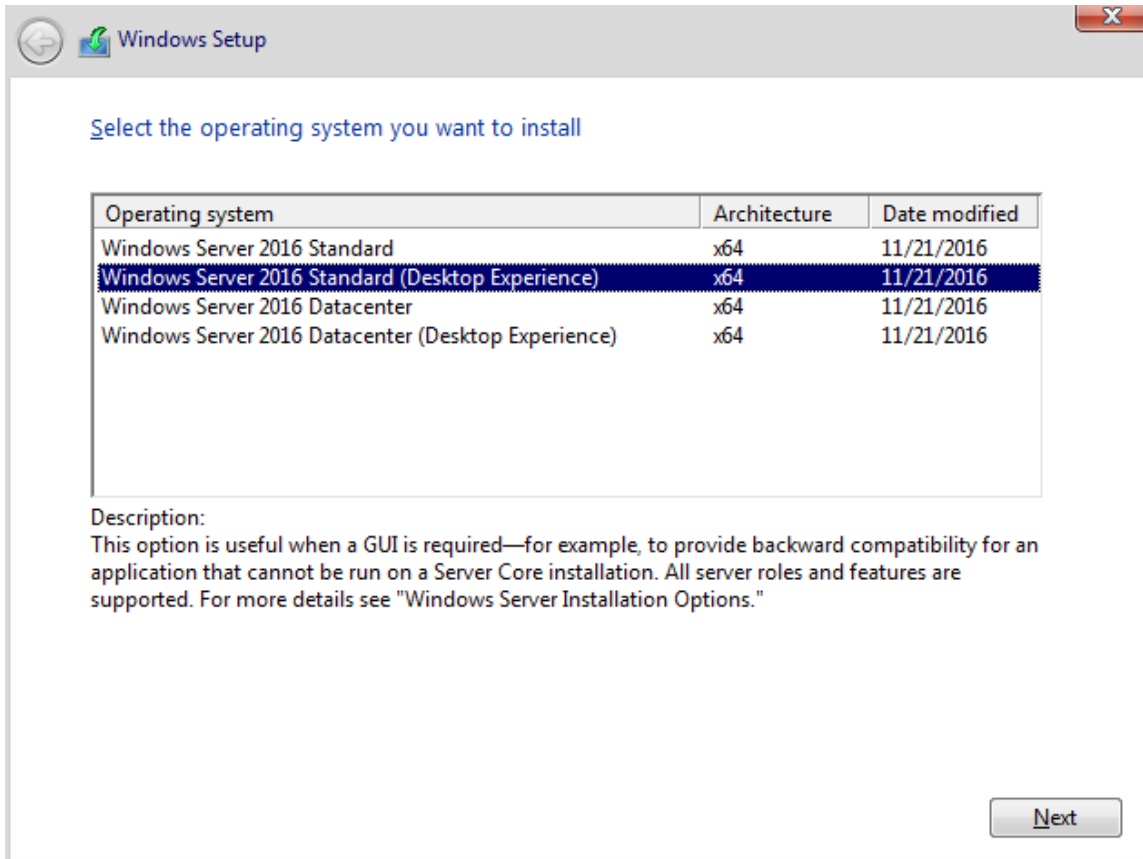
ii. If you select Troubleshoot, either you can browse for a System Image file to Recover Windows, or you can launch a Command Prompt.

iii. Review the Microsoft documentation:

Recover the Operating System or Full Server (referencing Windows Server 2008 R2),

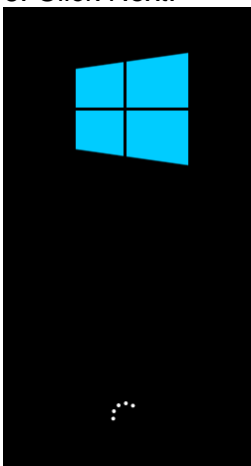
<https://technet.microsoft.com/library/cc755163.aspx>

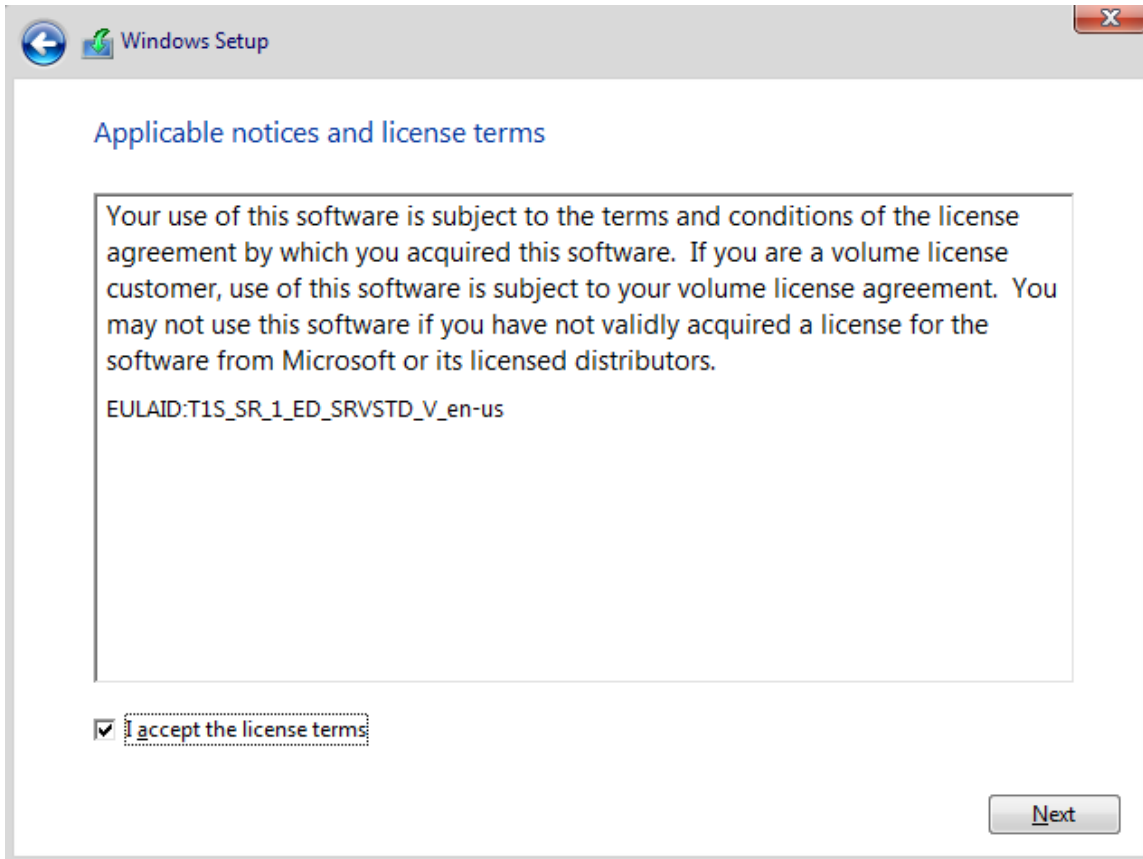
Wbadm Start sysrecovery, [https://technet.microsoft.com/en-us/library/cc742118\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc742118(v=ws.11).aspx)



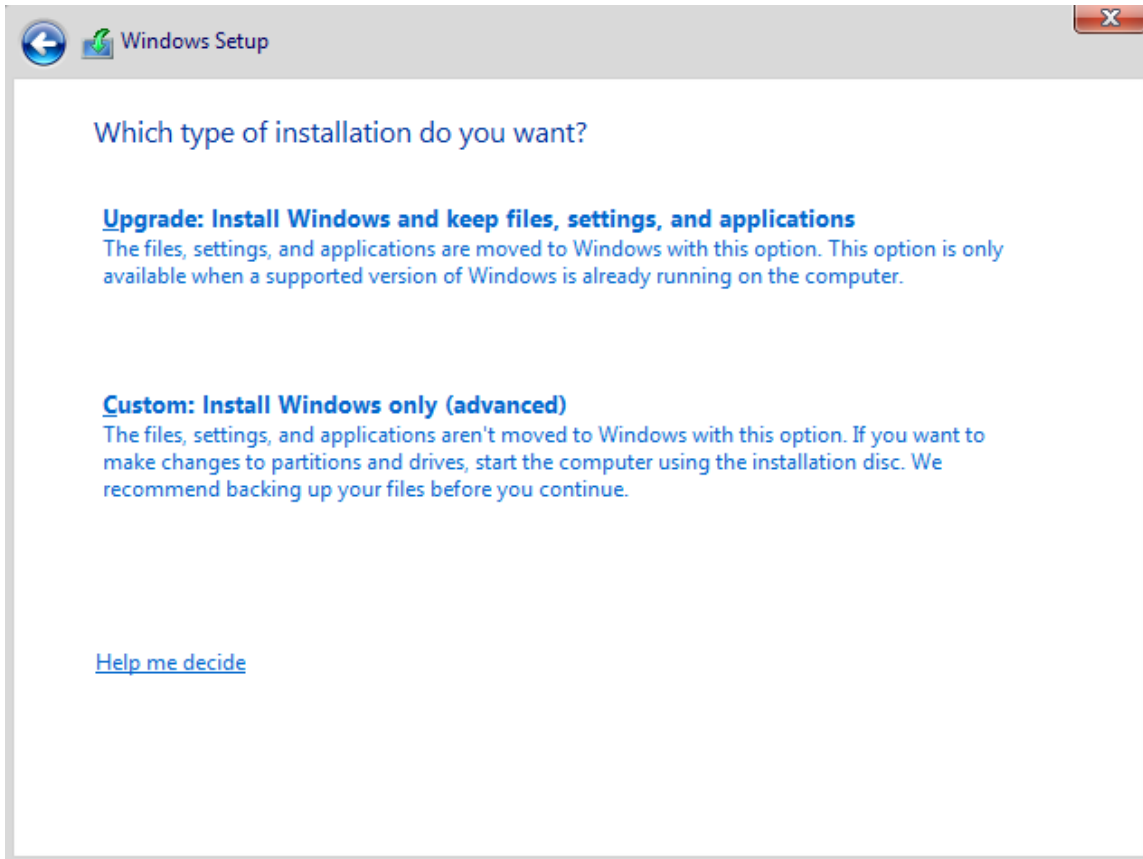
5. Select the operating system you want to install.
 - a. The default selection is Windows Server 2016 Standard. This is the Server Core Edition which is managed via Command Line, Powershell, or Remotely. Server Core is the Microsoft recommended option.
 - b. Windows Server 2016 Standard (Desktop Experience) loads with the graphical interface.
 - c. If you want to switch from either operating system option, you cannot convert from one to the other. You must perform a complete re-install.

6. Click Next.

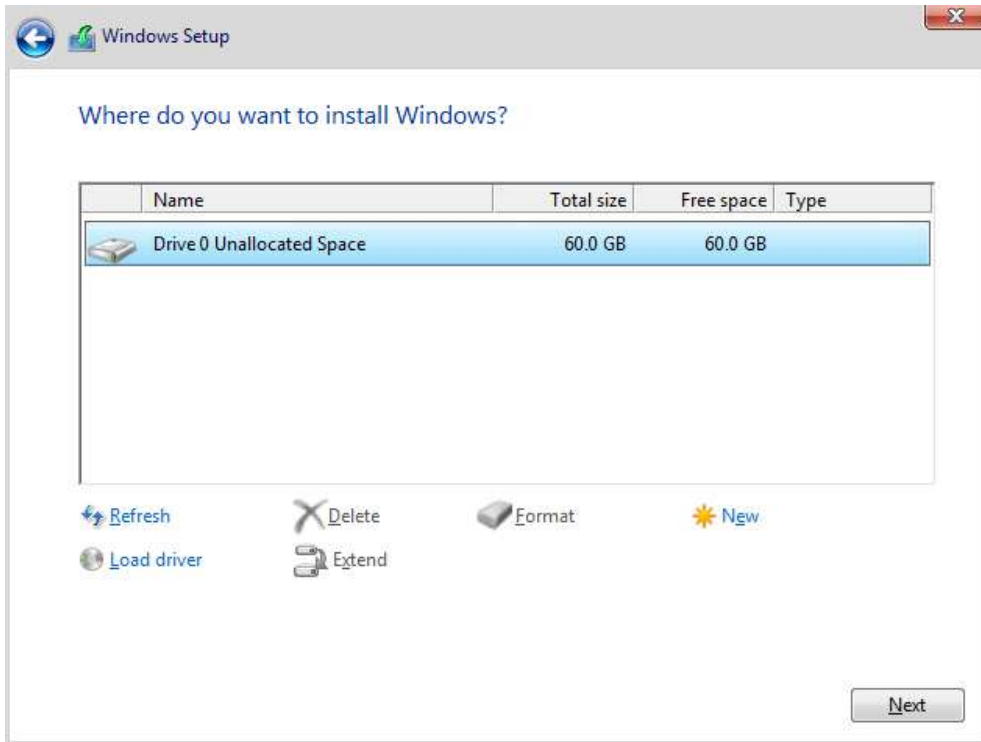




7. Please read the license terms.
 - a. Make sure to read and accept the licensing terms prior to installation.
 - b. You cannot proceed without checking the box accepting the license terms.
8. Click Next.



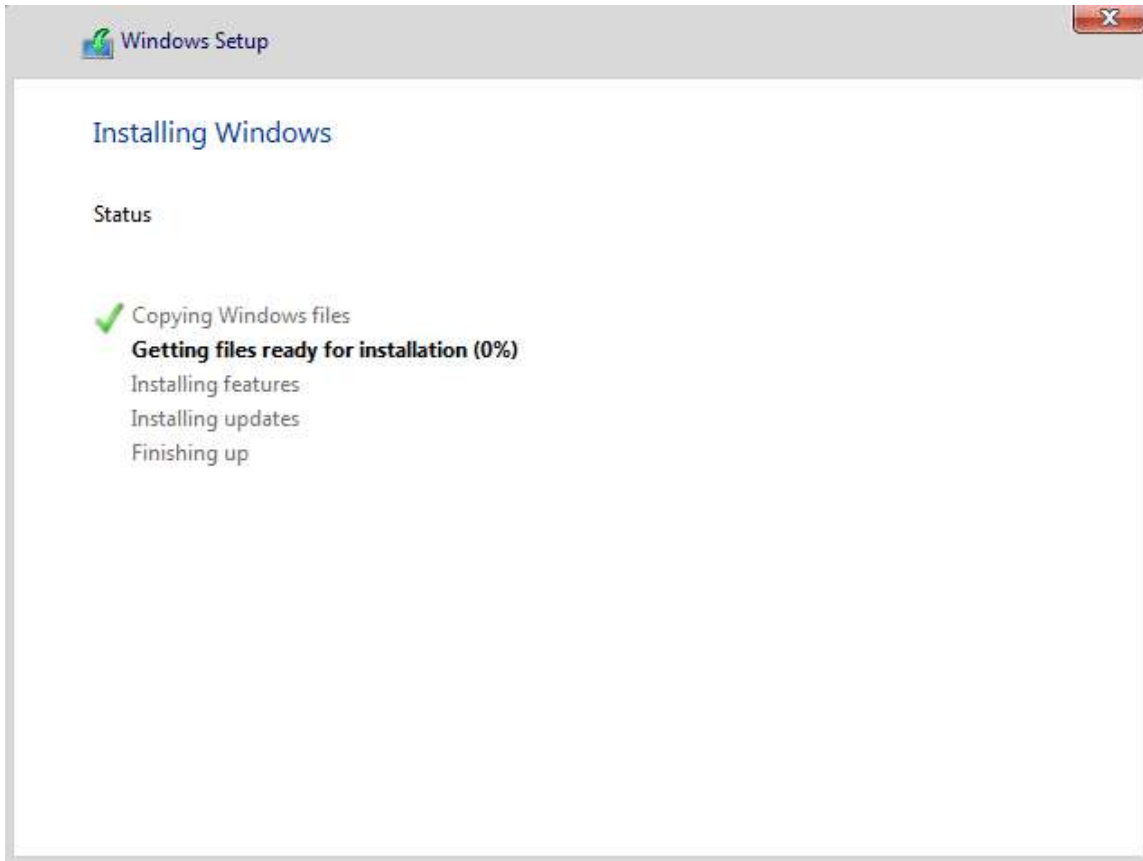
9. Which type of installation do you want?
- a. Upgrade
 - i. This option is used when upgrading from a previous version of Windows.
 - ii. All files, settings and programs will be kept intact.
 - b. Custom
 - i. This option is used to install a new copy of Windows
 - ii. This will erase the drive and any data that is on it.
10. This is a new install, Click Custom: Install Windows only



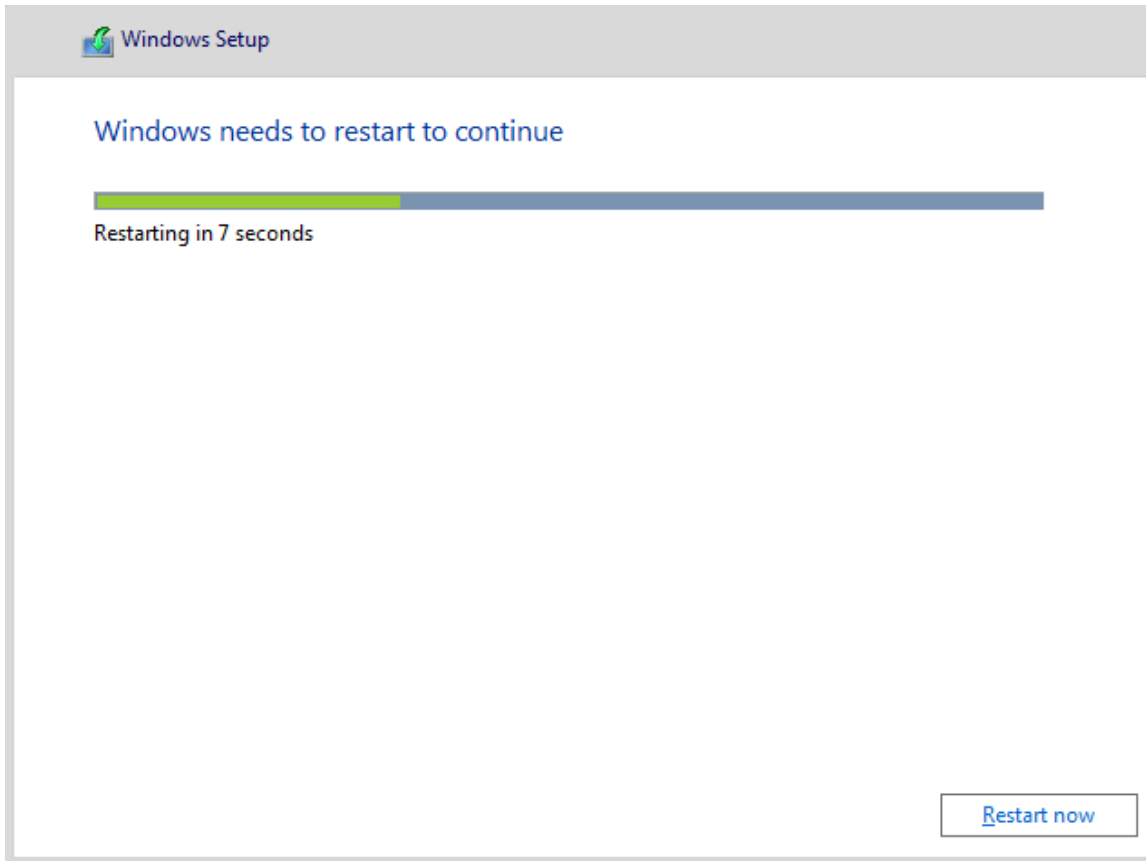
11. Where do you want to install Windows?
 - a. Choose the drive that you want to use to install Windows.
 - b. If the hard drive is not detected, you must load the proper drivers.
 - i. Click Load Driver



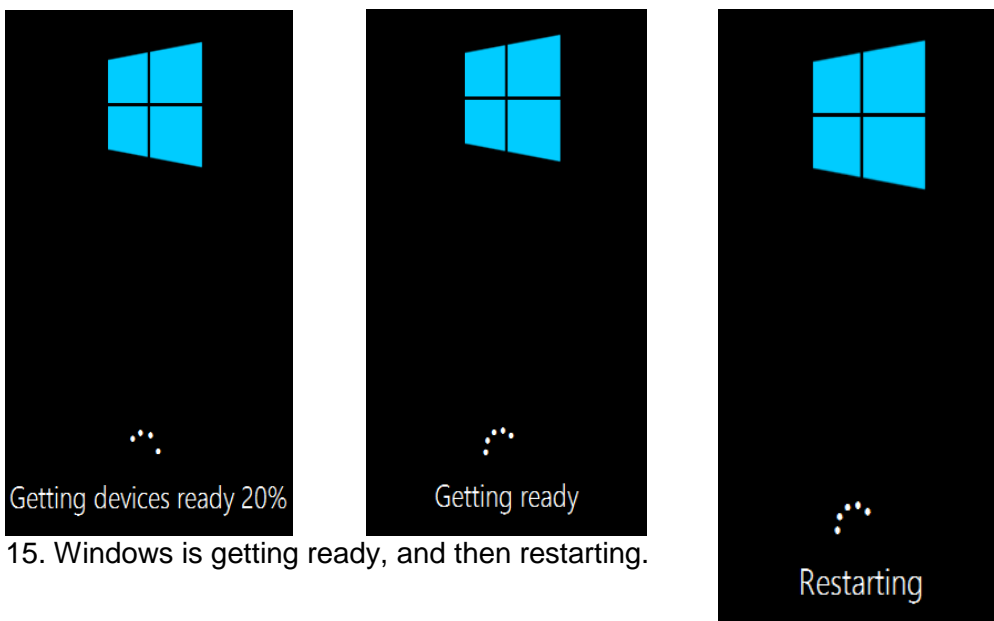
- ii. The driver can then be loaded from CD, DVD or USB drive.
 - iii. Once the driver is loaded the hard drive will be listed as an option in the installation wizard.
 - c. Additional Options (Delete, New, Extend, Format)
 - i. You can delete the current partition
 - ii. Create a New Partition
 - iii. Extend the partition, which allows you to make the partition larger. **This action cannot be reversed!**
 - iv. Format the partition
 - d. If this is a new disk, no other action needs to be taken. Clicking next will automatically create a partition using the entire disk, format and start the installation.
12. Click Next.



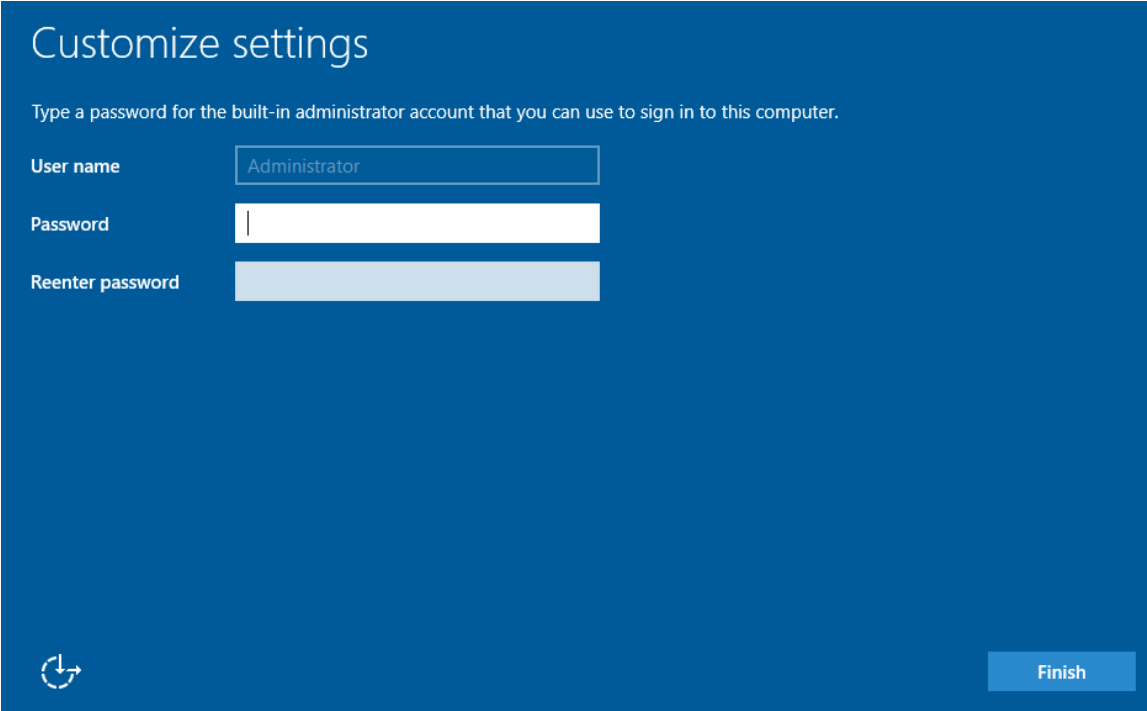
13. Installing Windows.



14. Windows restarts to complete installation.



15. Windows is getting ready, and then restarting.




Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name

Password

Reenter password

 Finish

16. Enter the password for the Built-in Administrator account.

17. Make sure to follow your organization's best practices and password policy.

a. To resist brute force attacks, your password would need to be 18-20 characters long.

b. Additional information provided by Microsoft here: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

18. Click Finish.

19. Your Password has been set.



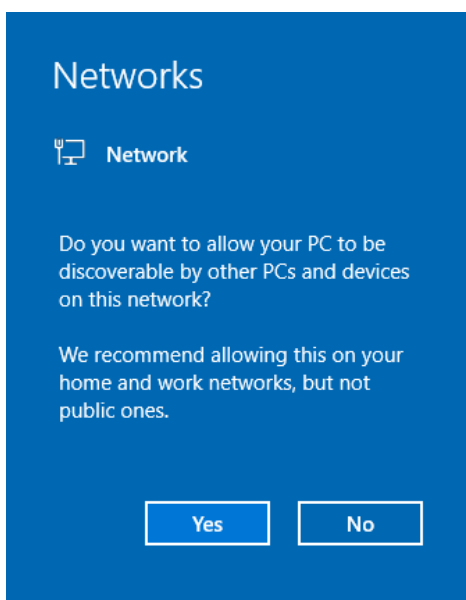
20. *The initial installation is now complete.*

In the next section, we will walk through installing updates and applying default security settings to the system. We recommend you perform these tasks in a non-production environment on a private NAT or firewalled network.

Section II: Windows Server 2016 Initialization

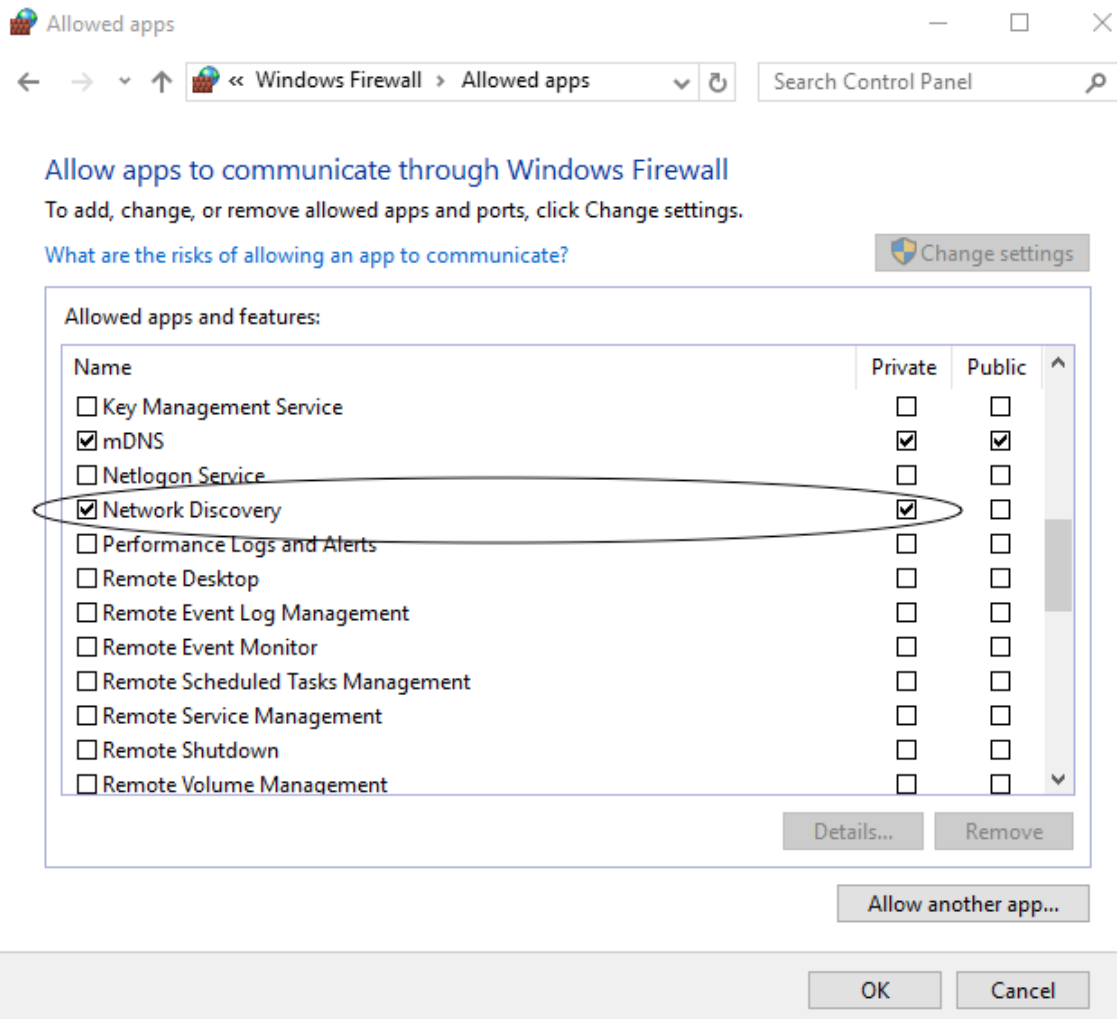


1. Log into the Administrator account using the password created during installation.

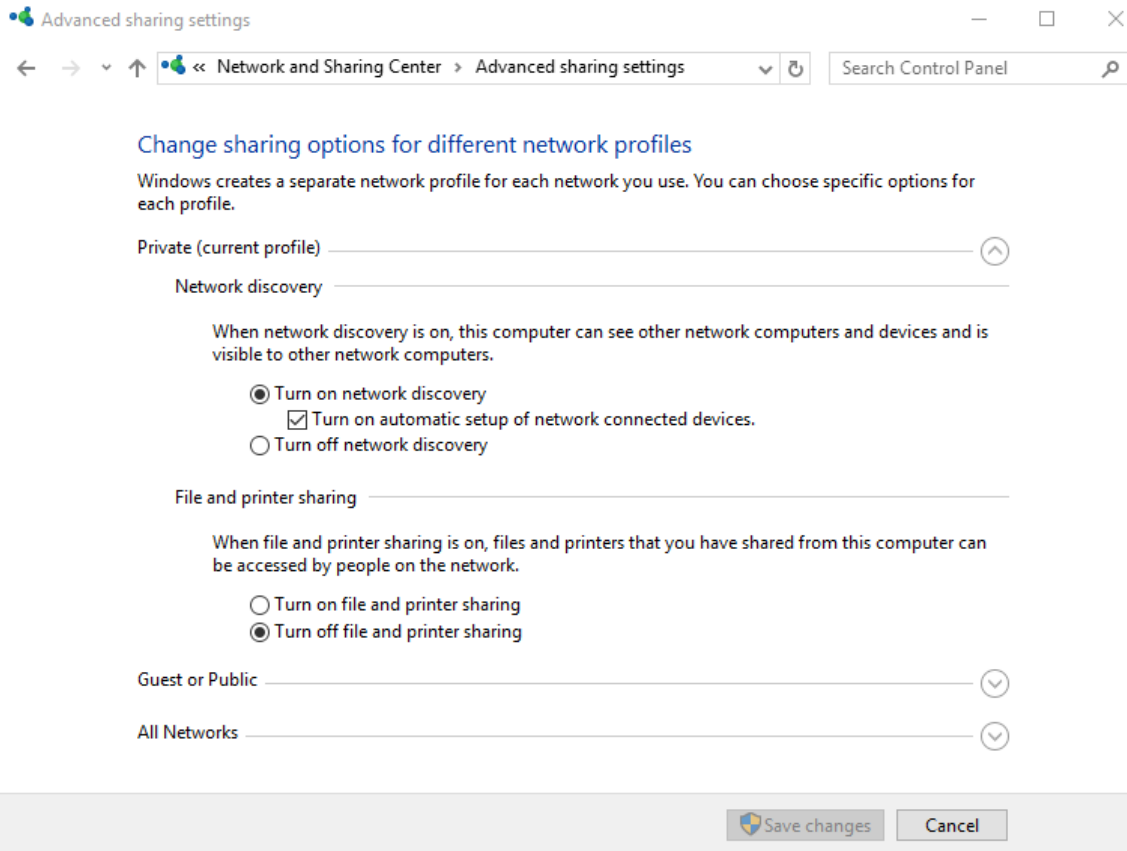


2. First, a prompt appears, asking if you want to allow Network Discoverability.

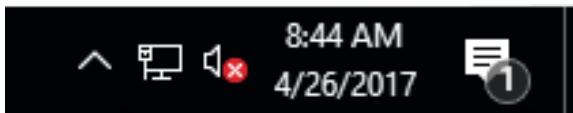
a. This enables the allowed computer to be viewable by other computers on the network.



b. If you click Yes, you will enable the Network Discovery application in the Windows Firewall for the Private network only (refer to the checkboxes in the image on the previous page). This setting is accessible from Control Panel > Windows Firewall > Allow an app or feature through Windows Firewall.



- c. If you click No, or miss the dialogue, this option is reconfigurable.
 - i. Go to Control Panel > Network and Sharing Center. Click Change advanced sharing settings from the left menu options.
 - ii. Customizable for Private, Guest or Public, and All Networks.
 - iii. You may also need to go back to the Windows Firewall, and enable Network Discovery, as indicated by the previous instruction.



3. You will also notice a notification in the system tray.



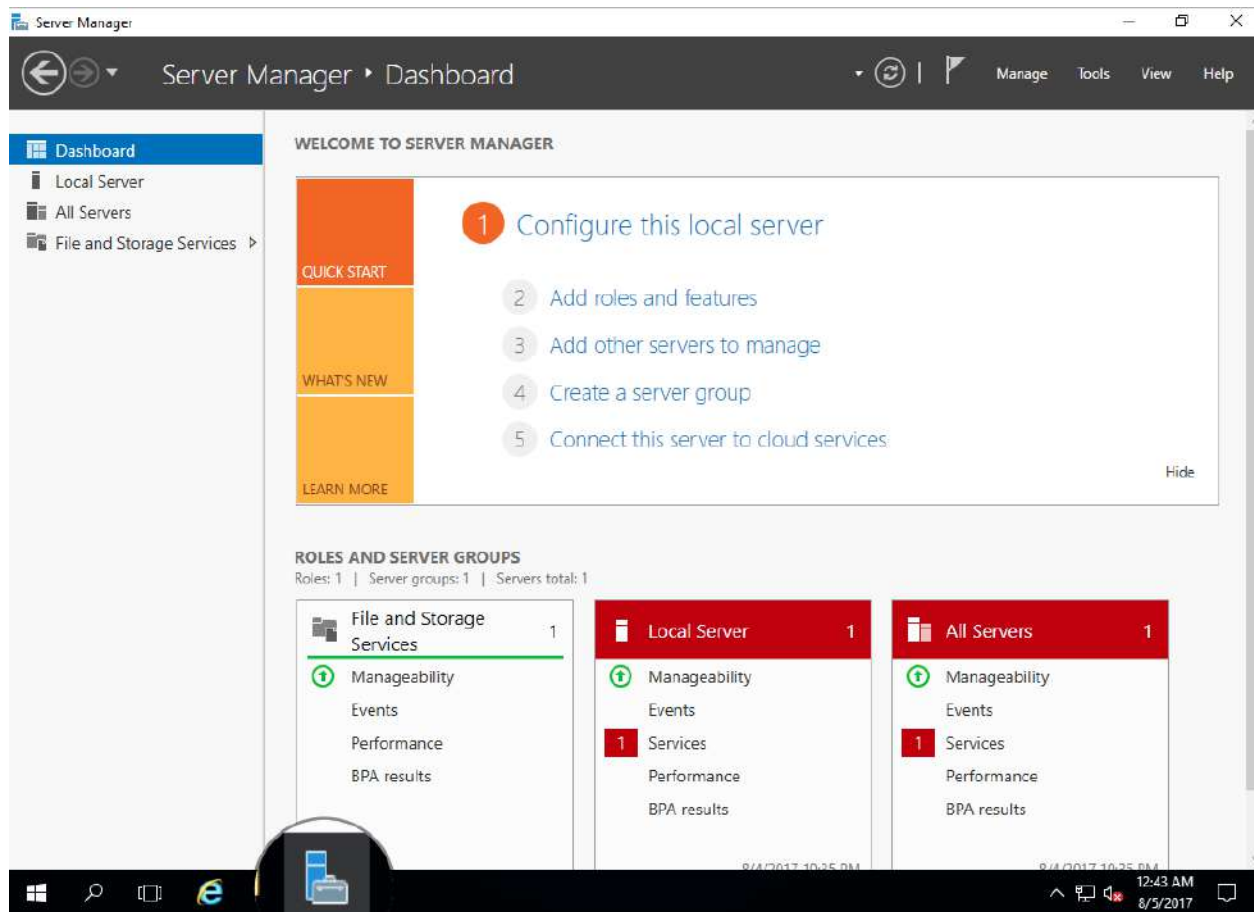
4. This is a notification from the Action Center to Turn on the [Windows SmartScreen](#).
- Windows SmartScreen is disabled by default, and is enabled using a domain administrator account through Group Policy.
 - Windows SmartScreen works with Internet Explorer and Microsoft Edge web browsers, comparing the URL of visited websites to a list of high traffic websites that are integrated with the filter. If the website does not match the list, the SmartScreen filters sends a query to the corresponding URL Reputation Service. If the URL had been determined unsafe, the filter displays a message to the user to warn them about entering personal data or downloading content from the site.
 - Telemetry is used to report additional information about the site.
 - An IPv4 connection is required to utilize software.

While you are working with these initial dialogues, the Server Manager is loading in the background. Introduced in Windows Server 2008, Server Manager remains the primary information and central management console for Windows Server 2016.



NOTE: Until you activate your copy of the Windows Server operating system, this message will appear on the bottom right corner of your desktop.

Section III: Welcome to Server Manager



The Server Manager Dashboard screen provides, at a glance, all roles installed on the server, and will notify you of any errors or concerns. It also offers a Quick Start menu of hyperlink options.

To manage servers running operating systems older than 2016, you must install the following software and updates on the remote server(s): <https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager>

1. Click (1) Configure this local server to view to edit the Server Properties, or click Local Server from the left menu pane. The configuration options include:
 - Computer Name
 - Workgroup/Domain
 - Windows Firewall
 - Remote Access Option
 - Configure Windows Updates
 - Set the time/time zone
 - See operating system and hardware details
 - View Events

- Access Services
- Run the Best Practices Analyzer
- View Performance details
- View and Edit Roles and Features

2. Add roles and features, launches the wizard to add or remove roles or features to your server.
3. Add other servers to manage (up to 100, depending on the hardware and network resources available to the server), adds domain and workgroup servers using one of three methods (see <https://docs.microsoft.com/en-us/windows-server/administration/server-manager/add-servers-to-server-manager>):
 - a. Active Directory
 - b. DNS
 - c. Import
4. Create a server group, allows you to group like systems logically, to monitor and manage. For example, a group of Database servers, an IIS group or a group of File Servers and so on.
5. Connect this server to cloud services, launches a browser to load the website, <https://www.microsoft.com/en-us/cloud-platform/operations-management-suite>.

NAVIGATING SERVER MANAGER

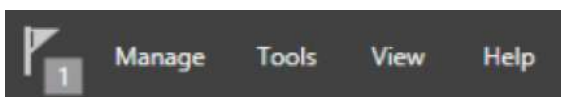
Getting to know the Server Manager in 2016 is one key to successfully manage your servers. Let's get familiar with the features!

Server Manager Console Header:

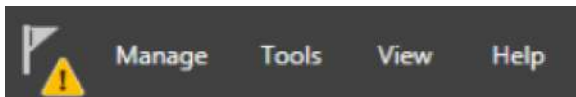


Along the top of the Server Manager you will find arrows and breadcrumb for navigation on the left. On the right, there is a refresh button, notification flag for tasks that are completed or pending, and other menu options so you can quickly manage your servers, access tools, change your view or search help documentation.

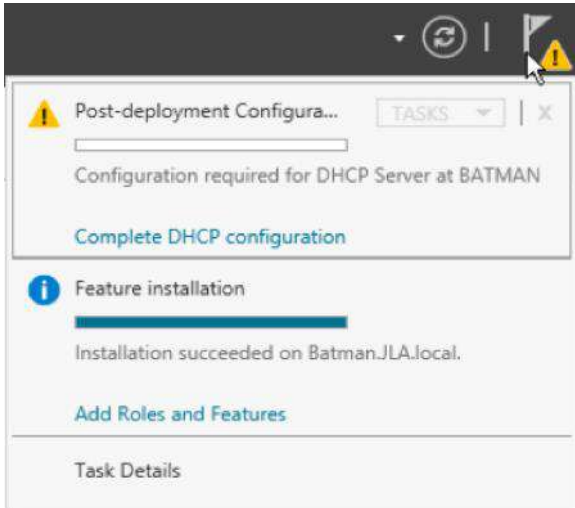
The Notifications Area:



The flag icon represents the Notifications Area and will display Task Details that are in progress, pending, or require additional actions. A number beside this icon indicates there are pending messages.

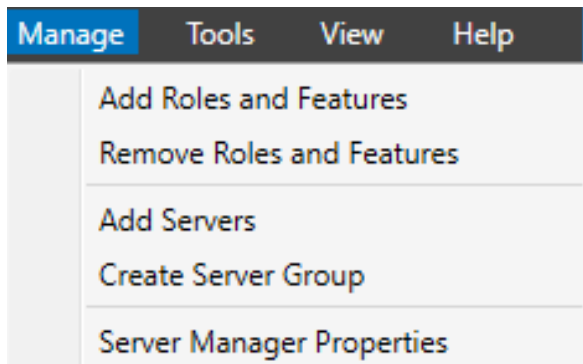


If a Warning Triangle appears this means there are pending tasks that require your immediate attention.



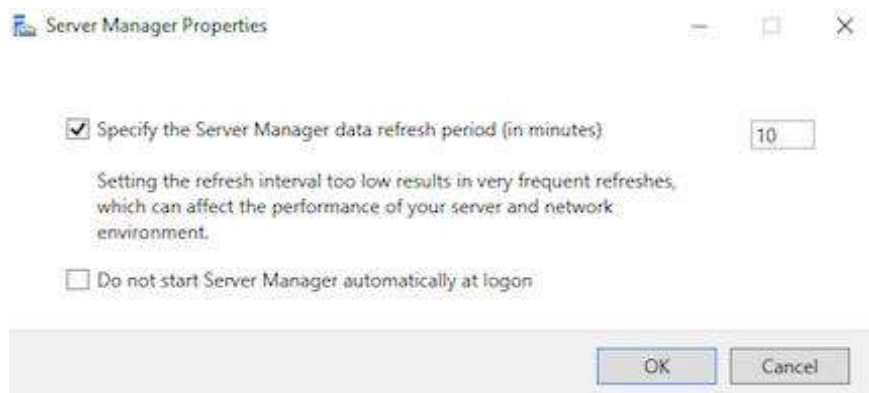
Clicking on the Flag displays progress of the pending event as well as a link to more information. To complete pending tasks, a link guides you to the next step.

Manage:



The Manage Menu gives you the option to:

- Add Roles and Features
- Remove Roles and Features
- Add Servers
- Create Server Group
- Server manager Properties



Default Settings (above):

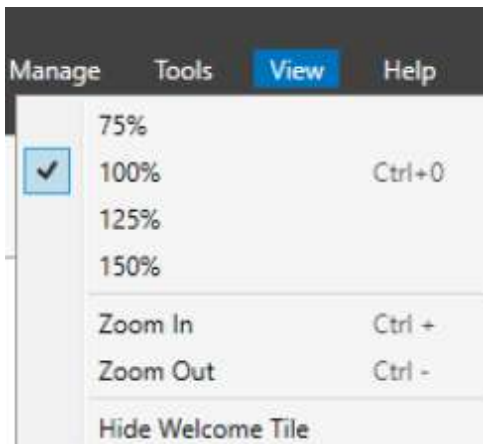
Tools:

Default Available Tools:



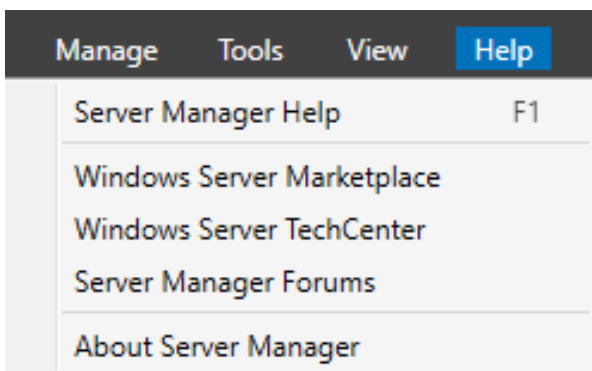
The Tools Menu gives you direct access to the Administrative Tools shortcuts. This is the fastest method to access your management tools. As you install more Roles and Features on the server, additional shortcuts appear in this menu. The Tools Menu is also customizable. Review management options here: <https://docs.microsoft.com/en-us/windows-server/administration/server-manager/manage-the-local-server-and-the-server-manager-console>

View:



The default View for Server Manager is set at 100%. Change the magnification of your Server Manager here.

Help:

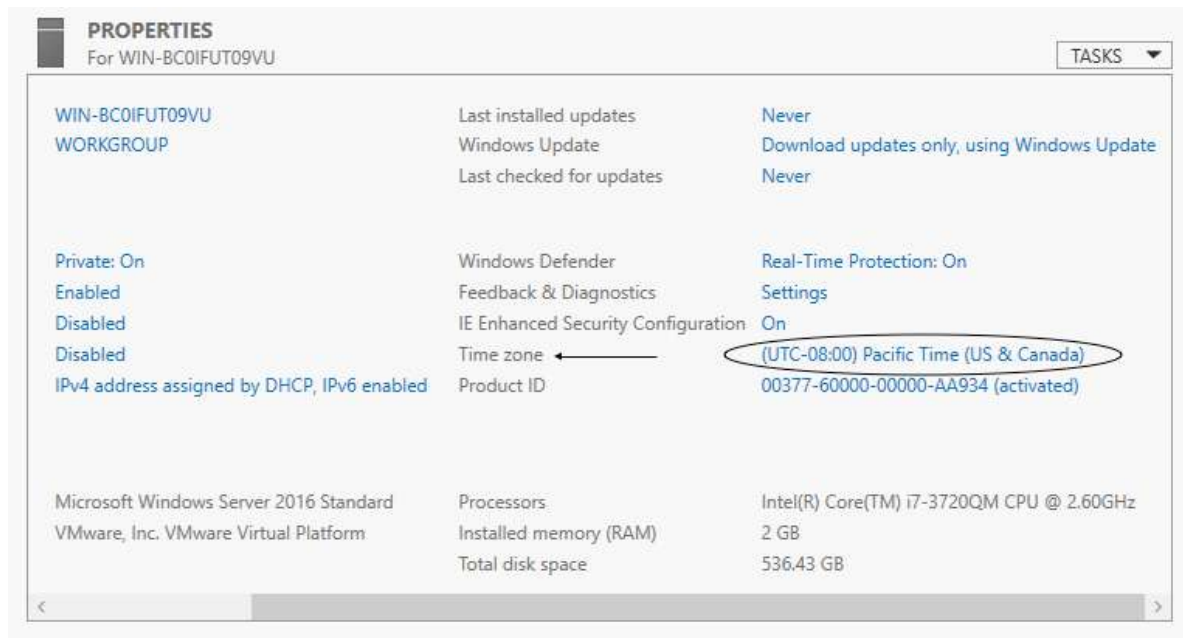


The Server Manager Help option launches the default browser to a Technet article, <https://technet.microsoft.com/library/2194da26-7e64-4497-b4ee-c2d815f655c0>. Windows Server Marketplace takes you here, <https://www.windowsservercatalog.com>. Windows Server TechCenter launches this, <https://technet.microsoft.com/en-us/library/hh831456>.

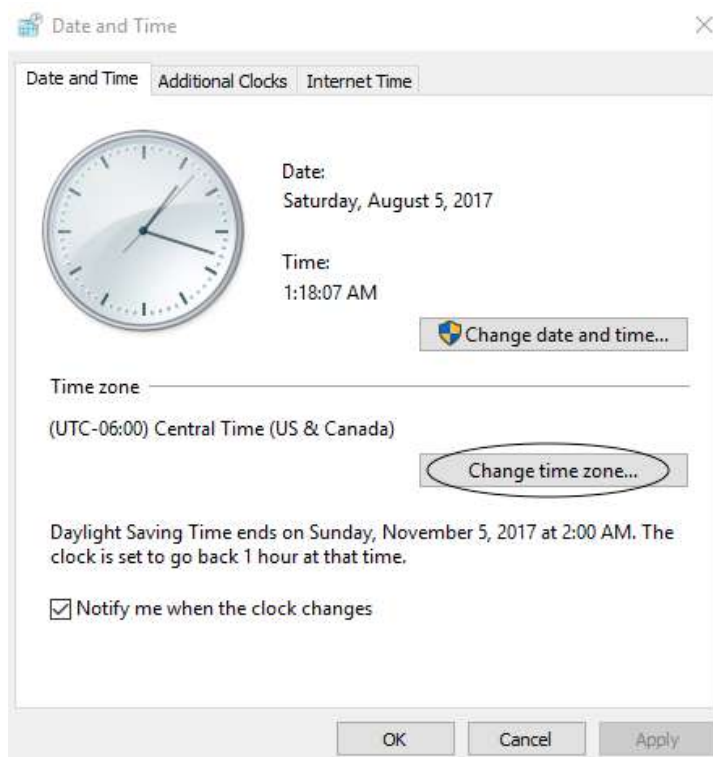
MANDATORY CONFIGURATIONS

Set the Time Zone

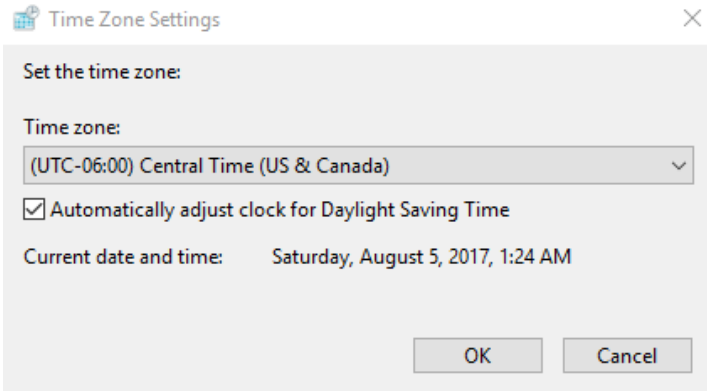
1. From the Server Manager Dashboard, click Local Server from the left menu pane.



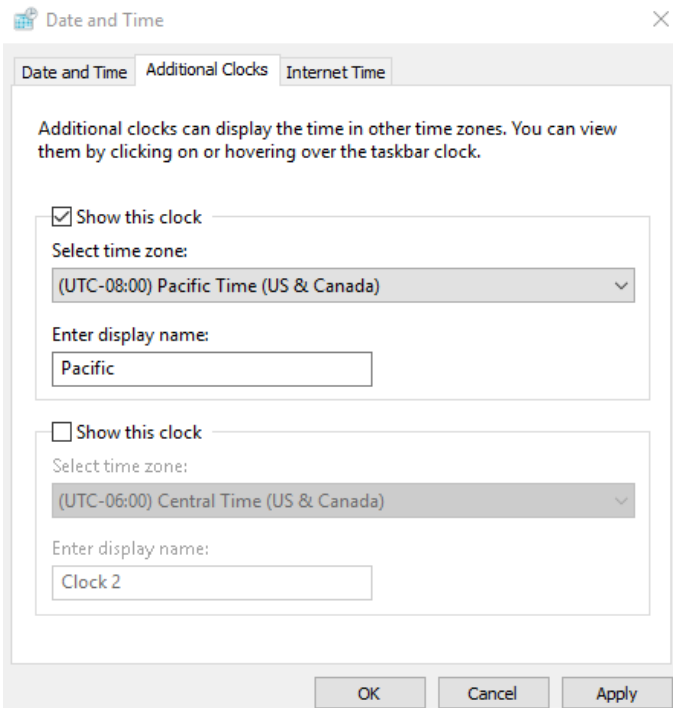
2. Click the hyperlink across from Time zone.



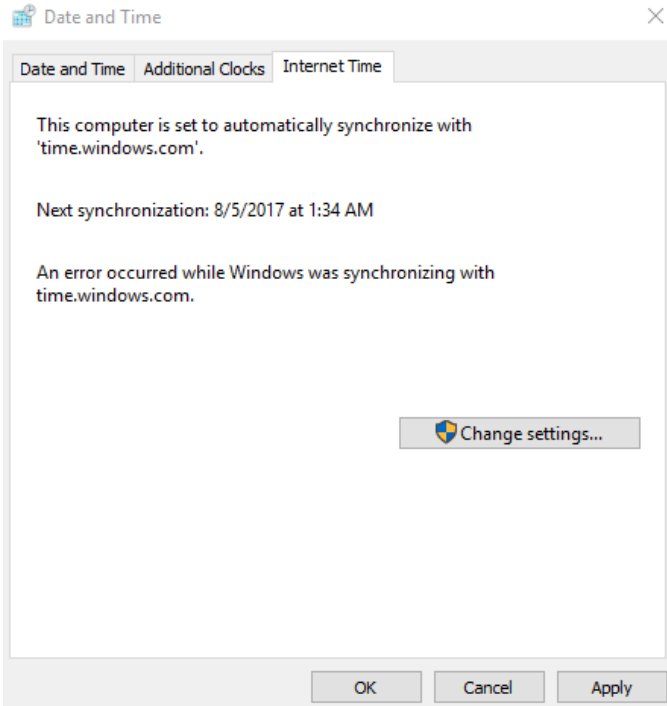
3. Click Change time zone...



4. Select the correct Time Zone from the drop-down menu, and click OK. In this case, we are in the Central Time Zone.

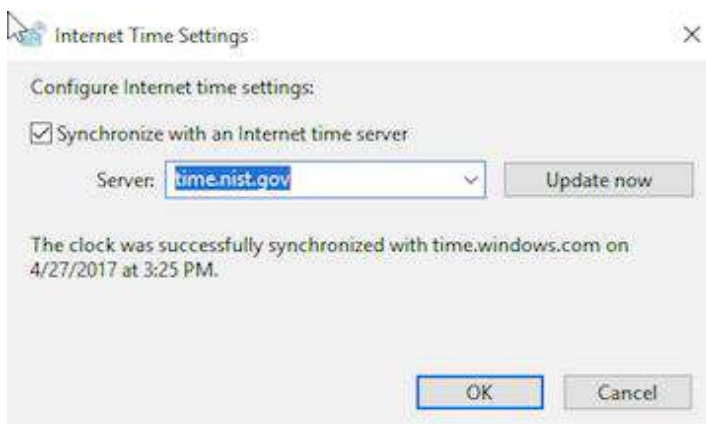


5. You can also set up Additional Clocks from the Additional Clocks tab.



6. The default Internet Time Server is synchronized with 'time.windows.com'. This is editable from the Internet Time tab.

a. Click Change settings.



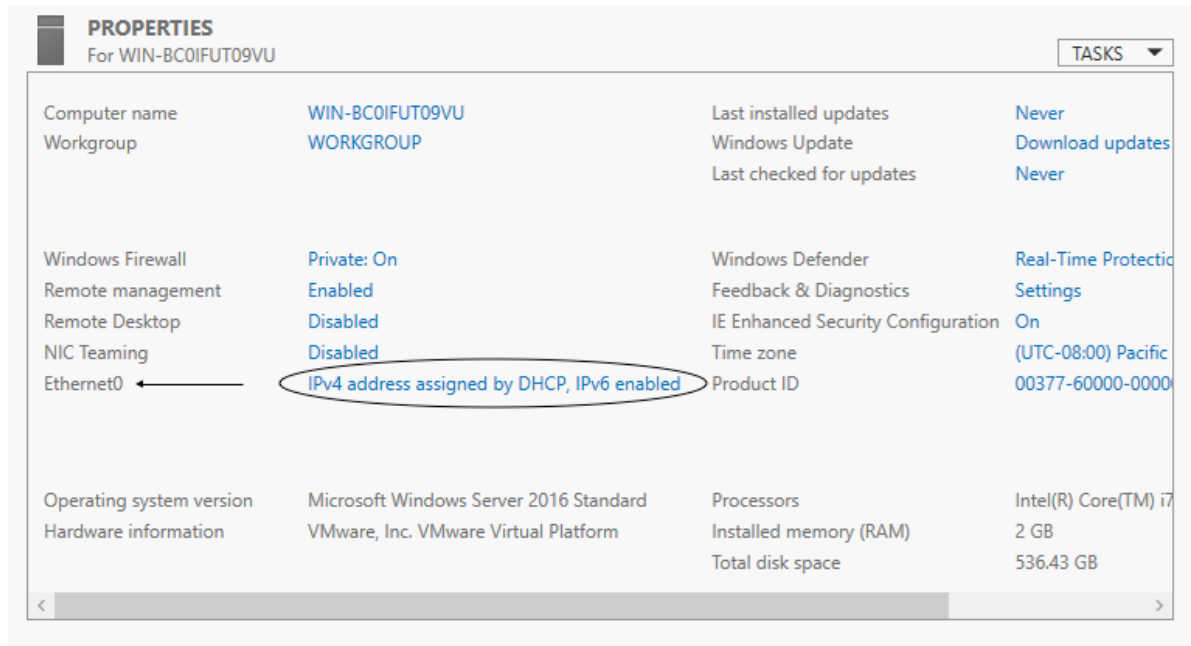
b. Change the dropdown option to the right of Server: The other option is time.nist.gov.

c. Update now; This will force an update of the time on the system once the Internet time server is setup.

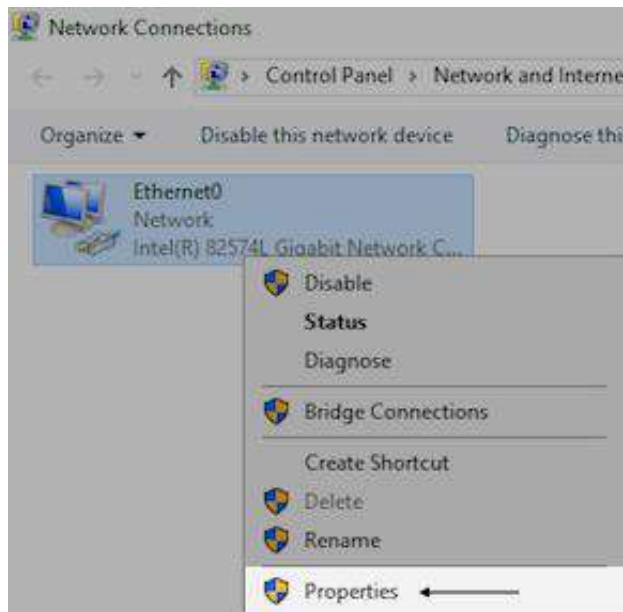
d. Click OK.

Setup the Network Card(s)

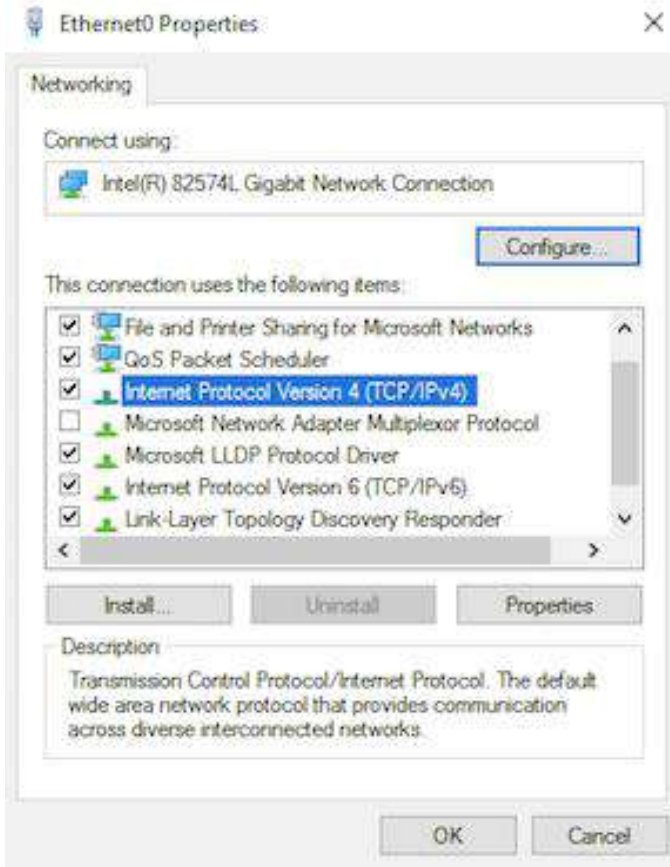
1. From the Server Manager Dashboard, click Local Server from the left menu pane.
 - a. If you are connected to a private network and already have access to the internet to patch the system, then changing the ip address can be done last.
 - b. If you need to connect to the network or need to assign a static IP address then proceed.



2. Click the hyperlink across from Ethernet0.



3. In the Network Connections window, right-click on Ethernet0 and select Properties.



4. Highlight Internet Protocol Version 4 (TCP/IPv4). Click Properties.
 - a. If your network is setup for IPv6, you can highlight Internet Protocol Version 6 (TCP/IPv6) from the Ethernet0 Properties window, and click Properties to configure.



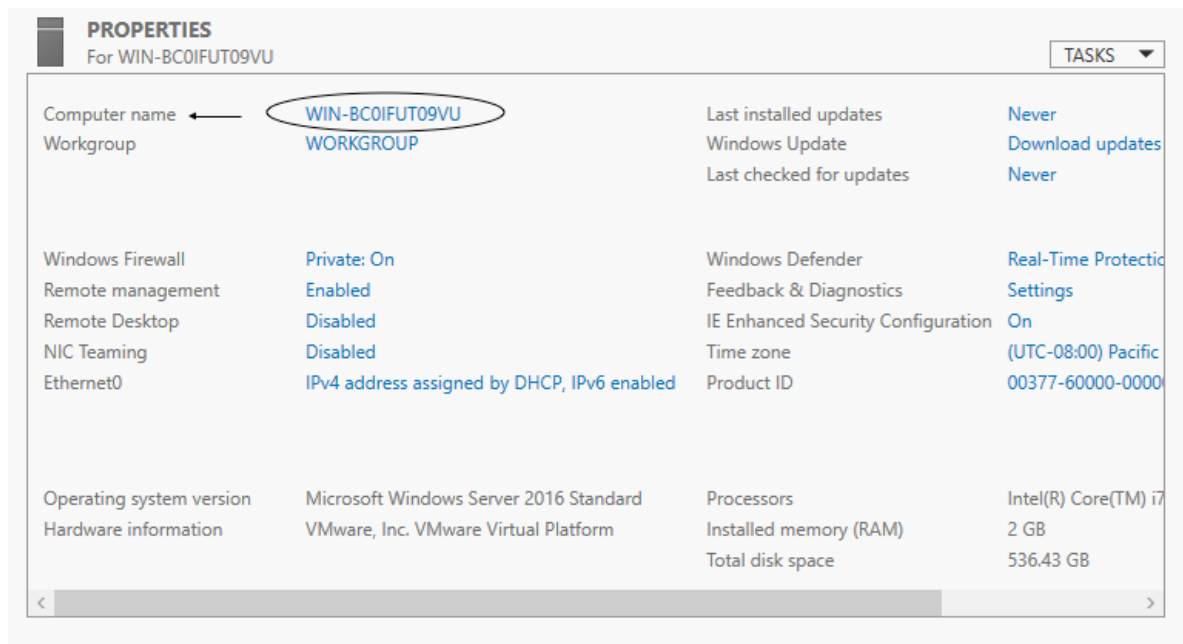
5. Fill in the IP information appropriate for your network. Enter the static ip address, subnet mask, and network default gateway. The preferred DNS server for your Domain Controller will always be itself and the alternate DNS server could be another DC on your network. Click OK.
6. When you are done configuring this network card, click OK.



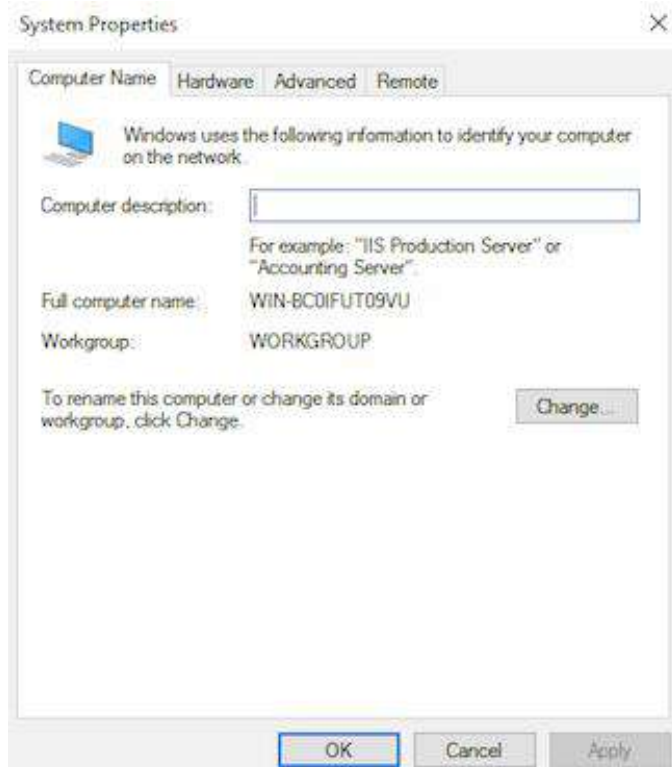
7. When an IP address is assigned, rename the network card to help distinguish your network cards and quickly identify the ip/network. If you have more than one network card installed, disable any cards that are not in use.

Change the Computer Name

1. From the Server Manager Dashboard, click Local Server from the left menu pane.



2. Click the hyperlink across from Computer name.




3. From the Computer Name tab, click Change...



4. Type your new server name in the Computer name: field and click OK.

Computer Name/Domain Changes

 You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

OK

5. You must restart your computer to apply these changes. Click OK
6. Close the System Properties window.

Microsoft Windows

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

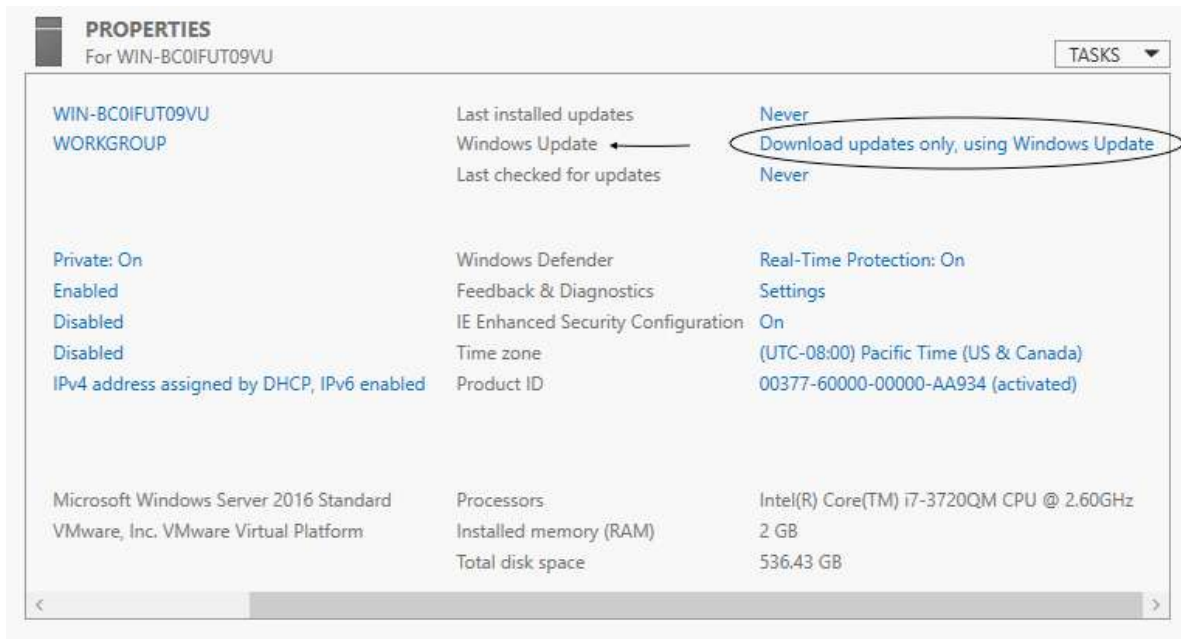
Restart Now

Restart Later

7. Click Restart Now.
8. Server will reboot.

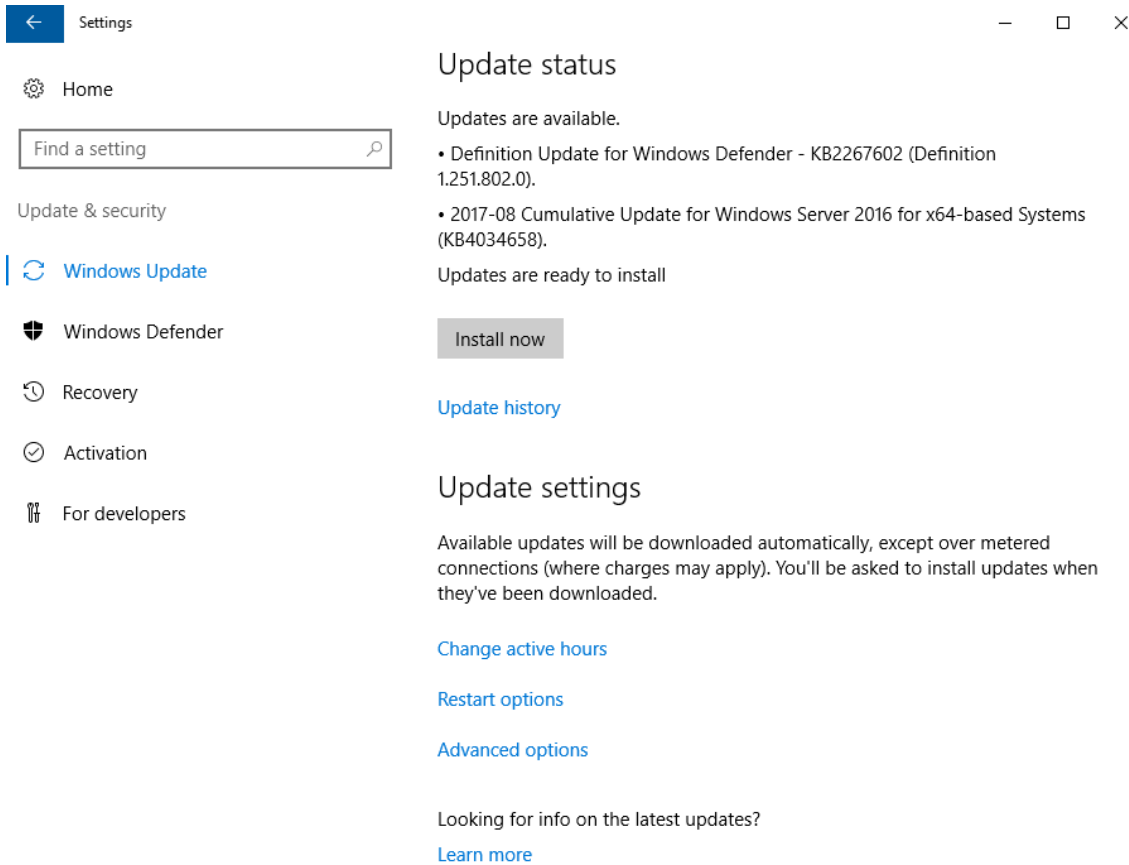
Windows Update

1. From the Server Manager Dashboard, click Local Server from the left menu pane.



2. Scroll right to Windows Update.

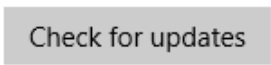
- The default is Download updates only, using Windows Update. Which means Automatic Update is enabled, and the updates will always be downloaded, but you have to configure when to install them. Click that hyperlink to view your options.
- Another option for accessing Windows Update is to left click on the Start Menu and click Settings > Update & Security



3. You may find that you already have updates available to install. Click Install now.

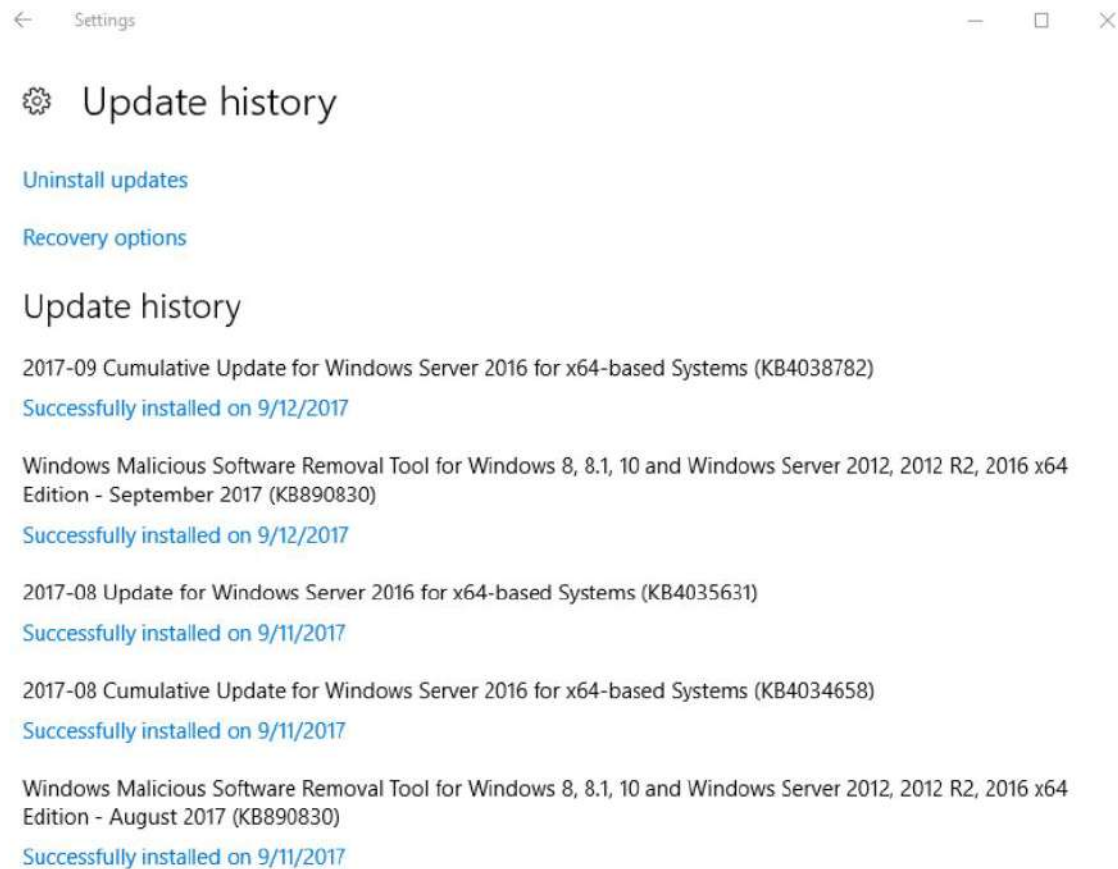
Update status

Your device is up to date. Last checked: Today,

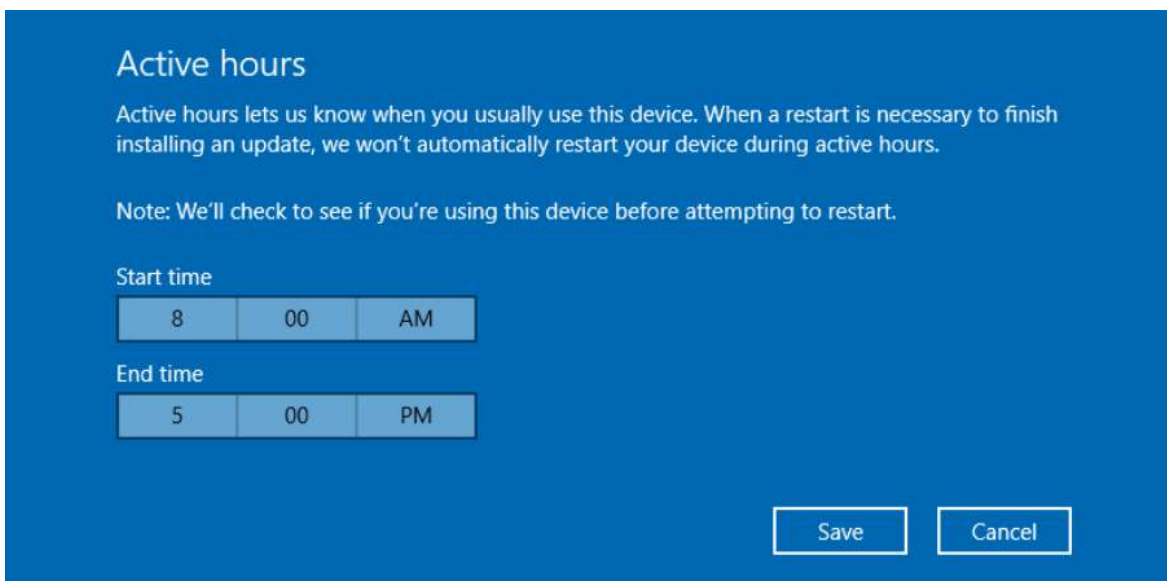


4. Continue to click 'Check for updates' until you receive the confirmation that Your device is up to date.

5. The available options for Windows Update are:



a. Update history



b. Change active hours

Restart options

Schedule a time

We'll restart to finish installing updates when you tell us to. Just turn this on and pick a time.

Off

Pick a time:

7 | 37 | PM

Pick a day:

Today ▾

c. Restart options

Advanced options

Choose how updates are installed

Give me updates for other Microsoft products when I update Windows.

Defer feature updates
[Learn more](#)

Note: Windows Update might update itself automatically first when checking for other updates.

[Privacy settings](#)

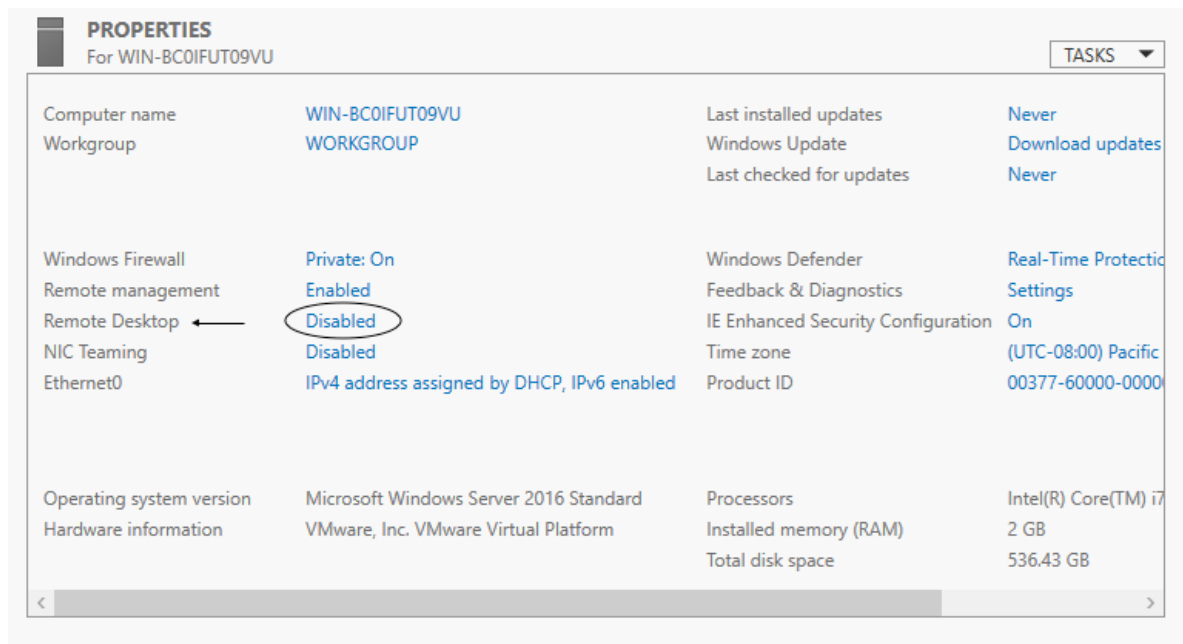
d. Advanced options. **Be sure to check the option to ‘Give me updates for other Microsoft products when I update Windows.’ This is not checked by default!**

e. Learn more, launches a browser and loads a website for Windows 10 Updates:
<https://support.microsoft.com/en-us/help/4018124/windows-10-update-history>

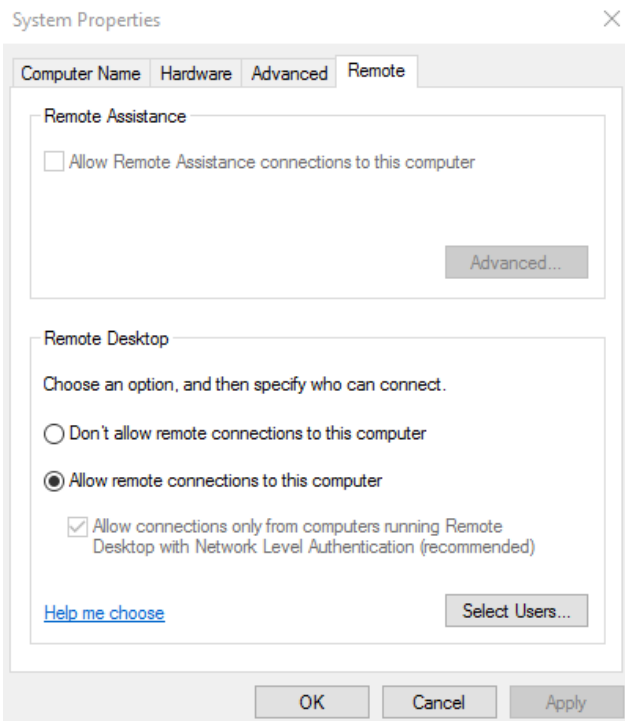
For additional information, visit: <https://blogs.technet.microsoft.com/mu/2017/06/27/patching-with-windows-server-2016/>

Enable Remote Desktop

1. From the Server Manager Dashboard, click Local Server from the left menu pane.



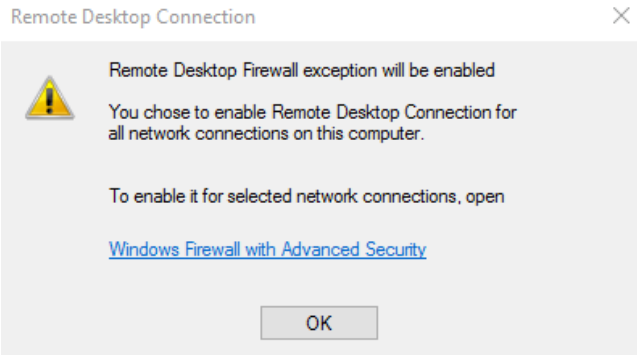
2. Remote Desktop is Disabled by Default. Click the 'Disabled' hyperlink across from Remote Desktop.



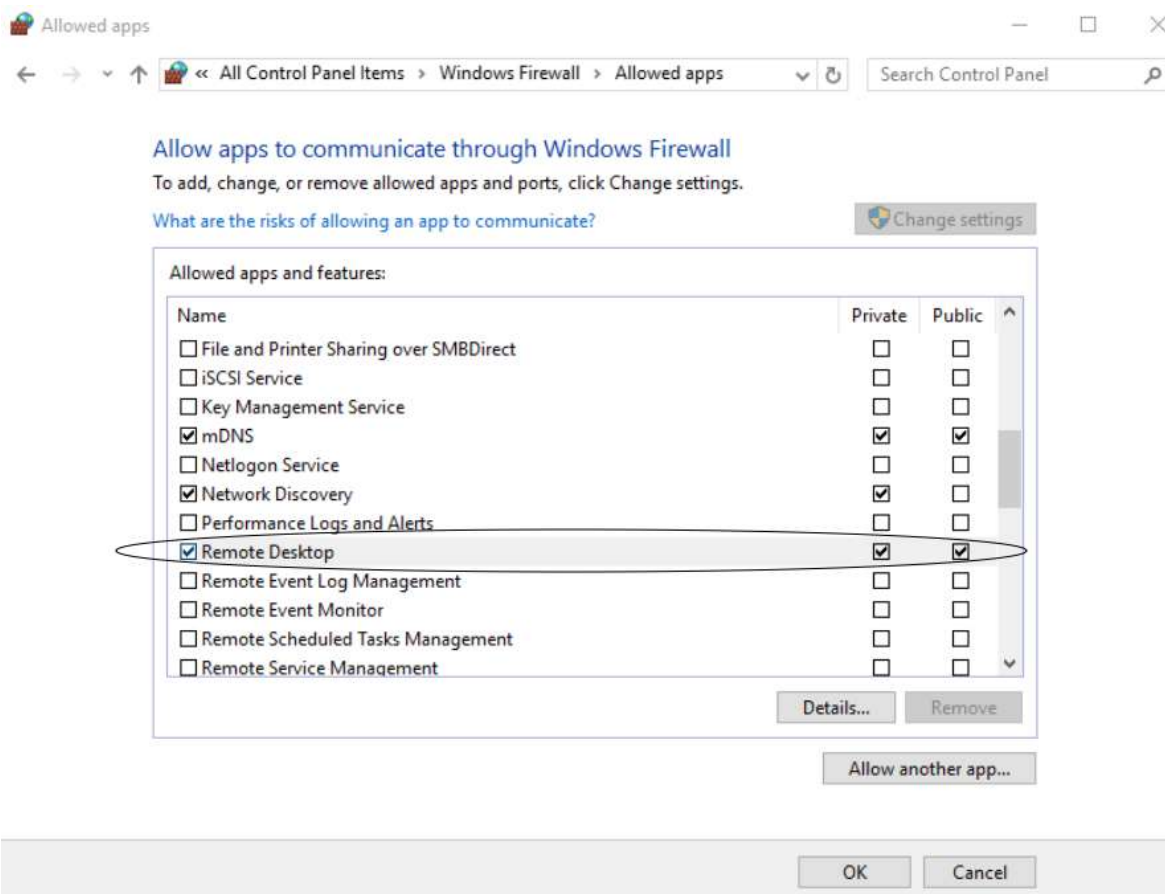
3. The System Properties then launches with the Remote tab active. Switch the radio to Allow remote connections to this computer. Keep the (recommended) option checked.

a. Be aware that Remote Desktop can be susceptible to Man-in-the-Middle infiltration.

b. If possible, limit Remote Desktop usage to your internal network, or connect via VPN or Direct Access.



4. An alert will prompt you to allow the Remote Desktop Firewall exception to be enabled. Acknowledge the alert and Click OK to save the Remote tab System Properties.



5. The Remote Desktop Firewall exception is located in Control Panel > Windows Firewall > Allow an app or feature through Windows Firewall.

Section IV: Building a Domain Controller

DEFINITIONS

Roles - Roles are sets of software programs that when installed and configured properly, function automatically to provide multiple users and/or computers with access to resources within a network. Examples: DHCP, Active Directory & DNS, File Services, Print Server Services, etc. Roles typically include their own databases, can queue requests or record information about the network participants. One or more roles can be installed on a server depending on the capabilities of the hardware.

Role Services – Role Services are software programs that add functionality to the role. Some Roles only have one specific function and do not have additional Role Services to choose from. Other Roles require a certain set of Role Services, which are installed without selection options.

Features – Features are optional software programs that can be installed without direct correlation to available and regardless selected Roles.

Functions - Functions are secondary or supporting features to the primary Roles that can be installed. Defining the Server management or administrative management functions (MMC), backing up files.

AD DS – Active Directory Domain Services is the directory services database for Windows Server, used to process logons, authentication and directory searches. Installed on a domain controller, it manages communications across users and domains.

Functional Level – Determines the available domain or forest capabilities of Active Directory Domain Services. Best practice is to set the domain and forest functional levels at the highest value that the environment can support. This will usually be the most currently available OS, unless you do not have any servers with the current OS. You can set the domain functional level to a value that is higher than the forest functional level; however, you cannot set it at a level that is lower.

MUST-READ LINKS!

Step-by-Step Guide for Setting up a Windows Server 2016 Domain Controller

<http://www.tactig.com/install-windows-server-step-by-step/>

<http://www.tactig.com/install-active-directory-domain-services-ad-ds/>

<http://www.tactig.com/promote-windows-server-domain-controller/>

Upgrade and Conversion Options for Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/get-started/supported-upgrade-paths>

In-Place Domain Controller Upgrade from Windows Server 2012R2 to 2016

<https://www.virtualizationhowto.com/2016/11/upgrade-windows-server-2012-r2-domain-controller-to-windows-server-2016/>

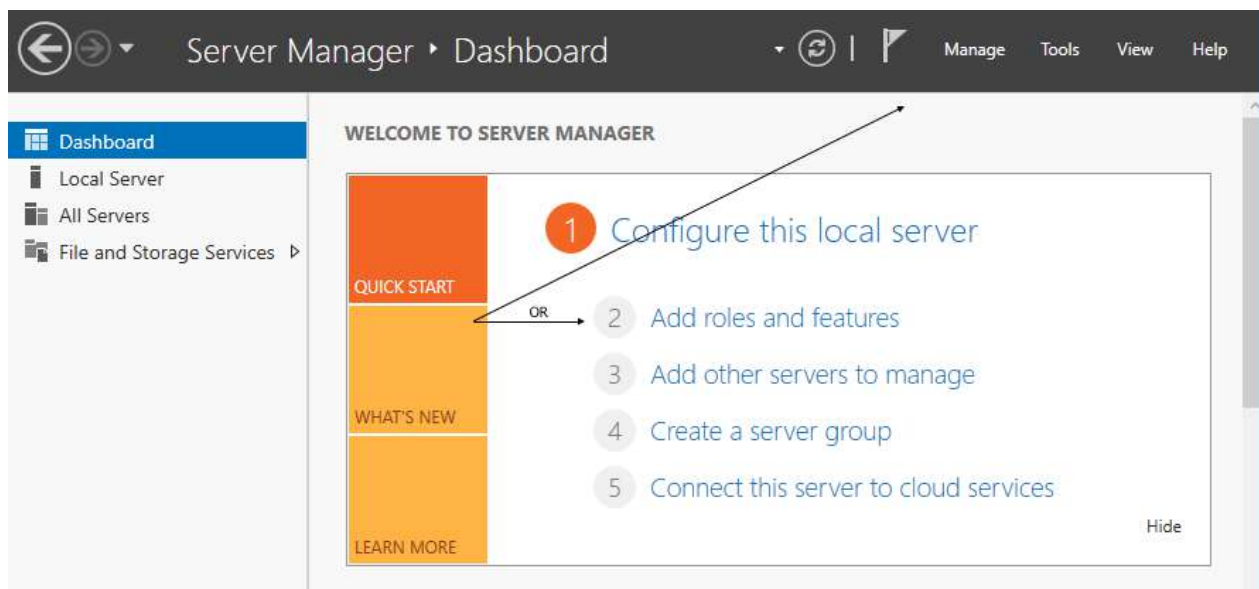
What's New in Windows Server 2016 Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/whats-new-active-directory-domain-services>

INSTALLING ACTIVE DIRECTORY DOMAIN SERVICES

The following steps will help you configure your server as an Active Directory Domain Controller on the network. DNS is an integral part of a Microsoft Active Directory Domain, and will need to be setup and tested first to ensure it is running properly. All services within a Windows Domain require DNS in order to operate.

Microsoft Best Practices specify a minimum of two domain controllers be installed within a domain. Having more than one domain controller allows for redundancy and continued operations even if one of the systems fails. The second system will continue to process user logins and DNS requests, continue to apply Group Policy and will maintain your Active Directory environment. **A single server domain is extremely risky and its' best to avoid that at all costs.**



1. Click Add roles and features from the Server Manager Dashboard or select the option from the Manage menu.

a. Before you begin, you must verify the following. You do have the option to select “Skip this page by default” so you no longer receive this reminder when you run this wizard:

- i. You have a strong Administrator Password.
- ii. Your Static IP address is configured.
- iii. You have installed the most current security updates from Microsoft.

b. Click Next.

The Wizard

Add Roles and Features Wizard

— □ ×

Select installation type

DESTINATION SERVER
Yourservername

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

- Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.
- Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

2. Select installation type
 - a. Choose Role-Based or Feature-based installation.
 - b. Click Next.

Select destination server

DESTINATION SERVER
Yourservername

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

Filter:

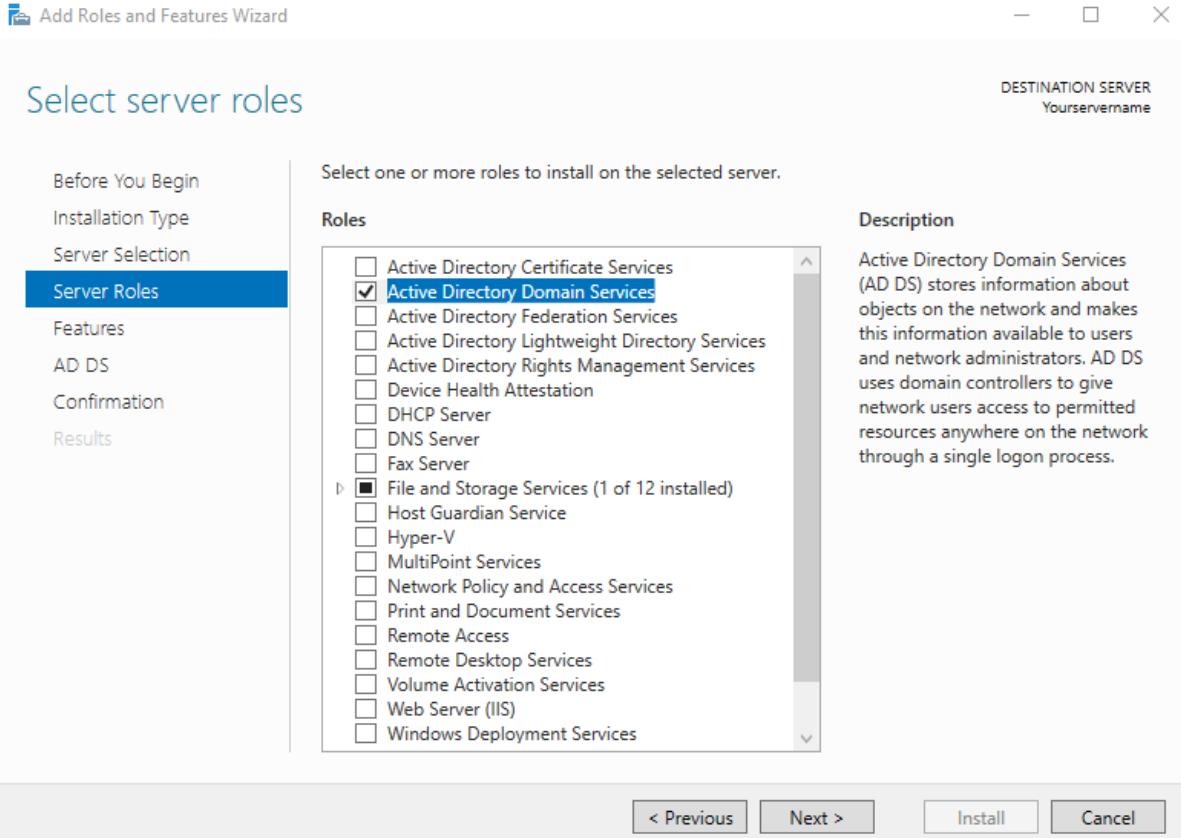
Name	IP Address	Operating System
Yourservername	192.168.250.13...	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

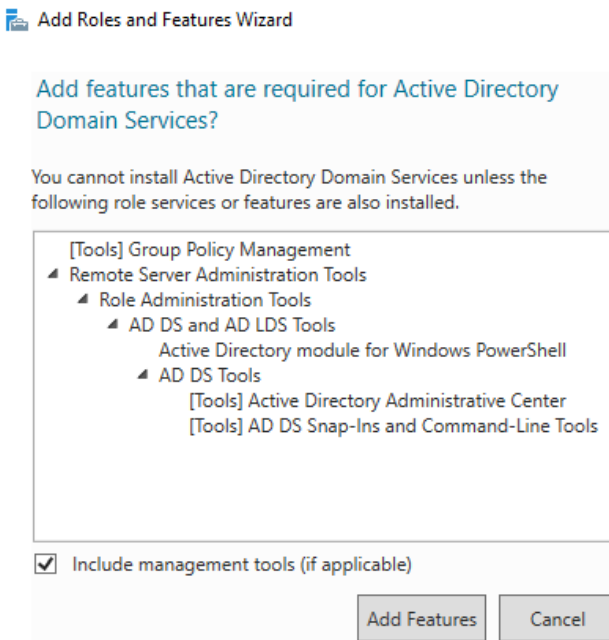
< Previous Next > Install Cancel

3. Select destination server
 - a. Select a server from the server pool.
 - b. Click Next.

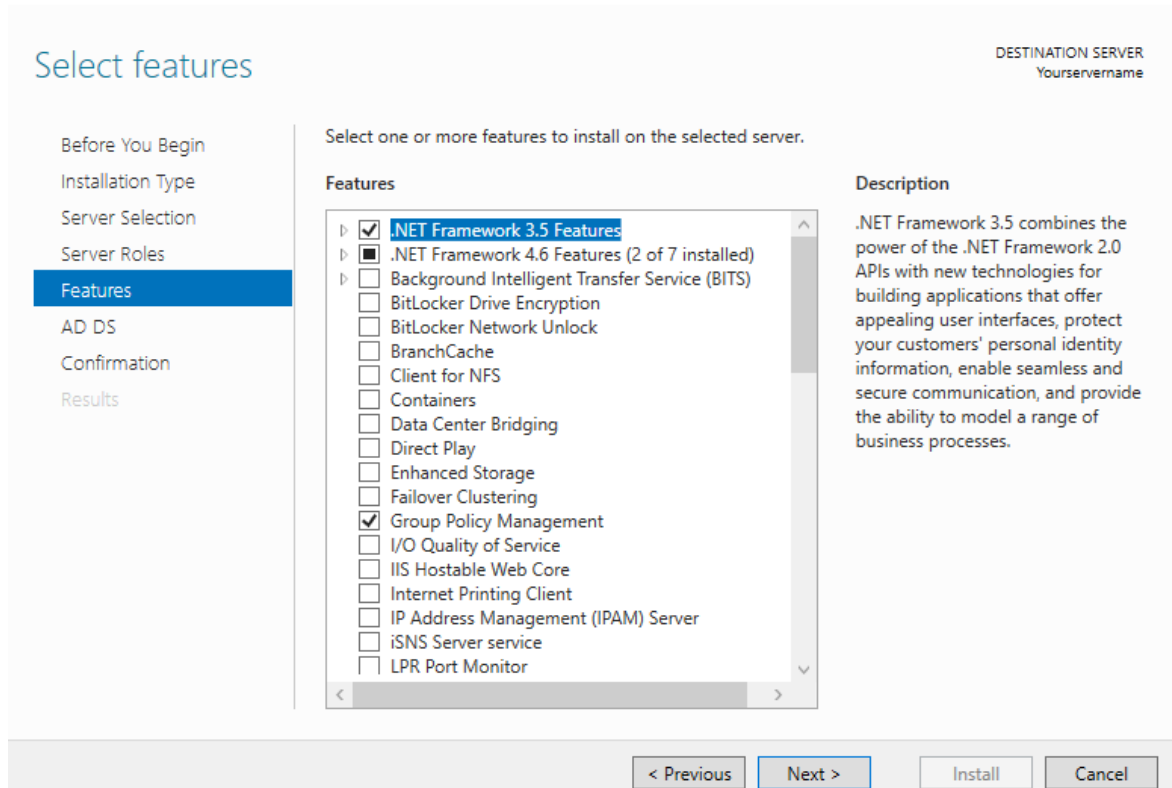


4. Select server roles:

- a. When you highlight a Role from the list, a brief description displays on the right.
- b. This is where you will select any Roles that are necessary for your server.
- c. For this installation, we will choose Active Directory Domain Services by checking the box.



- d. Using the Roles Wizard will always prompt you to install any additional Features that are needed to support the Role you have selected.
 - i. Required features for the Active Directory Domain Services Role are: Group Policy Management, Remote Server Administration Tools, Active Directory Module for Powershell, the Active Directory Administrative Center, and AD DS Snap-ins & Command Line Tools are required features.
 - ii. **We will leave the option to “Include management tools (if applicable) checked.**
 - iii. Click Add Features. You will be unable to proceed with the Roles Wizard without clicking Add Features.
- e. Back at the Select server roles screen (pictured on the previous page), click Next.



5. Select features:

- a. If you scroll through this list, you will notice that the Features you added via the previous prompt are now selected. For this installation, also check the box to install .NET Framework 3.5.
- b. When you highlight a Feature from this list, a brief description displays on the right.
- c. Click Next.

Active Directory Domain Services

DESTINATION SERVER
Yourservername

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS


Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

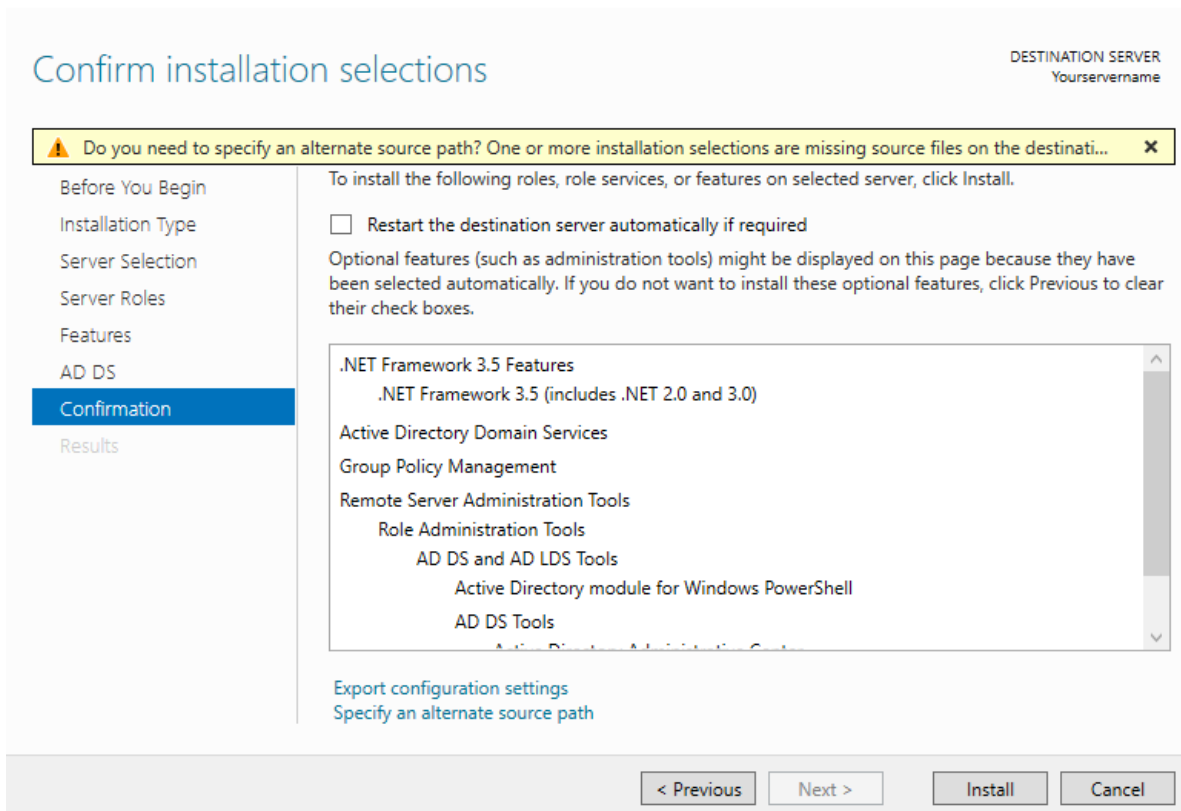


Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous
Next >
Install
Cancel

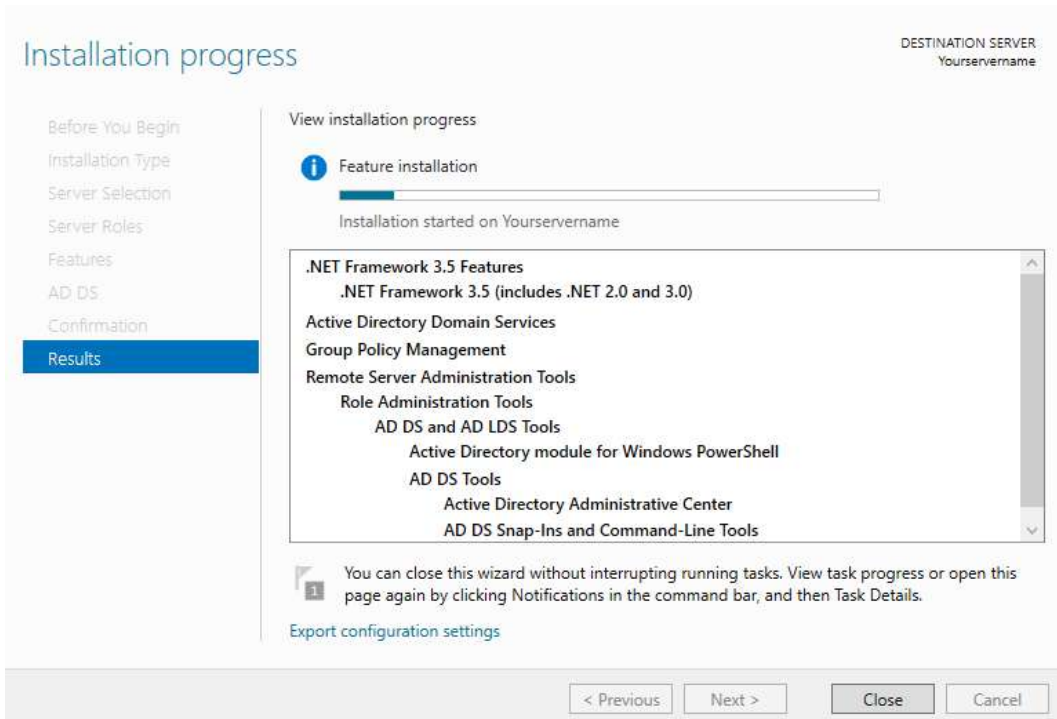
6. Active Directory Domain Services.

- a. Describes AD DS. Please read this to understand the AD DS role.
- b. Install a minimum of two domain controllers for your domain to avoid disrupting user logins in the case of a server outage.
- c. AD DS requires a DNS server be installed on the network. If one is not detected, you will be prompted to install the DNS role on this server.
- d. There is also a brief description of Azure Active Directory services, including a hyperlink to Learn more: <https://azure.microsoft.com/en-us/services/active-directory/>
- e. Click Next.



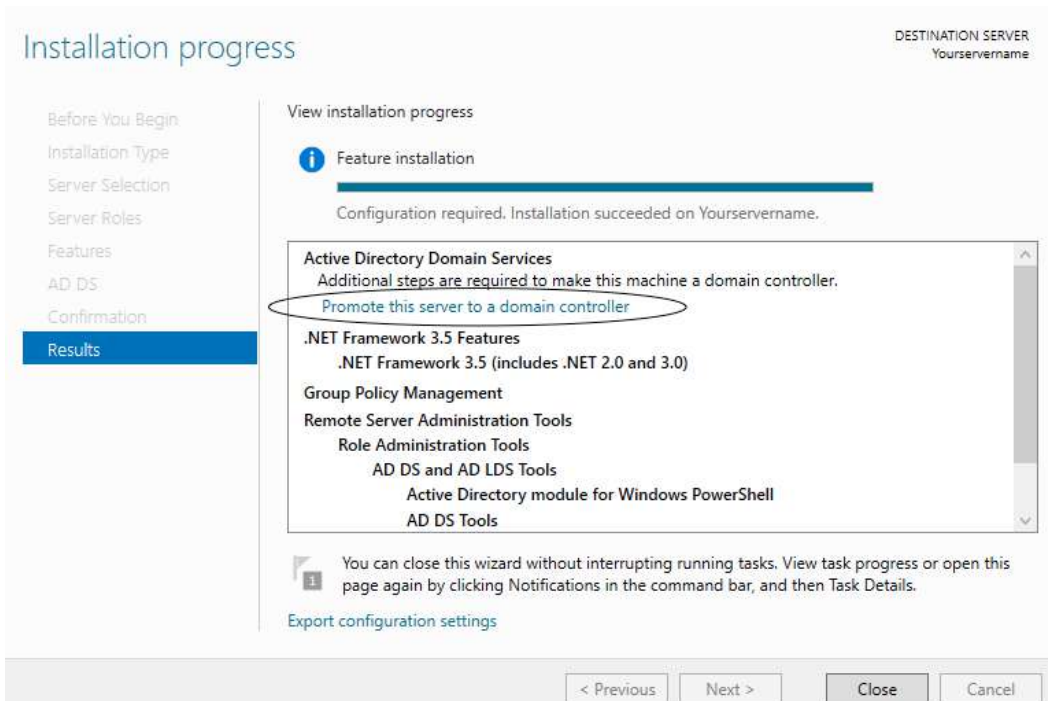
7. Confirm installation selections.

- a. Checking the option to add .NET framework 3.5 is what causes the warning “Do you need to specify an alternate source path?” In Server 2016, the actual binaries for .NET framework 3.5 are not included in the default Windows image. Its feature state is disabled with the payload removed.
 - i. If your server has access to Windows Update, the installation can complete without the need to enter an alternate source path.
 - ii. If Windows Update is not available, the installation files are accessible from the Server 2016 .iso. Mount the .iso files and click the link to “Specify an alternate source path”. In the window that launches enter the Path: <the drive letter to your .iso>\sources\sxs. Click OK.
- b. There is a checkbox option to Restart the destination server automatically if required. **If you do not check this box, and a restart is required, you will be prompted to do so after the installation is completed.**
- c. There is also a link to Export the configuration settings. This can be useful if you manage numerous servers.
- d. Click Install.



8. Installation Progress / Results

- a. Installation will take several minutes to complete.
- b. Progress is displayed.



- c. When completed, you will be prompted additional steps are required. Click the hyperlink to Promote this server to a domain controller.

PROMOTING YOUR SERVER TO A DOMAIN CONTROLLER

Naming Considerations for Your Domain

When considering a name for your internal domain, there are several things to consider:

- Does your organization have or need a public facing (external) domain name?
- Will you be using any cloud based services that sync with your Active Directory?
- Are you utilizing an Exchange server?

When installing an Active Directory server, it is recommended that you create an Internal Domain that is not the same as your external Domain name. This is used to increase security by separating your internal systems and functions from your external Domain structure. “Microsoft strongly recommends that you register a public domain and use subdomains for the internal DNS,”

<https://social.technet.microsoft.com/wiki/contents/articles/34981.active-directory-best-practices-for-internal-domain-and-network-names.aspx>.

Let’s discuss DNS, or Domain Name Services. To access webpages on the internet, DNS is used to translate domain names to ip addresses. TLD (or Top-Level Domains) are used for the public internet, and a complete list, <https://www.icann.org/resources/pages/tlds-2012-02-25-en>, is maintained by IANA (Internet Assigned Numbers Authority). Some examples are, .com, .org, .net, .biz, .gov, .edu, .info, etc.

If you do not already have a domain name registered, prior to setting up your Domain Controller, you will want to ensure that the domain name you have chosen is not already being used publically by another entity. Search websites similar to <http://whois.domaintools.com> to verify. If the domain name is not owned, register/purchase the rights to domain name from a reputable registrar like GoDaddy or Network Solutions. ICANN.org provides an accredited list, <https://www.icann.org/registrar-reports/accredited-list.html>.

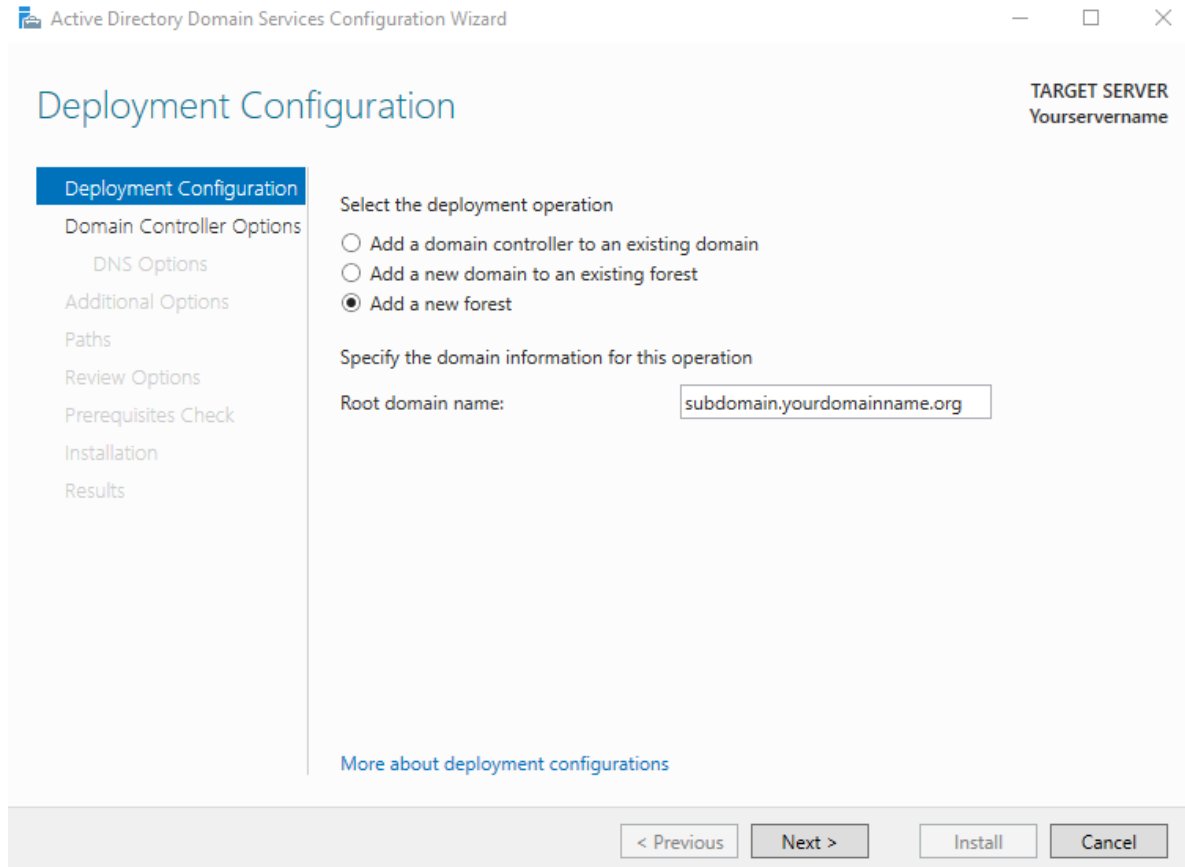
If you do have an external domain name registered to your organization, you could either consider using a subdomain, ex. subdomain.yourmaindomainname.org, or register your domain name with another TLD (Top-Level Domain), ex. yourmaindomainname.net, or yourmaindomainname.info, for your internal domain. If you register your main domain name with another TLD, you’ll want to make sure that it is not already being used publically by another entity. and then register accordingly.

Do not use .local! mDNS (multicast DNS)/Bonjour, appends .local when performing network searches to identify nodes on the local subnet without using a IP lookup. Single name host (ex. My-Computer.local) lookups default to Bonjour. Hosts with 2 or more names (ex. server.01.local) default to using a DNS server. Additionally, .local is considered a non-unique identifier, and UCC/SAN will no longer issue public trust certificates for non-TLD names, <https://cabforum.org/internal-names/>.

If you are loading your server to be the First Domain Controller within the domain configure the Network Properties primary DNS to point to itself. ***This should be done just prior to upgrading the server to a domain controller.*** When promoting a server to a Domain Controller, the system makes Active Directory changes during the setup where updating the Primary DNS to its own IP address helps avoid installation issues.

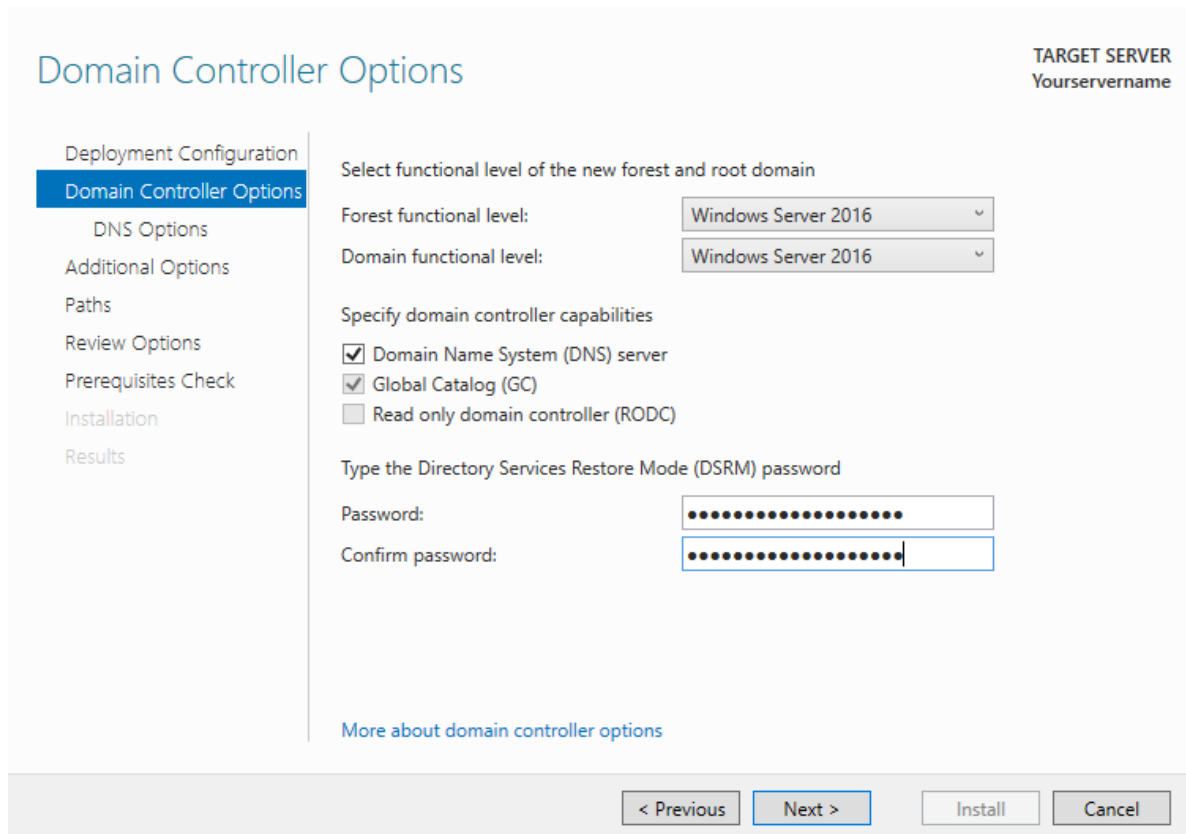
The Wizard

If you missed the opportunity to click Promote this server from the Add roles and features wizard after installing Active Directory, you are prompted to do so from the Notifications Flag in the Server Manager Dashboard.



1. Deployment Configuration

- a. As your first Domain Controller, you will select the option to Add a new forest. Alternatively, you could choose to add to an existing forest, if this is an additional domain controller.
- b. Re-read the page above, Naming Considerations for Your Domain.
- c. Once you have determined an internal domain name, enter your Root domain name.
- d. The hyperlink, More about deployment configurations, opens the Microsoft AD DS Wizard Page Descriptions: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DepConfigPage
- e. Click Next.



Domain Controller Options

TARGET SERVER
Yourservername

Deployment Configuration
Domain Controller Options
 DNS Options
 Additional Options
 Paths
 Review Options
 Prerequisites Check
 Installation
 Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

Domain Name System (DNS) server
 Global Catalog (GC)
 Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: [Masked]
 Confirm password: [Masked]

[More about domain controller options](#)

< Previous Next > Install Cancel

2. Domain Controller Options

a. Select Functional Level. See Definitions section to read more. The default is Windows Server 2016.

**** Once the Domain Functionality Level is selected, you can only increase the level. You cannot decrease the Domain Functionality Level. ****

b. Specify domain controller capabilities

- i. Domain Name System (DNS). This should be installed on all domain controllers, and is checked by default.
- ii. Global Catalog (GC). This is required on the first domain controller in a forest, and all subsequent DC's. This option is also checked by default. The Global Catalog allows domain controllers to process logons.
- iii. [Read only domain controller \(RODC\)](#). Introduced in Windows Server 2008, you might use this option for a remote site or DMZ.

c. Directory Restore Mode (DSRM) Password

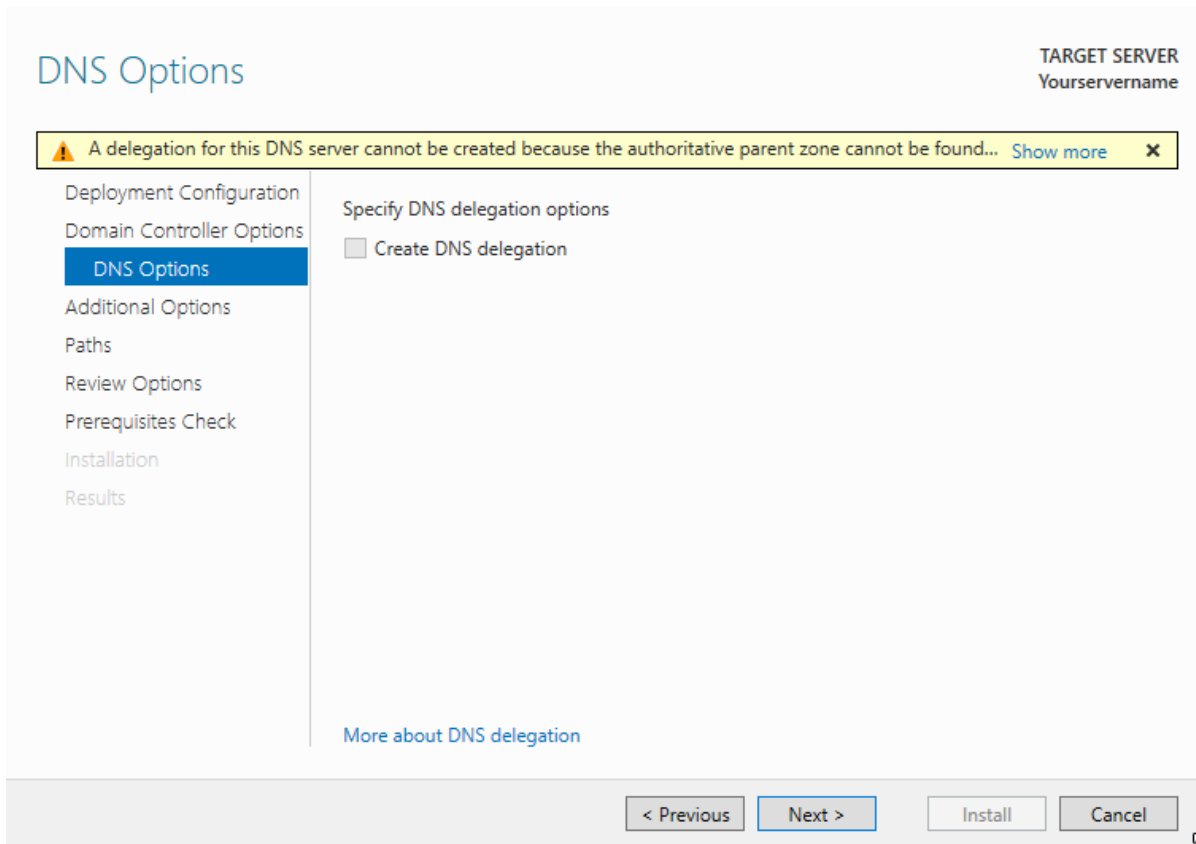
- i. Make sure to store your DSRM password in a secure location.
- ii. The password needs to follow your organizational password policy.
- iii. Enter your password.

d. Microsoft also provides a hyperlink for More about domain controller options:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DCOptionsPage

e. **We will use the default options on this page.**

f. Click Next.



3. DNS Options

DNS Options

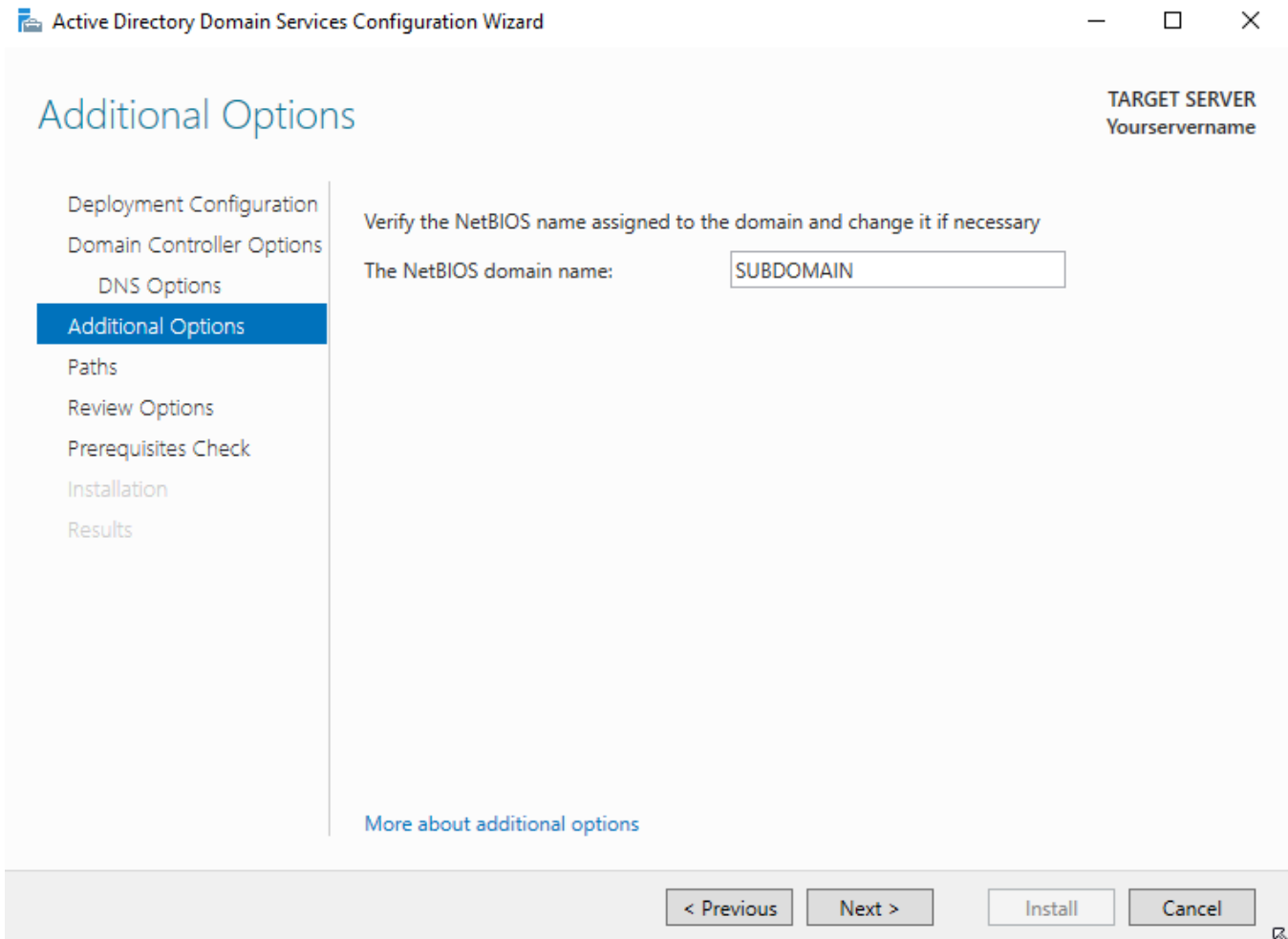


A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "subdomain.yourdomainname.org". Otherwise, no action is required.

OK

- a. If you click 'Show more' within the yellow warning box, another dialogue window opens.
 - i. Part of this process checks the network for a previously configured DNS authoritative parent zone, and A Host records that may already exist for this server.
 - ii. Since this is our first server with DNS, it will be set up with the authoritative parent zone, and delegation cannot be created.
 - iii. Click OK, if opened.
- b. Specify DNS Delegation options.
 - i. **Leave the "Create DNS Delegation" option, unchecked.**
 - ii. The AD DS Configuration Wizard will create the necessary NS (Name Server) and A

- Host (glue) records.
- iii. To learn more about the structure of DNS, click on the More about DNS delegation hyperlink: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DNSOptionsPage
- c. Click Next.



4. Additional Options

- a. Here we are prompted to verify and enter the NetBIOS name.
- b. Microsoft provides a hyperlink to learn More about additional options: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_AdditionalOptionsPage. If this were to be an added domain controller, you would instead be given the option to designate a replication source.
- c. Click Next.

Paths

TARGET SERVER
Yourservername

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder: ...

Log files folder: ...

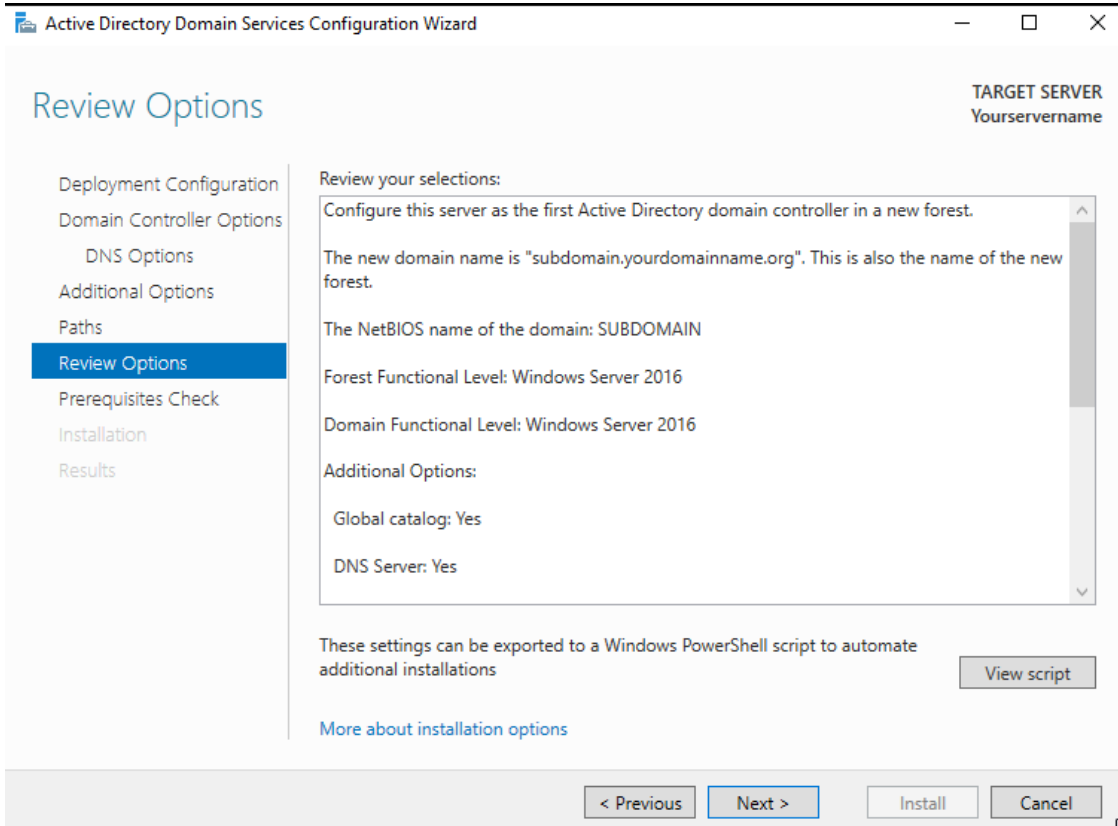
SYSVOL folder: ...

[More about Active Directory paths](#)

< Previous Next > Install Cancel

5. Paths

- This is the location for the Database, Logfiles and SYSVOL folders.
- Microsoft provides a hyperlink to learn More about Active Directory paths:
<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions - BKMK Paths>.
- Best Practice is to designate separate drives for these files.
- You can browse to the location you would like to use, or type the path.
- Click Next.



6. Review Options

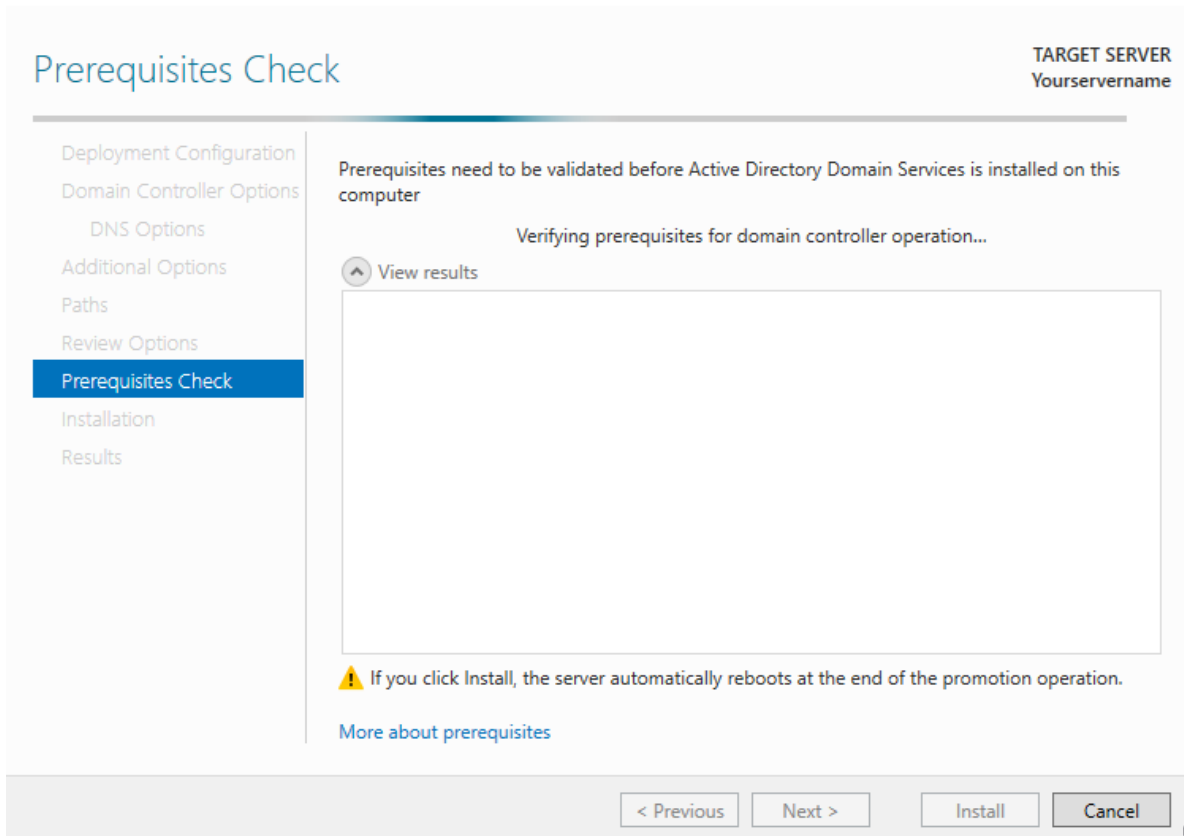
- a. Scroll through to verify the installation options you selected.
- b. If necessary, go back to make changes by clicking Previous. The hyperlink, More about installation options, simply discusses that this is the point of the wizard where you can view your previous selections and still have the opportunity to go back to make changes.

```

tmp1C59.tmp - Notepad
File Edit Format View Help
#
# Windows PowerShell script for AD DS Deployment
#

Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName "subdomain.yourdomainname.org" `
-DomainNetbiosName "SUBDOMAIN" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\Logfiles" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
    
```

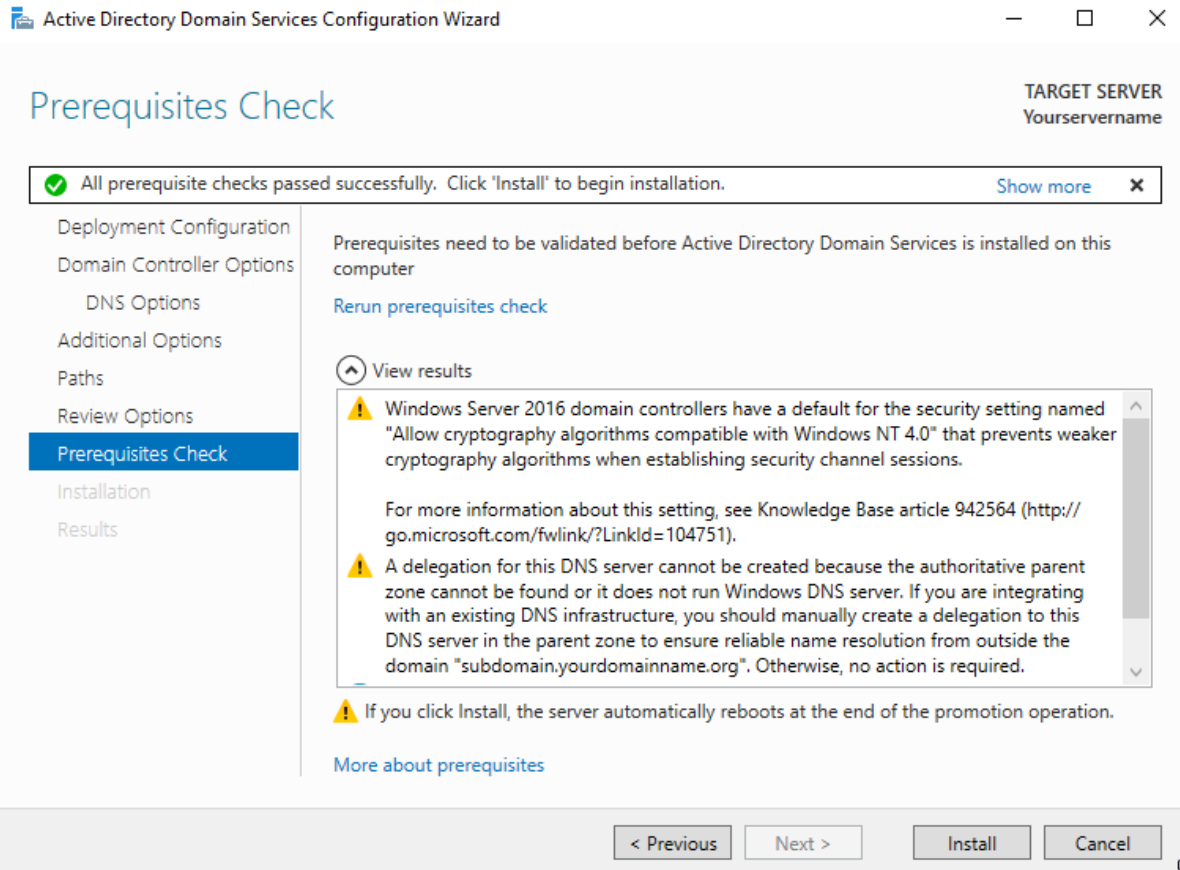
- c. Click View script to generate a Powershell Script that launches in Notepad to Save and use to automate subsequent installations.
- d. Click Next.



The screenshot shows the 'Prerequisites Check' step of the Active Directory Domain Services Configuration Wizard. The window title is 'Active Directory Domain Services Configuration Wizard'. The target server is identified as 'Yourservername'. The left-hand navigation pane includes the following steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options, Paths, Review Options, Prerequisites Check (highlighted in blue), Installation, and Results. The main content area displays the message: 'Prerequisites need to be validated before Active Directory Domain Services is installed on this computer'. Below this, it says 'Verifying prerequisites for domain controller operation...' and provides a 'View results' link. A warning icon and text state: 'If you click Install, the server automatically reboots at the end of the promotion operation.' A link for 'More about prerequisites' is also present. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

7. Prerequisites Check

- a. Verifies all requirements for installing the Domain Controller are met
- b. More about prerequisites are available here: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_PrerqCheckPage



c. If your validation passes, you will receive a green checkmark “All prerequisite checks passed successfully. Click ‘install’ to begin installation. The Show more link presents the same information in a separate dialogue window.

d. The following *Warnings* may be listed:

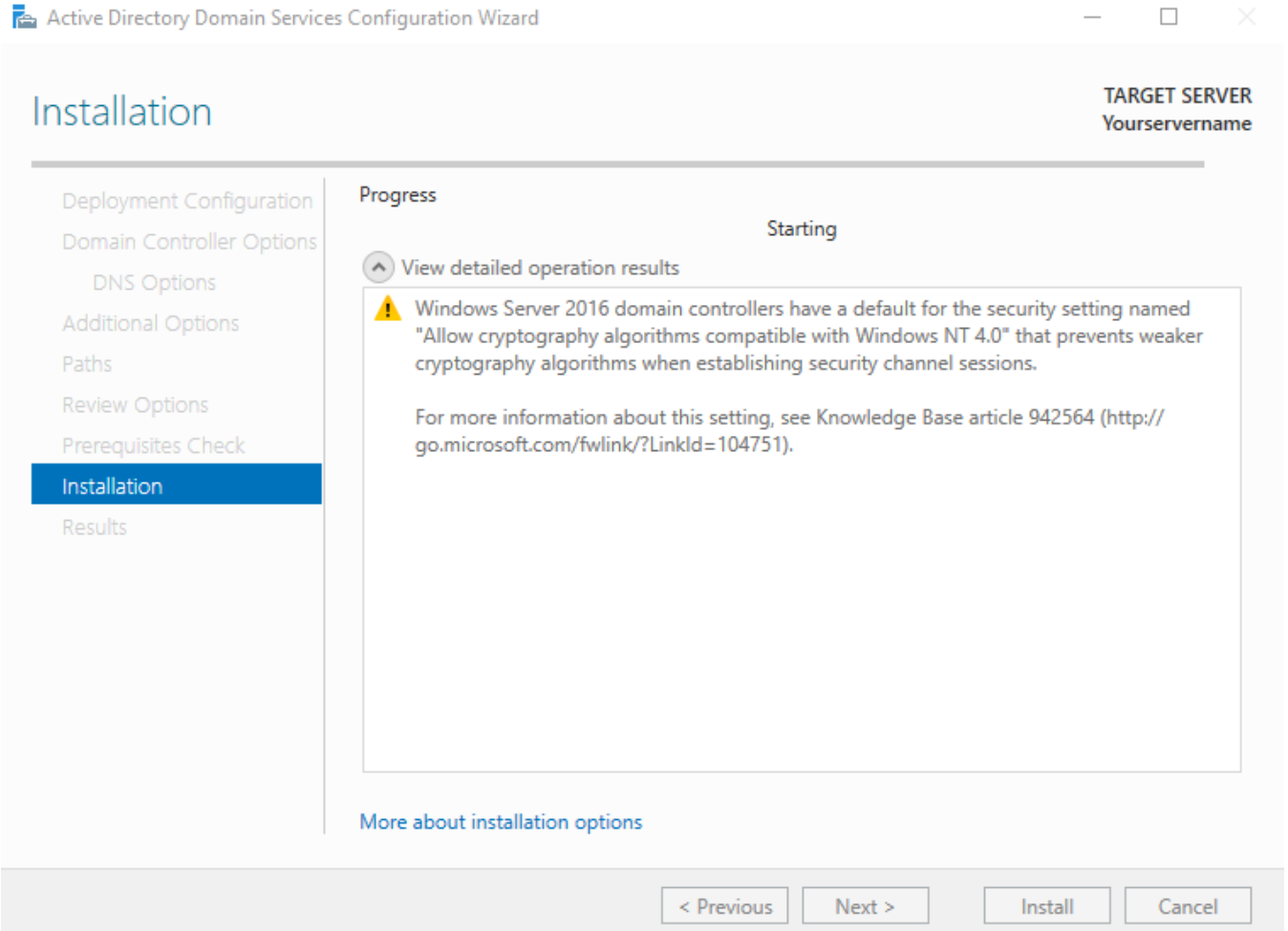
i. Windows Server 2016 domain controllers have a default for the security setting named “Allow cryptography algorithms compatible with Windows Nt4.0” that prevents weaker cryptography algorithms when establishing security channel sessions.

- 1) This setting is Disabled by default.
- 2) Windows NT 4 cannot establish a connection to this server.
- 3) This setting is preferred. NO Windows NT 4 systems should be on your network.

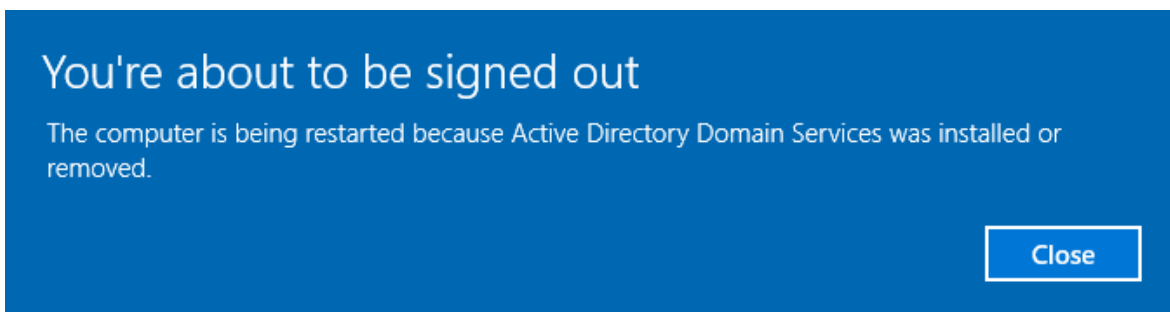
ii. A Delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to the DNS server in the parent zone to ensure name resolution from outside the domain “<LAN- domain-name-you-entered-here>”. Otherwise no action is required

- 1) DO NOT create external DNS Delegation for internal zones
- 2) NO Action is required, DNS will be installed on this server for the domain

e. Click Install.



- 8. Installation
 - a. The System will install Active Directory and DNS.
 - b. When completed, the System will RESTART.



- c. Click Close.

Installation Complete.

Congratulations you have created a Windows Server 2016 Active Directory Domain!

Section V: Customizing Your Domain Controller

MUST-READ LINKS!

Powershell Modules for Windows 10 and Windows Server 2016

<https://technet.microsoft.com/itpro/powershell/windows/index>

Microsoft Script Center

<http://technet.microsoft.com/en-us/scriptcenter>

Features Removed or Deprecated in Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/get-started/deprecated-features>

Guidance on Disabling System Services on Windows Server 2016 with Desktop Experience

<https://blogs.technet.microsoft.com/secguide/2017/05/29/guidance-on-disabling-system-services-on-windows-server-2016-with-desktop-experience/>

Best Practices Analyzer for Active Directory Domain Services: Configuration

[https://technet.microsoft.com/en-us/library/dd391912\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd391912(v=ws.10).aspx)

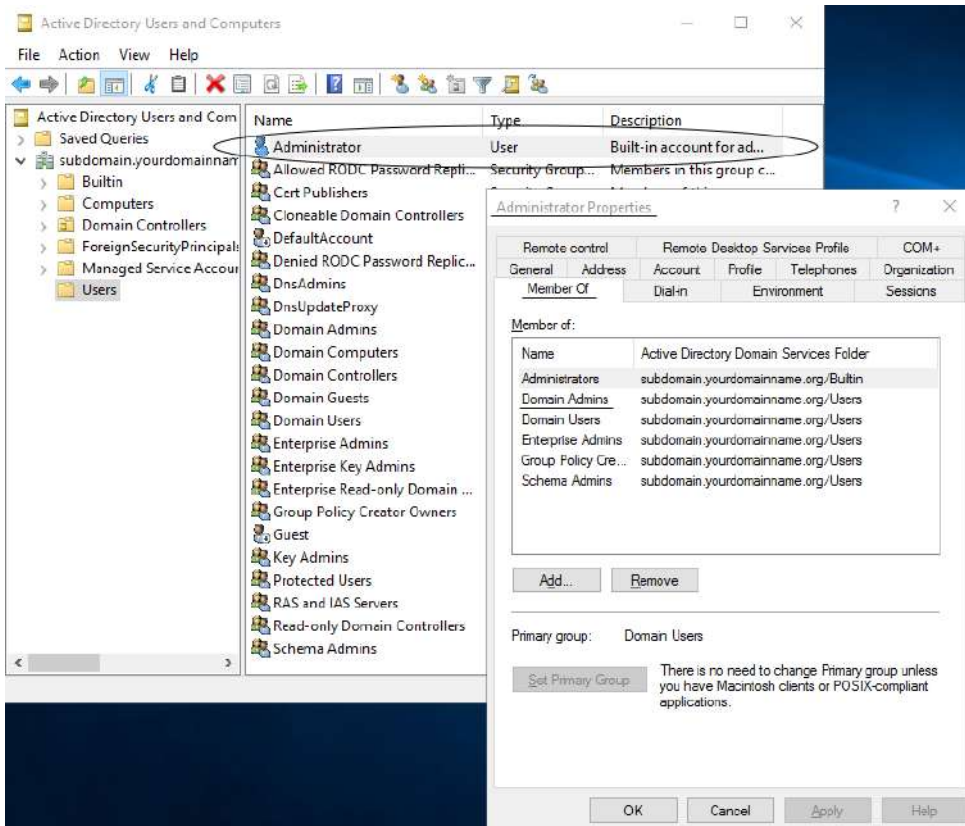
BGinfo

<https://docs.microsoft.com/en-us/sysinternals/downloads/bginfo>

ADMINISTRATOR ACCOUNTS

After your Domain Controller restarts, you are prompted to log in with a Domain Administrator Account.



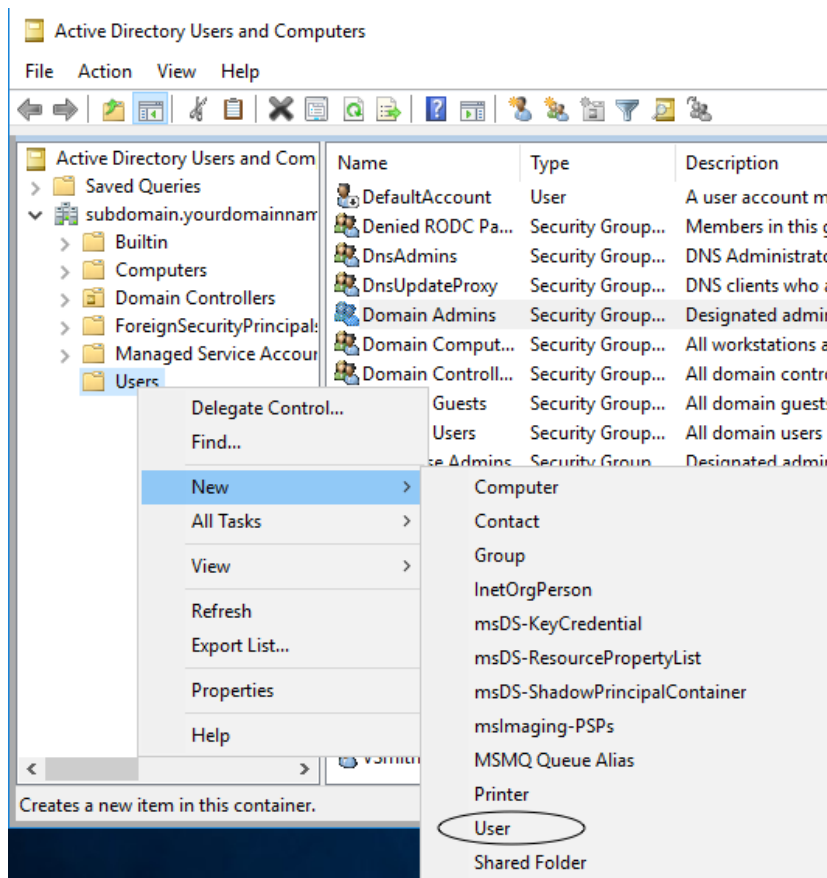


During the Active Directory installation, the original Built-in Administrator account is added to the Built-in Administrators Security Group and Domain Admins Security Group. You can now log in with the password you created during installation. You may be prompted to change the password. If so, create a strong password, that follows your organizational password policy for administrators.

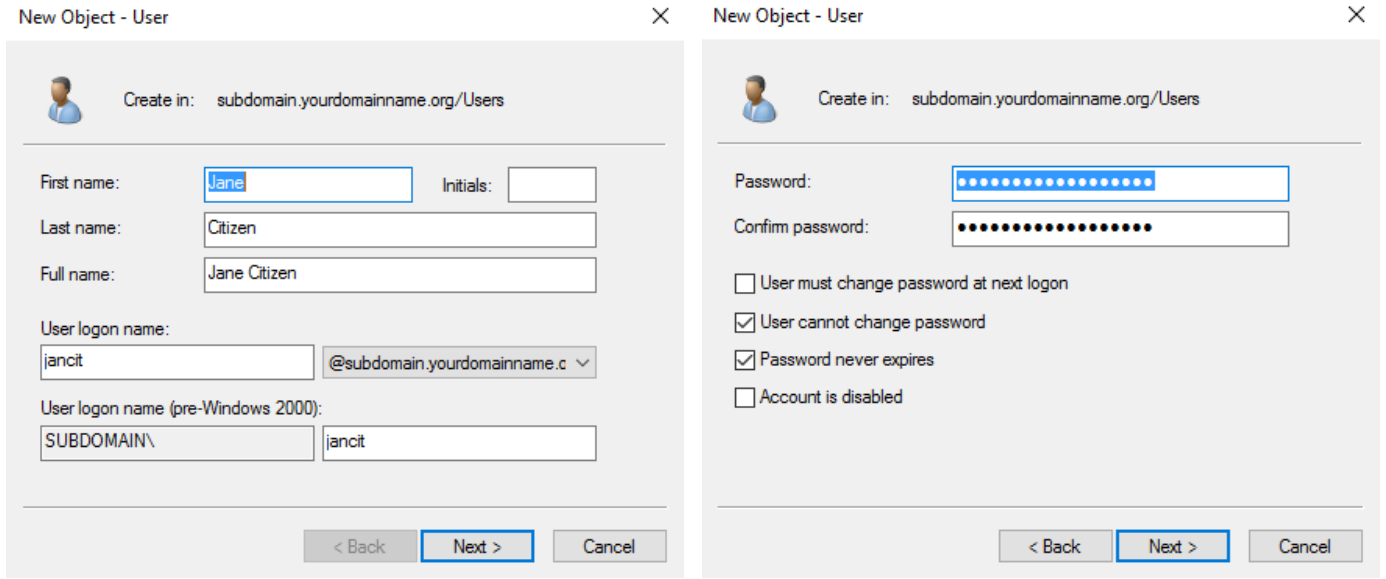
Every time you log into the server, Server Manager will launch at startup, unless you disable it.

Create a New Administrator Account

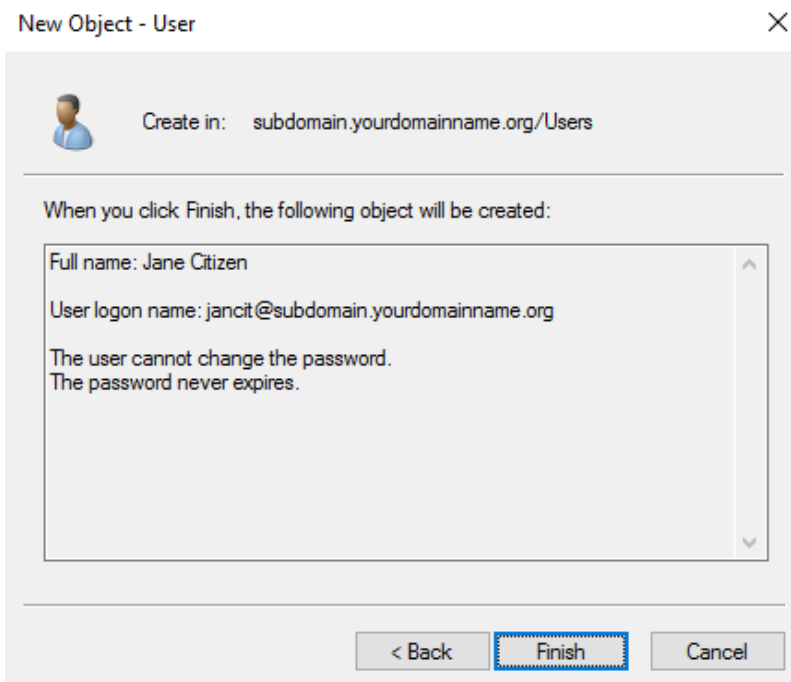
1. Open Active Directory Users and Computers from the Server Manager Tools Menu.



2. Right-click on the Users Container, hover your cursor over New and select User.



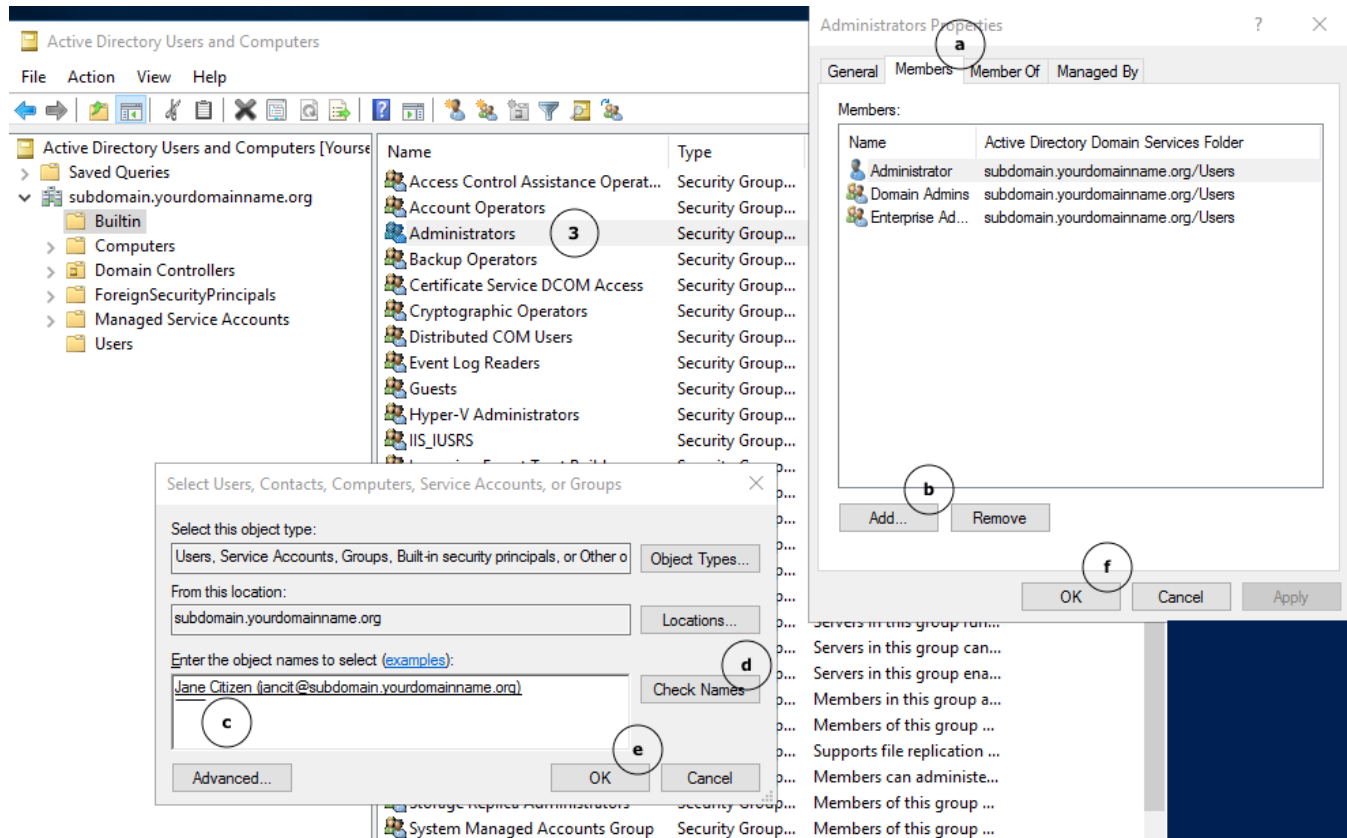
3. Enter the First name, Last name, and User logon name. Follow the naming convention designated by your Technology Policy.
4. Click Next.
5. Enter a strong password, following your organizational password policy for administrators.
6. Check the boxes User cannot change password, and Password never expires.
7. Click Next.



8. Review the summary.
9. Click Finish.

Add Your New Administrator Account to the Built-In Administrators Security Group

1. Open Active Directory Users and Computers from the Server Manager Tools Menu.
2. Click on the Builtin Container on the left.



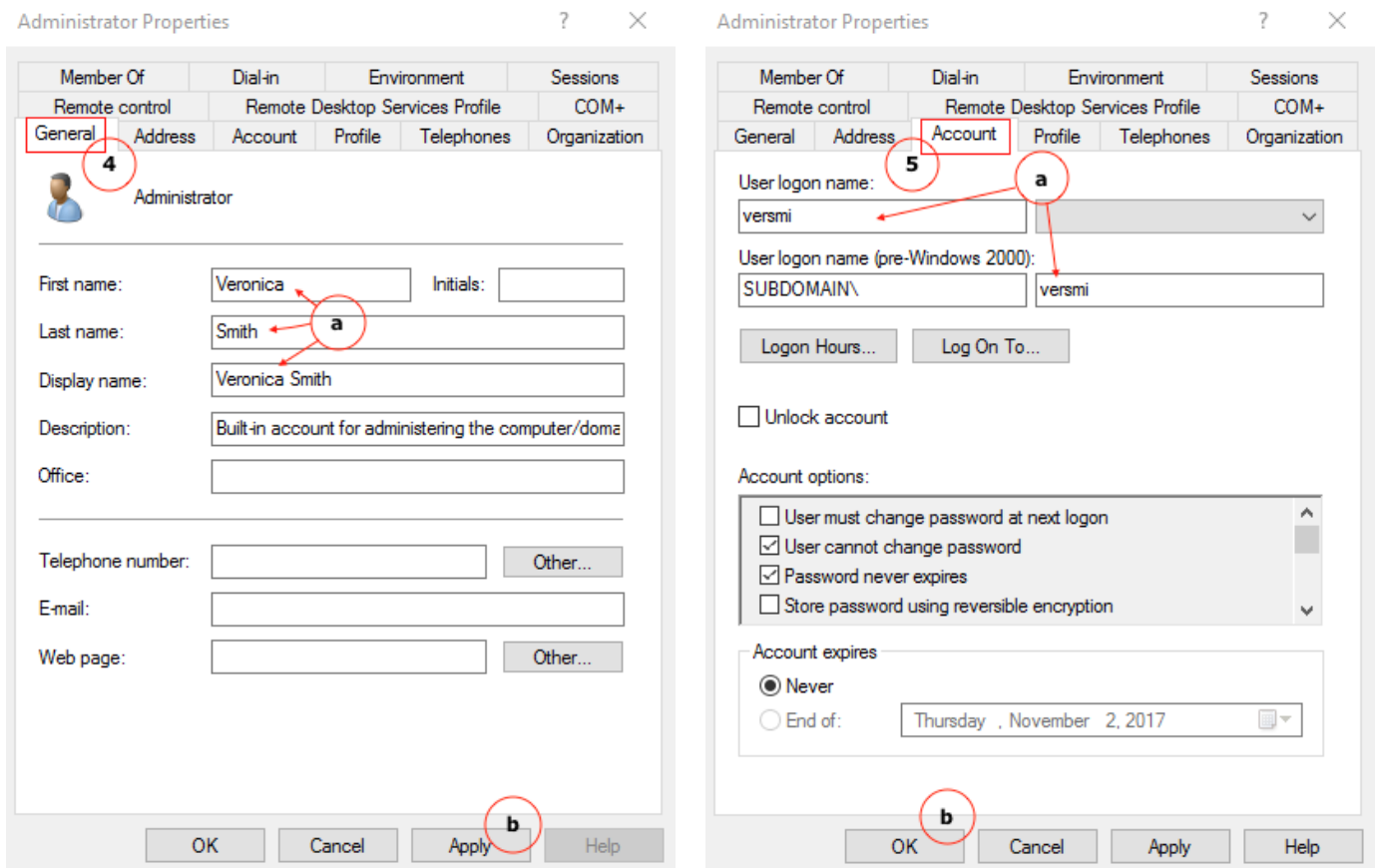
3. In the right-hand pane, double-click on the Administrators Security Group to open the Properties.
 - a. Click on the Members tab.
 - b. Click Add...
 - c. Type a portion of the username in the Object names to select box.
 - d. Click Check Names, and if the name is found, it will auto complete in the Object names box.
 - e. Click OK in the Select Users box.
 - f. Click OK in the Administrators Properties box.

Secure the Built-in Administrator Account

Now that you have created a new user account that is assigned to the Domain-level Built-in Administrators Security Group, sign out and log back in with your new domain account.

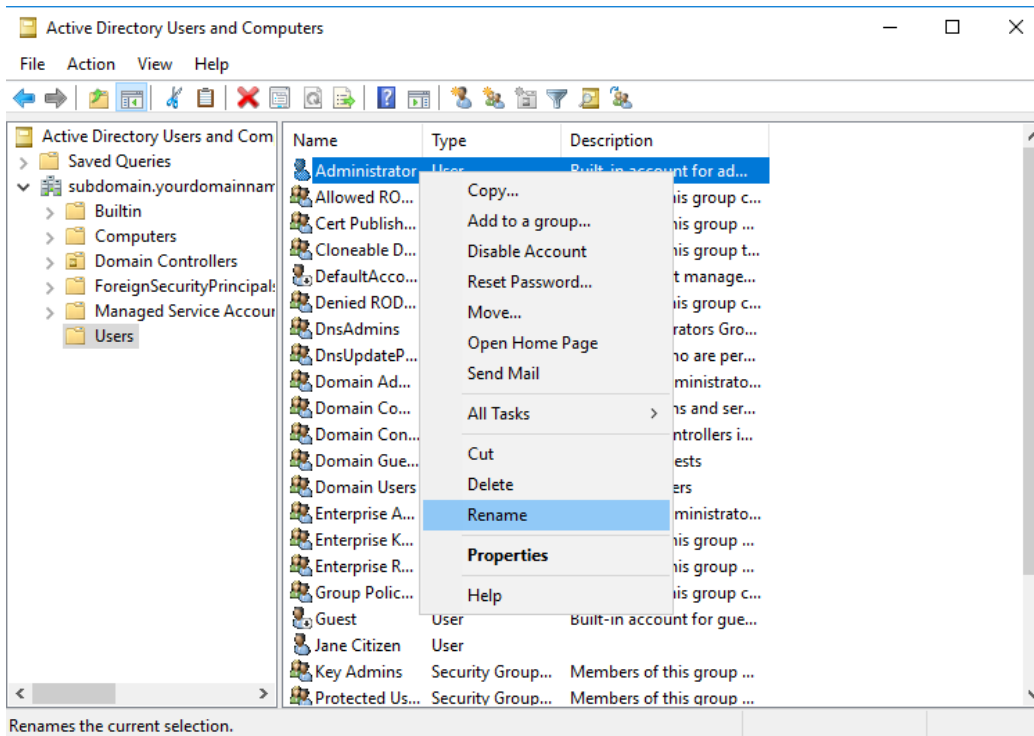
Consider renaming the Built-in Administrator account. One suggestion would be to use a similar naming convention (yet an uncommon name) as your other user accounts.

1. Open Active Directory Users and Computers from the Tools Menu.
2. Click on the Users Container on the left.
3. In the right-hand pane, double-click on the Administrator user account.



4. This will open the General tab of the Administrator Properties.
 - a. Enter the First name, Last name and Display Name.
 - b. Click Apply.
5. Click on the Account Tab.
 - a. Update the User logon name, and the right-side User logon name (pre-Windows 2000) field.
 - b. Click OK.

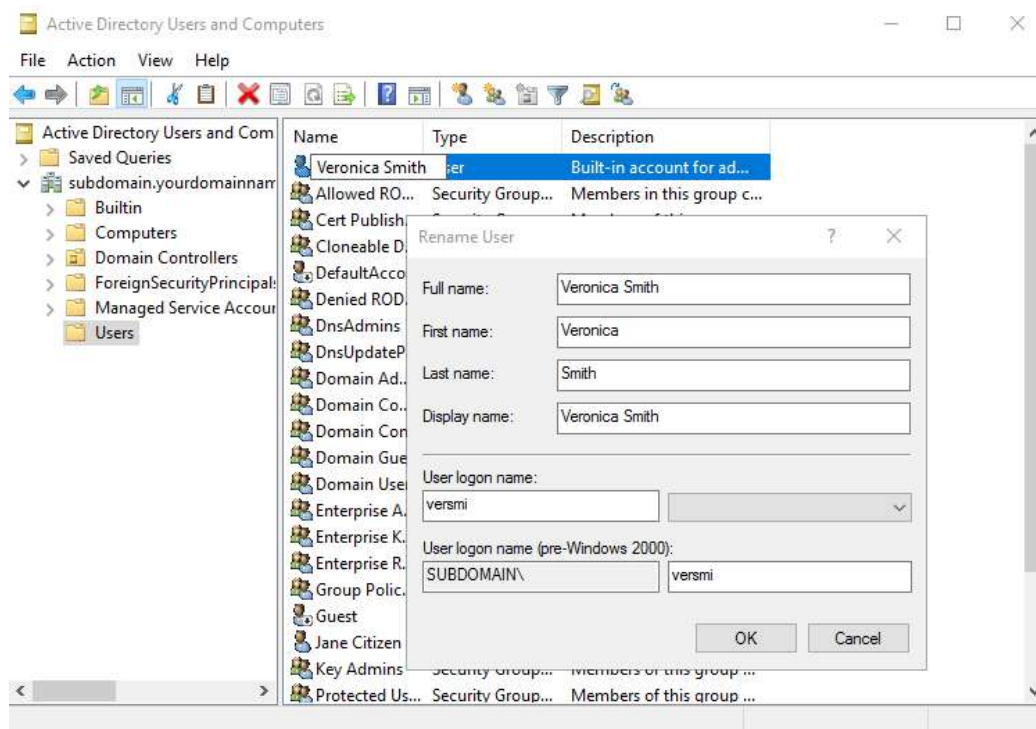
6. Open Active Directory Users and Computers.



Renames the current selection.

7. Right-click on the Administrator user, and select Rename.

- a. Type in the First name and last name of the Username you want to use.
- b. Press Enter.



- c. The Rename User window will appear to confirm the User logon name, and allow you to make any additional changes. Click OK.

NOTE: Even though you have changed the Administrator name and logon name, the User profile will continue to be labeled as Administrator (C:\Users\Administrator).

8. Right-click on the Built-in Administrator account, and then select Properties. Now we will enable the Account is sensitive and cannot be delegated flag, and disable the account.

- a. Click on the Account Tab.
- b. In the Account options section, make sure the following boxes are checked:
 - i. Password never expires
 - ii. Account is disabled
 - iii. Account is sensitive and cannot be delegated.
- c. Click OK.

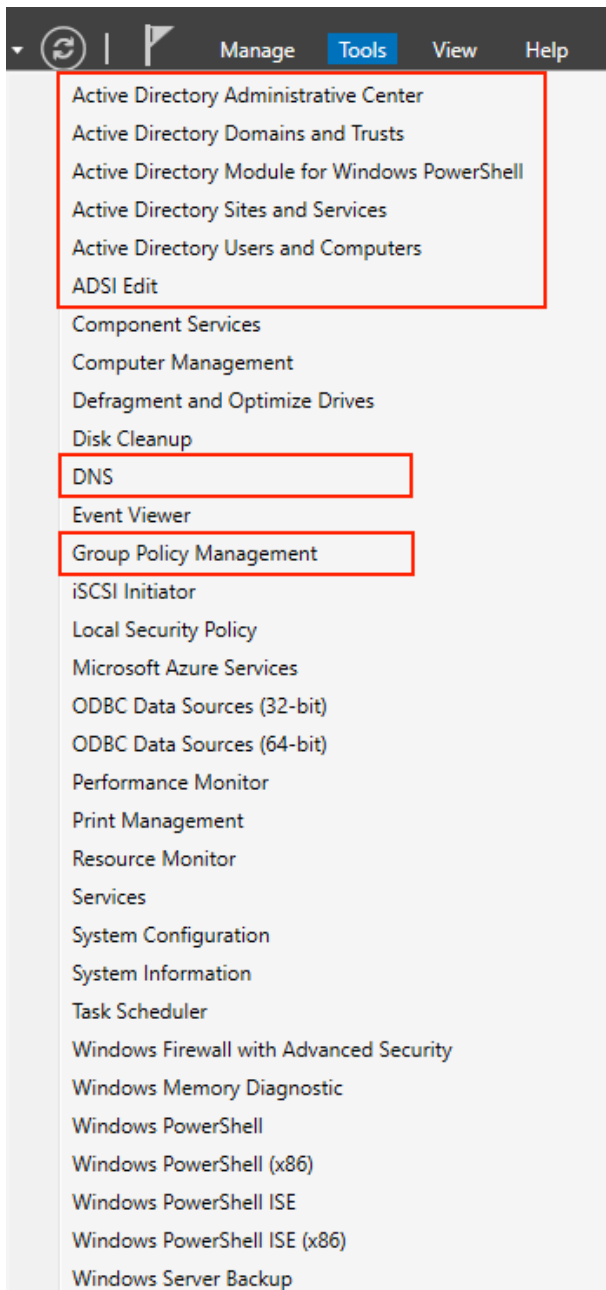
Double-check Active Directory Users & Computers to verify that the account is Disabled.
The user icon should have a down arrow next to it:



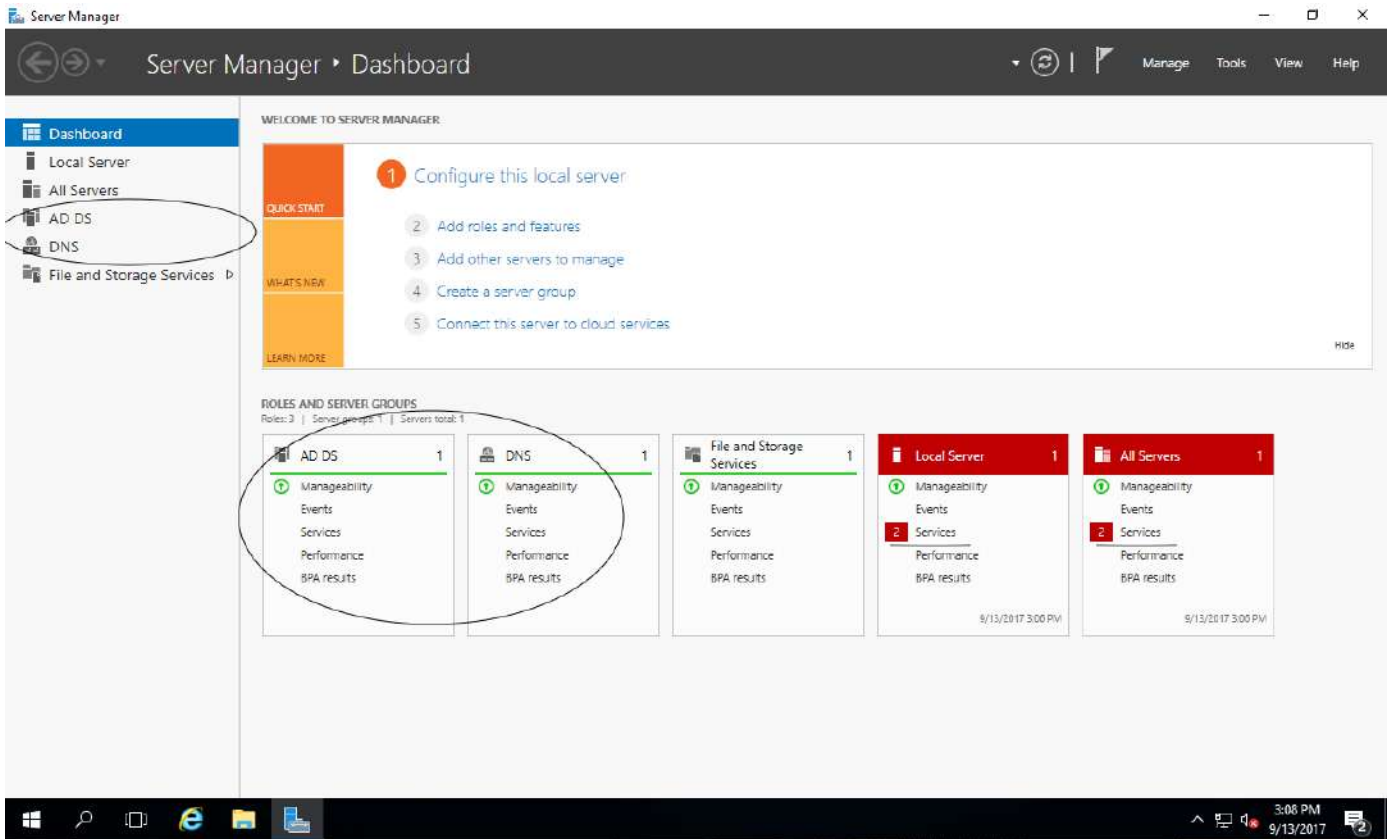
For additional options to secure the Built-in Administrator account using Group Policy, visit <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory>

ADDRESSING ERRORS

Let's go back to Server Manager and take a look at the Dashboard. You have completed the installation of one Active Directory and DNS server for your domain.



Notice your Tools Menu has expanded to include the Active Directory Management modules, ADSI Edit, DNS & Group Policy Management.



The new Roles have also been added to the Dashboard. Each item listed in the boxes under the Roles and Server Groups are links. From the Dashboard, you can quickly access Manageability, Events, Services, Performance and BPA results, grouped by Roles.

Now we will verify that everything is working properly.

Notice the 2 RED boxes under Roles and Server Groups. This indicates that there are Warnings or Errors. Click on Services under Local Server.

Local Server - Services Detail View

2 Services Hide Alert Criteria

Start types: Service status:
 Services: Servers:

Server Name	Display Name	Service Name	Status	Start Type
YOURSERVERNAME	Downloaded Maps Manager	MapsBroker	Stopped	Automatic (Delayed Start)
YOURSERVERNAME	Sync Host_119796	OneSyncSvc_119796	Stopped	Automatic (Delayed Start)

Go To Local Server

Two Services are listed as being Stopped with an Automatic (Delayed Start): Downloaded Maps Manager and Sync Host_119796. Eventually, the OneSyncSvc_119796 Stopped Service Notification will resolve without any further action and will no longer be listed.

The MapsBroker Service can be disabled. This is not needed on a Server. To disable this Service:

1. Open the Tools menu from the Server Manager Dashboard.
2. Click on Services.
3. Scroll down to Downloaded Maps Manager, and double-click on it.
4. This opens the Downloaded Maps Manager Properties. Change the dropdown menu for Startup type to: Disabled.
5. Click OK.

If you find that at a later time, you need this Service to be enabled, you can follow the same procedure, but at step #4, change the dropdown menu option to Automatic or Automatic (Delayed Start).

Event Viewer (Local)

Overview and Summary Last refreshed: 9/15/2017 11:27:47 PM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
<input type="checkbox"/> Error	-	-	-	3	56	109
	34	Time-Service	System	0	0	1
	69	AppModel-Runtime	Microsoft-Windows-AppModel-Runtime/Admin	0	14	14
	304	User Device Registration	Microsoft-Windows-User Device Registration/Admin	0	5	5
	307	User Device Registration	Microsoft-Windows-User Device Registration/Admin	0	5	5
	866	PrintService	Microsoft-Windows-PrintService/Admin	0	4	12
	1002	ThinPrint AutoConnect	ThinPrint Diagnostics	0	3	3
	1008	Perflib	Application	0	1	3
	1202	ADWS	Active Directory Web Services	0	2	5
	1202	DFSR	DFS Replication	0	2	9
	7023	Service Control Manager	System	0	4	20
	8198	Security-SPP	Application	0	0	5
	10016	DistributedCOM	System	3	16	27
<input type="checkbox"/> Warning	-	-	-	0	19	136
<input type="checkbox"/> Information	-	-	-	19	819	2,914

Recently Viewed Nodes

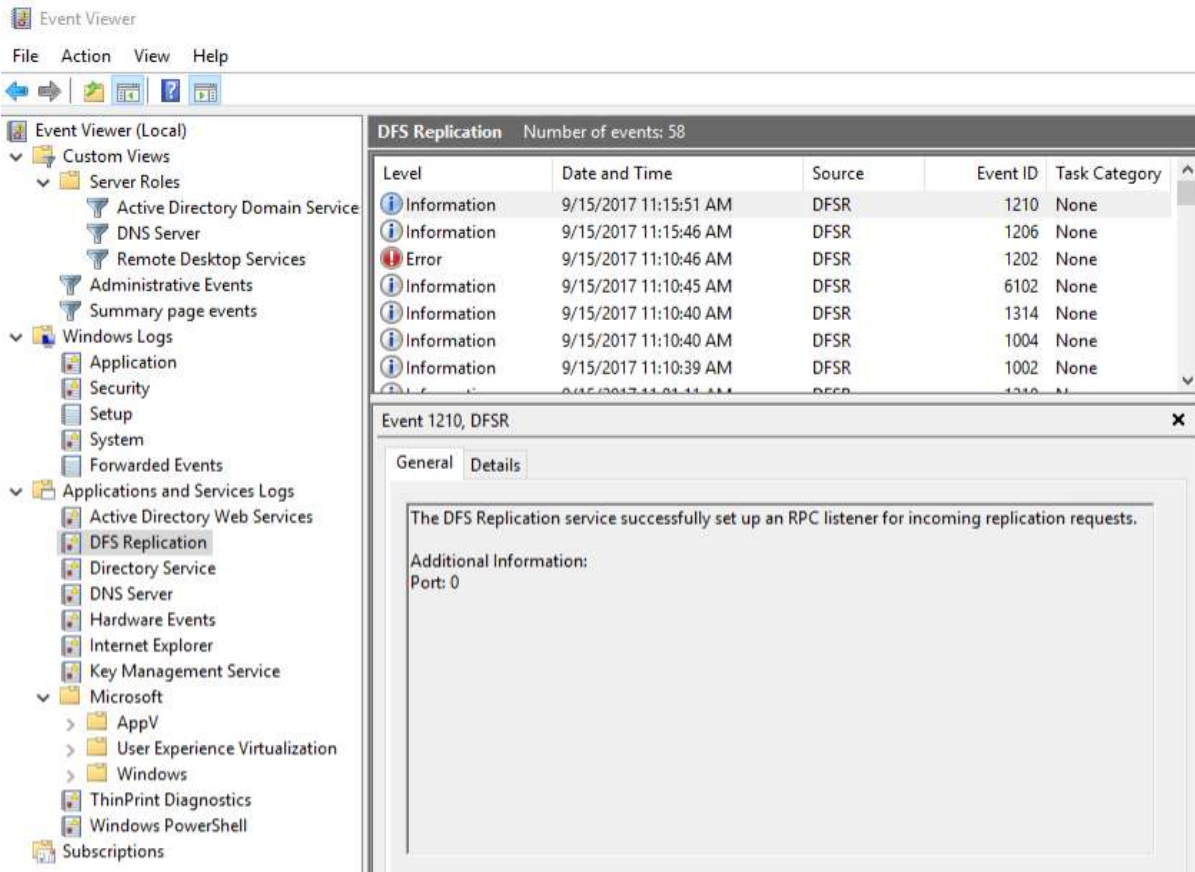
Log Summary

Log Name	Size (Curr...	Modified	Enabled	Retention Policy
Active Directory Web Ser...	68 KB/1.0...	9/15/2017 11:11:40 AM	Enabled	Overwrite events as necessary (oldest events first)
Application	1.07 MB/2...	9/15/2017 11:11:24 AM	Enabled	Overwrite events as necessary (oldest events first)
DFS Replication	68 KB/14...	9/15/2017 11:11:39 AM	Enabled	Overwrite events as necessary (oldest events first)
Directory Service	68 KB/1.0...	9/15/2017 11:11:24 AM	Enabled	Overwrite events as necessary (oldest events first)
DNS Server	68 KB/100...	9/15/2017 11:11:40 AM	Enabled	Overwrite events as necessary (oldest events first)
Hardware Events	68 KB/20 ...	5/23/2017 10:03:44 AM	Enabled	Overwrite events as necessary (oldest events first)

To look for other errors you may need to address, from the Server Manager, open the Tools Menu and click on Event Viewer. The Event Viewer will launch displaying the Overview and Summary, which includes a Summary of Administrative Events, Recently Viewed Nodes, and the Log Summary.

Under the Summary of Administrative Events each Event Type can be expanded. Expand the Error section. Double-click an error you would like to review to get more information.

Sometimes, you will see Errors or Warnings that end up being resolved in a subsequent logged event. This can commonly occur after a restart, if the services do not start in the correct order.



In which case, you will want to review not only the Errors Summary, but take a look at the complete event log for the specific Application or Service using the Console Tree on the left side of the window.

If you have unresolved errors, clear the logs and let the server sit for 24 hours and then revisit the logs. If the same error occurs after the 24-hour mark then these will need to be researched to ensure your domain is healthy. Unresolved errors can be researched online using Google or Microsoft's website to find resolutions.

Troubleshooting Tools

Top Support Solutions for Windows Server 2016:

<https://docs.microsoft.com/en-us/windows-server/troubleshoot/windows-server-support-solutions>

Microsoft offers several Free Tools for troubleshooting:

DCDiag: <http://technet.microsoft.com/en-us/library/cc731968.aspx>

ADSIEdit: [https://technet.microsoft.com/en-us/library/cc773354\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx)

DSACLs, Directory Services Access Control Lists Utility: [https://technet.microsoft.com/en-us/library/cc771151\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771151(v=ws.11).aspx)

DFSUTIL, Distributed File System Utility: <https://technet.microsoft.com/en-us/library/cc962134.aspx>

DNSCMD, DNS Server Troubleshooting Tool: [https://technet.microsoft.com/en-us/library/dd197560\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd197560(v=ws.10).aspx)

REPADMIN, Replication Diagnostics Tool: [https://technet.microsoft.com/en-us/library/cc770963\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc770963(v=ws.11).aspx)

NETDOM, Windows Domain Manager: [https://technet.microsoft.com/en-us/library/cc772217\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc772217(v=ws.11).aspx)

Windows Sysinternals

<https://docs.microsoft.com/en-us/sysinternals/>

Project Honolulu

<https://blogs.technet.microsoft.com/servermanagement/2017/09/22/project-honolulu-technical-preview-now-available/>

Additional Free Active Directory Tools from ManageEngine:

<https://www.manageengine.com/products/free-windows-active-directory-tools/free-active-directory-tools-index.html>

DNS SERVER CONFIGURATION

Definitions

Domain Name System – The decentralized, hierarchical, rule-based, database system of mapping and translating domain names, using records, predominantly to ip addresses (hosts). This system enables computer users to more easily access network resources like the internet and email, by remembering words rather than numbers. Initially, the Domain Name System concepts were developed to support ARPANET email communications.

Domain Name – Using the rules and procedures defined by the Domain Name System, the Domain Name is the portion of a url (uniform resource locator) or network address that classifies the ownership of resources being accessed.

Authoritative – Defined as the trusted primary source for the DNS records in a zone owned by an organization or entity.

Fully Qualified Domain Name (FQDN) – The absolute domain name for domain resource, specified by a trailing dot. Ex. www.domainname.com[.]

Zone(s) – A database logically dividing or compiling the records administered for a domain name. A domain name can have one or more zones.

Host(s) – The unique network devices providing the services included in the zone for a domain name.

Records – An standardized list of permissible resource labels to define the services available for a domain name zone.

Common Record Types:

Start of Authority (SOA) – A record that contains the primary details about the management of a domain name. It will list the primary name server, the zone administrator's email address, the serial number, and zone refresh timers (TTL). The domain name registrar maintains this information.

A / AAAA – Resource record used to correlate a subdomain name to an ip address.

CNAME – This is another term for Alias. This record is going to be a subdomain within the same zone or another domain name that has a corresponding A record backed by a network device configured to respond to requests for that domain name. CNAME records will not be an ip address.

MX – Email resource records. This record will be a subdomain with the same zone or another domain name, with a corresponding A record backed by an email server or network device that processes email (ex. Spam filter). MX records will not be an ip address.

Name Server (NS) – These are the authoritative servers containing the primary zone information for a domain name.

Time to Live (TTL) – The amount of time configure with each record in a zone that designates when the record expires, and the DNS requester should check the zone again for changes.

TXT – Text records contains machine-readable data. Used for SPF, DKIM, DMARC, etc.

Service Locator (SRV) – Contain hostname and port number details for the servers supporting specific services. Can be used in place protocol specific records, like MX.

PTR – Reverse Record. It is a map for the ip address back to the name, written as last octect first, ex. 1.0.168.192.in-addr.arpa. IN PTR dns1.example.org. The ISP where the network device is hosted, maintains this record type..

Top-Level Domain – Managed by ICANN (Internet Corporation for Assigned Names and Numbers), TLDs are at the highest level of DNS, forming the root zones. Also referred to as first-level domain names. Examples of TLDs are .com, .org, .net, .edu, .gov, .mil, .us...etcetera.

Top-Level Domain Name Servers – 13 root server clusters regulate the TLD root zones. These servers are authoritative for the TLDs.

Subdomain – The named portion of a domain name that distinguishes one resource from another utilized within a domain, allowing servers at differing ip addresses to perform services for the same domain. Ex. www.domainname.com: .com = TLD (first-level domain), domainname.com = Second-level domain, www.domainname.com = Subdomain (Third-level domain)

Domain-Level Name Servers – Are the servers that have the authoritative records for a domain, or can offer referrals (iterative name queries) to another source.

Resolving Name Server – These are the ip addresses of DNS servers configured to perform recursive lookups for a client to resolve DNS requests. There are free public DNS servers available from vendors like Google and OpenDNS, or your ISP could provide them. These settings are configured in your network card properties as static or dynamic. If they are dynamic, a network configuration defines the client settings. Another device on your network, like a server or firewall, provides these services.

Forwarder(s) – A list of ip addresses of other resolving name servers outside of your network, configured in your internal DNS server, to send DNS queries for any domain names not resolvable by its cache.

Conditional Forwarder – An ip address or list of ip addresses configured in your internal DNS server to resolve queries for a specific domain name. These would be the Authoritative or Domain-Level Name servers for a domain name.

Must-Read Links!

Educause Whois

<http://whois.educause.net>

MX Toolbox Network Tools

<https://mxtoolbox.com/NetworkTools.aspx>

DNSStuff

<https://www.dnsstuff.com>

Server 2016 DNS Policies Overview

<https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/dns-policies-overview>

What's New in DNS Server in Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/networking/dns/what-s-new-in-dns-server?f=255&MSPPErr=-2147217396>

Implement Domain Name System (sample chapter from Networking with Windows Server 2016)

<https://www.microsoftpressstore.com/articles/article.aspx?p=2756482>

Best Practices Analyzer for Domain Name System: Configuration (as related to Windows Server 2008 R2, Windows Server 2012)

[https://technet.microsoft.com/en-us/library/dd391879\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd391879(v=ws.10).aspx)

DNS: Installing and Configuring Servers (as related to Windows Server 2008 R2)

[https://technet.microsoft.com/en-us/library/cc755183\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc755183(v=ws.11).aspx)

Optimizing your network to keep your DNS squeaky clean

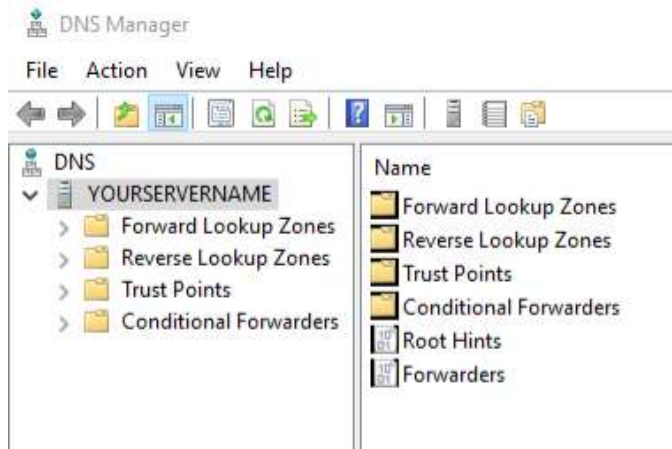
<https://blogs.technet.microsoft.com/networking/2009/02/09/optimizing-your-network-to-keep-your-dns-squeaky-clean/>

Troubleshoot DNS Problems Related to Active Directory

<https://technet.microsoft.com/en-us/library/cc526683.aspx>

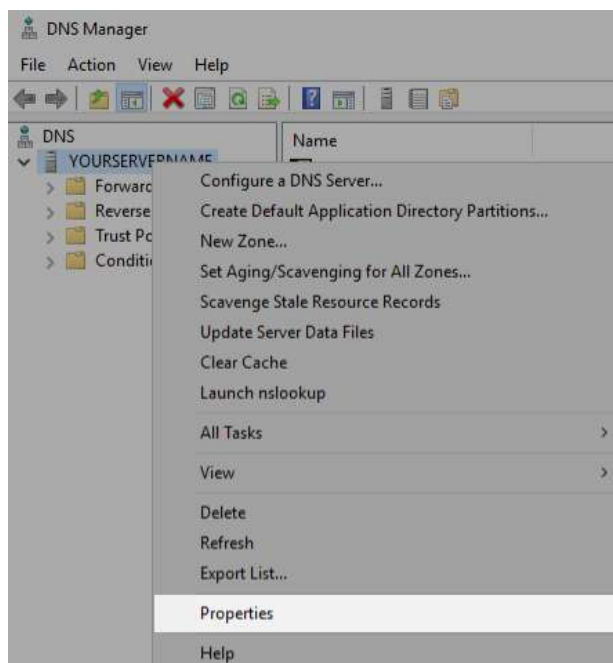
Navigating DNS Server Properties

1. Open the DNS (Manager) Console from the Server Manager Tools Menu.



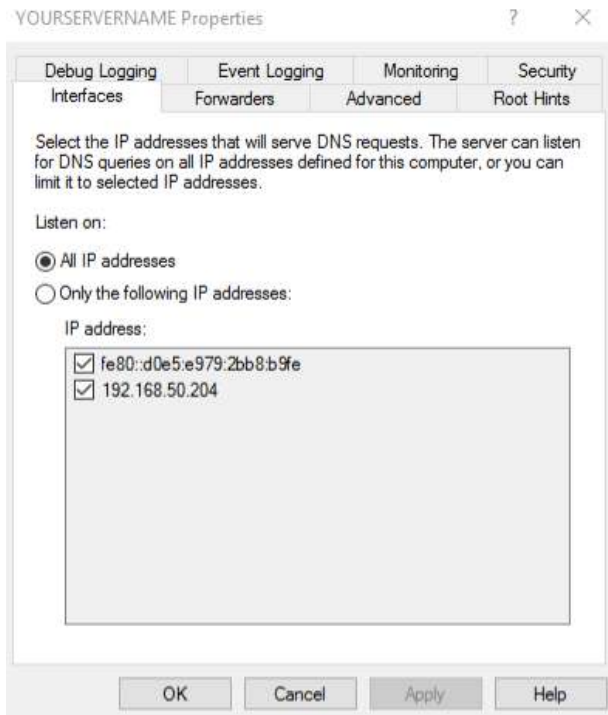
2. If the > doesn't appear, click on your server name. Then click the > beside your server name to expand the console tree.

- a. Forward Lookup Zones
- b. Reverse Lookup Zones
- c. Trust Points
- d. Conditional Forwarders



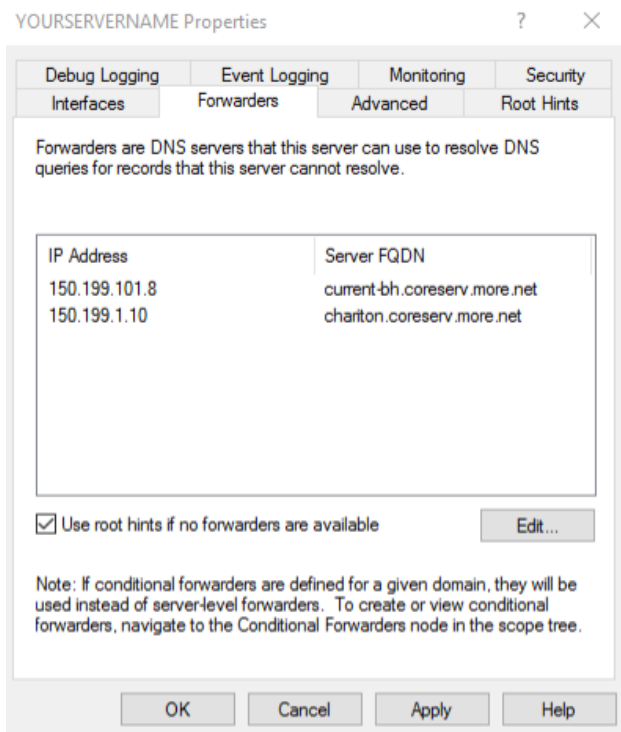
3. Right-click on your server name, and select Properties from the context menu. You can also access this option with your server name selected using the Action menu.

Interfaces Tab



- This tab allows you to designate which IP addresses are used to listen for DNS queries, TCP & UDP port 53.
- The options are All IP Addresses defined (default) or Only the following IP addresses.
- You can see which IP's are bound to this DNS server.
- There have been issues with removing IPv6 from the DNS server.
- Services such as Exchange will require that you have IPv6 enabled or they will not work properly.

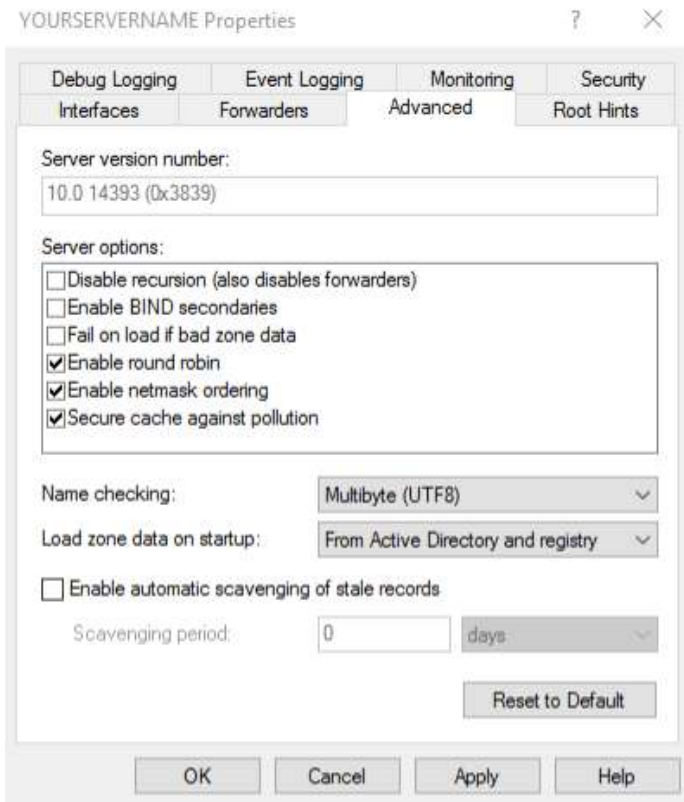
Forwarders Tab



- This tab initially displays the static IP's listed for DNS in your network interface card properties.
- Your DNS server is not authoritative for, nor can have cached, all of the website requests from the workstations in your domain. These queries will be sent to and resolved by the IP's in the Forwarders tab.
- Click Edit to add or remove IP's.
- You can add as many ip addresses as you require, or none at all.
- Use root hints if no forwarders are available checkbox; we will leave this checked. If the Forwarders fail to resolve any DNS requests, your DNS server will send the queries to the servers listed in the Root Hints tab.
- When using the MOREnet DNS servers, use at least 2 different servers assigned to your region. The IP's are available here: <https://www.more.net/services/black-hole-dns>. Click on Pricing for our Unfiltered DNS IP's. If MOREnet is your ISP, you can elect to use our BlackHole DNS service. Click on Eligibility for our

BlackHole DNS IP's. To optimize use of that service, the Blackhole IP's should be at the top of the Forwarders list.

Advanced Tab

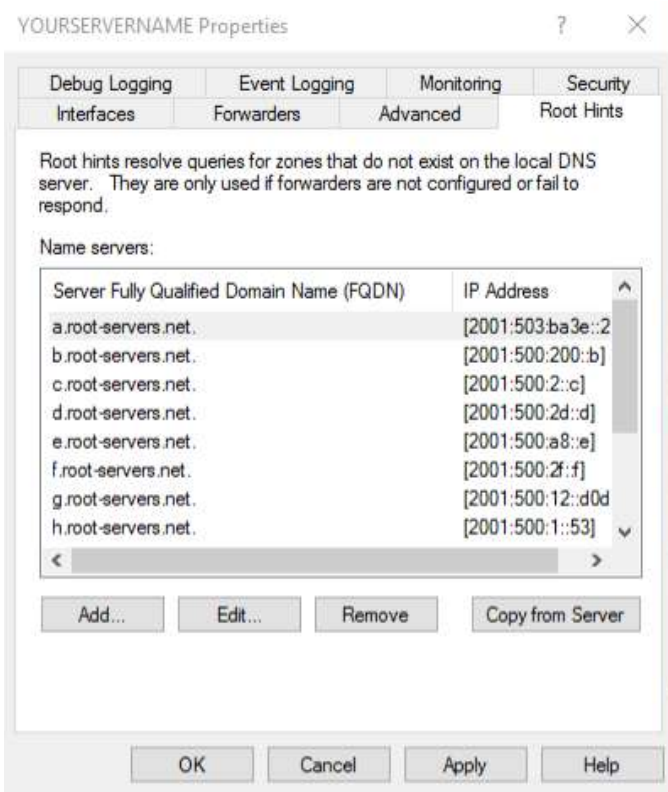


- Server version Number: Shows the current version of DNS installed.

- Server options:
 - Disable recursion: this allows for addresses to be forwarded to external DNS servers
 - BIND Secondary's: Optimizes the Zone transfer speed, Windows 2012 uses compression and submits multiple records in a packet, older BIND servers are incompatible, only check this if performing zone transfers to BIND server prior to vs. 4.9.4
 - Fail on load if bad zone data: Windows will continue to load the zone file if it detects errors; errors will be logged. Check if you want to stop loading the zone if errors are detected
 - Enable round robin: By default, DNS will rotate and re-order a list of Host records if a host is related to multiple IP addresses
 - Enable netmask ordering: If a zone has multiple Host records that map to multiple IP addresses the server checks the IP addresses of the records of the client and if one of the addresses is in the same subnet as the client it will set that address first in the list
 - Secure cache against pollution: The server will not add unrelated resource records added in a referral from another DNS server
 - Name Checking: Originally DNS could only support alphanumeric and hyphens; this causes issues with international character sets. By default Windows uses UTF8 (Unicode), which allows for the broadest and least restrictive character support. If necessary you can change this setting to RFC Strict to limit names to the standard format.
- Load Zone data on startup: You can load the zones from Active Directory, Registry or a BIND file. Loading from a BIND file allows you to duplicate a BIND server.

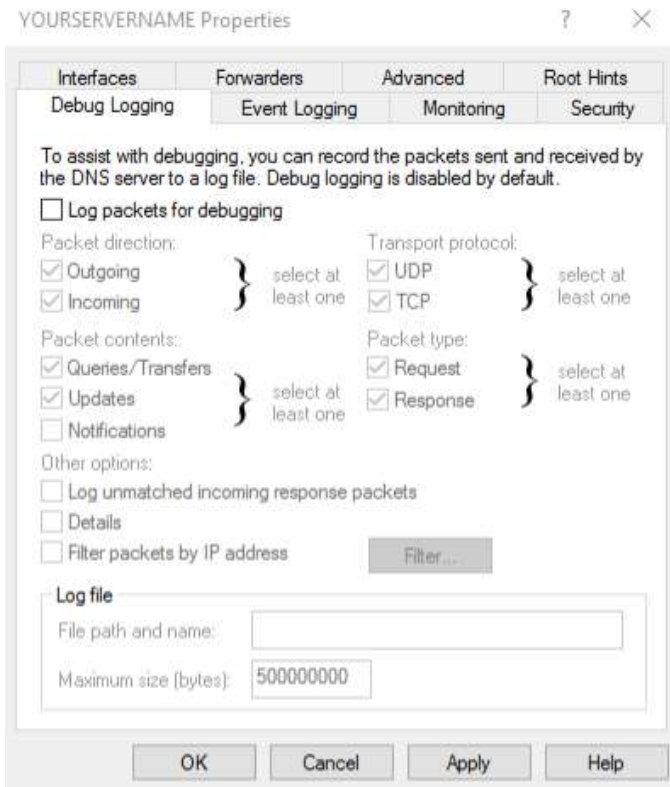
- Enable automatic scavenging of stale records: Stale records typically are those that no longer point to a host on the network. Enabling this feature will look at the timestamps and other properties. DDNS records will be automatically checked as will manual entries if a timestamp is added.
- Reset to default: Reset all Advanced settings to default values

Root Hints Tab



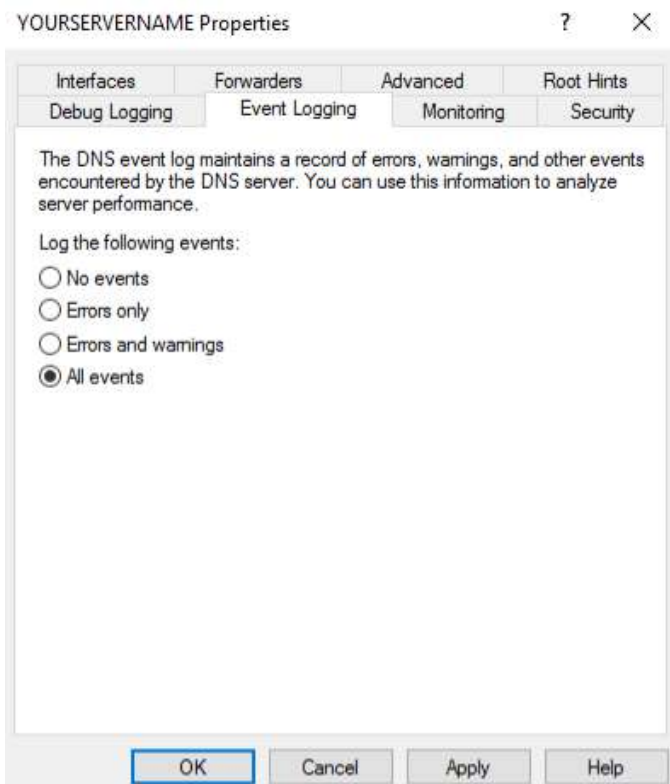
- The Root Hints tab contains a list of the names and addresses of the 13 internet root servers.
- If your local DNS server cannot resolve the DNS query, and Forwarders fail to respond or are not configured, the query is sent to one of the root DNS servers. The root server will initiate a query/referral process until your DNS server finds the authoritative host that can resolve the domain name request. Read more: <https://www.iana.org/domains/root/servers>, <http://www.root-servers.org/>
- You can add or remove entries within this list, if necessary.

Debug Logging Tab



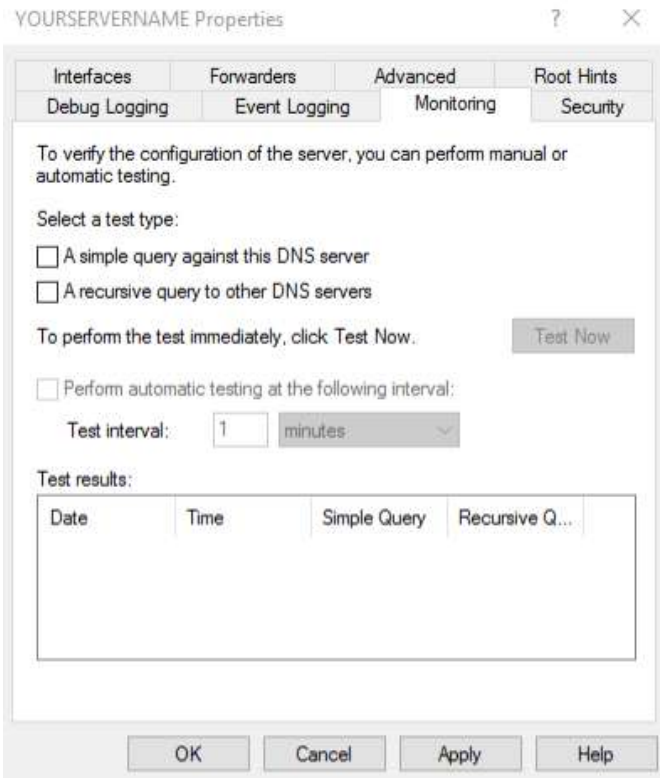
- Settings on this screen will allow you to setup packet-level logging to help troubleshoot DNS issues.
- It is disabled by default.
- To enable Debug Logging, check the box to Log packets for debugging.
- Enabling this feature may affect the performance and service delivery of your DNS server.

Event Logging Tab



- Select the level of events you want the DNS server to write to the Windows Event Logs.
- To enable Enhanced DNS logging and diagnostics, follow the procedures here, [https://technet.microsoft.com/en-us/library/dn800669\(v=ws.11\).aspx#en](https://technet.microsoft.com/en-us/library/dn800669(v=ws.11).aspx#en). The Audit events are enabled by default; however, the Analytic events are not.

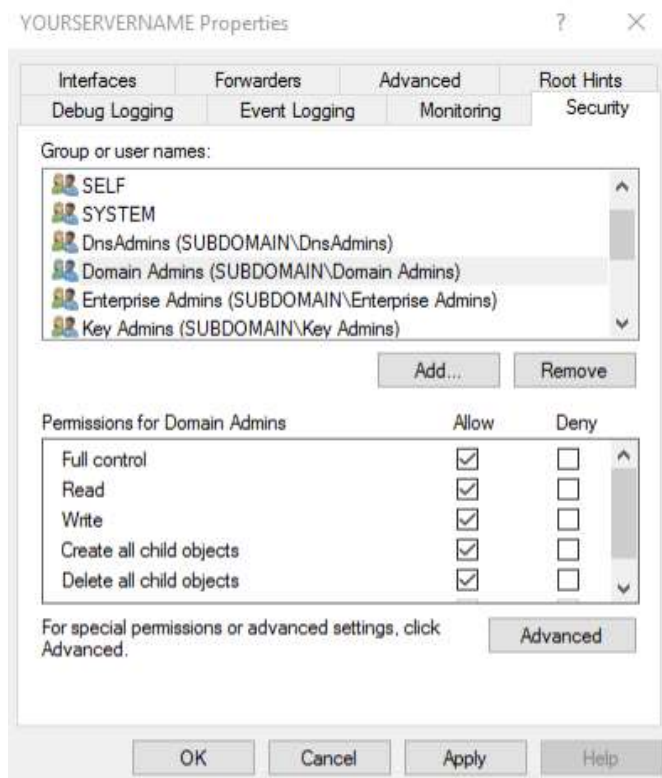
Monitoring Tab



- Used when you need to verify that your DNS is configured properly to respond to requests. Read more, <https://technet.microsoft.com/en-us/library/dd673658.aspx> (referencing Windows Server 2008).

<http://www.tech-faq.com/monitoring-and-troubleshooting-dns.html>

Security Tab



- Allows the Domain Administrator to define who has rights to manage this zone. Click Advanced for numerous granular permissions options.

This concludes the review of settings for the DNS Server Properties. You will also need to verify the settings for each Zone that you have setup.

Navigating Forward Lookup Zones

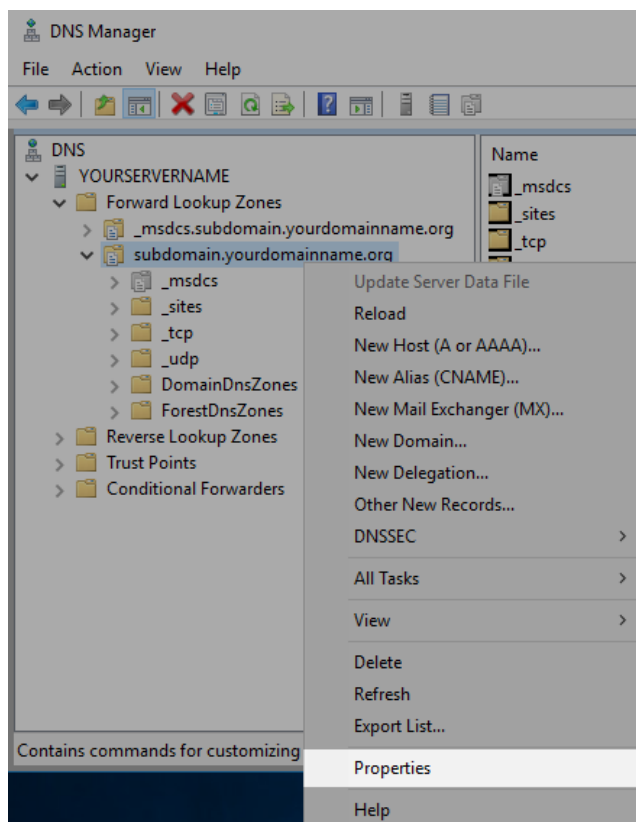
Using a web browser initiates a series of queries and responses from host to host, until the webpage loads. In all cases, there needs to be an authoritative server defined as the primary source for the domain name records. If there is no local Domain DNS server available, the workstation's query would first be processed by its local hosts file. If unresolved, the query would then go to the ip addresses listed in the DNS section of the network card properties.

In a Windows Domain, after the client checks its local hosts file, if unresolved, the DNS query is sent to the local domain DNS server. It will check the locally loaded zones to see if it can resolve the name to an ip address. If not, it will then check its local cache to see if it has resolved this in the recent past to respond to the client. If the local DNS server does not have the information stored locally, it will then FORWARD the request to the designated server(s). The query will be processed through the list of Forwarders, top to bottom, until the website address domain name query can be fulfilled.

Managing a Forward Lookup Zone (as related to Windows Server 2008)

[https://technet.microsoft.com/en-us/library/cc816891\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc816891(v=ws.10).aspx).

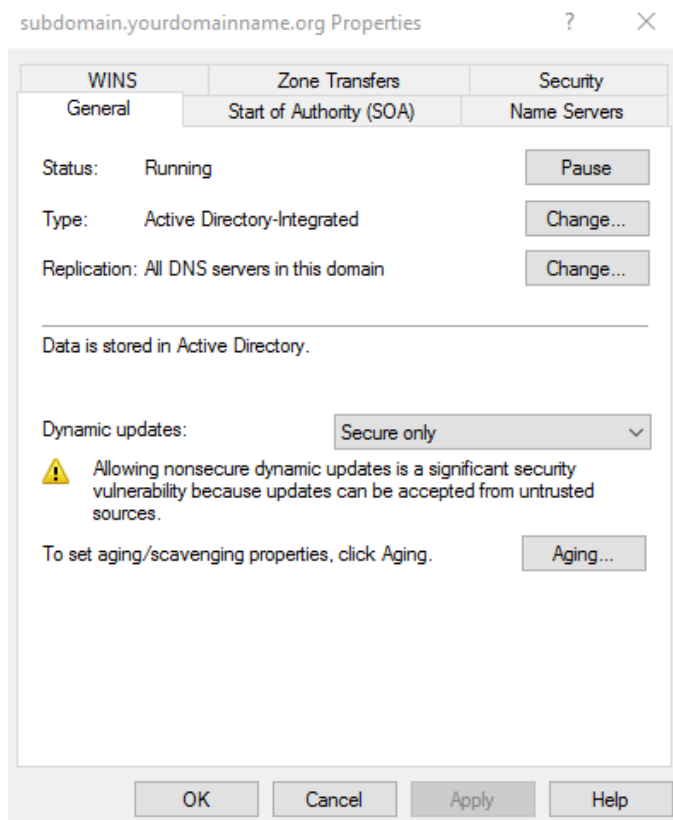
1. Open the DNS (Manager) Console from the Server Manager Tools Menu.



2. Click > next to your server name to expand the console.
3. Click > next to Forward Lookup Zones.
4. Right-click on your Domain Name. From this context menu you can initiate several tasks.
 - a. Update Server Data File
 - b. Reload the DNS zone file. Use this option when you have a secondary zone on another server. This resyncs the information from the Primary (Parent) zone.

- c. New Host (A or AAAA)...Create new host records for IPv4 (A) or IPv6 (AAAA) using domain names, subdomain names and ip addresses.
 - d. New Alias (CNAME)...This is the record type to create a new alias (subdomain name) for an existing host entry. This record will allow you to use multiple names for a single ip/host.
 - e. New Mail Exchanger (MX)...Used to add a record for a Mail Server. This is listed as a domain name, which must reference a corresponding Host (A) record. This can be a subdomain name within your zone, or another domain name depending on where your email is hosted.
 - f. New Domain...Used to link another domain to this local DNS server.
 - g. New Delegation... Allows you to define DNS servers that will handle specific Zones within your forest.
 - h. Other New Records...Used to add other record types, like PTR or NS, etc. that are not listed as options in this context menu.
 - i. DNSSEC > Sign the Zone, Unsign the Zone, or Properties
 - j. All Tasks > Update Server data file (if using a Bind file) or reload zone data
 - k. View > Allows you to modify what options you see in the Console and the layout you see it in.
 - l. Delete, Removes the highlighted zone from the server.
 - m. Refresh, Used to refresh the zone information displayed when you have made a change you are not seeing in the Console Tree.
 - n. Export List...
 - o. Properties, launches the zone properties for the domain name you have highlighted.
 - p. Help, links to the Microsoft help files for the Microsoft Management Console 3.0
5. Select Properties to open your internal domain DNS Properties.

General Tab



- o Status: Shows the current status of the zone
- o Type: Shows the type of zone. The options are Primary, Secondary or stub. You also have the option to Store this zone in Active Directory (ONLY available on a Domain Controller). Click Change to adjust the options. (see fig.1 on the following page)
- o Replication: Define how you want your DNS Zone to be replicated to other domain controllers. The options are Replicate to: All DNS servers in this forest, All DNS servers in this domain, or All domain controllers (for Windows 2000 compatibility). For redundancy and consistency, you should replicate your DNS to all DNS servers in this domain. Click Change to adjust the options. (see fig.2 on the following page)
- o Dynamic Updates: By default, this is set to secure only. If have older clients on your network you may need to change this to Nonsecure and secure (not recommended). You can also choose NONE, to disable dynamic updates, but then you would have to enter any client updates manually.

- To set aging/scavenging properties: This allows your DNS to check the timestamp of entries in this zone and mark them for deletion if they are past a specific date. Click Aging to adjust the settings. (see *fig.3 on the following page*). If preferred, Check the box to enable Scavenge stale resource records.

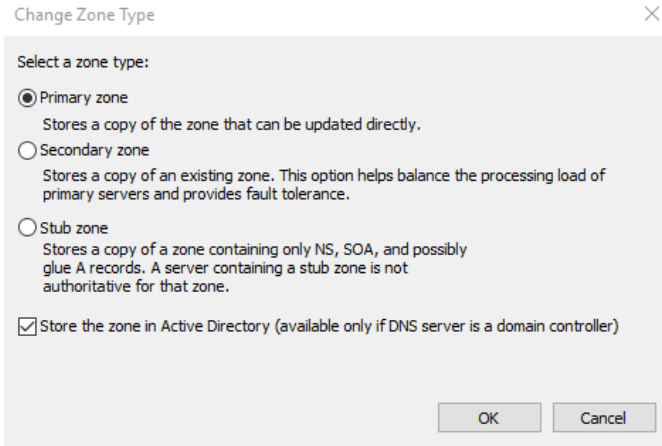


Fig.1 If you make changes, click OK.

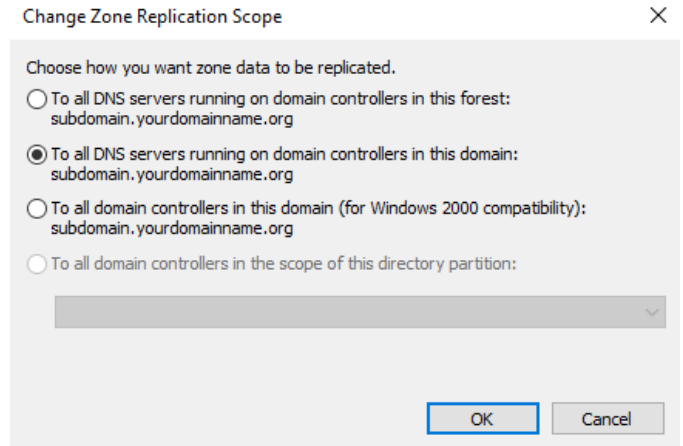


Fig.2 If you make changes, click OK.

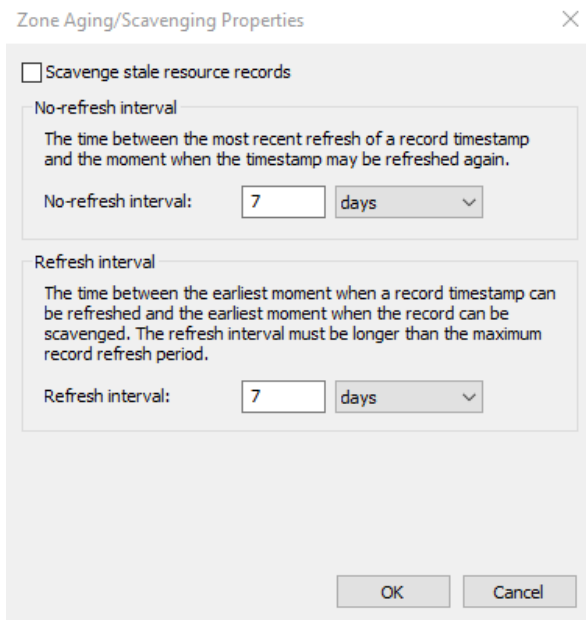


Fig.3 If you make changes, click OK.

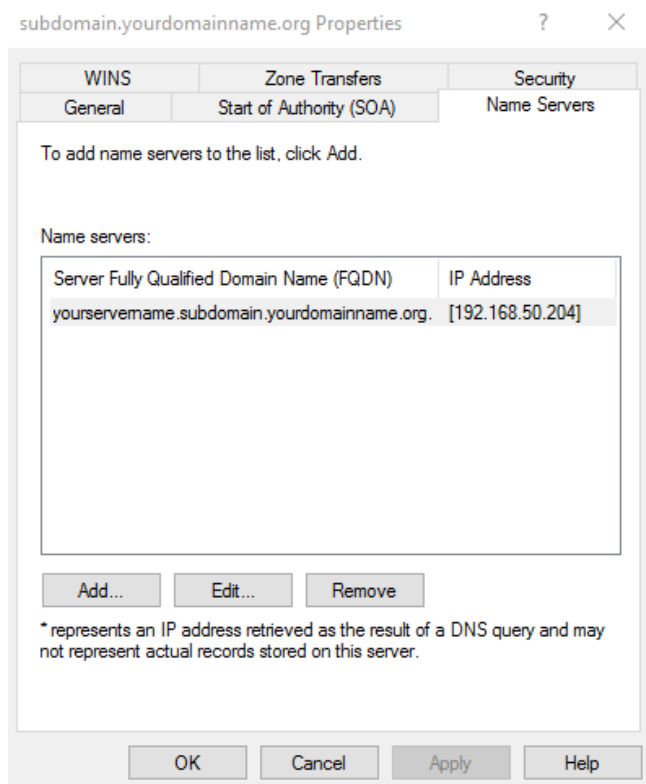
Start of Authority Tab

- Serial Number: Each time the zone file is loaded and changed the serial number will increment. If the serial numbers do not match, this will initiate a zone transfer to other DNS servers in the domain.
- Primary Server: Lists the primary DNS server within the domain. This can be changed to another DNS server within your domain, if you are experiencing issues with your primary server.
- Responsible Person: This shows the email of the DNS administrator. The @ symbol is not used. Default is hostmaster.
- Refresh Interval: the interval at which other DNS servers that host the zone should refresh their data from this server.
- Retry interval: This setting determines how often other DNS servers should retry a request to update the zone.
- Expires after: Determines the interval that other DNS servers that host the zone will expire the zone data if they are unable to contact the Primary server.
- Minimum (default) TTL: Time To Live for a zone

record; this determines how long other DNS servers should cache this record before discarding it, and check for a new record.

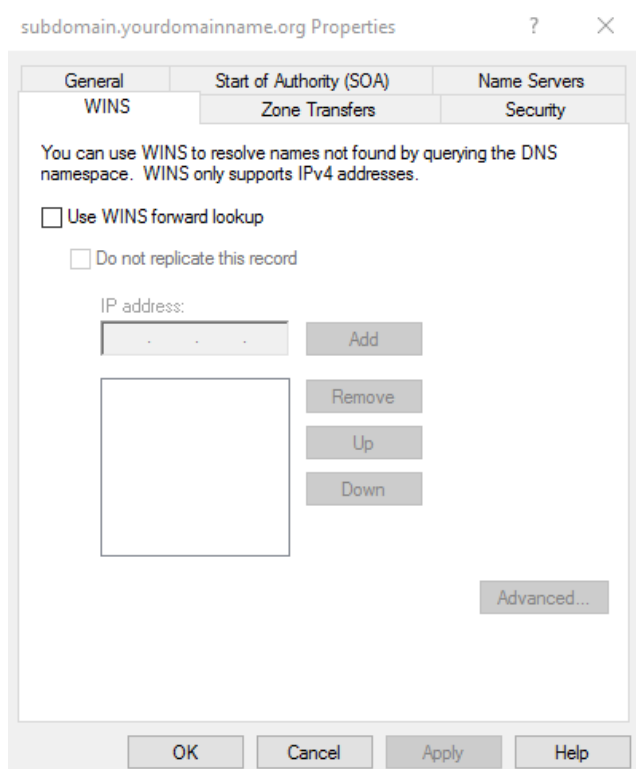
- TTL for this record: defines the TTL for this record

Name Servers Tab



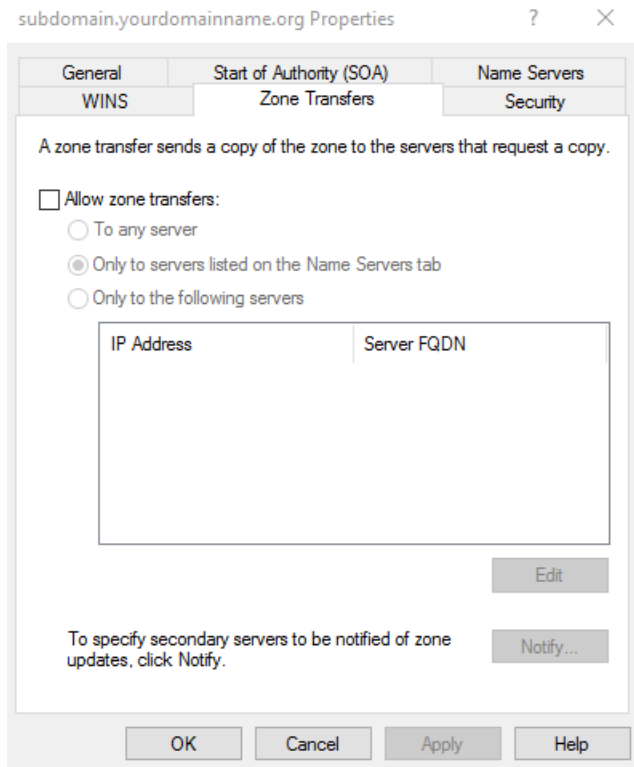
- Name Servers: Lists the FQDN and IP of the Name Servers that are authoritative for this zone. This will be the primary and any read-only secondary servers configured with this zone.
- Add: Enter additional Name Servers. You can add DNS servers outside your domain, as long as they are configured as authoritative for the zone.
- Edit: Edit the existing Name Server entries.
- Remove: Delete decommissioned or incorrect Name Servers.

WINS Tab



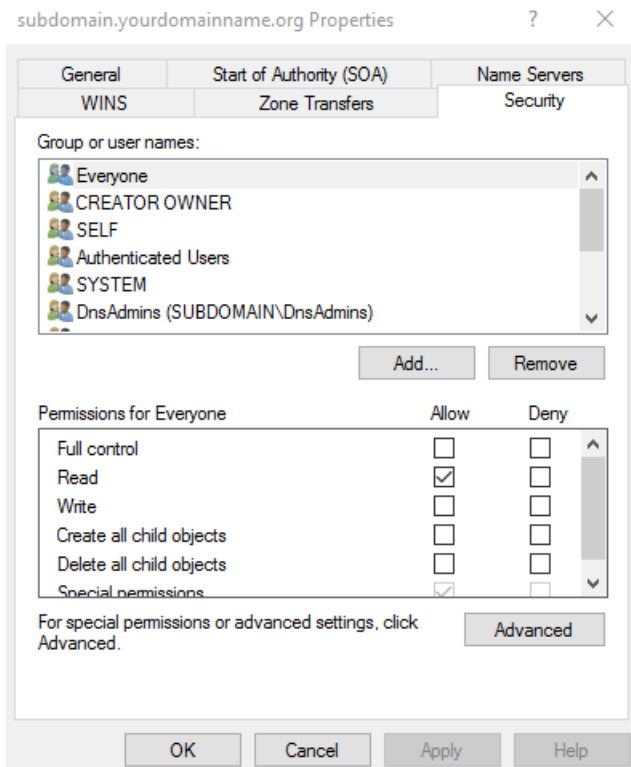
- Use WINS forward lookup: Check this box if you have and want to use a local WINS server for local forward lookups.
- Do not replicate this record: Check this box if you do not want to replicate this WINS setting to other DNS servers.
- IP Address: Add the IP addresses of the WINS servers on your network.

Zone Transfers Tab



- Allow Zone transfers: allows you to transfer the zone to other DNS servers. You would check this option if you have secondary authoritative servers for this zone.
 - (Default) To Any server: Allows any DNS servers to request a zone transfer from your server ***NOT SECURE**
 - Only to servers listed in the Name Servers tab: Allows the zone to be transferred to defined servers in the Name Servers tab. We will use this option.
 - Only to the following servers: allows you to define the servers allowed to request Zone transfers from this DNS server. Use this option, if different than what is in the Name Servers tab.
- To specify secondary servers to be notified of zone updates: Enables this server to automatically notify secondary servers when this zone is updated, and designate which servers to notify.

Security Tab



- Allows the Domain Administrator to define who has rights to manage this zone. Click Advanced for numerous granular permissions options.

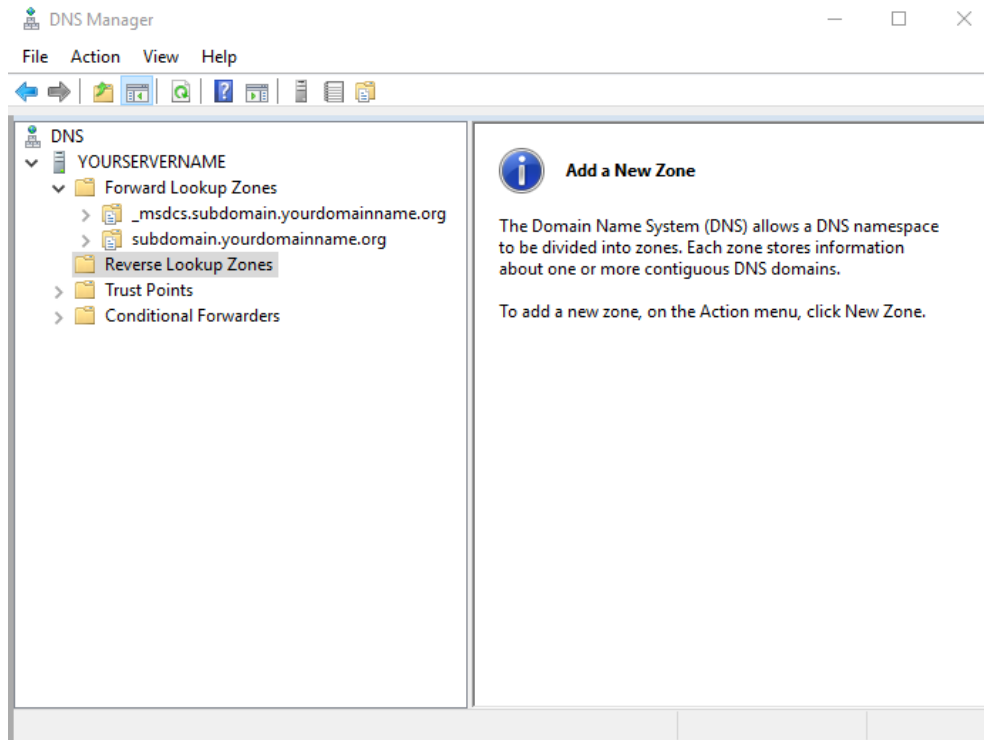
This completes the settings for the DNS zone.

Creating Reverse Lookup Zones

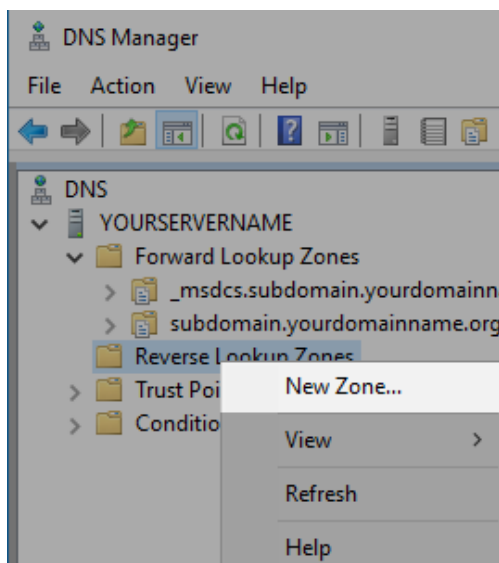
To create the reverse namespace, subdomains within the in-addr.arpa domain are formed, using the reverse ordering of the first three octets in the IP address of a host, plus the subdomain name of the host. While IETF RFC Standards do not require Reverse or PTR records, certain networked applications will require you to have Reverse DNS setup, as a function of security. Such examples include email services and spam filtering, ping and traceroute, Kerberos, Oracle Scan VIPs, etc.

Understanding Reverse Lookup (as related to Windows Server 2008 R2)

[https://technet.microsoft.com/en-us/library/cc730980\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc730980(v=ws.11).aspx)



1. Open the DNS (Manager) Console from the Server Manager Tools Menu.
2. Click > next to your server name to expand the console.



3. Right-click on Reverse Lookup Zones and select New Zone....

The Wizard

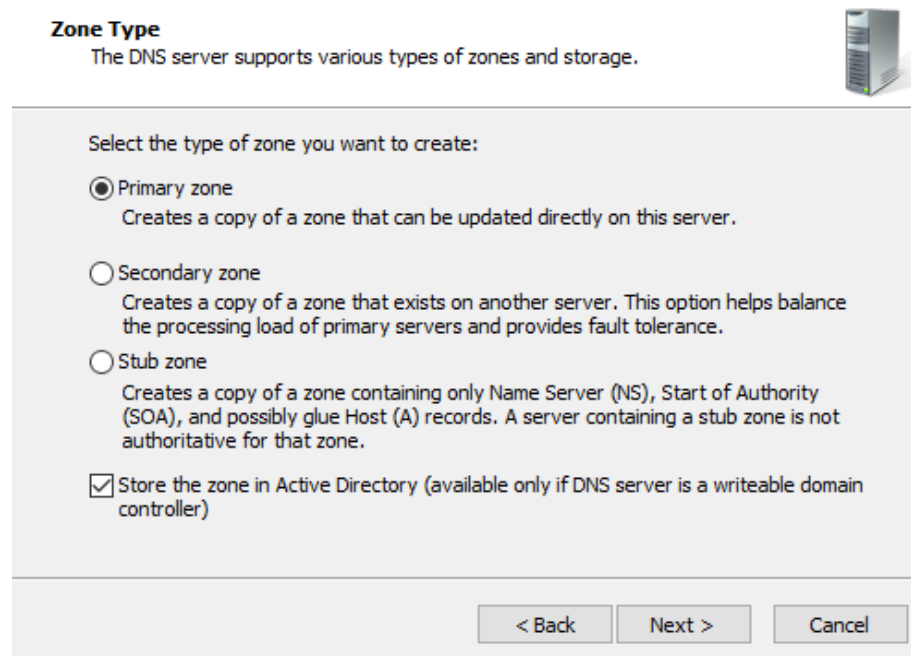
New Zone Wizard



1. New Zone Wizard

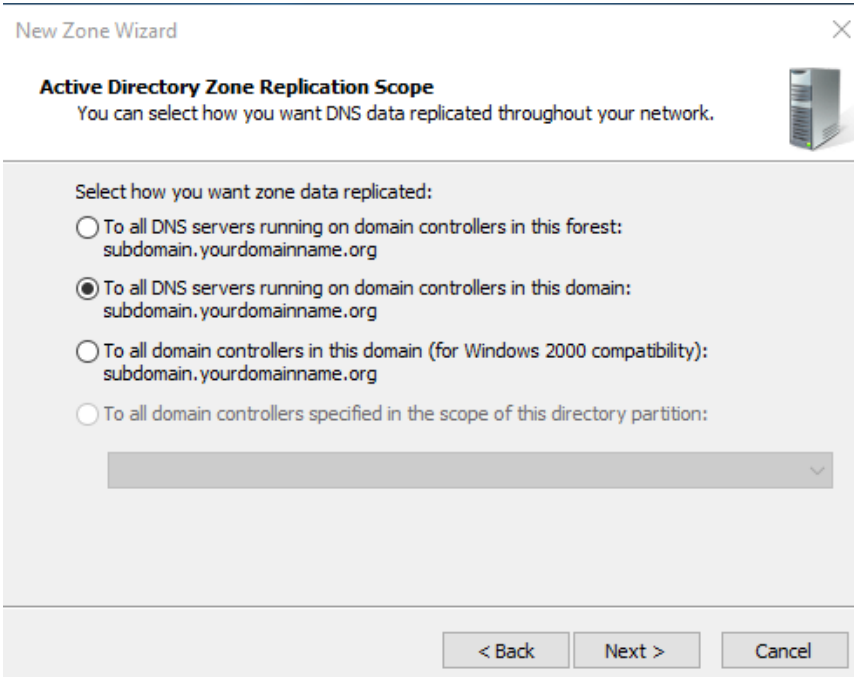
- a. You will use this New Zone Wizard to create a Reverse Lookup Zone for each Forward Lookup Zone in your DNS Manager, and for each ip subnet.
- b. Click Next

New Zone Wizard

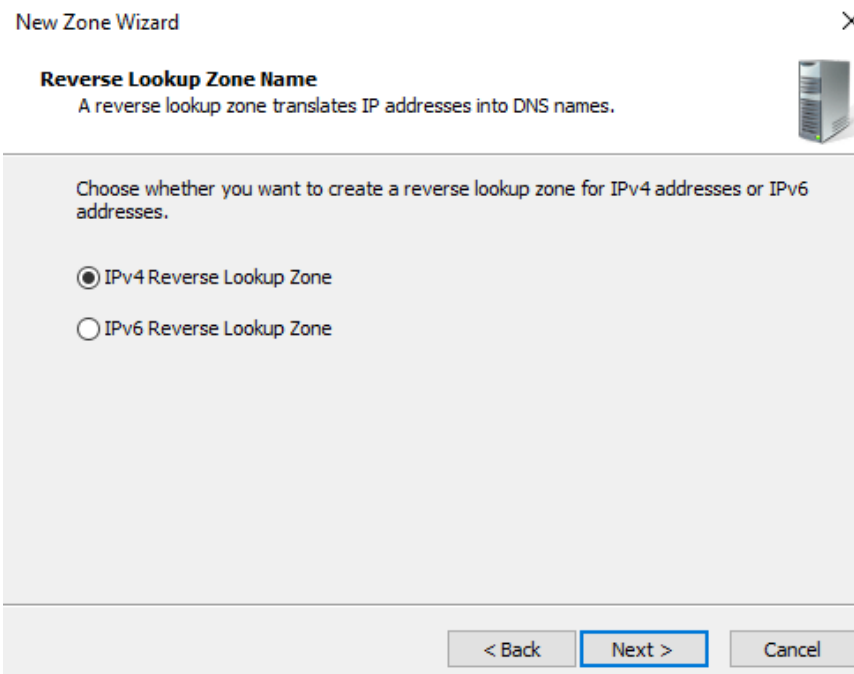


2. Zone Type

- a. Select the type of zone you want to create. In this case, since this is the initial DNS server for our Domain, we will leave Primary zone selected.
- b. Since this server is not Read-Only, we will leave the checkbox to Store the zone in AD.
- c. Click Next.



3. Active Directory Zone Replication Scope to select how this zone data will be replicated
 - a. If this DNS server was within a forest, you may want to have the zone replicated to all DNS servers within the forest for faster DNS resolution.
 - b. This Domain Controller is not currently part of a forest, so you can leave the option selected to replicate, To all DNS servers running on domain controllers in this domain. Considered best practice, this will establish redundancy in the case of failure.
 - c. Only choose, To all domain controllers in domain (for Windows 2000 compatibility) if you have Windows 2000 DNS servers.
 - d. Click Next.



4. Reverse Lookup Zone Name
 - a. Choose whether this will be an IPv4 or IPv6 reverse zone.
 - b. If you are using IPv6 on your network, you must create a separate zone for each type. We will leave the option selected for the IPv4 Reverse Lookup Zone.
 - c. Click Next.

New Zone Wizard

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.



To identify the reverse lookup zone, type the network ID or the name of the zone.

Network ID:

192 .168 .50 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

Reverse lookup zone name:

50.168.192.in-addr.arpa

< Back

Next >

Cancel

5. Reverse Lookup Zone Name, Pt. II
 - a. Enter the first three octets of the Network ID (IP Address) for the network you are setting up in this zone.
 - b. If you are using multiple subnets, you will need to run the New Zone wizard to create a reverse zone for each subnet.
 - c. Click Next.

New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.



Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.


Select the type of dynamic updates you want to allow:

Allow only secure dynamic updates (recommended for Active Directory)

This option is available only for Active Directory-integrated zones.

Allow both nonsecure and secure dynamic updates

Dynamic updates of resource records are accepted from any client.

 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

Do not allow dynamic updates

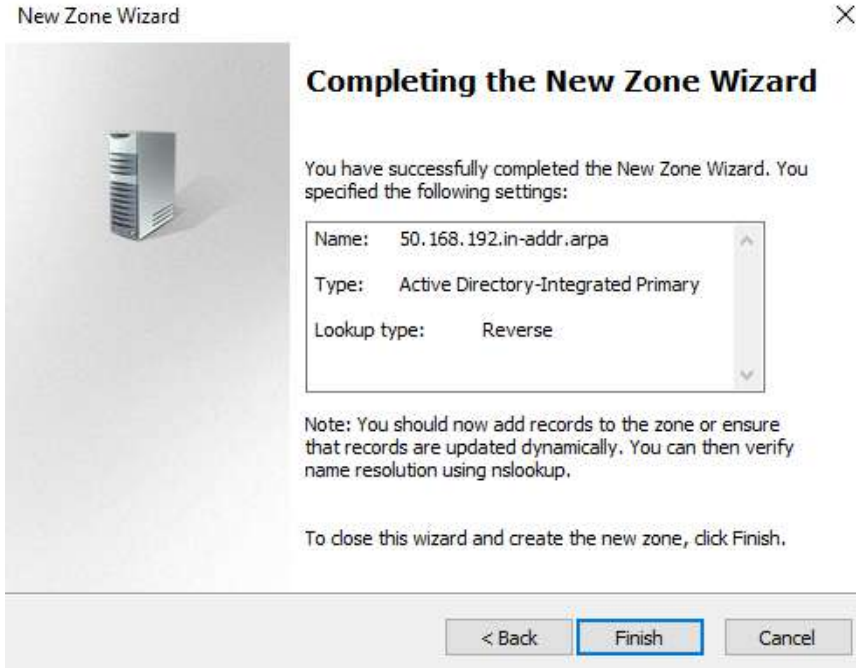
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back

Next >

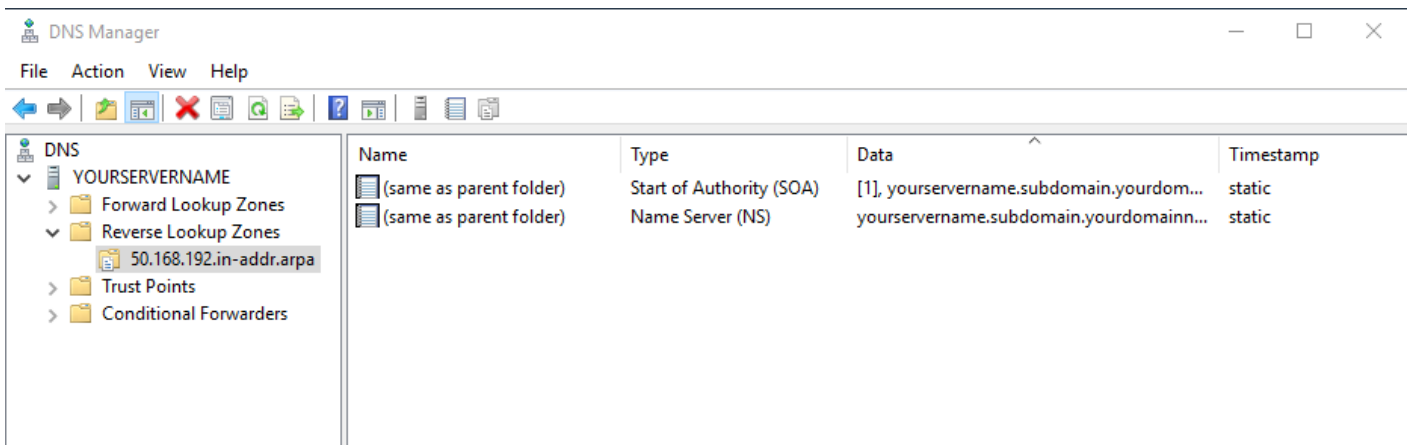
Cancel

6. Dynamic Updates
 - a. Select the type of Dynamic updates to be allowed in this zone.
 - b. The options are Only secure (for AD-integrated), Allow both nonsecure and secure (not advised), and Do not allow.
 - c. If you selected Do not allow, you would have to update any DNS records in your zone manually.
 - d. We will leave the default option to Allow only secure dynamic updates, since this domain utilizes Active Directory. This will enable client computers to register and update their resource records as changes occur.
 - e. Click Next.



7. Completing the New Zone Wizard
 - a. You have successfully completed the New Zone Wizard.
 - b. Review the summary of your selections.
 - c. Name resolution can be verified from Powershell or an Administrative Command Prompt using nslookup, <https://technet.microsoft.com/en-us/library/bb490950.aspx>.
 - d. Click Finish.

Your Reverse DNS Zone is now created and active.



Check the properties for the zone and verify all settings are correct. The properties options for the reverse DNS zone are the same as the forward zone, so we will not go back through the screens, please see the section above: Forward Lookup Zone to verify or review.

Creating Conditional Forwarders

Conditional Forwarders provide the implementation of name-based rules to define specific DNS servers to handle forward queries for specific domain names. This can promote faster query response, given the queries are then sent directly to the server(s) where the zone for those domain names are maintained. You have to ensure sure communications are not blocked to and from those ip addresses, as well as staying on ahead of ip address changes. Typically, Conditional Forwarders are used in multi-domain internal networks so partner organizations can quickly and securely access internal resources without the need to for zone transfers or stub zones.

For example, we could have all DNS queries for the domain more.net sent to the MOREnet core DNS servers, since those are hosts for the more.net Zone.

Understanding Forwarders (as related to Windows Server 2008 R2)

<http://technet.microsoft.com/en-us/library/cc730756.aspx>

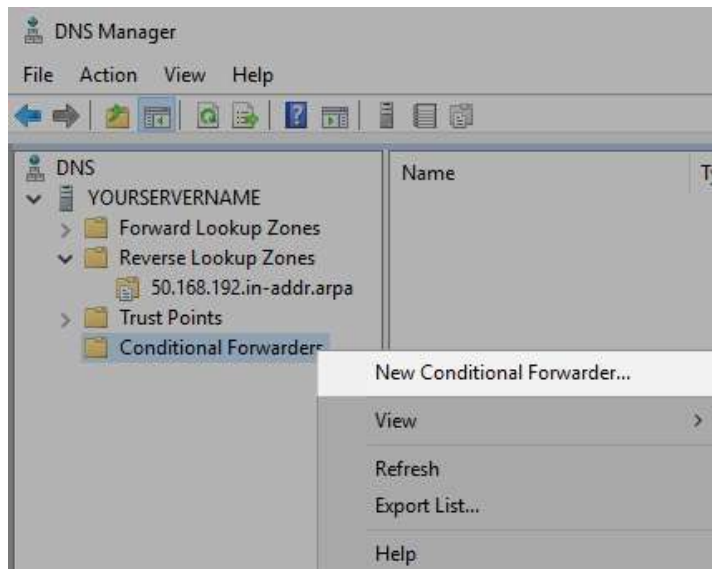
Using Forwarders (as related to Windows Server 2008 R2)

<http://technet.microsoft.com/en-us/library/cc754931.aspx>

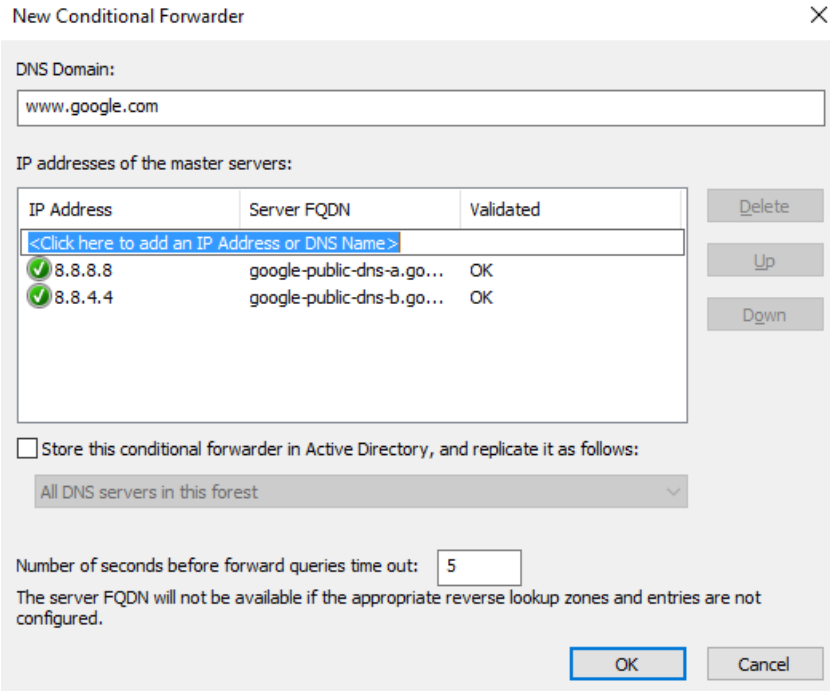
What should I use, a Stub, Conditional Forwarder, Forwarder, or Secondary Zone??

<https://blogs.msmvps.com/acefekay/2012/09/18/what-should-i-use-a-stub-conditional-forwarder-forwarder-or-secondary-zone/>

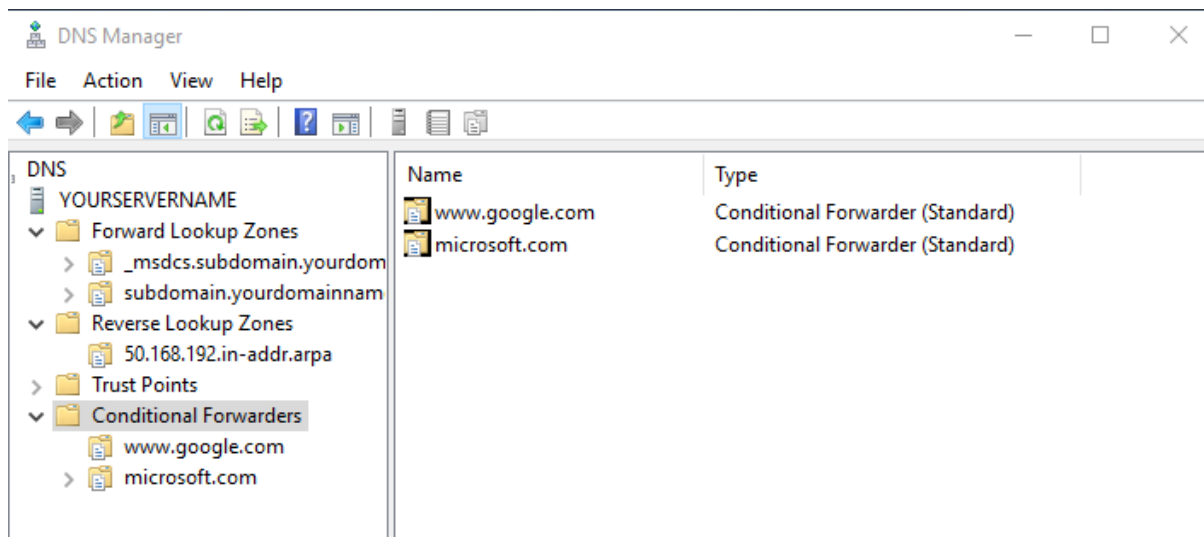
1. Open the DNS (Manager) Console from the Server Manager Tools Menu.
2. Click > next to your server name to expand the console.



3. Right Click Conditional Forwarders and select New Conditional Forwarder...



1. Enter the DNS Domain to be forwarded.
2. Enter the DNS server addresses. Best Practice is to enter at least 2 ip addresses, when possible.
3. Check the box if you want this conditional forwarder to be stored in Active Directory.
4. Select if this data will be replicated. If you do not store it in Active Directory, the replication option is grayed out.
5. Enter the number of seconds before forward queries time out. Of the DNS forwarding options, queries are processed through Conditional Forwarders, then the entries in your Forwarders tab, and lastly using Root Hints if the other methods fail.
6. Click Ok
7. Repeat this procedure for each DNS Domain.



Once you have completed creating your Conditional Forwarders, they are listed individually in the DNS Manager.

[Back to Contents](#)

Section VI: Security Policies for Windows Server 2016

MUST-READ LINKS!

CIS (Center for Internet Security) Microsoft Windows Server 2012R2 Benchmark

https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf

Security Baseline for Windows 10 & Windows Server 2016

<https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/>

Best Practices for Securing Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

Active Directory Security Groups

[https://technet.microsoft.com/en-us/library/dn579255\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx)

LAPS (Local Administrator Password Solution)

<https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Securing Domain Controllers Against Attack

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack>

Securing Domain Controllers to Improve Active Directory Security

<https://adsecurity.org/?p=3377>

Device Health Attestation

<https://docs.microsoft.com/en-us/windows-server/security/device-health-attestation>

Reinspecting Password, Account Lockout and Audit Policies

<https://www.isaca.org/Journal/archives/2014/Volume-2/Pages/JOnline-Reinspecting-Password-Account-Lockout-and-Audit-Policies.aspx>

The 1st step to implementing your Server Security Policies is to research and determine what Technology Security Policies are necessary for your organization. This includes deciding on any distinctive password policies, standards for software installation and desktop settings, acceptable use of personal external storage or network equipment, etc. These are just a few concepts you will want to consider including in your Technology Policies. For additional resources, visit <https://www.sans.org/security-resources/policies>, to review the Information Security Policy templates available from SANS.

The 2nd step is to ensure that your organization develops a corresponding WRITTEN POLICY supporting the settings that you will be applying to the domain. If necessary, enlist a lawyer to help you with the appropriate legal terminology.

The 3rd step is to research and use the Software and Tools you have available to setup and maintain these policies for your domain.

Beginning with Windows Server 2000, it became standard to create a password policy as part of your domain security. It was implemented in the Default Domain Policy, which meant being limited to one password policy that could be applied to the users in a single domain. With Windows Server 2008, Microsoft added Fine-Grained password policies (FGPP) and introduced the Active Directory Password Settings Container where Password Settings Objects could be created via wizard. This enabled administrators to create multiple password policies which could then be applied to various global security groups and user objects with an order of precedence. This was a welcomed feature; however, it was a multi-step process. Fine-grained password policies have been enhanced in Windows Server 2012, integrating the feature into a new GUI, Active Directory Administrative Center, making it significantly easier to create and administer FGPP(s). Despite the developments in FGPP, even with Server 2016, they still are still created in Active Directory utilizing the Password Settings Container, and can only be applied to global security groups or user objects. They are unable to be deployed with Group Policy Objects, and unable to be applied to OUs.

The other security policies we will discuss can be set up in separate/multiple Group Policy Objects (GPOs) to provide specific security settings to particular OUs or groups.

In this documentation, we are using the Default Domain Policy from the Group Policy Management Console. Once we open the Default Domain Policy, we will ONLY be working with the security settings under Computer Configuration.

NOTE: To edit the Default Domain and Default Domain Controllers policies, you must add your user to the Domain Admins Security Group in Active Directory Users and Computers before working with the instructions below. Remove that user account from the Domain Admins Security Group when you are done editing the policies.

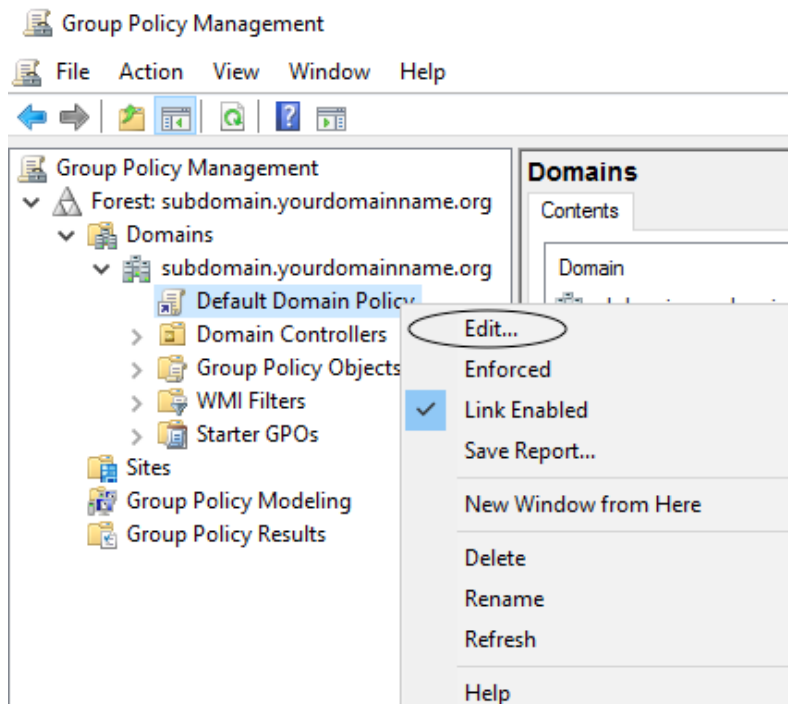
This Document is a guide to explain and provide examples of Active Directory Group Policy Objects, and how to institute them. The scope of the policies you decided to implement should not defined or limited by this guide.

Do not expect your domain or computers in your domain, are protected from hacking, viruses, worms or malware solely because you have setup the policies outlined in this document. It is imperative for you to analyze the baseline security of your environment, and adjust your policies accordingly. You must maintain installation of current service packs, updates, hot-fixes and security patches applied to the systems.

Enjoy the following with the goal to gain a better understand group policy and enable you to secure your domain using the tools that Active Directory provides.

GROUP POLICY MANAGEMENT

1. Open Group Policy Management from the Server Manager Tools Menu.



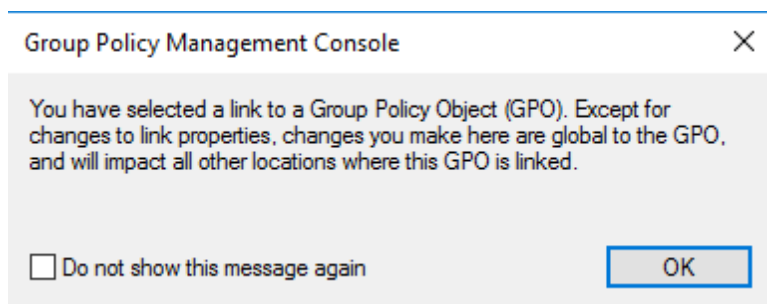
2. Click > next to your Forest: subdomain.yourdomainname.TLD
3. Click > next to Domains
 - a. If your domain does not appear, right-click on Domains.
 - b. Select Show Domains...
 - c. Check the box next to the name of your domain.
 - d. Click OK.

4. Click > next to your Domain Name (ex. Subdomain.yourdomainname.org)

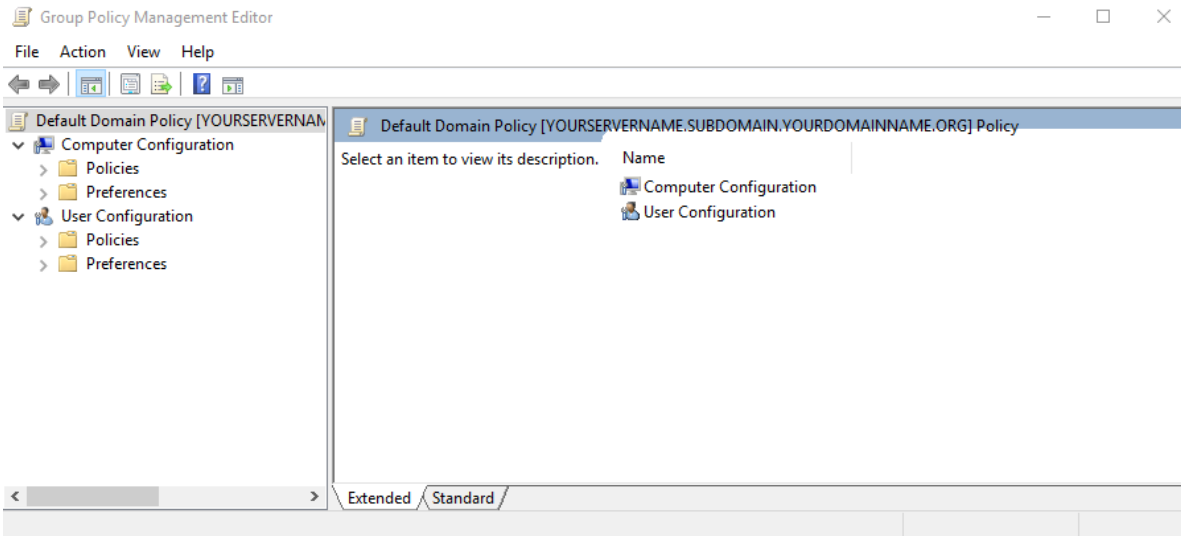
5. Right-click on the Default Domain Policy.

[NOTE: To edit the Default Domain and Default Domain Controllers policies, you must add the account you are using to the Domain Admins Security Group. Go back to Active Directory Users and Computers to do so before working with these instructions. Remove that user account from the Domain Admins Security Group when you are done editing the policies.]

6. Select Edit...



7. Read the warning message, then click OK.



8. This will launch the Group Policy Management Editor.

PASSWORD POLICIES

Review the following information to customize your Password Policies:

Microsoft Password Guidance, downloadable .pdf

<https://www.microsoft.com/en-us/research/publication/password-guidance/>

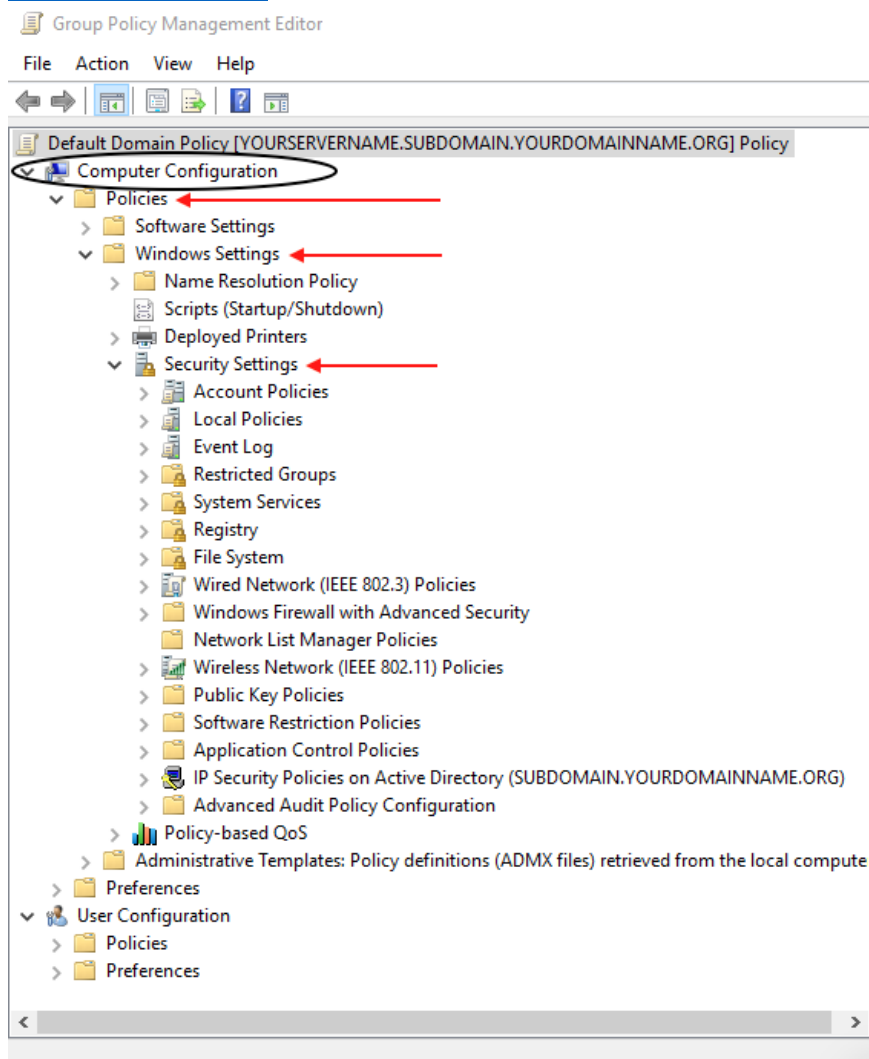
Step-by-Step: Enabling and Using Fine-Grained Password Policies in AD

<https://blogs.technet.microsoft.com/canitpro/2013/05/29/step-by-step-enabling-and-using-fine-grained-password-policies-in-ad/>

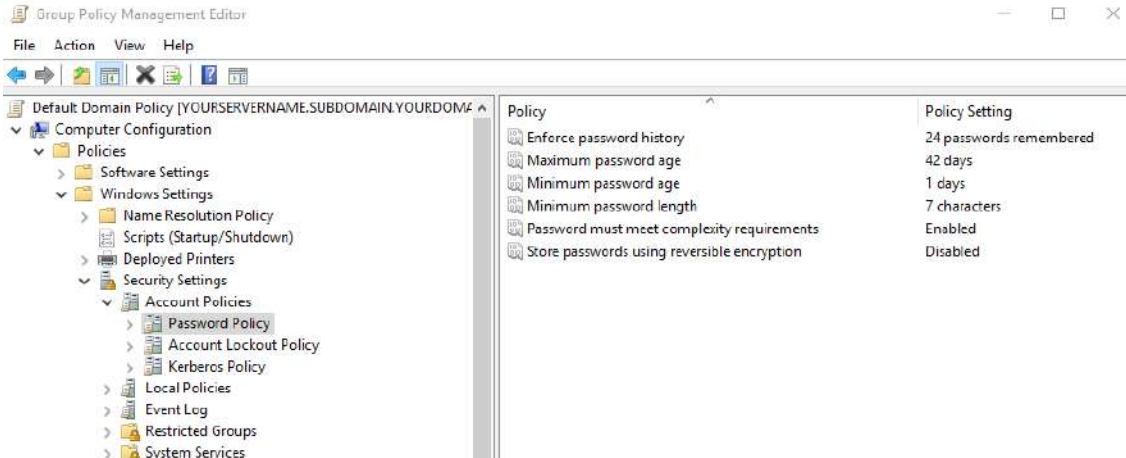
Fine-Grained Password Policies User Interface in Windows 2012 R2 and Newer

<https://blogs.msmvps.com/acefekay/2016/10/16/fine-grained-password-policies-user-interface-in-windows-2012-r2-and-newer/>

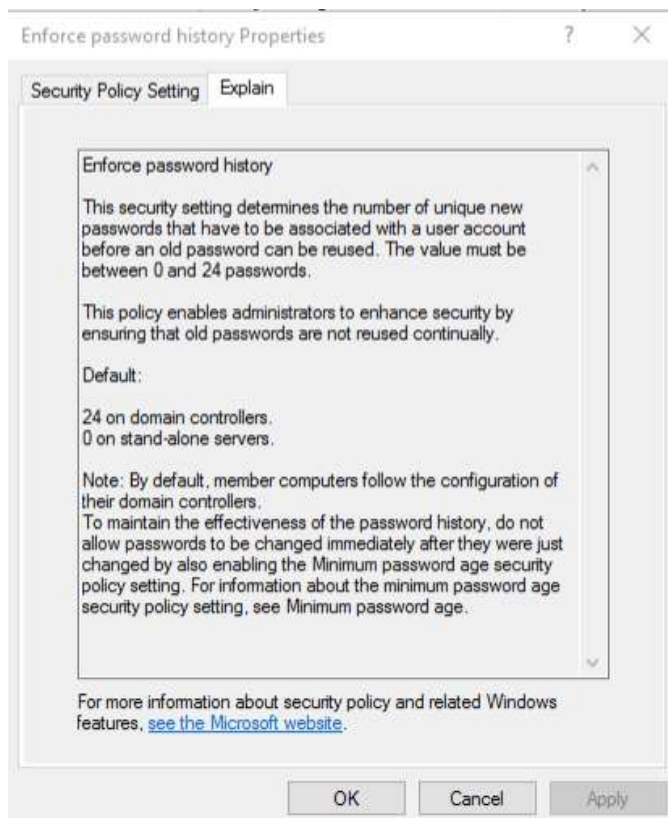
1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management](#) above.



2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.



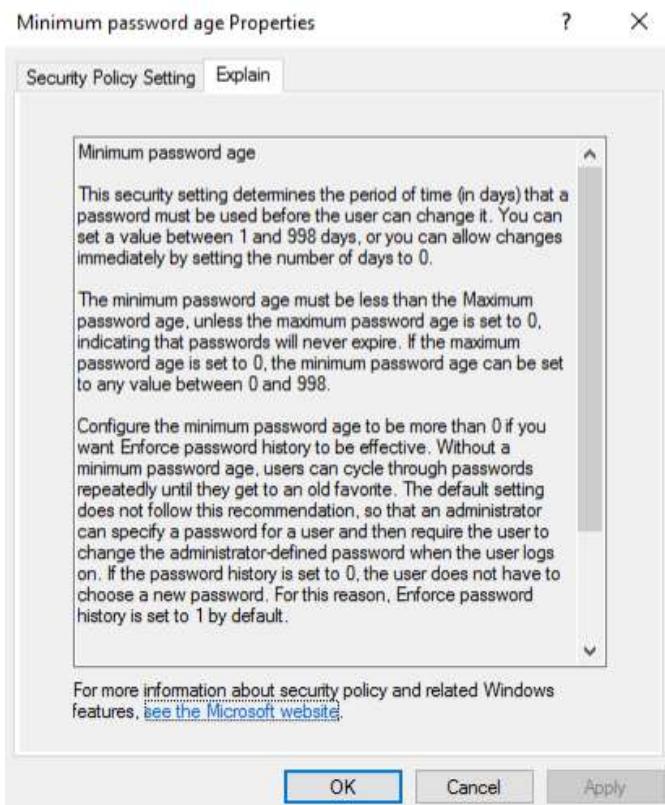
3. Click > next to Account Policies.
4. Click on Password Policy to view the policy options in the frame on the right.
 - a. All of the Password Policy options have the Define this policy setting, checked, by default. So, you will always have a base password policy enabled when you install Active Directory, unless you uncheck each one, setting them to Not Defined.
 - b. We are editing the Default Domain Policy, so these settings will be applied to everyone in the domain. Fine-Grained Password Policies should be used to apply different standards for specific users or groups of users.
 - c. The images below display the Explain tab. Changes to the policies are from the Security Policy Setting tab. The description refers to the Security Policy Settings tab.
 - d. Define and Edit these policies based on your organization's Technology Policies.



5. Double-click Enforce password history.
 - a. The options are 0-24 passwords. 0 = No unique passwords are enforced.
 - b. You can either keep the default of 24, arrow up/down or manually enter a new number.
 - c. If you want to utilize this setting, you must also set the Minimum password age to a value higher than 0.
 - d. Click OK to commit any changes.



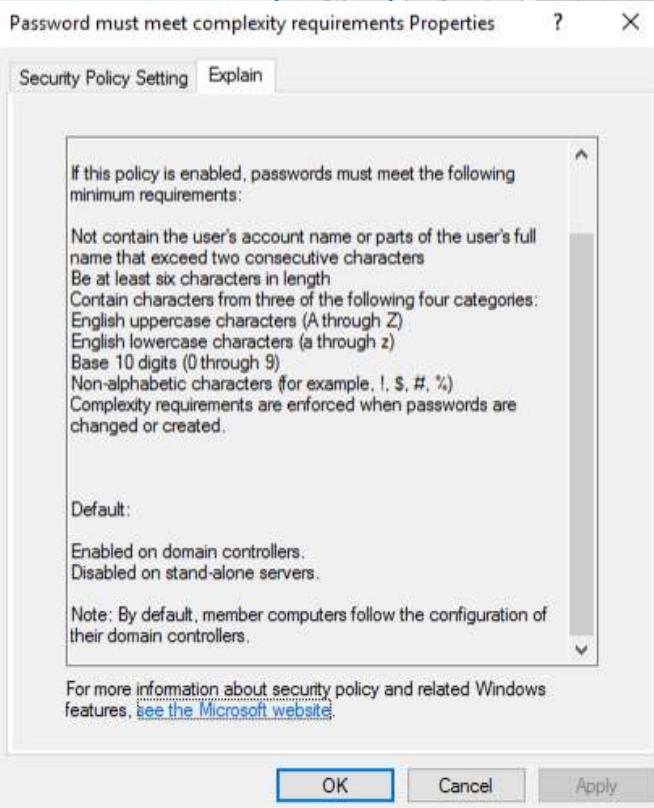
6. Double-click Maximum password age.
 - a. The options are between 0-999 days. 0 = passwords never expire.
 - b. You can either keep the default of 42 days, arrow up/down or manually enter a new number.
 - c. The Minimum password age must be less than the Maximum, unless this value is set to 0.
 - d. Click OK to commit any changes.



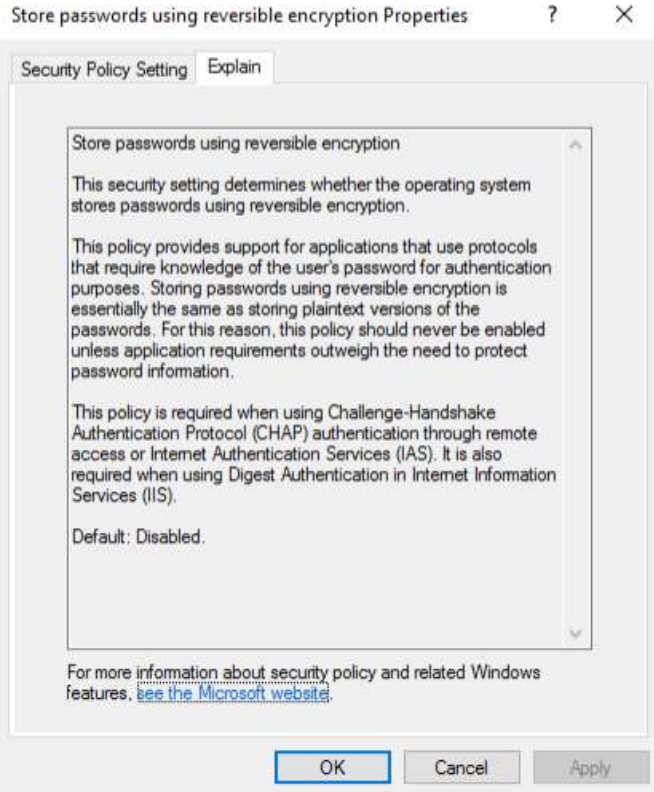
7. Double-click Minimum password age.
 - a. The options are between 0-998 days. 0 = passwords can be changed immediately.
 - b. The default is Password can be changed after 1 day(s). You can either keep the default value, arrow up/down or manually enter a new number.
 - c. This setting must be more than 0 to utilize the Enforce password history setting.
 - d. With this setting defined with values greater than 0, for a user to change their password after they first login, as an admin, you will need to check the user Properties option User must change password at next logon checkbox.
 - e. Click OK to commit any changes.



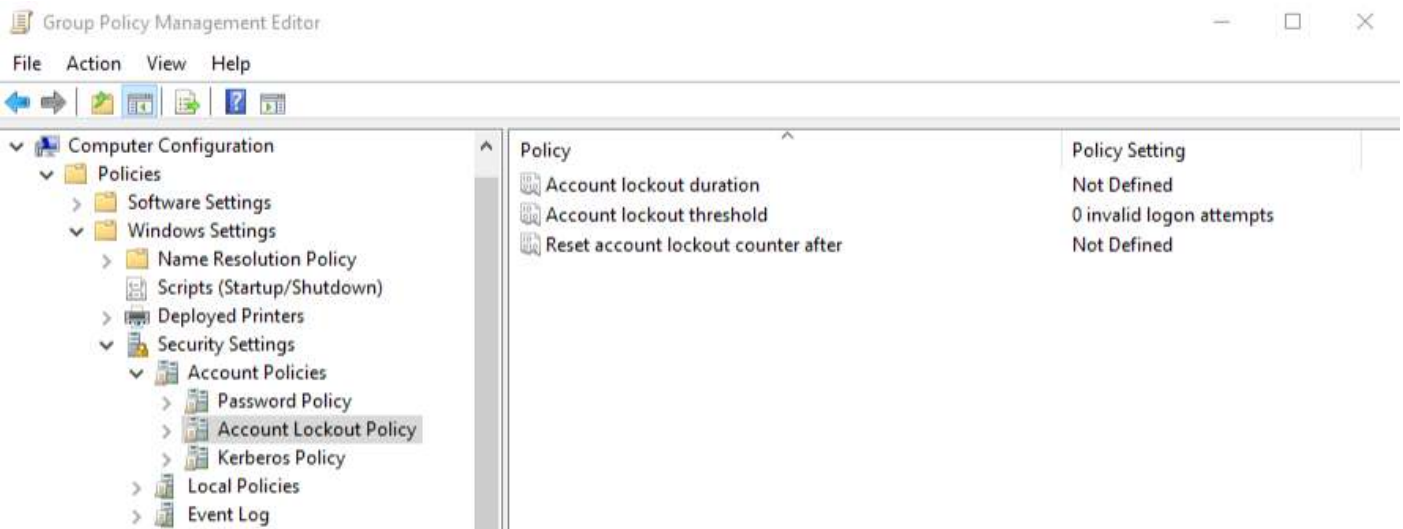
8. Double-click Minimum password length.
 - a. The options are between 0-14 characters. 0 = No password is required.
 - b. The default is 7 characters. You can either keep the default value, arrow up/down or manually enter a new number.
 - c. The longer a password is the more secure, It is difficult to require users to keep long passwords but you should encourage it
 - d. Click OK to commit any changes.



9. Double-click Password must meet complexity requirements.
 - a. The options are Enabled or Disabled.
 - b. The default is Enabled. You can either keep the default value, or change the radio button to Disabled.
 - c. Click OK to commit any changes.

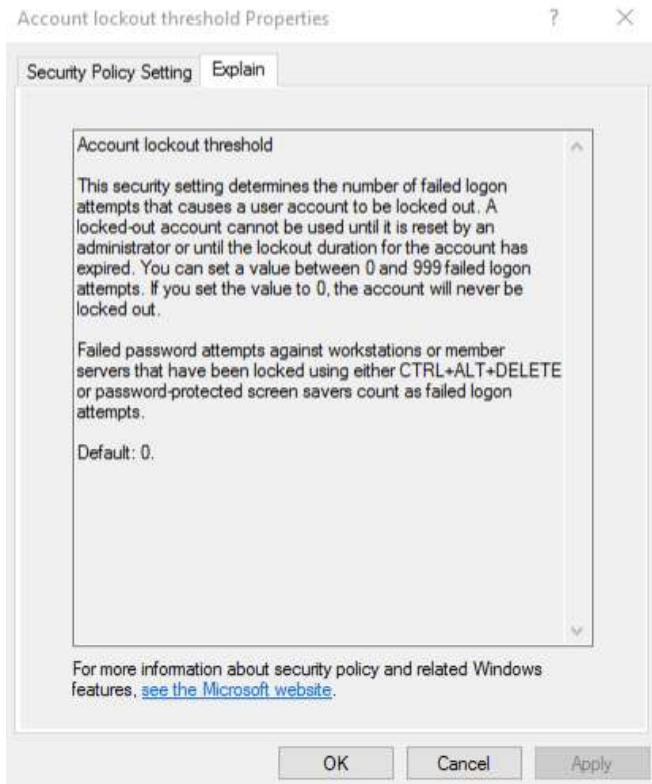


10. Double-click Store passwords using reversible encryption.
 - a. The options are Enabled or Disabled.
 - b. The default is Disabled. You can either keep the default value, or change the radio button to Enabled.
 - c. Only use this feature for specific systems that require this to connect to the domain.
 - d. Click OK to commit any changes.

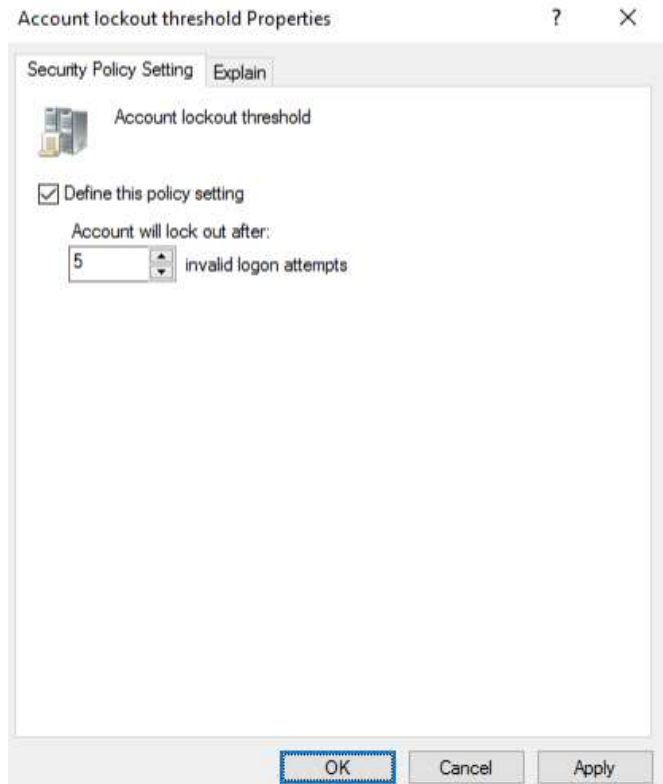


1. Now click on Account Lockout Policy to view the policy options in the frame on the right.

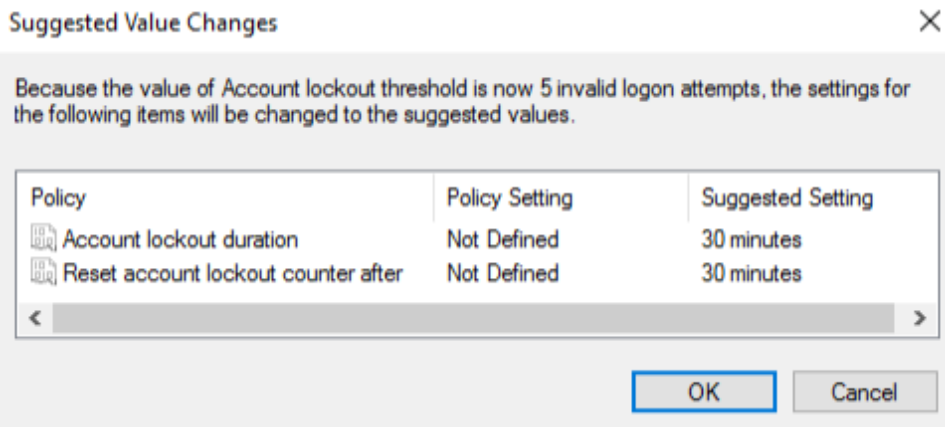
2. Double-click Account lockout threshold.



- a. Values range between 0-999. 0 = the account will never be locked out.
- b. The default is 0.



- c. From the Security Policy Setting tab, arrow up/down or manually enter a new number.
- d. We have entered 5.
- e. Click OK.



- f. Setting the lockout threshold greater than 0 prompts Suggested Value Changes.
- g. Click OK.

Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

h. The Account lockout duration and Reset account lockout counter after options, are now automatically updated and defined for the Account Lockout Policy.

- i. The amount of time can be edited by double-clicking on the option.
- ii. The suggested time is 30 minutes. You can either keep the default value, arrow up/down or manually enter a new number.
- iii. Values range between 0-99.99 minutes. 0 = the account will be locked until an administrator explicitly unlocks it.
- iv. Click OK to commit any changes.

When finished working with the Default Domain policy, [remove the user account you added when you began this section from the Domain Admins Security Group.](#)

AUDIT POLICY CONFIGURATION

Review the following information to customize your Audit Policies:

Advanced Security Auditing FAQ

[https://technet.microsoft.com/en-us/library/dn319046\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn319046(v=ws.11).aspx)

Audit Policy Recommendations, Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

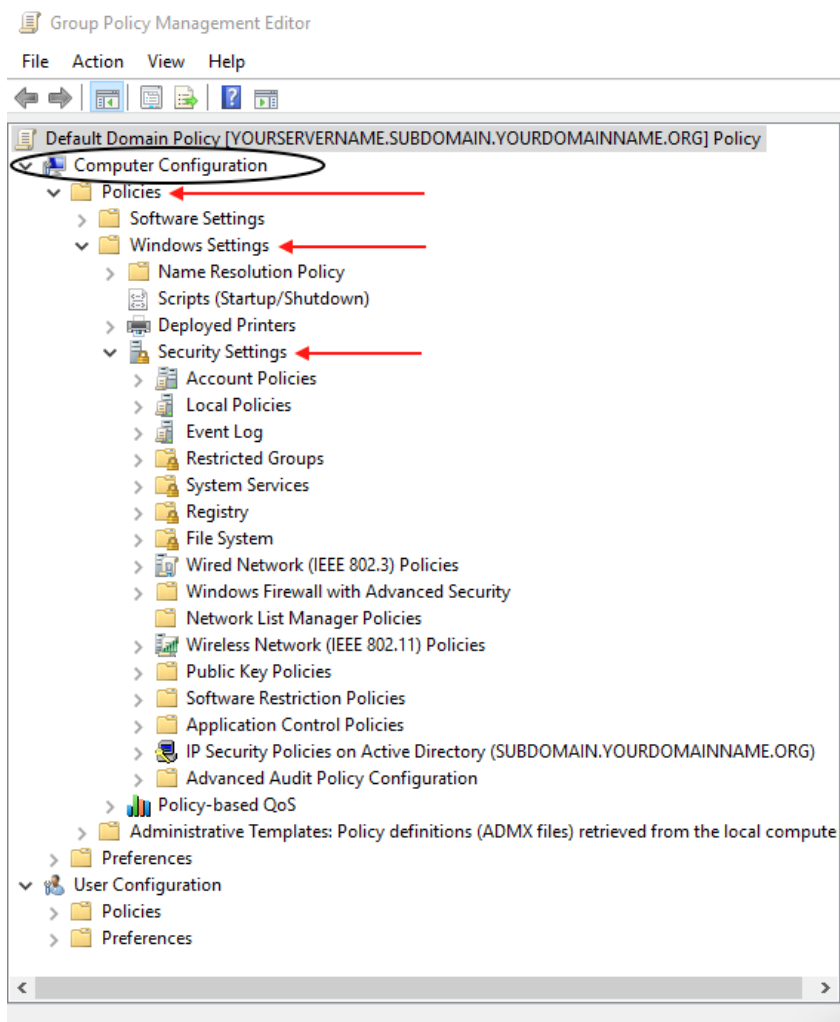
Monitoring Active Directory for Signs of Compromise

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise>

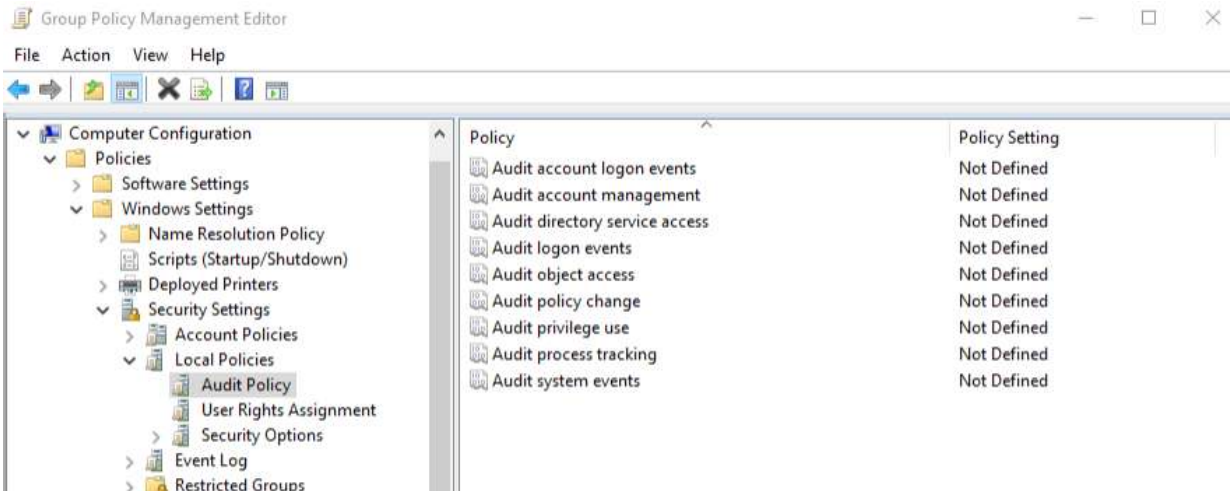
Windows 10 and Windows Server 2016 security auditing and monitoring reference

<https://www.microsoft.com/en-us/download/details.aspx?id=52630>

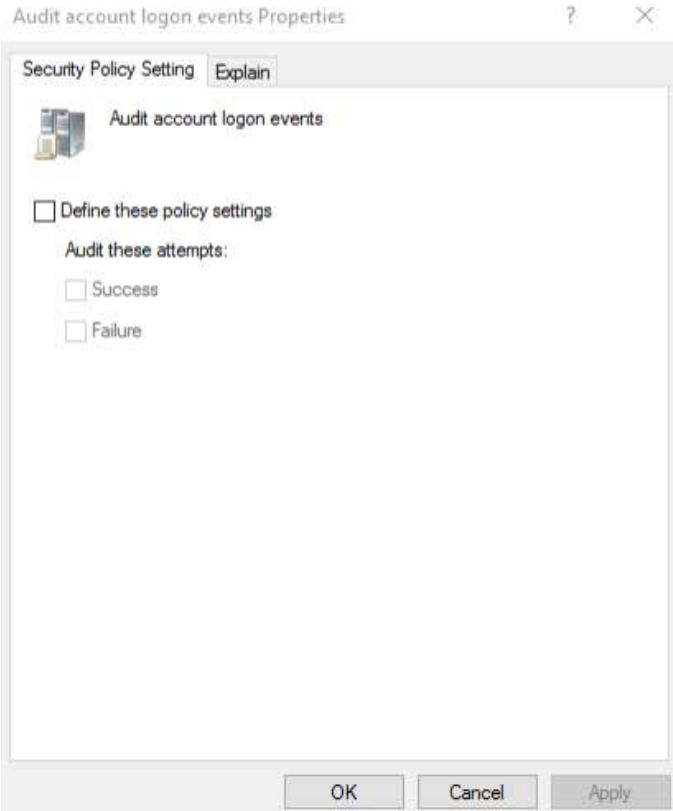
1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management above](#).



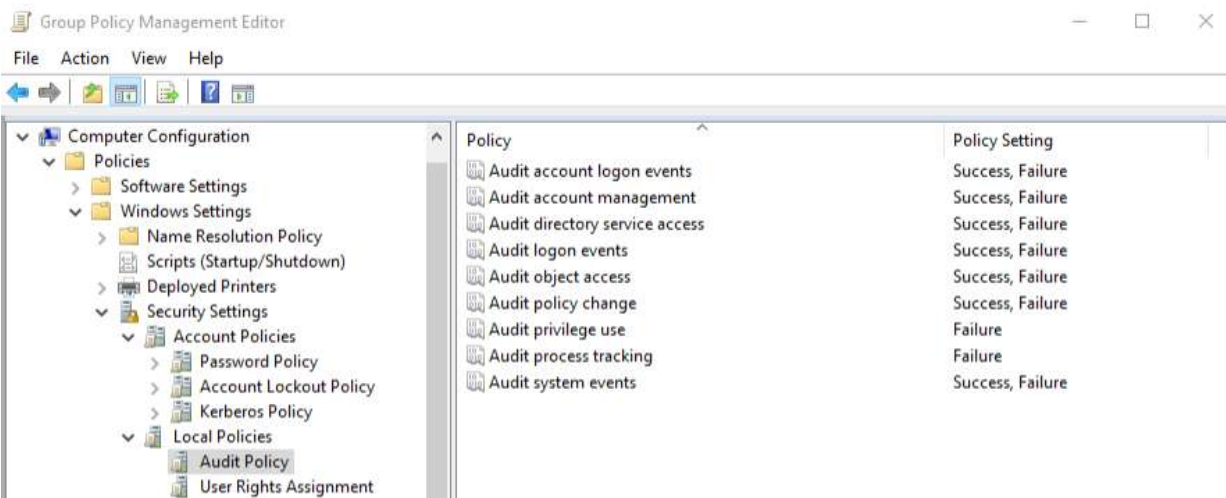
2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.



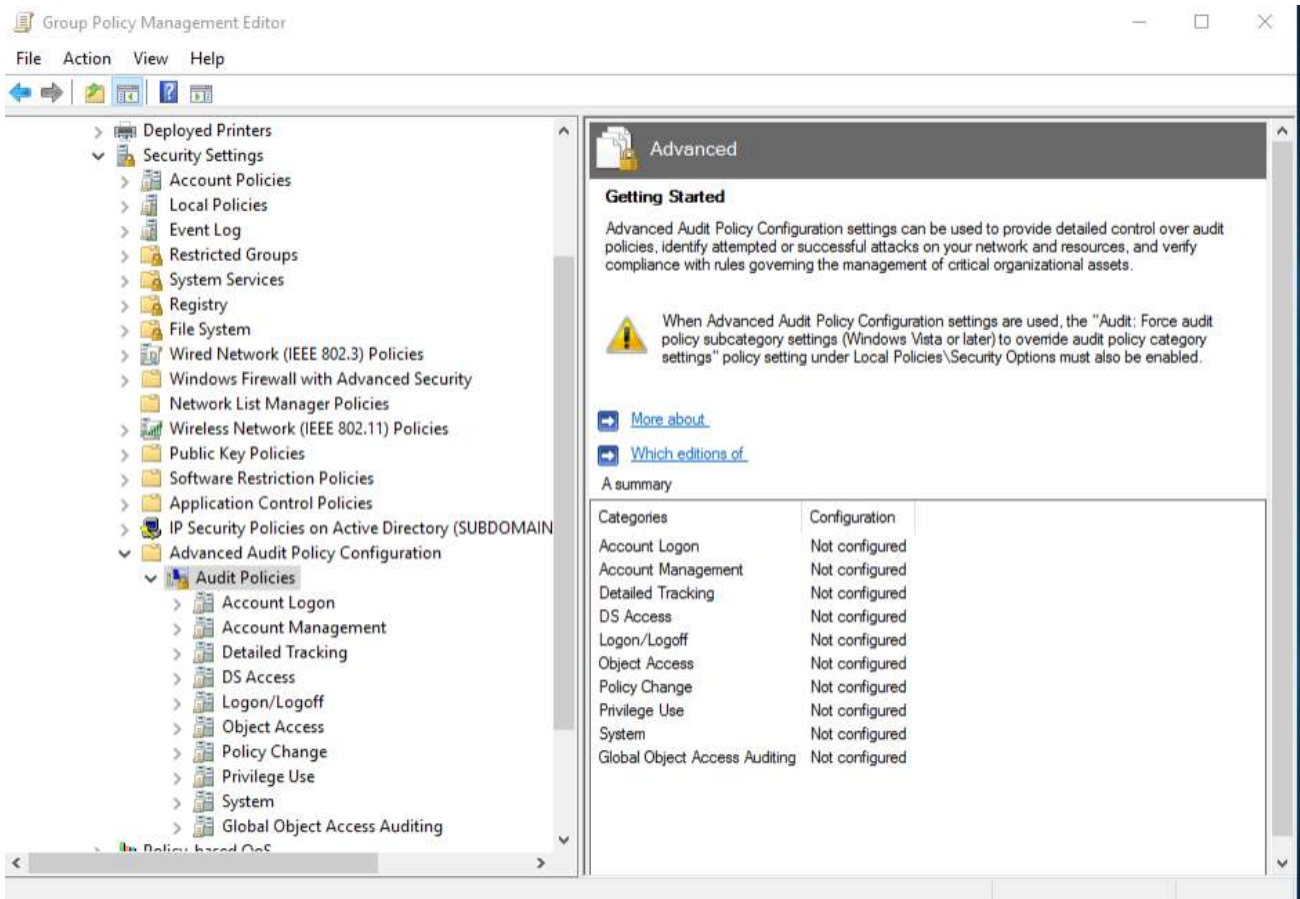
4. Click on Audit Policy to view the policy options in the frame on the right.
 - a. This policy defines the types of events that are written to the Security Log, accessible from the Event Viewer.
 - b. By default, these options are Not Defined in Group Policy.
 - c. These settings will enable logging on ALL machines in the domain.
 - d. Experiment with these options, then analyze the Security Logs to determine what information is best to monitor for your organization.



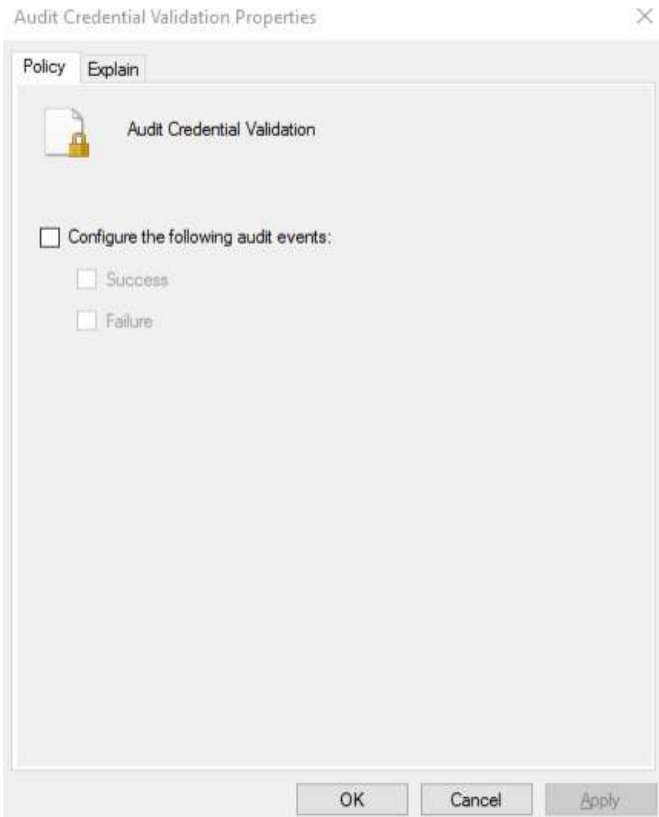
5. To edit, double-click on the option to open the Properties. The above example is for Audit account logon events.
 - a. From the Security Policy Setting tab, check the box to Define these policy settings.
 - b. Under Audit these attempts: Check the box(es) for Success, or Failure, or both Success and Failure.
 - c. Click OK to commit any changes.



- d. The above is a sample recommendation for these options.
- e. Continue editing each option until all settings are defined according to your Security Policy.



6. To configure the Audit Policies further, experiment with the Advanced Audit Policy Configuration options.
7. Under Security Settings, Click > next to Advanced Audit Policy Configuration.
8. Click > next to Audit Policies.
9. Here there are additional Audit Policies for the following:
 - a. Account Logon
 - b. Account Management
 - c. Detailed Tracking
 - d. DS Access
 - e. Logon/Logoff
 - f. Object Access
 - g. Policy Change
 - h. Privilege Use
 - i. System
 - j. Global Object Access Auditing
10. Click on each Policy to view the additional options available to configure in the frame on the right.



11. Double-click each option to open the Properties to edit.
 - a. These options are Not configured by default.
 - b. The example above is for Audit Credential Validation. For additional explanation of an option, click the Explain tab.
 - c. If you want to enable an option, from the Policy tab, check the box to Configure the following audit events:
 - d. Check the box(es) for Success, or Failure, or both Success and Failure.
 - e. Click OK to commit your settings.
 - f. Continue editing each option until all settings are defined according to your Security Policy.

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

USER RIGHTS ASSIGNMENT

Review the following information to customize your User Rights Assignment options:

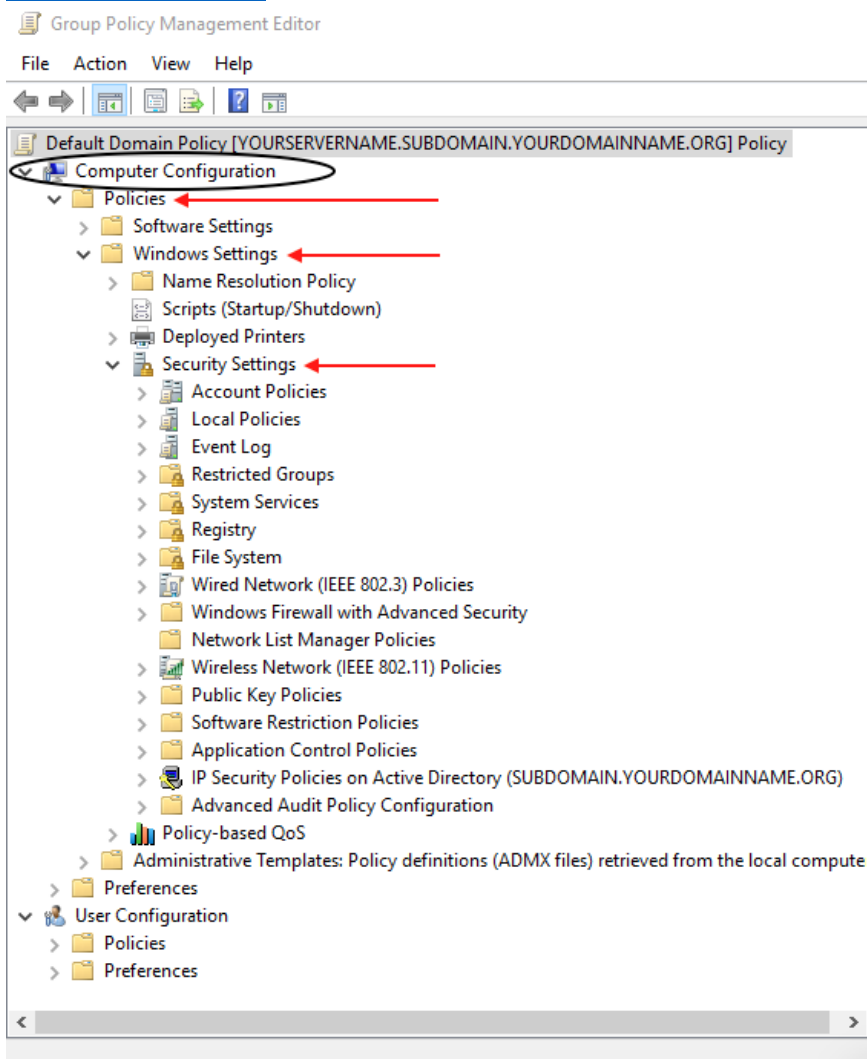
User Rights Assignment

[https://technet.microsoft.com/en-us/library/dn221963\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn221963(v=ws.11).aspx)

Securing Administrator Groups in Active Directory

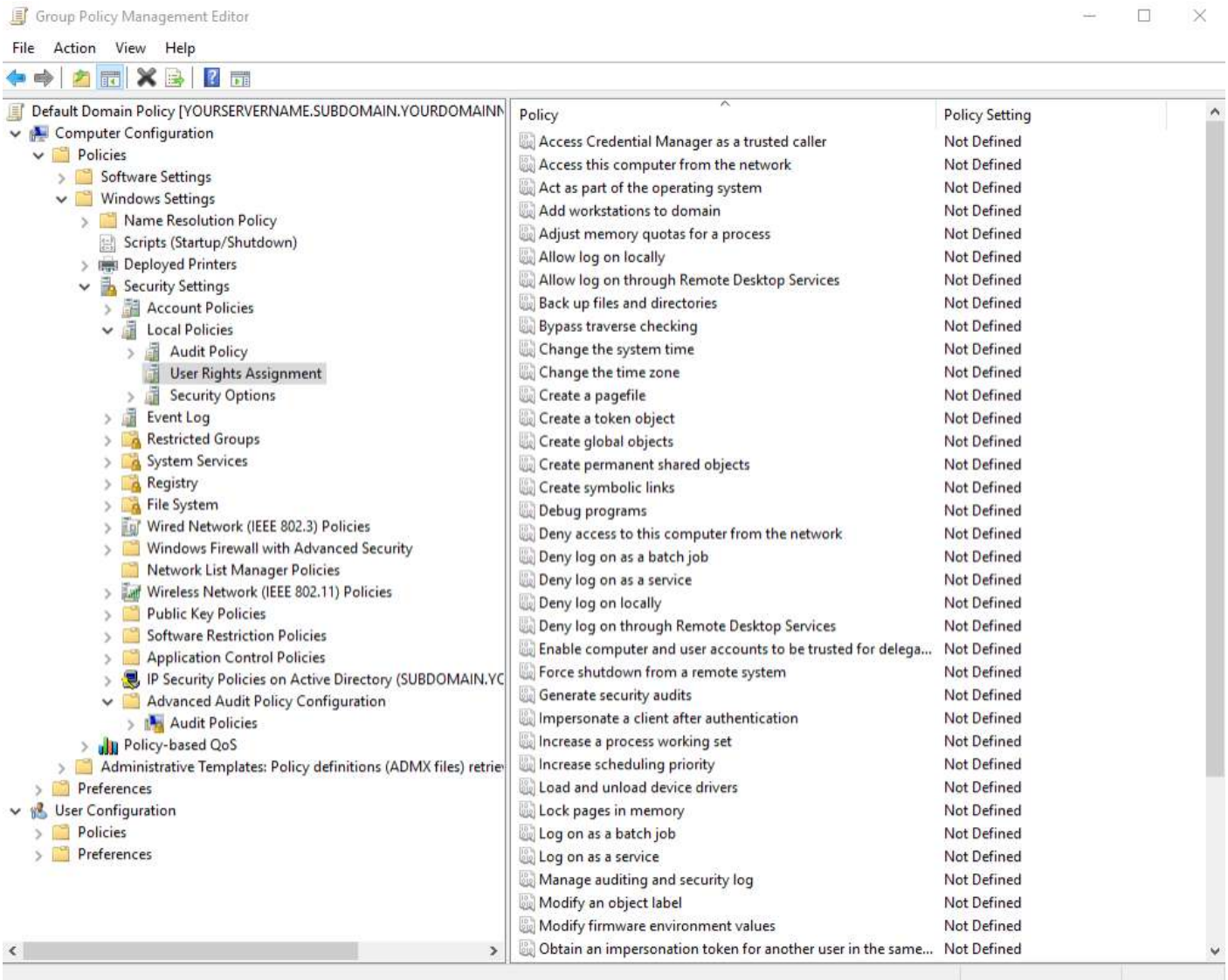
<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-g--securing-administrators-groups-in-active-directory>

1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management above](#).

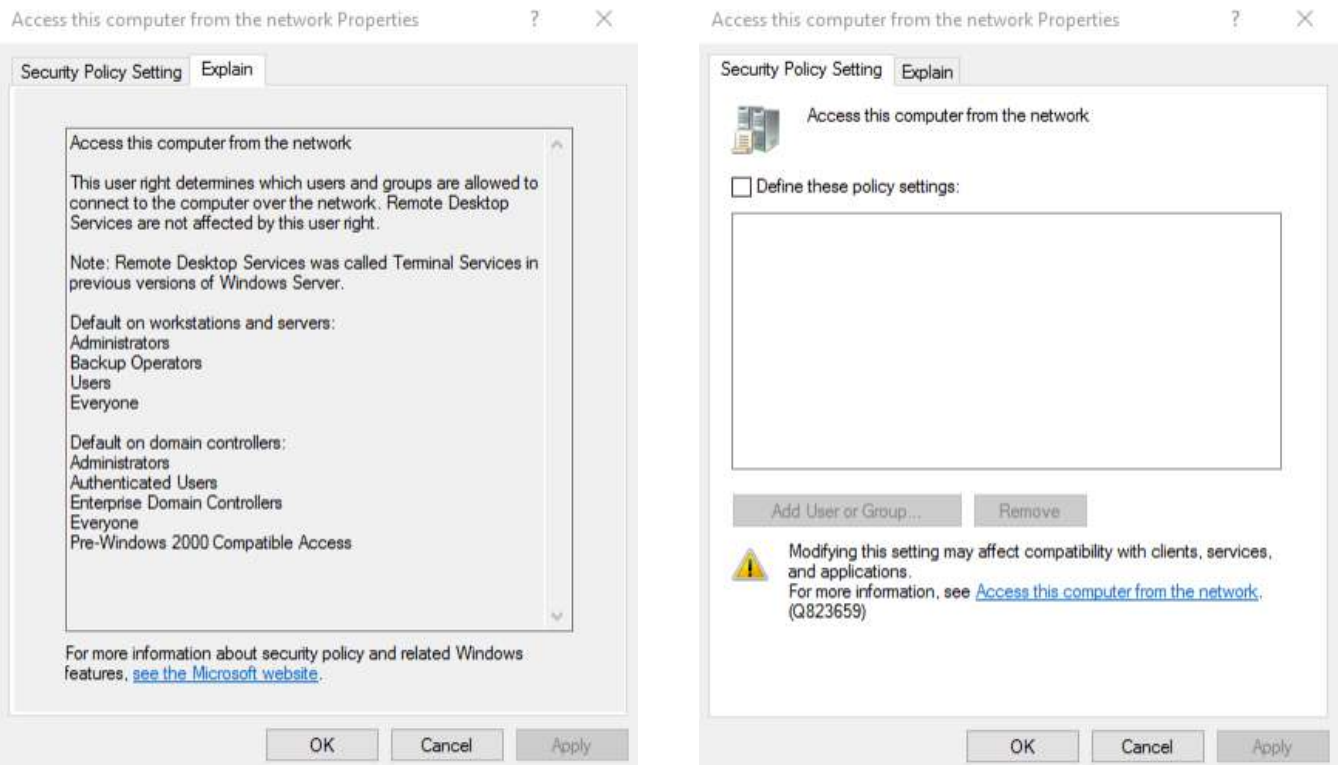


2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.

3. Click > next to Local Policies.



4. Click on User Rights Assignment to view the policy options in the frame on the right.
 - a. These are primarily domain specific policies that are used to enhance local security.
 - b. They can override permissions that have been set on specific objects.



5. Double-click each option you want to edit, to open the Properties.
 - a. These options are Not configured by default.
 - b. The example above is for Access this computer from the network. For additional explanation of an option, click the Explain tab.
 - c. If you want to enable an option, from the Security Policy Setting tab, check the box to Define these policy settings:
 - d. Click Add User or Group to define the accounts you want to apply this option.
 - e. If you have made an error adding the user or group, you can highlight the entry and click Remove.
 - e. Click OK to commit your settings.
 - f. Continue editing the options you need until all settings are defined according to your Security Policy.

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

SECURITY OPTIONS

Review the following information to customize your Security Options:

Security Options

[https://technet.microsoft.com/en-us/library/jj852268\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj852268(v=ws.11).aspx)

Network access: Allow anonymous DIS/name translation

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-access-allow-anonymous-sidname-translation>

Network security: Do not store LAN Manager hash value on next password change

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-do-not-store-lan-manager-hash-value-on-next-password-change>

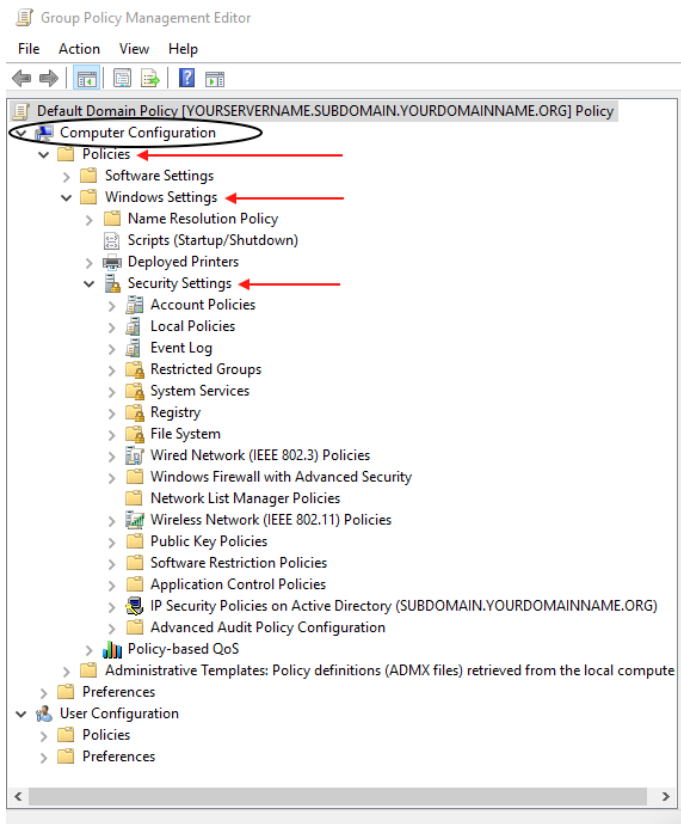
Network security: Force logoff when logon hours expire.

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-force-logoff-when-logon-hours-expire>

Network security:LAN Manager authentication level

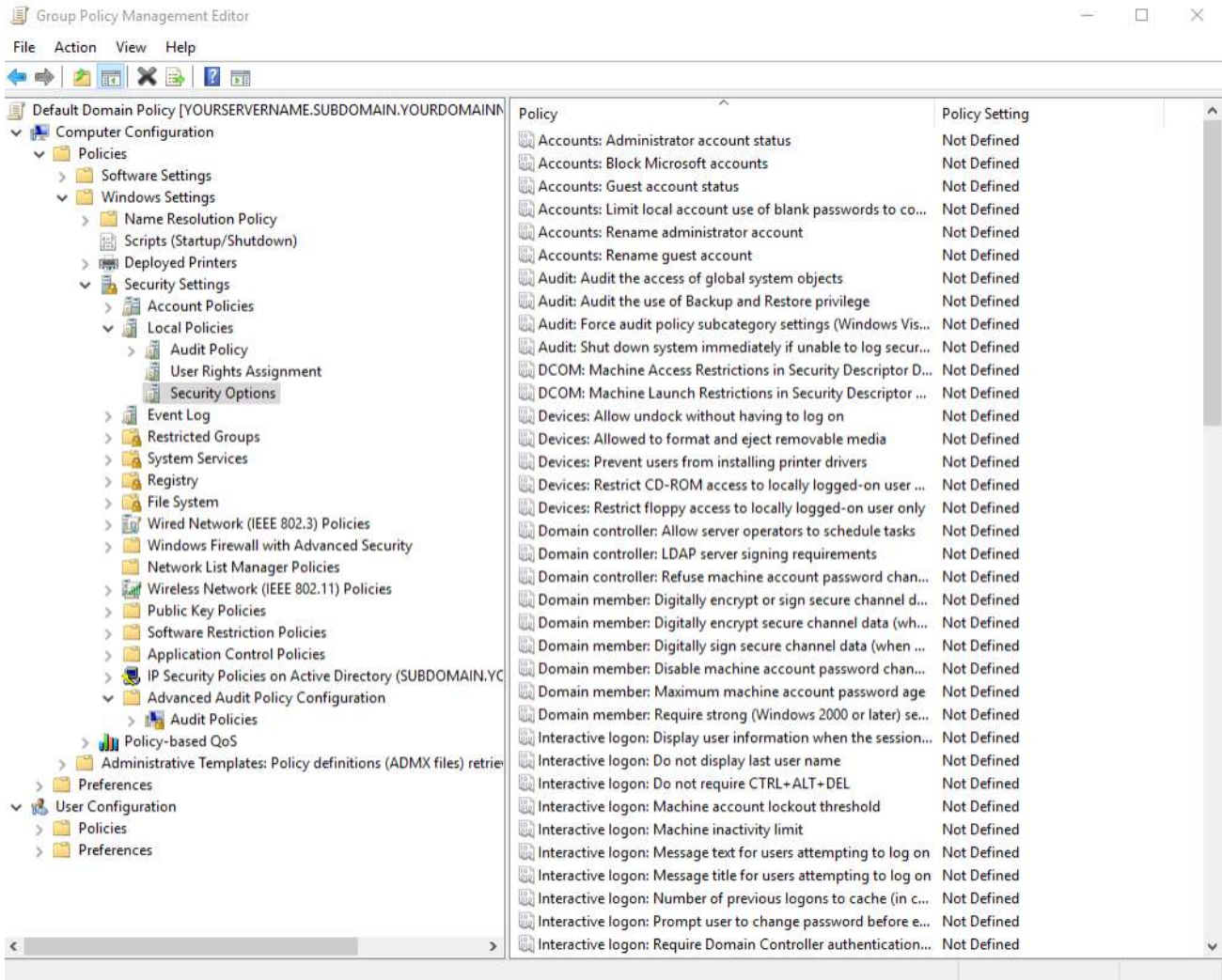
<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-lan-manager-authentication-level>

1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management above](#).



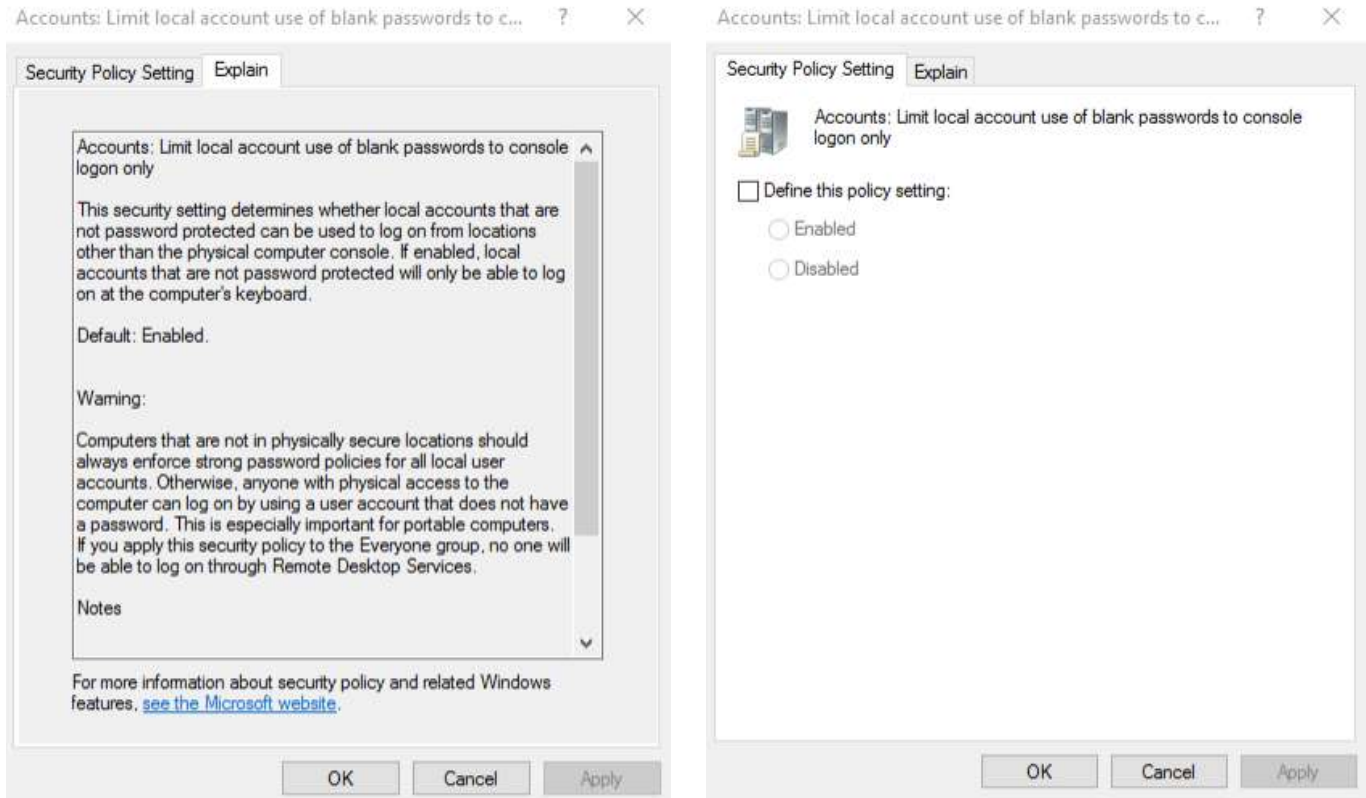
2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.

3. Click > next to Local Policies.



4. Click Security Options to view the options for this policy in the frame on the right.
 - a. There are 96 options available in the Security Options policy.
 - b. Most of these options are Not Defined; however, Not Defined options will automatically assume the default setting designated in the Explain tab of the Properties.
 - c. The following are Defined by default:
 - i. Network access: Allow anonymous DIS/name translation – Disabled
 - ii. Network security: Do not store LAN Manager hash value on next password change – Enabled
 - iii. Network security: Force logoff when logon hours expire – Disabled
 - d. Any options Defined in this policy will be applied to any computer in this domain that is linked to this Group Policy Object. The settings configured here via Active Directory Group Policy will overwrite any matching local security policy settings. When a local setting is inaccessible, that means a GPO is controlling that setting.
 - e. **Research each option and Define only the options that are acceptable and useful to your organization. TEST ALL CHANGES THOROUGHLY PRIOR TO IMPLEMENTATION!**
 - f. It is imperative to balance security settings and functionality.
5. Use the following settings as the minimum security for a domain controller. Although some of these options may technically be set as desired by their default status, explicitly defining them allows you to see their configuration at a glance.
 - a. *Accounts: Limit local account use of blank passwords to console logon only* – **Enabled**

- b. *Devices: Restrict CD-ROM access to locally logged-on user only* – **Enabled**
- c. *Devices: Restrict floppy access to locally logged-on user only* – **Enabled**
- d. *Interactive logon: Do not display last user name* – **Enabled**
- e. *Interactive logon: Message text for users attempting to log on* – **Unauthorized Access is Prohibited!** [Include AUP]
- f. *Interactive logon: Message title for users attempting to log on* – **Warning!**
- g. *Network access: Do not allow anonymous enumeration of SAM accounts* – **Enabled**
- h. *Network access: Do not allow anonymous enumeration of SAM accounts and shares* – **Enabled**
- i. *Network access: Do not allow storage of credentials or .NET Passports for network authentication* – **Enabled**
- j. *Network access: Let Everyone permissions apply to anonymous users* – **Disabled**
- k. *Network security: LAN Manager authentication level* – **Send NTLMv2 response only**
- l. *Shutdown: Allow system to be shut down without having to log on* – **Disabled**
- m. *System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)* – **Enabled**



6. Double-click each option you want to edit, to open the Properties.
 - a. For additional explanation of an option, click the Explain tab.
 - b. If you want to enable an option, from the Security Policy Setting tab, check the box to Define these policy settings:
 - c. Click OK to commit your settings.
 - d. Continue editing the options you need until all settings are defined according to your Security Policy.

NOTES:

- Denying access to anonymous information could cause problems with legacy systems or applications, test prior to implementing these changes.
- Minimal settings should be used only if necessary.
- Always restrict blank passwords.
- Always require a person to login prior to shutting the machine down for accountability.
- Not displaying the last user name makes it more difficult for local users to attempt to guess other user account information.

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

EVENT LOG POLICIES

Review the following information to customize your Event Log Policies:

Recommended Settings for Event Log Sizes in Windows

<https://support.microsoft.com/en-us/help/957662/recommended-settings-for-event-log-sizes-in-windows>

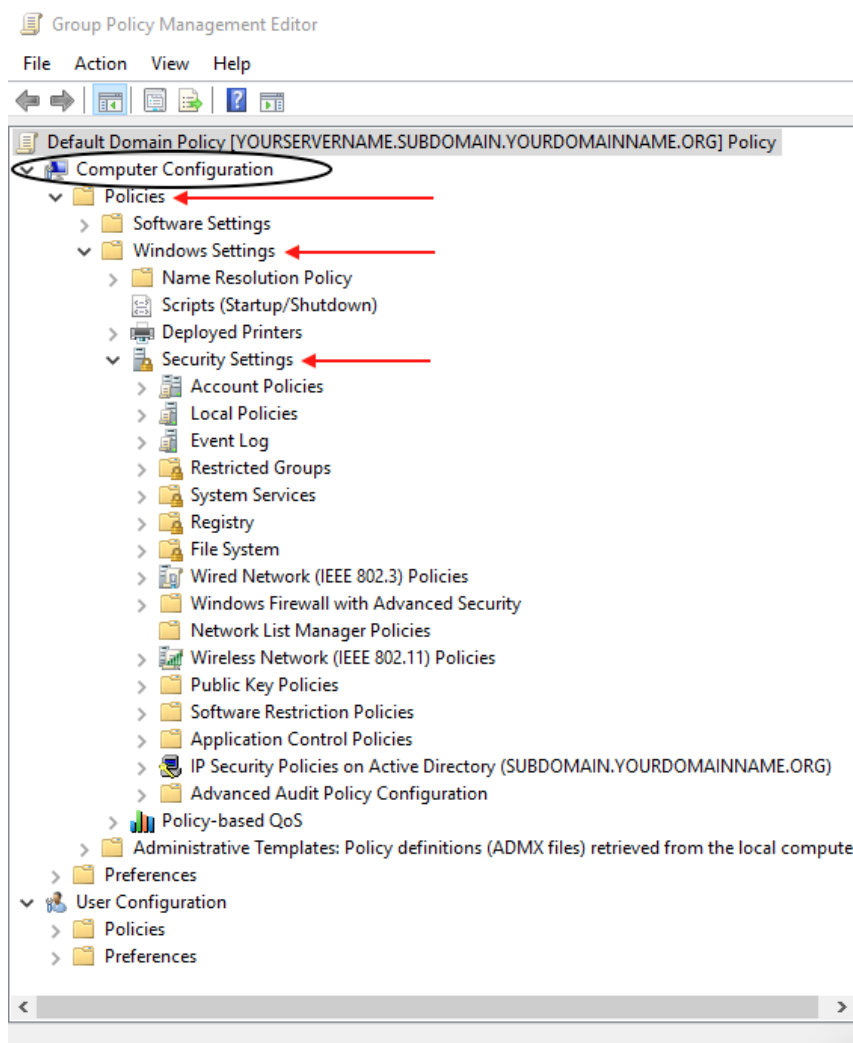
Back Up & Clear Your Event Logs with Windows Powershell

<https://technet.microsoft.com/en-us/library/2009.07.heyscriptingguy.aspx>

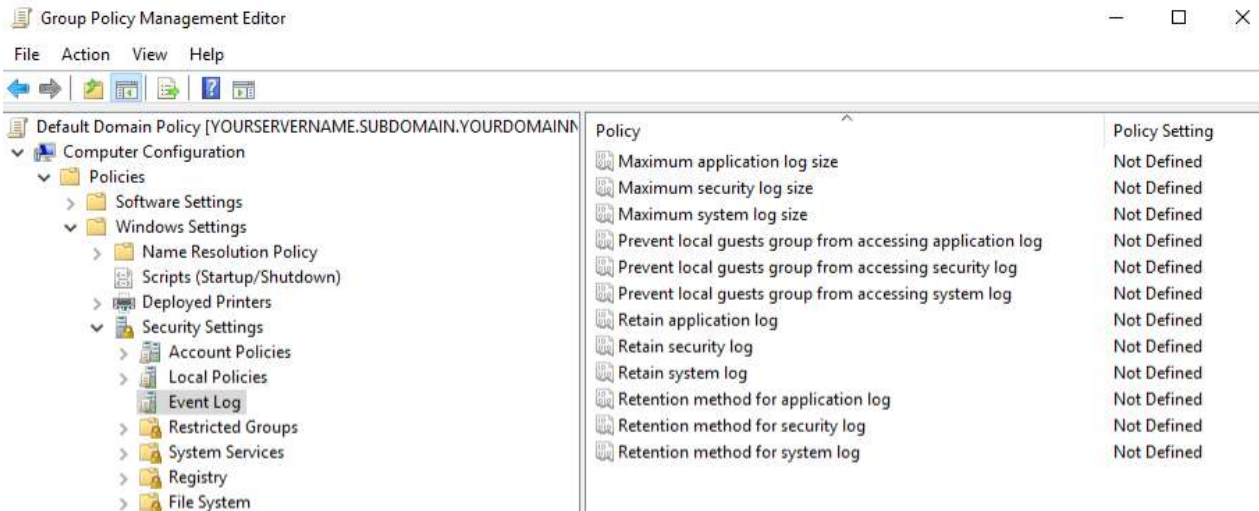
Event Log

<https://technet.microsoft.com/en-us/library/dd349798.aspx>

1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management](#) above.



2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.



3. Click on Event Log.

4. From the right-hand pane, double-click each option you want to edit, to open the Properties.

a. For explanation of an option, click the Explain tab.

b. To enable an option, from the Security Policy tab, check the box to Define this policy setting:

c. Click OK to commit your settings.

d. Continue editing the options you need until all settings are defined according to your Security Policy. Below are base recommended settings.

Policy	Policy Setting
Maximum application log size	16384 kilobytes
Maximum security log size	16384 kilobytes
Maximum system log size	16384 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retain application log	7 days
Retain security log	7 days
Retain system log	7 days
Retention method for application log	By days
Retention method for security log	By days
Retention method for system log	By days

NOTES:

- You can calculate a reasonable log size by multiplying the average event size by the average number of events per month, assuming that you back your logs up on a monthly schedule.
- The average event takes up about 500 bytes within each log, and the log file sizes must be a multiple of 64 KB.
- Default Windows 2003 log size was 16384 kB. When you enable the Maximum log sizes for each type, the field populates with 16384 kB.
- If you set the log files too large you may run out of disk space. So, you will need to consider your hardware and available storage when configuring your settings.
- Prevent guest access to ALL logs – ONLY Affects Servers Earlier than Windows 2003.
- When you set the Retention method for each log type to Overwrite by days, the Retain policy is enabled and defaults to 7 days.

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

RESTRICTED GROUPS

Review the following information to customize your Restricted Groups policy.

Description of Group Policy Restricted Groups

<https://support.microsoft.com/en-us/help/279301/description-of-group-policy-restricted-groups>

Restricted Groups

<https://technet.microsoft.com/en-us/library/cc957640.aspx>

Manage Local Active Directory Groups using Group Policy Restricted Groups

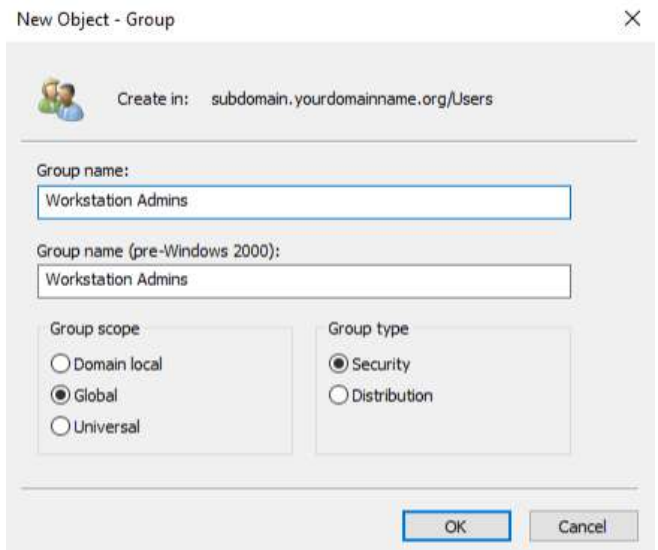
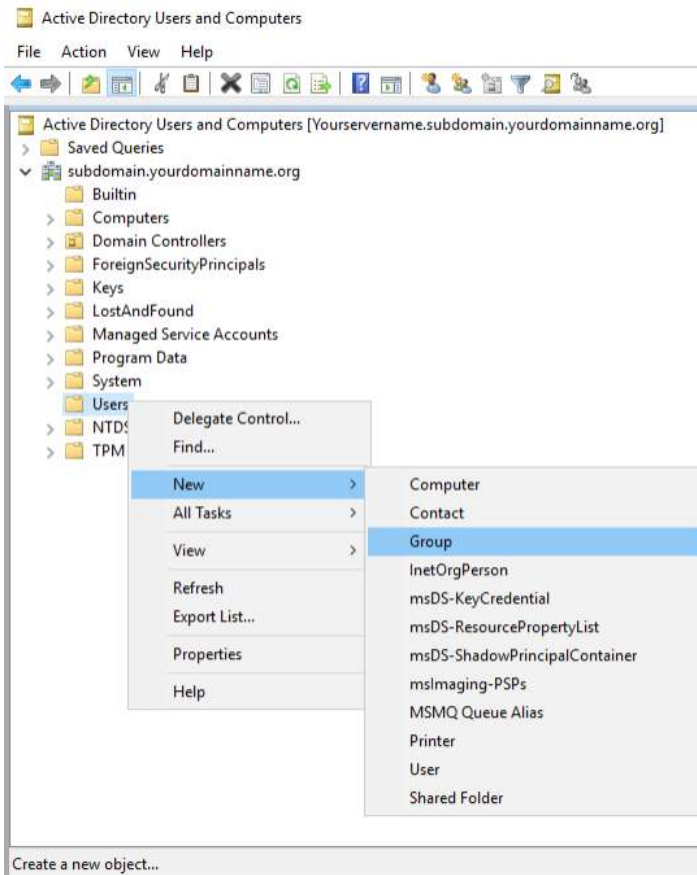
<https://www.petri.com/manage-local-active-directory-groups-using-group-policy-restricted-groups>

Implementing Least-Privilege Administrative Models

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>

Create a New Security Group to Manage Workstations & Member Servers

1. Open Active Directory Users and Computers from the Server Manager Tools Menu.



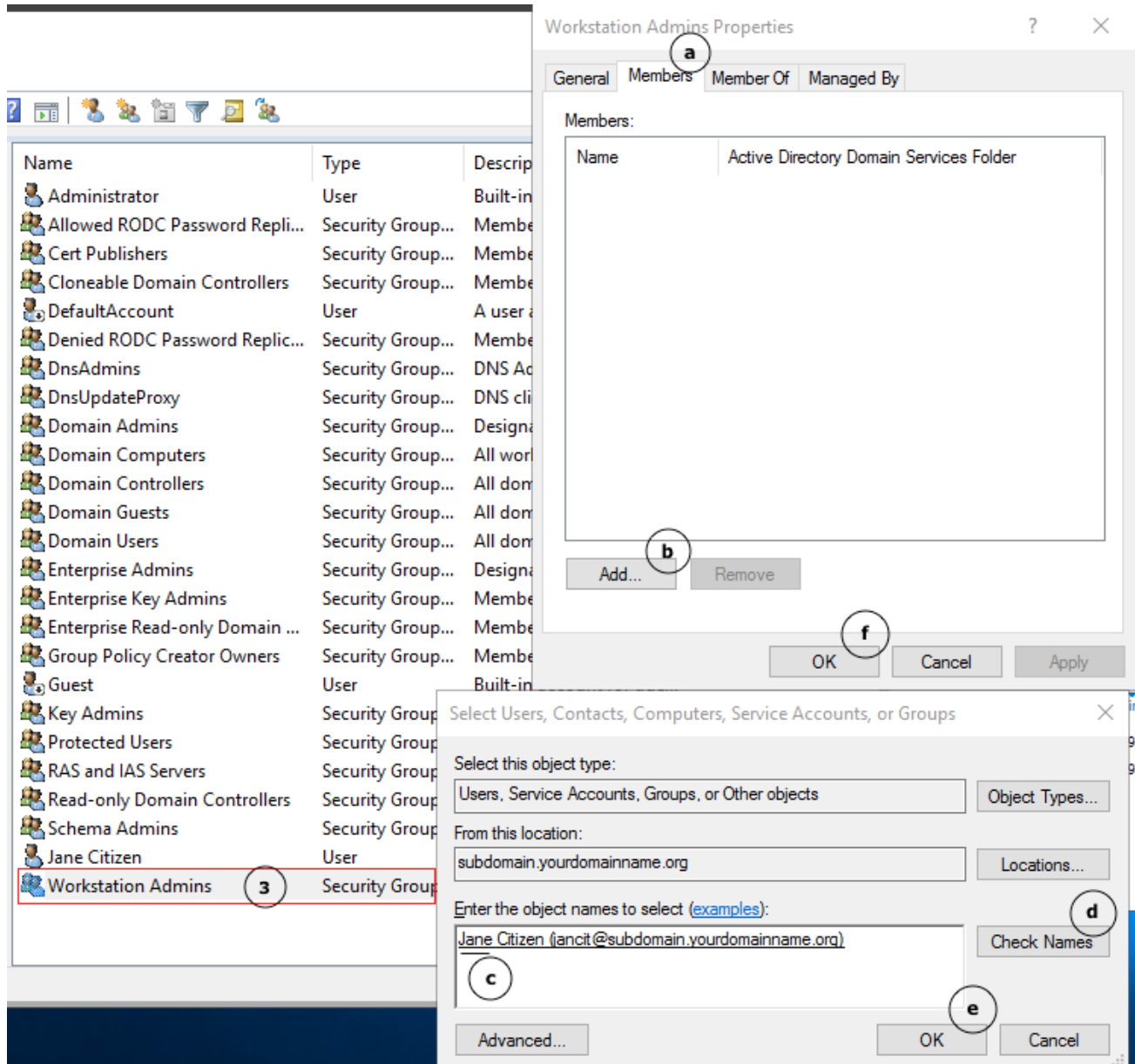
3. Type in the Group name: <Group name>
a. Leave the default Group Scope and Group Type.
b. Click OK.

2. Right-Click on the Users Container on the left.

- a. Mouse over New >
- b. Click Group.

Add Administrative Users to the New Security Group

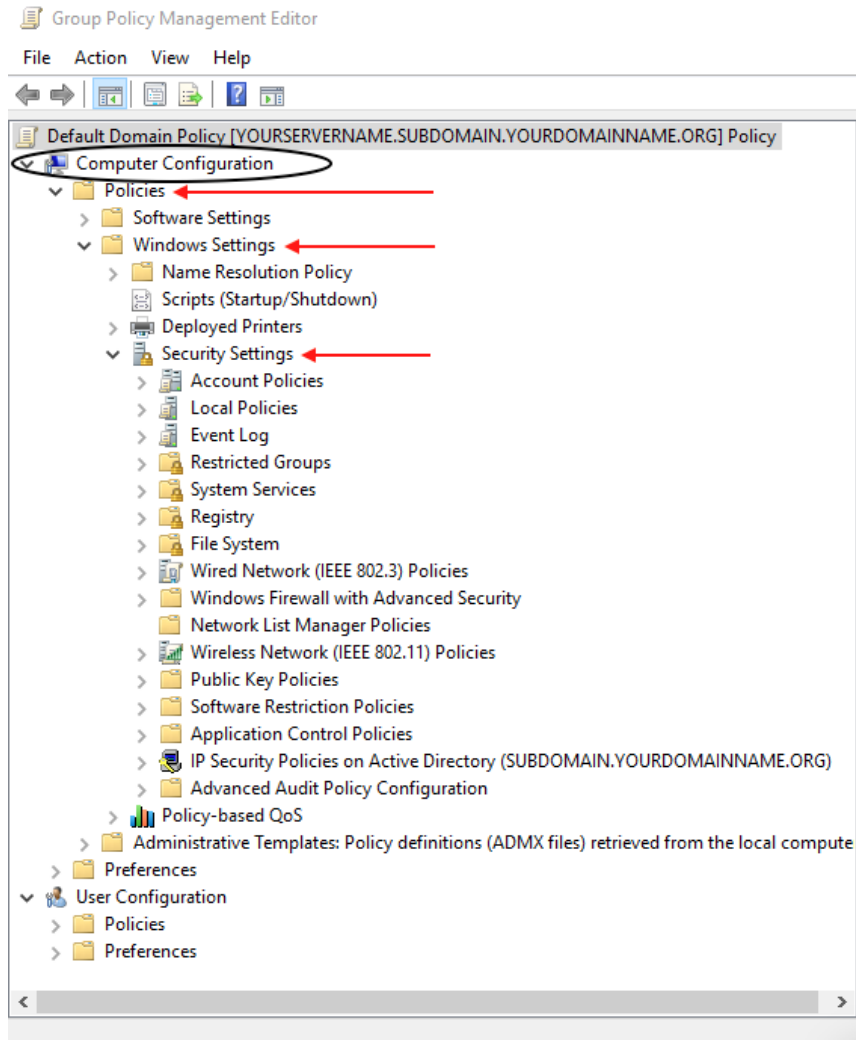
1. Open Active Directory Users and Computers from the Server Manager Tools Menu.
2. Click on the Users Container on the left.



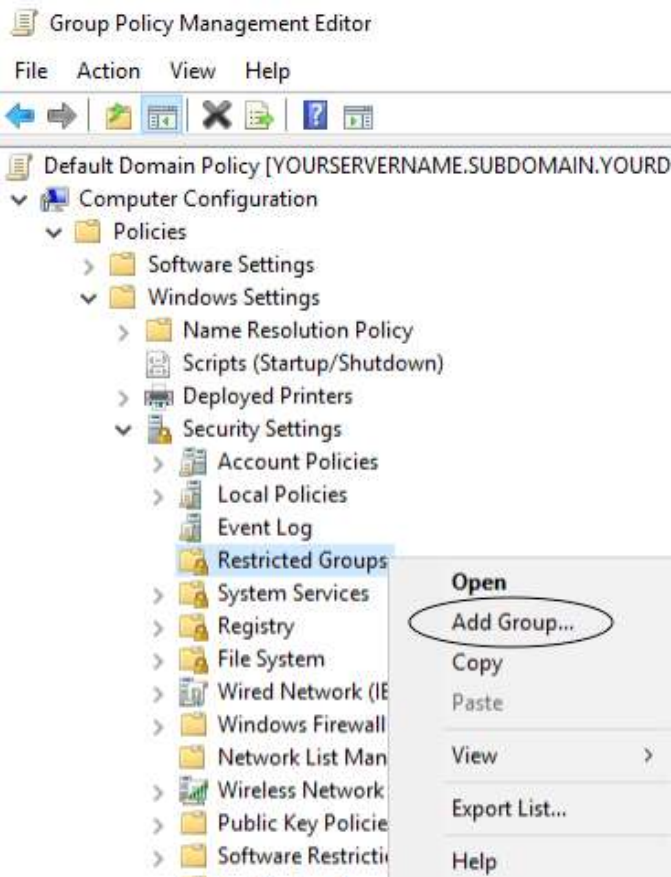
3. In the right-hand pane, double-click on the Workstation Admins Security Group to open the Properties.
 - a. Click on the Members tab.
 - b. Click Add...
 - c. Type a portion of the username in the Object names to select box.
 - d. Click Check Names, and if the name is found, it will auto complete in the Object names box.
 - e. Click OK in the Select Users... box.
 - f. Click OK in the Workstation Admin Properties box.

Create Your Local Administrator Group Policy

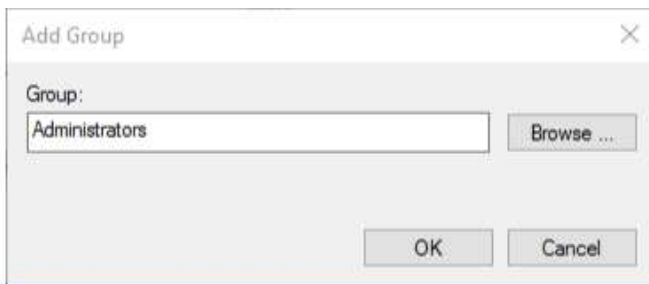
1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management above](#).



2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.

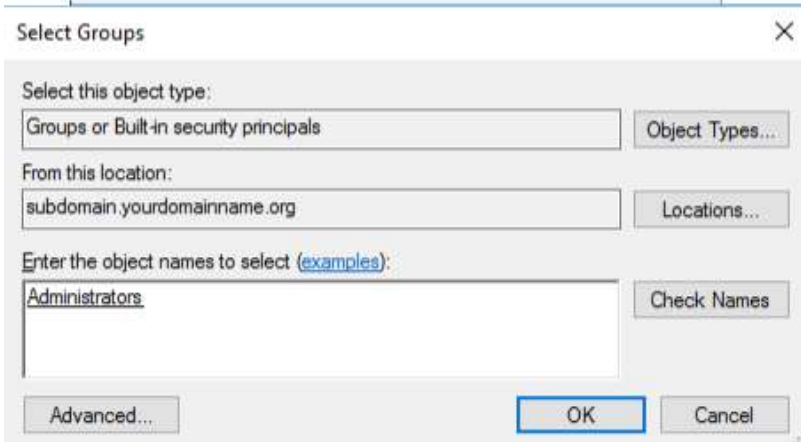


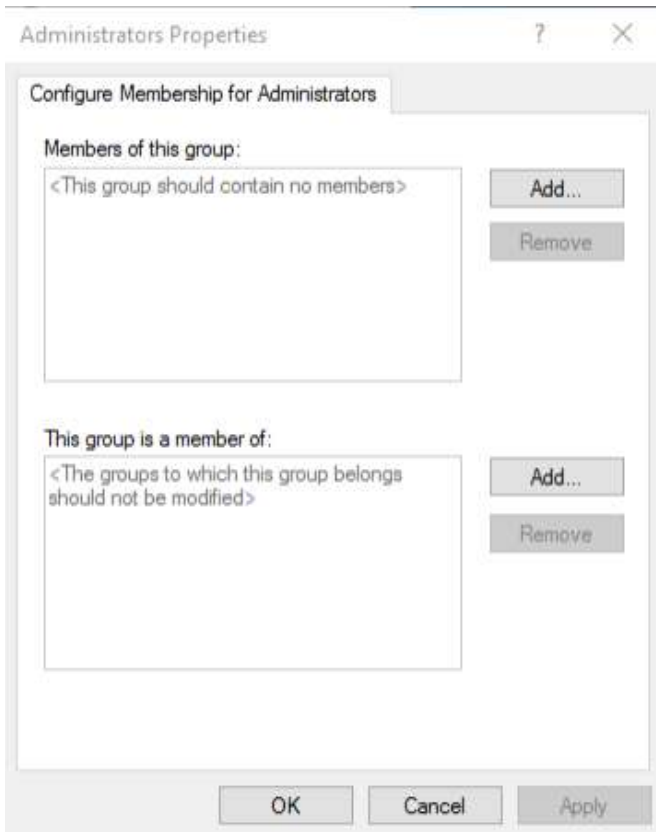
3. Right-click on Restricted Groups.
4. Click on Add Group...



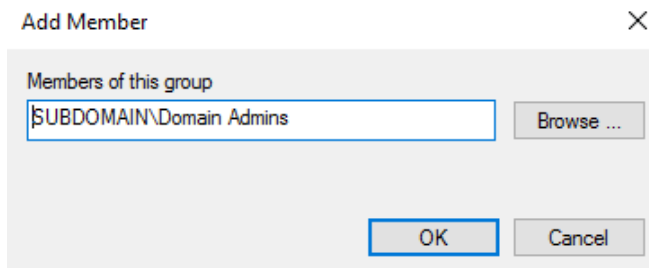
5. You can Add the Group in one of two ways:

- a. Add Group
 - i. Group: Type the <Group Name>. This does not have to be a Group that already exists in Active Directory, but we are Adding the (Local) Administrators Group. [Notice that the Object name is not preceded by <domain name>\Administrators.]
 - ii. Click OK.
- b. Select Groups box
 - i. From the Add Group box, click Browse.
 - ii. In the Select Groups box, under Enter the object names to select: type the <Group Name>. When you use the Select Groups box, the Group Name should already exist in Active Directory.
 - iii. Click Check Names.
 - iv. Once the name is resolved and underlined, Click OK.

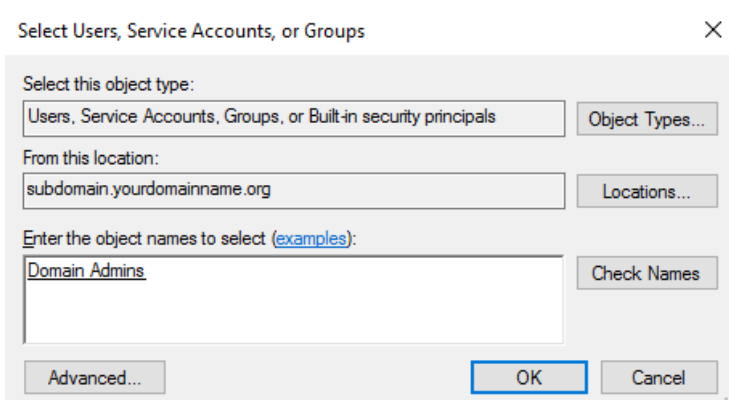




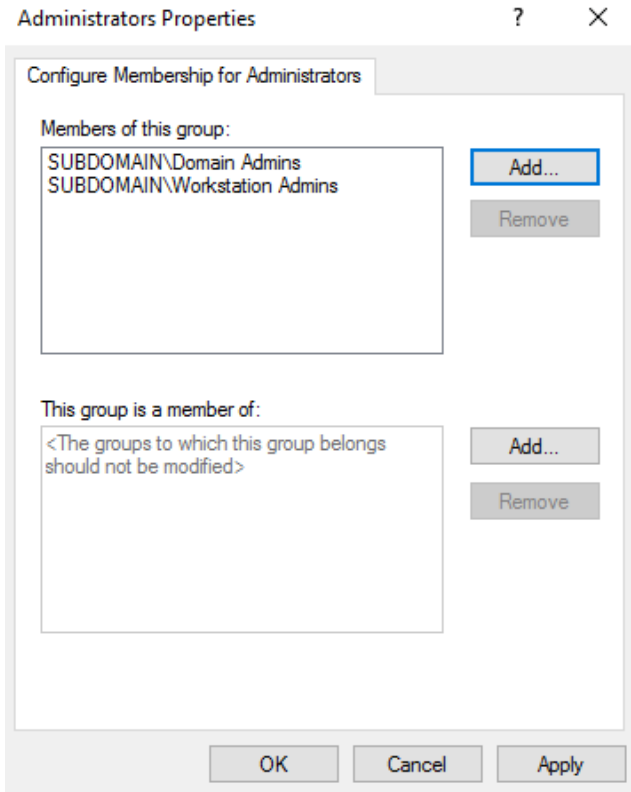
6. The Administrators Properties then launches to Configure Membership for Administrators.
7. Click Add... next to Members of this group:



8. You can Add Member one of two ways:
 - a. Add Member
 - i. Members of this group, Type the <Group Name>. When typing the name, the group does not need to exist in active directory.
 - ii. Click OK.



- b. Select Users, Service Accounts, or Groups
 - i. From the Add Member box, click Browse...
 - ii. In the Select Groups box, under Enter the object names to select: type the <Group Name>. When you use the Select Groups box, the Group Name should already exist in Active Directory.
 - iii. Click Check Names.
 - iv. Once the name is resolved and underlined, Click OK.



9. Before we are finished Configuring Membership for Administrators, use the example above to make sure the Domain and Workstation Admins Security Groups are added.

a. The Domain Admins Group needs to remain included in the Local Administrators Group for supportability and disaster recovery, so we are using this policy to enforce that recommendation.

b. Any user we add to the Workstation Admins group will be a Local Administrator on all of the domain member servers and workstations.

c. This policy does not prevent an account from being added to the Local Administrators Group, but every time Group Policy is applied or refreshed, any accounts added will be overwritten. The Local Admin Group will only contain the Groups or Users that you add here.

d. This setting can be used for any default installed groups and also for custom groups.

e. Click OK.

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

SYSTEM SERVICES

Review the following information to customize your System Services:

Guidance on disabling system services on Windows Server 2016 with Desktop Experience

<https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server>

This article includes a downloadable spreadsheet of services:

<https://msdnshared.blob.core.windows.net/media/2017/05/Service-management-WS2016.xlsx>

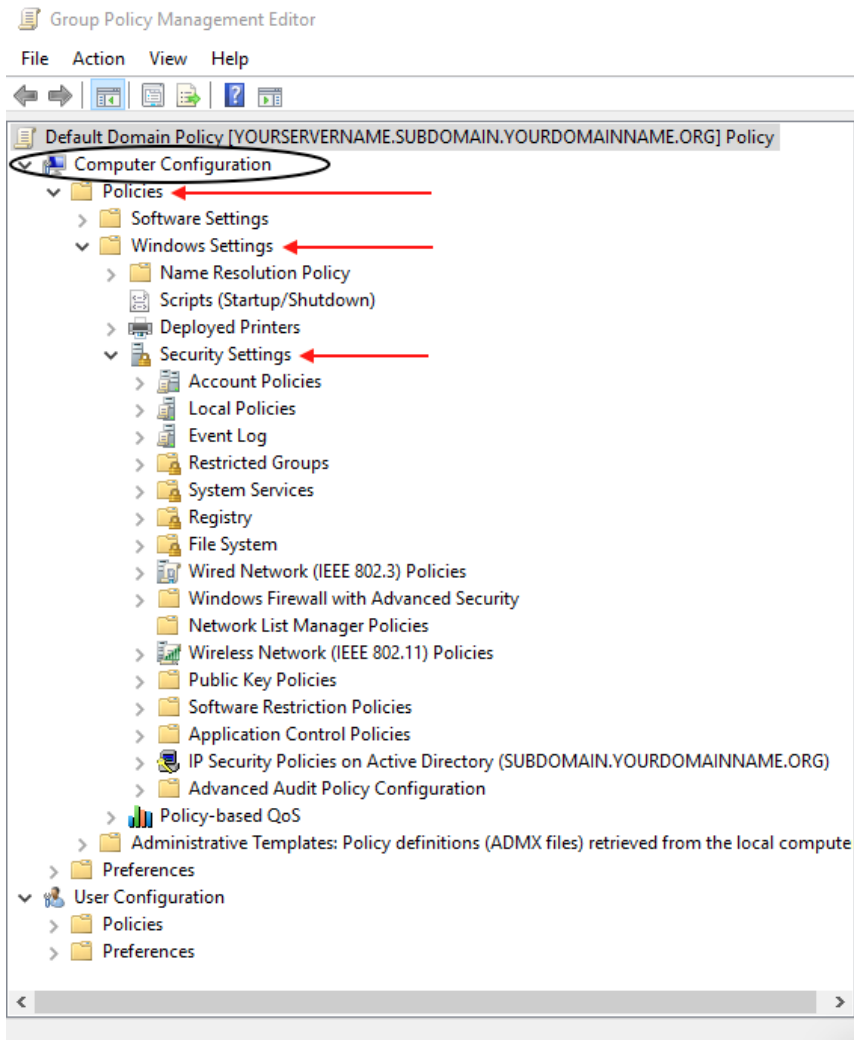
Per-User Services in Windows 10 and Windows Server

<https://docs.microsoft.com/en-us/windows/application-management/per-user-services-in-windows>

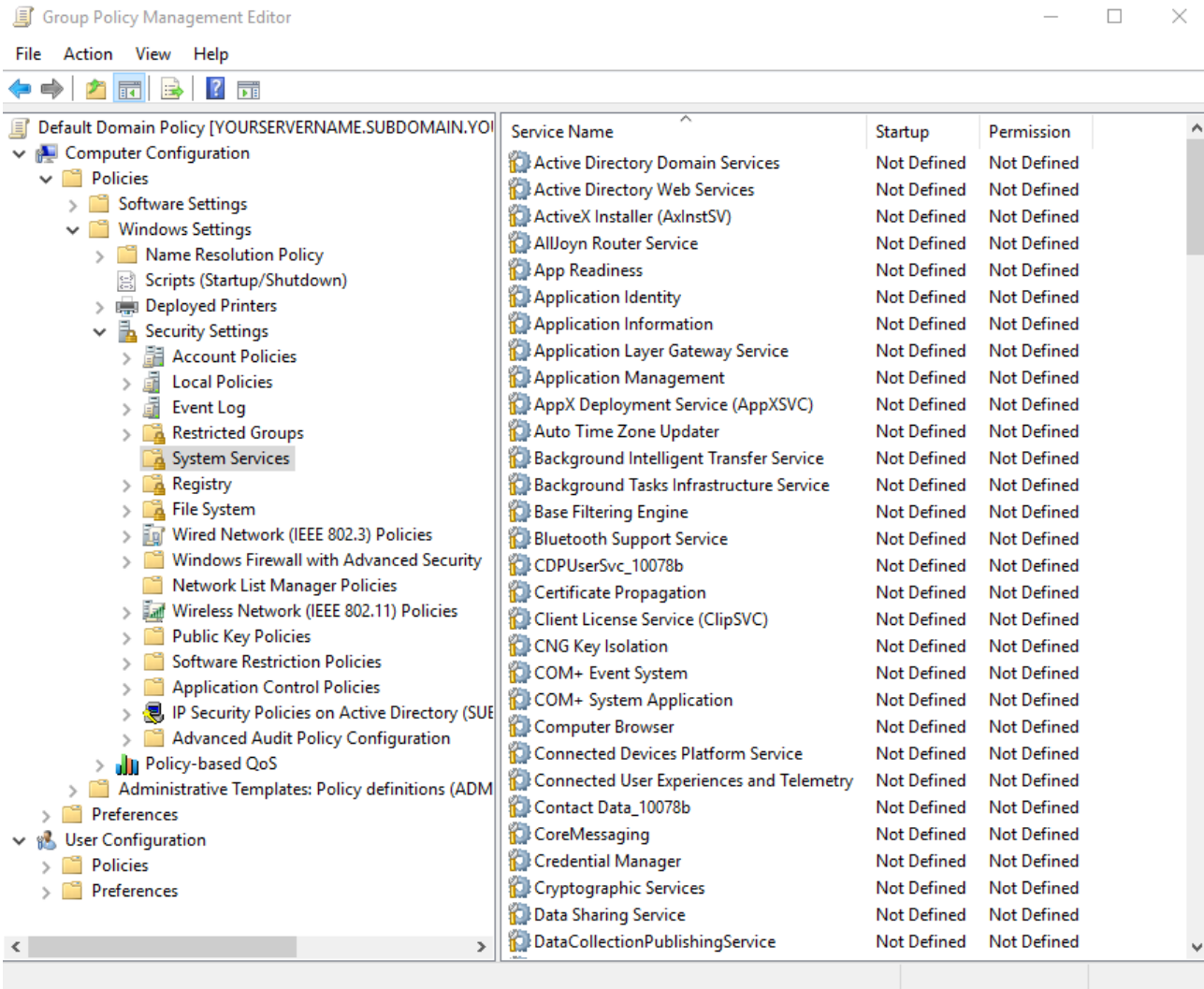
Access Control and Authorization Overview

[https://technet.microsoft.com/en-us/library/jj134043\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj134043(v=ws.11).aspx)

1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management above](#). Remember that in this exercise, you are editing the Default Domain Policy, which affects all domain workstations. You might consider separating any System Services GPO's, categorized by Service Startup Mode and the Users or Groups who can edit them.



2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.



3. Click on System Services.

4. From the right-hand pane, double-click each option you want to edit, to open the Properties. Refer to the [Guidance link](#) on the previous page for Microsoft recommendations.

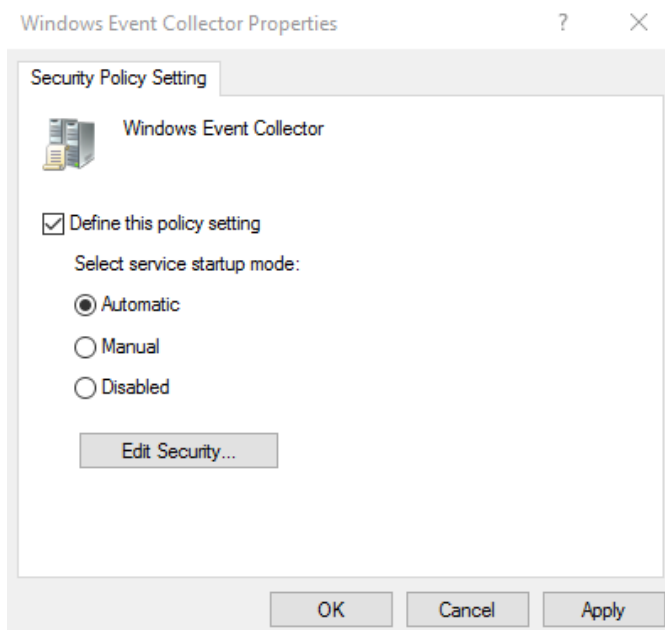
- a. Test the impact of each System Service policy you configure prior to implementing in your domain!!
- b. From the Security Policy Setting tab, check the box to Define this policy setting
- c. Select the service startup mode:
 - i. Automatic – Starts when the OS boots. It can gracefully shutdown when it is no longer needed by the system or an application, and can be triggered again when requested.
 - ii. Manual – Starts when triggered by an application
 - iii. Disabled – Will not start when the OS boots, and cannot be triggered by any applications.
- d. The default permissions for each Defined policy setting includes:
 - i. SYSTEM – Full Control
 - ii. Administrators (<Subdomain>\Administrators) – Full Control
 - iii. Interactive – Read only
- e. Click OK to commit your settings.

System Services Example Configuration

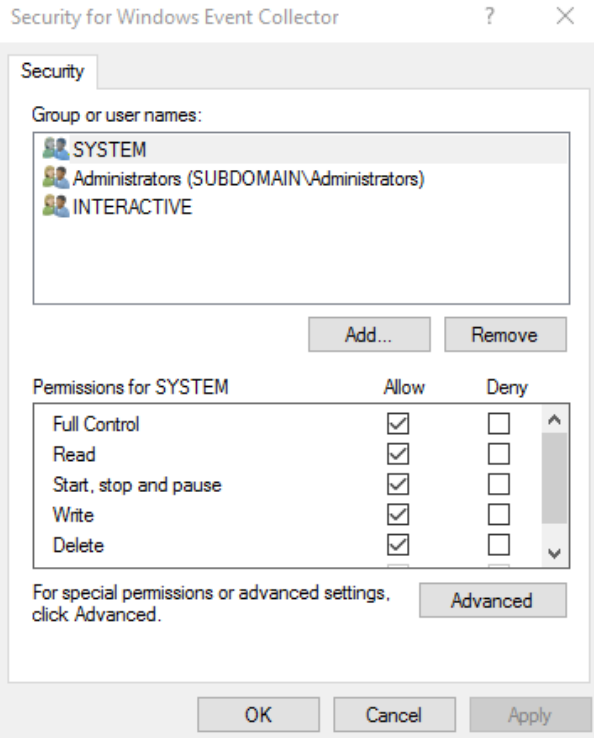
Windows Event Collector

Service description	This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted.
Service name	Wecsvc
Installation	Always installed
StartType	Manual
Recommendation	Do not disable
Comments	Collects ETW events (including security events) for manageability, diagnostics. Lots of features and third-party tools rely on it, including security audit tools

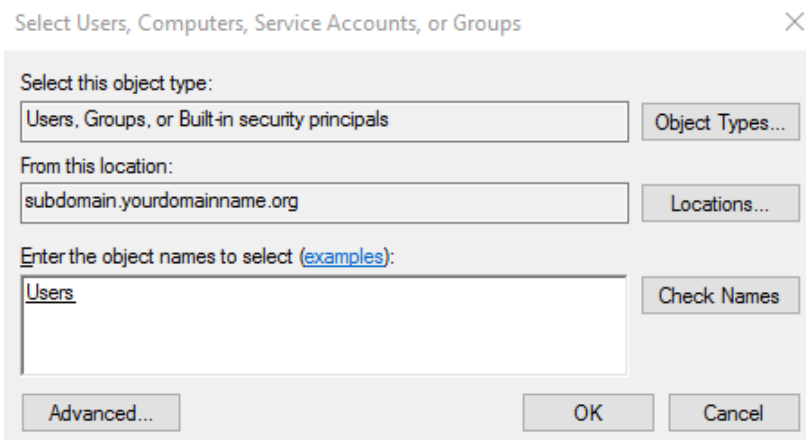
5. In this example, we will configure the Windows Error Reporting Service, to prevent it from being disabled by a domain user.



- a. From the Service Name column, double-click on the Windows Event Collector to open the Properties.
 - b. Click the box to Define this policy setting.
 - c. Change the radio button under Select service startup mode: to Automatic.
 - d. Click Apply.
6. All System Service Properties offer options to define User and Group permissions.
- a. From the <Service> Properties, click Edit Security...

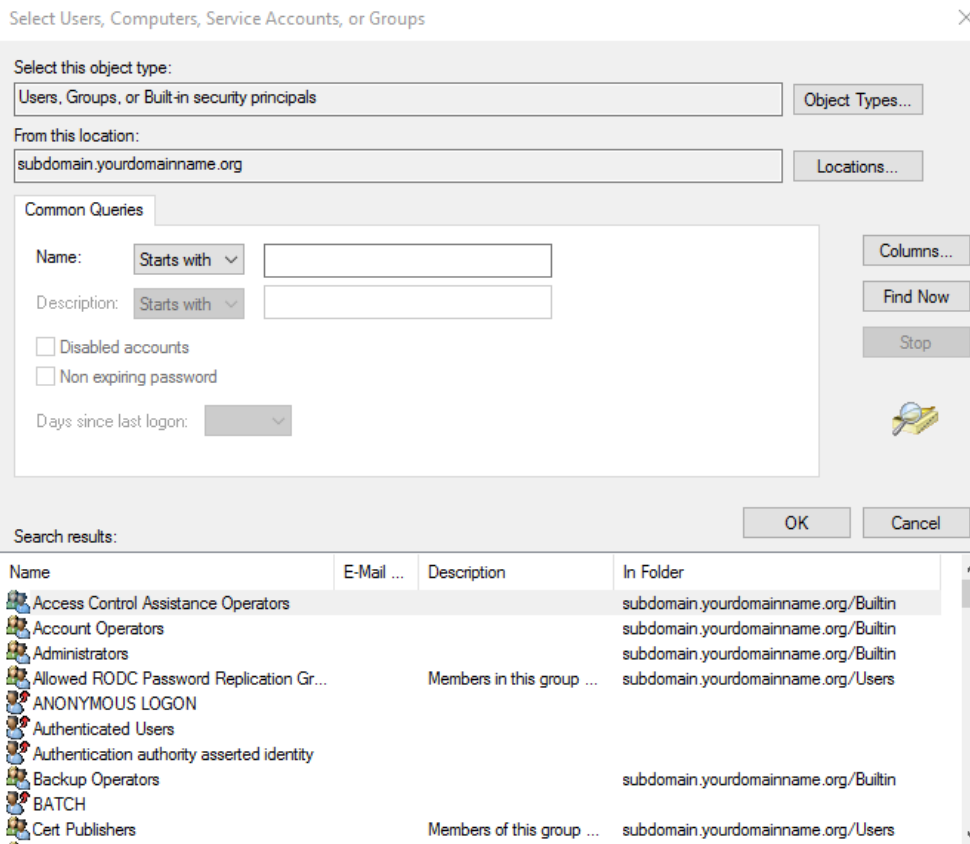


b. In the Security for <Service> box, Click Add...



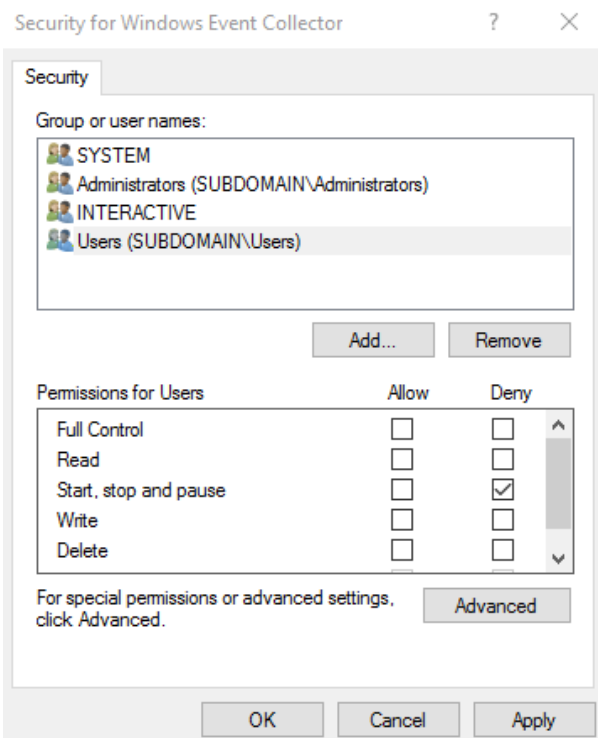
c. Type a portion of the username in the Object names to select box.

d. Click Check Names, and if the name is found, it will auto complete in the Object names box.

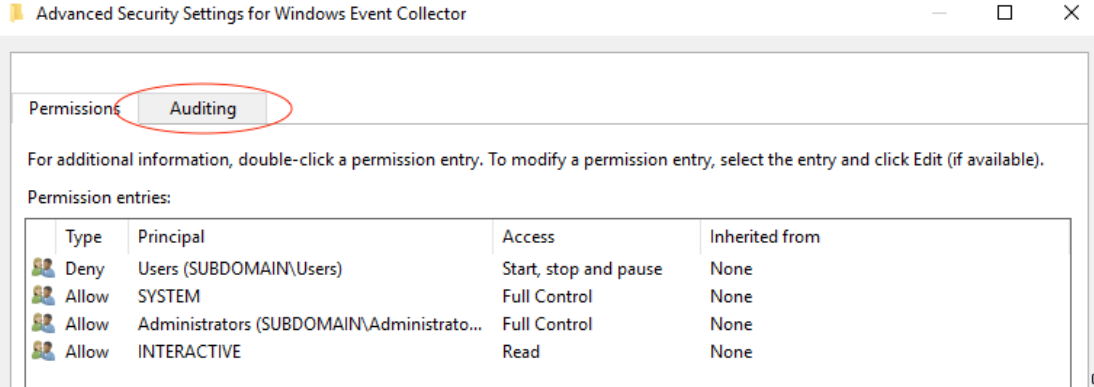


- i. If you have trouble locating the User or Group, you can click Advanced... for additional search options.
- ii. In the Select Users, Computers, Service Accounts, or Groups Advanced Search dialogue select from the Name: drop-down, Starts with or Is exactly. Then type the name or partial name into the Name: field, and click Find Now.
- iii. Alternatively, you can simply click Find Now to see a complete list of the User and Group options for your domain.
- iv. Select either the name you searched or that you browsed for from the Search results: section.
- v. Click OK.

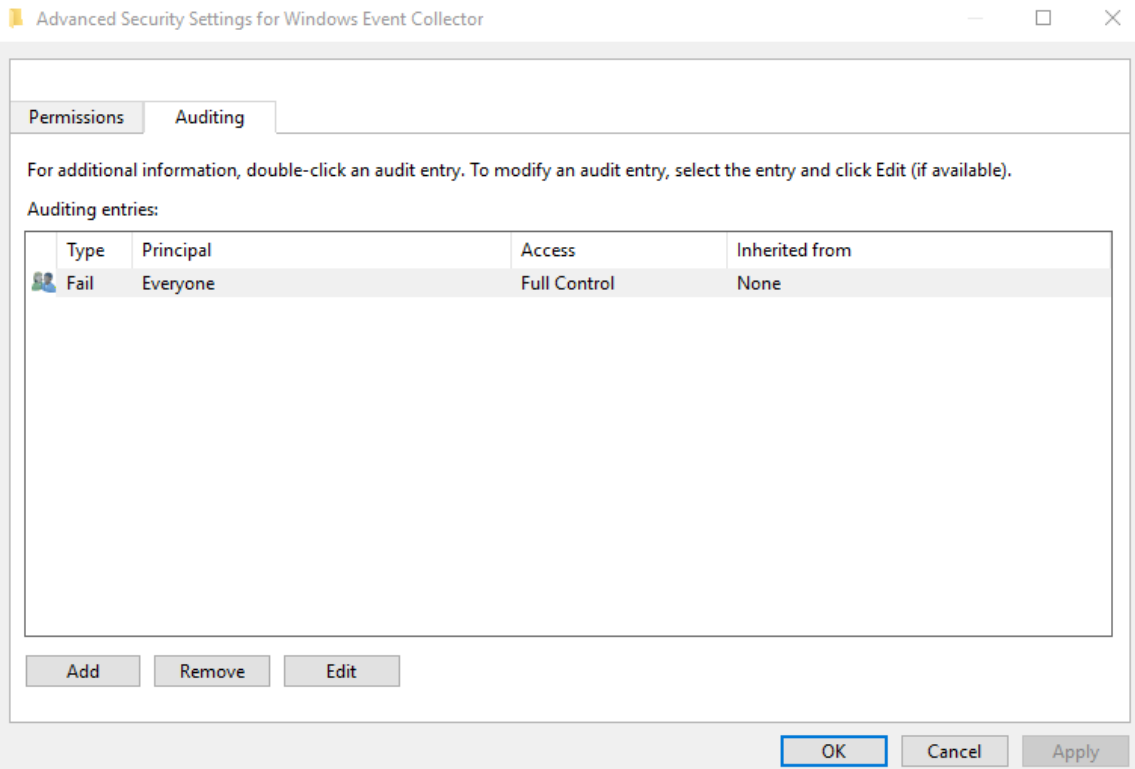
e. Click OK in the remaining Select Users... box.



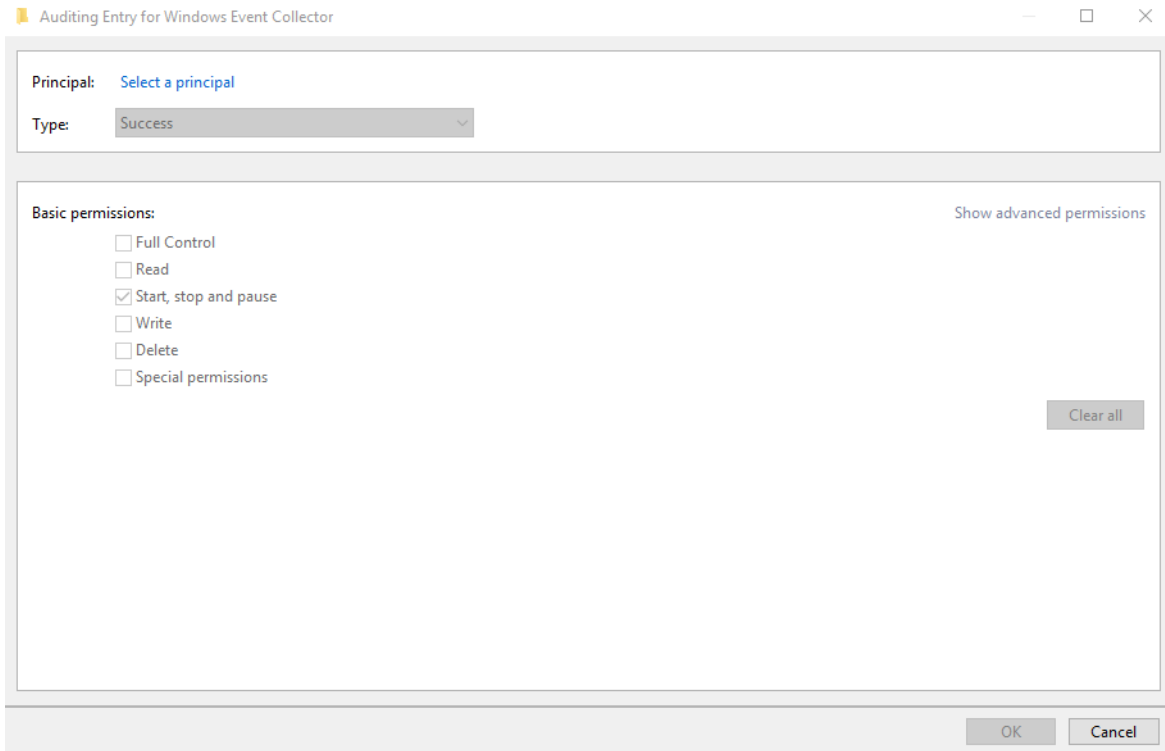
7. All System Service Properties also have the option to configure Auditing.
 - a. From the Security for <Service> dialogue, click Advanced.



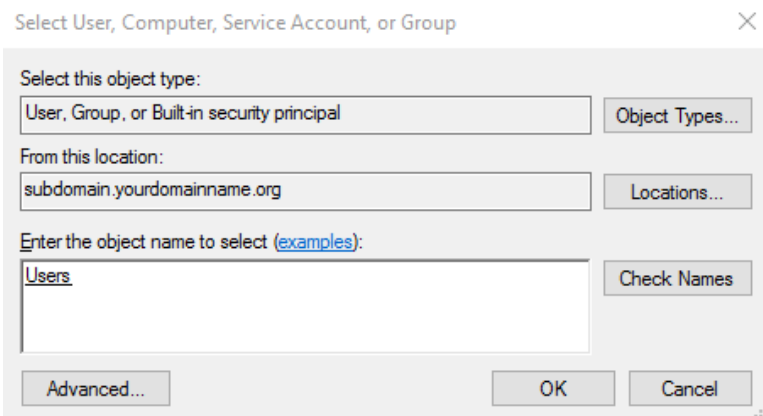
b. Click on the Auditing tab.



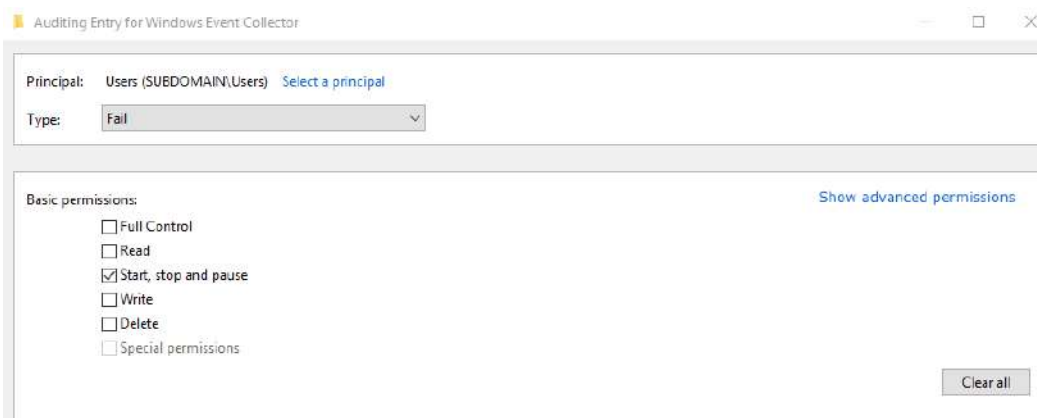
c. Click Add.



d. Click Select a principal.



e. Enter the object name and click Check Names or Click Advanced to search.
f. Click OK.



g. Change the Type: drop-down to Fail. Now when someone from the User Group attempts and subsequently fails to change the Windows Event Collector service, the event will be logged.

NOTE: Since the User Group is set to Deny, only failures can be logged.

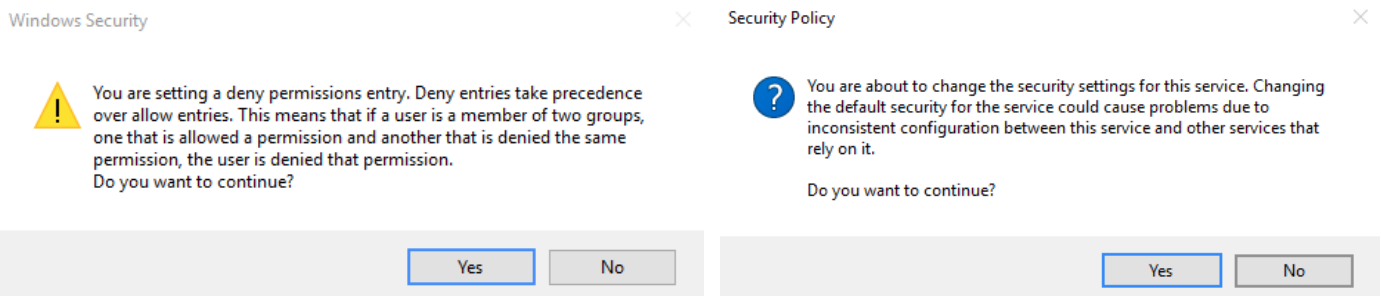
h. In the image above, notice on the right, the option to Show advanced permissions. Click to configure the following additional options:

- i. Query Template
- ii. Change Template
- iii. Query Status
- iv. Enumerate Dependents
- v. Interrogate
- vi. User-defined control
- vii. Change permissions
- viii. Take ownership

i. When you are finished with your Auditing configurations, click OK.

j. Click OK in the Advanced Security Setting for Windows Event Collector dialogue.

k. Click OK in the Security for Windows Event Collector dialogue.



8. When you configure deny permissions, you will receive this message. Click Yes to Continue.

9. When you add or remove users or groups from the security settings, you will receive this message. Click Yes to continue.

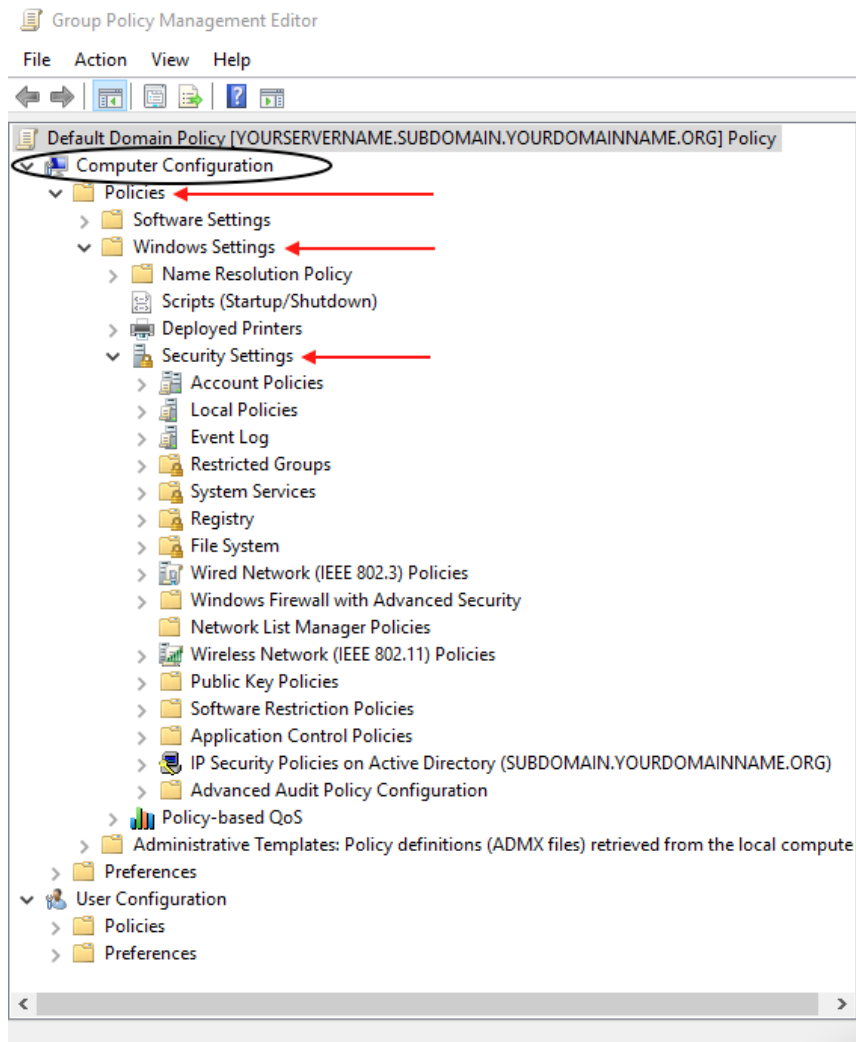
Service Name	Startup	Permission
Windows Connection Manager	Not Defined	Not Defined
Windows Defender Network Inspection Ser...	Not Defined	Not Defined
Windows Defender Service	Not Defined	Not Defined
Windows Driver Foundation - User-mode ...	Not Defined	Not Defined
Windows Encryption Provider Host Service	Not Defined	Not Defined
Windows Error Reporting Service	Not Defined	Not Defined
Windows Event Collector	Automatic	Configured
Windows Event Log	Not Defined	Not Defined
Windows Firewall	Not Defined	Not Defined

10. The System Services list updates to reflect the changes.

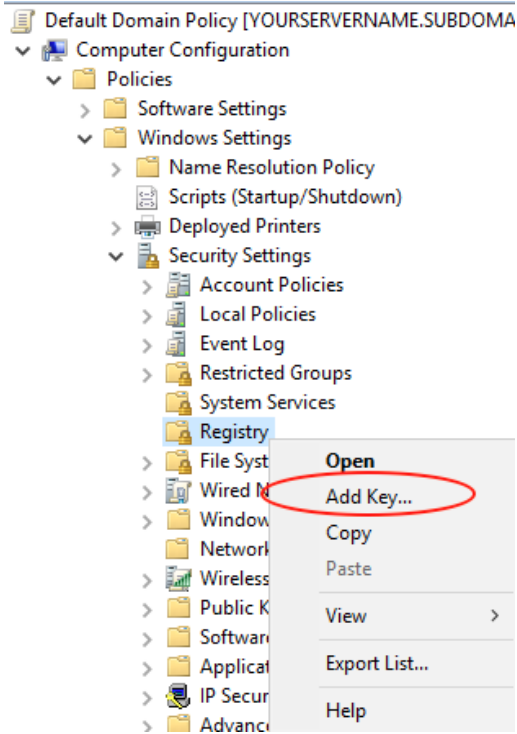
When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

REGISTRY POLICIES

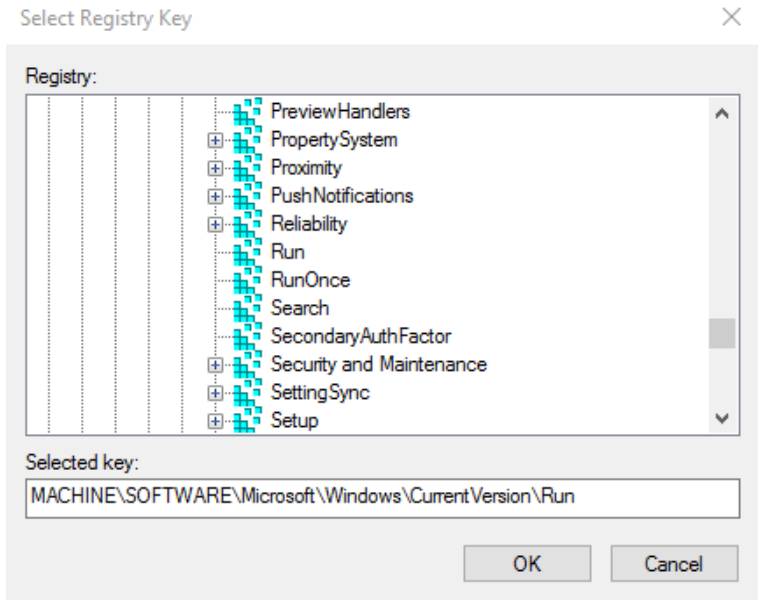
1. If you are not already at the GPME pictured below, follow the instructions under [Group Policy Management above](#).



2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.

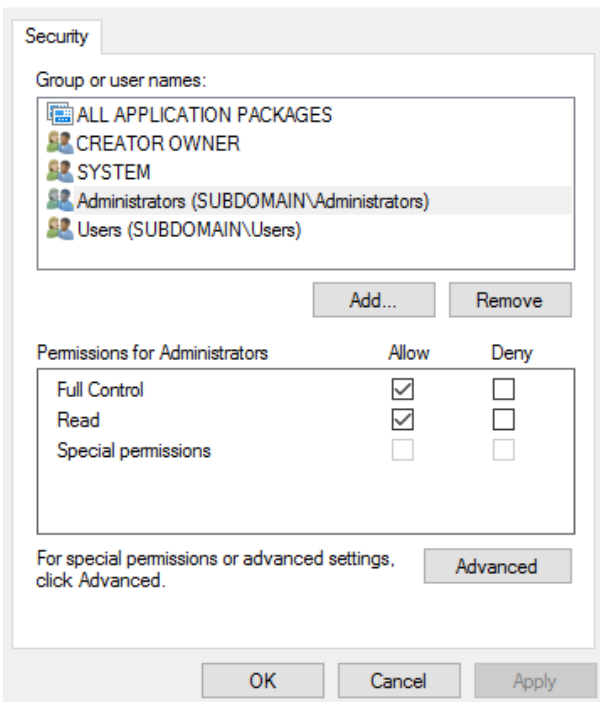


3. Right-click on Registry and select Add Key...
4. You will see 3 registry groups
 - a. CLASSES_ROOT
 - b. MACHINE
 - c. USERS



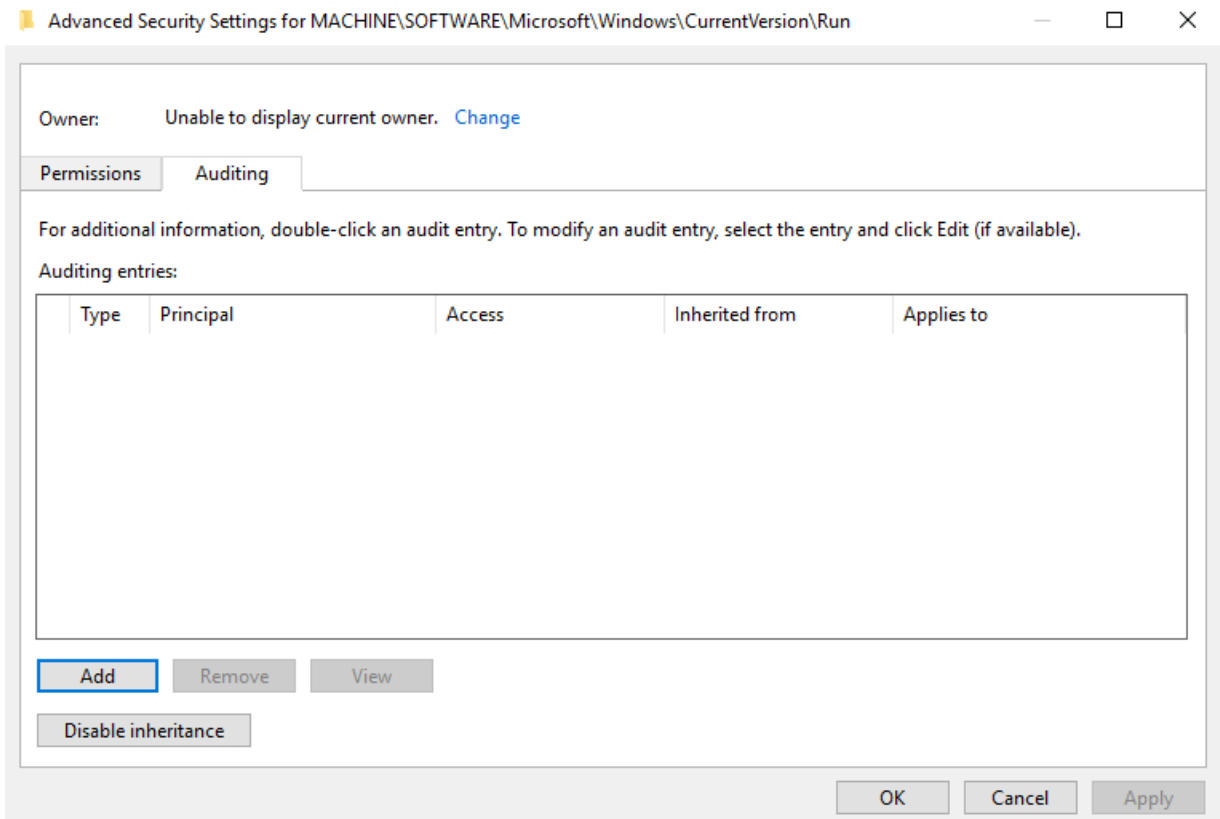
5. Expand +MACHINE +SOFTWARE +Microsoft +Windows +CurrentVersion
6. Click on Run.
7. As you expand, the path will appear under Selected key:
8. Click OK.

Database Security for MACHINE\SOFTWARE\M... ? X

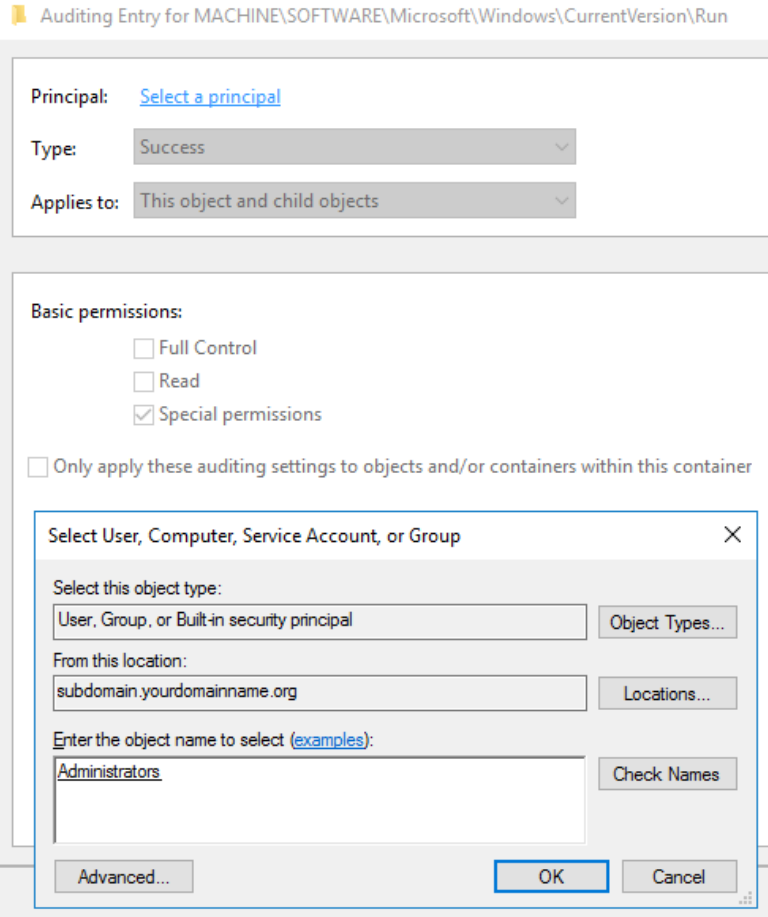


9. In the Database Security dialogue, click Advanced.

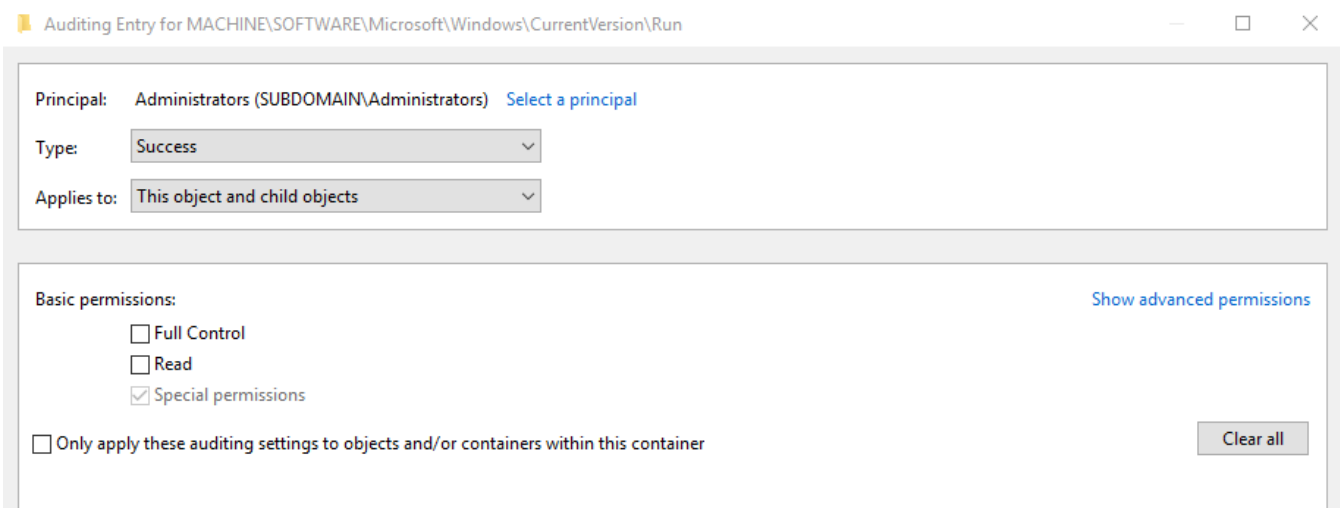
- 10. In this exercise, we will configure Auditing for the Registry Run Key & its Subkeys.
 - a. In the Advanced Security Settings, click the Auditing tab.



- b. Click Add.



- c. In the Auditing Entry dialogue, click Select a principal.
- d. In the Select User, Enter the object name box, Type Administrators.
- e. Click Check Names
- f. Click OK.



11. Back at the Auditing Entry dialogue, click Show advanced permissions.

Auditing Entry for MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Principal: Administrators (SUBDOMAIN\Administrators) [Select a principal](#)

Type: Success

Applies to: This key and subkeys

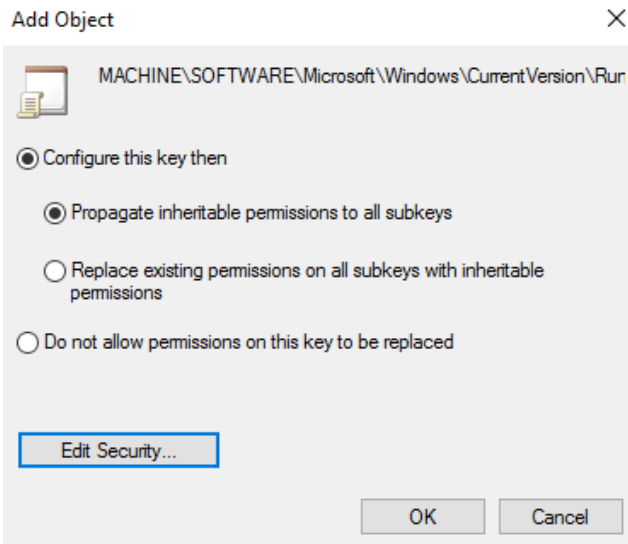
Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full Control	<input type="checkbox"/> Create Link
<input checked="" type="checkbox"/> Query Value	<input checked="" type="checkbox"/> Delete
<input checked="" type="checkbox"/> Set Value	<input type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Create Subkey	<input checked="" type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Enumerate Subkeys	<input checked="" type="checkbox"/> Take ownership
<input type="checkbox"/> Notify	

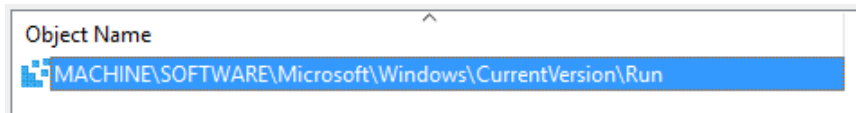
Only apply these auditing settings to objects and/or containers within this container Clear all

OK Cancel

- a. Check the following:
 - i. Query Value
 - ii. Set Value
 - iii. Create Subkey
 - iv. Enumerate Subkeys
 - v. Delete
 - vi. Change permissions
 - vii. Take ownership
- b. Change the Type: drop-down to Success
- c. Change the Applies to: drop-down to This key and subkeys
- d. Now when someone from the Domain Level Administrators Group attempts and successfully changes the Local Machine Run key, the event will be logged.
- e. Click OK.
- f. This window will close, leaving the Database Security dialogue. Click OK.

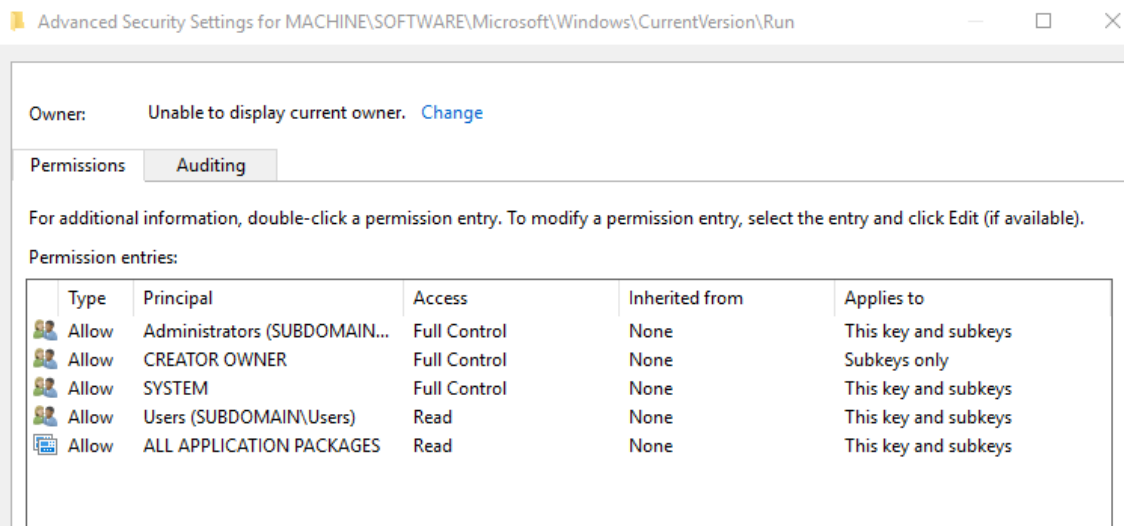


12. Add Object launches.
 - a. Configure this key then
 - i. Default - Propagate inheritable permissions to all subkeys
 - ii. Replace existing permissions on all subkeys with inheritable permissions
 - b. Do not allow permissions on this key to be replaced.
 - c. Click OK.



13. In the GPME > Computer Config > Windows Settings > Security Settings, when you click on Registry the keys where you have configured permissions or auditing will appear in the left-hand pane under Object Name.

NOTES:



- Notice the default Permissions. Administrators have Full Control, and Users have Read only access.
- You could also use this policy to restrict access to registry keys from certain groups by adding them to the Permissions tab and denying access.
- WARNING! Thoroughly test any settings you configure here, especially if removing access to a key!

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

FILE SYSTEM PERMISSIONS

Review the following information to customize your File System Permissions:

Dynamic Access Control Overview

[https://technet.microsoft.com/en-us/library/dn408191\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn408191(v=ws.11).aspx)

Dynamic Access Control: Scenario Overview

<https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/dynamic-access-control--scenario-overview>

Scenario: Central Access Policy

<https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/scenario--central-access-policy>

This section allows you to specify permissions and auditing on specific files and folders.

When finished working with the Default Domain policy, **remove the user account you added when you began this section from the Domain Admins Security Group.**

WIRELESS NETWORK POLICIES

Review the following information to customize your Wireless Network Policies:

Managing the New Wireless Network (IEEE 802.11) Policies Settings
[https://technet.microsoft.com/en-us/library/hh994701\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh994701(v=ws.11).aspx)

When finished working with the Default Domain policy, **remove the user account you added when you began this section from the Domain Admins Security Group.**

Section VII: Hosts File GPO

The Hosts file from MVPS.org lists known spyware/malware sites, including those that distribute images and advertisements. This file is licensed under Creative Commons, and has been maintained and updated since it was created in 1998. This Hosts file, if implemented, prevents client systems from contacting known MALICIOUS sites that could infect their systems with malware.

Remember to check the website regularly, <http://winhelp2002.mvps.org/hosts.htm>, to keep your share up-to-date with the latest Hosts file!

Compared to the current MOREnet Blackhole DNS Service, since we have had members report the need to access certain websites that we then determined allowable, the Hosts file can be more restrictive. Thoroughly test its use within your environment to ensure your users can access the resources that they need. Easily edit the hosts file to allow certain sites, by removing entries, if necessary. Internal resources can be added to the hosts file to aid faster resolution and access. Open the file in Notepad and save back to your network file share without the .txt extension, and the file will update on the client the next time Group Policy is refreshed (default every 90 minutes + or – 30 minutes). To hasten the refresh, restart the client computer or use gpupdate /force at an Administrative Command Prompt.

MUST READ LINKS!

Blocking Unwanted Connections with a Hosts File

<http://winhelp2002.mvps.org/hosts.htm>

How to Create a File Share in Windows Server 2016

<http://www.tomsitpro.com/articles/create-file-share-windows-server-2016,1-3364.html>

Managing Permissions for Shared Folders

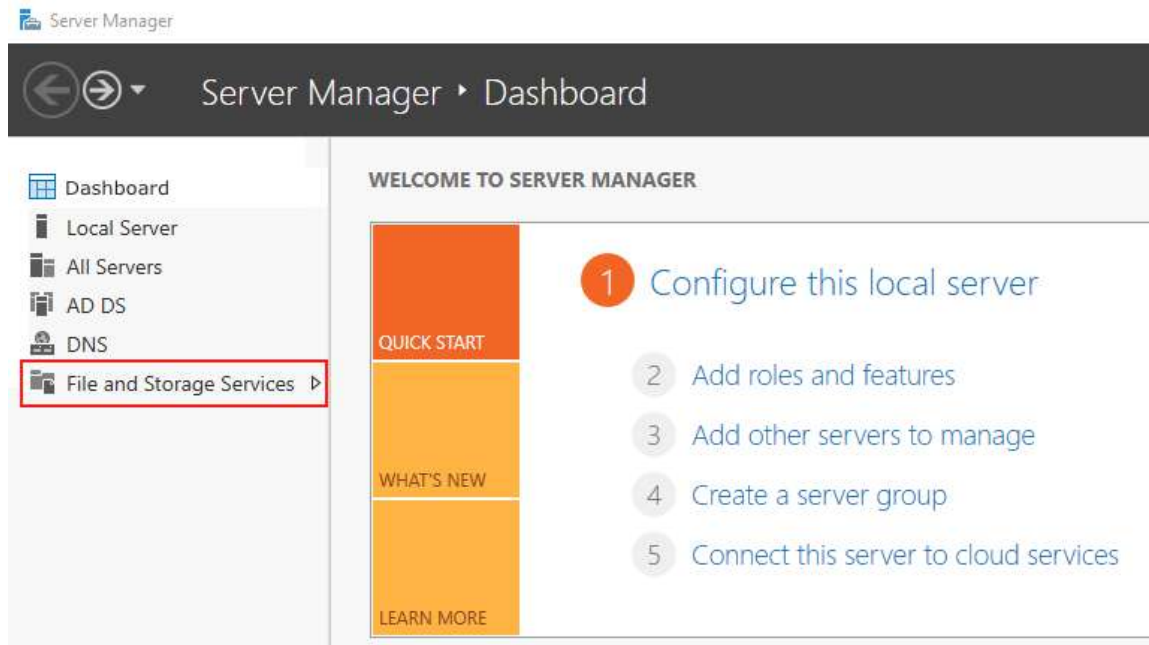
[https://technet.microsoft.com/en-us/library/cc753731\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc753731(v=ws.11).aspx)

Group Policy Preferences

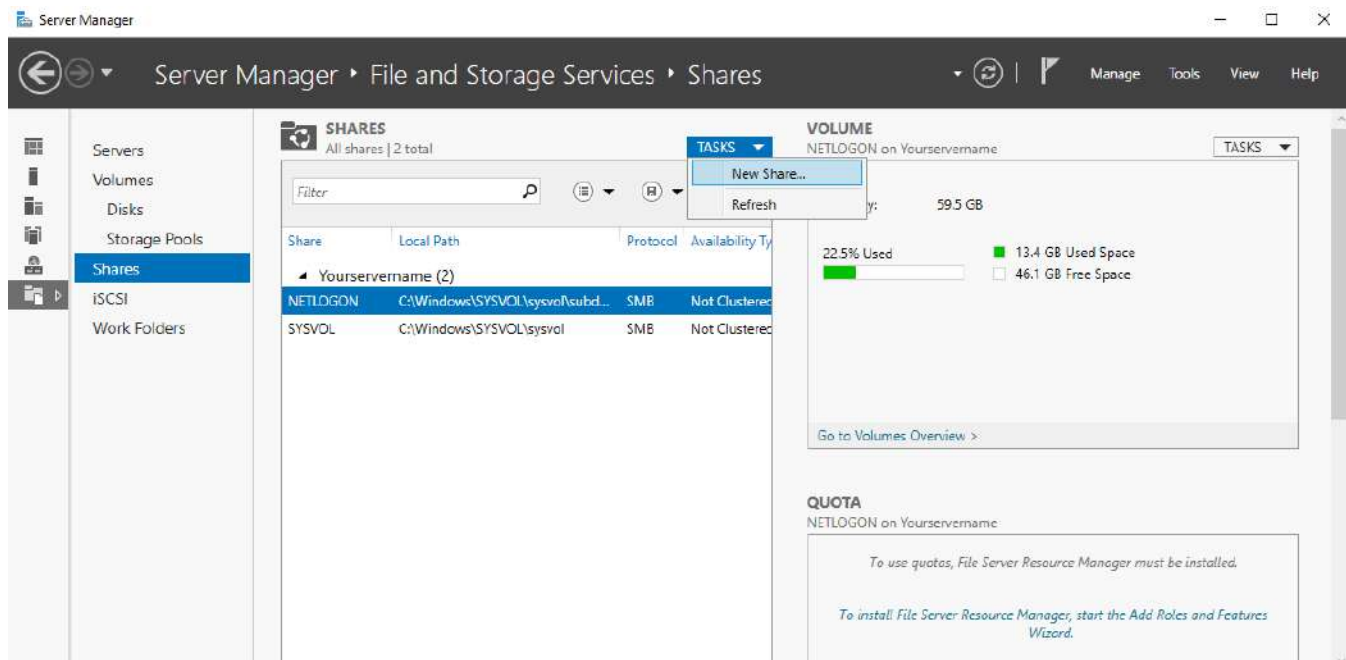
[https://technet.microsoft.com/en-us/library/dn581922\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn581922(v=ws.11).aspx)

CREATE A SHARE

1. Open Server Manager.



2. Click on File and Storage Services. This is the limited version of File and Storage Services that is installed with Windows Server 2016.

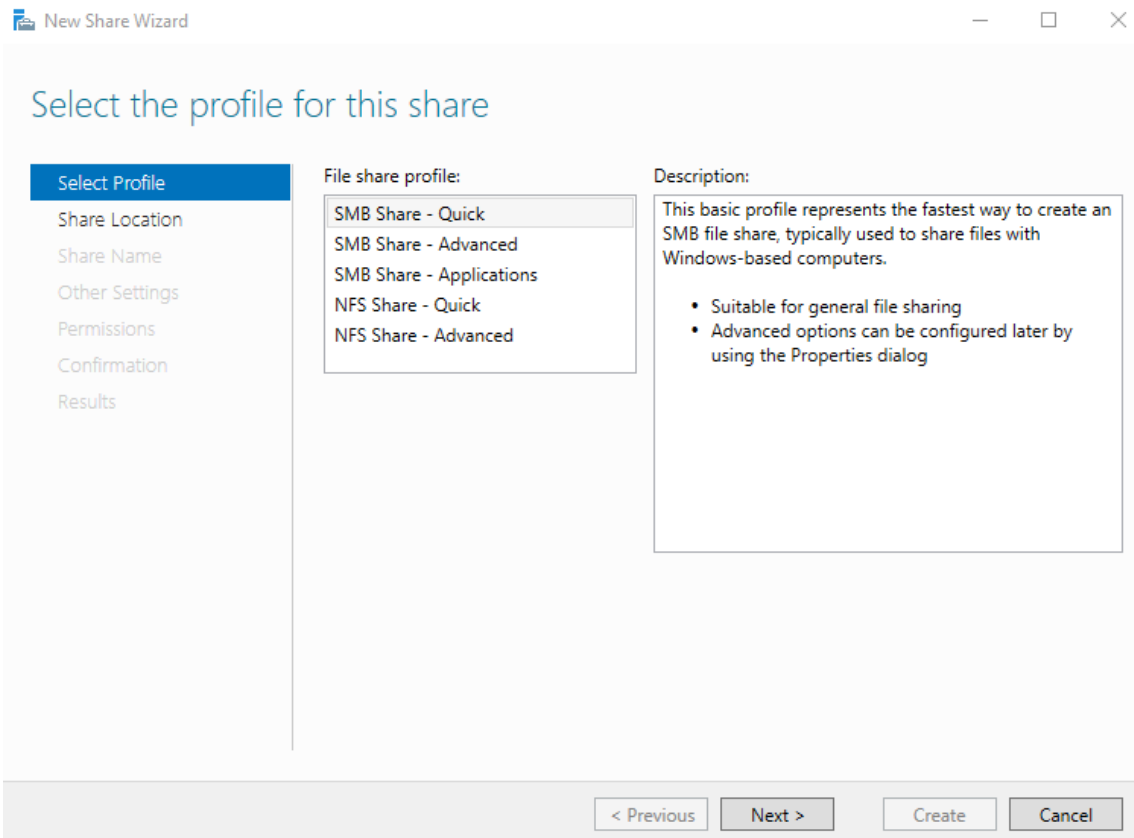


3. Click on Shares.

4. From the TASKS drop-down, select New Share...

5. This launches the New Share Wizard.

The Wizard



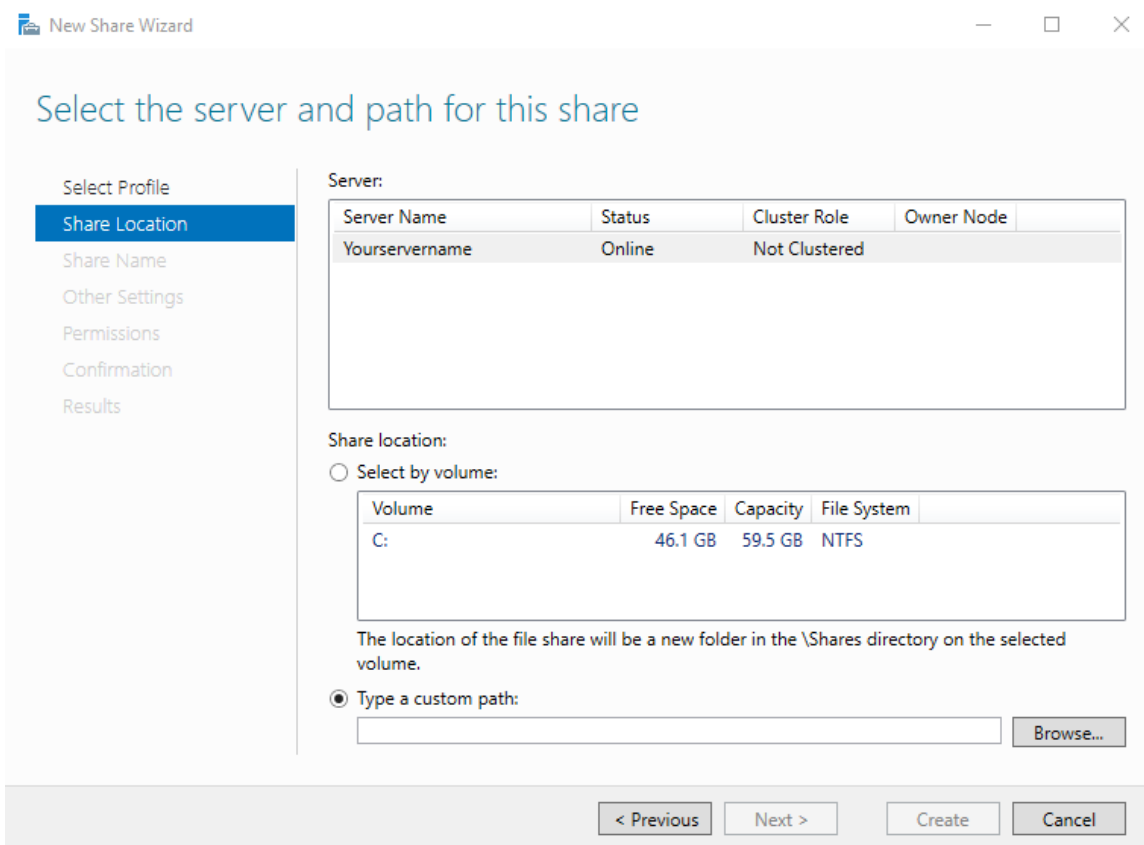
1. Select Profile

a. Options:

- i. SMB Share – Quick (basic profile, typically used with Windows-based computer file-sharing)
- ii. SMB Share – Advanced (requires the File Server Resource Manager be installed; enables quotas, folder level data classification for management and access policies, and set folder owners)
- iii. SMB Share – Applications (creates a file share appropriate for server applications like hyper-v and databases)
- iv. NFS Share – Quick (basic profile, typically used with Unix-based computers)
- v. NFS Share – Advanced (requires both the Server for NFS and File Server Resource Manager be installed; enables quotas, folder level data classification for management and access policies, and set folder owners))

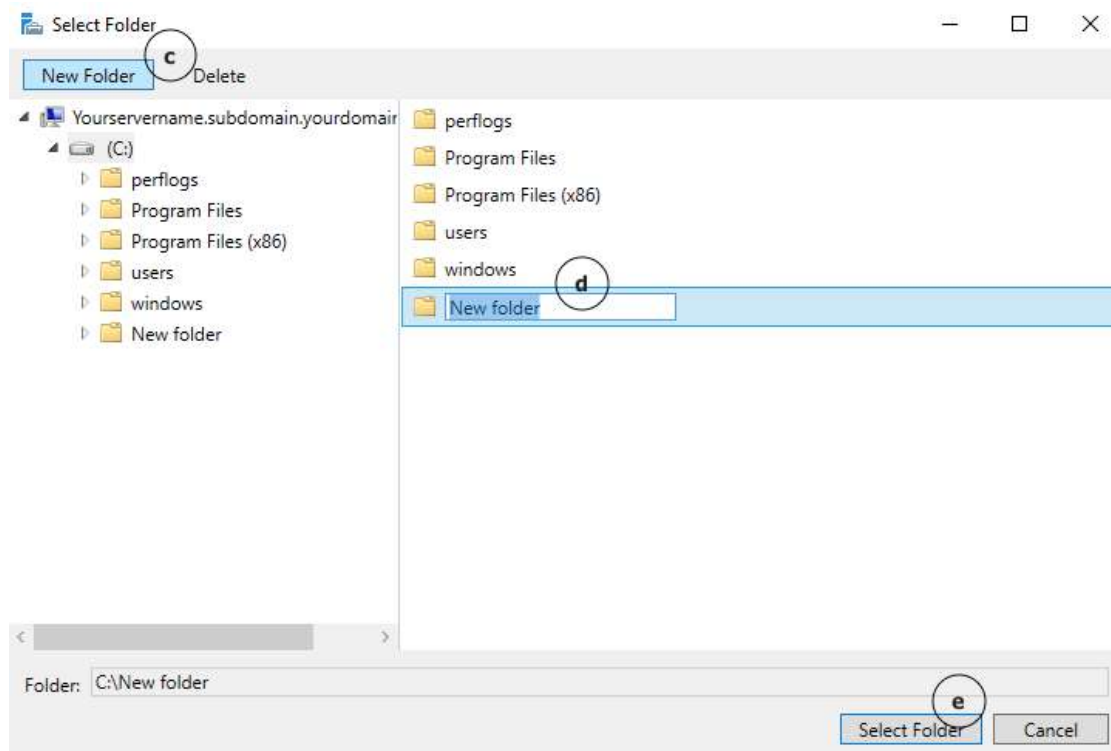
b. Select SMB Share – Quick

c. Click Next.

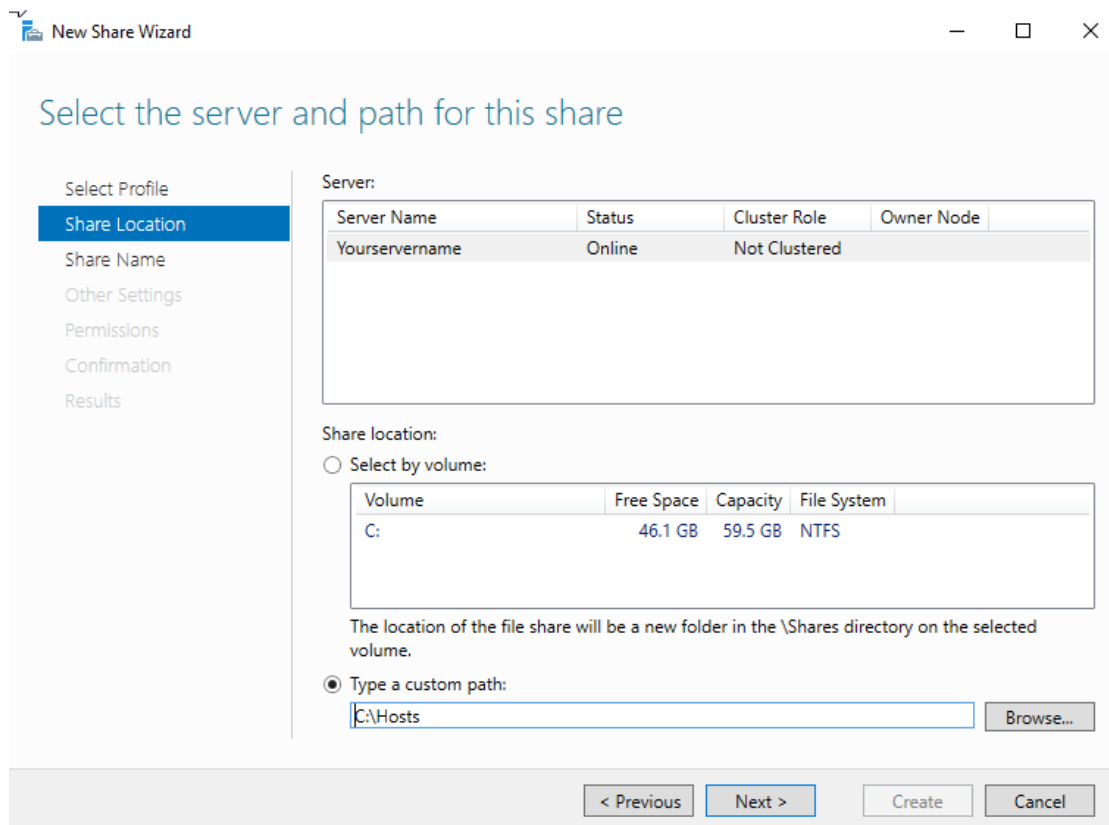


2. Share Location

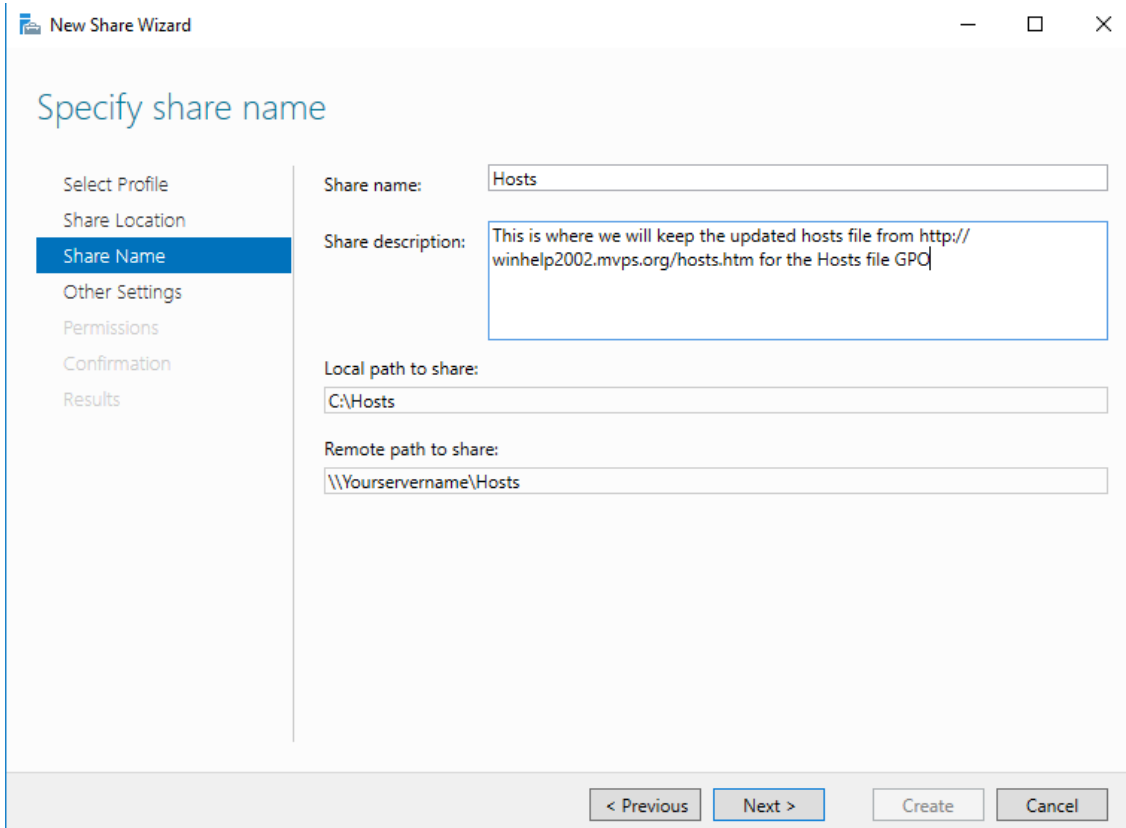
- a. Radio to Type a custom path:
- b. Click Browse...



- c. In the Select Folder window, click New Folder.
- d. Type in the New Folder name, and press Enter. In this case we used Hosts.
- e. Click Select Folder.



- f. Back at the New Share Wizard window, notice the path is now populated. Click Next >



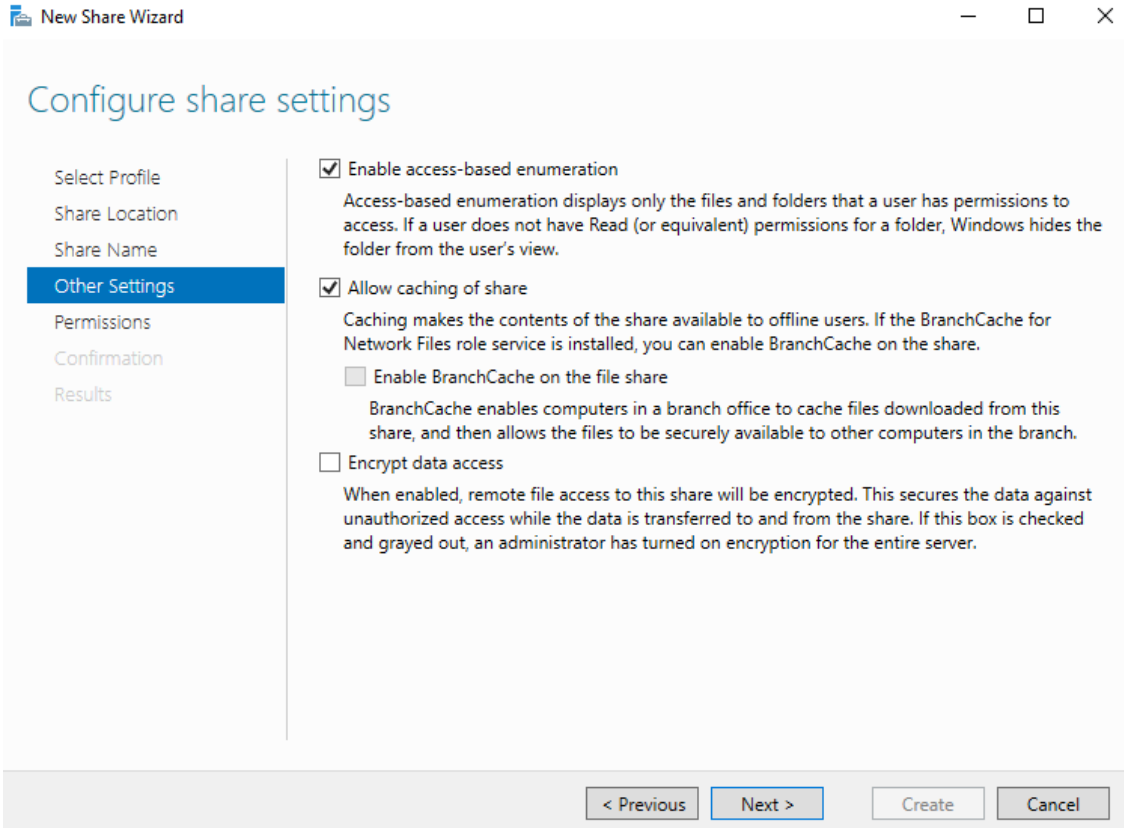
The screenshot shows the 'New Share Wizard' window with the 'Specify share name' step selected in the left-hand navigation pane. The main area contains the following fields:

- Share name:** Hosts
- Share description:** This is where we will keep the updated hosts file from <http://winhelp2002.mvps.org/hosts.htm> for the Hosts file GPC
- Local path to share:** C:\Hosts
- Remote path to share:** \\Yourservername\Hosts

At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Create', and 'Cancel'.

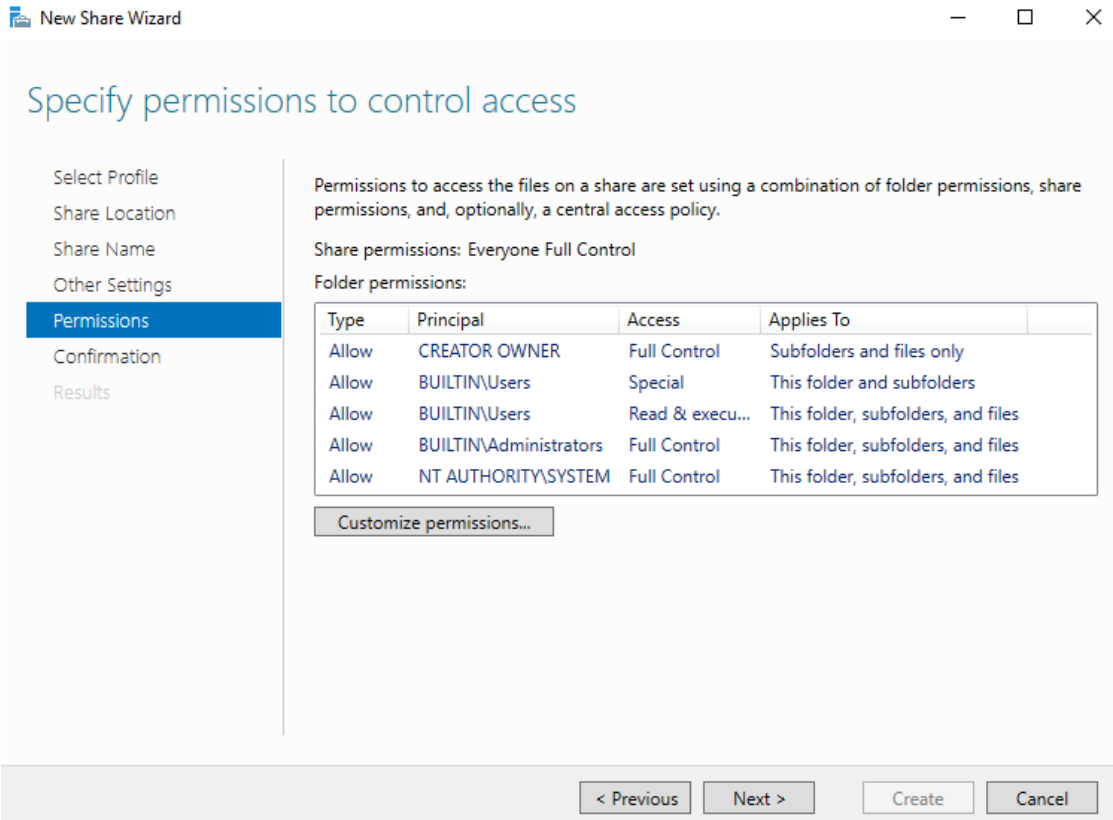
3. Share Name

- a. The Share name: auto-fills as the name of your folder designated in the previous screen, but the folder name and share name do not have to be the same. You can change it here.
- b. Type in a Share description.
- c. Local path and Remote path details are auto-filled.

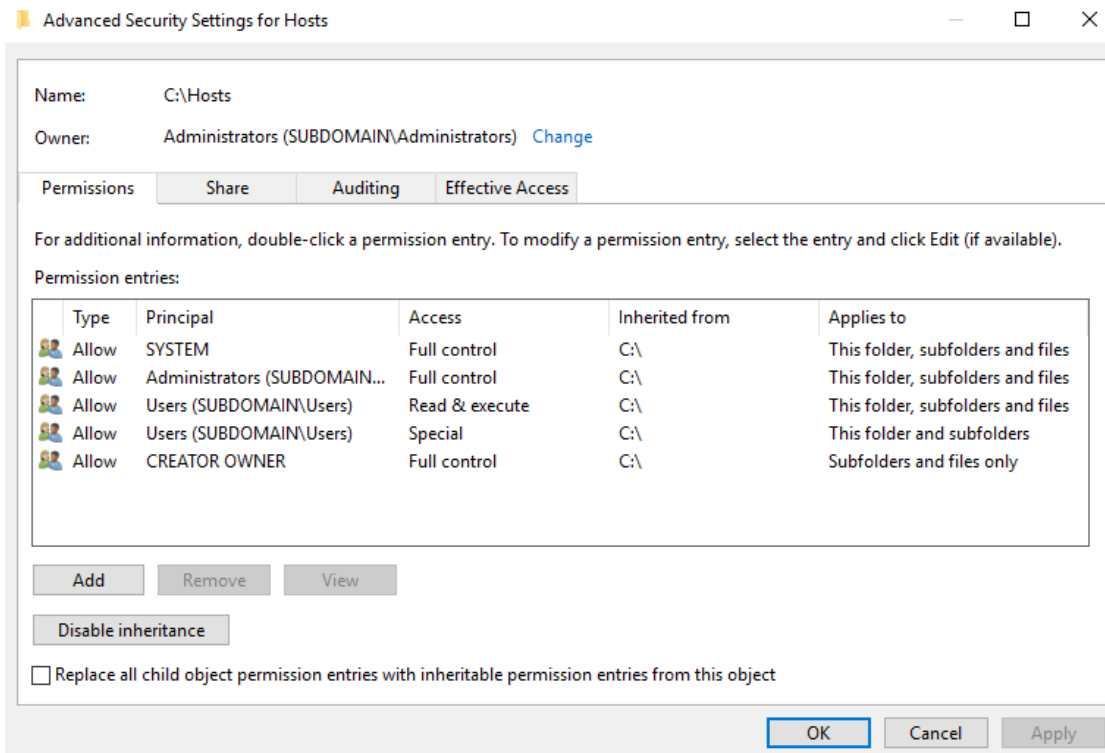


4. Other Settings

- Enable access-based enumeration displays for the user only the files and folders they have permission to. They must have at least Read permissions, otherwise the folder will be hidden from their view. Check this option.
- (Checked by Default) Allow caching of share, makes folder contents available to offline users.
- Encrypt data access encrypts remote file access. You may want to use this option for shares that contain sensitive data. In this case, we will leave this unchecked.
- Click Next >

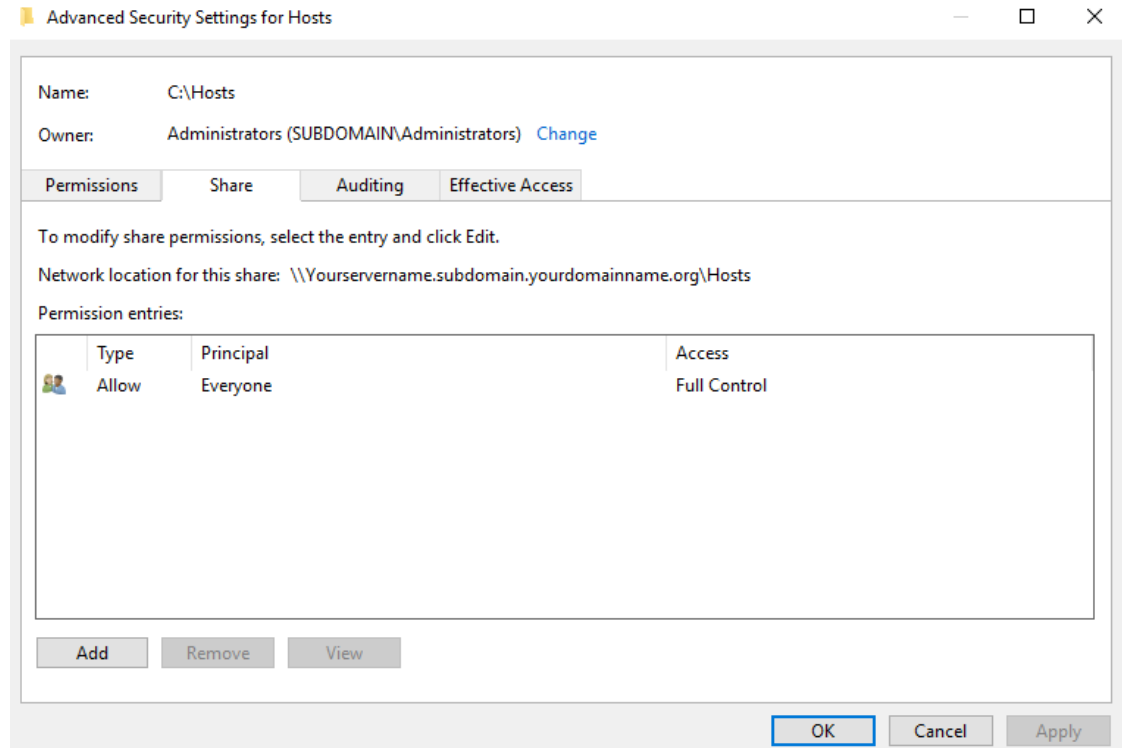


- 5. Permissions
 - a. Click Customize permissions...



b. The Advanced Security Settings dialogue has 4 tabs: Permissions, Share, Auditing & Effective Access.

i. Permissions tab – The default permissions are pictured in the image above. To change any of the options, click on the group, then click Edit. There are also options to Add or Remove.



ii. Share tab - The default setting is Type: Allow, Principal: Everyone, Access: Full Control. To change the existing option, highlight the group and click Edit. There are also options to Add or Remove.

iii. Auditing tab – This tab is not populated by default. You can add groups here, if you would like to log attempts to access or change this share. Once you have a group added, you then have the option to Remove or Edit.

Advanced Security Settings for Hosts

Name: C:\Hosts
Owner: Administrators (SUBDOMAIN\Administrators) [Change](#)

Permissions | Share | Auditing | **Effective Access**

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

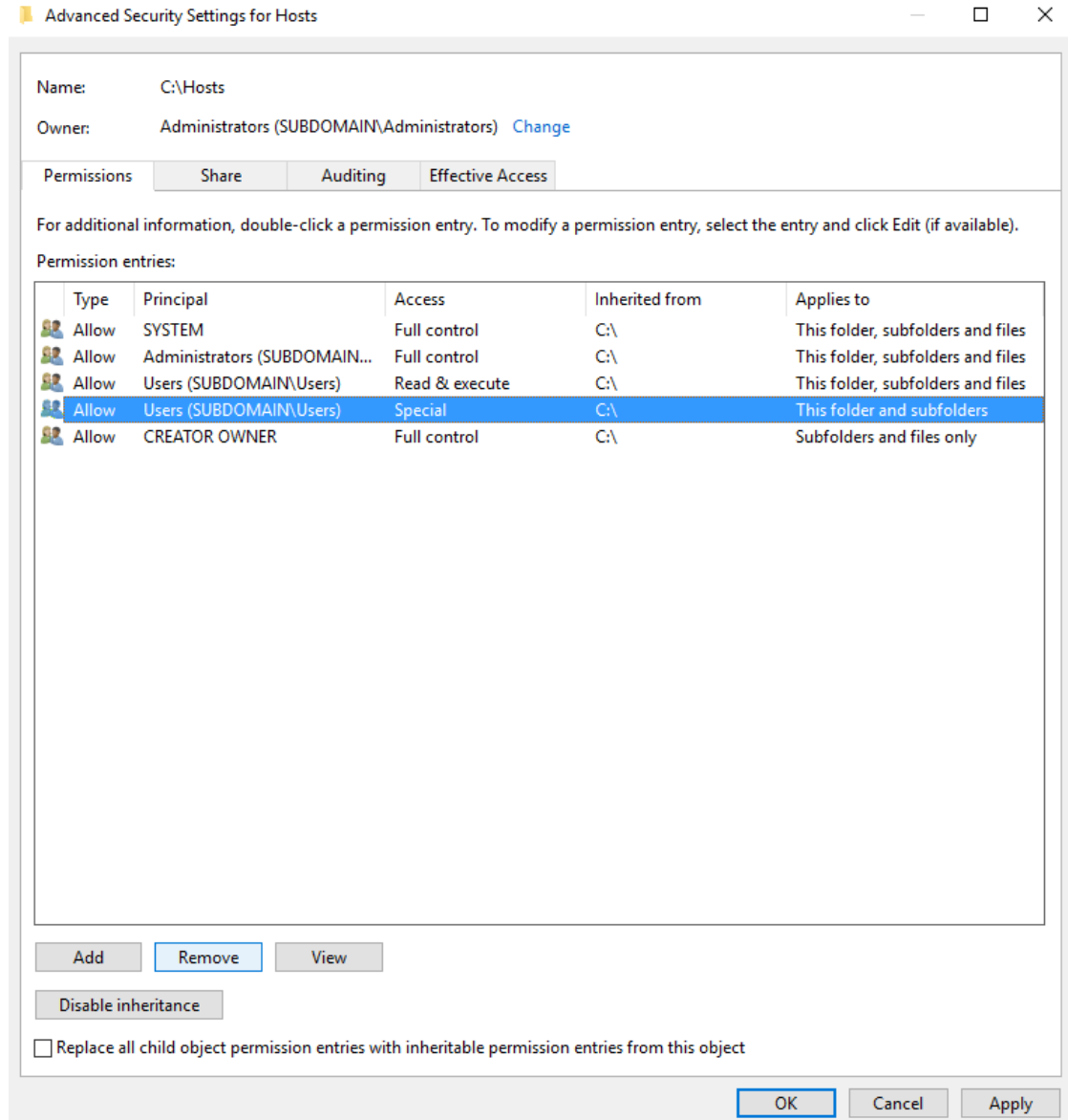
User/ Group: Users (SUBDOMAIN\Users) [Select a user](#)
 Include group membership [Click Add items](#)

Device: [Select a device](#)
 Include group membership [Click Add items](#)

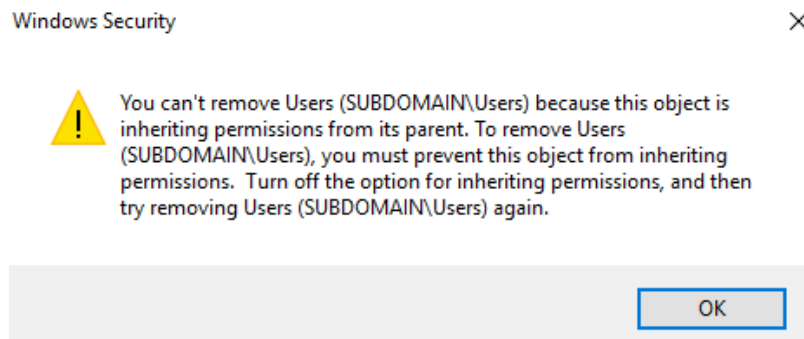
[Include a user claim](#)
[Include a device claim](#)

Effective access	Permission	Access limited by
✗	Full control	File Permissions
✓	Traverse folder / execute file	
✓	List folder / read data	
✓	Read attributes	
✓	Read extended attributes	
✓	Create files / write data	
✓	Create folders / append data	
✗	Write attributes	File Permissions
✗	Write extended attributes	File Permissions
✗	Delete subfolders and files	File Permissions
✗	Delete	File Permissions
✓	Read permissions	
✗	Change permissions	File Permissions
✗	Take ownership	File Permissions

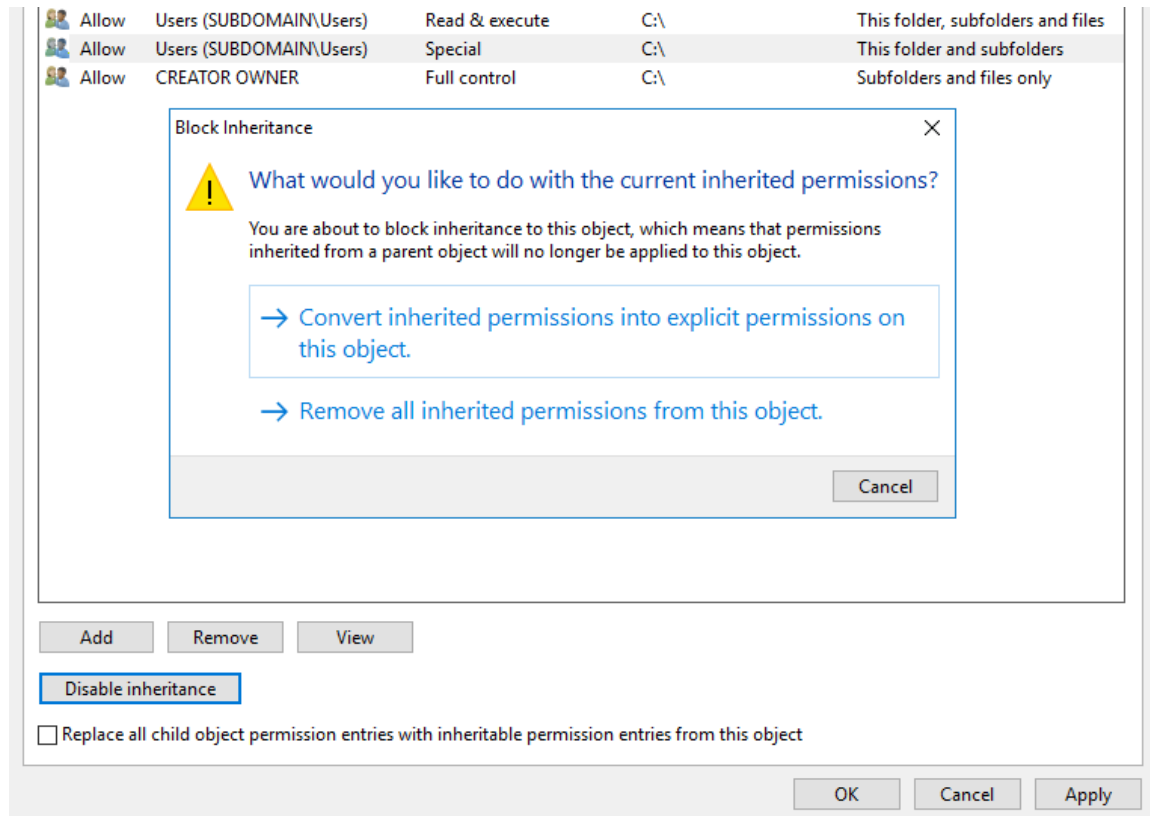
iv. Effective Access tab – Gives you the opportunity to view if a group can access the share (green checkmark), and if denied (red x) what setting is blocking access. Select a User; above we chose the Users group. Then click View effective access.



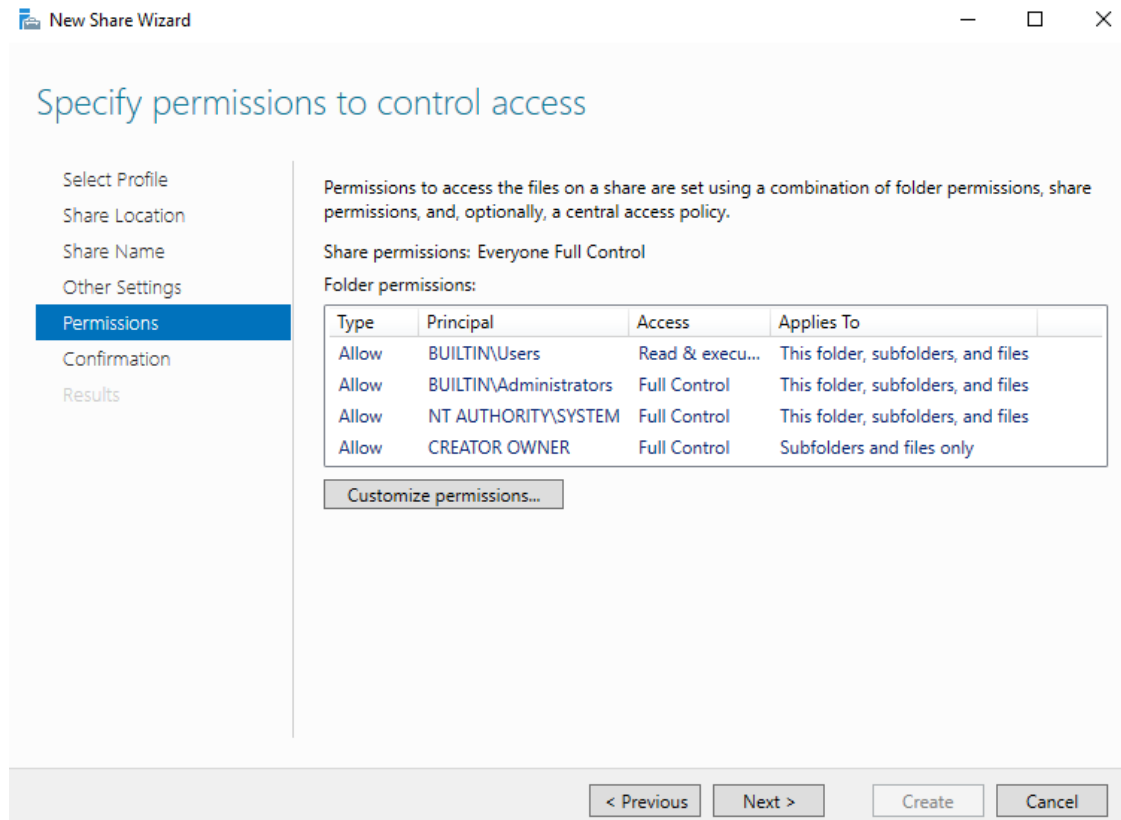
v. Back at the Permissions tab, this is the list of the default permissions. We want to remove the Users group that has the special access, so that they cannot create files or folders in this share. Highlight the Users group and click Remove.



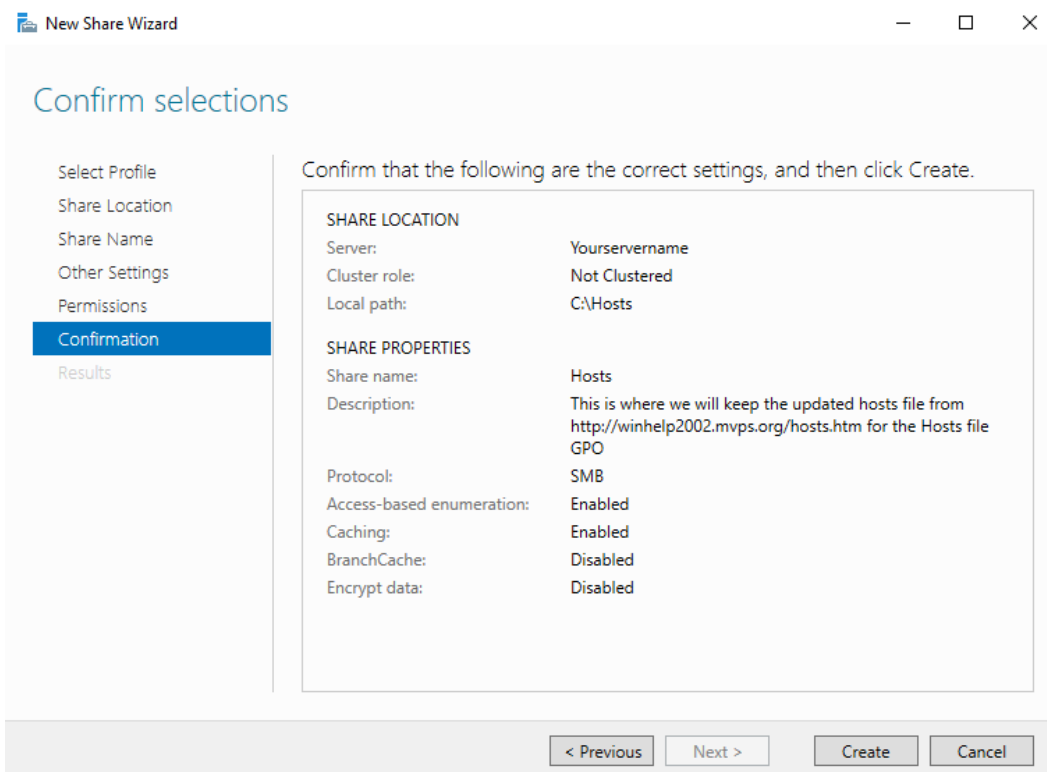
vi. You are prompted to turn off the option for inheriting permissions. Click OK.



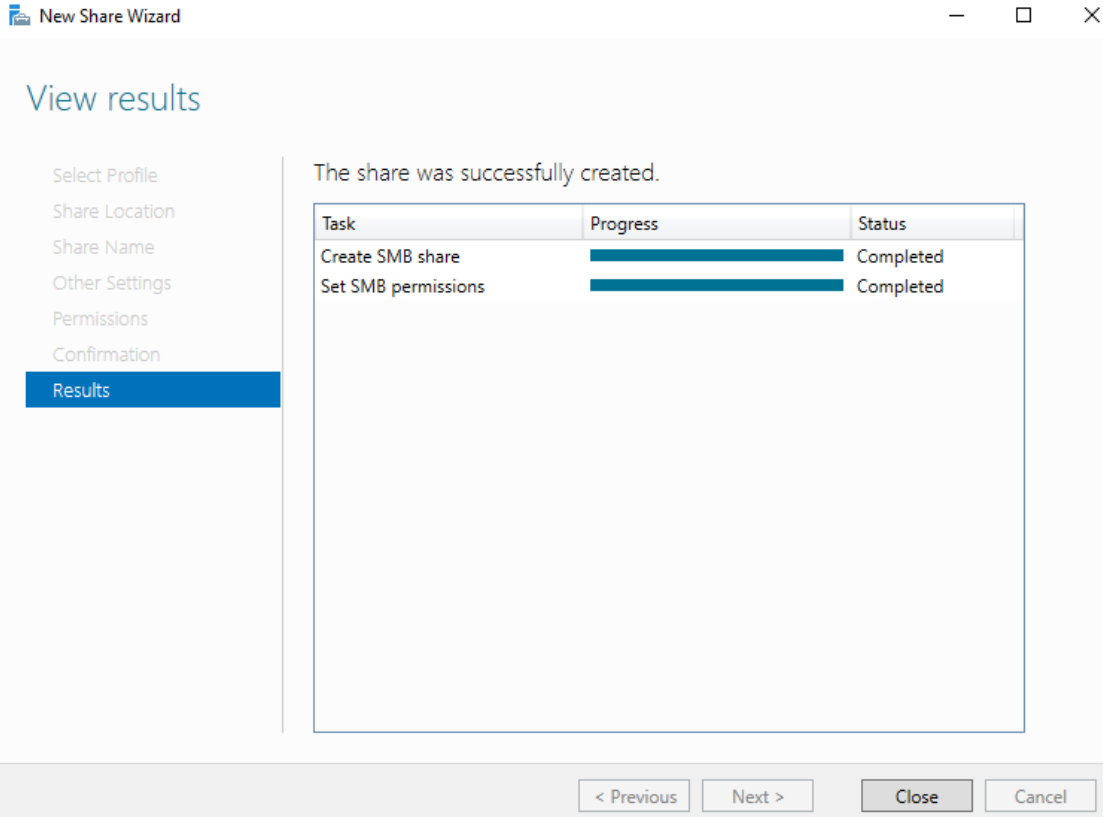
- vii. Highlight the group you want to Disable inheritance and click the button in the bottom left. In the Block Inheritance dialogue, click Convert inherited permission into explicit permissions on this object. If you click Remove all inherited permissions, all of the default groups will be removed.
- viii. After the inheritance has been adjusted, highlight the group you want to remove, and click the button in the bottom left.
- ix. Click OK.



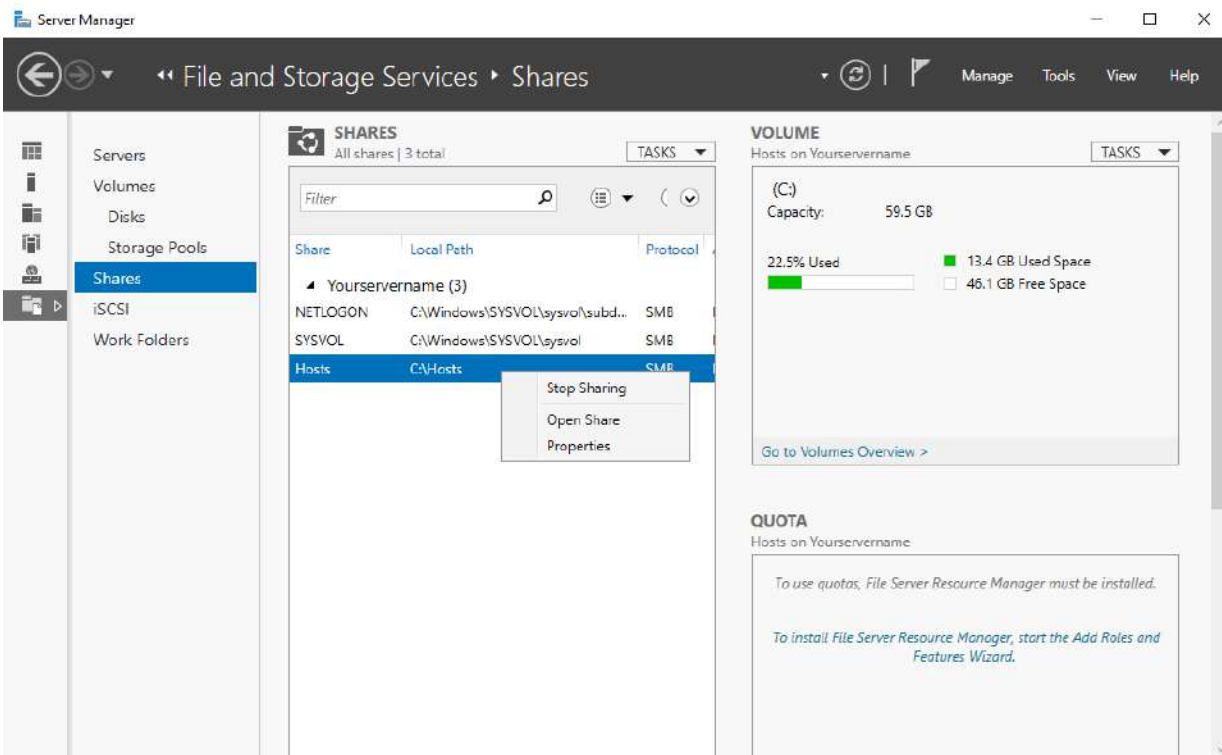
x. Back at the New Share Wizard, click Next >



6. Confirmation: Review your configuration and Click Create.

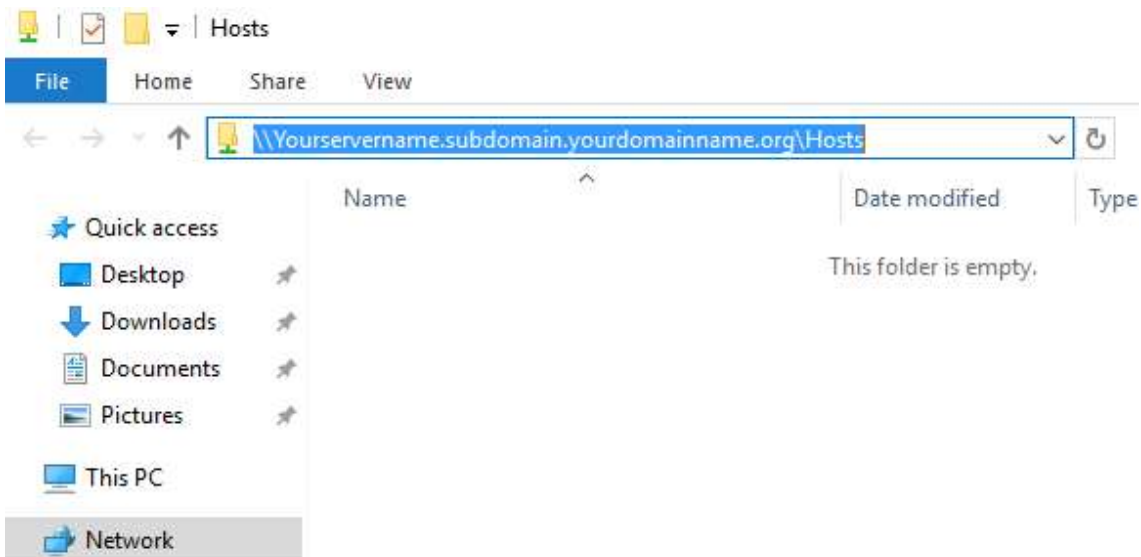


7. Results are pictured when the Share creation process is completed.



8. To edit your Share, from Server Manager click on File and Storage Services > Shares. Right-click on your share name. You have the option to:

- a. Stop Sharing, which disables sharing. It does not remove the folder.



- b. Open Share, in File Explorer.

Hosts

Show All

- General —
- Permissions —
- Settings —

General

Server Name: Yourservername

Share name: Hosts

Share description: This is where we will keep the updated hosts file from <http://winhelp2002.mvps.org/hosts.htm> for the Hosts file GPO

Folder path: C:\Hosts

Protocol: SMB

Availability type: Not Clustered

Permissions

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only

Customize permissions...

Settings

Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

OK

Cancel

Apply

c. Properties, to make changes to General, Permissions and/or Settings.

DOWNLOAD THE CURRENT MVP HOSTS FILE

1. Log into a domain computer with your Administrator credentials.
2. Open an internet browser.
3. Navigate to: <http://winhelp2002.mvps.org/hosts.htm>. Carefully read the documentation on this site to review how the Hosts file works.
4. Scroll down until you see the link, To view the Hosts file in plain text form.
 - a. Right-click on the link, and choose Save Target As...
 - b. In the Save As window type the network file share into the address bar: <\\yourservername.subdomain.yourdomainname.org\Hosts>
 - c. The filename will be hosts.txt
 - d. Click Save.

```

hosts.txt - Notepad
File Edit Format View Help
# This MVPS HOSTS file is a free download from: #
# http://winhelp2002.mvps.org/hosts.htm #
# #
# Notes: The Operating System does not read the "#" symbol #
# or anything after the # symbol on the same line #
# #
# This *must* be the first line: 127.0.0.1 localhost #
# #
#*****#
# ----- Updated: September-15-2017 ----- #
#*****#
# #
# Disclaimer: this file is free to use for personal use #
# only. Furthermore it is NOT permitted to copy any of the #
# contents or host on any other site without permission or #
# meeting the full criteria of the below license terms. #
# #
# This work is licensed under the Creative Commons #
# Attribution-NonCommercial-ShareAlike License. #
# https://creativecommons.org/licenses/by-nc-sa/4.0/ #
# #
# License info for commercial purposes contact Winhelp2002 #

127.0.0.1 localhost

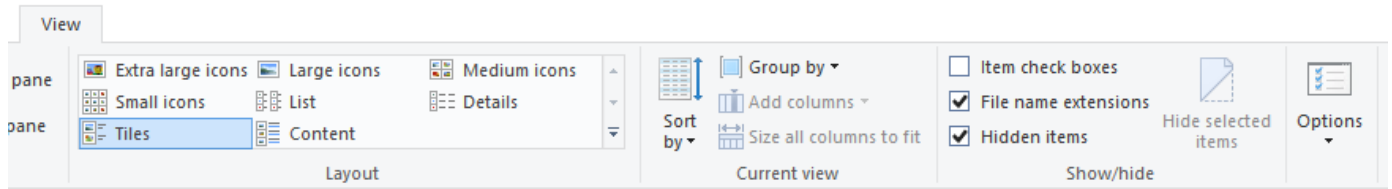
::1 localhost #[IPv6]

# My test line
192.168.5.17 mytest
#
# [Start of entries generated by MVPS HOSTS]
#
# [Misc A - Z]
0.0.0.0 fr.a2dfp.net
0.0.0.0 m.fr.a2dfp.net

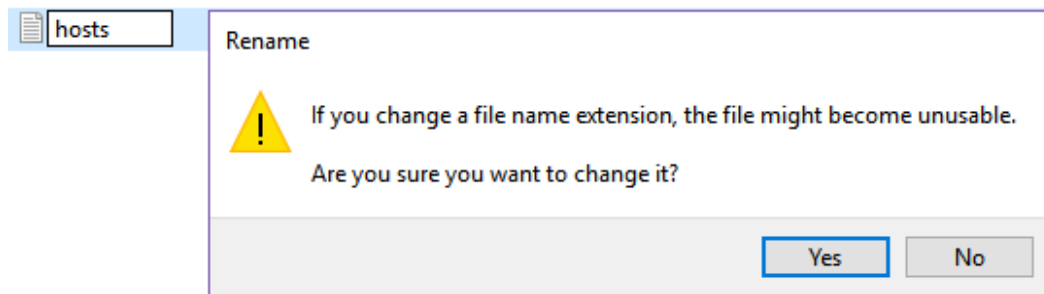
```

5. Open the hosts.txt from the network file share in Notepad.
 - a. Under the line in the text file ::1 localhost #[IPv6] type:


```
# My test line
192.168.5.17 mytest
```
 - b. Go to File > Save.



6. If you cannot see the .txt extension on the hosts.txt file, do the following:
 - a. Open File Explorer
 - b. Click on the View tab of the ribbon bar.
 - c. Above Show/hide, check the boxes for File name extensions and Hidden items.



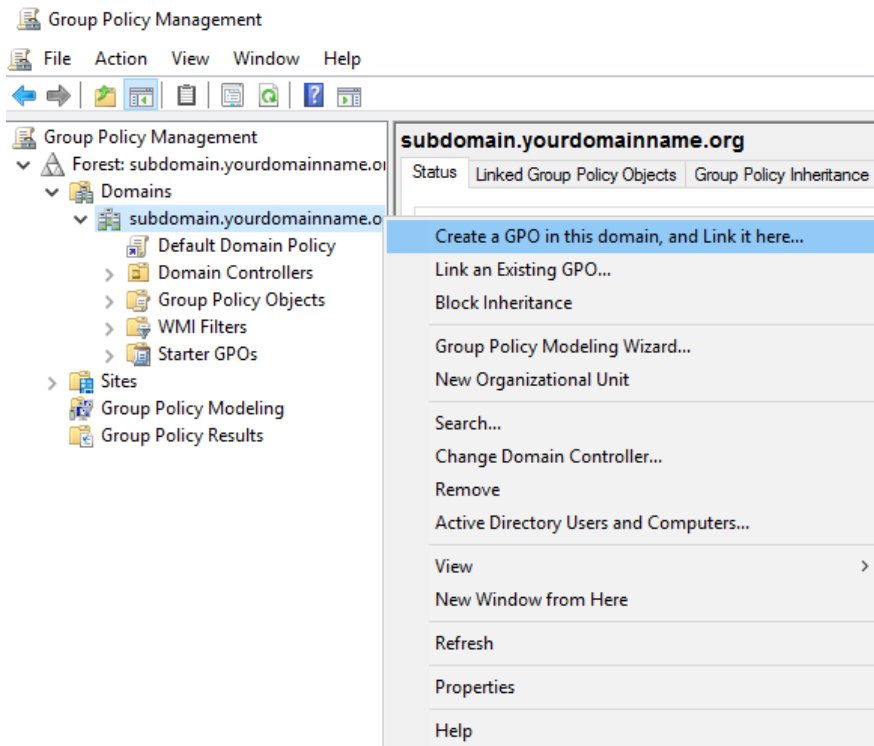
7. Go back to the hosts.txt file in the network file share.
 - a. Rename the file, removing the .txt extension.
 - b. Click Yes despite the warning.

CREATE THE GPO

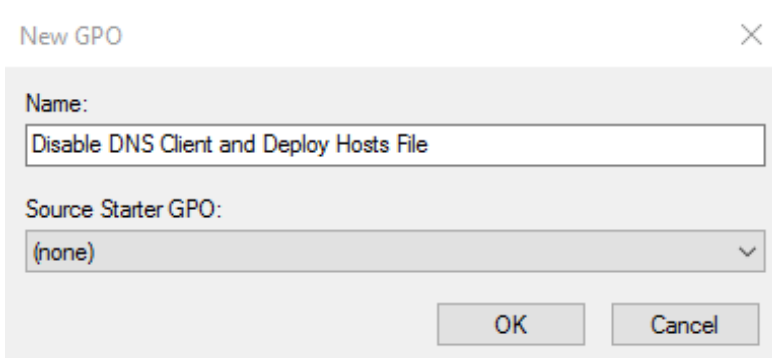
Remember that the placement of your GPO will determine which systems are affected. In this example, we are creating the GPO at the Domain level. This will affect all the systems in my domain, including the servers.

A typical Group Policy Object would be created on the specific OU that holds the computer accounts to be affected. For your own deployment, while it should not affect server performance, since internet browsing should be performed on a server, you may want to consider linking your Hosts file GPO to more specific OU's.

1. Open Group Policy Management from the Server Manager Tools Menu.



2. Right-click on your domain name and click Create a GPO in this domain, and Link it here



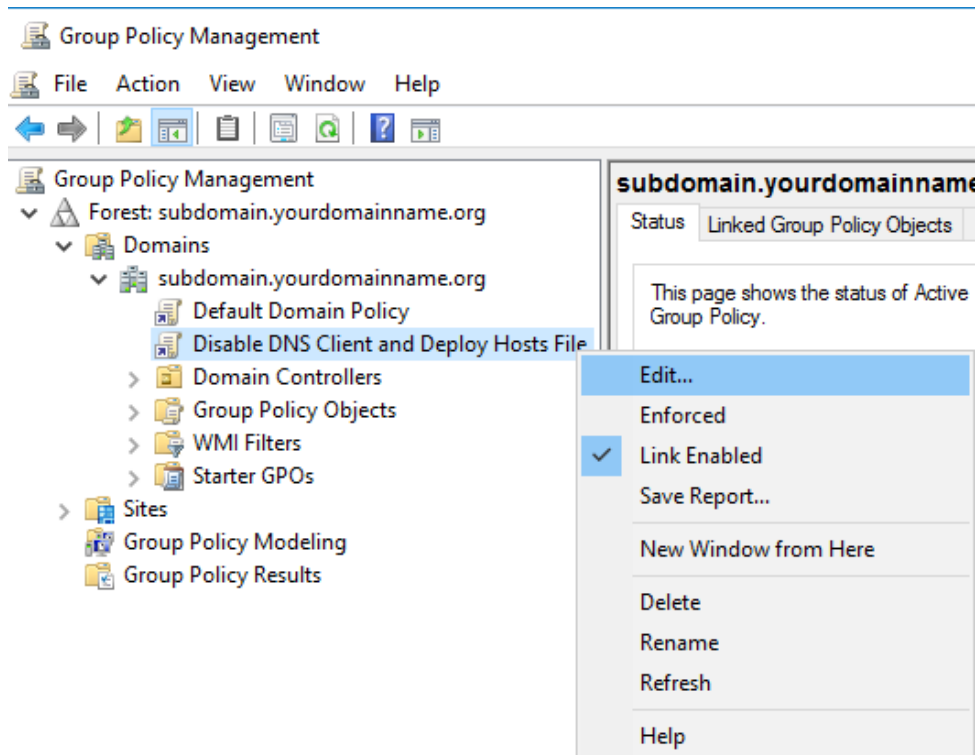
- a. Type a descriptive label in the Name: field.
- b. Click OK.

Disable the DNS Client Services

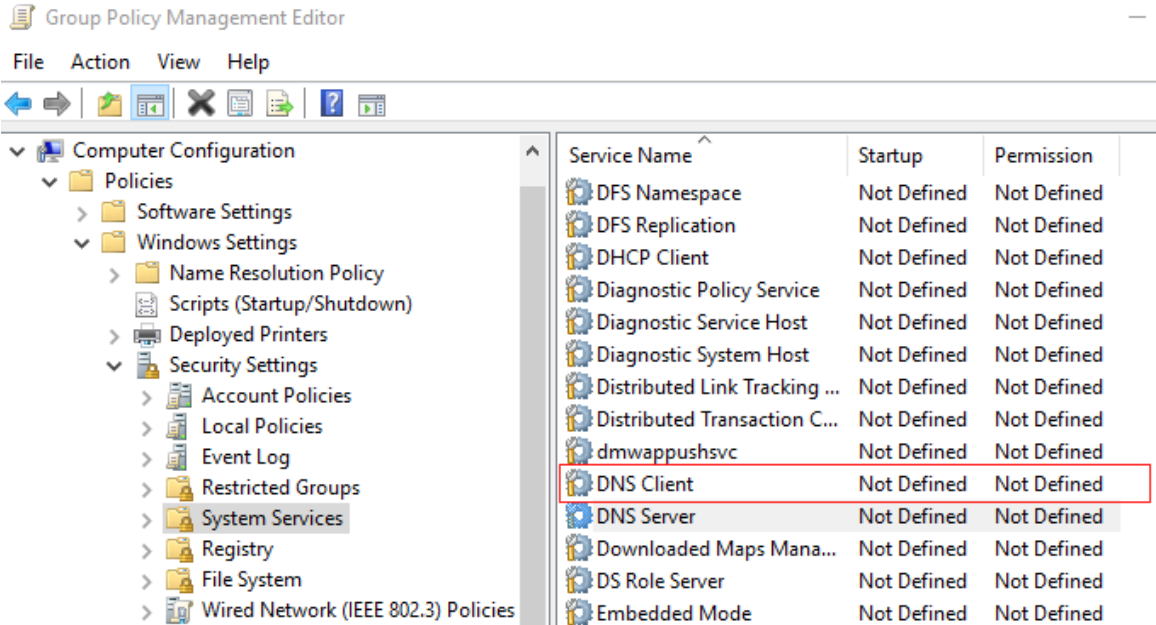
DNS has been required to establish a domain, ever since Windows XP. Therefore, the search order is DNS, Hosts, LMHosts. If the new Hosts file is deployed without making changes to the DNS Client Services, the DNS server specified in our Network card properties would always be checked first to resolve search requests, nullifying the benefits of the Hosts file. Disabling the DNS client service doesn't prevent the service entirely. It changes the search order to: Hosts, LMhosts and then DNS.

You may be concerned that using the Hosts file could slow browsing. Rest assured, clients will be able to query the Hosts file very quickly. You should see no delay in processing requests for the internet.

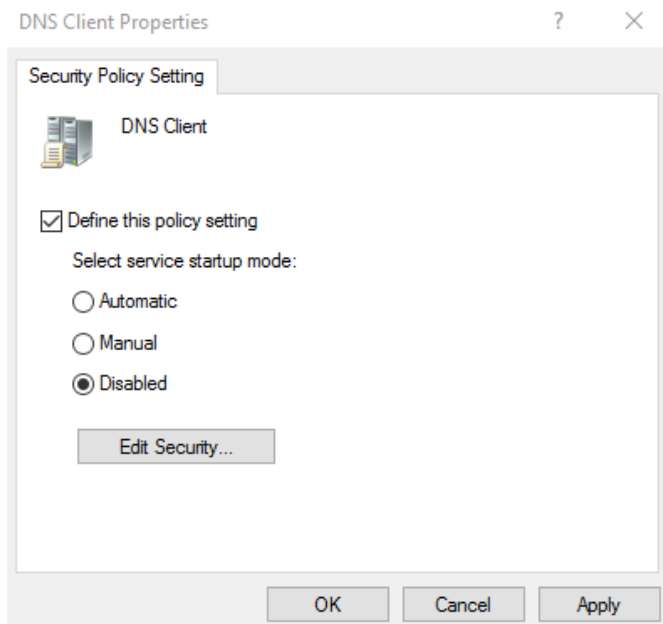
****** Older systems with limited specs, may experience a slight slowdown when processing larger host files or DNS requests.**



1. Right-click on the new GPO and click Edit...



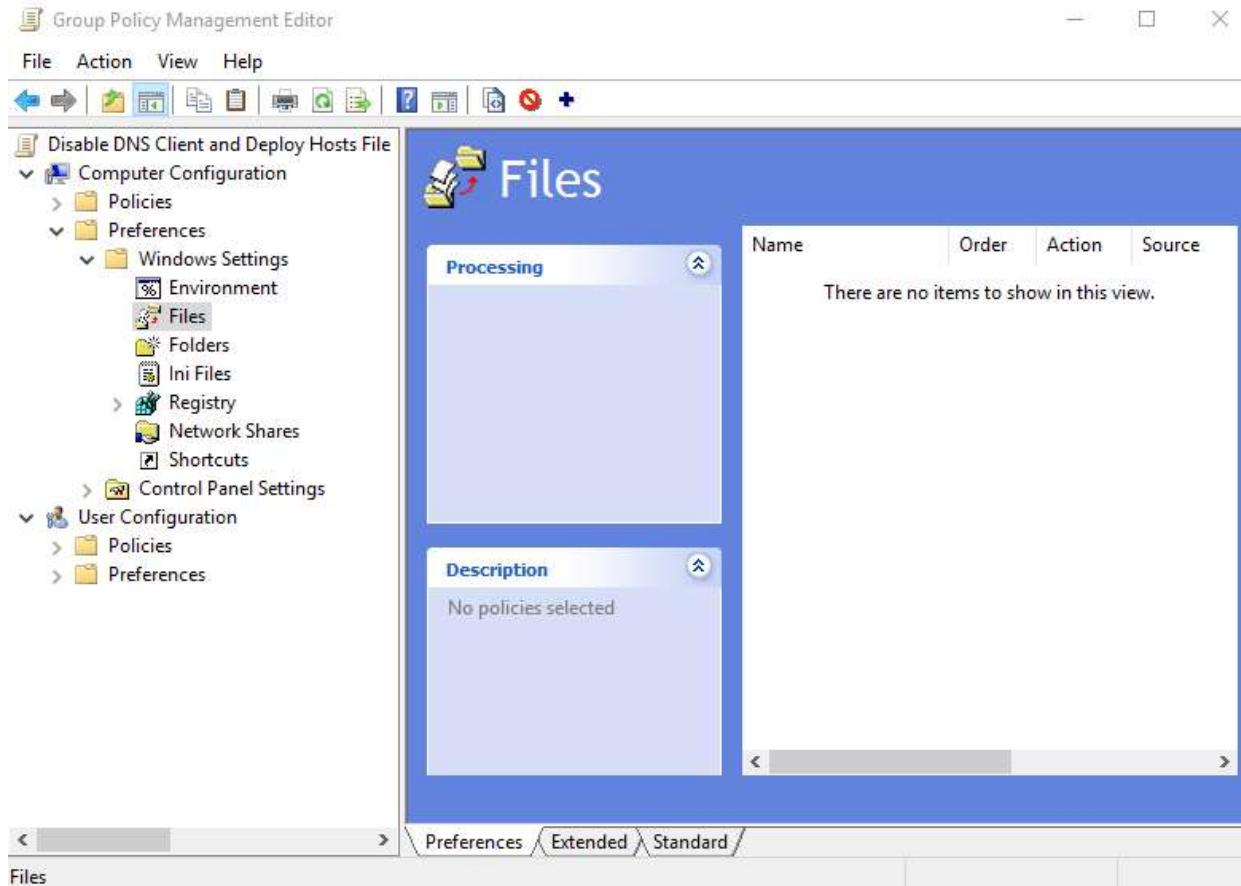
2. In the Console Tree, under Computer Configuration, click > next to Policies & Windows Settings & Security Settings, expanding each container.
3. Click on System Services
 - a. Double-click DNS Client in the right-hand pane.



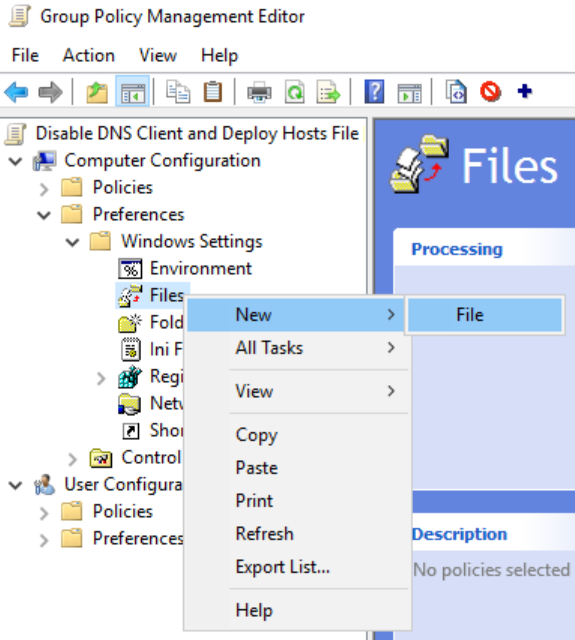
- b. Check the box to Define this policy setting
- c. Radio the Select service startup mode to Disabled
- d. Click OK

Deploy the Hosts File GPO with Group Policy Preferences

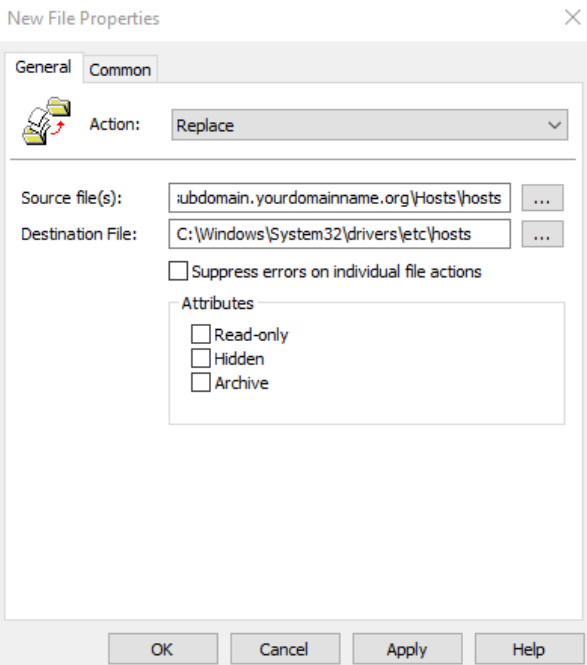
1. Open Group Policy Management from the Server Manager Tools Menu.
2. Right-click on the DNS/Hosts file GPO and click on Edit...



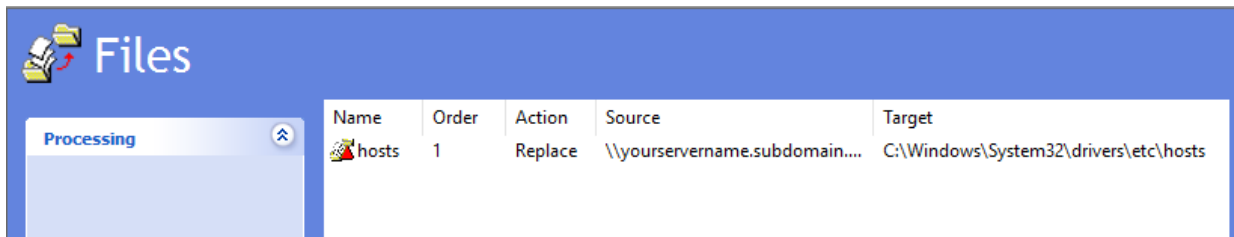
3. In the Console Tree, under Computer Configuration, click > next to Preferences & Windows Settings expanding each container.



4. Right-click Files, hover over New > and click File.



5. New File Properties, General tab:
- Action: Select Replace from the drop-down
 - Source file(s): Type in the network file share path or click ... to browse
\\yrservername.subdomain.yrdomain.org\Hosts\hosts
 - Destination File: Type the location where you want to place the file, including the filename or click ... to browse
C:\Windows\System32\drivers\etc\hosts
 - Uncheck Archive attribute
 - Click OK



6. The new configuration is now listed in the right-hand pane of the GPME.

TEST, TEST, TEST!!

Logged into a domain joined computer (in the OU you have linked this policy), open an Administrative command prompt.

Right-click on the Start Menu, select Command Prompt (Admin).

At the prompt enter, notepad c:\windows\system32\drivers\etc\hosts

When notepad launches, you should see your test entry near the top. If you do not, try to restart the computer.

At the elevated Command Prompt you could also ping the ip address from your test entry. Or use nslookup to query the ip address you added, to see what name is resolved. If the name returned is mytest, then you know the Hosts file is working.

Confirm the DNS Client Service is disabled by opening Services on a domain joined computer. If you see that the DNS Client is disabled, you know the policy was applied.

NOTE: The system does not *require* a restart for these particular settings to take effect. The new policies otherwise will be implemented with the next network refresh of Group Policy. The default is every 90 minutes + or – 30 minutes. You can specify an update rate from 0 to 64,800 minutes (45 days). If you select 0 minutes, the computer tries to update user Group Policy every 7 seconds. Configuring shorter periods of time will generate more internal network traffic. You will have to test to find the setting complements your network.

Another useful command using the Administrative Command Prompt for troubleshooting Group Policy is gprestart /r. This will list the policies applied to the machine and the order of precedence; however, it is best to confirm manually that the settings you configured were actually changed.

When finished working with the Default Domain policy, remove the user account you added when you began this section from the Domain Admins Security Group.

Section VIII: ALL Links (in the order of appearance)

Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/windows-server-2016>

System Requirements for Windows 2016 Server

<https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements>

Important Issues in Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/get-started/windows-server-2016-ga-release-notes>

Recover the Operating System or Full Server (referencing Windows Server 2008 R2)

<https://technet.microsoft.com/library/cc755163.aspx>

Wbadmin Start sysrecovery

[https://technet.microsoft.com/en-us/library/cc742118\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc742118(v=ws.11).aspx)

Windows SmartScreen

[https://technet.microsoft.com/en-us/library/jj618329\(v=ws.11\).aspx#BKMK_How](https://technet.microsoft.com/en-us/library/jj618329(v=ws.11).aspx#BKMK_How)

Server Manager

<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager>

Add Servers to Server Manager

<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/add-servers-to-server-manager>):

Microsoft Operations Management Suite

<https://www.microsoft.com/en-us/cloud-platform/operations-management-suite>.

Manager the Local Server and Server Manager Console

<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/manage-the-local-server-and-the-server-manager-console>

Server Manager Help

<https://technet.microsoft.com/library/2194da26-7e64-4497-b4ee-c2d815f655c0>

Windows Server Marketplace

<https://www.windowsservercatalog.com>

Windows Server TechCenter

<https://technet.microsoft.com/en-us/library/hh831456>

Windows 10 update history

<https://support.microsoft.com/en-us/help/4018124/windows-10-update-history>

Patching with Windows Server 2016

<https://blogs.technet.microsoft.com/mu/2017/06/27/patching-with-windows-server-2016/>

Step-by-Step Guide for Setting up a Windows Server 2016 Domain Controller

<http://www.tactig.com/install-windows-server-step-by-step/>

<http://www.tactig.com/install-active-directory-domain-services-ad-ds/>

<http://www.tactig.com/promote-windows-server-domain-controller/>

Upgrade and Conversion Options for Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/get-started/supported-upgrade-paths>

In-Place Domain Controller Upgrade from Windows Server 2012R2 to 2016

<https://www.virtualizationhowto.com/2016/11/upgrade-windows-server-2012-r2-domain-controller-to-windows-server-2016/>

What's New in Windows Server 2016 Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/whats-new-active-directory-domain-services>

Azure Active Directory Services

<https://azure.microsoft.com/en-us/services/active-directory/>

Active Directory: Best Practices for Internal Domain and Network Names

<https://social.technet.microsoft.com/wiki/contents/articles/34981.active-directory-best-practices-for-internal-domain-and-network-names.aspx>

List of Top-Level Domains

<https://www.icann.org/resources/pages/tlds-2012-02-25-en>

Domain Tools

<http://whois.domaintools.com>

ICANN-Accredited Registrars

<https://www.icann.org/registrar-reports/accredited-list.html>

AD DS Installation Wizard Page Descriptions: Deployment Configuration

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DepConfigPage

What is an RODC?

[https://technet.microsoft.com/en-us/library/cc771030\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771030(v=ws.10).aspx)

AD DS Installation Wizard Page Descriptions: Domain Controller Options

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DCOptionsPage

AD DS Installation Wizard Page Descriptions: DNS Options

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DNSOptionsPage

AD DS Installation Wizard Page Descriptions: Additional Options

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_AdditionalOptionsPage

AD DS Installation Wizard Page Descriptions: Paths

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions - BKMK_Paths

AD DS Installation Wizard Page Descriptions: Prerequisites Check

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_PrerqCheckPage

Powershell Modules for Windows 10 and Windows Server 2016

<https://technet.microsoft.com/itpro/powershell/windows/index>

Microsoft Script Center

<http://technet.microsoft.com/en-us/scriptcenter>

Server 2016 Server Manager

<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager>

Features Removed or Deprecated in Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/get-started/deprecated-features>

Guidance on Disabling System Services on Windows Server 2016 with Desktop Experience

<https://blogs.technet.microsoft.com/secguide/2017/05/29/guidance-on-disabling-system-services-on-windows-server-2016-with-desktop-experience/>

Best Practices Analyzer for Active Directory Domain Services: Configuration

[https://technet.microsoft.com/en-us/library/dd391912\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd391912(v=ws.10).aspx)

BGinfo

<https://docs.microsoft.com/en-us/sysinternals/downloads/bginfo>

Securing Built-In Administrator Accounts in Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory>

Top Support Solutions for Windows Server 2016:


<https://docs.microsoft.com/en-us/windows-server/troubleshoot/windows-server-support-solutions>

DCDiag: <http://technet.microsoft.com/en-us/library/cc731968.aspx>

ADSIEdit: [https://technet.microsoft.com/en-us/library/cc773354\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx)

DSACLs, Directory Services Access Control Lists Utility: [https://technet.microsoft.com/en-us/library/cc771151\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771151(v=ws.11).aspx)

DFSUTIL, Distributed File System Utility: <https://technet.microsoft.com/en-us/library/cc962134.aspx>

Missouri Research and Education Network  University of Missouri System

221 N. Stadium Blvd., Ste. 201  Columbia, MO 65203  P: (573) 884-7200  F: (573) 884-6673  www.MORE.net

DNSCMD, DNS Server Troubleshooting Tool: [https://technet.microsoft.com/en-us/library/dd197560\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd197560(v=ws.10).aspx)

REPADMIN, Replication Diagnostics Tool: [https://technet.microsoft.com/en-us/library/cc770963\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc770963(v=ws.11).aspx)

NETDOM, Windows Domain Manager: [https://technet.microsoft.com/en-us/library/cc772217\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc772217(v=ws.11).aspx)

Windows Sysinternals

<https://docs.microsoft.com/en-us/sysinternals/>

Project Honolulu

<https://blogs.technet.microsoft.com/servermanagement/2017/09/22/project-honolulu-technical-preview-now-available/>

Free Active Directory Tools from ManageEngine:

<https://www.manageengine.com/products/free-windows-active-directory-tools/free-active-directory-tools-index.html>

Educause Whois

<http://whois.educause.net>

MX Toolbox Network Tools

<https://mxtoolbox.com/NetworkTools.aspx>

DNSStuff

<https://www.dnsstuff.com>

Server 2016 DNS Policies Overview

<https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/dns-policies-overview>

What's New in DNS Server in Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/networking/dns/what-s-new-in-dns-server?f=255&MSPPErr=-2147217396>

Implement Domain Name System (sample chapter from Networking with Windows Server 2016)

<https://www.microsoftpressstore.com/articles/article.aspx?p=2756482>

Best Practices Analyzer for Domain Name System: Configuration (as related to Windows Server 2008 R2, Windows Server 2012)

[https://technet.microsoft.com/en-us/library/dd391879\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd391879(v=ws.10).aspx)

DNS: Installing and Configuring Servers (as related to Windows Server 2008 R2)

[https://technet.microsoft.com/en-us/library/cc755183\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc755183(v=ws.11).aspx)

Optimizing your network to keep your DNS squeaky clean

<https://blogs.technet.microsoft.com/networking/2009/02/09/optimizing-your-network-to-keep-your-dns-squeaky-clean/>

Troubleshoot DNS Problems Related to Active Directory
<https://technet.microsoft.com/en-us/library/cc526683.aspx>

MOREnet BlackHole DNS
<https://www.more.net/services/black-hole-dns>

IANA Root Servers
<https://www.iana.org/domains/root/servers>

Root-Servers.org
<http://www.root-servers.org/>

Enable DNS Diagnostic Logging
[https://technet.microsoft.com/en-us/library/dn800669\(v=ws.11\).aspx#en](https://technet.microsoft.com/en-us/library/dn800669(v=ws.11).aspx#en)

Use Built-In Tools to Monitor DNS Servers
<https://technet.microsoft.com/en-us/library/dd673658.aspx>

Monitoring and Troubleshooting DNS
<http://www.tech-faq.com/monitoring-and-troubleshooting-dns.html>

Managing a Forward Lookup Zone (as related to Windows Server 2008)
[https://technet.microsoft.com/en-us/library/cc816891\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc816891(v=ws.10).aspx)

Understanding Reverse Lookup (as related to Windows Server 2008 R2)
[https://technet.microsoft.com/en-us/library/cc730980\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc730980(v=ws.11).aspx)

NSLookup
<https://technet.microsoft.com/en-us/library/bb490950.aspx>

Understanding Forwarders (as related to Windows Server 2008 R2)
<http://technet.microsoft.com/en-us/library/cc730756.aspx>

Using Forwarders (as related to Windows Server 2008 R2)
<http://technet.microsoft.com/en-us/library/cc754931.aspx>

What should I use, a Stub, Conditional Forwarder, Forwarder, or Secondary Zone??
<https://blogs.msmvps.com/acefekay/2012/09/18/what-should-i-use-a-stub-conditional-forwarder-forwarder-or-secondary-zone/>

CIS (Center for Internet Security) Microsoft Windows Server 2012R2 Benchmark
https://www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf

Security Baseline for Windows 10 & Windows Server 2016
<https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/>

Best Practices for Securing Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

Active Directory Security Groups

[https://technet.microsoft.com/en-us/library/dn579255\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx)

LAPS (Local Administrator Password Solution)

<https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Securing Domain Controllers Against Attack

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack>

Securing Domain Controllers to Improve Active Directory Security

<https://adsecurity.org/?p=3377>

Device Health Attestation

<https://docs.microsoft.com/en-us/windows-server/security/device-health-attestation>

Reinspecting Password, Account Lockout and Audit Policies

<https://www.isaca.org/Journal/archives/2014/Volume-2/Pages/JOnline-Reinspecting-Password-Account-Lockout-and-Audit-Policies.aspx>

SANS Information Security Policy Templates

<https://www.sans.org/security-resources/policies>

Microsoft Password Guidance, downloadable .pdf

<https://www.microsoft.com/en-us/research/publication/password-guidance/>

Step-by-Step: Enabling and Using Fine-Grained Password Policies in AD

<https://blogs.technet.microsoft.com/canitpro/2013/05/29/step-by-step-enabling-and-using-fine-grained-password-policies-in-ad/>

Fine-Grained Password Policies User Interface in Windows 2012 R2 and Newer

<https://blogs.msmvps.com/acefekay/2016/10/16/fine-grained-password-policies-user-interface-in-windows-2012-r2-and-newer/>

Advanced Security Auditing FAQ

[https://technet.microsoft.com/en-us/library/dn319046\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn319046(v=ws.11).aspx)

Audit Policy Recommendations, Windows Server 2016

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

Monitoring Active Directory for Signs of Compromise

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise>

Windows 10 and Windows Server 2016 security auditing and monitoring reference

<https://www.microsoft.com/en-us/download/details.aspx?id=52630>

User Rights Assignment

[https://technet.microsoft.com/en-us/library/dn221963\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn221963(v=ws.11).aspx)

Securing Administrator Groups in Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-g--securing-administrators-groups-in-active-directory>

Security Options

[https://technet.microsoft.com/en-us/library/jj852268\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj852268(v=ws.11).aspx)

Network access: Allow anonymous DIS/name translation

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-access-allow-anonymous-sidname-translation>

Network security: Do not store LAN Manager hash value on next password change

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-do-not-store-lan-manager-hash-value-on-next-password-change>

Network security: Force logoff when logon hours expire.

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-force-logoff-when-logon-hours-expire>

Network security: LAN Manager authentication level

<https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-lan-manager-authentication-level>

Recommended Settings for Event Log Sizes in Windows

<https://support.microsoft.com/en-us/help/957662/recommended-settings-for-event-log-sizes-in-windows>

Back Up & Clear Your Event Logs with Windows Powershell

<https://technet.microsoft.com/en-us/library/2009.07.heyscriptingguy.aspx>

Event Log

<https://technet.microsoft.com/en-us/library/dd349798.aspx>

Description of Group Policy Restricted Groups

<https://support.microsoft.com/en-us/help/279301/description-of-group-policy-restricted-groups>

Restricted Groups

<https://technet.microsoft.com/en-us/library/cc957640.aspx>

Manage Local Active Directory Groups using Group Policy Restricted Groups

<https://www.petri.com/manage-local-active-directory-groups-using-group-policy-restricted-groups>

Implementing Least-Privilege Administrative Models

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>

Guidance on disabling system services on Windows Server 2016 with Desktop Experience

<https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server>

This article includes a downloadable spreadsheet of services:

<https://msdnshared.blob.core.windows.net/media/2017/05/Service-management-WS2016.xlsx>

Per-User Services in Windows 10 and Windows Server

<https://docs.microsoft.com/en-us/windows/application-management/per-user-services-in-windows>

Access Control and Authorization Overview

[https://technet.microsoft.com/en-us/library/jj134043\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj134043(v=ws.11).aspx)

Dynamic Access Control Overview

[https://technet.microsoft.com/en-us/library/dn408191\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn408191(v=ws.11).aspx)

Dynamic Access Control: Scenario Overview

<https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/dynamic-access-control--scenario-overview>

Scenario: Central Access Policy

<https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/scenario--central-access-policy>

Managing the New Wireless Network (IEEE 802.11) Policies Settings

[https://technet.microsoft.com/en-us/library/hh994701\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh994701(v=ws.11).aspx)

Blocking Unwanted Connections with a Hosts File

<http://winhelp2002.mvps.org/hosts.htm>

How to Create a File Share in Windows Server 2016

<http://www.tomsitpro.com/articles/create-file-share-windows-server-2016,1-3364.html>

Managing Permissions for Shared Folders

[https://technet.microsoft.com/en-us/library/cc753731\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc753731(v=ws.11).aspx)

Group Policy Preferences

[https://technet.microsoft.com/en-us/library/dn581922\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn581922(v=ws.11).aspx)