

# 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

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



## Contents

<u>CONTENTS</u>	<u>2</u>
INTRODUCTION	<u>4</u>
SECTION I: INSTALLING WINDOWS 2016 SERVER SOFTWARE	5
MUST-READ LINKS!	5
BEST PRACTICES	<u>5</u>
SECTION II: WINDOWS SERVER 2016 INITIALIZATION	<u>16</u>
SECTION III: WELCOME TO SERVER MANAGER	
NAVIGATING SERVER MANAGER	
Server Manager Console Header:	
The Notifications Area:	
Manage:	
Tools:	
View:	
Help:	24
MANDATORY CONFIGURATIONS	25
Set the Time Zone	
Setup the Network Card(s)	
Change the Computer Name	
Windows Update	
Enable Remote Desktop	<u>37</u>
	30
DEFINITIONS	<u>55</u> 39
<u>DELINITIONS</u>	<u>39</u> 39
INSTALLING ACTIVE DIRECTORY DOMAIN SERVICES	
The Wizard	<u>40</u> .41
PROMOTING YOUR SERVER TO A DOMAIN CONTROLLER	
Naming Considerations for Your Domain	
The Wizard	<u>48</u>
SECTION V: CUSTOMIZING YOUR DOMAIN CONTROLLER	
MUST-READ LINKS!	57
ADMINISTRATOR ACCOUNTS	57
Create a New Administrator Account	
Add Your New Administrator Account to the Built-In Administrators Security Group	
Secure the Built-in Administrator Account	
ADDRESSING ERRORS	65
Troubleshooting Tools	
DNS SERVER CONFIGURATION	
Definitions	
Must-Read Links!	
Navigating DNS Server Properties	
Interfaces Tab	
Forwarders Tab	<u>75</u>
Advanced Tab	<u>76</u>

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



Root Hints Tab	<u>77</u>
Debug Logging Tab	<u>78</u>
Event Logging Tab	<u>78</u>
Monitoring Tab	<u>79</u>
<u>Security Tab</u>	<u>79</u>
<u>Navigating Forward Lookup Zones</u>	
<u>General Tab</u>	<u>81</u>
<u>Start of Authority Tab</u>	
Name Servers Tab	
WINS Tab	
Zone Transfers Tab.	<u>85</u> 05
Creating Reverse Lookun Zones	
The Wizard	
Creating Conditional Forwarders	
SECTION VI: SECURITY POLICIES FOR WINDOWS SERVER 2016	<u>93</u>
	<u>93</u>
	<u>95</u>
PASSWORD POLICIES	<u>97</u>
	<u>104</u>
USER RIGHTS ASSIGNMENT.	<u>109</u>
SECURITY OPTIONS	
EVENT LUG POLICIES	<u>116</u>
<u>RESTRICTED GROUPS</u>	<u>118</u>
Create a New Security Group to Manage Workstations & Member Servers	
Add Administrative Users to the New Security Group	
<u>Create Your Local Administrator Group Policy</u>	
<u>SYSTEM SERVICES</u>	
System Services Example Configuration	
REGISTRY POLICIES	<u>132</u>
FILE SYSTEM PERMISSIONS	<u>138</u>
WIRELESS NETWORK POLICIES	<u>139</u>
SECTION VII: HOSTS EILE GPO	140
MUST READ LINKS!	<u>140</u>
CREATE A SHARE	<u></u> 141
The Wizard	<u>142</u>
DOWNLOAD THE CURRENT MVP HOSTS FILE	
CREATE THE GPO	
Disable the DNS Client Services	<u>159</u> 159
Deploy the Hosts File GPO with Group Policy Preferences	
TEST. TEST. TEST!!	163
<u>· · , · · , · · ·</u>	<u></u>

Missouri Research and Education Network 🎾 University of Missouri System



## 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!



**Back to Contents** 

5

## 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

🖆 Windows Setup	
Windows Server• 2016	
Languag <u>e</u> to install: <mark>English (United States)</mark>	
<u>Lime and currency format:</u> English (United States)	•
Enter your language and other preferences and click "Next" to continue.	
© 2016 Microsoft Corporation. All rights reserved.	<u>N</u> ext

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

3. Click Next.



receive a message

7

🛍 Windows Setup	
Windows Server* 2016	Setup is starting
Install now	a. You will receive a mee "Setup is starting".
Papair your computer	
<u>R</u> epair your computer	

4. Click Install now.

Choose an option	Advanced options
Reset your PC or see advanced options	System Image Recovery Recover Windows using a specific system image file
Turn off your PC	C:\ C:\ C:\ C:\

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 Wbadmin Start sysrecovery, https://technet.microsoft.com/enus/library/cc742118(v=ws.11).aspx

Missouri Research and Education Network 🎾 University of Missouri System 221 N. Stadium Blvd., Ste. 201 X Columbia, MO 65203 P: (573) 884-7200 F: (573) 884-6673 X www.MORE.net



Operating system	Architecture	Date modified
Windows Server 2016 Standard	хб4	11/21/2016
Windows Server 2016 Standard (Desktop Experience)	хб4	11/21/2016
Windows Server 2016 Datacenter	хб4	11/21/2016
Windows Server 2016 Datacenter (Desktop Experience	) x64	11/21/2016
'his option is useful when a GUI is required—for exam pplication that cannot be run on a Server Core installa	ple, to provide backward ation. All server roles and t	compatibility for an features are
upported. For more details see "Windows Server Insta	llation Options."	

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.





🔏 Windows Setup	
Applicable notices and license terms	
Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. Yo may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.	u
EULAID:T1S_SR_1_ED_SRVSTD_V_en-us	
accent the license terms	
	levt
	ext

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.





- 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



1.0.00010		Total size	Free space	Туре
🧼 Drive 0 Una	allocated Space	60.0 GB	60.0 GB	

#### 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

ad driver	_
To install the device driver driver files, and then click C	for your drive, insert the installation media containing the DK.
Note: The installation medi	ia can be a CD_DVD_or USB flash drive.

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.

Missouri Research and Education Network 🎾 University of Missouri System



4	Windows Setup	X
Ir	nstalling Windows	
St	tatus	
	Copying Windows files Getting files ready for installation (0%) Installing features Installing updates Finishing up	



13. Installing Windows.



Windows needs to res	start to continue		
Restarting in 7 seconds			

14. Windows restarts to complete installation.





Customize	settings		
Type a password for the	built-in administrator account that you can u	se to sign in to this computer.	
User name	Administrator		
Password			
Reenter password			
Ġ			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: <u>https://www.microsoft.com/en-us/research/wp-</u> 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.



Back to Contents

## 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.

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 16



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

Allowed apps		_		
- → · ↑ 🝻 « Windows Firewall > Allowed apps 🛛 🗸 さ	Search C	ontrol Par	nel	
Allow apps to communicate through Windows Firewall To add, change, or remove allowed apps and ports, click Change settings. What are the risks of allowing an app to communicate?		Ch	ange setti	ings
Allowed apps and features:				
Name		Private	Public	^
Key Management Service				
I mDNS		✓	~	
Netlogon Service				
Vetwork Discovery			>	
Performance Logs and Alerts				
Remote Desktop				
Remote Event Log Management				
□ Remote Event Monitor				
Remote Scheduled Tasks Management				
Remote Service Management				
□ Remote Shutdown				
Remote Volume Management				~
	Deta	ils	Remove	2
		Allow an	other app	)
		ОК	Cano	el

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.



nced	I sharing settings - 🗆
¥	↑ • < < Network and Sharing Center > Advanced sharing settings v 🕑 Search Control Panel
	Change sharing options for different network profiles
	Windows creates a separate network profile for each network you use. You can choose specific options for each profile.
	Private (current profile)
	Network discovery
	When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.
	<ul> <li>Turn on network discovery</li> <li>Turn on automatic setup of network connected devices.</li> <li>Turn off network discovery</li> </ul>
	File and printer sharing
	When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.
	<ul> <li>Turn on file and printer sharing</li> <li>Turn off file and printer sharing</li> </ul>
	Guest or Public
	All Networks 🚫
	Save changes Cancel
u c i.	click No, or miss the dialogue, this option is reconfigurable. Go to Control Panel > Network and Sharing Center, Click Change advance

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.

a. Windows SmartScreen is disabled by default, and is enabled using a domain administrator account through Group Policy.

b. 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.

c. Telemetry is used to report additional information about the site.

d. 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.

Activate Windows Go to Settings to activate Windows.

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



**Back to Contents** 



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

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
- o Workgroup/Domain
- Windows Firewall
- Remote Access Option
- o Configure Windows Updates
- o Set the time/time zone
- o See operating system and hardware details
- o View Events

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



- Access Services
- o Run the Best Practices Analyzer
- View Performance details
- o 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 <a href="https://docs.microsoft.com/en-us/windows-server/administration/server-manager/add-servers-to-server-manager">https://docs.microsoft.com/en-us/windows-server/administration/server-manager/add-servers-to-server-manager</a>):

- 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, <a href="https://www.microsoft.com/en-us/cloud-platform/operations-management-suite">https://www.microsoft.com/en-us/cloud-platform/operations-management-suite</a>.

#### 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.

Missouri Research and Education Network 》 University of Missouri System



	- 🗇 I 🌠
	Post-deployment Configura TASKS V
	Configuration required for DHCP Server at BATMAN
	Complete DHCP configuration
0	Feature installation
	Installation succeeded on Batman.JLA.local.
	Add Roles and Features
	Task Details

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:





#### Tools:

#### Default Available Tools:

Manage Tools View Help	
Component Services	
Computer Management	
Defragment and Optimize Drives	
Disk Cleanup	
Event Viewer	
iSCSI Initiator	
Local Security Policy	
Microsoft Azure Services	
ODBC Data Sources (32-bit)	
ODBC Data Sources (64-bit)	
Performance Monitor	
Print Management	
Resource Monitor	
Services	
System Configuration	
System Information	
Task Scheduler	
Windows Firewall with Advanced Security	
Windows Memory Diagnostic	
Windows PowerShell	
Windows PowerShell (x86)	
Windows PowerShell ISE	
Windows PowerShell ISE (x86)	
Windows Server Backup	

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



iew:				
	Manag	je Tools	View	Help
		75%		
	~	100%		Ctrl+0
		125%		
	-	150%		
		Zoom In		Ctrl +
		Zoom Out		Ctrl -
		Hide Welcon	ne Tile	

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,

<u>https://technet.microsoft.com/library/2194da26-7e64-4497-b4ee-c2d815f655c0</u>. Windows Server Marketplace takes you here, <u>https://www.windowsservercatalog.com</u>. Windows Server TechCenter launches this, <u>https://technet.microsoft.com/en-us/library/hh831456</u>.



#### MANDATORY CONFIGURATIONS

#### Set the Time Zone

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

For WIN-BC0IFUT09VU		TASKS	
WIN-BC0IFUT09VU	Last installed updates	Never	
WORKGROUP	Windows Update	Download updates only, using Windows Upda	te
	Last checked for updates	Never	
Private: On	Windows Defender	Real-Time Protection: On	
Enabled	Feedback & Diagnostics	Settings	
Disabled	IE Enhanced Security Configuration	On	
Disabled	Time zone 🔶 🦳 <	(UTC-08:00) Pacific Time (US & Canada)	
IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00377-60000-00000-AA934 (activated)	
Microsoft Windows Server 2016 Standard	Processors	Intel(R) Core(TM) i7-37200M CPU @ 2.60GHz	
VMware Inc. VMware Virtual Platform	Installed memory (RAM)	2 GB	
0	Total disk space	536.43 GB	
			r

2. Click the hyperlink across from Time zone.

🖀 Date and Ti	me	×	3. CI
Date and Time	Additional Clocks Internet Time Date: Saturday, August 5, 2017 Time: 1:18:07 AM Central Time (US & Canada)		
Daylight Sa clock is set	ving Time ends on Sunday, November 5, 2017 at 2:00 AM. The to go back 1 hour at that time.	No co	

3. Click Change time zone...

Missouri Research and Education Network 🎾 University of Missouri System



📸 Time Zone Settings			×
Set the time zone:			
Time zone:			
(UTC-06:00) Central Time	e (US & Canada)		~
Automatically adjust c	lock for Daylight S	aving Time	
Current date and time:	Saturday, Augu	st 5, 2017, 1:24 /	AM
		ОК	Cancel

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

🖁 Date and Time	>
Date and Time Additional Clocks Internet Time	
Additional clocks can display the time in other time zones. You can vie them by clicking on or hovering over the taskbar clock.	2W
Show this clock	
Select time zone:	
(UTC-08:00) Pacific Time (US & Canada)	$\sim$
Pacific	
Show this clock	
Select time zone:	
(UTC-06:00) Central Time (US & Canada)	$\sim$
Enter display name:	
Clock 2	
OK Cancel	Apply

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



💣 Date and Ti	me			$\times$
Date and Time	Additional Clocks	Internet Time		
This comput 'time.window	ter is set to autom ws.com'.	atically synchr	onize with	
Next synchro	onization: 8/5/201	7 at 1:34 AM		
An error occ time.windov	urred while Windo vs.com.	ows was synch	ronizing with	
			Change	settings
		OK	Cancel	Apply

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

a. Click Change settings.

internet Time Settings		2
Configure Internet time settings:		
Synchronize with an Internet time se	erver	
Server: time-nist-gov	~	Update now
The clock was successfully synchronize 4/27/2017 at 3:25 PM.	d with time.wine	dows.com on
The clock was successfully synchronize 4/27/2017 at 3:25 PM.	d with time.wind	lows.com on

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.

For WIN-BC0IFUT09VU			TASKS 💌
Computer name	WIN-BCOIFUT09VU	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates
5 1		Last checked for updates	Never
Windows Firewall	Private: On	Windows Defender	Real-Time Protection
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific
Ethernet0 +	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00377-60000-0000
Operating system version	Microsoft Windows Server 2016 Standard	Processors	Intel(R) Core(TM) i7
Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	2 GB
		Total disk space	536.43 GB
<			>

2. Click the hyperlink across from Ethernet0.



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



#### Ethernet0 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.

Internet Protocol Version 4 (TCP/IPv4) Properties

ou can get IP settings assigned au his capability. Otherwise, you need or the appropriate IP settings.	tomatically if your network supports I to ask your network administrator
O Obtain an IP address automati	cally
• Use the following IP address:	
IP address:	10 . 10 . 10 . 250
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 10 . 10 . 1
Obtain DNS server address au	tomatically
Use the following DNS server a	ddresses:
Preferred DNS server:	10 . 10 . 10 . 250
Alternate DNS server:	10 . 10 . 10 . 251
Validate settings upon exit	Advanced

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.

29

Missouri Research and Education Network 🎾 University of Missouri System



10.10.10.250  Thetwork			
Intel(R) 82574L Gigabit Network C Intel(R) 82574L Gigabit Net		Disable 🔺	
		Status Diagnose	
		Bridge Connections	
		Create Shortcut	
	0	Delete	
	9	Rename	
	0	Properties	

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.

PROPERTIES For WIN-BC0IFUT09VU			TASKS 🔻
Computer name 🔶 < Workgroup	WIN-BCOIFUT09VU WORKGROUP	Last installed updates Windows Update Last checked for updates	Never Download updates Never
Windows Firewall Remote management Remote Desktop NIC Teaming Ethernet0	Private: On Enabled Disabled Disabled IPv4 address assigned by DHCP, IPv6 enabled	Windows Defender Feedback & Diagnostics IE Enhanced Security Configuration Time zone Product ID	Real-Time Protectic Settings On (UTC-08:00) Pacific 00377-60000-0000
Operating system version Hardware information	Microsoft Windows Server 2016 Standard VMware, Inc. VMware Virtual Platform	Processors Installed memory (RAM) Total disk space	Intel(R) Core(TM) i7 2 GB 536.43 GB
<			>

2. Click the hyperlink across from Computer name.



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



You can change the name and the members computer. Changes might affect access to n	ship of this etwork resource
Computer name:	
Yourservemame	
Full computer name: Yourservemame Member of	More
O Domain:	
Workgroup	
WORKGROUP	
	-

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

Compu	iter Name/Domain Changes
1	You must restart your computer to apply these changes
	Before restarting, save any open files and close all programs.
	ОК
5. Yo 6. Clo	u must restart your computer to apply these changes. Click OK ose the System Properties window.
Micros	oft Windows X
You r chan	must restart your computer to apply these ges
Before	restarting, save any open files and close all programs.
	Restart Now Restart Later
7. Cli 8. Se	ck Restart Now. rver will reboot.



#### Windows Update

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

WIN-BCOIFUT09VU	Last installed updates	Never	
WORKGROUP	Windows Update 🔶 🤇	Download updates only, using Windows U	
	Last checked for updates	Never	
Private: On	Windows Defender	Real-Time Protection: On	
Enabled	Feedback & Diagnostics	Settings	
Disabled	IE Enhanced Security Configuration	On	
Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)	
IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00377-60000-00000-AA934 (activated)	
Microsoft Windows Server 2016 Standard	Processors	Intel(R) Core(TM) i7-3720QM CPU @ 2.60GHz	
VMware, Inc. VMware Virtual Platform	Installed memory (RAM)	2 GB	
	Total disk space	536.43 GB	

2. Scroll right to Windows Update.

a. 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.

b. Another option for accessing Windows Update is to left click on the Start Menu and click Settings > Update & Security



**MORE**ne<sup>®</sup>

- Learn more
- 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,

Check for updates

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:

← Settings

– 🗆 🗙

## Opdate history

Uninstall updates

**Recovery options** 

#### Update history

2017-09 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4038782)

Successfully installed on 9/12/2017

Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - September 2017 (KB890830)

Successfully installed on 9/12/2017

2017-08 Update for Windows Server 2016 for x64-based Systems (KB4035631)

Successfully installed on 9/11/2017

2017-08 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4034658)

Successfully installed on 9/11/2017

Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - August 2017 (KB890830)

Successfully installed on 9/11/2017

#### 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.



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


#### Enable Remote Desktop

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

PROPERTIES For WIN-BC0IFUT09VU			TASKS 💌
Computer name Workgroup	WIN-BCOIFUT09VU WORKGROUP	Last installed updates Windows Update Last checked for updates	Never Download updates Never
Windows Firewall Remote management Remote Desktop ← NIC Teaming Ethernet0	Private: On Enabled Disabled Disabled IPv4 address assigned by DHCP, IPv6 enabled	Windows Defender Feedback & Diagnostics IE Enhanced Security Configuration Time zone Product ID	Real-Time Protectic Settings On (UTC-08:00) Pacific 00377-60000-0000
Operating system version Hardware information	Microsoft Windows Server 2016 Standard VMware, Inc. VMware Virtual Platform	Processors Installed memory (RAM) Total disk space	Intel(R) Core(TM) i7 2 GB 536.43 GB
<			>

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

System Properties	$\times$
Computer Name Hardware Advanced Remote	
Remote Assistance	
Allow Remote Assistance connections to this computer	
Advanced	
Remote Desktop	
Choose an option, and then specify who can connect.	
O Don't allow remote connections to this computer	
Allow remote connections to this computer	
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)	
Help me choose Select Users	
OK Cancel Appl	у

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.

ΥT		~ 0	Sear	ch Contro	ol Panel
	To add, change, or remove allowed apps and ports, click Change settings.				
	What are the risks of allowing an app to communicate?		Ch	ange sett	ings
	Allowed apps and features:				
	Name		Private	Public	^
	File and Printer Sharing over SMBDirect				
	iSCSI Service				
	Key Management Service				
	✓ mDNS				
	Netlogon Service				
	Network Discovery				
	Performance Logs and Alerts				
$\leq$	Remote Desktop			V	>
	Remote Event Log Management				
	Remote Event Monitor				
	Remote Scheduled Tasks Management				
	Remote Service Management				~
		Detail	s	Remov	e
			Allow an	other ap	D

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

OK

Cancel

38



**Back to Contents** 

39

# Section IV: Building a Domain Controller

#### DEFINITIONS

<u>Roles</u> - 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.

<u>Role Services</u> – 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.

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

<u>Functions</u> - 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.

<u>AD DS</u> – 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.

<u>Functional Level</u> – 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 <u>http://www.tactig.com/install-windows-server-step-by-step/</u> <u>http://www.tactig.com/install-active-directory-domain-services-ad-ds/</u> <u>http://www.tactig.com/promote-windows-server-domain-controller/</u>

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

What's New in Windows Server 2016 Active Directory https://docs.microsoft.com/en-us/windows-server/identity/whats-new-active-directory-domain-services

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



## 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.

Missouri Research and Education Network 阶 University of Missouri System



#### The Wizard 📥 Add Roles and Features Wizard $\times$ DESTINATION SERVER Select installation type Yourservername Select the installation type. You can install roles and features on a running physical computer or virtual Before You Begin machine, or on an offline virtual hard disk (VHD). Installation Type Role-based or feature-based installation Server Selection Configure a single server by adding roles, role services, and features. O Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment. R 2. Select installation type a. Choose Role-Based or Feature-based installation. b. Click Next. DESTINATION SERVER Select destination server Yourservername Select a server or a virtual hard disk on which to install roles and features. Before You Begin Installation Type Select a server from the server pool O Select a virtual hard disk Server Selection Server Roles Server Pool Features Filter: Name IP Address Operating System Microsoft Windows Server 2016 Standard Yourservernan 192.168.250.13.. 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.

Missouri Research and Education Network 泌 University of Missouri System



 $\times$ 

📥 Add Roles and Features Wizard

#### DESTINATION SERVER Select server roles Yourservername Select one or more roles to install on the selected server. Before You Begin Installation Type Roles Description Server Selection Active Directory Domain Services Active Directory Certificate Services (AD DS) stores information about Server Roles Active Directory Domain Services objects on the network and makes Active Directory Federation Services Features this information available to users Active Directory Lightweight Directory Services and network administrators. AD DS AD DS Active Directory Rights Management Services uses domain controllers to give Device Health Attestation Confirmation network users access to permitted DHCP Server resources anywhere on the network DNS Server through a single logon process. Fax Server File and Storage Services (1 of 12 installed) Host Guardian Service Hyper-V MultiPoint Services Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services < Previous Next > Install Cancel 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.

```
📥 Add Roles and Features Wizard
```

#### Add features that are required for Active Directory **Domain Services?**

You cannot install Active Directory Domain Services unless the following role services or features are also installed.



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.

42

Missouri Research and Education Network 🎾 University of Missouri System



×

#### 📥 Add Roles and Features Wizard

Select features

Before You Begin Installation Type

Server Selection

Server Roles

# DESTINATION SERVER Yourservername Select one or more features to install on the selected server. Features Description .NET Framework 3.5 Features > > NET Framework 4.6 Features (2 of 7 installed) > Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock

Features appealing user interfaces, protect AD DS your customers' personal identity BranchCache Confirmation information, enable seamless and Client for NFS secure communication, and provide Containers the ability to model a range of Data Center Bridging business processes. Direct Play Enhanced Storage Failover Clustering Group Policy Management I/O Quality of Service IIS Hostable Web Core Internet Printing Client IP Address Manage
 iSNS Server service IP Address Management (IPAM) Server LPR Port Monitor < Previous Next > Install Cancel

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.



#### DESTINATION SERVER Active Directory Domain Services Yourservername Active Directory Domain Services (AD DS) stores information about users, computers, and other devices Before You Begin on the network. AD DS helps administrators securely manage this information and facilitates resource Installation Type sharing and collaboration between users. Server Selection Things to note: Server Roles To help ensure that users can still log on to the network in the case of a server outage, install a Features 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 AD DS installed, you will be prompted to install the DNS Server role on this machine. Confirmation 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 logons 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: <u>https://azure.microsoft.com/en-us/services/active-directory/</u>

e. Click Next.



Add Koles and Features Wizard		DESTINA		/FR
Confirm installatio	on selections	You	irserverna	me
🔥 Do you need to specify an	alternate source path? One or more installation selections are missing source files on	the destin	ati	×
Before You Begin	To install the following roles, role services, or features on selected server, click Ins	tall.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this page	because th	ey have	
Server Roles	been selected automatically. If you do not want to install these optional features, their check boxes.	click Previo	ous to cle	ear
Features				_
AD DS	.NET Framework 3.5 Features			^
Confirmation	.NET Framework 3.5 (includes .NET 2.0 and 3.0)			
Results	Active Directory Domain Services			
	Group Policy Management			
	Remote Server Administration Tools			
	Kole Administration Tools			
	Active Directory module for Windows PowerShell			
	AD DS Tools			
	Autor Discussion Advision data discussion			$\sim$
	Export configuration settings			
	Specify an alternate source path			
	< Previous Next > Ins	tall	Cance	1

#### 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.



	View installation progress
Installation Tune	
Server Roles	Installation started on Yourservername
Features	.NET Framework 3.5 Features
AD DS	.NET Framework 3.5 (includes .NET 2.0 and 3.0)
	Active Directory Domain Services
Results	Group Policy Management
nesuns	Remote Server Administration Tools
	Role Administration Tools
	AD DS and AD LDS Tools
	Active Directory module for Windows PowerShell
	AD DS Tools
	Active Directory Administrative Center
	AD DS Snap-Ins and Command-Line Tools
	You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings
	< Previous Next > Close Cancel

DESTINATION SERVER Yourservername	allation progress
	ore You Begin
	allation Type
d. Installation succeeded on Yourservername.	
Services	tures
uired to make this machine a domain controller.	DS
a domain controller	firmation
ures (includes .NET 2.0 and 3.0)	ults
nt	
ation Tools	
Tools	
.DS lools	
ctory module for windows Powersnell	
zard without interrupting running tasks. View task progress or open this ng Notifications in the command bar, and then Task Details. Is	
zard without interrupting running tasks. View task progress or ig Notifications in the command bar, and then Task Details. s	

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-internaldomain-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, <u>https://www.icann.org/resources/pages/tlds-2012-02-25-en</u>, 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 <u>http://whois.domaintools.com</u> 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, <u>https://www.icann.org/registrar-reports/accredited-list.html</u>.

If you do have an external domain name registered to your organization, you could either consider using a subdomain, ex. <u>subdomain</u>.yourmaindomainname.org, or register your domain name with another TLD (Top-Level Domain), ex. yourmaindomainname.<u>net</u>, or yourmaindomainname.<u>info</u>, 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.

🚖 Active Directory Domain Service	s Configuration Wizard		- 🗆 X
Deployment Conf	iguration		TARGET SERVER Yourservername
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths	Select the deployment operatio Add a domain controller to Add a new domain to an exi Add a new forest Specify the domain information	n an existing domain sting forest for this operation	
Prerequisites Check Installation Results	Root domain name:	subdomain.yourdomainna	ame.org
	More about deployment config	urations	
		< Previous Next >	Install Cancel

#### 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: <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK\_DepConfigPage</u> e. Click Next.



📥 Active Directory Domain Services Configuration Wizard	_		$\times$
Domain Controller Options	TAR( Your	GET SER serverna	VER ame
Deployment Configuration Domain Controller Options Select functional level of the new forest and root domain			
DNS Options Forest functional level: Windows Server 2016 *			
Additional Options Domain functional level: Windows Server 2016 ~			
Paths Specify domain controller capabilities			
Review Options   Domain Name System (DNS) server			
Prerequisites Check I Global Catalog (GC)			
Installation Read only domain controller (RODC)			
Results Type the Directory Services Restore Mode (DSRM) password			
Password:			
Confirm password:			
More about domain controller options			
< Previous Next > Instal		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. <u>Read only domain controller (RODC)</u>. 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-andremoval-wizard-page-descriptions#BKMK\_DCOptionsPage

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

f. Click Next.

Missouri Research and Education Network >> University of Missouri System



📥 Active Directory Domain Service	s Configuration Wizard		-	- 0	×
DNS Options				TARGET Yourserv	SERVER ername
A delegation for this DNS se	erver cannot be created because the	authoritative parent zone cannot	t be found S	how more	×
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify DNS delegation options				
	More about DNS delegation				
		< Previous Next >	Install	Ca	ncel 🛛
3. DNS Options					
DNS Options			×		
A delega authorita DNS serv you shou parent zo domain '	tion for this DNS server cann ative parent zone cannot be f yer. If you are integrating with uld manually create a delegat one to ensure reliable name r "subdomain.yourdomainnan	ot be created because the ound or it does not run Win an existing DNS infrastruc tion to this DNS server in th esolution from outside the ne.org". Otherwise, no actio	ndows ture, e on is		

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

i. Part of this process checks the network for a previously configured DNS authoritative

ii. Since this is our first server with DNS, it will be set up with the authoritative parent

ΟК

Missouri Research and Education Network 🎾 University of Missouri System

zone, and delegation cannot be created.

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

a. If you click 'Show more' within the yellow warning box, another dialogue window opens.

parent zone, and A Host records that may already exist for this server.



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.

📥 Active Directory Domain Service	es Configuration Wizard		-	-		×
Additional Option	IS			TARG Yours	ET SER	/ER ime
Deployment Configuration Domain Controller Options DNS Options Additional Options	Verify the NetBIOS name assigne The NetBIOS domain name:	ed to the domain and change it if nece SUBDOMAIN	essary			
Paths Review Options Prerequisites Check Installation Results						
	More about additional options	< Previous Next >	Install		Cancel	

## 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-andremoval-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.

Missouri Research and Education Network 泌 University of Missouri System



📥 Active Directory Domain Services	s Configuration Wizard		- 🗆 ×
Paths			TARGET SERVER Yourservername
Deployment Configuration Domain Controller Options	Specify the location of the AD DS	database, log files, and SYSVOL	
DNS Options	Database folder:	C:\Windows\NTDS	
Additional Options	Log files folder:	E:\Logfiles	
Paths	SYSVOL folder:	F:\SYSVOL	
Review Options			
Prerequisites Check			
Installation			
Results			
	More about Active Directory paths	;	
		< Previous Next >	nstall Cancel

- 5. Paths
  - a. This is the location for the Database, Logfiles and SYSVOL folders.

b. Microsoft provides a hyperlink to learn More about Active Directory paths: <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions - BKMK\_Paths</u>.

- c. Best Practice is to designate separate drives for these files.
- d. You can browse to the location you would like to use, or type the path.
- e. Click Next.



	×
TARGET SE Yourserver	RVER name
view your selections:	
onfigure this server as the first Active Directory domain controller in a new forest.	^
he new domain name is "subdomain.yourdomainname.org". This is also the name of the new	, I
orest.	
he NetBIOS name of the domain: SUBDOMAIN	
orest Functional Level: Windows Server 2016	
omain Functional Level: Windows Server 2016	
dditional Options:	
Global catalog: Yes	
DNS Server: Yes	~
ese settings can be exported to a Windows PowerShell script to automate Iditional installations View scrip	ot
	View your selections: onfigure this server as the first Active Directory domain controller in a new forest. The new domain name is "subdomain.yourdomainname.org". This is also the name of the new rest. The NetBIOS name of the domain: SUBDOMAIN orest Functional Level: Windows Server 2016 omain Functional Level: Windows Server 2016 dditional Options: Global catalog: Yes DNS Server: Yes ese settings can be exported to a Windows PowerShell script to automate iditional installations

#### 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.

Missouri Research and Education Network 🎾 University of Missouri System



Deployment Configuration Domain Controller Options	Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
DNS Options Additional Options Paths Review Options Prerequisites Check Installation	Verifying prerequisites for domain controller operation  View results

## 7. Prerequisites Check

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



📥 Active Directory Domain Services Configuration Wizard

TARGET SERVER

Yourservername

55

# Prerequisites Check

All prerequisite checks pass	ed successfully. Click 'Install' to begin installation. Show more	×
Deployment Configuration	Prerequisites need to be validated before Active Directory Domain Services is installed on this	
Domain Controller Options	computer	
DNS Options	Rerun prerequisites check	
Additional Options		
Paths	View results	
Review Options	Windows Server 2016 domain controllers have a default for the security setting named     "Allow server are a setting and the security with the security setting named	^
Prerequisites Check	cryptography algorithms when establishing security channel sessions.	
Installation		
Results	For more information about this setting, see Knowledge Base article 942564 (http:// go.microsoft.com/fwlink/?Linkld=104751).	
	▲ 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.	~
	If you click Install, the server automatically reboots at the end of the promotion operation.  More about prerequisites	~

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-nameyou-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.



📥 Active Directory Domain Services Configuration Wizard

- 🗆 🛛

# Installation

TARGET SERVER Yourservername

56

Domain Controller Options	Starting
DNS Options	View detailed operation results
Additional Options	Windows Server 2016 domain controllers have a default for the security setting named     "Allow server to prove the security level by the security setting named
Paths	cryptography algorithms when establishing security channel sessions.
Review Options	For more information about this setting, see Knowledge Pase article 0/256/ (http://
Prerequisites Check	go.microsoft.com/fwlink/?Linkld=104751).
Installation	
Results	
	More about installation options

8. Installation

a. The System will install Active Directory and DNS.

b. When completed, the System will RESTART.

You're about to be signed out	
The computer is being restarted because Active Directory Domain Services was removed.	installed or
	Close

c. Click Close.

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



**Back to Contents** 

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

Best Practices Analyzer for Active Directory Domain Services: Configuration 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.





Active Directory Users and Com	Name	Type De	scription	
Saved Queries     Subdomain.yourdomainnan     Builtin     Computers     Domain Controllers     ForeignSecurityPrincipal:     Managed Service Accour     Users	Administrator Administrator Carl Allowed RODC Password Repli Cert Publishers Coneable Domain Controllers DefaultAccount Denied RODC Password Replic DnsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Enterprise Admins Enterprise Key Admins Enterprise Read-only Domain Group Policy Creator Cymers	type         De           User         Bu           Security Group         M           Administrator Prope         Remote control           General         Address           Member Of         Member of:           Name         Administratore           Domain Admins         Bornain Users           Enterprise Administratore         Schema Admins           Group Policy Cre         Schema Administratore	Active Directory Domain S subdomain yourdomainnai subdomain yourdomainnai subdomain yourdomainnai subdomain yourdomainnai subdomain yourdomainnai subdomain yourdomainnai subdomain yourdomainnai subdomain yourdomainnai	7 > icee Profile COM+ Telephones Drganization ment Sessions iervices Folder me.org/Users me.org/Users me.org/Users me.org/Users me.org/Users me.org/Users
2	置 Guest 器 Key Admins 器 Protected Users 線 RAS and IAS Servers 題 Read-only Domain Controllers 義 Schema Admins	Add Primary group: Set Primary Group	Remove Domain Users There is no need to ch you have Macintosh c	ange Primary group unless ients or POSIX-compliant

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.

Active Directory File Action View	Users and Comp / Help	uters			
in the second se	K 🗈   🗙 🖻	ا 😖	? 🖬 🕈	s 🐮 👕 🖉 🖻	<b>B</b>
Active Directory Active Directory Saved Querie Subdomain.y Builtin Compute Domain C ForeignSe Managed Users	Users and Com s ourdomainnan rs Controllers ecurityPrincipal: Service Accour Delegate Contro Find	Name	Account RODC Pa nins lateProxy Admins Comput Controll Guests Users se Admins	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account m Members in this DNS Administrat DNS clients who Designated admi All workstations a All domain contr All domain users Designated admi
	New All Tasks	>	Comp	puter	
	Aii Tasks View	>	Group	9 2	
	Refresh		msDS	rgPerson -KevCredential	
	Export List		msDS	-ResourceProperty	List
	Properties		msDS	-ShadowPrincipalC	Container
	Help		mslm	aging-PSPs	
<	>	🕒 vərnici	MSM	Q Queue Alias	
Creates a new item in	this container.		User Share	er od Folder	

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



New Object - User	$\times$	New Object - User
Create in: subdomain.yourdomainname.org/Users		Create in: subdomain.yourdomainname.org/Users
First name: Jane Initials:		Password:
Last name: Citizen		Confirm password:
Full name: Jane Citizen		User must change password at next logon
User logon name:		User cannot change password
jancit @subdomain.yourdomainname.c ∨		Password never expires
User logon name (pre-Windows 2000):		Account is disabled
SUBDOMAIN\ jancit		
< Back Next > Cancel	ł	< Back Next > Cancel

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.

New Object - User	×
Create in: subdomain.yourdomainname.org/Users	
When you click Finish, the following object will be created:	
Full name: Jane Citizen	~
User logon name: jancit@subdomain.yourdomainname.org	
The user cannot change the password. The password never expires.	
	~
< Back Finish C	ancel

- 8. Review the summary.
- 9. Click Finish.

Missouri Research and Education Network 🎾 University of Missouri System



#### 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.

Active Director	v Users and Computers			Administrators Poperties ?	· ×
Ele Artise Vie	y osers and computers			General Members Member Of Managed By	
File Action Vie	ew Help				
	4 🗉 🗙 🗒 🖸 📑			Members:	
Active Directory	/ Users and Computers [Yourse	Name	Туре	Name Active Directory Domain Services Folder	
> 📋 Saved Queri	es	Access Control Assistance Operat	Security Group	& Administrator subdomain.yourdomainname.org/Users	
<ul> <li>subdomain.</li> </ul>	yourdomainname.org	Account Operators	Security Group	Company Admins subdomain.yourdomainname.org/Users     Setempted Administration yourdomainname.org/Users	
📙 Builtin		Administrators (3)	Security Group	Chieppise Ad Subdomain.yourdomainname.org/ osers	
> Comput	Controllers	💐 Backup Operators	Security Group		
> Corrigns	SecurityPrincipals	Access Certificate Service DCOM Access	Security Group		
> 🧾 Manage	d Service Accounts	K Cryptographic Operators	Security Group		
📔 Users		Representation of the text of text	Security Group		
		Event Log Readers	Security Group		
		4 Guests	Security Group		
		Hyper-V Administrators	Security Group		
			Security Group		
	Select Users, Contacts, Comp	outers, Service Accounts, or Groups	× [		
			p	Add Bemove	
	Select this object type:			Aud Hemove	
	Users, Service Accounts, Grou	ps, Built-in security principals, or Other o	bject Types	( f )	
	From this location:		p	OK Cancel	Apply
	subdomain.yourdomainname.or	g I	Locations p	Servers in this group run	11.2
	Enter the object names to cales	t (avamalaa):	· · · ·	Servers in this group can	
	Enter the object hames to select	t ( <u>examples</u> ).	<b>d</b>	Servers in this group ena	
			p	Members in this group a	
	( c )	$\bigcirc$	p	Members of this group	
		(e)	p	Supports file replication	
	Advanced	ок	Cancel p	Members can administe	
I			occurry oroup	Members of this group	
		🏻 🍇 System Managed Accounts Group	Security Group	Members of this group	

- 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 Builtin 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.

	Dial-in	Enviro	onment	Sessions	Membe	r Of	Dial-in	Envi	ironment	Sessions
Remote control	Remote D	lesktop Serv	vices Profile	COM+	Remote	control	Remote	Desktop Se	rvices Profile	COM
ieneral Address	Account	Profile	Telephones	Organization	General	Address	Account	Profile	Telephones	Organizat
4 Administr	ator				User logo	n name: 🔍	5	( a )		
	80				versmi	-		M		~
					User logo	n name (pre	-Windows 200	0):		
first name:	Veronica		Initials:		SUBDOM	IAIN\		versmi		
Last name:	Smith +	a			Logon	Hours	Log On T			
Display name:	Veronica Smit	h								
	D the		1			caccount				
Jescription:	Built-In accou	nt for admini	istering the com	nputer/doma						
Office:					Account of	ptions:				
						r muet oban	ne password a	t next logo	n	
						i iliusi cilali		at the At 10 you	11	
				01	Use	r cannot chi	ange passwor	d		
Felephone number:				Other	Use	r cannot chi sword neve	ange passwor r expires	d		
Felephone number:				Other	Use	r cannot chi sword never e password	ange passwor r expires using reversib	d le encryptic	'n	v
Felephone number: E-mail:				Other	☐ Use ☐ Use ☐ Pas ☐ Stor	r cannot cha sword never e password t expires	ange passwor r expires l using reversib	d le encryptic	n	v
Telephone number: E-mail: Neb page:				Other	☐ Use ☑ Use ☑ Pas ☐ Stor Account ④ Nev	r cannot chi sword never e password t expires	ange passwor r expires using reversib	d le encryptic	n	v
Telephone number: E-mail: Neb page:				Other	☐ Use ☑ Use ☑ Pas ☐ Stor — Account ④ Nev	r cannot chan sword never e password t expires ver	ange passwor r expires using reversib	d le encryptic	2 2017	v 
Felephone number: Ξ-mail: Neb page:				Other	☐ Use ☑ Use ☑ Pas ☐ Stor ● Nev ○ End	r cannot chan sword never e password t expires ver of:	r expires using reversib	d le encryptic	2, 2017	· · · · · · · · · · · · · · · · · · ·
elephone number: -mail: Veb page:				Other	☐ Use ☑ Use ☑ Pas ☐ Stor Account ④ Nev ○ End	r cannot chan sword never e password t expires ver	ange passwor r expires using reversib Thursday , 1	d le encryptic	2, 2017	•

- 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.
----	------	--------	-----------	-------	-----	------------

Active Directory Users and Com	puters			-	- 🗆	~
ile Action View Help						
• 🔿 🖄 📰 🔏 📋 🗙 🛛	j 🖸 📑 🚺 🖡	1 8 🕺 🕯	7 🗾 🍇			
Active Directory Users and Com	Name	Туре	Description			^
Saved Queries	& Administrator	Hear	Puilt in account for a	d		
subdomain.yourdomainnam	Allowed RO	Сору	is grou	р с		
	🗟 Cert Publish	Add to a gr	oup is grou	p		
Computers     Domain Controllers	💐 Cloneable D	Disable Acc	ount is grou	p t		
ForeignSecurityPrincipal:	DefaultAcco	Reset Passw	vord t mana	ge		
> 📋 Managed Service Accour	Benied ROD	Move	iis grou	р с		
📋 Users	A DnsAdmins	Open Hom	e Page rators G	iro		
	DnsUpdateP	Send Mail	no are p	er		
	Domain Ad		ministr	ato		
	Domain Co	All Tasks	> is and s	er		
	Reportain Con	Cut	ests	5 1		
	B Domain Users	Delete	ers			
	Enterprise A	Rename	ministr	ato		
	Enterprise K		nis grou	p		
	👫 Enterprise R	Properties	nis grou	p		
	Sroup Polic	Help	iis grou	р с		
	Guest	User	Built-in account for g	ue		
	👗 Jane Citizen	User				
	Key Admins	Security Group	Members of this grou	p		
/	Protected Us	Security Group	Members of this grou	p		*
Right-click on the / a. Type in the b. Press Ente	Administrat First name r.	or user, ar e and last i	nd select Rena name of the U	ame. Isername you	u want	t to use.
Right-click on the / a. Type in the b. Press Ente Active Directory Us File Action View	Administrat First name r. ers and Computers Help	or user, ar e and last i	nd select Rena name of the U	ame. Isername you	u want	to use.
Right-click on the / a. Type in the b. Press Ente Active Directory Us File Action View	Administrat First name r. ers and Computers Help	or user, ar and last r	nd select Rena name of the U	ame. Isername you	u want	t to use.
Right-click on the / a. Type in the b. Press Ente Active Directory Us File Action View	Administrat First name r. ers and Computers Help I X II Computers Additional Computers	or user, ar and last r	nd select Rena name of the U & & T 2 &	ame. Isername you	u want	t to use.
Right-click on the / a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries	Administrat First name r. ers and Computers Help Tomainar rdomainar	or user, ar and last r ie models for the second ie Type eronica Smith	nd select Rena name of the U	ame. Isername you	u want	t to use.
Right-click on the / a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries	Administrat First name r. ers and Computers Help Ters and Com rdomainnarr	or user, ar and last r e and last r r e Typ eronica Smith llowed RO Sec	e Descripti rung Group Member	ame. Sername you	u wani	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Saved Queries Builtin Computers	Administrat First name r. ers and Computers Help ers and Com rdomainnarr	or user, ar e and last r e Typ eronica Smith llowed RO Sec ert Publish Ioneable D	e Descripti r Built-in z urity Group Member me User	ame. Sername you on account for ad s in this group c	u want	t to use.
Right-click on the / a. Type in the b. Press Ente Active Directory Us File Action View Prile Action View Active Directory Use Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Builtin Sign Computers Sign Computers Sign Computers Sign Computers	Administrat First name r. ers and Computers Help ers and Com rdomainnarr	or user, ar e and last r e and last r e Typ eronica Smith llowed RO Sec ert Publish loneable D efaultAcco	e Descripti r Built-in z urity Group Member me User	ame. Sername you	u want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Saved Save	Administrat First name r. ers and Computers Help ers and Com rdomainnarr ertollers rityPrincipal: vice Accourt	or user, ar e and last r e and last r e Typ eronica Smith loneable D efaultAcco enied ROD	e Descripti r Built-in a urity Group Member me User ame: Veronica Si	ame. Sername you on account for ad s in this group c	u want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Use File Action View Active Directory Use Saved Queries Saved Queries Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Computers Computers Computers Computers Computers Computers Computers Computers Computers Computers	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rtrollers rityPrincipal: price Accour	or user, ar e and last r e and last r e Typ eronica Smith lowed RO Sec ert Publish loneable D efaultAcco enied ROD nsAdmins nsAdmins nsAdmins	and select Rena name of the U	ame. Sername you	u want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Builtin Computers Computers	Administrat First name r. ers and Computers Help ers and Com rdomainnar trollers rityPrincipal:	or user, ar e and last r e and last r e Typ eronica Smith loneable D refaultAcco enied ROD nsAdmins nsUpdateP omain Ad Last r	e Descripti re Descripti re Descripti re User ame: Veronica Si name: Smith	ame. Sername you	2 want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Builtin Sign Domain Com Domain Com ForeignSecu Saves	Administrat First name r. ers and Computers Help ers and Com rdomainnar rdomainnar rityPrincipal: vvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you	2 want	touse.
Right-click on the a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Builtin Sign Domain Con Sign Domain Con	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rtollers rityPrincipal: vvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the J a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Saved Queries Builtin S Computers Domain Con S ForeignSecu Sus	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rtollers rityPrincipal: vvice Accour	or user, ar e and last r e and last r e and last r e Typ eronica Smith loneable D efaultAcco enied ROD nsAdmins nupdateP omain Ad. omain Con omain Gue omain Gue	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Builtin Signo Computers Domain Con Signo Domain Con Signo Do	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rtollers rityPrincipal rvice Accoul	or user, ar e and last r e and	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Builtin Sign Domain Con Sign Domain Con	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rtollers rityPrincipal rvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Builtin Sign Domain Con Sign Domain Con	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rtrollers rityPrincipal rvice Accour	or user, ar e and last r e and last r e and last r e Typ eronica Smith loneable D efaultAcco enied ROD nsAdmins msUpdateP tomain Ad omain Con oomain Gue oomain Use nterprise A. netroprise R.	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the J a. Type in the b. Press Ente Active Directory Us File Action View Computers Saved Queries Saved Queries Sav	Administrat First name r. ers and Computers Help ers and Com rdomainnarr rityPrincipal rvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Computers Saved Queries Saved Queries Sav	Administrat First name r. ers and Computers Help ers and Com rdomainnar rityPrincipal: rvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you	2 want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Builtin Computers Domain Con Managed Se Users	Administrat First name r. ers and Computers Help ers and Com rdomainnar rityPrincipal: rvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you	2 Want	t to use.
Right-click on the A a. Type in the b. Press Ente Active Directory Us File Action View Active Directory Use Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Domain Con Saved Saved Domain Con Saved Saved Saved Saved Saved Saved Saved Saved Saved Saved Saved Sa	Administrat First name r. ers and Computers Help ers and Com rdomainnar rityPrincipal: rvice Accour	or user, ar and last r and last r	and select Rena name of the U	ame. Sername you on on occount for ad s in this group c mith mith 2000): Versmi OK s or this group	2 Vand	t to use.

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

Missouri Research and Education Network 🎾 University of Missouri System



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



#### 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.

• (i	🕉   🚩 Manage <u>Tools</u> View Help
	Active Directory Administrative Center
	Active Directory Domains and Trusts
	Active Directory Module for Windows PowerShell
	Active Directory Sites and Services
	Active Directory Users and Computers
	ADSI Edit
	Component Services
	Computer Management
	Defragment and Optimize Drives
	Disk Cleanup
	DNS
	Event Viewer
	Group Policy Management
	iSCSI Initiator
	Local Security Policy
	Microsoft Azure Services
	ODBC Data Sources (32-bit)
	ODBC Data Sources (64-bit)
	Performance Monitor
	Print Management
	Resource Monitor
	Services
	System Configuration
	System Information
	Task Scheduler
	Windows Firewall with Advanced Security
	Windows Memory Diagnostic
	Windows PowerShell
	Windows PowerShell (x86)
	Windows PowerShell ISE
	Windows PowerShell ISE (x86)
	Windows Server Backup

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



🛼 Server Manager							×
Server M	lanager • Dashboar	d		• ®	Manage	Tools View	Help
Dashboard     Local Server     All Servers     AD DS     DNS     File and Storage Services b	WELCOME TO SERVER MANAGER	gure this local server d roles and features d other servers to manage sate a server group anect this server to cloud servic	85				Hide
	ROLES AND SERVER CROUPS Role: 3 Song word 1 Servers total AD DS 1 Manageability Events Services Reformance BPA results	The DNS THE DN	File and Storage     1       Services     1       Manageability     Events       Services     Performance       PPA results     5	Local Server 1     Manageability     Events     Events     Performance     BPA results     9/13/2017 300 PW	All Servers     Manageability     Events     Services     Performance     BPA results     s/15/	1 26 IT 300 PM	
# ^ @ 🤗 I					^	13:08 PM 9/13/201	7 5

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 Multiple   Services All  Services	ice status All ers All	•		
Server Name Display Name YOURSERVERNAME Downloaded Maps Manager YOURSERVERNAME Sync Host_119796	Service Name MapsBroker OneSyncSvc_119796	Status Start Stopped Autor Stopped Autor	Type matic (Delayed Sta matic (Delayed Sta	rt) rt)
	Go To Lo	cal Server	OK	Cancel

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)	Event	Viewer	(Local)
----------------------	-------	--------	---------

Directory Service

Hardware Events

DNS Server

#### Overview and Summary

ast refreshed: <u>9/15/2017 11:27:47 PM</u>

#### 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 Admir	nistrative E	vents								
Event Type	Event II	) Source		Log			Last hour	24 hours	7 days	^
	-	-		-			3	56	109	- 6
	34	Time-Se	vice	Syste	em		0	0	1	
	69	AppMod	el-Runtime	Micr	osoft-Windov	vs-AppModel-Runtime/Admin	0	14	14	
	304	User Dev	r Device Registration Microsoft-Windows-User Device Registration/Admin				0	5	5	
	307	User Dev	ice Registration	Micr	osoft-Windov	vs-User Device Registration/Admin	0	5	5	
·	866	PrintServ	ice	Micr	osoft-Windo	vs-PrintService/Admin	0	4	12	
1002		ThinPrin	ThinPrint AutoConnect		ThinPrint Diagnostics		0	3	3	
	1008	Perflib		Application		0	1	3		
	1202	ADWS DFSR		Active Directory Web Services DFS Replication		0 0	2 2	5 9		
	1202									
	7023	Service C	ervice Control Manager		System		0 0	4 0	20 5	
81	8198	Security-	SPP	Application						
	10016	Distribut	edCOM	Syste	em		3	16	27	
🕀 Warning	-	-		-		0	19	136		
⊞ Information	-	-		-			19	819	2,914	~
8198 Security-SPP 10016 DistributedCOM ⊞ Warning ⊞ Information tecently Viewed Nodes		edCOM	System - -		3 0 19	16 19 819	27 136 2,914			
og 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)			
DES Replication		68 KB/14	9/15/2017 11:11:39	AM	Enabled	bled 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.

Enabled Overwrite events as necessary (oldest events first)

Overwrite events as necessary (oldest events first)

Overwrite events as necessary (oldest events first)

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.

Enabled

Enabled

68 KB/1.0... 9/15/2017 11:11:24 AM

68 KB/100... 9/15/2017 11:11:40 AM

68 KB/20 ... 5/23/2017 10:03:44 AM

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.



Event Viewer

File Action View Help

Event Viewer (Local)	DFS Replication	Number of events: 58				
Custom Views     Server Roles	Level	Date and Time	Source	Event ID	Task Category	1
Active Directory Domain Service	(1) Information	9/15/2017 11:15:51 AM	DFSR	1210	None	H
TONS Server	(1) Information	9/15/2017 11:15:46 AM	DFSR	1206	None	
Remote Desktop Services	🕕 Error	9/15/2017 11:10:46 AM	DFSR	1202	None	
Maninistrative Events	Information	9/15/2017 11:10:45 AM	DFSR	6102	None	
T Summary page events	(1) Information	9/15/2017 11:10:40 AM	DFSR	1314	None	
🗸 🙀 Windows Logs	<ol> <li>Information</li> </ol>	9/15/2017 11:10:40 AM	DFSR	1004	None	
Application	(1) Information	9/15/2017 11:10:39 AM	DFSR	1002	None	
F Security	lau .	0/15/2017 11 01 11 11	DECD.	1210.	<u>NI</u>	
Setup	Event 1210, DFSR					×
System	Coursel and					
Forwarded Events	General Details					
Applications and Services Logs						
Active Directory Web Services	The DFS Replica	ition service successfully set up a	in RPC listener for in	ncoming replicati	on requests.	
Disasters Casica	Additional Infor	mation:				
Directory Service	Port: 0					
Und Server						
Hardware Events						
Hardware Events     Internet Explorer						
Hardware Events  Key Management Service						
Hardware Events Hardware Events Key Management Service Microsoft						
Hardware Events     Hardware Events     Internet Explorer     Key Management Service     Microsoft     Microsoft     AppV						
<ul> <li>Hardware Events</li> <li>Hardware Events</li> <li>Internet Explorer</li> <li>Key Management Service</li> <li>Microsoft</li> <li>AppV</li> <li>User Experience Virtualization</li> </ul>						
<ul> <li>Hardware Events</li> <li>Hardware Events</li> <li>Internet Explorer</li> <li>Key Management Service</li> <li>Microsoft</li> <li>AppV</li> <li>User Experience Virtualization</li> <li>Windows</li> </ul>						
<ul> <li>Hardware Events</li> <li>Hardware Events</li> <li>Internet Explorer</li> <li>Key Management Service</li> <li>Microsoft</li> <li>AppV</li> <li>User Experience Virtualization</li> <li>Windows</li> <li>ThinPrint Diagnostics</li> <li>Windows PowerShell</li> </ul>						

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

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

DSACLS, Directory Services Access Control Lists Utility: <u>https://technet.microsoft.com/en-us/library/cc771151(v=ws.11).aspx</u>

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

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

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

NETDOM, Windows Domain Manager: 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-toolsindex.html



#### DNS SERVER CONFIGURATION

#### Definitions

<u>Domain Name System</u> – 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.

<u>Domain Name</u> – 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.

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

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

<u>Zone(s)</u> – 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.

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

#### Common Record Types:

<u>Start of Authority (SOA)</u> – 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.

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

<u>CNAME</u> – 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.

<u>MX</u> – 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.

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

<u>Time to Live (TTL)</u> – 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.

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

<u>PTR</u> – 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..

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



<u>Top-Level Domain</u> – 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.

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

<u>Subdomain</u> – 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)

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

<u>Resolving Name Server</u> – 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.

<u>Forwarder(s)</u> – 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.

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

Implement Domain Name System (sample chapter from Networking with Windows Server 2016) <u>https://www.microsoftpressstore.com/articles/article.aspx?p=2756482</u>

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

DNS: Installing and Configuring Servers (as related to Windows Server 2008 R2) <u>https://technet.microsoft.com/en-us/library/cc755183(v=ws.11).aspx</u>

Optimizing your network to keep your DNS squeaky clean <a href="https://blogs.technet.microsoft.com/networking/2009/02/09/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/</a>

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

🛔 DNS Manager		
File Action View	Help	
4 🔿 🗹 📆 🗙		
DNS VOURSERVEPAN Solution Office DNS Office	Name           Configure a DNS Server           Create Default Application Directory Partitions           New Zone           Set Aging/Scavenging for All Zones           Scavenge Stale Resource Records           Update Server Data Files           Clear Cache           Launch nslookup           All Tasks           View           Delete           Refresh	>
	Properties	
	Help	

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

Debug Logging	Event Logging	Monitoring	Security
Interfaces	Forwarders	Advanced	Root Hints
Select the IP addre for DNS queries on limit it to selected IF Listen on: All IP addresses Only the followir	sses that will serve D all IP addresses defir 2 addresses. ng IP addresses:	NS requests. The se red for this computer	erver can lister r, or you can
IP address:			
Intel®0::d0ef ✓ 192.168.5	5:e979:2068:b9fe 0.204		

• 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: <u>https://www.more.net/services/blackhole-dns</u>. 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.

Missouri Research and Education Network 》 University of Missouri System

0



#### Advanced Tab

Debug Logging	Event Logg	jing	Monitoring	Secu	rity
Interfaces	Forwarders	1	Advanced	Root Hin	ts
Server version num	ber:				
10.0 14393 (0x383	39)				
Server options:					
Disable recursion	n (also disables fo	orwarde	rs)		
land	it fairs and and the it		10/		
Enable BIND se	condaries		,		
Enable BIND se	condaries ad zone data		,		
Enable BIND se	condaries ad zone data bin				
Enable BIND se Fail on load if ba Enable round rol Enable netmask	condaries ad zone data bin ordering				
Enable BIND se Fail on load if ba Enable round rol Enable netmask Secure cache a	condaries ad zone data bin ordering gainst pollution				
Enable BIND se Fail on load if ba Enable round rol Enable netmask Secure cache a Vame checking:	condaries nd zone data bin ordering gainst pollution	lultibyte	(UTF8)		~
Enable BIND se Fail on load if ba Enable round rol Enable netmask Secure cache a Name checking:	condaries id zone data bin ordering gainst pollution N startup: F	lultibyte	· (UTF8) ive Directory and	d registry	~ ~
Enable BIND se Fail on load if ba Enable round rol Enable netmask Secure cache a Name checking: Load zone data on	condaries id zone data bin ordering gainst pollution startup: E ic scavenging of	lultibyte rom Act	(UTF8) ive Directory and cords	1 registry	~ ~
□ Enable BIND se □ Fail on load if ba ☑ Enable round rol ☑ Enable netmask ☑ Secure cache a Name checking: .oad zone data on □ Enable automati Scavenging pe	condaries Id zone data bin ordering gainst pollution startup: Ic scavenging of riod: 0	lultibyte rom Act	(UTF8) ive Directory and cords	d registry	1 1
□ Enable BIND se □ Fail on load if ba ☑ Enable round rol ☑ Enable netmask ☑ Secure cache a Name checking: Load zone data on □ Enable automati Scavenging pe	condaries id zone data bin ordering gainst pollution startup: ic scavenging of riod: 0	lultibyte rom Act stale re	(UTF8) ive Directory and cords days	1 registry	~ ~

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

Server options:

0

- 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

Debug Logging	Event Loggi	ng i	Monitoring	Secur	ity
Interfaces	Forwarders	Adva	nced	Root Hint	ts
Root hints resolve erver. They are o espond. lame servers:	queries for zones ti only used if forward	hat do not e lers are not	exist on the lo configured o	ocal DNS orfailto	
Server Fully Qual	ified Domain Name	(FQDN)	IP Addr	ress	^
a.root-servers.net			[2001:5	03:ba3e::2	
b.root-servers.net			[2001:5	500:200::b]	
c.root-servers.net			[2001:5	00:2::c]	
d.root-servers.net	10		[2001:5	500:2d::d]	
e.root-servers.net			[2001:5	00:a8::e]	
f.root-servers.net			[2001:5	500:2f:f]	
g.root-servers.net			[2001:5	00:12::d0d	
h.root-servers.net	<b>L</b> .		[2001:5	500:1::53]	v
<				>	
Add	Edit	Remove	Cop	y from Serve	er

 $\circ$  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: <u>https://www.iana.org/domains/root/servers</u>, http://www.root-servers.org/



## 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

Interfaces	Forwarders	Advanced	Root Hint	s
Debug Logging	Event Loggin	Monitoring	Secur	ity
The DNS event log encountered by the server performance Log the following er No events Errors only Errors and warni All events	maintains a record DNS server. You vents: ings	d of errors, warnings, a can use this informati	and other eve	ent

• 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-

<u>us/library/dn800669(v=ws.11).aspx#en</u>. The Audit events are enabled by default; however, the Analytic events are not.



#### Monitoring Tab

	Forwarders	Advance	ed	Root Hints
Debug Logging	Event Lo	gging Mo	nitoring	Security
Fo verify the conf sutomatic testing. Select a test type A simple query A recursive qu Fo perform the test Perform autom Test interval:	iguration of the s r against this DN: lery to other DNS st immediately, cl natic testing at the 1 mir	erver, you can po S server S servers ick Test Now. a following interva	erform ma	nual or Test Now
Fest results:				
Fest results: Date	Time	Simple Query	Recurs	ive Q

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

http://www.tech-faq.com/monitoring-andtroubleshooting-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.

79



#### 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.

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

🛔 DNS Manager	
File Action View Help	
🗢 🔿 📰 🗶 📰 🖄	
DNS VURSERVERNAME VIM Forward Lookup Zones Image: Subdomain.you VIM subdomain.yourdoma Image: S	urdomainname.org
<ul> <li>image: Intersection</li> <li>image: Intersection&lt;</li></ul>	Reload New Host (A or AAAA) New Alias (CNAME) New Mail Exchanger (MX) New Domain New Delegation Other New Records DNSSEC > All Tasks > View
Contains commands for customizing	Delete Refresh Export List Properties Help

- 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.

Missouri Research and Education Network 阶 University of Missouri System

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



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.

0

I. 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

subdomain.yourdo	mainname.org	Properties		?	$\times$		
WINS General	Zone T Start of Autho	ransfers nity (SOA)	N	Security ame Server	s		
Status: Runnir	ng			Pause			
Type: Active	Directory-Integra	ted		Change.			
Replication: All DN	S servers in this d	omain		Change.			
Data is stored in Ac Dynamic updates: Allowing non vulnerability b sources.	Data is stored in Active Directory.  Dynamic updates:  Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted						
To set aging/scave	nging properties,	click Aging		Aging			
0	K Car	icel	Apply	He	lp		

Status: Shows the current status of the zone

• 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*)

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)

• 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.

Zone Aging/Scavenging	Properties		×
Scavenge stale resource	e records		
No-refresh interval			
The time between the mand the moment when the	nost recent re the timestamp	fresh of a record may be refreshed	timestamp d again.
No-refresh interval:	7	days	~
Refresh interval The time between the e be refreshed and the e scavenged. The refresh record refresh period.	earliest momer arliest momen n interval must	nt when a record t t when the record t be longer than th	imestamp can can be ne maximum
Refresh interval:	7	days	$\sim$
		OK	Cancel

Fig.3 If you make changes, click OK.

Fig.2 If you make changes, click OK.



#### Start of Authority Tab

subdomain.yourdomainname.org Properties ? X

WINS	Zone Transfers	Security
General	Start of Authority (SOA)	Name Servers
Serial number:		
43		Increment
Primary server:		
yourservemame.st	ubdomain.yourdomainname.org	Browse
Responsible perso	n:	
hostmaster.subdor	main.yourdomainname.org.	Browse
Refresh interval:	15 minutes	~
Retry interval:	10 minutes	$\sim$
Expires after:	1 days	$\sim$
Minimum (default)	TTL: 1 hours	~
TTL for this record	: 0 :1 :0 :0	(DDDDD:HH.MM.SS)
C	OK Cancel	Apply Help

• 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.

o TTL for this record: defines the TTL for this record



## Name Servers Tab

General o add name serv	Start of Authority (SOA)	Name Servers
o add name serv	ere to the list click Add	
	era to the list, click hud.	
ame servers: Server Fully Qua	ified Domain Name (FQDN)	IP Address
yourservemame.	subdomain.yourdomainname.org.	[192.168.50.204]
Add	Edit Remove	a DNS query and may
represents an IP ot represent actu	al records stored on this server.	

## WINS Tab

subdomain.yourdom	ainname.org Properties	? ×					
General	Start of Authority (SOA)	Name Servers					
WINS	Zone Transfers	Security					
You can use WINS to namespace. WINS o	You can use WINS to resolve names not found by querying the DNS namespace. WINS only supports IPv4 addresses.						
Use WINS forwar	d lookup						
Do not replica	te this record						
IP address:							
	Add						
	Remove						
	Up						
	Dave						
	Down						
		Advanced					
OK	Cancel /	Apply Help					

• 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 an 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.

• 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

subdomain.yourdor	mainname.org Properties	? ×			
General WINS	General         Start of Authority (SOA)         Name Servers           WINS         Zone Transfers         Security				
A zone transfer sends a copy of the zone to the servers that request a copy.					
Allow zone transfers:					
Io any server     Only to server listed on the Name Server tab					
Only to servers listed on the Name Servers tab Only to the following servers					
IP Addres	s Server FC	NUC			
		Edit			
To specify secondary servers to be notified of zone updates, click Notify					
0	K Cancel A	pply Help			

• 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

WINS     Zone Transfers     Sec       iroup or user names:     Everyone     Image: Second Secon					
	curity				
CREATOR OWNER SELF Authenticated Users SYSTEM DnsAdmins (SUBDOMAIN\DnsAdmins)  Add Re missions for Everyone Allow Full control Read Write Create all child objects Delete all child objects Special permissions or special permissions or advanced settings, click dvanced. Adva					
SELF         Authenticated Users         SYSTEM         DnsAdmins (SUBDOMAIN\DnsAdmins)         Add         Remissions for Everyone         Allow         Full control         Read         Write         Create all child objects         Delete all child objects         Special permissions         or special permissions or advanced settings, click         Advanced.	SCREATOR OWNER				
Authenticated Users         SYSTEM         DnsAdmins (SUBDOMAIN\DnsAdmins)         Add         Remissions for Everyone         Allow         Full control         Read         Write         Create all child objects         Delete all child objects         Special permissions         or special permissions or advanced settings, click         Advanced.	M SELF				
SYSTEM     DnsAdmins (SUBDOMAIN\DnsAdmins)      Add      Remissions for Everyone     Allow     I      Full control     Read     V      Read     V      Read     V      Create all child objects     Delete all child objects     Soecial permissions     or special permissions or advanced settings, click     Adva	Authenticated Users				
Add       Re         ermissions for Everyone       Allow         Full control       I         Read       I         Write       I         Create all child objects       I         Delete all child objects       I         Special permissions       I         or special permissions or advanced settings, click       Adva	SYSTEM .				
Add     Re       ermissions for Everyone     Allow     I       Full control     I     I       Read     I     I       Write     I     I       Create all child objects     I     I       Delete all child objects     I     I       Special permissions     I     I       or special permissions or advanced settings, click     Advanced.					
ermissions for Everyone       Allow         Full control       I         Read       I         Write       I         Create all child objects       I         Delete all child objects       I         Special permissions       I         or special permissions or advanced settings, click       Adva	emove				
Full control       Image: Control in the second section of the second	Deny				
Read     Image: Constraint of the second settings and the second settings are second settings ar					
Write       Image: Create all child objects       Image: Create all child objects         Delete all child objects       Image: Create all child objects       Image: Create all child objects         Special permissions       Image: Create all child objects       Image: Create all child objects       Image: Create all child objects         Special permissions       Image: Create all child objects       Image: Create all child objects       Image: Create all child objects         or special permissions or advanced settings, click dvanced.       Advanced.					
Create all child objects					
Delete all child objects					
Special permissions or advanced settings, click Adva dvanced.					
or special permissions or advanced settings, click Adva dvanced.					
dvanced.	anced				
	a				

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

85

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) <u>https://technet.microsoft.com/en-us/library/cc730980(v=ws.11).aspx</u>



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

86



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



#### The Wizard

New Zone Wizard



 $\times$ 

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

< Back Next > Cance	< Back	Next >	Cance
---------------------	--------	--------	-------

New Zone Wizard

#### Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:	f F	
Primary zone Creates a copy of a zone that can be updated directly on this server.	F	
<ul> <li>Secondary zone</li> <li>Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.</li> <li>Stub zone</li> <li>Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.</li> </ul>		
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)		
< Back Next > Cancel		

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.



New Zone Wizard	$\times$
Active Directory Zone Replication Scope You can select how you want DNS data replicated throughout your network.	
Select how you want zone data replicated:	
<ul> <li>To all DNS servers running on domain controllers in this forest: subdomain.yourdomainname.org</li> </ul>	
To all DNS servers running on domain controllers in this domain: subdomain.yourdomainname.org	
O To all domain controllers in this domain (for Windows 2000 compatibility): subdomain.yourdomainname.org	
$\bigcirc$ To all domain controllers specified in the scope of this directory partition:	
	$\sim$
< Back Next > C	ancel

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.

Х

d. Click Next.

New Zone Wizard

Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.	
Choose whether you want to create a reverse lookup zone for IPv4 addresses addresses.	or IPv6
IPv4 Reverse Lookup Zone	
◯ IPv6 Reverse Lookup Zone	
< Back Next >	Cancel

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.

88

c. Click Next.



Reverse Lookup Zone Name	
A reverse lookup zone translates IP addresses into DNS names.	A ALLER
To identify the reverse lookup zone, type the network ID or the name of the zone. <ul> <li>Network ID:</li> <li>192 .168 .50 .</li> </ul> <li>The network ID is the portion of the IP addresses that belongs to this zone. Enternetwork ID in its normal (not reversed) order.</li> <li>If you use a zero in the network ID, it will appear in the zone name. For example.</li>	er the
network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would cr zone 0.10.in-addr.arpa.	eate
O Reverse lookup zone name:	
50. 168. 192.in-addr.arpa	
< Back Next > Car	ncel
New Zone Wizard	×
	-



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.

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.
<ul> <li>Select the type of dynamic updates you want to allow:</li> <li>Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones.</li> </ul>
<ul> <li>Allow both nonsecure and secure dynamic updates</li> <li>Dynamic updates of resource records are accepted from any client.</li> <li>This option is a significant security vulnerability because updates can be accepted from untrusted sources.</li> </ul>
O Do not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must update these records manually.



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.



90

#### New Zone Wizard

New Zone Wizard		X 7. Completing the New Zone Wizard
	Completing the New Zone Wizard You have successfully completed the New Zone Wizard. You specified the following settings:	a. You have successfully completed the New Zone Wizard. b. Review the summary of your selections.
	Name: 50.168.192.in-addr.arpa Type: Active Directory-Integrated Primary Lookup type: Reverse	verified from Powershell or an Administrative Command Prompt using nslookup, <u>https://technet.microsoft.com/en-</u> <u>us/library/bb490950.aspx</u> .
	Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup. To dose this wizard and create the new zone, dick Finish.	Your Reverse DNS Zone is now created and active.
	< Back Finish Cancel	

🍰 DNS Manager				_		$\times$
File Action View Help						
<ul> <li>DNS</li> <li>YOURSERVERNAME</li> <li>Forward Lookup Zones</li> <li>Reverse Lookup Zones</li> <li>50.168.192.in-addr.arpa</li> <li>Trust Points</li> <li>Conditional Forwarders</li> </ul>	Name (same as parent folder) (same as parent folder)	Type Start of Authority (SOA) Name Server (NS)	Data [1], yourservername.subdomain.yourdom yourservername.subdomain.yourdomainn	Timest static static	tamp	

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

- 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...



New Conditional Forwar	der		×
DNS Domain:			
www.google.com			
IP addresses of the maste	er servers:		
IP Address	Server FQDN	Validated	Delete
<click add="" an="" here="" ip<="" td="" to=""><td>Address or DNS Name&gt;</td><td>· · · · · · · · · · · · · · · · · · ·</td><td></td></click>	Address or DNS Name>	· · · · · · · · · · · · · · · · · · ·	
8.8.8.8	google-public-dns-a.go	ОК	Up
8.8.4.4	google-public-dns-b.go	ОК	Down
			<u> </u>
Store this conditional for	orwarder in Active Directory, an	d replicate it as follows:	
All DNS servers in this f	forest		
Number of seconds before	e forward queries time out: 5		
The server FQDN will not b configured.	be available if the appropriate re	everse lookup zones and entrie	es are not
		ОК	Cancel

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** 

Missouri Research and Education Network 🎾 University of Missouri System 221 N. Stadium Blvd., Ste. 201 X Columbia, MO 65203 P: (573) 884-7200 F: (573) 884-6673 W www.MORE.net



# **Section VI: Security Policies for Windows Server 2016**

#### MUST-READ LINKS!

CIS (Center for Internet Security) Microsoft Windows Server 2012R2 Benchmark <u>https://www.cisecurity.org/wp-</u> 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-v1607anniversary-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-practicesfor-securing-active-directory

Active Directory Security Groups

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/securingdomain-controllers-against-attack

Securing Domain Controllers to Improve Active Directory Security <a href="https://adsecurity.org/?p=3377">https://adsecurity.org/?p=3377</a>

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 1<sup>st</sup> 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 <u>https://www.sans.org/security-resources/policies</u>, to review the Information Security Policy templates available from SANS.

The 2<sup>nd</sup> 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 3<sup>rd</sup> 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. <u>Remove</u> 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.

Missouri Research and Education Network 阶 University of Missouri System

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



## **GROUP POLICY MANAGEMENT**

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

🛃 Group Policy Management		
📓 File Action View Window	Help	
🗢 🏟 🙇 📊 🧟 🖬		
Group Policy Management Control Forest: subdomain.yourdomain Control Forest: Subdomain.yourdomain. Control Forest: Subdomain. Control Forest: Subdomain. Con	name.org Domains Contents Domain Edit Enforced Link Enabled Save Report New Window from Here Delete Rename Refresh	
	Help	

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. <u>Remove that user account from the Domain Admins Security</u> <u>Group</u> when you are done editing the policies.]

6. Select Edit...

Group Policy Management Console	×
You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPC and will impact all other locations where this GPO is linked.	),
Do not show this message again OK	

7. Read the warning message, then click OK.



Group Policy Management Editor				_	$\times$
File Action View Help					
Jefault Domain Policy [YOURSERVERNAM	J Default Domain Policy [YOURSERVERNAME.SUB	DOMAIN.YOURDOMAINNAN	/E.ORG] Policy		
Computer Configuration     Policies	Select an item to view its description. Name				
> Preferences	👰 Computer	Configuration			
V 🕵 User Configuration	📶 User Confi	guration			
Policies     Preferences					
< >	Fxtended (Standard /				
	(//				

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 <a href="https://blogs.technet.microsoft.com/canitpro/2013/05/29/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/</a>

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 <u>Group Policy</u> <u>Management above</u>.



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

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



ile Action View Help  Action V	Policy	Policy Setting
▼       ● Policies         >       Software Settings         >       Name Resolution Policy         ⊗       Scripts (Startup/Shutdown)         >       Deployed Printers         >       Account Policies         >       Password Policy         >       Account Policies         >       Password Policy         >       Account Lockout Policy         >       Event Log         >       Event Log         >       Stricted Groups	<ul> <li>Enforce password history</li> <li>Maximum password age</li> <li>Minimum password length</li> <li>Password must meet complexity requirements</li> <li>Store passwords using reversible encryption</li> </ul>	24 passwords remembered 42 days 1 days 7 characters Ensbled Disabled

- 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.

98

d. Click OK to commit any changes.



	Explain		
Maximum passw This security set password can b change it. You o days between 1 never expire by password age is password age m the maximum pa age can be any Note: It is a secu every 30 to 90 d an attacker has user's password Default: 42.	tord age ting determines the period of time e used before the system require; an set passwords to expire after and 999, or you can specify that setting the number of days to 0, it between 1 and 999 days, the M uist be less than the maximum pa ssword age is set to 0, the minimu value between 0 and 998 days. unity best practice to have passw lays, depending on your environn a limited amount of time in which and have access to your networ	(in days) that a s the user to a number of passwords the maximum nimum ssword age. If um password ords expire nent. This way, to crack a k resources.	
		v	

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.

Minimum password age

7

×

Minimum password age Properties

Security Policy Setting Explain



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.
unty Policy Setting Explain			a. The options are between 0-14 characters.
			= No password is required.
Minimum password length	of characters		b. The default is 7 characters. You can eithe keep the default value, arrow up/down or manually
that a password for a user account may contain. value of between 1 and 14 characters, or you ca	You can set a n establish that		enter a new number.
no password is required by setting the number of Default:	characters to 0.		is difficult to require users to keep long passwords b
7 on domain controllers.			you should encourage it
0 on stand-alone servers.	optiquization of		u. Click OK to commit any changes.
their domain controllers.	Shingulation of		
	~		
For more information about security policy and rela	ited Windows	-	
reatures, <u>see the Microsoft Websits</u> .			
vord must meet complexity requirements Pro	perties ?	×	9. Double-click Password must meet complexity
· · · · · · · · · · · · · · · · · · ·			requirements.
utty Policy Setting Explain			
unty Policy Setting Explain			a. The options are Enabled or Disabled. b. The default is Enabled. You can either ke
If this policy is enabled, passwords must meet the	following	•	a. The options are Enabled or Disabled. b. The default is Enabled. You can either ke the default value, or change the radio button to
If this policy is enabled, passwords must meet the minimum requirements:	following	•	a. The options are Enabled or Disabled. b. The default is Enabled. You can either ke the default value, or change the radio button to Disabled. c. Click OK to commit any changes.
If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t	following he user's full	•	a. The options are Enabled or Disabled. b. The default is Enabled. You can either ke the default value, or change the radio button to Disabled. c. Click OK to commit any changes.
If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of the name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following four contain characters from the contain characters from three of the following four contain characters from the contain char	following he user's full ir categories:		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either keet the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy setting Explain If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following fou English lowercase characters (a through Z) English lowercase characters (a through z)	following he user's full ir categories:		a. The options are Enabled or Disabled. b. The default is Enabled. You can either ke the default value, or change the radio button to Disabled. c. Click OK to commit any changes.
If this policy setting Explain If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following fou English uppercase characters (a through Z) English lowercase characters (a through Z) Base 10 digits (0 through 9) Non-alphabetic characters for example, 1, S, #, 3	following he user's full ir categories:	× Í	<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy setting Explain If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following four English uppercase characters (A through Z) English lowercase characters (A through Z) English lowercase characters (a through Z) Base 10 digits (0 through 9) Non-alphabetic characters for example, 1, \$, #, \$ Complexity requirements are enforced when pass changed or created.	following he user's full ir categories: () words are	•	<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of the name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following four English uppercase characters (A through Z) English lowercase characters (A through Z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, 1, \$, #, \$ Complexity requirements are enforced when pass changed or created.	following he user's full ir categories: () words are		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy setting Explain If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following fou English uppercase characters (A through Z) English lowercase characters (A through Z) Base 10 digits (0 through 9) Non-alphabetic characters for example, 1, \$, #, \$ Complexity requirements are enforced when pass changed or created. Default: Enabled on domain controllers.	following he user's full ir categories: (a) words are		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of the name that exceed two consecutive characters. Be at least six characters in length Contain characters from three of the following four English uppercase characters (A through Z) English lowercase characters (a through Z) English lowercase characters (a through Z) Base 10 digits (0 through 9) Non-alphabetic characters for example, 1, S, <i>H.</i> , 3 Complexity requirements are enforced when pass changed or created. Default: Enabled on domain controllers. Disabled on stand-alone servers.	following he user's full ir categories: (a) words are		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy setting Explain If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following fou English uppercase characters (A through Z) English lowercase characters (a through Z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, 1, \$, #, * Complexity requirements are enforced when pass changed or created. Default: Enabled on domain controllers. Disabled on stand-alone servers. Note: By default, member computers follow the c their domain controllers.	e following he user's full ir categories: (a) words are onfiguration of		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of the name that exceed two consecutive characters are the end of the following for English lowercase characters (A through Z) Base 10 digits (0 through 9) Non-alphabetic characters for example, 1, \$, #, \$ Complexity requirements are enforced when pass changed or created. Default: Enabled on domain controllers. Disabled on stand-alone servers. Note: By default, member computers follow the context for their domain controllers. For more information about security policy and relations and the following follow the security policy and relations and the following following the security policy and relations and the following follo	onfiguration of sted Windows		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>
If this policy setting Explain If this policy is enabled, passwords must meet the minimum requirements: Not contain the user's account name or parts of t name that exceed two consecutive characters Be at least six characters in length Contain characters from three of the following fou English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters for example, 1, \$, #, 3 Complexity requirements are enforced when pass changed or created. Default: Enabled on domain controllers. Disabled on stand-alone servers. Note: By default, member computers follow the c their domain controllers. For more information about security policy and relatives, see the Microsoft website.	e following he user's full ir categories: (a) words are omfiguration of sted Windows		<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Enabled. You can either key the default value, or change the radio button to Disabled.</li> <li>c. Click OK to commit any changes.</li> </ul>



security Policy Setting Exprain	encryption.
Store passwords using reversible encryption         This security setting determines whether the operating system stores passwords using reversible encryption.         This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.         This policy is required when using Challenge-Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS). It is also required when using Digest Authentication in Internet Information Services (IIS).         Default: Disabled.         For more information about security policy and related Windows features, see the Microsoft website.	<ul> <li>a. The options are Enabled or Disabled.</li> <li>b. The default is Disabled. You can either keep the default value, or change the radio button to Enabled.</li> <li>c. Only use this feature for specific systems that require this to connect to the domain.</li> <li>d. Click OK to commit any changes.</li> </ul>



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

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

101



Security Policy Setting Explain Account lockout threshold The security setting determines the number of failed logon administration or until the lockout duration for the account has secured. You can set a value between 0 and 999 failed logon attempts. You also workstations or member servers that have been locked using either CTRL+ALT-DELETE prevent in the Microsoft website. Default: 0. Default: 0. A Valuess range between 0-999.0 = the account will never be locked out. b. The default is 0. C K Cancel Account of the decount has servers that have between 0-999.0 = the account will never be locked out. b. The default is 0. Suggested Value Changes C Cancel C Account lockout threshold is now 5 invalid logon attempts, the settings for the following terms will be changed to the suggested values. Policy Policy Setting Suggested Setting Not Defined 30 minutes	out threshold Properties ?	< A	7		operties	threshold Pro	ount lockout t
Account lockout threshold The security setting determines the number of failed logon stempts that causes a user account to be locked out. A power of vocces out a user account to be locked out. A power of vocces out a user account to be locked out. A power of vocces out a user account to be locked out. A power of vocces out a user account will never be locked out. The depassword attempts against workstations or member prevents that have been locked using either CTRL+ALT-DELETE prevent will never be locked out. a. Values range between 0-9999. 0 = the for more information about security policy and related Windows lectures: sec the Microsoft website. b. The default is 0. Suggested Value Changes Suggested Value Changes Policy Policy Policy Policy Setting Not Defined 30 minutes	Setting Explain	5				tting Explain	urity Policy Sett
OK Cancel   a. Values range between 0-999. 0 = the ccount will never be locked out. b. The default is 0. c. From the Security Policy 3 up/down or manually enter a new d. We have entered 5. e. Click OK. Suggested Value Changes Because the value of Account lockout threshold is now 5 invalid logon attempts, the settings for the following items will be changed to the suggested values. Policy Policy Setting Not Defined 30 minutes	count lockout threshold s policy setting will lock out after: invalid logon attempts		is in LETE	r of failed logon locked out. A is reset by an or the account ha nd 999 failed logo ount will never be ions or member r CTRL+ALT+DE it as failed logon	d mines the number er account to be ot be used until it ockout duration fo ilue between 0 ar alue to 0, the acco against workstati cked using either reen savers count t security policy ar t website.	ckout threshold ty setting deter at causes a us account cannor or until the lo u can set a va you set the va word attempts t have been lo d-protected sci ormation about e the Microsoft	Account loc This security attempts tha locked-out a administrator expired. You attempts. If y locked out. Failed password attempts. Default: 0.
a. Values range between 0-999. 0 = the account will never be locked out. b. The default is 0. Suggested Value Changes Because the value of Account lockout threshold is now 5 invalid logon attempts, the settings for the following items will be changed to the suggested values. Policy Account lockout duration Not Defined Suggested Setting Suggested Seting Suggested Seting Suggested Set	OK Cancel A		Ap	Cancel	ОК		
Suggested Value Changes       ×         Because the value of Account lockout threshold is now 5 invalid logon attempts, the settings for the following items will be changed to the suggested values.         Policy       Policy Setting       Suggested Setting         Image: Account lockout duration       Not Defined       30 minutes	om the Security Policy Setting tab, or manually enter a new number. e have entered 5. ck OK.	uţ	) = the	0-999. 0 out.	e between e locked o s 0.	ies range never b default i	a. Value ount will b. The o
Because the value of Account lockout threshold is now 5 invalid logon attempts, the settings for the following items will be changed to the suggested values.         Policy       Policy Setting       Suggested Setting         Account lockout duration       Not Defined       30 minutes	×				e Changes	ested Value	Sugge
Policy         Policy Setting         Suggested Setting           Account lockout duration         Not Defined         30 minutes	ts, the settings for	5 invalid lo ues.	hold is n ggested	lockout thres ged to the su	ue of Account s will be chan	use the valu llowing item	Becau the foll
Account lockout duration Not Defined 30 minutes	jested Setting	ting	Policy			cy	Polic
	inutes	ed	Not D		kout duration	Account loc	80 A
Reset account lockout counter after Not Defined 30 minutes	inutes	ed	Not D	ounter after	unt lockout co	Reset accou	11 R

2. Double-click Account lockout threshold.

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

ОΚ

Cancel



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, <u>remove the user account you added when</u> 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 <a href="https://technet.microsoft.com/en-us/library/dn319046(v=ws.11).aspx">https://technet.microsoft.com/en-us/library/dn319046(v=ws.11).aspx</a>

Audit Policy Recommendations, Windows Server 2016

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

Monitoring Active Directory for Signs of Compromise

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

Windows 10 and Windows Server 2016 security auditing and monitoring reference <a href="https://www.microsoft.com/en-us/download/details.aspx?id=52630">https://www.microsoft.com/en-us/download/details.aspx?id=52630</a>

# 1. If you are not already at the GPME pictured below, follow the instructions under <u>Group Policy</u> <u>Management above</u>.

🗐 Group Policy Management Editor
File Action View Help
Jefault Domain Policy [YOURSERVERNAME.SUBDOMAIN.YOURDOMAINNAME.ORG] Policy
Computer Configuration
✓ <sup>™</sup> Policies
> 🚞 Software Settings
✓ Image: Vindows Settings
> 🚞 Name Resolution Policy
Scripts (Startup/Shutdown)
> 💼 Deployed Printers
✓ La Security Settings
> 📑 Account Policies
> 🧃 Local Policies
> 📓 Event Log
> 📴 Restricted Groups
> 📴 System Services
> 🔀 Registry
> 📴 File System
> iii Wired Network (IEEE 802.3) Policies
> iii Windows Firewall with Advanced Security
Network List Manager Policies
> Interpretation Wireless Network (IEEE 802.11) Policies
> Public Key Policies
> 📔 Software Restriction Policies
> Application Control Policies
> IP Security Policies on Active Directory (SUBDOMAIN.YOURDOMAINNAME.ORG)
> 📔 Advanced Audit Policy Configuration
> 🍿 Policy-based QoS
> 📔 Administrative Templates: Policy definitions (ADMX files) retrieved from the local comp
> 🛗 Preferences
🗸 🌿 User Configuration
> 📋 Policies
> 📋 Preferences
× .

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.



Audit account logon e	events Properties	? ×
Security Policy Setting	Explain	
Audit accou	nt logon events	
Define these policy	y settings	
Audit these attemp	ots:	
Success		
Failure		
	OK C	ancel Apply

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.

<ul> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Deployed Printers</li> </ul>	Policy Audit account logon events Audit account management Audit directory service access Audit logon events Audit logon events Audit object access	Policy Setting Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure
<ul> <li>Security Settings</li> <li>Account Policies</li> <li>Password Policy</li> <li>Account Lockout Policy</li> <li>Kerberos Policy</li> <li>Local Policies</li> <li>Audit Policy</li> <li>User Rights Assignment</li> </ul>	Image       Image         Im	Success, Failure Failure Failure Success, Failure

- 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.



- 🗆 🗙

Group Policy Management Editor

2 🗊 🛛 🖬		
<ul> <li>Image: Deployed Printers</li> <li>Security Settings</li> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Event Log</li> <li>Restricted Groups</li> <li>System Services</li> <li>Registry</li> <li>File System</li> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Wireless Network (IEE 802.11) Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Maplication Control Policies</li> <li>Replication Control Policies</li> <li>Account Logon</li> <li>Account Logon</li> <li>Account Logon</li> <li>Account Logon</li> <li>Maccunt Management</li> <li>Dotailed Tracking</li> <li>DS Access</li> <li>Policy Change</li> <li>Privilege Use</li> </ul>	Advanced Getting Started Advanced Audit Policy Config policies, identify attempted or a compliance with rules governia when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin when Advanced Aud policy subcategory se settings" policy settin Subcategory se Global Object Access Auditing	uration settings can be used to provide detailed control over audit successful attacks on your network and resources, and verify ing the management of critical organizational assets. dit Policy Configuration settings are used, the "Audit: Force audit ettings (Windows Vista or later) to override audit policy category g under Local Policies\Security Options must also be enabled. Not configured Not configured
System     System     Global Object Access Auditing     Multiplicer based OpS		

- 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.



olicy	Explain			
	Audit Credential V	alidation		
c	onfigure the following au	dit events:		
	Success			
	Failure			
		OK	Connel	21.01

- 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, <u>remove the user account you added when you</u> 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

#### 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 <u>Group Policy</u> <u>Management above</u>.

Group Policy Management Editor					
File Action View Help					
🗢 🔿   📰 🗟   👔 🖬					
Cefault Domain Policy [YOURSERVERNAME.SUBDOMAIN.YOURDOMAINNAME.ORG] Policy					
Computer Configuration					
🗸 🚞 Policies ┥					
> 🚞 Software Settings					
✓ I Windows Settings					
> Canal Name Resolution Policy					
scripts (Startup/Shutdown)					
> 📖 Deployed Printers					
Security Settings					
> 📑 Account Policies					
> 👔 Local Policies					
> 👔 Event Log					
> A Restricted Groups					
> System Services					
> Cille Sustem					
File System     File Wired Network (IEEE 202.2) Dolicies					
Windows Firewall with Advanced Security					
Network List Manager Policies					
Wireless Network (IFFF 802.11) Policies					
Public Key Policies					
Software Restriction Policies					
> C Application Control Policies					
IP Security Policies on Active Directory (SUBDOMAIN.YOURDOMAINNAME.ORG)					
> 🧮 Advanced Audit Policy Configuration					
> Policy-based QoS					
> 📋 Administrative Templates: Policy definitions (ADMX files) retrieved from the local compute					
> 🦳 Preferences					
🗸 🕵 User Configuration					
> 🦰 Policies					
> 📋 Preferences					
< >					

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.

Group Policy Management Editor

File Action View Help

🗢 🔿 🚾 🗙 🔒 🛛 🖬			
<ul> <li>Perfault Domain Policy [YOURSERVERNAME.SUBDOMAIN.YOURDOMAINN</li> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Software Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Becurity Settings</li> <li>Security Settings</li> <li>Security Settings</li> <li>Local Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Sotripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Security Options</li> <li>Event Log</li> <li>System Services</li> <li>System Services</li> <li>Signature Security</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Software Restriction Policy Configuration</li> <li>Software Restriction Policy Directory (SUBDOMAIN.YC</li> <li>Advanced Audit Policy Configuration</li> <li>Preferences</li> <li>Sufficient P</li></ul>	Policy         Access Credential Manager as a trusted caller         Access this computer from the network         Act as part of the operating system         Add workstations to domain         Adjust memory quotas for a process         Allow log on locally         Allow log on through Remote Desktop Services         Back up files and directories         Bypass traverse checking         Change the system time         Change the system time         Change the time zone         Create a pagefile         Create global objects         Create global objects         Create symbolic links         Debug programs         Deny log on as a batch job         Deny log on as a batch job         Deny log on locally         Deny log on through Remote Desktop Services         Enable computer and user accounts to be trusted for delega         Force shutdown from a remote system         Generate security audits         Impersonate a client after authentication         Increase scheduling priority         Load and unload device drivers         Lock pages in memory	Policy Setting Not Defined Not Defined	
<ul> <li>Preferences</li> <li>User Configuration</li> <li>Policies</li> <li>Preferences</li> </ul>	<ul> <li>Load and unload device drivers</li> <li>Lock pages in memory</li> <li>Log on as a batch job</li> <li>Log on as a service</li> <li>Manage auditing and security log</li> <li>Modify an object label</li> <li>Modify firmware environment values</li> </ul>	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined	
< >>	💐 Obtain an impersonation token for another user in the same	Not Defined	Y

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.



\_\_\_\_

 $\Box$   $\times$ 



[a			Access this computer from the network
Access this computer	r from the network	10 A	
This user right determ connect to the comp Services are not affect	nines which users and groups are allowe uter over the network. Remote Desktop cted by this user right.	d to	Define these policy settings:
Note: Remote Deskto previous versions of 1	op Services was called Terminal Service Windows Server.	es in	
Default on workstatio	ons and servers:		
Administrators Backup Operators Users Everyone			
Administrators Backup Operators Users Everyone Default on domain co Administrators Authenticated Users Enterprise Domain Co	ontrollers:		Add User or Group Remove
Administrators Backup Operators Users Everyone Default on domain co Administrators Authenticated Users Enterprise Domain Co Everyone Pre-Windows 2000 C	ontrollers: ontrollers Compatible Access		Add User or Group Remove Modifying this setting may affect compatibility with clients, service and applications. For more information, see Access this computer from the network

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, <u>remove the user account you added when</u> 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

#### Network access: Allow anonymous DIS/name translation

https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-access-allowanonymous-sidname-translation

Network security: Do not store LAN Manager hash value on next password change <u>https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-do-not-</u> 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-forcelogoff-when-logon-hours-expire

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

1. If you are not already at the GPME pictured below, follow the instructions under <u>Group Policy</u> <u>Management above</u>.



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.



Group Policy Management Editor

- 🗆 🗙

File Action View Help		
🗢 🐟 🚾 🗙 🔒 🛛 🖬		
<ul> <li>Image: Security Settings</li> <li>Image: Security Sec</li></ul>	Policy Accounts: Administrator account status Accounts: Block Microsoft accounts Accounts: Block Microsoft accounts Accounts: Guest account status Accounts: Limit local account use of blank passwords to co Accounts: Rename administrator account Accounts: Rename guest account Accounts: Rename guest account Audit: Audit the access of global system objects Audit: Audit the use of Backup and Restore privilege Audit: Force audit policy subcategory settings (Windows Vis Audit: Shut down system immediately if unable to log secur	Policy Setting Not Defined Not Defined
User Rights Assignment User Rights Assignment Event Log Security Options Registry Registry Registry Mindows Firewall with Advanced Security Windows Firewall with Advanced Security Vireless Network (IEEE 802.31) Policies Wireless Network (IEEE 802.11) Policies Software Restriction Policies Software Restriction Policies	<ul> <li>DCOM: Machine Access Restrictions in Security Descriptor D</li> <li>DCOM: Machine Launch Restrictions in Security Descriptor T</li> <li>Devices: Allow undock without having to log on</li> <li>Devices: Allowed to format and eject removable media</li> <li>Devices: Allowed to format and eject removable media</li> <li>Devices: Restrict CD-ROM access to locally logged-on user</li> <li>Devices: Restrict floppy access to locally logged-on user only</li> <li>Domain controller: Allow server operators to schedule tasks</li> <li>Domain controller: Refuse machine account password chan</li> <li>Domain member: Digitally encrypt or sign secure channel data (when</li> <li>Domain member: Digitally sign secure channel data (when</li> </ul>	Not Defined Not Defined
<ul> <li>Security Policies on Active Directory (SUBDOMAIN.YC</li> <li>Advanced Audit Policy Configuration</li> <li>Mathematical Policy</li> <li>Advinistrative Templates: Policy definitions (ADMX files) retries</li> <li>Administrative Templates: Policy definitions (ADMX files) retries</li> <li>Preferences</li> <li>Security Policies</li> <li>Policies</li> <li>Preferences</li> <li>Preferences</li> </ul>	Domain member: Disable machine account password chan     Domain member: Maximum machine account password age     Domain member: Require strong (Windows 2000 or later) se     Interactive logon: Display user information when the session     Interactive logon: Do not display last user name     Interactive logon: Do not require CTRL+ALT+DEL     Interactive logon: Machine account lockout threshold     Interactive logon: Machine inactivity limit     Interactive logon: Message text for users attempting to log on     Interactive logon: Number of previous logons to cache (in c     Interactive logon: Prompt user to change password before e     Interactive logon: Require Domain Controller authentication	Not Defined Not Defined

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 THOROUGLY 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

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



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
- I. 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



This security setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If enabled, local accounts that are not password protected will only be able to log on at the computer's keyboard. Default: Enabled. Warning: Computers that are not in physically secure locations should always enforce strong password policies for all local user accounts. Otherwise, anyone with physical access to the computer can log on by using a user account that does not have a password. This is especially important for portable computers. If you apply this security policy to the Everyone group, no one will be able to log on through Remote Desktop Services. Notes	<ul> <li>Define this policy setting:</li> <li>Enabled</li> <li>Disabled</li> </ul>
--	--

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, <u>remove the user account you added when you</u> 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 <u>Group Policy</u> <u>Management above</u>.



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



X

Group Policy Management Editor

<ul> <li>Default Domain Policy [YOURSERVERNAME.SUBDOMAIN.YOURDOMAINN</li> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Beployed Printers</li> <li>Security Settings</li> <li>Account Policies</li> <li>Local Policies</li> <li>Event Log</li> <li>System Services</li> <li>System Services</li> <li>Registry</li> <li>Sub System Services</li> </ul>	Policy Maximum application log size Maximum security log size Maximum system log size Maximum system log size Prevent local guests group from accessing application log Prevent local guests group from accessing system log Retain application log Retain system log Retain system log Retention method for application log Retention method for system log	Policy Setting Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined

- 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 Setting
16384 kilobytes
16384 kilobytes
16384 kilobytes
Enabled
Enabled
Enabled
7 days
7 days
7 days
By days
By days
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, <u>remove the user account you added when</u> you began this section from the Domain Admins Security Group.

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



#### 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.

Active Director	y Users and Computers		New Object - Group	×	
File Action Vie	ew Help 🔏 📋   🗙 🗐 💽 📑 🛛 y Users and Computers [Yourserv	🗊 🔏 🐮 😭 🍸 🗾 🐍 ername.subdomain.yourdomainname.org]	Create in: subdor	main.yourdomainname.org/Users	
<ul> <li>Saved Quer</li> <li>Subdomain</li> <li>Builtin</li> <li>Compu</li> <li>Domair</li> <li>Domair</li> <li>Domair</li> <li>Foreign</li> <li>Keys</li> <li>LostAnc</li> <li>Managu</li> <li>Program</li> </ul>	nes Lyourdomainname.org n Controllers SecurityPrincipals dFound ed Service Accounts n Data		Group name: Workstation Admins Group name (pre-Windows 200 Workstation Admins Group scope O Domain local	0): Group type Security	
> System Users > MTD > TPM	System     Users     Delegate Control     TPM     Find		<ul> <li>● Global</li> <li>○ Universal</li> </ul>	ODistribution	
	New > All Tasks >	Computer Contact		OK Cancel	
	View >	Group	OK Cancel		
	Refresh msDS-KeyCredential mcDS-ResourcePropertyl ist		3. Type in the Group name: <group name=""> a. Leave the default Group Scope and</group>		
	Properties	msDS-ShadowPrincipalContainer	Group Type.		
	Help msImaging-PSPs MSMQ Queue Alias		b. Click OK.		
		Printer User Shared Folder			

Create a new object...

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.

			General	Members	Member Of	Managed	By		
🗊 浅 🔌 🛍 🍸 🗾 🍇			Membe	rs:		_			
Name	Туре	Descrip	Name	•	Active Dir	ectory Doma	ain Services F	older	
Administrator	User	Built-in							
Allowed RODC Password Repli	Security Group	Membe							
Cert Publishers	Security Group	Membe							
Koneable Domain Controllers	Security Group	Membe							
😓 DefaultAccount	User	A user a							
Rode Rode Password Replic	Security Group	Membe							
A DnsAdmins	Security Group	DNS Ac							
A DnsUpdateProxy	Security Group	DNS cli							
🚇 Domain Admins	Security Group	Designa							
Real Domain Computers	Security Group	All worl							
🚇 Domain Controllers	Security Group	All dom							
💐 Domain Guests	Security Group	All dom							
💐 Domain Users	Security Group	All dom							
💐 Enterprise Admins	Security Group	Designa	Ad	d	Remove				
🂐 Enterprise Key Admins	Security Group	Membe							
🂐 Enterprise Read-only Domain	Security Group	Membe				f	)		
💐 Group Policy Creator Owners	Security Group	Membe				ок	Cancel	Apply	,
ᡖ Guest	User	Built-in							
🧟 Key Admins	Security Group S	elect User	s, Contact	s, Compute	ers, Service A	Accounts, o	or Groups		$\times$
💐 Protected Users	Security Group								
💐 RAS and IAS Servers	Security Group	Select this o	bject type:						
🂐 Read-only Domain Controllers	Security Group	Users, Serv	rice Accour	nts, Groups,	or Other obje	cts		Object Types	
💐 Schema Admins	Security Group F	rom this loc	ation:						
🛃 Jane Citizen	User	subdomain.	yourdomair	nname.org				Locations	
🂐 Workstation Admins 🛛 🔒 🖉	Security Group						[		
	Ē	Inter the ob	ject names	to select (e	<u>xamples</u> ):			(	<b>d</b> )
	2	Jane Citizer	n (jancit@s	ubdomain.yo	ourdomainnan	ne.org)		Check Name	s
		(c)							
		$\bigcirc$					( e	)	
		Advance	be				OK	Cancel	

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 <u>Group Policy</u> <u>Management above</u>.

Group Policy Management Editor File Action View Help 🗢 🔿 📅 🛅 🗟 🛛 🖬 Default Domain Policy [YOURSERVERNAME.SUBDOMAIN.YOURDOMAINNAME.ORG] Policy Computer Configuration 🗸 📔 Policies ┥ > 📔 Software Settings 🗸 🚞 Windows Settings ┥ > Mame Resolution Policy Scripts (Startup/Shutdown) > 拱 Deployed Printers 🗸 🚡 Security Settings 🗲 > 🛗 Account Policies > 🝶 Local Policies > 🚮 Event Log > A Restricted Groups > 🔀 System Services Registry 🚡 File System Wired Network (IEEE 802.3) Policies Windows Firewall with Advanced Security Network List Manager Policies > Im Wireless Network (IEEE 802.11) Policies > Public Key Policies Software Restriction Policies > Application Control Policies > 😞 IP Security Policies on Active Directory (SUBDOMAIN.YOURDOMAINNAME.ORG) > 📔 Advanced Audit Policy Configuration > 🌓 Policy-based QoS > 🧾 Administrative Templates: Policy definitions (ADMX files) retrieved from the local compute > Preferences 🗸 💰 User Configuration > Policies > 📔 Preferences < >

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



Group Policy Management Editor		
File Action View Help		
🗢 🏟 🖄 📷 🗙 🗟 🛛 📅		
Default Domain Policy [YOURSERVE	RNAME.SUBDOMAIN.YOURD	4. Click
Computer Configuration		
Software Settings		
Windows Settings		
Name Resolution Pol	icv	
Scripts (Startup/Shute	down)	
> Deployed Printers		
🗸 🗟 Security Settings		
> 🔠 Account Policies		
> 📑 Local Policies		
Event Log		
Ca Restricted Groups		
> 📑 System Services	Open	
> 📴 Registry	Add Group	
> 📴 File System	Сору	
> Wired Network (I	Paste	
> I Windows Firewall		
🔛 Network List Man	View >	
> 📷 Wireless Network	Export List	
> Public Key Policie		
> Software Restriction	Help	

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

	Add Group			×
	Group:			
	Administrators		Browse	1
		ок	Cancel	
Select	Groups			
Select	this object type:			
Group	s or Built-in security principa	als	Obj	ect Types.
From th	nis location:			
subdo	main.yourdomainname.org		L	ocations
Entert	he object names to select (	(examples):		
Admin	istrators		Ch	eck Names
-				

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.

121



Administrators Properties	? ×	
Configure Membership for Administrators	6.	The Administrators Properties then launches to
Members of this group:	7.	Click Add next to Members of this group:
<this contain="" group="" members="" no="" should=""></this>	Add	<b>U</b>
	Remove	
This group is a member of: <the belongs<br="" group="" groups="" this="" to="" which="">should not be modified&gt;</the>	Add Remove	
OK Cancel	Apply	
Members of this group  \$UBDOMAIN\Domain Admins	Browse OK Cancel	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.</group>
Select Users, Service Accounts, or Groups Select this object type: Users, Service Accounts, Groups, or Built-in security prince From this location: subdomain.yourdomainname.org Enter the object names to select (examples): Domain Admins	Cipals Object Types.	<ul> <li>b. Select Users, Service Accounts, or Groups         <ul> <li>i. From the Add Member box,</li> <li>click Browse</li> <li>ii. In the Select Groups box,</li> <li>under Enter the object names to select:</li> <li>type the <group name="">. When you use</group></li> <li>the Select Groups box, the Group Name</li> <li>should already exist in Active Directory.</li> <li>iii. Click Check Names.</li> </ul> </li> </ul>



Administrators Properties	? ×
Configure Membership for Administrators	
Members of this group:	
SUBDOMAIN\Domain Admins SUBDOMAIN\Workstation Admins	Add Remove
This group is a member of: <the belongs<br="" group="" groups="" this="" to="" which="">should not be modified&gt;</the>	Add Remove
OK Cancel	Apply

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, <u>remove the user account you added when</u> 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 <u>https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-for-</u> <u>disabling-system-services-in-windows-server</u>

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

1. If you are not already at the GPME pictured below, follow the instructions under <u>Group Policy</u> <u>Management above</u>. 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.

Group Policy Management Editor File Action View Help 🗢 🔿 | 📰 📴 📑 🚺 🖬 Contemporary Conte Computer Configuration 🗸 📋 Policies ┥ > 📔 Software Settings > 📔 Name Resolution Policy Scripts (Startup/Shutdown) > 🚔 Deployed Printers 🗸 🚡 Security Settings 🗲 > 🛗 Account Policies > 📓 Local Policies > 🗿 Event Log > 🔂 Restricted Groups > System Services > Registry > File System > III Wired Network (IEEE 802.3) Policies > 🦳 Windows Firewall with Advanced Security Network List Manager Policies > III Wireless Network (IEEE 802.11) Policies > Public Key Policies Software Restriction Policies > Application Control Policies > 🛃 IP Security Policies on Active Directory (SUBDOMAIN.YOURDOMAINNAME.ORG) > Advanced Audit Policy Configuration > 🃗 Policy-based QoS > 🦳 Administrative Templates: Policy definitions (ADMX files) retrieved from the local compute > Preferences 🗸 💰 User Configuration > Policies > iii Preferences < >

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



Not Defined Not Defined

Not Defined Not Defined

 $\times$ 

Group Policy Management Editor

File Action View Help

Default

• 🔿 🔁 📆 🗟 📝 📅			
Default Domain Policy [YOURSERVERNAME.SUBDOMAIN.YO	Service Name	Startup	Permission
Computer Configuration	🙀 Active Directory Domain Services	Not Defined	Not Defined
V Policies	Active Directory Web Services	Not Defined	Not Defined
Software Settings	ActiveX Installer (AxInstSV)	Not Defined	Not Defined
Windows Settings	AllJoyn Router Service	Not Defined	Not Defined
IName Resolution Policy     Sectors (Startum (Startum))	App Readiness	Not Defined	Not Defined
Scripts (startup/shutdown)	Application Identity	Not Defined	Not Defined
Security Settings	Application Information	Not Defined	Not Defined
Account Policies	Application Layer Gateway Service	Not Defined	Not Defined
Local Policies	Application Management	Not Defined	Not Defined
> 🗟 Event Log	AppX Deployment Service (AppXSVC)	Not Defined	Not Defined
> 🔀 Restricted Groups	Auto Time Zone Updater	Not Defined	Not Defined
System Services	Background Intelligent Transfer Service	Not Defined	Not Defined
> 🙀 Registry	Background Tasks Infrastructure Service	Not Defined	Not Defined
> 📑 File System	Base Filtering Engine	Not Defined	Not Defined
> 🧾 Wired Network (IEEE 802.3) Policies	Bluetooth Support Service	Not Defined	Not Defined
> I Windows Firewall with Advanced Security	CDPUserSvc_10078b	Not Defined	Not Defined
Network List Manager Policies	Certificate Propagation	Not Defined	Not Defined
> Interpretation Wireless Network (IEEE 802.11) Policies	Client License Service (ClipSVC)	Not Defined	Not Defined
> Public Key Policies	CNG Key Isolation	Not Defined	Not Defined
Software Restriction Policies	COM+ Event System	Not Defined	Not Defined
> Application Control Policies	COM+ System Application	Not Defined	Not Defined
> IP Security Policies on Active Directory (SUE)	Computer Browser	Not Defined	Not Defined
Advanced Audit Policy Configuration	Connected Devices Platform Service	Not Defined	Not Defined
> III Policy-based QoS A designitization Translatory Deliver definitization (ADM)	Connected User Experiences and Telemetry	Not Defined	Not Defined
Administrative Templates: Policy definitions (ADM)	Contact Data 10078b	Not Defined	Not Defined
Iter Configuration	CoreMessaging	Not Defined	Not Defined
Dolicies	Credential Manager	Not Defined	Not Defined
> Preferences	Cryptographic Services	Not Defined	Not Defined
·			

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.

DataCollectionPublishingService

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

🙀 Data Sharing Service

- 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	This service manages persistent subscriptions to events from remote sources that support WS-
description	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 thir
	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.

Windows Event Collector Properties	?	$\times$
Security Policy Setting		
Windows Event Collector		
Define this policy setting		
Select service startup mode:		
<ul> <li>Automatic</li> </ul>		
◯ Manual		
◯ Disabled		
Edit Security		
OK Cancel	Ap	ply

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...



Security for	Windows Event	Collector	?	×
security for	WILLIGOWS LYCIN	Concetor		100

Security Group or user names: SYSTEM Source Administrators (SUBDOMA Source INTERACTIVE	UN/Administrators)	
	Add	Remove
Permissions for SYSTEM	Allow	Deny
Full Control Read Start, stop and pause Write Delete		
For special permissions or advar click Advanced.	nced settings,	Advanced
ОК	Cancel	Apply

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

Select Users, Computers, Service Accounts, or Groups		×
Select this object type:		
Users, Groups, or Built-in security principals		Object Types
From this location:		
subdomain.yourdomainname.org		Locations
Enter the object names to select ( <u>examples</u> ):		
<u>Users</u>		Check Names
Advanced	OK	Cancel

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.



Select Users, Computers, Service Account	s, or Group	IS				$\times$
Select this object type: Users, Groups, or Built in security principals				Object	Types	
From this location:					.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
subdomain.yourdomainname.org				Locat	tions	
Common Queries						
Name: Starts with $\checkmark$					Columns	
Description: Starts with $\checkmark$					Find Now	
Disabled accounts					Stop	
Non expiring password						
Days since last logon: 🔍 🗸					<del>?</del>	
Search results:				ОК	Cancel	
Name	E-Mail	Description	In Folder			^
Access Control Assistance Operators			subdomain.your	domainname.org/	/Builtin	
Account Operators			subdomain.youn	domainname.org/ domainname.org/	/Builtin /Builtin	
Administrators Allowed RODC Password Replication Gr ANONYMOUS LOGON		Members in this group	subdomain.your	domainname.org/	/Users	
Authentication authority asserted identity						
Backup Operators			subdomain.your	domainname.org/	/Builtin	
Cert Publishers		Members of this group	subdomain.your	domainname.org/	/Users	

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.

Security for Windows Event Colle Security Group or user names: SYSTEM & Administrators (SUBDOMAIN' & INTERACTIVE & Users (SUBDOMAIN\Users)	ctor VAdministrators)	? ×
Permissions for Users	Add	Remove
Full Control Read Start, stop and pause Write Delete		
For special permissions or advance click Advanced.	ed settings,	Advanced
OK	Cancel	Apply

7. All System Service Properties also have the option to configure Auditing.

a. From the Security for <Service> dialogue, click Advanced.



Permiss	ssions	Auditing			
	114.1	12 K K K K K K K K K K K K K K K K K K K		المامانين فراغا فالمارية المتعامين ومقوم والاخترامي والم	
or add	ditiona	il information, double-click a permission entry.	To modify a permission e	ntry, select the entry and click Edit (if available	e).
or add Permiss	ditiona ssion e	il information, double-click a permission entry. ntries:	To modify a permission e	ntry, select the entry and click Edit (if available	e).
or add Permiss Tyr	ditiona ssion e ype	l information, double-click a permission entry. ntries: Principal	To modify a permission e	Inherited from	e).
or add Permiss Typ S& De	ditiona ssion e ype eny	I information, double-click a permission entry. ntries: Principal Users (SUBDOMAIN\Users)	Access Start, stop and pause	Inherited from None	e).
Permiss Typ S& De S& All	ditiona ssion e ype eny llow	I Information, double-click a permission entry. ntries: Principal Users (SUBDOMAIN\Users) SYSTEM	Access Start, stop and pause Full Control	Inherited from None None	e).
Permiss Typ S& Dei S& Alli S& Alli	ditiona ssion e ype eny Ilow Ilow	I Information, double-click a permission entry. ntries: Principal Users (SUBDOMAIN\Users) SYSTEM Administrators (SUBDOMAIN\Administrato	Access Start, stop and pause Full Control Full Control	Inherited from None None None	e).

b. Click on the Auditing tab.

missio	as Auditing			
additic	nal information, double-click an a	udit entry. To modify an audit entry	select the entry and click Edit (if	available).
diting e	ntries:	uni entry i concenty en ecent entry,		
Туре	Principal	Access	Inherited from	
Fail	Everyone	Full Control	None	

c. Click Add.



📕 Auditing	Entry for Windows Event Collector			
Principal: Type:	Select a principal Success			d. Click Select a principal.
Basic perm	nissions: Full Control Read Start, stop and pause Write Delete		Show advanced pa	rmissions
	Special permissions		C	iear all
			OK	Cancel
Select Select User, From t	User, Computer, Service Account, or Group this object type: Group, or Built-in security principal his location:	Object Types	e. Enter the object r Names or Click Adv f. Click OK.	name and click Check anced to search.
subdo <u>E</u> nter t <u>Users</u>	omain.yourdomainname.org the object name to select ( <u>examples</u> ):	Locations Check Names		
Ad	vanced	OK Cancel		
Principal: Type: Basic per	Users (SUEDOMAIN\Users) Select a principal Fail		Shew advanced permissions	g. Change the Type: drop-down to Fail. Now when someone from the User Group attempts and
	Full Control     Read     Start, stop and pause     Write     Delete     Special permissions		Clear all	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.

Windows Security	× Security Policy >
You are setting a deny permissions entry. Deny entries take precedence over allow entries. This means that if a user is a member of two groups, one that is allowed a permission and another that is denied the same permission, the user is denied that permission. Do you want to continue?	You are about to change the security settings for this service. Changing the default security for the service could cause problems due to inconsistent configuration between this service and other services that rely on it. Do you want to continue?
Yes No	Yes No
8. When you configure deny permissions, you will	9 When you add or remove users or groups from

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
din	··· - ·· ·	··· <del>-</del> -· ·

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

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



#### **REGISTRY POLICIES**

1. If you are not already at the GPME pictured below, follow the instructions under <u>Group Policy</u> <u>Management above</u>.

Group Policy Management Editor File Action View Help 🗢 🔿 | 📰 | 🔄 🗟 | 🚺 📷 Default Domain Policy [YOURSERVERNAME.SUBDOMAIN.YOURDOMAINNAME.ORG] Policy Computer Configuration 📔 Policies ┥ > 📔 Software Settings 🗸 📋 Windows Settings ┥ > 📔 Name Resolution Policy Scripts (Startup/Shutdown) > Reployed Printers 🗸 🚡 Security Settings 🗲 > 🛗 Account Policies > 🗿 Local Policies > 👔 Event Log > 📴 Restricted Groups > 📴 System Services > 📸 Registry > 📴 File System > iii Wired Network (IEEE 802.3) Policies > Windows Firewall with Advanced Security Network List Manager Policies > 🚂 Wireless Network (IEEE 802.11) Policies Public Key Policies Software Restriction Policies Application Control Policies > 📵 IP Security Policies on Active Directory (SUBDOMAIN.YOURDOMAINNAME.ORG) > Advanced Audit Policy Configuration > Policy-based QoS > 🦳 Administrative Templates: Policy definitions (ADMX files) retrieved from the local compute > 📔 Preferences User Configuration > Policies > 📔 Preferences <

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



 $\times$ 



key:

 $\times$ 

8. Click OK.

Advance Right-click on Registry and select Add Key...

Help

- 4. You will see 3 registry groups
  - a. CLASSES\_ROOT
  - **b. MACHINE**
  - c. USERS

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

Group or user names: Image: ALL APPLICATION PACKAGES CREATOR OWNER SYSTEM Administrators (SUBDOMAIN\Administrators) Users (SUBDOMAIN\Users)					
	Add	Remove			
Permissions for Administrators	Allow	Deny			
Full Control Read Special permissions					
For special permissions or advanc click Advanced.	ed settings,	Advanced			
OK	Canaal	A			

9. In the Database Security dialogue, click Advanced.

7. As you expand, the path will appear under Selected



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.

vner	Unable to display curr	rent owner. Change			
rmissions	Auditing				
r additional	l information, double-c	lick an audit entry. To modify	/ an audit entry, select the entry	and click Edit (if availal	ble).
Туре	Principal	Access	Inherited from	Applies to	
Add	Remove	View			

b. Click Add.



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

Principal:	Select a principal	
Гуре:	Success V	
Applies to:	This object and child objects $\qquad \lor$	
Basic permi	ssions:	
	Full Control	
	Read	
	neuu	
Only app	Special permissions	within this contain
Only app	Special permissions  ty these auditing settings to objects and/or containers  r, Computer, Service Account, or Group	within this contain
Only app Select Use Select this User, Grou	Special permissions  y these auditing settings to objects and/or containers  r, Computer, Service Account, or Group  object type: up, or Built-in security principal	within this contain
Only app Select Use Select this User, Grow	Special permissions  Special permissions  r, Computer, Service Account, or Group  object type: up, or Built-in security principal coation:	within this contain
Only app Select Use Select this User, Gro From this k subdomain	Special permissions  y these auditing settings to objects and/or containers  r, Computer, Service Account, or Group  object type: up, or Built-in security principal ocation: n.yourdomainname.org	• within this contain
Only app Select Use Select this User, Grou From this k subdomain Enter the c	Special permissions  y these auditing settings to objects and/or containers  er, Computer, Service Account, or Group  object type:  up, or Built-in security principal  ocation:  n.yourdomainname.org  object name to select (examples):	Within this contain  Object Types  Locations
Only app Select Use Select this User, Grou From this k subdomain Enter the c Administra	Special permissions  Special permissions  System 2  Special permissions  System 2  Sy	<ul> <li>Within this contain</li> <li>Object Types</li> <li>Locations</li> <li>Check Names</li> </ul>
Only app Select Use Select this User, Grow From this k subdomain Enter the c Administra	Special permissions  Special permissions  System 2  Special permissions  System 2  Sy	<ul> <li>Within this contain</li> <li>Object Types</li> <li>Locations</li> <li>Check Names</li> </ul>

- 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.

Auditing E	ntry for MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				×
Principal:	Administrators (SUBDOMAIN\Administrators) Select a principal				
Туре:	Success ~				
Applies to:	This object and child objects $$				
Basic permi	ssions:	Show adva	nced p	ermissi	ons
	Full Control				
	Read				
	☐ Read ✓ Special permissions				
🗌 Only app	ly these auditing settings to objects and/or containers within this container		(	Clear all	

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



Auditing Entry for MACHINE/SOFTWARE/MICrosoft/Windows/Current/ersion/Run	L	Auditing Entry	for MACHINE	SOFTWARE\Micros	oft\Windows\CurrentVersion\Run	
--	---	----------------	-------------	-----------------	--------------------------------	--

— 🗆 X

Principal: Type:	Administrators (SUBDOMAIN\Administrators)	Select a principal		
Applies to:	This key and subkeys	$\sim$		
Advanced p	permissions:			Show basic permissions
	Full Control		Create Link	
	Query Value		🗹 Delete	
	☑ Set Value		Read permissions	
	Create Subkey		Change permissions	
	Enumerate Subkeys		✓ Take ownership	
	Notify			
🗌 Only app	oly these auditing settings to objects and/or cont	ainers within this cor	tainer	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.



137

Add Object X	12. Add Object launches.	
<ul> <li>MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Rur</li> <li>Configure this key then</li> <li>Propagate inheritable permissions to all subkeys</li> </ul>	<ul> <li>a. Configure this key then</li> <li>i. Default - Propagate inheritable permissions to all subkeys</li> <li>ii. Replace existing permissions on all subkeys with inheritable permissions</li> </ul>	
<ul> <li>Replace existing permissions on all subkeys with inheritable permissions</li> </ul>	b. Do not allow permissions on this key to be replace c. Click OK.	
$\bigcirc$ Do not allow permissions on this key to be replaced		
Edit Security OK Cancel		
<u>^</u>		
Object Name		
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\F	tun	

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:

wner:	Unable to display current owner	. Change		
ermissions	Auditing			
r addition	al information, double-click a pern	nission entry. To mod	ify a permission entry, select	the entry and click Edit (if available).
ermission e	ntries:			
Type	Principal	Access	Inherited from	Applies to
Type Allow	Principal Administrators (SUBDOMAIN	Access Full Control	Inherited from None	Applies to This key and subkeys
Type Allow	Principal Administrators (SUBDOMAIN CREATOR OWNER	Access Full Control Full Control	Inherited from None None	Applies to This key and subkeys Subkeys only
Type Allow Allow Allow	Principal Administrators (SUBDOMAIN CREATOR OWNER SYSTEM	Access Full Control Full Control Full Control	Inherited from None None None	Applies to This key and subkeys Subkeys only This key and subkeys
Type Allow Allow Allow Allow	Principal Administrators (SUBDOMAIN CREATOR OWNER SYSTEM Users (SUBDOMAIN\Users)	Access Full Control Full Control Full Control Read	Inherited from None None None None	Applies to This key and subkeys Subkeys only This key and subkeys This key and subkeys

- 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, <u>remove the user account you added when</u> you began this section from the Domain Admins Security Group.

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



#### 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

Dynamic Access Control: Scenario Overview https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/dynamic-access-control--scenariooverview

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, <u>remove the user account you added when</u> 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

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



**Back to Contents** 

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

Compared to the current MOREnet Blackhole DNS Serivce, 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 <a href="http://winhelp2002.mvps.org/hosts.htm">http://winhelp2002.mvps.org/hosts.htm</a>

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

Group Policy Preferences https://technet.microsoft.com/en-us/library/dn581922(v=ws.11).aspx



### CREATE A SHARE

### 1. Open Server Manager.

# 🚡 Server Manager

Server M	anager • Dashboard
Dashboard	WELCOME TO SERVER MANAGER
Local Server     All Servers     AD DS	1 Configure this local server
<ul> <li>B DNS</li> <li>■ File and Storage Services ▷</li> </ul>	QUICK START 2 Add roles and features
	3 Add other servers to manage
	4 Create a server group
	5 Connect this server to cloud services
	LEARN MORE

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

Server	<sup>™anager</sup> Server M	lanager • F	ile and Storage Serv	ices 🕨	Shares	- 🗆 🗙 • 🎯   🚩 Manage Tools View Help
	Servers Volumes	Filter	\$ s 2 total ₽ (Ⅲ) ▼	(H) •	TASKS  New Shar Refresh	VOLUME NETLOGON on Yourservername TASKS
	Storage Pools Shares	Share Yourserv	Local Path ername (2)	Protocol	Availability Ty	22.5% Used 13.4 GB Used Space
<b>••</b>	ISCSI Work Folders	NETLOGON SYSVOL	C:\Windows\\$Y\$VOL\sysvol C:\Windows\\$Y\$VOL\sysvol	SMB	Not Clusterec	Go to Volumes Overview >
					QUOTA NETLOGON on Yourservername To use quatas, File Server Resource Manager must be installed. To install File Server Resource Manager, start the Add Roles and Features Wizard.	
3. Cli	ck on Shares.					5

- 4. From the TASKS drop-down, select New Share...
- 5. This launches the New Share Wizard.



#### The Wizard

r

SMB Share - Quick     This basic profile represents the fastest work       SMB Share - Advanced     SMB Share - Advanced       SMB Share - Applications     SMB Share - Applications       Dther Settings     NFS Share - Quick       Vermissions     NFS Share - Advanced       Confirmation     NFS Share - Advanced	way to create a iles with ired later by
hare Name hare Name SMB Share - Advanced SMB Share - Applications NFS Share - Quick onfirmation esults	ired later by
ther Settings SMB Share - Applications NFS Share - Quick • Suitable for general file sharing • Advanced options can be configur using the Properties dialog • Suitable for general file sharing • Advanced options can be configur using the Properties dialog	ired later by
INFS Share - Quick     • Suitable for general file sharing       Infrastion     • Advanced       esuits     • Suitable for general file sharing	ired later by
using the Properties dialog usults	
sults	

### 1. Select Profile

a. Options:

i. SMB Share - Quick (basic profile, typically used with Windows-based computer filesharing)

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.



re location: Select by volume: Volume C: The location of the file volume. Type a custom path:	Status Online Free Spa 46.1 ( e share will be a new < Previous	Cluster Role Not Clustered ce Capacity File Sy 38 59.5 GB NTFS folder in the \Shares	Owner Node /stem directory on the se	elected Browse	2
re location: Select by volume: Volume C: The location of the file volume. Type a custom path:	Free Spa 46.1 ( e share will be a new < Previous	ce Capacity File Sy 58 59.5 GB NTFS folder in the \Shares	/stem directory on the se	elected Browse	<u>a</u>
Volume C: The location of the file volume. Type a custom path:	Free Spa 46.1 ( e share will be a new < Previous	ce Capacity File S 58 59.5 GB NTFS folder in the \Shares Next >	directory on the se	elected Browse	2
The location of the file volume. Type a custom path:	e share will be a new	folder in the \Shares	directory on the se	Browse	2
ustom path:	< Previous	Next >	Create	Cance	e
ustom path:	< Previous	Next >	Create	Cance	
nain.yourdomair 36)	perflogs Program Files Program Files (x86) users windows New folder				
	nain.yourdomair	nain.yourdomair 😭 perflogs <table-cell> Program Files More Program Files (x86) 😭 users 🐨 windows</table-cell>	nain.yourdomair imperflogs improgram Files improgram Files (x86) important view folder important view folder	nain.yourdomair e perflogs Program Files Program Files (x86) e users windows New folder	nain.yourdomair e perflogs Program Files Program Files (x86) users windows New folder



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.

hare Location	Server Name	Status	Chustes Delo		
hare Name			Cluster Kolé	Owner Node	
CONTINUE TRAFFIC THE	Yourservername	Online	Not Clustered		
onfirmation					
	Share location:				
	Select by volume:				
	Volume	Free Space	Capacity File Syst	tem	
	C:	46.1 GB	59.5 GB NTFS		
	The location of the fill	e share will be a new fold	der in the \Shares di	rectory on the sele	ected
	the location of the life				
	volume.				
	C:	46.1 GB	59.5 GB NTFS	n	ectory on the sele

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


📥 New Share Wizard		-		×
Specify share nam	е			
Select Profile	Share name:	Hosts		
Share Location				
Share Name	Share description:	This is where we will keep the updated hosts file from http:// winhelp2002.mvps.org/hosts.htm for the Hosts file GPO		
Other Settings				
Permissions				
Confirmation	Local path to share:			
Results	C:\Hosts			
	Remote path to sha	re:		
	\\Yourservername\}	losts		
		< Previous Next > Create	Car	ncel

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.



 $\times$ 

#### 📥 New Share Wizard

Select Profile	Enable access-based enumeration
Share Location Share Name	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.
Other Settings	✓ Allow caching of share
Permissions	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
	<ul> <li>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.</li> <li>Encrypt data access</li> <li>When enabled, remote file access to this share will be encrypted. This secures the data agains' 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.</li> </ul>

#### 4. Other Settings

a. 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.

b. (Checked by Default) Allow caching of share, makes folder contents available to offline users.

c. 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.

d. Click Next >



#### 🚡 New Share Wizard

– 🗆 🗙

# Specify permissions to control access

Select Profile Share Location	Permission permission	s to access t s, and, optio	he files on a sha nally, a central a	ire are set using a access policy.	combination	of folder permissi	ons, share	
Share Name	Share perm	nissions: Eve	rvone Full Cont	rol				
Other Settings	Folder per	nissions:	i yone i un com					
Pormissions	Type	Principal		Access	Applies To			1
Confirmation	Allow	CREATOR	OWNER	Full Control	Subfolders	and files only		
Confirmation	Allow	RUITINA	lsers	Special	This folder	and subfolders		
Results	Allow	BUILTINA	lsers	Read & executor	This folder	subfolders and fil	es	
	Allow	RUITINA	dministrators	Full Control	This folder	subfolders, and fil	e5	
	Allow			Full Control	This folder	subfolders, and fil	e5	
	Custom	ize permissio			This folder,	Subrolacis, and in		
•. Permissions a. Click Cus Advanced Secu Name:	stomize perr urity Settings for Ho C:\Hosts	nissions	S	Previous	xt >	Create	Cancel	]
Owner:	Administrators (SU	BDOMAIN	Administrators)	Change				
Permissions	Share	Auditing	Effective A	ccess				
For additional in Permission entri Type Pr & Allow S <sup>1</sup> Allow A & Allow U & Allow U	formation, double- ies: rincipal YSTEM dministrators (SUBE sers (SUBDOMAIN\ sers (SUBDOMAIN\ REATOR OWNER	click a perm DOMAIN Users) Users)	Access Full control Full control Read & execute Special Full control	nodify a permission Inherit C:\ C:\ e: C:\ C:\ C:\	on entry, sele	ct the entry and cliu Applies to This folder This folder This folder Subfolders	ck Edit (if av ; subfolders ; subfolders ; subfolders ; aud subfol ; and subfol	railable). and files and files and files ders hly
Allow C								
Add Disable inher	Remove	View						

Missouri Research and Education Network 🎾 University of Missouri System



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.

varme	8	C:\Hosts					
wne	er:	Administrators (S	UBDOMAIN\Ad	Iministrators) Change			
Pern	nissions	Share	Auditing	Effective Access			
o m	odify shar	e permissions, selec	t the entry and	click Edit.			
etw	ork locati	on for this share: \\	Yourservernam	e.subdomain.yourdomainn	ame.org\Hosts		
erm	ission ent	ries:					
	Туре	Principal			Access		
2	Allow	Everyone			Full Control		

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 Sec	curity Settings for H	osts		— L	X
Name:	C:\Hosts				
Owner:	Administrators (S	UBDOMAIN\Adm	ninistrators) Change		
Permissions	Share	Auditing	Effective Access		
Effective Acces domain, you ca of adding a gro	is allows you to view an also evaluate the oup, any group that	w the effective per e impact of potent the intended gro	rmissions for a user, group tial additions to the securit up is a member of must b	, or device account. If the account is a member of a y token for the account. When you evaluate the impact e added separately.	^
User/ Group:	Users (SUBDOMA	AIN\Users) Selec	t a user		
	Include group m	embership	Click Add items	✓ Add items	
Device:	Select a device				
	Include group m	embership	Click Add items	✓ Add items	
	Include a user cla	im			-
	Include a device of	claim			
View effecti	ve access				
Effective acce	ss l	Permission		Access limited by	٦
×	F	Full control		File Permissions	-
*	1	Traverse folder / e	xecute file		
*	l	List folder / read d	lata		
1	F	Read attributes			
*	F	Read extended att	ributes		
1	0	Create files / write	data		
2	0	Create folders / ap	opend data		
×	N	Write attributes		File Permissions	
×	١	Write extended at	tributes	File Permissions	
×	I	Delete subfolders	and files	File Permissions	
×	I	Delete		File Permissions	
2	F	Read permissions			
×	c	Change permissio	ins	File Permissions	
×	1	Take ownership		File Permissions	~
				OK Cancel App	bly

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.



Administrators (S	UBDOMAIN	Administrators) Change	1	
Share	Auditing	g Effective Access		
al information, double	e-click a pern	nission entry. To modify a	permission entry, select	the entry and click Edit (if available).
ntries:		, ,		
Principal		Access	Inherited from	Applies to
SYSTEM		Full control	C:\	This folder, subfolders and files
Administrators (SUE	BOMAIN	Full control	C:\	This folder, subfolders and files
Users (SUBDOMAIN	\Users)	Read & execute	C:\	This folder, subfolders and files
Users (SUBDOMAIN	l\Users)	Special	C:\	This folder and subfolders
Remove	View			
	Share Il information, double ntries: Principal SYSTEM Administrators (SUE Users (SUBDOMAIN Users (SUBDOMAIN CREATOR OWNER	Share     Auditing       al information, double-click a permittries:     Principal       SYSTEM     Administrators (SUBDOMAIN       Users (SUBDOMAIN\Users)     Users (SUBDOMAIN\Users)       Users (SUBDOMAIN\Users)     CREATOR OWNER	Share     Auditing     Effective Access       al information, double-click a permission entry. To modify a ntries:     Principal     Access       Principal     Access     SYSTEM     Full control       Administrators (SUBDOMAIN     Full control     Users (SUBDOMAIN\Users)     Read & execute       Users (SUBDOMAIN\Users)     Special       CREATOR OWNER     Full control	Share       Auditing       Effective Access         II information, double-click a permission entry. To modify a permission entry, select ntries:       Principal       Access       Inherited from         SYSTEM       Full control       C:\       Administrators (SUBDOMAIN       Full control       C:\         Vsers (SUBDOMAIN\Users)       Read & execute       C:\       C:\       CREATOR OWNER       Full control       C:\

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.

Windows	Security	×	
	You can't remove Users (SUBDOMAIN\Users) because this object is inheriting permissions from its parent. To remove Users (SUBDOMAIN\Users), you must prevent this object from inheriting permissions. Turn off the option for inheriting permissions, and then try removing Users (SUBDOMAIN\Users) again.		
	ОК	]	

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

Missouri Research and Education Network 🎾 University of Missouri System



🞎 Allow	Users (SUBDOMAIN\Users)	Read & execute	C:\	This folder, subfolders and files
🞎 Allow	Users (SUBDOMAIN\Users)	Special	C:\	This folder and subfolders
🚨 Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only
	Block Inheritance What would y You are about to b inherited from a p → Convert i this object	rou like to do with the second	ne current inher oject, which means o r be applied to this o ns into explicit p	× rited permissions? that permissions object.
	→ Remove	all inherited permis	sions from this	Object.
Add	Remove View			
Disable ir	nheritance			
Replace a	all child object permission entries	with inheritable permissi	on entries from this	object

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.



#### 📥 New Share Wizard

## Specify permissions to control access

-	Sharo Namo	normissions: Evanyona Evill Cont	rol				
	Other Settieren Eolde	Folder permissions: Everyone run Control					
	Other Settings Folde	er permissions:					
	Permissions lyp	e Principal	Access	Applies to			
(	Confirmation Allo	ow BUILTIN\Users	Read & execu	This folder, subfolders, and files			
	Results	bw BUILTIN\Administrators	Full Control	This folder, subfolders, and files			
	Allo	W NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files			
	Alle	OW CREATOR OWNER	Full Control	Subfolders and files only			
x. Ba	ack at the New Share V	Vizard, click Next >	Previous Ne	xt > Create C	an		
w Share Wizard			_	_ ×			
w Share Wizard			-				
w Share Wizard	ons		_	- x			
w Share Wizard Onfirm selectio	Ons	are the correct settings and	_				
w Share Wizard )nfirm selectio elect Profile hare Location	Confirm that the following	are the correct settings, and	_ then click Creat	□ × te.			
w Share Wizard Onfirm selectio elect Profile hare Location	Confirm that the following	are the correct settings, and	_ then click Creat	te.			
w Share Wizard Difirm selectio elect Profile hare Location hare Name	Confirm that the following SHARE LOCATION Server:	are the correct settings, and Yourservername	_ then click Creat	□ × te.			
w Share Wizard Onfirm selectio elect Profile hare Location hare Name Xther Settings	Confirm that the following SHARE LOCATION Server: Cluster role:	are the correct settings, and Yourservername Not Clustered	_ then click Creat	te.			
w Share Wizard Onfirm selectio elect Profile hare Location hare Name Yther Settings ermissions	Confirm that the following SHARE LOCATION Server: Cluster role: Local path:	are the correct settings, and Yourservername Not Clustered C:\Hosts	_ then click Creat	□ × te.			
w Share Wizard Onfirm selection elect Profile hare Location hare Name Other Settings ermissions	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES	are the correct settings, and Yourservername Not Clustered C:\Hosts	_ then click Creat	e ×			
w Share Wizard onfirm selection elect Profile hare Location hare Name Other Settings ermissions confirmation esults	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts	_ then click Creat	e ×			
w Share Wizard Onfirm selection elect Profile hare Location hare Name Other Settings termissions Confirmation esults	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO	then click Creat	n s file			
w Share Wizard Onfirm selection elect Profile hare Location hare Name Other Settings termissions Confirmation esults	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description: Protocol:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO SMB	then click Creat	n sfile			
w Share Wizard Onfirm selection elect Profile hare Location hare Name Other Settings termissions Confirmation lesults	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description: Protocol: Access-based enumeration:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO SMB Enabled	then click Creat dated hosts file fror its.htm for the Host	n s file			
w Share Wizard Onfirm selectio elect Profile hare Location hare Name Dther Settings ermissions Confirmation lessults	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description: Protocol: Access-based enumeration: Caching:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO SMB Enabled Enabled	then click Creat dated hosts file fror its.htm for the Host	n s file			
w Share Wizard onfirm selectio elect Profile hare Location hare Name Dther Settings ermissions confirmation lesults	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description: Protocol: Access-based enumeration: Caching: BranchCache:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO SMB Enabled Enabled Disabled	then click Creat dated hosts file fror its.htm for the Host	n s file			
w Share Wizard onfirm selectio elect Profile hare Location hare Name 2ther Settings termissions confirmation lesuits	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description: Protocol: Access-based enumeration: Caching: BranchCache: Encrypt data:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO SMB Enabled Enabled Disabled Disabled	then click Creat	n s file			
w Share Wizard onfirm selection elect Profile hare Location hare Name Dther Settings termissions confirmation lesuits	Confirm that the following SHARE LOCATION Server: Cluster role: Local path: SHARE PROPERTIES Share name: Description: Protocol: Access-based enumeration: Caching: BranchCache: Encrypt data:	are the correct settings, and Yourservername Not Clustered C:\Hosts Hosts This is where we will keep the up http://winhelp2002.mvps.org/hos GPO SMB Enabled Enabled Disabled Disabled	then click Creat	n s file			

6. Confirmation: Review your configuration and Click Create.

Missouri Research and Education Network 🎾 University of Missouri System



🚘 New Share Wizard			_		×
View results					
Select Profile	The share was success	fully created.			
Share Location	Task	Progress	Status		
Share Name	Create SMB share		Completed		
Other Settings	Set SMB permissions		Completed		
Permissions					
Confirmation					
Results					
		C Previous Next >	Close	Cancol	
		< Previous Next >	Close	Cancel	

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



Serve	rManager ⊙▼     •• File anc	d Storage 1	Services •	Shares		- 🗆 X • 🗭   🏴 Manage Tools View Help
	Servers Volumes Disks Storage Pools Shares iSCSI Work Folders	Filter Share NETLOGON SYSVOL	S s 3 total Local Path vername (3) C:\Windows\SY C:\Windows\SY	م EXOL\sysvol\subd.	TASKS	VOLUME Hosts on Yourservername (C:) Capacity: 59.5 GB 22.5% Used 46.1 GB Free Space
		Hosts	CAHasts	Stop Sharing Open Share Properties	SUR 9	Ga to Volumes Overview > QUOTA Hosts on Yourservername To use quotas, File Server Resource Manager must be installed. To install File Server Resource Manager, start the Add Roles and Features Wizard.

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.

T Y	\\Yours	servername.sub	domain.yourdomainna	ame.org\Hosts	~ Č
		Name	^	Date modified	Тур
🖈 Quick access					
Desktop	*			This folder is empty.	
👆 Downloads	*				
Documents	*				
Fictures	*				

b. Open Share, in File Explorer.



#### Hosts Properties

– 🗆 🗙

#### Hosts

-
-
-

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

-						
EO		er	ner	mis	SIO	nc
	-	<b>_</b>	PCI		510	1121

Туре	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.

ОК

Cancel

Apply

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

Missouri Research and Education Network 🎾 University of Missouri System



#### DOWNLOAD THE CURRENT MVP HOSTS FILE

1. Log into a domain computer with your Administrator credentials.

2. Open an internet browser.

3. Navigate to: <u>http://winhelp2002.mvps.org/hosts.htm</u>. 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: <u>\\yourservername.subdomain.yourdomainname.org\Hosts</u>

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:
              # Mv test line
              192.168.5.17 mytest
      b. Go to File > Save.
```



Vie	w								
nane	Extra large icons	; 📧 Large icons	Medium icons			🔲 Group by 🝷	ltem check boxes		3=
pune	Small icons	E List	EE Details	-		📺 Add columns 🔻	File name extensions		<b>X</b>
pane	📲 Tiles	Content		Ŧ	Sort by •	🖶 Size all columns to fit	✓ Hidden items	Hide selected items	Options •
		Lavout				Current view	Show/hide		

- 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.

hosts	Rename
	If you change a file name extension, the file might become unusable. Are you sure you want to change it?
	Yes No

- 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.

🛃 Group Policy Management

🔜 File Action View Window Help 🗢 🔿 🔁 📆 📋 🗒 🧟 📝 🤝 🔜 Group Policy Management subdomain.yourdomainname.org A Forest: subdomain.yourdomainname.o Status Linked Group Policy Objects Group Policy Inheritance 📓 Domains subdomain.yourdomainname.o Create a GPO in this domain, and Link it here... 🗊 Default Domain Policy Link an Existing GPO ... > 📓 Domain Controllers > 📑 Group Policy Objects Block Inheritance > 📑 WMI Filters Group Policy Modeling Wizard... > 🛅 Starter GPOs New Organizational Unit > 📑 Sites 👸 Group Policy Modeling Search... 🕞 Group Policy Results Change Domain Controller... Remove Active Directory Users and Computers... View > New Window from Here Refresh Properties Help

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

New GPO		×
Name:		
Disable DNS Client and Deploy H	losts File	
Source Starter GPO:		
(none)		~
	ОК	Cancel

a. Type a descriptive label in the Name: field.

b. Click OK.

Missouri Research and Education Network 》 University of Missouri System



#### **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.

🗟 Group Policy Management			
属 File Action View Window Help			
🔶 🔿 🔁 🖬 🗎 🗎 🖓 🖓			
Group Policy Management		subdo	main.yourdomainname
<ul> <li>A Forest: subdomain.yourdomainname.org</li> <li>I pomains</li> </ul>		Status	Linked Group Policy Objects
<ul> <li>subdomain.yourdomainname.org</li> <li>Default Domain Policy</li> </ul>			page shows the status of Active Policy.
Disable DNS Client and Deploy Hosts Fil Domain Controllers	e	Edit	-
> iii Group Policy Objects > iii WMI Filters		Enford	ced
> 💼 Starter GPOs > 📬 Sites	~	Save F	Report
Group Policy Modeling		New Window from Here	
		Delete	2
		Renan Refres	ne :h
		Help	

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



Group Policy Management Editor

File Action View Help				
<table-cell-rows> 🔿 🗾 🗙 🗐 🔒 🛛 🖬</table-cell-rows>				
<ul> <li>Computer Configuration</li> <li>Policies</li> </ul>	^	Service Name	Startup Not Defined	Permission
<ul> <li>Software Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Deployed Printers</li> <li>Security Settings</li> </ul>		DFS Namespace	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined
<ul> <li>Account Policies</li> <li>I Local Policies</li> <li>I Event Log</li> <li>Restricted Groups</li> </ul>		Distributed Transaction C dmwappushsvc	Not Defined Not Defined Not Defined	Not Defined Not Defined Not Defined
<ul> <li>System Services</li> <li>Registry</li> <li>File System</li> <li>File System</li> <li>File Wired Network (IEEE 802.3) Policies</li> </ul>		DNS Server Downloaded Maps Mana DS Role Server	Not Defined Not Defined Not Defined Not Defined	Not Defined Not Defined Not Defined Not Defined

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.

DNS Client Properties	?	$\times$
Security Policy Setting		
DNS Client		
Define this policy setting		
Select service startup mode:		
○ Automatic		
◯ Manual		
Disabled		
Edit Security		
OK Cancel	App	ply

- 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...



Files

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



File Action View Help	<ol><li>Right-click Files, hover over New &gt; and click File.</li></ol>
🗢 🧼 🙍 💼 🗈 🖶 💀 💁 🚺 🔂 🔶 🔸	
<ul> <li>Disable DNS Client and Deploy Hosts File</li> <li>Computer Configuration</li> <li>Policies</li> <li>Preferences</li> <li>Windows Settings</li> <li>Environment</li> <li>Files</li> </ul>	es a la companya de la
Fold     New     File       Ini F     All Tasks     >       Regi     View     >       Net     Copy       Ini F     Paste       Policies     Print       Print     Export List       Help     No policies sele	ected
New File Properties         General       Common         Image: Common       Replace         Source file(s):       :ubdomain.yourdomainname.org\Hosts\hosts         Destination File:       C:\Windows\System32\drivers\etc\hosts         Suppress errors on individual file actions         Attributes         Read-only         Hidden         Archive	<ul> <li>S. New File Properties, General tab: <ul> <li>a. Action: Select Replace from the drop-down</li> <li>b. Source file(s): Type in the network file share path or click to browse</li> <li>(Vyrservername.subdomain.yrdomain.org\Hosts\hosts</li> <li>c. Destination File: Type the location where you want to place the file, including the filename or click to browse</li> <li>C:Windows\System32\drivers\etc\hosts</li> <li>d. Uncheck Archive attribute</li> <li>e. Click OK</li> </ul> </li> </ul>
🛷 Files	

Group Policy Management Editor

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

Action

Replace

Source

Order

1

Name

💰 hosts

۲

Processing

Target

\\yourservername.subdomain.... C:\Windows\System32\drivers\etc\hosts



## 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 gpresult /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, <u>remove the user account you added when</u> 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) <u>https://technet.microsoft.com/library/cc755163.aspx</u>

Wbadmin Start sysrecovery 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

Server Manager https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager

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

Microsoft Operations Management Suite https://www.microsoft.com/en-us/cloud-platform/operations-management-suite.

Manager the Local Server and Server Manager Console <u>https://docs.microsoft.com/en-us/windows-server/administration/server-manager/manage-the-local-server-</u> 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

Missouri Research and Education Network  $\mathcal{W}$  University of Missouri System 221 N. Stadium Blvd., Ste. 201  $\mathcal{W}$  Columbia, MO 65203  $\mathcal{W}$  P: (573) 884-7200  $\mathcal{W}$  F: (573) 884-6673  $\mathcal{W}$  www.MORE.net <sup>164</sup>



## 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 <u>http://www.tactig.com/install-windows-server-step-by-step/</u> <u>http://www.tactig.com/install-active-directory-domain-services-ad-ds/</u> <u>http://www.tactig.com/promote-windows-server-domain-controller/</u>

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

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-internaldomain-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-removalwizard-page-descriptions#BKMK\_DepConfigPage

What is an RODC?

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-andremoval-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-andremoval-wizard-page-descriptions#BKMK\_DNSOptionsPage

Missouri Research and Education Network 🎾 University of Missouri System

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



AD DS Installation Wizard Page Descriptions: Additional Options

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-andremoval-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-andremoval-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-andremoval-wizard-page-descriptions#BKMK PrergCheckPage

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

Best Practices Analyzer for Active Directory Domain Services: Configuration <a href="https://technet.microsoft.com/en-us/library/dd391912(v=ws.10).aspx">https://technet.microsoft.com/en-us/library/dd391912(v=ws.10).aspx</a>

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

DSACLS, Directory Services Access Control Lists Utility: <u>https://technet.microsoft.com/en-us/library/cc771151(v=ws.11).aspx</u>

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

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: <u>https://technet.microsoft.com/en-us/library/dd197560(v=ws.10).aspx</u>

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

NETDOM, Windows Domain Manager: 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 <u>https://docs.microsoft.com/en-us/windows-server/networking/dns/what-s-new-in-dns-</u> server?f=255&MSPPError=-2147217396

Implement Domain Name System (sample chapter from Networking with Windows Server 2016) <a href="https://www.microsoftpressstore.com/articles/article.aspx?p=2756482">https://www.microsoftpressstore.com/articles/article.aspx?p=2756482</a>

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

DNS: Installing and Configuring Servers (as related to Windows Server 2008 R2) https://technet.microsoft.com/en-us/library/cc755183(v=ws.11).aspx

Optimizing your network to keep your DNS squeaky clean <a href="https://blogs.technet.microsoft.com/networking/2009/02/09/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/</a>

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 🕺



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

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

Understanding Reverse Lookup (as related to Windows Server 2008 R2) 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) <a href="http://technet.microsoft.com/en-us/library/cc730756.aspx">http://technet.microsoft.com/en-us/library/cc730756.aspx</a>

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

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

CIS (Center for Internet Security) Microsoft Windows Server 2012R2 Benchmark <u>https://www.cisecurity.org/wp-</u> content/uploads/2017/04/CIS\_Microsoft\_Windows\_Server\_2012\_R2\_Benchmark\_v2.2.0.pdf

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

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



Best Practices for Securing Active Directory <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-</u> <u>for-securing-active-directory</u> Active Directory Security Groups 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/securingdomain-controllers-against-attack

Securing Domain Controllers to Improve Active Directory Security <u>https://adsecurity.org/?p=3377</u>

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

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 <a href="https://technet.microsoft.com/en-us/library/dn319046(v=ws.11).aspx">https://technet.microsoft.com/en-us/library/dn319046(v=ws.11).aspx</a>

Audit Policy Recommendations, Windows Server 2016

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

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

Windows 10 and Windows Server 2016 security auditing and monitoring reference <a href="https://www.microsoft.com/en-us/download/details.aspx?id=52630">https://www.microsoft.com/en-us/download/details.aspx?id=52630</a>

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 169



#### **User Rights Assignment**

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

Network access: Allow anonymous DIS/name translation

https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-access-allowanonymous-sidname-translation

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

Network security: Force logoff when logon hours expire.

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

Network security:LAN Manager authentication level

https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/network-security-lanmanager-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 <u>https://www.petri.com/manage-local-active-directory-groups-using-group-policy-restricted-groups</u>

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

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

Missouri Research and Education Network 》 University of Missouri System

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



https://docs.microsoft.com/en-us/windows-server/security/windows-services/security-guidelines-fordisabling-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

Dynamic Access Control Overview

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

Blocking Unwanted Connections with a Hosts File <a href="http://winhelp2002.mvps.org/hosts.htm">http://winhelp2002.mvps.org/hosts.htm</a>

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

Group Policy Preferences https://technet.microsoft.com/en-us/library/dn581922(v=ws.11).aspx