
Windows Notes

Table of Contents

Table of Contents	1
Hardening Priorities	3
Downloads for Each Machine	3
Credentials	4
Important Info	4
First 15 Minutes Checklist	5
Phases	5
Administration Tasks from the Command Line	11
Configuration and Installation	11
Backing Up Everything	13
Networking and Firewall	14
Updates, Error Reporting, and Feedback	15
Windows Defender (Powershell)	16
Services, Processes, and Performance	16
Event Logs	17
Core NET Suite	17
Disk and File System	18
Hardware	18
Windows Server Backup	19
Net Share Commands	20
Applocker Commands	20
Setting up Active Directory, DNS, and DHCP on Server Core using PowerShell	22
Install and Configure Route and Remote Access Service on Server Core	25
Step by Step Installation of Active Directory on Windows Server 2019 Core	27

How to Build a Server 2016 Domain Controller (Non-GUI) and Make it Secure	32
How to Create and Delete a Network Share	36
Creating a File Share with PowerShell and Windows Server Core	37
Find all Hidden Network Shares	38
How to Patch Windows Server Core	39
Installing Splunk on Windows Server Core	40
Active Directory Hardening	50
MMC	53
IIS Hardening	55
IIS HTTP -> HTTPS	56

Hardening Priorities

Host	Who	Services
Dell 2 Core (dc1)	Liam	AD/DNS/DHCP
Dell 5 Gui (mgmt1)	Ally	Management/Utility/IIS
HyperV	Liam	Server 16
Dell 4 Spare	Ally	Possible Firewall
Dell 1 Workstation	Liam	DHCP Client
Dell 7 Traveler	Ally	Possible orange team use

Downloads for Each Machine

NMAP

RSAT

SYSinternals

Splunk Fowarder

Wireshark

Credentials

Name	Password	Name	Password

Important Info

Host	IP	Users

First 15 Minutes Checklist

Phases

1. Initial Setup + Documentation

#	Task	Steps/Command
1	Liam - DC Machine	<pre>net user eric * /add /domain /workstations:win1.blueteam.local net user liambackup * /add /domain /workstations:dc.blueteam.local net user lockout * /add /domain /workstations:dc.blueteam.local Net group liambackup "Domain Admins" /add /domain Net group lockout "Domain Admins" /add /domain Net user Allyhw * /add /domain /workstations:win1.blueteam.local Net group Allyhw "Domain Admins" /add /domain Net user allyhdhcp * /add /domain /workstations:dhcp.blueteam.local Net group allyhdhcp "Domain Admins" /add /domain Net user liamhdc * /add /domain /workstations:dc.blueteam.local Net group liamhdc "Domain Admins" /add /domain</pre>
2	Ally - Win1	Using Allyhw - Go over the backup and hardening Section
3	Ally - DHCP	Using allyhdhcp - Go over the backup and hardening Sections
4	Liam - DC	Using liamhdc - Go over Backup and Hardening sections Net user liamhadmin * /add /domain

		/workstations:admin.blueteam.local Net group liamhadmin "Domain Admins" /add /domain
5	Liam - Admin	Using liamhadmin - Go over Backup and Harden Download sysinternals
6	Liam - DC	Net user liamadc * /add /domain /workstations:admin.blueteam.local, dc.blueteam.local Net group liamadc "Domain Admins" /add /domain
7	Liam - Admin	Using liamadc Implement Group Policy
8	Liam / Ally - All	Confirm that all machines have - Changed User passwords Core backups Disable hardening accounts Create new Admin Account Rename old one
9	Liam / Ally - Take a breath	What do you call a fake noodle? An Impasta. I wouldn't buy anything with velcro. It's a total rip-off.

2. Backing Up Everything

#	Task	Steps/Command
1	Make a new folder c:/windows/Backup	Mkdir c:\windows\Backup Cd c:\windows\backup
2	Check network	Ipconfig /all Ipconfig /all > ipinfo.txt
3	Output of the workstation config	Net config workstation Net config workstation > workconf.txt
4	List users	Net user Net user > users.txt
5	List all services	net start net start > service.txt

6	List currently active services	Get-Service Where-Object {\$_.Status -eq "Running"}
7	List scheduled tasks	wmic startup get caption,command wmic startup get caption,command > startup.txt
8	List shares	Net shares Net shares > shares.txt
9	View registry	reg export hkey_local_machine\software\microsoft\windows %userprofile%\regbackup
10	The Service the machine is running	

3. Hardening

#	Task	Command
1	Lockdown local users	Net user Take note of users on sheet. Net user "username" /active:no
2	Put powershell into constrained language mode	[Environment]::SetEnvironmentVariable('__PSLockdownPolicy', '4', 'Machine')
3	Check constrained language mode settings	\$ExecutionContext.SessionState.LanguageMode
4	Get commands that launch on startup.	wmic startup get caption,command Make sure nothing looks too weird... consult google + partner
5	Disable Teredo	netsh interface teredo set state disabled
6	Check installed programs	Get-WmiObject -Class Win32_Product -ComputerName <remote_computer_name>
7	Uninstall any suspicious programs	\$app = Get-WmiObject -Class Win32_Product -Filter "Name = '<Package Name>'" \$app.Uninstall()
8	Check Shares for weirdness	Net share
9	Check for open Sessions	Net session

10	Check for listening ports	Netstat -at Netstat -abon
Firewall		
11	Limit workstation to workstation communication (Windows Firewall)	Do later with Admin GUI
12	Test psexec with good credentials between two workstations. If it works, you have a lateral movement problem.	psexec \RemotePCName [-u username[-p password]] command [arguments]
13	Block inbound traffic from internet	(Remind to do via the GUI on Admin machine)
14	Log everything to desktop	To start logging: Start-Transcript -Path "C:\transcripts\transcript0.txt" -NoClobber (Since the NoClobber parameter is used, the command prevents any existing files from being overwritten) To stop logging: trans = stop-transcript
Registry Edit		
15	Clear credentials of logged off users after 30 seconds (mimicking the behavior of Windows 8.1+)	Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecs = 30
16	Prevent Wdigest credentials being stored in memory, again as is the default for Windows 8.1+.	Set HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential = 0

4. GROUP POLICY

#	Task	Command
---	------	---------

1	Install Group Policy App	Add Under Roles and Features
2	Create Harden GPO	
	<p>Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment</p> <p>Deny Access to this computer from the network - Guests;ANON Logon</p> <p>Network security: LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM</p> <p>Network security: Do not store LAN Manager hash value on next password change - Enabled</p> <p>Network access: Do not allow anonymous enumeration of SAM accounts and shares - Enabled</p> <p>Network access: Do not allow anonymous enumeration of SAM accounts - Enabled</p> <p>Network access: Allow anonymous SID/name translation - Disabled</p> <p>Interactive logon: Message text for users attempting to log on - sometimes an inject</p> <p>Debug programs - Remove all groups/users</p> <p>Allow log on through Terminal Services - Leave blank to disallow login via TS even if it has been started.</p> <p>Interactive logon: Message text for users attempting to log on - sometimes an inject "That's against the student code of conduct."</p> <p>Computer Configuration > Administrative Templates > Windows Components > Windows Defender - Turn off Window Defender - Disabled</p> <p>Computer Configuration > Preferences > Windows Settings > Right click registry > New Registry Item</p> <ul style="list-style-type: none"> - Action: Create - Hive: HKEY_LOCAL_MACHINE - Key Path: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters - Value name: SMB1 - Value type: REG_DWORD - Value data: 0 <p>This Group Policy needs to be applied to all necessary workstations, servers, and domain controllers in the domain.</p>	
3	Create Audit Policy	Apply to All machines
	<p>Administrative Templates → Windows Components → Windows PowerShell</p> <p>1. Turn on Module - > Set *</p>	

	2. Scripting Block -> Log Script Block checked 3. Transcript -> Include Invo Checked CC -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Audit process tracking - Successes Audit account management - Successes, Failures Audit logon events - Successes, Failures Audit Account Lockout: S&F Audit Other Logon/Logoff Events: S&F Audit Special Logon: S&F	
4	Create Applocker Policy	Apply to Win1 to Test
	Create new Policy CC > POL > SEC > SYS > Application Identity App Locker create default policies Block Powershell Block User Folder	
5	Create Lockout Policy	
	Create new User lockout, with password Add a new OU Add Lockout to Lockout OU Set lockout threshold to 0 Enforce	
6	Create Service Lockdown	
	CC > POL > SEC > SYS > Disable: Remote Access Connection Manager, Remote Desktop Configuration, Remote Desktop Services, Telnet, IP Telephony, Print Spooler, Multimedia Class Scheduler	

5. System Administration

- a. Injects are always more important than whatever you think is.
- b. Run Ping Castle
- c. Install Splunk
 - i. Server location:
%SPLUNK_HOME%\etc\apps\SA-ModularInput-PowerShell
- d. ADRecon
- e. Bloodhound

6. Threat Hunting

Administration Tasks from the Command Line

Configuration and Installation

Task	Command
Set to local administrator password	net user administrator *
Join a computer to a domain	netdom join %computername% /domain:<domain> /userd:<domain\username> /passwordd:* <i>Restart the computer.</i>
Confirm that the domain has changed	set
Remove a computer from a domain	netdom remove <computername>
Add a user to the local Administrators group	net localgroup Administrators /add <domain\username>
Remove a user from the local Administrators group	net localgroup Administrators /delete <domain\username>
Add a user to the local computer	net user <domain\username> * /add
Add a group to the local computer	net localgroup <group name> /add
Change the name of a domain-joined computer	netdom renamecomputer %computername% /NewName:<new computer name> /userd:<domain\username> /passwordd: *
Confirm the new computer name	set
Change the name of a computer in a work group	netdom renamecomputer <currentcomputername> /NewName:<newcomputername> <i>Restart the computer.</i>
Disable paging file management	wmic computersystem where name="<computername>" set AutomaticManagedPagefile=False
Configure the paging file	wmic pagefileset where name="<path/filename>" set InitialSize=<initialsize>,MaximumSize=<maxsize>

	<p><i>Where path/filename is the path to and name of the paging file, initialsize is the starting size of the paging file, in bytes, and maxsize is the maximum size of the page file, in bytes.</i></p>
Change to a static IP address	<p>ipconfig /all <i>Record the relevant information or redirect it to a text file (ipconfig /all >ipconfig.txt).</i> netsh interface ipv4 show interfaces <i>Verify that there is an interface list.</i> netsh interface ipv4 set address name <ID from interface list> source=static address=<preferred IP address> gateway=<gateway address> <i>Run ipconfig /all to verify that DHCP enabled is set to No.</i></p>
Set a static DNS address	<p>netsh interface ipv4 add dnsserver name=<name or ID of the network interface card> address=<IP address of the primary DNS server> index=1 netsh interface ipv4 add dnsserver name=<name of secondary DNS server> address=<IP address of the secondary DNS server> index=2** <i>Repeat as appropriate to add additional servers.</i> <i>Run ipconfig /all to verify that the addresses are correct</i></p>
Change to a DHCP-provided IP address from a static IP address	<p>netsh interface ipv4 set address name=<IP address of local system> source=DHCP <i>Run Ipconfig /all to verify that DCHP enabled is set to Yes.</i></p>
Enter a product key	slmgr.vbs -ipk <product key>
Activate the server locally	slmgr.vbs -ato
Activate the server remotely	<p>cscript slmgr.vbs -ipk <product key><server name><username><password> cscript slmgr.vbs -ato <servername> <username> <password> <i>Get the GUID of the computer by running cscript slmgr.vbs -did</i> <i>Run cscript slmgr.vbs -dli <GUID></i> <i>Verify that License status is set to Licensed (activated).</i></p>

Backing Up Everything

Task	Command
Backup DNS	<pre>dnscmd DNS-SERVER /zoneexport "blah.com" "blahexport.txt"</pre> <p><i>Backup into txt file:</i></p> <pre>xcopy %systemroot%\system32\dns d:\backups\dns /y</pre>
Import DNS	<p>So the way to import a zone is as follows: first, copy the exported file into the c:\windows\system32\dns folder of the DNS server and preferably rename it so the extension is a .dns (not required, just a nice thing to do). Then run a command similar to below:</p> <pre>dnscmd DNS-SERVER /zoneadd "blah.com" /primary /file blah.com.dns</pre> <p>That's it. This will create a primary zone called "blah.com" and use the zone file that's already in the location.</p>
Backup DHCP (Powershell)	<pre>Backup-DhcpServer -ComputerName "dhcpserver.contoso.com" -Path "C:\Windows\system32\dhcp\backup"</pre>
Restore DHCP	<pre>Restore-DhcpServer -ComputerName "dhcpserver.contoso.com" -Path "C:\Windows\system32\dhcp\backup"</pre>
Export DHCP configs	<pre>Export-DhcpServer -ComputerName "dhcpserver.contoso.com" -File "C:\exportdir\dhcpxport.xml"</pre>
Backup CA	<pre>Backup-CARoleService -Path "C:\CABackup"</pre>
Backup GPO	<p>https://docs.microsoft.com/en-us/powershell/module/grouppolicy/backup-gpo?view=win10-ps</p>

Backup Active Directory	wbadmin start systemstatebackup -backupTarget:<VolumeName>
System State Backup	wbadmin start systemstatebackup -backupTarget:D:

Networking and Firewall

Task	Command
Configure your server to use a proxy server	netsh Winhttp set proxy <servername>:<port number> <i>Note: Server Core installations can't access the Internet through a proxy that requires a password to allow connections.</i>
Configure your server to bypass the proxy for internet addresses	netsh winhttp set proxy <servername>:<port number> bypass-list="<local>"
Display or modify IPSEC configuration	netsh ipsec
Display or modify NAP configuration	netsh nap
Display or modify IP to physical address translation	arp
Display or configure the local routing table	route
View or configure DNS server settings	nslookup
Display protocol statistics and current TCP/IP network connections	netstat
Display TCP/UDP connections	netstat /t Netstat /i
Display protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP (NBT)	nbtstat
Display hops for network connections	pathping
Trace hops for network connections	tracert
Display to configuration of the multicast router	mrinfo

Enable/Disable remote administration of the firewall	netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes
Get a new DHCP lease	ipconfig /release ipconfig /renew

Updates, Error Reporting, and Feedback

Task	Command
Install an update	wusa <update>.msu /quiet
List installed updates	systeminfo
Remove an update	expand /f:* <update>.msu c:\test <i>Navigate to c:\test\ and open <update>.xml in a text editor.</i> <i>Replace Install with Remove and save the file.</i> pkgmgr /n:<update>.xml
Configure automatic updates	<i>To verify the current setting:</i> cscript %systemroot%\system32\scregedit.wsf /AU /v ** <i>To enable automatic updates:</i> **cscript scregedit.wsf /AU 4 <i>To disable automatic updates:</i> cscript %systemroot%\system32\scregedit.wsf /AU 1
Enable error reporting	<i>To verify the current setting:</i> serverWerOptin /query <i>To automatically send detailed reports:</i> serverWerOptin /detailed <i>To automatically send summary reports:</i> serverWerOptin /summary <i>To disable error reporting:</i> serverWerOptin /disable
Participate in the Customer Experience Improvement Program (CEIP)	<i>To verify the current setting:</i> serverCEIPOptin /query <i>To enable CEIP:</i> serverCEIPOptin /enable <i>To disable CEIP:</i> serverCEIPOptin /disable

Windows Defender (Powershell)

<https://docs.microsoft.com/en-us/powershell/module/defender/index?view=win10-ps>

Task	Command
Get-MpComputerStatus	Gets the status of antimalware software on the computer.
Update-MpSignature	Updates the antimalware definitions on a computer.
Start-MpScan	Starts a scan on a computer.

Services, Processes, and Performance

Task	Command
Get commands that launch on startup.	wmic startup get caption,command
List the running services	sc query or net start
Start a service	sc start <service name> or net start <service name>
Stop a service	sc stop <service name> or net stop <service name>
Retrieve a list of running applications and associated processes	tasklist
Start Task Manager	taskmgr
Create and manage event trace session and performance logs	<i>To create a counter, trace, configuration data collection or API: logman ceate</i> <i>To query data collector properties: logman query</i> <i>To start or stop data collection: logman start stop</i> <i>To delete a collector: logman delete</i> <i>To update the properties of a collector: logman update</i> <i>To import a data collector set from an XML file or export it to an XML file: logman import export</i>

Event Logs

Task	Command
List event logs	wevtutil el
Query events in a specified log	wevtutil qe /f:text <log name>
Export an event log	wevtutil epl <log name>
Clear an event log	wevtutil cl <log name>

Core NET Suite

Task	Command
Get help on all the parts	Net help <command>
Groups that exist on the machine Look for Administrators, Backup Operators, Network Configuration Operators, Crypto Operators, Remote Desktop Users, Users	net localgroup Net localgroup <group>
Output of the workstation config	net config workstation
See all shares on the machine	net share NET SHARE <share> NET SHARE <share> \delete
List users on the machine	Net user /active:{yes no} /passwordchg:{yes no} (can user change thier password) /logonpasswordchg:{yes no} /workstations:{computername[,...] *} (what computer can you log onto)
List all sessions connected to this machine	NET SESSION
Disconnect all sessions connected to this machine (without any prompts)	NET SESSION /DELETE /y

Create user for one machine	Net user <username> * /add /passwordchg:no /workstations:<machine> Net group "Domain Admins" Testtest /add /domain
-----------------------------	---

Disk and File System

Task	Command
Manage disk partitions	<i>For a complete list of commands, run diskpart /?</i>
Manage software RAID	<i>For a complete list of commands, run diskraid /?</i>
Manage volume mount points	<i>For a complete list of commands, run mountvol /?</i>
Defragment a volume	<i>For a complete list of commands, run defrag /?</i>
Convert a volume to the NTFS file system	convert <volume letter> /FS:NTFS
Compact a file	<i>For a complete list of commands, run compact /?</i>
Administer open files	<i>For a complete list of commands, run openfiles /?</i>
Administer VSS folders	<i>For a complete list of commands, run vssadmin /?</i>
Administer the file system	<i>For a complete list of commands, run fsutil /?</i>
Take ownership of a file or folder	<i>For a complete list of commands, run icacls /?</i>

Hardware

Task	Command
Add a driver for a new hardware device	<i>Copy the driver to a folder at %homedrive%\<driver folder>. Run pnputil -i -a %homedrive%\<driver folder>\<driver>.inf</i>

Remove a driver for a hardware device	<i>For a list of loaded drivers, run <code>sc query type=driver</code>. Then run <code>sc delete <service_name></code></i>
---------------------------------------	--

Windows Server Backup

Task	Command
Configures and enables a daily backup schedule	<code>Wbadmin enable backup</code>
Disables your daily backups	<code>Wbadmin disable backup</code>
Runs a one-time backup. If used with no parameters, uses the settings from the daily backup schedule.	<code>Wbadmin start backup</code>
Stops the currently running backup or recovery operation.	<code>Wbadmin stop job</code>
Lists details of backups recoverable from the local computer or, if another location is specified, from another computer.	<code>Wbadmin get versions</code>
Lists the items included in a specific backup.	<code>Wbadmin get items</code>
Runs a recovery of the volumes, applications, files, or folders specified.	<code>Wbadmin start recovery</code>
Shows the status of the currently running backup or recovery operation.	<code>Wbadmin get status</code>
Lists disks that are currently online.	<code>Wbadmin get disks</code>
Runs a system state recovery.	<code>Wbadmin start systemstaterecovery</code>
Runs a system state backup.	<code>Wbadmin start systemstatebackup</code>
Deletes one or more system state backups.	<code>Wbadmin delete systemstatebackup</code>
Runs a recovery of the full system (at least all the volumes that contain the operating system's state). This subcommand is only available if you are using the Windows Recovery Environment.	<code>Wbadmin start sysrecovery</code>
Recovers a backup catalog from a specified storage location in the case where the backup catalog on the local computer has been corrupted.	<code>Wbadmin restore catalog</code>

Deletes the backup catalog on the local computer. Use this command only if the backup catalog on this computer is corrupted and you have no backups stored at another location that you can use to restore the catalog.	Wbadmin delete catalog

Net Share Commands

Task	Command
Share folder with everyone in the domain and to give full permissions	net share Docs=<folder path> /grant:everyone,FULL
Limiting number of users to access the share	net share Docs=<folder path> /grant:everyone,FULL /users:<amount of user>
Command to share with a specific user and to grant only read rights	net share Docs=<folder path> /grant:username,READ
Delete network share(i.e to disable sharing of the folder) from command line	net share sharename /delete
List the shared creating on the local computer	Net share
Delete the share on a remote computer	Net share sharename \\remotepc /delete
Accessing shares on core through firewall	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes

Applocker Commands

Task	Command
Retrieve application information	Get-AppLockerFileInformation
Set AppLocker policy	Set-AppLockerPolicy
Retrieve an AppLocker policy	Get-AppLockerPolicy
Generate rules for a given user or group	New-AppLockerPolicy

Test AppLocker policy against a file set	Test-AppLockerPolicy
Help	Get-Help -Name Get-AppLockerPolicy

Setting up Active Directory, DNS, and DHCP on Server Core using PowerShell

```
Select Administrator: C:\Windows\system32\cmd.exe - powershell

PS C:\Users\Administrator> Get-Service adws,kdc,netlogon,dns

Status      Name      DisplayName
-----
Running     adws      Active Directory Web Services
Running     dns       DNS Server
Running     kdc       Kerberos Key Distribution Center
Running     Netlogon  netlogon

PS C:\Users\Administrator> Get-SMBShare

Name      ScopeName Path      Description
-----
ADMIN$    *        C:\Windows Remote Admin
C$        *        C:\       Default share
IPC$      *        C:\       Remote IPC
NETLOGON  *        C:\Windows\SYSVOL\sysvol\test.local\SCRIPTS Logon server share
SYSVOL    *        C:\Windows\SYSVOL\sysvol Logon server share
```

Get the server ready

That includes

- Setting up network settings with a static IP for the server;
- Assigning a meaningful NetBIOS name (ComputerName);
- Install all updates to keep the system up-to-date;
- Activate the Windows Server installation;

You can use either the PowerShell cmdlets such as **New-NetIPAddress** and **Set-DNSClientServerAddress** to make these changes or the Server Core built-in tool **sconfig.exe** if you would like something easier.

Install Active Directory Service

Start with

```
Install-WindowsFeature -Name AD-Domain-Services
```

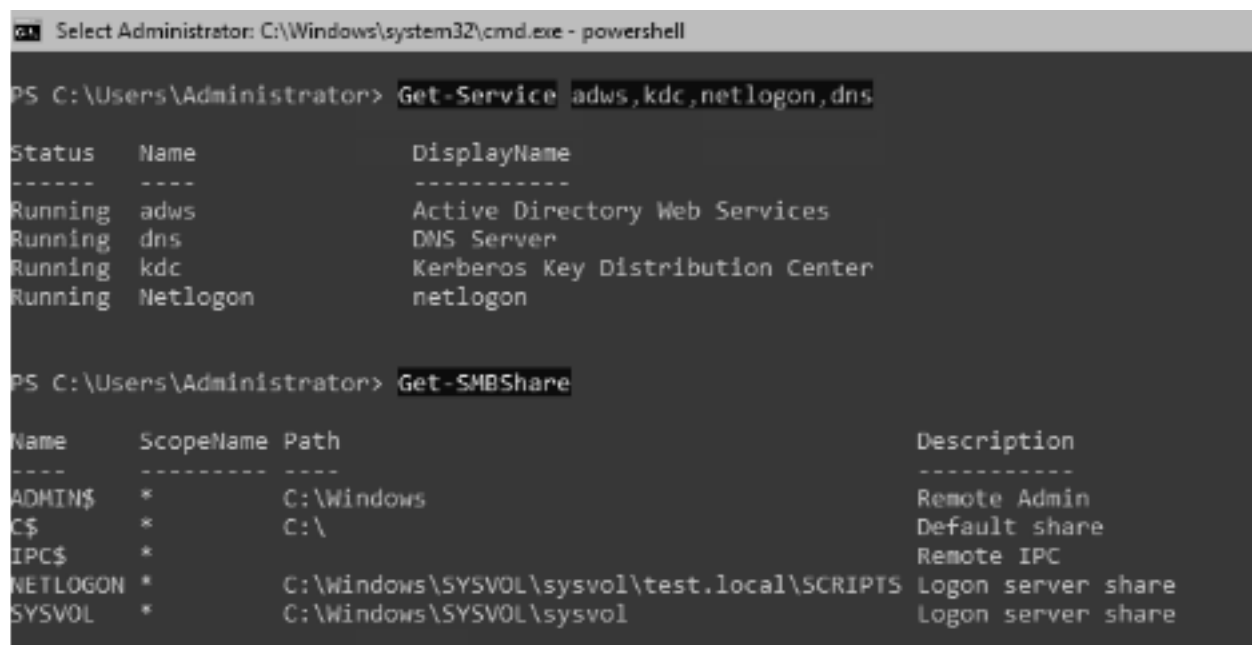
to install the Active Directory server role. No restart needed.

And then

```
Install-ADDSForest -DomainName test.local
```

to install the first Forest with the name test.local. You will need to provide the **safemodeadministratorpassword** and confirm the server to be configured and rebooted afterward along the way. Note that the DNS server will be installed and properly configured automatically during the process.

Once rebooted, use **DCDiag** to verify the new Domain Controller and make sure the AD and DNS services are running and **sysvol** and **netlogon** shares are properly configured.



The screenshot shows a PowerShell terminal window titled "Select Administrator: C:\Windows\system32\cmd.exe - powershell". The user is running the command `Get-Service adws,kdc,netlogon,dns`. The output is a table with columns Status, Name, and DisplayName. All four services (adws, dns, kdc, Netlogon) are listed as "Running". Below this, the user runs `Get-SMBShare`, which outputs a table with columns Name, ScopeName, Path, and Description. It lists shares ADMIN\$, C\$, IPC\$, NETLOGON, and SYSVOL, with their respective paths and descriptions.

Status	Name	DisplayName
Running	adws	Active Directory Web Services
Running	dns	DNS Server
Running	kdc	Kerberos Key Distribution Center
Running	Netlogon	netlogon

Name	ScopeName	Path	Description
ADMIN\$	*	C:\Windows	Remote Admin
C\$	*	C:\	Default share
IPC\$	*		Remote IPC
NETLOGON	*	C:\Windows\SYSTEM32\sysvol\test.local\SCRIPTS	Logon server share
SYSVOL	*	C:\Windows\SYSTEM32\sysvol	Logon server share

Now let's add a first user account using

```
New-ADUser -Name kent -AccountPassword(Read-Host -AsSecureString  
"AccountPassword") -PassThru | Enable-ADAccount
```

Type in the password twice and it's all set. And then use

```
ADD-ADGroupMember
```

to add the newly created user to the group you would like, such as **Administrators** group.

Install DHCP Service

Start with

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

And then use

```
Add-DHCPServerv4Scope -Name "Internal" -StartRange 192.168.30.51 -EndRange 192.168.30.100 -SubnetMasking 255.255.255.0 -State Active
```

to add a new DHCP scope and use

```
Set-DHCPServerv4OptionValue -ScopeID 192.168.30.0 -DnsDomain test.local -DnsServer AD-IP -Router IP-of-Router
```

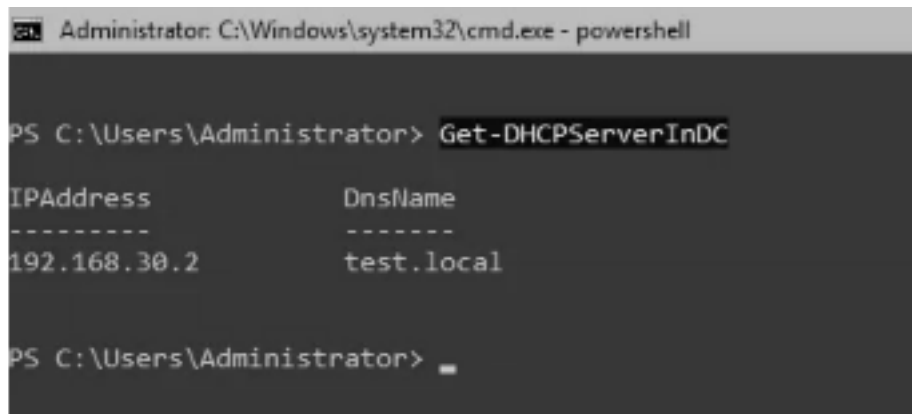
to set up the DHCP options.

The final step, use

```
Add-DHCPServerInDC -DnsName test.local -IPAddress IP-of-DC
```

to authorize the DHCP server to operate in the specified domain.

To verify, use **Get-DHCPServerInDC**.



```
Administrator: C:\Windows\system32\cmd.exe - powershell

PS C:\Users\Administrator> Get-DHCPServerInDC

IPAddress          DnsName
-----
192.168.30.2       test.local

PS C:\Users\Administrator>
```


Install and Configure Route and Remote Access Service on Server Core

Install the remote Access Server Role

1. On Server Core console, type **PowerShell** to start.

2. Install Remote Access feature by

```
Install-WindowsFeature RemoteAccess
```

Then, type **Restart-Computer** to restart the computer.

3. Once rebooted, install Remote Access PowerShell module by:

```
Install-WindowsFeature RSAT-RemoteAccess-PowerShell
```

No need to restart the computer.

4. Install the Routing feature by:

```
Install-WindowsFeature Routing
```

Type **Restart-Computer** to restart the computer.

Configure and Enable Routing

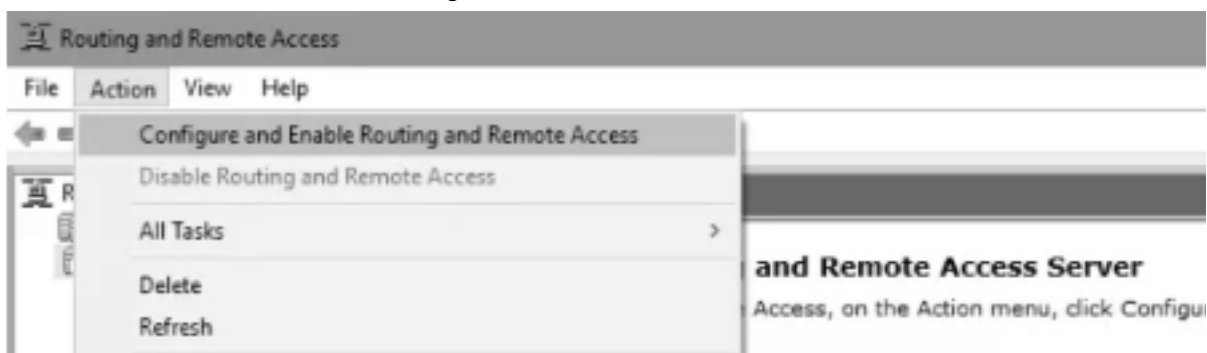
Launch **Remote Access Management Console** and click **Manage a Remote Server** on the right Tasks list.



Once connected successfully, click **DirectAccess and VPN** on the left pane and Open **RRAS Management** under VPN on the right.



In Route and Remote Access, click **Action** and choose **Configure and Enable Routing and Remote Access** to launch the configuration wizard.



Select **Network address translation (NAT)** option from the list, and Next.



Select the NIC that has internet access to Provide internet and the private Virtual Switch for VMs as the Internal Network. If all go well as planned, you will be up and running in a few seconds.

Step by Step Installation of Active Directory on Windows Server 2019 Core

To install Active Directory, we need to set our Server as per the recommended configuration for AD.

- System Name
- Static IP
- Date and Time

This will make sure that everything is set as per the recommendation. Once your server is ready, open the command prompt and type *start PowerShell*

Then, you need to run the *sconfig command*. This gives you the system details.

Next, we need to change the system name. It will prompt you to restart the system.

The next step will be to set the static IP for the system.

By opening PowerShell, type the following commands.

Run

Get-NetAdapter

This will give the name of the adapter which we will use as the interface alias.

```
$ipaddress = "10.0.64.2"
```

```
$dnsaddress = "127.0.0.1"
```

```
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress -AddressFamily IPv4 -PrefixLength 24
```

```
C:\Users\Administrator> $ipaddress = "10.0.64.2"  
C:\Users\Administrator> $dnsaddress = "127.0.0.1"  
C:\Users\Administrator> New-NetIPAddress -InterfaceAlias Ethernet -IPAddress $ipaddress -AddressFamily IPv4 -PrefixLength 24
```

Update DNS

`Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses $dnsaddress`

A screenshot of a PowerShell terminal window. The prompt is 'PS C:\Users\Administrator\Documents>'. The command entered is 'Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses \$dnsaddress'. The command is highlighted in blue.

```
PS C:\Users\Administrator\Documents> Set-DnsClientServerAddress -InterfaceAlias Ethernet -ServerAddresses $dnsaddress
```

Once done, restart the server.

Now, let us set the time zone. For that, type the following commands in PowerShell.

Get-timezone

Set-TimeZone -Id "Eastern Standard Time"

Once everything is set, it will start installing AD Service.

We can do the installation in two ways here.

- Windows Admin Center (this will help you to install roles and features but to configure the same, we need to use PowerShell only).
- PowerShell command

Using Windows Admin Center

For Windows Admin Center, we need to set up and add a server.

Once the server is connected to Windows Admin Center, you need to connect the server.

A screenshot of the Windows Admin Center interface showing a list of servers. The table has columns for Name, Type, Last Connected, Managing As, and Tags. There are three servers listed: 'id' (Windows PC), 'test' (Server), and 'win-2016-09-14' (Server). The 'test' server is selected.

Name ↑	Type	Last Connected	Managing As	Tags
id	Windows PC	Never	KR@luna1	
test	Server	8/8/2018 10:41:11 PM	administrator	
win-2016-09-14	Server	8/8/2018 9:17:09 PM	KR@luna1	

Once the server is connected, you will find the overview of the system utilization page.

On the left side tools, you have to select Roles & features. Now you can select whichever role you need to install and click Install.

This will start checking dependencies

It will give you a list of the roles you are going to install.

You will find a notification window with a progress update there.

Using PowerShell

PowerShell Command to start creating Domain Controller

Get-WindowsFeature AD-Domain-Service | Install-WindowsFeature

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-WindowsFeature AD-Domain-Service | Install-WindowsFeature
```

Import-Module ADDSDeployment

Install-ADDSForest

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-WindowsFeature AD-Domain-Service | Install-WindowsFeature

PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator> Install-ADDSForest

cmdlet Install-ADDSForest at command pipeline position 1
Supply values for the following parameters:
DomainName: teammicro.dom
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): _
```

This will ask you for the Domain Name and SafeMode password. Make sure you write this down in a safe place. It will be very useful in case of disaster recovery.

You can select Y or A as an answer to the question.

While installation is going on you will see some warning.

```
C:\Administrator: Windows PowerShell
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Install-ADFSForest

Validating environment and user input
Verifying prerequisites for domain controller operation...
[ ]

True No NoChangeNeeded {}

PS C:\Users\Administrator> Import-Module ADOSDeployment
PS C:\Users\Administrator> Install-ADFSForest

cmdlet Install-ADFSForest at command pipeline position 1
Supply values for the following parameters:
DomainName: teammicro.dom
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
WARNING: Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography
algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security
channel sessions.

For more information about this setting, see Knowledge Base article 942564
(http://go.microsoft.com/fwlink/?LinkID=104751).
```

Once everything is done the server will reboot automatically.

Once a server is ready we will create a new Admin user which helps admin to do day to day work.

New-ADUser -Name "Helpdesk" -GivenName Help -Surname Desk -SamAccountName Helpdesk
-UserPrincipalName Helpdesk@teammicro.dom

To verify the user details:

Get-ADUser Helpdesk

You will find the user is not active yet. Before enabling the user, set the password for that user.

Command to set password:

Set-ADAccountPassword 'CN=Helpdesk,CN=users,DC=Teammicro,DC=Dom' -Reset
-NewPassword (ConvertTo-SecureString -AsPlainText "Test@123" -Force)

```
PS C:\Users\Administrator> Set-ADAccountPassword 'CN=Helpdesk,CN=users,DC=Teammicro,DC=Dom' -Reset -NewPassword (Convert
To-SecureString -AsPlainText "Test@123" -Force)
PS C:\Users\Administrator>
```

Enable the AD user

Enable-ADAccount -Identity Helpdesk

```
PS C:\Users\Administrator> Enable-ADAccount -Identity Helpdesk
PS C:\Users\Administrator> █
```

Add the user to Domain Admins group

Add-AdGroupMember 'Domain Admins' Helpdesk

```
PS C:\Users\Administrator> Add-ADGroupMember 'Domain Admins' Helpdesk
PS C:\Users\Administrator> █
```

Now it will configure over Active Directory and be ready for use.

How to Build a Server 2016 Domain Controller (Non-GUI) and Make it Secure

To get started and if you haven't already done so you will need to download a copy of Server 2016. I downloaded an evaluation copy from the TechNet Evaluations website.

URL: <https://www.microsoft.com/en-us/evalcenter/>

This next part assumes you have already installed server 2016.

One very important command to remember when you log in for the first time is the "sconfig" command. When you invoke this command you will be met with a blue screen with several numeric options.

Run option 6 immediately. This option will help you install security updates to your server. It's a very straight forward process.

The other options you will need to do is #2 to create a computer name. #8 configure a static IP to your server and #9 to ensure the date and time are correct. Once you are finished with these options you can choose #15 and exit to the command line. Run powershell.exe on the next steps.

Powershell Commands to create your first domain controller

Get-WindowsFeature AD-Domain-Services | Install-WindowsFeature



Import-Module ADDSDeployment
Install-ADDSForest

```
PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator> Install-ADDSForest

cmdlet Install-ADDSForest at command pipeline position 1
Supply values for the following parameters:
DomainName: contoso.com
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A_
```

You will see several warnings these are normal.

Creating a domain account with domain admin access through powershell

(This will create a user)

Example powershell code:

```
New-ADUser -Name "rootsecdev" -GivenName Root -Surname Secdev -SamAccountName pgibbins
-UserPrincipalName rootsecdev@contoso.com
```

Here is a look at the user that we just created. Take note that this account is not enabled and see the entire distinguished name of where it is sitting

Example powershell code:

```
Get-ADUser rootsecdev
```

Next Example is to set a password for this account. We need to set a password before we can enable this account. Remember this is an example. I suggest creating a stronger password than what I am doing below.

Example:

Set-ADAccountPassword 'CN=rootsecdev,CN=users,DC=contoso,DC=com' -Reset -NewPassword
(ConvertTo-SecureString -AsPlainText "p@ssw0rd" -Force)

Lets go ahead and enable the AD object with the following:

Enable-ADAccount -Identity rootsecdev

Next we will add Domain Admin membership to the new user.

Example:

Add-ADGroupMember 'Domain Admins' rootsecdev

```
PS C:\Users\Administrator> ADD-ADGroupMember 'Domain Admins' rootsecdev
PS C:\Users\Administrator> _
```

At this point we can log out of the domain controller and set up a Windows 10 Client machine and add it to the contoso.com domain. I'm not going over that because the purpose of this is to secure the domain controller.

We will need a few things for your Windows 10 client after you add it to the domain.

Windows 10 RSAT: <https://www.microsoft.com/en-us/download/details.aspx?id=45520>

Server 2016 and Windows 10 Security Baselines: (Download file and unzip)
<https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/>

Open the group policy management console and create a blank GPO called "2016 DC Security".
Right click on the Blank GPO and select import settings. A wizard screen will appear.

Navigate to the security compliance file that you unzipped earlier and select the GPO directory.

Select the Domain Controller Baseline and then click on next

Select Copy them identically from the source and select next

From this point you can finish and your import should complete. You can not link it to the domain controllers OU. After you do I would do a gpupdate /force on your domain controller and reboot it.

It also isn't a bad idea to import the rest of the policy's and take a look at them. The domain security (which contains password policies) and the User security policies is something you should do also.

How to Create and Delete a Network Share

To create a network share in a Windows 2008 Server Core computer, use **net share** command as shown below.

```
C:\>net share MyShare=C:\MyShare  
MyShare was shared successfully.
```

Here, the shared folder is C:\MyShare and it is shared using the share name "MyShare". By default, Windows will assign read permission to Everyone when a share is created without specifying any permissions.

If you want to grant specific permissions to individual users or groups, for the network share, use the **net share** command with /GRANT option as shown below.

```
C:\>net share MyShare=C:\MyShare /GRANT:jajish,FULL  
MyShare was shared successfully.
```

If you want to create a network share with everyone full access, use the **net share** command as shown below

```
C:\>net share MyShare=C:\MyShare /GRANT:Everyone,FULL  
MyShare was shared successfully.
```

If you want to create a share with only read permission for a user, use the **net share** command as shown below.

```
C:\>net share MyShare=C:\MyShare /GRANT:tintin,read  
MyShare was shared successfully.
```

To create a network share with comments use the **net share** command with /REMARK option as shown below.

```
C:\>net share MyShare=C:\MyShare /GRANT:Everyone,FULL /REMARK:"Applications and  
Files"  
MyShare was shared successfully.
```

To delete a network share, use the **net share** command as shown below. Remember, only "share" is deleted, folder will not be deleted.

```
C:\>net share MyShare /DELETE  
MyShare was deleted successfully.
```

Creating a File Share with PowerShell and Windows Server Core

With Windows Server Core, you don't have all the old GUI tools that we're all used to. So you have to make do with PowerShell and the old fake DOS prompt. Fortunately, with a little help, it's pretty easy.

First, create the folder you want to share. In this case, c:\share

Next, modify the ACL to grant the DOMAIN\File Server Admins group full control

```
$sharepath = "c:\share"
$Acl = Get-ACL $SharePath
$AccessRule= New-Object System.Security.AccessControl.FileSystemAccessRule("DOMAIN\File
Server Admins","full","ContainerInherit,ObjectInherit","none","Allow")
$Acl.AddAccessRule($AccessRule)
Set-Acl $SharePath $Acl
```

Finally, create the share and grant everyone full access.

```
NET SHARE sharename=c:\share "/GRANT:Everyone,FULL"
```

Find all Hidden Network Shares

I have a Windows file server with thousands of shares. Occasionally, create hidden shares for data migration or other administrative tasks. How do you find these shares?

Some websites suggest running `Get-WmiObject -Class Win32_Share` and piping the output of that to `Where-Object` to filter. That can work, but it has the computer send you all the share objects. If you want to run this command to get shares from a remote computer, this is highly inefficient.

Instead, we can specify a filter in the initial `Get-` cmdlet. I'm also going to switch to the `Get-CimInstance` cmdlet, which is optimized for remote execution.

```
PS Z:\> Get-CimInstance -ComputerName ServerName -ClassName Win32_Share  
-Filter 'Type = "0" AND Name LIKE "%$"'
```

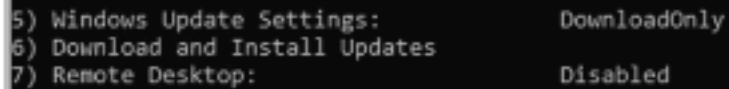
The `Filter` parameter uses a [WQL query](#) to specify that I want regular shares (not administrative shares like `C$` or `IPC$`; see the [Win32_Share class doc](#) for details) AND whose names end with a dollar sign. It may not return data much faster, but it sends much less data over the wire, which is important especially for remote scenarios.

How to Patch Windows Server Core

The SCONFIG utility offers 90% of the required administrative tasks and options.

To access the SCONFIG, simply type SCONFIG.

To access the updates menu, Select option 6 from the SCONFIG menu



```
5) Windows Update Settings:      DownloadOnly
6) Download and Install Updates
7) Remote Desktop:              Disabled
```

Click A for all updates, this will Install available updates for Server Core

Once all the updates have downloaded, Select A to start the Installation process

Once done, You will get a prompt to restart the Server

Installing Splunk on Windows Server Core

Invoke **msiexec.exe** to install Splunk Enterprise from the command line or a PowerShell prompt.

For 32-bit platforms, use **splunk-<...>-x86-release.msi**:
msiexec.exe /i splunk-<...>-x86-release.msi [<flag>]... [/quiet]

For 64-bit platforms, use **splunk-<...>-x64-release.msi**:
msiexec.exe /i splunk-<...>-x64-release.msi [<flag>]... [/quiet]

The value of <...> varies according to the particular release; for example,

splunk-6.3.2-aaff59bb082c-x64-release.msi.

Command-line flags let you configure Splunk Enterprise at installation. Using command-line flags, you can specify a number of settings, including but not limited to:

- Which Windows event logs to index.
- Which Windows Registry hives to monitor.
- Which Windows Management Instrumentation (WMI) data to collect.
- The user Splunk Enterprise runs as. See Choose the Windows user Splunk Enterprise should run as for information about what type of user you should install your Splunk instance with.
- An included application configuration for Splunk to enable (such as the light forwarder.)
- Whether Splunk Enterprise should start automatically when the installation is finished.

Supported Flags:

Flag	Purpose	Default
AGREETOLICENSE=Yes No	Use this flag to agree to the EULA. You must set this flag to Yes to perform a silent installation. The flag does not work when you click the MSI to start installation.	No
INSTALLDIR="<directory_path>"	Use this flag to specify directory to install. The Splunk	C:\Program Files\Splunk

	Enterprise installation directory is referred to as \$SPLUNK_HOME or %SPLUNK_HOME% throughout this documentation set.	
SPLUNKD_PORT=<port number>	Use this flag to specify alternate ports for splunkd and splunkweb to use. If you specify a port and that port is not available, Splunk Enterprise automatically selects the next available port.	8089
WEB_PORT=<port number>	Use this flag to specify alternate ports for splunkd and splunkweb to use. If you specify a port and that port is not available, Splunk Enterprise automatically selects the next available port.	8000
WINEVENTLOG_APP_ENABLE=1/0 WINEVENTLOG_SEC_ENABLE=1/0 WINEVENTLOG_SYS_ENABLE=1/0 WINEVENTLOG_FWD_ENABLE=1/0 WINEVENTLOG_SET_ENABLE=1/0	Use these flags to specify whether or not Splunk Enterprise should index a particular Windows event log. You can specify multiple flags: Application log Security log System log Forwarder log Setup log	Off
REGISTRYCHECK_U=1/0 REGISTRYCHECK_BASELINE_U=1/0	Use these flags to specify whether or not Splunk Enterprise should index events from capture a baseline snapshot of the Windows Registry user hive (HKEY_CURRENT_USER). Note: You can set both of these at the same time.	Off

<p>REGISTRYCHECK_LM=1/0 REGISTRYCHECK_BASELINE_LM=1/0</p>	<p>Use these flags to specify whether or not Splunk Enterprise should index events from capture a baseline snapshot of the Windows Registry machine hive (HKEY_LOCAL_MACHINE). Note: You can set both of these at the same time.</p>	<p>Off</p>
<p>WMICHECK_CPUTIME=1/0 WMICHECK_LOCALDISK=1/0 WMICHECK_FREEDISK=1/0 WMICHECK_MEMORY=1/0</p>	<p>Use these flags to specify which popular WMI-based performance metrics Splunk should index: CPU usage Local disk usage Free disk space Memory statistics Note: If you need this instance of Splunk Enterprise to monitor remote Windows data, then you must also specify the LOGON_USERNAME and LOGON_PASSWORD installation flags. Splunk Enterprise cannot collect any remote data that it does not have explicit access to. Additionally, the user you specify requires specific rights, administrative privileges, and additional permissions, which you must configure before installation. Read "Choose the Windows user Splunk Enterprise should run as" in this manual for additional information about the required credentials. There are many more WMI-based metrics that Splunk can index. Review "Monitor WMI Data" in the</p>	<p>Off</p>

	Getting Data In Manual for specific information.	
LOGON_USERNAME="<domain\username>" LOGON_PASSWORD="<password>"	<p>Use these flags to provide domain\username and password information for the Windows user that Splunk Enterprise will run as. The splunkd and splunkweb services are configured with these credentials. For the LOGON_USERNAME flag, you must specify the domain with the username in the format "domain\username." Do not use this flag to set the Splunk administrator password.</p> <p>These flags are mandatory if you want this Splunk Enterprise installation to monitor any remote data. Review "Choose the Windows user Splunk Enterprise should run as" in this manual for additional information about which credentials to use.</p>	None
SPLUNK_APP="<SplunkApp>"	<p>Use this flag to specify an included Splunk application configuration to enable for this installation of Splunk Enterprise. Currently supported options for <SplunkApp> are: SplunkLightForwarder and SplunkForwarder. These specify that this instance of Splunk will function as a light forwarder or heavy forwarder, respectively. Refer to the "About forwarding and receiving" topic in the</p>	None

	<p>Forwarding Data manual for more information.</p> <p>If you specify either the Splunk forwarder or light forwarder here, you must also specify FORWARD_SERVER="<server:port>".</p> <p>To install Splunk Enterprise with no applications at all, omit this flag.</p> <p>Note: The full version of Splunk Enterprise does not enable the universal forwarder. The universal forwarder is a separate downloadable executable, with its own installation flags.</p>	
FORWARD_SERVER="<server:port>"	<p>Use this flag only when you also use the SPLUNK_APP flag to enable either the Splunk heavy or light forwarder.</p> <p>Specify the server and port of the Splunk server to which this forwarder will send data.</p>	None
DEPLOYMENT_SERVER="<host:port>"	<p>Use this flag to specify a deployment server for pushing configuration updates. Enter the deployment server name (hostname or IP address) and port.</p>	None
LAUNCHSPLUNK=0/1	<p>Use this flag to specify whether or not Splunk software should start up after the installation completes, and automatically when the machine boots.</p> <p>Note: If you enable the Splunk Forwarder by using the SPLUNK_APP flag, the installer configures Splunk to start automatically, and ignores this flag.</p>	1 (on)

INSTALL_SHORTCUT=0/1	Use this flag to specify whether or not the installer should create a shortcut to Splunk on the desktop and in the Start Menu.	1 (on)
SPLUNKUSERNAME=<username>	Create a username for the Splunk administrator user. If you specify a quiet installation with the /quiet flag and do not specify this setting, then the software uses the default value of admin, but you must still specify a password with the SPLUNKPASSWORD or GENRANDOMPASSWORD flags for the installation to add the credentials successfully.	admin
SPLUNKPASSWORD=<password>	Create a password for the Splunk admin user. The password must meet eligibility requirements. If you specify a quiet installation with the /quiet flag and do not specify this flag or the SPLUNKUSERNAME flag, then the software installs without a user, and you must create one by editing the user-seed.conf configuration file.	N/A
MINPASSWORDLEN=<positive integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDLEN flag specifies the minimum length that a password must be to meet these eligibility requirements going forward. It cannot be set to 0 or a negative integer. Any new	> 1

	password you create and any existing password you change must meet the new requirements after you set this flag.	
MINPASSWORDDIGITLEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDDIGITLEN flag specifies the minimum number of numeral (0 through 9) characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
MINPASSWORDLOWERCASELEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDLOWERCASELEN flag specifies the minimum number of lowercase ('a' through 'z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must	0

	meet the new requirements after you set this flag.	
MINPASSWORDUPPERCASE LEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDUPPERCASELEN flag specifies the minimum number of uppercase ('A' through 'Z') characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. Any new password you create and any existing password you change must meet the new requirements after you set this flag.	0
MINPASSWORDSPECIALCHARLEN=<integer>	When using the SPLUNKPASSWORD flag to set a password, you can also set password eligibility requirements for password creation and modification. The MINPASSWORDSPECIALCHARLEN flag specifies the minimum number of special characters that a password must contain to meet these eligibility requirements going forward. It cannot be set to a negative integer. The ':' (colon) character cannot be used as a special character. Any new password you create and any existing password you change must meet the new	0

	requirements after you set this flag.	
GENRANDOMPASSWORD=1 /0	Generate a random password for the admin user and write the password to the installation log file. The installer writes the credentials to %TEMP%\splunk.log. After the installation completes, you can use the findstr utility to search that file for the word "PASSWORD". After you get the credentials, delete the installation log file, as retaining the file represents a significant security risk.	0

Silent installation:

To run the installation silently, add /quiet to the end of your installation command string. If your system has User Access Control enabled (the default on some systems), you must run the installation as Administrator. To do this:

- When opening a command prompt or PowerShell window, right click on the app icon and select "Run As Administrator".
- Use this command window to run the silent install command.

Examples:

Silently install Splunk Enterprise to run as the Local System Windows user and set the Splunk administrator credentials to "SplunkAdmin/MyNewPassword":

```
msiexec.exe /I Splunk.msi SPLUNKUSER=SplunkAdmin SPLUNKPASSWORD=MyNewPassword
/quiet
```

Enable the Splunk heavy forwarder and specify credentials for the user Splunk Enterprise should run as:


```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder"  
SPLUNKPASSWORD=MyNewPassword FORWARD_SERVER="<server:port>"  
LOGON_USERNAME="AD\splunk" LOGON_PASSWORD="splunk123"
```

Enable the Splunk heavy forwarder, generate a random password for the default Splunk administrator user, enable indexing of the Windows System event log, and run the installer in silent mode:

```
msiexec.exe /i Splunk.msi SPLUNK_APP="SplunkForwarder" GENRANDOMPASSWORD=1  
FORWARD_SERVER="<server:port>" WINEVENTLOG_SYS_ENABLE=1 /quiet
```

Where "<server:port>" are the server and port of the Splunk server to which this machine should send data.

Install Splunk Enterprise with verbose logging to C:\TEMP\SplunkInstall.log:

```
msiexec.exe /i Splunk.msi /l*v C:\TEMP\SplunkInstall.log
```

Active Directory Hardening

1. Go into Active Directory Users and Computers
2. Expand Server Local and Users
3. Add a user -> right click new -> users
 1. Create a new user with name and complex password (use random name)
 2. Uncheck box saying to change password at first login
4. Right click on new user, properties
 1. Member of
 2. Add
 3. Advanced
 4. Click on Find now
 5. CTRL key to collect multiple items
 1. Account operations
 2. Administrators
 3. DHCP Administrators
 4. DNS Admins
 5. Domain Admins
 6. Enterprise Admins
 7. Event Log Readers
 8. Group Policy Creator Owners
 9. Performance Log Users
 10. Performance Monitor Users
 11. Print Operators
 12. Remote Desktop Users
 13. System Admins
 14. Server Operators
 6. Click OK and Apply Changes
5. Right click new -> users
 1. Create a new user with name and complex password (use random name)
 2. Uncheck box saying to change password at first login
6. Right click on new user, properties
 1. Member of
 2. Add
 3. Advanced
 4. Find now
 5. CTRL key to collect multiple items
 1. Account operations
 2. Administrators
 3. DHCP Administrators
 4. DNS Admins

5. Domain Admins
6. Enterprise Admins
7. Event Log Readers
8. Group Policy Creator Owners
9. Performance Log Users
10. Performance Monitor Users
11. Print Operators
12. Remote Desktop Users
13. System Admins
14. Server Operators
6. Click OK and Apply Changes
7. Log out of Windows and log into newest account
8. Go into Active Directory Users and Computers
9. Expand Server Local and Users
10. Go into users
11. Right click on original Administrator account
 1. Disable account
12. Disable all unneeded accounts
13. Go to Group Policy Management on Windows
 1. Go to Forest -> Domains -> Server -> Group Policy Objects -> Default Domain Policy
 2. Right click, Edit
 3. Go back to group policy management editor
 1. Default -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy -> Configuration -> Audit Policies
 2. Open Account Logon
 1. Audit Credential Validation: double click and configure failure
 2. Audit Other Account Logon Events: success and failure
 3. Account Management
 1. Audit other account management events: success and failure
 2. Audit Security group management: success and failure
 3. Audit user account management: success and failure
 4. Logon/Logoff
 1. Audit account logout: success and failure
 2. Audit logoff: success and failure
 3. Audit logon: failure
 4. Audit other logon logoff events: success and failure
 5. Audit special logon: success and failure
 5. Object Access
 1. Audit kernel object: success and failure
 2. Audit other object access events: success and failure
 3. Audit registry: success and failure
 4. Audit SAM: failure
 6. Policy Change
 1. Audit audit policy change: success and failure
 2. Audit authentication policy change: success and failure

3. Audit authorization policy change: success and failure
 4. Audit other policy change events: success and failure
7. Privilege Use
 1. Audit non sensitive privilege use properties: success and failure
 2. Audit other privilege use events properties: success and failure
 3. Audit sensitive privilege use: success and failure
8. System
 1. Audit other system events properties: success and failure
 2. Audit security system extension properties: success and failure
 3. Audit system integrity: failure

MMC

To use an MMC snap-in to manage a Server Core server that is a domain member:

1. Start an MMC snap-in, such as Computer Management.
2. Right-click the snap-in, and then click Connect to another computer.
3. Type the computer name of the Server Core server, and then click OK. You can now use the MMC snap-in to manage the Server Core server as you would any other PC or server.

To use an MMC snap-in to manage a Server Core server that is *not* a domain member:

Establish alternate credentials to use to connect to the Server Core computer by typing the following command at a command prompt on the remote computer:

```
cmdkey /add:<ServerName> /user:<UserName> /pass:<password>
```

1. If you want to be prompted for a password, omit the /pass option.
2. When prompted, type the password for the user name you specified. If the firewall on the Server Core server is not already configured to allow MMC snap-ins to connect, follow the steps below to configure Windows Firewall to allow MMC snap-in. Then continue with step 3.
3. On a different computer, start an MMC snap-in, such as Computer Management.
4. In the left pane, right-click the snap-in, and then click Connect to another computer. (For example, in the Computer Management example, you would right-click Computer Management (Local).)
5. In Another computer, type the computer name of the Server Core server, and then click OK. You can now use the MMC snap-in to manage the Server Core server as you would any other computer running a Windows Server operating system.

To configure Windows Firewall to allow MMC snap-in(s) to connect

To allow all MMC snap-ins to connect, run the following command:

```
Enable-NetFirewallRule -DisplayGroup "Remote Administration"
```

To allow only specific MMC snap-ins to connect, run the following:

```
Enable-NetFirewallRule -DisplayGroup "<rulegroup>"
```

Where *rulegroup* is one of the following, depending on which snap-in you want to connect:

MMC snap-in	Rule group
Event Viewer	Remote Event Log Management
Services	Remote Service Management
Shared Folders	File and Printer Sharing
Task Scheduler	Performance Logs and Alerts, File and Printer Sharing
Disk Management	Remote Volume Management
Windows Firewall and Advanced Security	Windows Firewall Remote Management

IIS Hardening

Rename administrator account and set a strong password

Disable FTP Server under Windows Features -> Turn Windows features on or off -> Internet Information Services -> FTP Server (uncheck)

Edit IP and Domain Restrictions Settings

- Windows features -> Turn windows features on or off -> IIS -> Web Server -> Security -> IP and Domain Restrictions
- Add allow restriction rule
- Type in IP addresses

Turn on logging

Error Pages Settings - Turn on detailed errors for local requests and custom error pages for remote requests

Disable directorybrowsing

- Alter the web.config file and set directoryBrowse to false (C:/inetpub/wwwroot)

Configure web server extensions at the web server

- Web Server (IIS) -> Web Server -> Application Development -> ISAPI Extensions
- Expand the local computer and click Web Service Extensions
- Click the web service extension that needs to be enabled/disabled

Configure Web Site Permissions

- Make sure permissions for remote are read, not write or execute

Create a backup: %windir%\system32\inetsrv\appcmd.exe add backup "My Backup Name"

Restore the backup: %windir%\system32\inetsrv\appcmd.exe restore backup "My Backup Name"

Delete a backup: %windir%\system32\inetsrv\appcmd.exe delete backup "My Backup Name"

Web Server (IIS) -> Web Server -> Health and Diagnostics -> Custom Logging & Logging tools

IIS HTTP -> HTTPS

1. Download and install URL Rewrite module
2. Open IIS Manager console and select the website you would like to apply the redirection to in the left-side menu
3. Double click "URL Rewrite"
4. Click "Add Rules"
5. Select "Blank Rule" in the Inbound section, then OK
6. Enter a rule name
7. In the "Match URL" section:
 - a. Select: ""Matches the Pattern" in the "Requested URL" drop-down menu
 - b. Select "Regular Expressions" in the "Using" drop-down menu
 - c. Enter the following pattern in the "Match URL" section: "(.*)"
 - d. Check the "Ignore case" box



Edit Inbound Rule

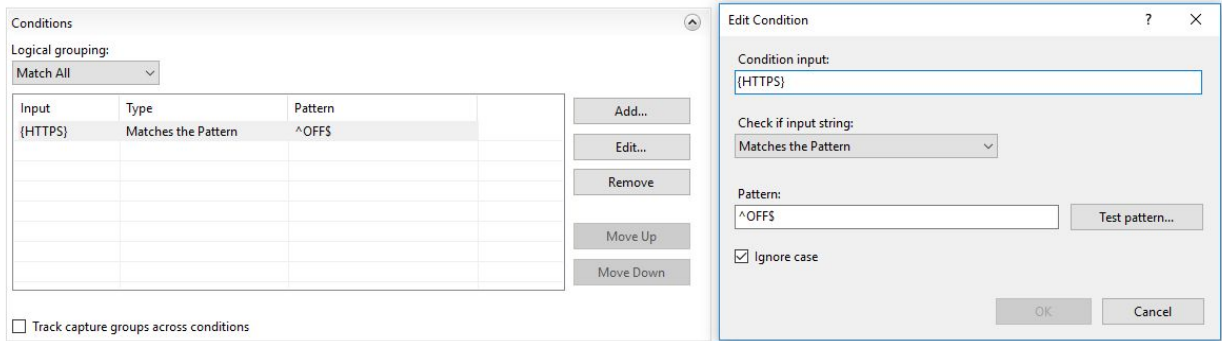
Match URL

Requested URL: Matches the Pattern Using: Regular Expressions

Pattern: Test pattern...

☒ Ignore case

8. In the "Conditions" section, select "Match all" under the "Logical Grouping" drop-down menu and press "Add"
9. In the prompted window:
 - a. Enter "{HTTPS}" as a condition input
 - b. Select "Matches the Pattern" from the drop-down menu
 - c. Enter "^OFF\$" as a pattern
 - d. Press "OK"



10. In the “Action” section, select “Redirect” as the action type and specify the following for “Redirect URL”:

https://{HTTP_Host}{REQUEST_URI}

11. Check the “Append query string” box.

12. Select the Redirection Type of your choice. The whole “Action” section should look like this:



13. Click on “Apply” on the right side of the “Actions” menu.

<https://www.namecheap.com/support/knowledgebase/article.aspx/9953/38/iis-redirect-http-to-https>