The Comprehensive Active Directory Penetration Testing & Lab

By Muhammad Sada Mainasara

CCNA R&S, CCNP SECURITY, CISCO SECURITY SPECIALIST, CEH, CHFI, MCSA, OSCP

Lab Preparation and Setup

Tools of the Trade

- 1 Windows Server 2019
- 2 Windows 10 Enterprise Edition

3 Metesploitable3 on Windows Server 2008

4 Microsoft Sql Server 2017

Domain Enumeration Tools

Tools of the Trade

1 Remote Server Administration Tools (RSAT) AD PowerShell Module

2 PowerView

3 PowerUpSql

4 SharpHound

5 BloodHound

6 SQLRecon

Exploitation, Post Exploitation and Lateral Movement

Tools of the Trade

1 PowerView

2 PowerUpSql

3 Inveigh

4 SQLRecon

5 Mimikatz

6 Rubeus

7 SharpSpray

Exploitation, Post Exploitation and Lateral Movement Cont...

8 DomainPasswordSpray

9 PsExec

10 Netcat

11 Invoke-SqlServer-Escalate-ExecuteAs

12 john-the-ripper

13 Hashcat

14 Kekeo

15 Invoke-SqlServer-Escalate-Dbowner

Exploitation, Post Exploitation and Lateral Movement Cont...

16 Invoke-BruteForce

17 PrintSpoofer

Downloading Virtual Machines

1 Windows Server 2019 Evaluation Copy from Microsoft website https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

2 Windows Enterprise Evaluation Copy from Microsoft website https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise

3 MetaSploitable3 VM from Rapid7 Github Repo https://github.com/rapid7/metasploitable3

Downloading Virtual Machines

4 MicroSoft SQL Server Express edition from Microsoft Website https://www.microsoft.com/en-us/download/details.aspx?id=55994

5 Downloading VirtualBox <u>https://download.virtualbox.org/virtualbox/7.0.12/VirtualBox-7.0.12-159484-Win.exe</u>

Downloading VirtualBox Extension Pack <u>https://download.virtualbox.org/virtualbox/7.0.12/Oracle_VM_VirtualBox_Extension_</u> <u>Pack-7.0.12.vbox-extpack</u>

Installing Windows Server 2019

🗿 Create Virtual Machine



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

2

X

ISO Image:	<not selected=""></not>			
Edition:				
Type:	Microsoft Windows			V 64
Version:	Windows 2019 (64-bit)	9		~
	Skip Unattended Installation			
	(1) No ISO image is selected, the	quest OS will need to be	installed manually.	

Let's go with the Default Setting

🔞 Create Virtual Machine ? \times Hardware You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible. 2048 MB 🗘 Base Memory: C.L.C. 1004 4 MB 32768 MB 1 🗘 Processors: 1 CPU 8 CPUs Enable EFI (special OSes only) Help Back Next Cancel



	Summary		
	The following table summarizes you are happy with the configu go back and modify the configu	the configuration you have chosen for the new virtual machine. When ration press Finish to create the virtual machine. Alternatively you can ration.	
	😽 Machine Name and 05	Туре	
	Machine Name	DC01	
	Machine Folder	C:/Users/mohas/VirtualBox VMs/DC01	
AYT.	ISO Image		
	Guest OS Type	Windows 2019 (64-bit)	
	🔵 Hardware		
	Base Memory	2048	
	Processor(s)	1	
	EFI Enable	false	
	Disk		
	Disk Size	50.00 GB	
	Pre-allocate Full Size	false	

Let's Change Some Settings



Network Adapter Settings





Creating New Nat Network

🗿 Oracle VM VirtualBox Manager

File Machine	Snapshot Help
Create Remov	Properties orks NAT Networks Cloud Networks
Ceneral Ontions	Part Forwarding
General Options	Fortrorwarding
Name:	BS-Network
IPv4 Prefix:	10.10.1.0/24
	Enable DHCP
—	

😳 DC01 - Settings	- 🗆 X
General	Network
System	Adapter 1 Adapter 2 Adapter 3 Adapter 4
Display	Enable Network Adapter
Storage	Attached to: NAT Network
Audio	Name: BS-Network
Network	
Serial Ports	
🌽 USB	
Shared Folders	
User Interface	
	OK Cancel Help

Clipboard Sharing and Drag and Drop between guest and host Operating system



Installing the OS



Installing the OS



Install now



Choose windows server with Desktop Experience

		1
Vindows Server 2019 Standard	хб4	9/15/2018
Vindows Server 2019 Standard (Desktop Experience	e) x64	9/15/2018
Vindows Server 2019 Datacenter	x64	9/15/2018
escription:		
is option installs the full Windows graphical envir eful if you want to use the Windows desktop or ha	onment, consuming extra ave an app that requires it	a drive space. It can be t.

Accept and Click Next



Choose Custom install and Click Next

Windows Se	tup				<u> </u>
Where do y	ou want to install Window	s?			
Name		Total size	Freespace	Type	
	0 Upallocated Space	50.0 GB	50.0 GB	туре	
		50.0 00	50.0 00		
€ <u>∱</u> <u>R</u> efresh	Delete	✓ Eormat	<mark>∦</mark> N <u>e</u> w		
€ <u>R</u> efresh	r <u>P</u> elete	₩ <u>F</u> ormat	<mark>∦</mark> N <u>e</u> w		
€ <u>R</u> efresh	r <u>A</u> E <u>x</u> tend	₽ <u>F</u> ormat	<mark>∦</mark> N <u>e</u> w		
€ <u>P</u> efresh	r <u>A</u> E <u>x</u> tend	₩ Eormat	<mark>∦</mark> N <u>e</u> w		
∲ <u>R</u> efresh ፼ <u>L</u> oad driver	r <u>a</u> E <u>x</u> tend	₩ <u>F</u> ormat	<mark>∦</mark> N <u>e</u> w		

Now allow the OS to be copied the VM we created



Here we will Create the Administrator's Password and Click Finish

Pie Madwie View Input Devices Help
-

Successfully Installed the OS





Go Devices and Click insert guest edition CD image



Double Click on it and follow the installation wizard to install it

		Name	Date modified	Туре	Size
:55			10/12/2023 10:41	File folder	
	7	NT3x	10/12/2023 10:41	File folder	
ds	A	OS2	10/12/2023 10:41	File folder	
nts	*	🗟 AUTORUN	7/26/2023 9:44 AM	Setup Information	2 KB
	*	autorun.sh	10/12/2023 10:19	SH File	7 KB
		📄 runasroot.sh	10/12/2023 10:19	SH File	5 KB
		VBoxDarwinAdditions.pkg	10/12/2023 10:19	PKG File	2,153 KB
		VBoxDarwinAdditionsUninstall.tool	10/12/2023 10:19	TOOL File	5 KB
		VBoxLinuxAdditions.run	10/12/2023 10:19	RUN File	6,159 KB
		VBoxSolarisAdditions.pkg	10/12/2023 10:19	PKG File	9,185 KB
		💱 VBoxWindowsAdditions	10/12/2023 9:57 AM	Application	237 KB
		🚳 VBoxWindowsAdditions-amd64	10/12/2023 10:41	Application	15,361 KB
		🏘 VBoxWindowsAdditions-x86	10/12/2023 10:19	Application	9,017 KB
		📄 windows11-bypass	7/26/2023 9:44 AM	Registration Entries	1 KB

Open the Computer Search bar and Type computer, View your PC name

Settings	
Settings	н
View your PC name	
③ See if you have a 32-bit or 64-bit version of Windows	
다고 Change braille output table type	
Taskbar notification area	
다고 Change braille input table type	
Search indexing was turned off. Turn indexing back on.	

Click on rename this pc and enter DC01 in the name, click Next and restart the Vm

settings		- L
ධ Home	About	
		har ta
Find a setting ,	P Installed RAM	2.00 GB
	Device ID	79509815-2326-4FCE-A50C-EE88588D1212
ystem	Product ID	00429-70000-00000-AA946
	System type	64-bit operating system, x64-based processor
Display	Pen and touch	No pen or touch input is available for this display
) Sound	Rename this F	20
Notifications & actions		
D Focus assist	Windows s	pecifications
	Edition	Windows Server 2019 Standard
/ Power & sleep	Version	1809
	Installed on	11/17/2023
D Battery	Installed on OS build	11/17/2023 17763.1
⊃ Battery ⊐ Storage	Installed on OS build Change product	11/17/2023 17763.1 t key or upgrade your edition of Windows
⊃ Battery ⊐ Storage	Installed on OS build Change product Read the Micros	11/17/2023 17763.1 I key or upgrade your edition of Windows soft Services Agreement that applies to our services
⊃ Battery ⊐ Storage ♂ Tablet mode	Installed on OS build Change product Read the Micros Read the Micros	11/17/2023 17763.1 It key or upgrade your edition of Windows oft Services Agreement that applies to our services oft Software License Terms

Installing AD-DS and Domain Controller on the Server



Next





Next

Add Roles and Features Wiz	zard			-		×
Select destination	on server			DESTINA	TION SERV	/ER 201
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a Select a server Select a virtual Server Pool	a virtual hard disk on which from the server pool hard disk	n to install roles and features.			
Confirmation Results	Name DC01 1 Computer(s) fou	IP Address 10.10.1.4 nd	Operating System Microsoft Windows Server 2	2019 Standard		
	and that have bee newly-added serve	n added by using the Add ers from which data collect	Servers command in Server Ma ion is still incomplete are not sh	Install	Cance	d

Select Active Directory DomainService and Click add features



Select server role	🚡 Add Roles and Features Wizard	COLORINATION SERVER
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	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. [Tools] Group Policy Management Remote Server Administration Tools Role Administration Tools A D DS and AD LDS Tools Active Directory module for Windows PowerShell AD DS Tools [Tools] Active Directory Administrative Center [Tools] AD DS Snap-Ins and Command-Line Tools Include management tools (if applicable)	X Directory Domain Services) stores information about a on the network and makes ormation available to users twork administrators. AD DS pmain controllers to give k users access to permitted ces anywhere on the network h a single logon process.
	Add Features Cancel	
Next to Install

📥 Add Roles and Features Wizard		_		\times
Confirm installation	n selections	DESTINAT	ION SERVE	R 1
Before You Begin	To install the following roles, role services, or features on selected server, click Instal	п.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this page be	cause the	ey have	
Server Roles	been selected automatically. If you do not want to install these optional features, cl their check boxes.	ick Previo	us to clea	ar
Features				
AD DS	Active Directory Domain Services			
Confirmation	Group Policy Management			
Results	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			
	Export configuration settings			
	Specify an alternate source path			
	< Previous Next > Insta		Cancel	

After the installation click close



Installing Domain Controller



Adding new forest and FQDN

📥 Active Directory Domain Services	Configuration Wizard			_		\times
Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment operation Add a domain controller to a Add a new domain to an exis Add a new forest Specify the domain information Root domain name: More about deployment configu	n an existing domain sting forest for this operation BYTESHIELD.local		TAR	GET SER\ D	/ER CO1
		< Previous Next >	Instal		Cancel	

Creating a memorable Domain Services Recovery mode password (DSRM)

🔁 Active Directory Domain Service	s Configuration Wizard		—		\times
Domain Controlle	r Options		TAR	GET SERV D	VER C01
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest a Forest functional level: Domain functional level: Specify domain controller capabilities Obmain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mod Password: Confirm password:	e (DSRM) password			
	More about domain controller options				
	< Pre	vious Next > Insta		Cancel	

Next > Next > Install to Finish

🚵 Active Directory Domain Service	s Configuration Wizard		—		×
Additional Option	S		TAR	GET SER [VER DC01
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check	Verify the NetBIOS name assigned to the doma The NetBIOS domain name:	in and change it if necessary			
Installation Results					-
	More about additional options				
	< Previous	Next > Insta		Cance	

AD-DS and Domain Controller has been Successfully installed



Network Configuration, ipconfig shows the dynamic ip address, let's make it static

🔁 Administrator: Windows PowerShell	—	×
PS C:\Users\Administrator> ipconfig		
Windows IP Configuration		
Ethernet adapter Ethernet:		
Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::16c:55bb:130f:60e1%3 IPv4 Address : 10.10.1.4 Subnet Mask : 255.255.255.0 Default Gateway : 10.10.1.1 PS C:\Users\Administrator>		

Network Settings

Internet Protocol Version 4 (TCP/IPv4)	Properties	\times
General		
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator	
Obtain an IP address automatical	у	
• Use the following IP address:		
IP address:	10 . 10 . 1 . 4	
Subnet mask:	255.255.255.0	
Default gateway:	10 . 10 . 1 . 1	
Obtain DNS server address autom	atically	
• Use the following DNS server add	resses:	
Preferred DNS server:	127.0.0.1	
Alternate DNS server:	8.8.8.8	
Validate settings upon exit	Advanced	
	OK Cance	

Creating Policy to Disable Windows Defender

📓 Group Policy Management —	\Box \times
📓 File Action View Window Help	- 5 :
Group Policy Management Contents Group Policy Management Contents BYTESHIELD.local Sites Group Poli Contents Co	

Naming the Policy

	Group Policy Management	Group Policy Management
	🤗 Demeine	Control to
1	V in Domains	A
	> 🙀 BYTESHIELD.local	Name
	> 📫 Sites	A Forest: BYTESHIELD.local
	Group Policy Modeling	New GPO ×
	Group Policy Results	
		Name:
		Disabling Windows Defender
		0
		Source Starter GPU:
		(none) V
		OK Cancel

Now right click on the policy you just created and click edit to edit it

🗢 🔿 🔽 🔽 🖬				
Group Policy Management	Group Policy Me	odeling		
 Porest: BYTESHIELD.local Domains Default Domain Policy Disabling Windows Defender Domain Controllers Comp Policy Objects WMI Filters Starter GPOs Sites Group Policy Modeling Group Policy Results 	Contents	User	Computer	Last Refresh Date





Scroll Down to Select windows defender antivirus and real-time protection



Double Click on turn off real-time Protection



Select enable and Ok

Turn off real-time	protection									\times
Turn off real-time	protection			Previous S	etting	Nex	t Setting	9		
 Not Configured Enabled Disabled 	Comment:									< >
	Supported on:	At least Window	ws Vista							$\hat{}$
Options:			Help:							
			This policy known ma Window potentially on your co If you er will not pro If you di Defender A detections	setting turns lware detection unwanted so mputer. hable this poli compt users to sable or do no Antivirus will p	s off real- on. ntivirus a oftware at take act ot config prompt u	time pr lerts yo ttempts g, Winc ions on jure this isers to	ou when s to insta dows Def malwar s policy : take act	m prom malwa fender re dete setting ions o	are or f or to ru Antiviru ctions. g, Windon n malwa	n s vre
					ОК		Canc	el	Арр	bly

Creating Smb Share

🔛 Dashboard	WELCOME TO SERVER MANAGER
Local Server All Servers AD DS	1 Configure this local server
B DNS ■ File and Storage Services ▷	QUICK START 2 Add roles and features 3 Add other servers to manage WHAT'S NEW 4 Create a server group
	5 Connect this server to cloud services

	Servers	SERVERS All servers 1 total
i i:	Volumes Disks	Filter P 🔅 🕶
	Storage Pools	Server Name IPv4 Address Manageability Last Update Windows Activation
≞ ∎r⊳	Shares 🔸 🖌	DC01 10.10.1.4 Online - Performance counters not started 11/17/2023 4:32:51 PM Not activated
	Work Folders	

SHARES All shares 2 total				TAS	iks 🔻	VOLUN NETLOG	/IE ON on I	DC01	
Filter		•			New Share		-	49.5 GR	
Share DC01 (2)	Local Path	Protocol	Availability Type		henesh	20.6%	Used	45.5 65	 10.2 GB Used Space 39.3 GB Free Space
NETLOGON	C:\Windows\SYSVOL\sysvol\BYTE	SMB	Not Clustered						
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered			C- 44	v-1	- O	



Select Profile	Share name:	
Share Location	Share description:	
Other Settings		
	Local path to share:	
	If the folder does not exist, the folder is created.	
	Remote path to share:	
	\\DC01\IT-DEPT	

Next > Next > Create

📥 New Share Wizard

 \Box \times

_

Confirm selections

Select Profile	Confirm that the following	are the correct settings, and then click Create.	
Share Location	SHARE LOCATION		
Share Name	Server:	DC01	
Other Settings	Cluster role:	Not Clustered	
Permissions	Local path:	C:\Shares\IT-DEPT	
Confirmation	SHARE PROPERTIES		
Results	Share name:	IT-DEPT	
	Protocol:	SMB	
	Access-based enumeration:	Disabled	
	Caching:	Enabled	
	BranchCache:	Disabled	
	Encrypt data:	Disabled	
			_
		< Previous Next > Create Cancel	

Installing Windows 10 Enterprise edition

🗿 Create Virtual Machine



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

7

X

Name;	Win10-Client-01				
Folder:	C:\Users\mohas\VirtualBox VM	S			~
ISO Image:	<not selected=""></not>				~
Edition:					
Type:	Microsoft Windows				~ 4
Version:	Windows 10 (64-bit)				~
	Skip Unattended Installation				
	🚯 No ISO image is selected, the g	uest OS will nee <mark>d to l</mark>	be inst <mark>a</mark> lled ma	nually.	
		Evport Mada	Pade	Neut	Cancal
		Expert Mode	DOUK	Next	Cancel

We are going to go with the default setting as we did on the Domain Controller, the same way we installed the DC



When you get to this level instead of Creating a local user click join domain instead





Creating User



Create a memorable Password and Confirm it



Select 3 memorable Security question and move on

Security question (1 of 3)	
Your answer	
	Nort

Accept

Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

Location

You won't be able to get location-based experiences like directions Windo and weather or enjoy other services that require your location to work. lose it.



Diagnostic data

Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements.



Send Required diagnostic data

Tailored experiences

The tips, ads, and recommendations you see will be more generic and may be less relevant to you.



Select 'Learn more' for info on the above settings, how Microsoft

Find my device

Windows won't be able to help you keep track of your device if you lose it.



Inking & typing

Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of apps and services running on Windows.



Advertising ID

The number of ads you see won't change, but they may be less relevant to you.



Learn more

Accept

Windows Successfully Installed, you can install guest edition cd and change PC name as Win10-Client-01 the same way you did on the Domain Controller



Joining the Client to the Domain, Let's Assign static ip address to the Client

Select Windows PowerShell	-	×
Ethernet adapter Ethernet:		
Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::a935:2bad:755:652c%6 IPv4 Address : 10.10.1.5 Subnet Mask : 255.255.255.0 Default Gateway : 10.10.1.1 PS C:\Users\p.brown> _		

Here is the network configuration with the Domain Controller as DNS Server

nternet Protocol Version 4 (TCP/IPv4) Properties					
General					
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings. Obtain an IP address automaticall	atically if your network supports ask your network administrator y				
IP address: Subnet mask:	10 . 1 . 5 255 . 255 . 0				
Obtain DNS server address automatically					
Use the following DNS server addr	esses:				
Preferred DNS server:	10 . 10 . 1 . 4				
Alternate DNS server:	8.8.8.8				
Validate settings upon exit	Advanced				
	OK Cance	1			
Litem selected					

Joining the Client, search for work or school

control parler		
See more search results	>	Change workgroup name Control panel
Apps		
WordPad	>	⊂" Open
Settings		
Access work or school	>	
Nork Folders	>	
🙀 Manage Work Folders	>	
✓ Remote desktop settings	>	
Search the web		
> work - See more search results	>	
✓ workday	>	
work from home jobs	>	
𝒫 workouts	>	
𝒫 work		o et 💽 🚍 🔒 <

Connect

Accounts	such as which settings you can change. For sp them.
R≡ Your info	+ Connect
🖾 Email & accounts	
ିକ୍ତ Sign-in options	Related settings
Access work or school	Add or remove a provisioning package
우, Family & other users	Export your management log files
Svnc vour settings	Set up an account for taking tests

pecific info about this, ask

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Email address

Alternate actions:

These actions will set up the device as your organization's and give your organization full control over this device.

Join this device to Microsoft Entra ID

Join this device to a local Active Directory domain

lext


RE	Your info	_	L Connect		_
	Email & accounts	Join a domain	Windows Security	×	
Q,	Sign-in options	Join a de	Enter your domain account info	to verify you have permission to	
Þ	Access work or scho	Domain nam	connect to the domain.		
A⁺	Family & other users	BYTESHIELI	p.brown	•	
С	Sync your settings				Cancel
			ОК	Cancel	

Accounts	such as which settings you can change. For specific into about this, ask them.
	Add an account
R≡ Your info	
🖾 Email & accounts	Add an account Enter the account info for the person who'll be using this PC. If you skip this step, the person will
🔍 Sign-in options	have default permissions for the domain.
Access work or sch	User account p.brown
\mathcal{R}_{+} Family & other user	s Account type
\mathcal{C} Sync your settings	Administrator ~
	Next Skip
	Using Remote Deskton

This PC

Active Network

Creating Smb Share on Windows Client



Right Click and go the Properties and share it



Now we are done setting up Win10-Client-01 Machine

Instruction

Replicate the same process to create another Machine and name it Win10-Client-02

Setting up DNS conditional forwarders for both side

	•	3		Manage	Tools	View	Help
		Active	Director	y Administrati	ive Center		
		Active	Director	y Domains an	d Trusts		
DC01	_	Active	Director	y Module for	Windows I	PowerShell	
		Active	Director	y Sites and Se	rvices		
49.5 GB		Active	Director	y Users and C	omputers		
		ADSI	Edit				
10.2 GB Used Space		Comp	onent Se	rvices			
39.3 GB Free Space		Comp	uter Man	agement			
		Defra	gment an	d Optimize D	rives		
		Disk (Cleanup				
		DNS	-				
		Event	Viewer				

머

х

Adding Forwarder

🗢 🔿 🔀 📰				
B DNS ■ DC01 > ■ Forward > ■ Reverse I > ■ Trust Poi	Lookup Zones Lookup Zones ints	Name	Type There are no items	s to show in this view.
📔 Conditic	New Cond	litional Forwarder		
	View	>		
-	Refresh			
	Export List			
	Help			

Here we add the FQDN and IP address pointing to the target domain

🚊 DNS Manager				-	-	\times
File Action Vie	··· Llele				г	
🗢 🔿 👩	New Conditional Forward	er		×		
	DNS Domain:					
× ≣ DC01	TRUSTEDCORP. local					
> iii Forward						
> 🦳 Reverse I	IP addresses of the master :	servers:				
> 🧾 Trust Poi	TD Address	S 5001	M-Rd-A-d	Delete		
📔 Conditio	IP Address	Server FQDN	validated			
	10.10.1.6			Up		
				D <u>o</u> wn		
	Store this conditional for	warder in Active Directory, a	nd replicate it as follows:			
	All DNS servers in this for	est				
	Number of seconds before f	orward queries time out:	5			
	The server FQDN will not be	available if the appropriate r	everse lookup zones and entr	ies are not		
	configured.					
			OK	Cancel		

Doing the same from the other side pointing to Byteshield

🚊 DNS Manager				-	-	\times
File Action Vie	New Conditional Forward	er		×]	
DNS DC03	DNS Domain:					
> 📫 Forward > 📫 Reverse	IP addresses of the master	servers:				
> 📫 Trust Poi	IP Address	Server FQDN	Validated	Delete		
	<click a<br="" add="" here="" to="">(3) 10.10.1.4</click>	DC01	The server with this IP	Up		
				D <u>o</u> wn		
	Store this conditional for	warder in Active Direct	ory, and replicate it as follows:			
	All DNS servers in this fo	rest				
	Number of seconds before to The server EODN will not be	forward queries time ou available if the appror	it: 2	es are not		
	configured.					
			ОК	Cancel		

We can now ping the DC by its hostname

PS C:\Users\p.brown.BYTESHIELD> ping DC01

Pinging DC01.BYTESHIELD.local [10.10.1.4] with 32 bytes of data: Reply from 10.10.1.4: bytes=32 time<1ms TTL=128 Reply from 10.10.1.4: bytes=32 time<1ms TTL=128 Reply from 10.10.1.4: bytes=32 time<1ms TTL=128 Reply from 10.10.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms PS C:\Users\p.brown.BYTESHIELD> _

We can also ping back from the DC

PS C:\Users\Administrator> ping win10-client-01

Pinging win10-client-01.BYTESHIELD.local [10.10.1.5] with 32 bytes of data: Reply from 10.10.1.5: bytes=32 time<1ms TTL=128 Reply from 10.10.1.5: bytes=32 time<1ms TTL=128 Reply from 10.10.1.5: bytes=32 time=1ms TTL=128 Reply from 10.10.1.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.1.5: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

We have Successfully Installed windows server 2019, installed AD-DS and domain Controller on it, also installed Windows 10 enterprise edition as a client and joined to it to the domain,

INSTRUCTION

Install 2 Domain Controllers DCO2 and DCO3, the DCO3 should be installed the same way you installed DCO1, but with different Domain name as TRUSTEDCORP.local, but every other thing should be the same,

DCO2 should only be installed without installing AD-DS and Domain Controller, because we are going to make it a child to DCO1 as the Parent or Root Domain, while DCO3 would later be as a trusted domain to DCO1, aTransitive/bidirectional Trust

If you have Successfully done what you're instructed in the last section, it is now time to create forest bidirectional trust between BYTESHIELD and TRUSTEDCORP



Right click on the Domain name and go to properties, select trusts tab to start



Enter the Domain



Forest trust



Bidirectional Trust







Create a memorable trust password, it's going to be the same for both side



Next > Next



Do the same on the other side



Now validate outgoing and incoming trust

🗢 🔿 🞽 📰 🖾 🗟 🖬		
Active Directory Domains and Trust	BYTESHIELD.local Properties ? ×	
BYTESHIELD.local	Ge TRUSTEDCORP.local Properties ? ×	^
	General Name Suffix Routing Authentication	•
i l	This Domain: BYTESHIELD.local	
2	Other Domain: TRUSTEDCORP.local	
	Trust type: Forest	
	The other domain supports Kerberos AES Encryption	
	Direction of trust:	
	Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.	
	Transitivity of trust:	
	This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.	
	To confirm or reset this trust relationship and update its validate	
	To save a file with the details about the status of the names associated with this trust, click Save As. Save As.	
<	OK Cancel Apply Help]

We have Successfully Created a Transitive Trust between BYTESHIELD & TRUSTEDCORP, it is now time to Configure DC02 as a Child Domain to BYTESHIELD

First thing first let's configure network and DNS setting of the Domain

nternet Protocol Version 4 (TCP/IPv4)	Properties	>
General		
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.	atically if your network supports ask your network administrator	
Obtain an IP address automatically	Y	
Use the following IP address:		
IP address:	10 . 10 . 1 . 7	
Subnet mask:	255.255.255.0	
Default gateway:	10 . 10 . 1 . 1	
Obtain DNS server address autom	atically esses:	
Preferred DNS server:	10 . 10 . 1 . 4	
Alternate DNS server:	8.8.8.8	
Validate settings upon exit	Advanced	
	OK Cance	4

Here We are going to AD-DS

• ③	I	7	Manag	e Tools	View	Help
			A R	dd Roles and emove Roles	l Features and Featu	res
			A	dd Servers reate Server	Group	
			S	erver Manag	er Properti	es

The same way we did on the other domain Controllers

📥 Add Roles and Features Wizard

DC02

DESTINATION SERVER

Before you begin

Before You Begin	This wizard helps you install roles, role services, or features. You determine which roles, role services, or
Installation Type	hosting a website.
Server Selection	To remove roles, role services, or features:
Server Roles	Start the Remove Roles and Features Wizard
Features	Before you continue, verify that the following tasks have been completed:
Confirmation	The Administrator account has a strong password
Results	 Network settings, such as static IP addresses, are configured The most current security updates from Windows Update are installed
	If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
	To continue, click Next.
	Skip this page by default
	< Previous Next > Install Cancel

Let's Promote it to Domain Controller

- (© 🍢	Manage	Tools	View	Help
Post-deployment Configuration Configuration required for Active Direct Services at DC02 Promote this server to a domain contro Feature installation Configuration required. Installation succ DC02. Add Roles and Features Task Details	tory Domain				
				ł	Hide

Now instead of selecting forest

📠 Active Directory Domain Services Configuration Wizard

Deployment Configuration

Somain Controller Option Additional Options	Select the deployme Add a domain cc Add a new doma Add a new doma	administrator@BYTES	HIELD.local		
anno laviaw Optional frenegulaties Check nstallation tesuits	Specify the domain i Select domain type: Parent domain name	•••••		0	
	Supply the credentia	ОК		Car	ncel
Credentials for	deployment open				
Supply credentials fo	or the deployment operation	7			
Supply credentials fo	or the deployment operatio		ext >	Install	Cancel

Windows Security

Credentials for deployment operation

Supply credentials for the deployment operation

\sim domain to an existing

Supplying the Credentials of our Root Domain

Windows Security			
Credentials for deployment operation			
Supply credentials for the deployment operation			
administrator@BYTESHIELD.local			
••••••	ି		
ОК	Cancel		

Creating DSRM Passowrd

🚘 Active Directory Domain Services Configuration Wizard					\times
Domain Controller	r Options		TAR	GET SERV	/ER 202
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new domain Domain functional level: Specify domain controller capabilities and O Domain Name System (DNS) server O Global Catalog (GC) Read only domain controller (RODC) Site name: Type the Directory Services Restore Mode Password: Confirm password:	Windows Server 2016 Vindows Server 2016 Default-First-Site-Name (DSRM) password Output			
	< Pre	vious Next > Insta		Cancel	

Follow the Wizard Next > Next and installed the same way you did on the other Domain Controllers



We have Successfully Create a child domain, now let's create DNS conditional forwarder pointing to the root domain



Creating Conditional Forwarder pointing to the root domain

DNS Manager					_ □	\times
	New Conditional Forwarde	r		×		
DNS DC02 Forward	DNS Domain: BYTESHIELD.local					
I > Reverse I	IP addresses of the master s	ervers:	Validated	Delete		
il	<click a<="" add="" here="" td="" to=""><td>Dent</td><td>The serves with this ID</td><td>Up</td><td></td><td></td></click>	Dent	The serves with this ID	Up		
	10.10.1.4	DC01	The server with this 1P	Down		
		arder in Active Directory - a	od replicate it as follows:			
All DNS servers in this forest						
Number of seconds before forward queries time out: 5 The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured. OK Cancel						

Now we can ping the FQDN of the root domain and vice versa

Create Share on the Child domain as you did on the root domain name it TRI-Share

PS C:\Users\Administrator> ping DC01.BYTESHIELD.local

Pinging DC01.BYTESHIELD.local [10.10.1.4] with 32 bytes of data: Reply from 10.10.1.4: bytes=32 time<1ms TTL=128 Reply from 10.10.1.4: bytes=32 time<1ms TTL=128 Reply from 10.10.1.4: bytes=32 time<1ms TTL=128 Reply from 10.10.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms PS G:\Usens\Administrator>

Downloading and Installing SQL Server on DC01, DC02 and Win10-Client-01

You can Download Microsoft Sql Server developer or express edition from MicroSoft website, after downloading it copy it to DC01 IT-DEPT share so that you can access it other machines

https://download.microsoft.com/download/5/A/7/5A7065A2-C81C-4A31-9972-8A31AC9388C1/SQLServer2017-SSEI-Dev.exe

SQL Server installation

SQL Server 2017 Developer Edition

Select an installation type:

Basic

Quickly install just the SQL Server for Windows database engine feature.

Custom

Download and execute the full SQL Server for Windows Setup experience for a customized install with multiple features.

SQL Server transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation

Download Media

 $\odot - \times$

Download SQL Server setup files now and install them later on a machine of your choice.

14.2204.5490.2
Install

sql Server 2017 Developer Edition			© – ×
Specify SQL Server media download MEDIA LOCATION CASQLServer2017Media	target location	MINIMUM FREE SF 9240 MB DOWNLOAD SIZE 1543 MB	ACE
	Close < Pr	evious	Install 14.2204.5490.2

This will take sometimes depending on your network speed and Computer performance

SQL Server 2017	☺ – ×
Developer Edition	
Downloading install package	
Acquiring setup files 75.556 MB / 1,536.032 MB 25.158 Mbps	
Samples	
You use the Official Microsoft GitHub Repository containing code samples for SQL Server (<u>https://github.com/Microsoft/sql-master/samples</u>) for samples on connecting to a SQL Server database, development samples for using different features like Services and much more.	server-samples/tree/ In-Memory OLTP, R-

Select New Sql server stand-alone installation and continue

髋 SQL Server Installation Center

Planning

Installation

Maintenance

Tools

Resources

Advanced

Options

New SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2017 in a non-clustered environment or to add features to an existing SQL Server 2017 instance. Install SQL Server Reporting Services Launch a download page that provides a link to install SQL Server Reporting Services. An internet connection is required to install SSRS. Install SQL Server Management Tools Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools. Install SQL Server Data Tools Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT. New SQL Server failover cluster installation Launch a wizard to install a single-node SQL Server 2017 failover cluster. Add node to a SQL Server failover cluster Launch a wizard to add a node to an existing SQL Server 2017 failover cluster. Upgrade from a previous version of SQL Server Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2017. New Machine Learning Server (Standalone) installation Launch a wizard to install Machine Learning Server (Standalone) on a Windows machine. This is typically used by data scientists as a standalone analysis server or as a

Microsoft SQL Server 2017

 \times

Product Key

- License Terms
- Global Rules
- Microsoft Update
- Product Updates
- Install Setup Files
- Install Rules
- Feature Selection
- Feature Rules
- Feature Configuration Rules
- Ready to Install
- Installation Progress
- Complete

Validate this instance of SQL Server 2017 by entering the 25-character key from the Microsoft certificate of authenticity or product packaging. You can also specify a free edition of SQL Server: Developer, Evaluation, or Express. Evaluation has the largest set of SQL Server features, as documented in SQL Server Books Online, and is activated with a 180-day expiration. Developer edition does not have an expiration, has the same set of features found in Evaluation, but is licensed for non-production database application development only. To upgrade from one installed edition to another, run the Edition Upgrade Wizard.

\sim	_					-
	Spa	cife,	- f	roo.	odii	tion
_	spe	CITY	aı	ree.	eui	uona

Developer	\sim
-----------	--------

Enter the product key:



Accept and Next



Next > Next

Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	 Looking for Reporting Service Features: Database Engine Services SQL Server Replication Machine Learning Ser R Python Full-Text and Semanti Data Quality Services PolyBase Query Service Analysis Services Select All Unselect All Instance root directory: Shared feature directory (x86): 	ces? Download it fro n vices (In-Database) ic Extractions for Sea ce for External Data C:\Program Files\Mid C:\Program Files\Mid C:\Program Files\Mid	Im the web Feature description: The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Prerequisites for selected features: Already installed: Windows PowerShell 3.0 or higher Microsoft .NET Framework 4.6 Disk Space Requirements Drive C: 1001 MB required, 36710 MB available Crosoft SQL Server\ So\Microsoft SQL Server\
			< Back Next > Cancel

Choose named instance and change its name from the default

Product Key License Terms Global Rules	 Default instance Named instance: 	BS_SQLSERVER]
Microsoft Update							
Product Updates	Instance ID:	MSSQLSERVER					
Install Setup Files							
Install Rules							
Feature Selection	SQL Server directory:	C:\Program Files\Mici	rosoft SQL Se	rver\MSSQL1	4.MSS	SQLSERVER	
Feature Rules	Installed instances:						
Instance Configuration			-				
Server Configuration	Instance Name	Instance ID	Features	Ec	lition		Version
Database Engine Configuration							
Feature Configuration Rules							
Ready to Install							
Installation Progress							
Complete							
				< Back		Next >	Cancel

Next > Next and choose mixed mode authentication, click add current user or add to select another user

Product Key	Server Configuration	D (D') (T 00	EU ECTREALA		
	Server Configuration	Data Directories	TempDB	FILESTREAM		
Clobal Puler	Specify the authent	ication mode and	administrat	tors for the Database E	ngine.	
Giobal Rules						
Microsoft Update	Authentication Mod	le				
Product Updates	O Windows authen	tication mode				
Install Setup Files	Mixed Mode (SO)	L Server authentica	ation and V	Vindows authentication	1)	
Install Rules	1				·	
Feature Selection	Specify the passwor	rd for the SQL Serv	er system a	idministrator (sa) accou	unt.	
Feature Rules	Enter password:	•••••				
f Instance Configuration						
Server Configuration	Confirm password:	•••••				
Database Engine Configuration	Specify SQL Server a	administrators —				
Feature Configuration Rules	BYTESHIELD\Admin	nistrator (Administ	rator)			desinistrators
Ready to Install					have unrestr	icted access
Installation Progress					to the Datab	ase Engine.
Complete						
	Add Current User	Add B	emove			
	Add Current Oser	Add	emove			
	1					
				< De als	Nexts	Connect
1				< Back	Next >	Cancel

Next and Install

Product Key	Ready to install SQL Server 2017:
Product Key License Terms Global Rules Microsoft Update Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install	Ready to install SQL Server 2017:
Ready to Install Installation Progress Complete	<pre> Instance ID: BS_SQLSERVER Instance IDs Instance IDs</pre>
	C:\Program Files\Microsoft SQL Server\140\Setup Bootstrap\Log\20231118_143015\ConfigurationFile.ini
	< Back Install Cancel

Product Key	Information about the Setup operation or	possible next steps:	
License Terms	Eastura	Status	<u>^</u>
Global Rules		Status	
Microsoft Update		Succeeded	
Product Updates	SOL Writer	Succeeded	
Install Setup Files	SQL Client Connectivity	Succeeded	
Install Rules	SQL Client Connectivity SDK	Succeeded	
Feature Selection	Setun Sunnort Files	Succeeded	*
Feature Rules			
Instance Configuration	Details:		
Server Configuration	Install successful.		
Database Engine Configuration			
Feature Configuration Rules			
Ready to Install			
Installation Progress			
Complete			
	Summary log file has been saved to the fol	llowing location:	
	C:\Program Files\Microsoft SQL Server\14	0\Setup Bootstrap\Log\20231118 143015	
	\Summary DC01 20231118 143015.txt	· · · ·	
			Close

Since we installed the Server let's install Sql server management studio SSMS, clicking install sql server management tools, we will get redirected to Microsoft website



Scroll Down and Click the link to Download this Version

Download SSMS

SSMS 19.2 is the latest general availability (GA) version. If you have a *preview* version of SSMS 19 installed, uninstall it before installing SSMS 19.2. If you have SSMS 19.x installed, installing SSMS 19.2 upgrades it to 19.2.

- Release number: 19.2
- Build number: 19.2.56.2
- Release date: November 13, 2023

Installing SSMS



RELEASE 19.2

Microsoft SQL Server Management Studio with Azure Data Studio

Welcome. Click "Install" to begin.





RELEASE 19.2 Microsoft SQL Server Management Studio with Azure Data Studio

Package Progress

overall Progress		
	Cancel	

Successfully Installed

RELEASE 19.2



Microsoft SQL Server Management Studio with Azure Data Studio

_

Setup Completed

All specified components have been installed successfully.



The next thing is to make it accessible remote, let's use a windows command line utility to check Connection status

PS C:\Users\Administrator> netstat -an | more Active Connections Proto Local Address Foreign Address State TCP 0.0.0.0:88 0.0.0.0:0 LISTENING 0.0.0.0:135 TCP 0.0.0.0:0 LISTENING TCP 0.0.0.0:389 0.0.0.0:0 LISTENING TCP 0.0.0.0:445 0.0.0.0:0 LISTENING TCP 0.0.0.0:464 0.0.0.0:0 LISTENING TCP 0.0.0.0:593 0.0.0.0:0 LISTENING TCP 0.0.0.0:636 0.0.0.0:0 LISTENING TCP 0.0.0.0:3268 0.0.0.0:0 LISTENING TCP LISTENING 0.0.0.0:3269 0.0.0.0:0 TCP LISTENING 0.0.0.0:5357 0.0.0.0:0 TCP LISTENING 0.0.0.0:5985 0.0.0.0:0 TCP 0.0.0.0:9389 0.0.0.0:0 LISTENING TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING TCP 0.0.0.0:49664 0.0.0.0.0 LISTENING TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING TCP 0.0.0.0:49670 0.0.0.0:0 LISTENING TCP 0.0.0.0:49673 0.0.0.0:0 LISTENING TCP 0.0.0.0:49678 0.0.0.0:0 LISTENING TCP 0.0.0.0:49698 0.0.0.0:0 LISTENING TCP 0.0.0.0:49749 0.0.0.0:0 LISTENING TCP 10.10.1.4:53 0.0.0.0:0 LISTENING TCP 10.10.1.4:139 0.0.0.0:0 LISTENING TCP 10.10.1.4:389 10.10.1.4:49697 ESTABLISHED 10.10.1.4:49742 TCP 10 10 1.4:389 ESTABLISHED TCP 10.10.1.4:389 10.10.1.4:49746 ESTABLISHED TCP 10.10.1.4:389 10.10.1.7:57947 ESTABLISHED TCP 10.10.1.4:49667 10.10.1.7:51897 ESTABLISHED TCP 10.10.1.4:49697 10.10.1.4:389 ESTABLISHED 10.10.1.4:49742 TCP 10.10.1.4:389 ESTABLISHED 10.10.1.4:389 TCP 10.10.1.4:49746 ESTABLISHED TCP 10.10.1.4:51144 10.10.1.7:49667 TIME_WAIT

Mssql server by default listens on port 1433, previous command shows that port 1344 is not in listening state, Let's configure it so that we can access it remotely



After searching and clicking Configuration manager, select network configuration

File Action View Help

🗢 🔿 🗟 🔽		
SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration (32bit) SQL Native Client 11.0 Configuration SQL Server Network Configuration SQL Native Client 11.0 Configuration	Items SQL Server Services SQL Server Network Configuration (SQL Native Client 11.0 Configuration SQL Server Network Configuration SQL Native Client 11.0 Configuration	

Double click or right click to go toTCP/IP properties



Select Ip address Tab scroll down and set the port 1344 apply and Ok

rotocol IP Addresses		
TCP Dynamic Ports	0	
TCP Port		
Active	Yes	
Enabled	No	
IP Address	::1	
TCP Dynamic Ports	0	
TCP Port		
Active	Yes	
Enabled	No	
IP Address	127.0.0.1	
TCP Dynamic Ports	0	
TCP Port		
TCP Dynamic Ports	0	
TCP Port	1433	
		`
TCP Port		
TCP port		

The TCP/IP protocol is in disable state, let's right click on it and enable it

🗢 🔿 | 🞽 | 🗒 | 🖉



Now Let's go sql server services and start the services, right click go to the properties

SQL Server Configuration Manager (Local)	Name	State		Start M	Mode	Log On As	Process ID	Service Type
SQL Server Services	🐞 SQL Server Browser	Stonne	h	Other	(Boot, Syste	NT AUTHORITY\LO	0	
5 SQL Server Network Configuration (32bit)	SQL Server (BS_S	R	Start		natic	NT Service\MSSQL	5360	SQL Server
 SQL Native Client 11.0 Configuration (32) SQL Server Network Configuration 	SQL Server Agent	s	Stop		al	NT Service\SQLAge	0	SQL Agent
■ Protocols for BS_SQLSERVER			Pause					
> 💂 SQL Native Client 11.0 Configuration			Resume					
			Restart					
			Properties					
			Help					

On the Service tab make it start automatically, Apply and Ok, Do the same to the other services

Service eneral nary Path ror Control it Code	Advanced	*C:\Pro	aram Eiler (200		
eneral nary Path ror Control it Code	1	"C:\Pro	gram Files (v96)		
nary Path ror Control it Code	I	"C:\Pro	gram Files (v26)		
ror Control it Code	l		gram Files (XOD)	Microso	oft Se
it Code		1			
		1077			
ost Name		DC01			
ame		SQL Se	rver Browser		
ocess ID		0			
L Service Tj	/pe				
art Mode		Disabl	ed		-
ate		Auton	natic		
		Disabl	ed		
		Manu	al		
Mode					
tart mode (of this service.				
	Mode tart mode (Mode tart mode of this service.	Mode tart mode of this service.	Mode tart mode of this service.	Mode tart mode of this service.

Now Let's bring up SSMS and connect to it to restart the service

Best match



Apps

- SQL Server 2017 Error and Usage Reporting
- SQL Server Profiler 19
- SQL Server Management Studio 19



Click Connect

🖵 Connect to Server		×
	SQL Server	
Server type:	Database Engine	~
Server name:	DC01\BS_SQLSERVER	\sim
Authentication:	Windows Authentication	\sim
User name:	BYTESHIELD\Administrator	\sim
Password:		
	Remember password	
	Connect Concel Hole Options >>>	
	Connect Cancel Help Options >>	,

Right Click on the server instance and select restart



Going back to Powershell console and Check we discovered that the port is in listening state

S C:\Users\Administrator> netstat -an | more

Active Connections

Proto	Local Address	Foreign Address	State	
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:9389	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49678	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49698	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49749	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:52061	0.0.0.0:0	LISTENING	
TCP	10.10.1.4:53	0.0.0.0:0	LISTENING	
TCP	10.10.1.4:139	0.0.0.0:0	LISTENING	
TCP	10.10.1.4:389	10.10.1.4:49697	ESTABLISHED	
TCP	10.10.1.4:389	10.10.1.4:49742	ESTABLISHED	
TCP	10 10 1 4.390	10 10 1 4.49746	ESTABLITSHED	

We have Successfully installed Microsoft sql server developer edition and basic Configuration needed for our purpose.

Instruction

Follow the same steps and install Sql server on DC03 and Windows 10 Client Machine

Installing Metasploitable3 on windows server 2008, Let's follow the Installation guide on rapid7 github page

https://github.com/rapid7/metasploitable3

PS C:\Users\mohas> cd .\Desktop\ PS C:\Users\mohas\Desktop> mkdir metasploitable3-workspace

Directory: C:\Users\mohas\Desktop

DS Cilliana mahaa Daaktan

Download Metasploitable zip file to th folder you created and unzip it there

6	aRobinson-R7 Approving cortex.yaml		Local	Codespaces	
	.github	Updated issue_template.md	>- Clone		?
	chef	Land #491, update docs for usi	HTTPS GitHub CLI		
	iso	Initial commit.	https://github.com/rapid7/	/metasploitable3.git	C
	packer	download windows pre-req file	Use Git or checkout with SVN usin	g the web URL.	
	resources	download windows pre-req file	단 Open with GitHub Deskt	ор	
	scripts	Land #566, guard token in Mar	_		
	versions/pro	ub1404 dev workflow	🗿 Download ZIP 🚽		
-					

Downloading requirement

Building Metasploitable 3

System Requirements:

- OS capable of running all of the required applications listed below
- VT-x/AMD-V Supported Processor recommended
- 65 GB Available space on drive
- 4.5 GB RAM

Requirements:

- Packer
- <u>Vagrant</u>
- <u>Vagrant Reload Plugin</u>
- VirtualBox, libvirt/qemu-kvm, or vmware (paid license required), or parallels (paid license required)
- Internet connection

Downloading and Installing Packer

Operating Syst	em						
macOS Windo	ws Linux	FreeBSD	NetBSD	OpenBSD	Solaris		
Binary download	for Window	'S					
386 Version: 1.9.4							Download 🛓
AMD64 Version: 1.9.4							Download 🛓

*

ıdi

I have Downloaded all the requirement, do the same and save and unzip them all in one folder

	Name	Date modified	Туре	Size
	🚾 metasploitable3-master	11/19/2023 1:19 AM	WinRAR ZIP archive	151,903 KB
·	🚾 packer_1.9.4_windows_amd64	8/18/2023 8:12 PM	WinRAR ZIP archive	22,188 KB
e	😼 vagrant_2.4.0_windows_i686	10/16/2023 8:20 PM	Windows Installer	281,460 KB
*	🏪 vagrant-reload-master	11/19/2023 1:29 AM	WinRAR ZIP archive	6 KB

Installing Vagrant 🛃 Vagrant Setup \times ____ Please read the Vagrant License Agreement License text copyright (c) 2020 \wedge MariaDB Corporation Ab, All Rights Reserved. "Business Source License" is a trademark of MariaDB Corporation Ab. Parameters • Licensor: HashiCorp, Inc. • Licensed Work: Vagrant 2.4.0. The Licensed Work is ¥ (c) 2023 HashiCorn Inc. ✓ I accept the terms in the License Agreement Print Back 💎 Install Cancel

Now we have all the files available it is time to build the Virtual machine

Mode	Lastl	WriteTime	Length	Name
	10/4/2023	2:20 PM		metasploitable3-master
	11/19/2023	1:32 AM		packer_1.9.4_windows_amd64
d	11/19/2023	1:32 AM		vagrant-reload-master
-a	10/16/2023	8:20 PM	288215040	vagrant_2.4.0_windows_i686.msi
PS C:\User	s\mohas\Desktop`	\metasploita	ble3-workspa	ce> Set-ExecutionPolicy -Scope CurrentUser Unrestricted

[T] TES [A] TES LO ATT [N] NO [L] NO LO ATT [S] Suspend [F] Help (detau.

Vagrant file Download, all the files should be saved in one folder

PS C:\Users\mohas\Desktop\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/me tasploitable3/master/Vagrantfile" -OutFile "Vagrantfile" PS C:\Users\mohas\Desktop\metasploitable3-workspace>
Now open your command prompt and install some dependencies with vagrant

Command Prompt

- 🗆 🗙

C:\Users\mohas>Vagrant plugin install vagrant-vbguest _____ Installing the 'vagrant-vbguest' plugin. This can take a few minutes... Installed the plugin 'vagrant-vbguest (0.31.0)'!

C:\Users\mohas>Vagrant plugin install vagrant-reload Installing the 'vagrant-reload' plugin. This can take a few minutes... Installed the plugin 'vagrant-reload (0.0.1)'!

C:\Users\mohas>

It is now time to build the VM using a powershell script called build.ps1 inside metasplitable3 folder we downloaded, running the script without any argument with prompt us for confirmation, if we y the script will build 2 VMs for us linux and windows version of the VM, but typing n will make the script to exit show us the arguments to choose from.

PS C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master> .\build.ps1

Compatible version of VirtualBox found. Compatible version of Packer found. Compatible version of Vagrant found. Compatible version of vagrant-reload plugin found. All requirements found. Proceeding... No box name passed as input. Build both the boxes ? (y/n): n To build metasploitable boxes separately, use the following commands: - .\build.ps1 windows2008 - .\build.ps1 ubuntu1404

We interested in building windows server 2008 so we will choose it

PS C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master> .\<mark>build.ps1</mark> windows2008

Compatible version of VirtualBox found. Compatible version of Packer found. Compatible version of Vagrant found. Compatible version of vagrant-reload plugin found. All requirements found. Proceeding... Building metasploitable3-win2k8 Vagrant box... Warning: Bundled plugins used

This template relies on the use of plugins bundled into the Packer binary. The practice of bundling external plugins into Packer will be removed in an upcoming version.

To remove this warning and ensure builds keep working you can install these external plugins with the 'packer plugins install' command

* packer plugins install github.com/hashicorp/virtualbox * packer plugins install github.com/hashicorp/qemu * packer plugins install github.com/hashicorp/vagrant * packer plugins install github.com/hashicorp/vmware

Alternatively, if you upgrade your templates to HCL2, you can use 'packer init' with a 'required_plugins' block to automatically install external plugins.

You can try HCL2 by running 'packer hcl2_upgrade C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master\packer\templates\windows_2008_r2.json'

virtualbox-iso: output will be in this color.

==> virtualbox-iso: Retrieving Guest additions

==> virtualbox-iso: Trying C:\Program Files\Oracle\VirtualBox/VBoxGuestAdditions.iso

==> virtualbox-iso: Trying file://C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso

==> virtualbox-iso: file://C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso => C:/Program Files/Oracle/Virtua 1Box/VBoxGuestAdditions.iso

==> virtualbox-iso: Retrieving ISO

==> virtualbox-iso: Trying https://download.microsoft.com/download/4/1/D/41DEA7E0-B30D-4012-A1E3-F24DC03BA1BB/7601.17514 .101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN_DVD.iso

The Downloading and Building the VM takes longer time to complete, it depends on your system performance and network speed, after building the VM type vagrant up win2k8 to import it to Virtualbox

PS C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master> vagrant up win2k8 Bringing machine 'win2k8' up with 'virtualbox' provider... ==> win2k8: Importing base box 'rapid7/metasploitable3-win2k8'... ==> win2k8: Matching MAC address for NAT networking... ==> win2k8: Checking if box 'rapid7/metasploitable3-win2k8' version '0.1.0-weekly' is up to date... ==> win2k8: Checking if box 'rapid7/metasploitable3-win2k8' version '0.1.0-weekly' is up to date... ==> win2k8: Setting the name of the VM: metasploitable3-master_win2k8_1700418129117_8961 ==> win2k8: Clearing any previously set network interfaces... A host only network interface you're attempting to configure via DHCP already has a conflicting host only adapter with DHCP enabled. The DHCP on this adapter is incompatible with the DHCP settings. Two host only network interfaces are not allowed to overlap, and each host only network interface can have only one DHCP server. Please reconfigure your host only network or remove the virtual machine using the other host only network. PS C:\Users\mohas\Desktop\metasploitable3-workspace\metasploitable3-master>

Here we go, we logon with username vagrant and password vagrant



Now before renaming and joining the Vm to the Domain, let's change the network configuration

Z Administrator: Windows PowerShell	
√indows PowerShell Copyright (C) 2016 Microsoft Corporation. All rights reserved.	_
Loading personal and system profiles took 11145ms. PS C:\Users\vagrant> ipconfig	
lindows IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::fd63:83a2:85e3:4729%11 IPv4 Address : 10.10.1.8 Subnet Mask : 255.255.255.0 Default Gateway : 10.10.1.1	
funnel adapter isatap.{6FEEDED4-FC1E-4857-BEB8-72167D5BDAA6}:	
Media State Media disconnected Connection-specific DNS Suffix . : PS C:\Users\vagrant> _	
Link-local IPv6 Address : fe80::fd63:83a2:85e3:4729×11 IPv4 Address : 10.10.1.8 Subnet Mask : 255.255.25 Default Gateway : 10.10.1.1 Funnel adapter isatap.<6FEEDED4-FC1E-4857-BEB8-72167D5BDAA6>: Media State : Media disconnected Connection-specific DNS Suffix . : PS C:\Users\vagrant> _	

Here is the IPv4 Static Configuration

Internet Protocol Version 4 (TCP/IPv	14) Properties
General	
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
Obtain an IP address automatical	ly
• Use the following IP address:	
IP address:	10 . 10 . 1 . 8
Subnet mask:	255.255.255.0
Default gateway:	10 . 10 . 1 . 1
C Obtain DNS server address auton	natically
└ Use the following DNS server add	resses:
Preferred DNS server:	10 . 10 . 1 . 4
Alternate DNS server:	· · ·
Validate settings upon exit	Advanced
	OK Cancel

Search for rename this Computer to change the name of the computer to WS01 and join it to Byteshield Domain

Control Panel (4)	System Properties
🛃 Rename this computer	Computer Name/Domain Changes
I型 Change workgroup name I型 See the name of this computer	You can change the name and the membership of this computer. Changes might affect access to network resources. <u>More information</u> computer
Schange your Windows password	Computer name: WS01 Full computer name: WS01 More Member of Omain: BYTESHIELD.local Workgroup:
₽ See more results	OK Cancel
rena 🛛 Log off 🕨	OK Cancel Apply

🚬 Administrator: Windows PowerShell

Now We can Verify our setup

PS C:\Users\uagrant> ping dc01
Pinging DC01.BYTESHIELD.local [10.10.1.4] with 32 bytes of data:
Reply from 10.10.1.4: bytes=32 time=1ms TTL=128
Reply from 10.10.1.4: bytes=32 time(1ms TTL=128
Ping statistics for 10.10.1.4:
 Packets: Sent = 4. Received = 4. Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maxinum = 1ms, Average = 0ms
PS C:\Users\uagrant> ping win10-client-01
Pinging win10-client-01.BYTESHIELD.local [10.10.1.5] with 32 bytes of data:
Reply from 10.10.1.5: bytes=32 time(1ms TTL=128
Reply from 10.10.1.9: bytes=32 time(1ms TTL=128
Repl

We have done a lot of Installation setup, now we will focus on Domain and Sql server users and groups creation and their respective access rights

DC01 Users

joe.smith	david.williams	jessica.williams
lisa.jones	james.brown	mike.johnson
p.brown	justin.smith	Richard.White
enox	michelle.smith	
S.Service	Sql Service	

Users & Groups DC02 Users anthony.smith christopher.smith jessica.williams Jessy_adm tom.smith TRSql_Service

DC03 Users

amanda.jonespaul.jonesmichelle.Moorejason.johnsonjennifer.williamsClement.Kevinmichelle.johnsonmike.davisBrown.leeRuth.DavidTCSql_Service

Win10-Client-01 Users

jessica.williams joe.smith justin.smith local_adm p.brown

Win10-Client-02 Users

Ruth.David Brown.lee Richard.White

Clement.Kevin michelle.Moore

Now it is to start Creating users and groups, starting with DC01, logon and open sever manager



Right click on the administrator and click copy to Create an Admin user

Active Directory Users and Com	puters					_		\times		
File Action View Help										
⇐ ➡ Ź 💼 🗶 🗟 @ 🕞 🛛 🖬 🖏 🛍 🍸 💆 🍇										
Active Directory Users and Com Saved Queries BYTESHIELD.local BUIItin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator Allowed Cert Put Cloneab Coneab Coneab Coneab Donain Comain	Copy Add to a group Disable Account Reset Password Move Open Home Page Send Mail All Tasks Cut Delete Rename Properties Help	Type User re re re re re re re re re re re re r	oup oup oup oup oup oup oup oup oup oup oup	Description Built-in account for ad Members in this group c Members of this group Members of this group t Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue					
	Peter Brown		User	oup	members of this group			ļ		
< >	Revealed Use	rs	Security Gro	oup	Members of this group			~		
Contains actions that can be perform	ed on the item.									

David Williams as Admin User

Conv Object - User	Copy Object - User
Create in: BYTESHIELD.local/Users	Create in: BYTESHIELD.local/Users
First name: David Initials: Last name: Williams Full name: David Williams User logon name: @BYTESHIELD.local David.Williams @BYTESHIELD.local User logon name (pre-Windows 2000): David.Williams	Password: ••••••• Confirm password: ••••••• User must change password at next logon User cannot change password User cannot change password Password never expires Account is disabled Account is disabled
< Back Next > Can	cel C

 \times

Cancel

Right click on the users container > new to Create a Regular user

Active Directory Users and Com	puters				_		\times
File Action View Help							
⇐ ⇒ 🚈 🖬 🖌 📋 🗙 🛙	i 🗟 🖸	2 🖬 🗏 🐮 🖬	7 🗾 🐍				
Active Directory Users and Com Saved Queries Saved Queries BYTESHIELD.local Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Delegate Control Find Delegate Control Find New All Tasks View Refresh Export List Properties Help	Name Administ Allowed Cert Pub Cloneabl David Wi Denied R David Wi Denied R David Wi Denied R David Wi Denied R David Wi Cloneabl David Wi David David Wi David David	trator RODC Password Repl lishers le Domain Controllers illiams RODC Password Repli ins ateProxy Admins Computer Contact Group InetOrgPerson msDS-KeyCredential msDS-ResourcePrope msDS-ShadowPrincip msImaging-PSPs	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato I workstations and ser I domain controllers i I domain guests I domain users ssignated administrato embers of this group embers of this group embers in this group c ilt-in account for gue	•		
< >	Key Pete	MSMQ Queue Alias Printer		embers of this group			~
Creates a new item in this container.	Services	User 🚽				5	anvicas

Joe Smith as a regular user

New Object - User	× New Object - User ×
Create in: BYTESHIELD.local/Users	Create in: BYTESHIELD.local/Users
First name: joe Initials:	Password:
Last name: smith	Confirm password:
Full name: joe smith	User must change password at next logon
User logon name:	User cannot change password
joe.smith @BYTESHIELD.local ~	Password never expires
User logon name (pre-Windows 2000):	Account is disabled
BYTESHIELD\ joe.smith	
< Back Next > Cance	< Back Next > Cancel

We have Created two domain users, admin and a regular user Instruction

- > On DC01 Create the rest of the users with Sql_Service as Domain admin
- > On DC02 Create the Users with TRSql_Service and Jessy_admin as Domain Admins
- > On DC03 Create the Users with TCSql_Service and Paul.jones as Domain Admins
- > On the two Windows Clients logon with the respective Domain users
- > On WS01 make justin.smith a local admin, logon with p.brown Credentials also

After Users Creation, the next thing is to create user's groups, right anywhere within and select new > group

Active Directory Users and Com	puters		_	\times		
File Action View Help						
1 🗢 🔿 🚈 📰 🗋 🖾 🗟	🛓 🛛 📷 🐍 📚 🛅 🔻 🔎	38				
 Active Directory Users and Com Saved Queries BYTESHIELD.local Builtin 	Name Domain Controllers Domain Guests	Type Security Group Security Group	Description All domain controllers i All domain guests	Delega	te Control	
 Computers Domain Controllers 	Enterprise Admins	Security Group	Designated administrato	Find		
 ForeignSecurityPrincipal: Managed Service Accourties 	Enterprise Key Admins	Security Group Security Group	Members of this group Members of this group Members in this group c	New All Tasl	ks	Computer Contact
Users	Guest james brown	User User	Built-in account for gue	Refresh Export L	n List	Group
	bissica williams joe smith	User User		View		msDS-KeyCredential msDS-ResourcePropertyList
	 justin smith Keith Morgan Key Admins Security lisa jones User 	User User Sourite Course	March and a fability and an	Arrang Line up	e lcons o lcons	 msDS-ShadowPrincipalContainer msImaging-PSPs
		User User		Properties		MSMQ Queue Alias Printer
	Smike johnson Peter Brown	User User			Storage	User Shared Folder

Remote Desktop Users Group Creattion

Vew Oł	oject - Group		>
87	Create in:	BYTESHIELD.local/Users	
Group	o name:		
RDP	Users		
Group	o name (pre-Wind	lows 2000):	
RDP	Users		
Gro	up scope	Group type	
0	Domain local	 Security 	
۲	Global	ODistribution	
0	Universal		
		OK	Cancel

Now let's Create localuser group Policy for remote desktop access

🗐 Rup	· ·	×	J	Local Group Policy Editor				_	\times	
				File Action View Help						
Open:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. gpedit.msc Image: Start			File Action View Help Action View Help Computer Policy Computer Configuration Software Settings View Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Security Settings Administrative Templates View Configuration	Local Computer Policy Select an item to view its description.	Name Proputeton User Con	er Configuration figuration			

File Action View Help Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings <th>🗐 Local Group Policy Editor</th> <th></th> <th>- 🗆 X</th> <th></th> <th></th>	🗐 Local Group Policy Editor		- 🗆 X		
 In the second sec	File Action View Help			Allow log on through Remote Desktop Services Properties	? ×
Uccal Computer Policy Computer Configuration Software Settings Windows Settings Mame Resolution Policy Socurity Setting Access this computer from the network Exercise a papelile Administrators Socurity Setting Local Policies Local Policies Mindows Defender Fire Nume Resolution Policy Socurity Settings Allow log on through Remote Desktop Services Administrators Security Settings Local Policies Numok Defender Fire Numok Definder Create a papelile Create a papelile on Control Policies Policy-based QoS Policy-based QoS Pelly log on as a service<	🗢 🄿 🙍 📷 🗟 🖬			Local Security Setting Explain	
OK Cancel Apply	 Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Local Policies Local Policy Security Options Windows Defender Fire Network List Manager F Software Restriction Po Software Restriction Po Software Restriction Po Software Audit Policy IP Security Policies on L Advanced Audit Policy Policy-based QoS Administrative Templates 	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 time zone Create a pagefile Create a token object Create global objects Create permanent shared objects Create symbolic links Debug programs Deny access to this computer from the network Deny log on as a batch job	Security Setting Everyone, Authenticated Authenticated Users LOCAL SERVICE, NETWO Administrators, Account Administrators, Server O. Everyone, Authenticated LOCAL SERVICE, Admini. LOCAL SERVICE, Admini. Administrators LOCAL SERVICE, NETWO Administrators Administrators	Allow log on through Remote Desktop Services Administrators Add User or Group	
	< · · · · · · · · · · · · · · · · · · ·	<	>	OK Cancel	Apply

Now Let's Search for the RDP users Group we just Created

Allow log on through Remote Desktop Services Properties ?	\times		Multiple Names F	ound			
Select Users, Computers, Service Accounts, or Groups Select this object type: Users, Service Accounts, Groups, or Built-in security principals From this location: BYTESHIELD.local	Object Ty	ypes	More than one obje from this list, or, reer Matching name	ct matched the name "RD nter the name. s:	". Select one or mor	e names	
Enter the object names to select (examples): RD Advanced OK Advanced Rd Add User or Group Remove	Check N	lames LOC, Adm LOC, Adm Adm	Name RDP Users RDS Endp RDS Mana RDS Remo	Logon Name (pr RDP Users noint RDS Endpoint S age RDS Manageme ote RDS Remote Ac	E-Mail Address	Description	In Folder BYTESHIELD.Io BYTESHIELD.Io BYTESHIELD.Io BYTESHIELD.Io
OK Cancel	Apply						OK Cancel

Remote Desktop Service is disabled by default, we can enable it

			System Properties ×
Dashboard	For DC01		Computer Name Hardware Advanced Remote
Local Server	Committee assess	0(2)	Remote Assistance Allow Remote Assistance connections to this computer
All Servers	Domain	BYTESHIELD.local	
AD DS			Advanced
B DNS			Remote Desktop
ii File and Storage Services ♪	Windows Defender Firewall Remote management Remote Desktop NIC Teaming Ethernet	Private: On Enabled Disabled Disabled 10.10.1.4	Choose an option, and then specify who can connect.

Let's Jessica Williams to the RDP users and Remote management service Groups

General Members Member Of Managed By Members: Name Active Directory Domain Services Folder & jessica williams BYTESHIELD.local/Users	
Members: Name Active Directory Domain Services Folder & jessica williams BYTESHIELD.local/Users	
Name Active Directory Domain Services Folder § jessica williams BYTESHIELD.local/Users	
🔏 jessica williams 🛛 BYTESHIELD.local/Users	
Add Remove	
OK Cancel Apply	

Remote N	/lanageme	nt Users Pro	perties		?	×
General	Members	Member Of	Managed B	У		
Member	rs:					
Name		Active Dir	rectory Domai	in Services Folde	er	
👗 jes	sica williams	BYTESH	ELD.local/U	sers		
Ad	d	Remove				
			ОК	Cancel	Ap	ply

Foreign Group membership, we are Create a local and Universal BYTESHIELD Domain Group and map them to TRUSTEDCORP as Foreign Members and and vise versa, By default Domain groups are created as global groups, we will change that to domain local group, we have michelle and mike as member of the domain local group

ew Object - Group			
Create in: BYTE	SHIELD.local/Users		
Group name:			
Foreign Members Group			
Group name (pre-Windows 20	000):		
Foreign Members Group			
Group scope	Group type		
Domain local	Security		
O Global	Oistribution		
OUniversal			
		OK Capita	

oreign Members Group Properties			\times				
General Members	Member Of Managed By						
Members:							
Name	Active Directory Domain Service	s Folder					
👗 michelle smith	BYTESHIELD.local/Users						
گ mike johnson	BYTESHIELD.local/Users						
Add	Add Remove						
	OK Canc	el /	Apply				

We will Create Domain localgroup in BYTESHIELD and add some TRUSTEDCORP domain Users as foreign group members and vice versa.

TC Foreig	gn Group M	lembers Loc	al Properties		?	\times
General	Members	Member Of	Managed By			
Membe	rs:					
Name	•	Active Dire	ectory Domain	Services Folder		
8 M	ichelle.Smith	BYTESHI	ELD			
👫 М	ike.Johnson	BYTESHI	ELD			
0.0		Demaura				
AC	JU	nemove				
			ОК	Cancel	App	oly

Foriegn Group Members Local Properties	?	×
General Members Member Of Managed By		-
Members:		
Name Active Directory Domain Services Folder		
Amanda.Jones TRUSTEDCORP Ruth.David TRUSTEDCORP		
Add Remove OK Cancel	Appl	У

Creating SQL Server Users Frank and Robert, Win10-Client-01 we Create 3 Users, 2 with Sql Authentication while 1 Windows authentication



Creating SQL User



Select a page	🗊 Sonat 🔹 🕢 Help			
A Server Roles A User Mapping Socurables A Status	Login name:	man at read larger		Search
	Mapped to asymmetric key Map to Credential	-		10.44
Connection Server: WINTOCLIENT-01 Connection BYTESHELD/P-Brown VT Mew connection properties	Mapped Grederitain	Credential	E	100
Progress		¢	,	Remove
Ready	Default database	matter	é	
200	Default language:	(default)	Ŷ	

Select User, Service Account, or Group		×
Select this object type: User or Built-in security principal		Object Types
From this location: Entire Directory		Locations
<u>E</u> nter the object name to select (<u>examples</u>): Justin Smith (Justin.Smith@BYTESHIELD.local)		Check Names
Advanced	ОК	Cancel

We have made justin.smith as SQL server user with public role, we are going to make the user to impersonate the the systemadmin

			Ye Select Objects	
Select a page General Server Roles User Mapping Securables Status	Login name: BYTESHIELD'Justin.Smith Securables:	Search	Select these object types:	hiert Tynes
	Name WIN10-CLIENT-01	Type Server		jeer types
			Enter the object names to select (<u>examples</u>):	
			C	Check Names
	<			Browse
Connection Server:	< Permissions for WIN10-CLIENT-01: Control - Permissions			Browse
Connection Server: WIN10-CLIENT-01 Connection: BYTESHIELD\P_Brown	< Permissions for WIN10-CLIENT-01: Explicit Effective Permission Grantor Administer bulk operat	Grant With Grant Deny		Browse
Connection Server: WIN10-CLIENT-01 Connection: BYTESHIELD\P Brown YF Mew connection propertie	Permissions for WIN10-CLIENT-01: Explicit Effective Permission Granter Administer bulk operat Alter any availability gr Alter any connection Alter any connection Alter any condential	Grant With Grant Deny	OK Cancel	Browse Help
Connection Server: WIN10-CLIENT-01 Connection: BYTESHIELD\P Brown Y¥ Mew connection propertie	Permissions for WIN10-CLIENT-01: Explicit Effective Permission Grantor Administer bulk operat Ater any connection Ater any connection Ater any database Ater any database Ater any database	Grant With Grant Deny	OK Cancel	Browse Help

Impersonating sa

🐕 Select Object Types		×	📽 Select Objects		×
Select the types of objects to find:			Select these object types:		
Object Type 🔺			Logins	Object Types	
🔲 👯 Availability Groups					
Endpoints					
🔽 📲 Logins					
Server roles			Enter the object names to select (<u>examples</u>):		
Servers				Check Names	
				Chicon Hamoo	
				Browse	
				1	
	OK Cancel Help		OK	ancel Help	
		—		neip	

Impersonating sa

		Login Properties - BYTESHIELD\Justin.Smith				53		
S Browse for Objects	×	Select a page D General D Server Roles D User Mapping D Securables Status	ゴ Sonpt 👻 🚱 Help					
· · · · · · · · · · · · · · · · · · ·			Login name: BYTESHIELD\Juittin Smith					
			Securables Name			Search		
13 objects were found matching the types you selected.							Login	
Mataking akingto.								
Name	Typ ^							
INT SERVICE\SQLTELEMETRY]	Lo.							
INT SERVICE\SQLWriter]	Lo.		x				,	
□ 🔐 [NT SERVICE\Winmgmt]	Lo.	Server:	Permissions for sa: Explicit Effective					
Robert]	Lo.	Connection	Permission	Grantor	Grant	With Grant	Deny	
	10	BYTESHIELD\P.Brown	Alter		8			
	LU.	View connection properties	Impersonate					
			View definition					
<	>	Program						
		(Ready						
OK Cancel	Help		(e				-	
	· · ·					ОК	Cancel	

On ROOT-DC01 we are also going to Create 2 SQL users David and Kevin, David with have public role on database with Kevin will have db_owner role on the same database, we are going to make David to Impersonate Kevin

Creating the Database



Here we create the database owned by Administrator

Select a page & General	🗊 Script 👻 🕜 Help									
General Options Filegroups	Database name Owner: Database full-text (Database files Logical Name IT-DEPT IT-DEPT_Jog	File Type RoWS LOG	Filegroup PRIMARY Not Applicable	ELD Administrator Initial Size (MB) 8	Autogrowth By 64 MB, By 64 MB,	∕ Maxsize Unlimited Unlimited		Pa C: C:		
Connection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator Y# Mew connection properties										
Progress								_		
C Ready	¢			Add		Re	move	>		
Creating the users the same way Created for Win10-Client-01

			. Ц. 100					
🖵 Soript 👻 🕜 Help				Select a page & General	💭 Sonpt 👻 🕢 Help			
Login name: Viindows authentication SQL Server authentication Password: Confirm password: Specify old password Old password Enforce password policy Enforce password policy Enforce password expire User must change pass Maped to certificate	David		Search.	 Server Koles Securables Securables Status 	Login name: Vindows authentication SQL Server authentication Password: Confirm password: Specify eld password Old password Old password Enforce password polic Enforce password polic User must change pass Mapped to certificate	Kevin		Search
Mapped to asymmetric key			1		Map to Credential		20 20	644
Mapped Credentials	Credential	F	100	Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator	Mapped Credentials	Credential	F	nuu
	٤	>	Remove	Progress		¢	>	Remove
Default database: Default language:	master <default></default>	~ ~		C Ready	Default database: Default language	mester <default></default>	* *	
	Soript Heip Login name: Vindows authentication SQL Server authentication Password: Confirm password: Specify old perevord Off password Enforce password policy Enforce password policy Enforce password expira User must change passa Mapped to certificate Mapped to asymmetric key Map to Credential Mapped Credentials Default database: Default database:	Image: Soript ▼ Payle Login name: David ○ Windows authentication ● SOL Server authentication Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	Soript Help Login name: David Windows authentication SQL Server authentication Password: Confirm password: Specify old presword Ott password Ott password Enforce password expiration User must change password at next login Mapped to certificate Mapped to certificate Mapped Credential Mapped Credentials Credential Mapped Credentials Credential F Default database: Default language:	Script Help Login name: David Search, Add Add Apped to certificate Mapped Credential Credential Credential Add Terferetit database: Default database: Cedefult> Cedefult> Cedefult> Cedefult> Cedefult Cedefult Cedefult Cedefult Cedefu	Script ▼ Help Login name: David Windows authentication Search, ♥ Server Authentication Search, ♥ SQL Server authentication Security of password: Ording password: Ording password: ○ Decdy of password: Security of password: ○ Decdy of password: Security of password: ○ Decdy of password: Security of password: ○ Decdy of password policy Enforce password expiration ○ User must change password at next login Mapped to certificate ○ Mapped to certificate Y ○ Mapped Credential f Mapped Credentials Credential Credential f Wapped Credentials Remove Progress Ready	Soript → → Help Soript → → Help Login name: □ avid O Windows authentication Search, S SQL Server authentication Search, S SQL Server authentication Search, Password: ••••••••••••••••••••••••••••••••••••	Script ▼ Help Script ▼ Help Login name: David Windows authentication Select noce Password: User Mapping Society of password: Windows authentication Password: Status General Society of password: Outpassword: Windows authentication Password: Windows authentication Bacedry of password Status Grin password: Windows authentication Windows authentication Password: Grin password: Windows authentication Bacedry of password Status Grin password: Windows authentication Defeation password policy Enforce password policy Enforce password policy Enforce password an reat login Mapped to asymmetric key Mapped to asymmetric key Mapped to certificate Windows authentication Broce Codential Connection Broce Codential Cedential Mapped Credentials Credential Connection: Broce Codential Mapped Credentials Credential	Soript ▼ Help Soript ▼ Help Login name: David Soript ▼ Help Soript ▼ Help Soript ▼ Help Login name: Karvin Soript ▼ Help Soript ▼ Soript ♥ Soript ♥

Now Let's Give Kevin the db_owner role on the database we created, that give Kevin the ability to elevate his role sa, while David can impersonate Kevin

🔎 General	LJ Script ∓ 😡 Help			
Server Roles	Users mapped to this login:			
Securables	Map Database	User	Default Schema	
Status	IT-DEPT	Kevin		i e
	master			
	model			
	msdb			
	L tempdb			
Connection	c			>
Connection	C Guest account enabled for:	IT-DEPT		>
Connection Server: ROOT-DC01\BS_SQLSERVER	C Guest account enabled for: Database role membership for:	IT-DEPT		>
Connection Server: ROOT-DC01\BS_SQLSERVER Connection:	C Guest account enabled for: Database role membership for:	IT-DEPT		>
Connection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator	Guest account enabled for Detabase role membership for: db_accessadmin db_backupoperator	IT-DEPT		>
Connection Server: ROOT-DC01\B5_SQLSERVER Connection: BYTESHIELD\Administrator YTESHIELD\Administrator	Guest account enabled for Database role membership for: db_accessadmin db_backupoperator db_detareader	IT-DERT		>
Connection Server: ROOT-DC01\B5_SQLSERVER Connection: BYTESHIELD\Administrator YTESHIELD\Administrator	Cuest account enabled for Database role membership for: db_accessadmin db_backupoperator db_datareader db_datawriter db_datadmin	IT-DEPT		>
Connection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator YTESHIELD\Administrator	Cuest secount enabled for Database role membership for: db_accessadmin db_backupoperator db_datareader db_datawriter db_datawriter db_datarin db_denydatareader	IT-DEPT		>
Connection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator YT View connection properties	Guest account enabled for Database role membership for: db_accessadmin db_backupoperator db_datamader db_ddtawniter db_ddtadmin db_ddenydat areader db_denydat awriter	IT-DEPT		>
Connection Server: ROOT-DC01\B5_SQLSERVER Connection: BYTESHIELD\Administrator YT Mew connection properties	 Guest account enabled for Database role membership for: db_accessadmin db_backupoperator db_dataevader db_datawriter db_datawriter db_denydat avriter db_decurityadmin 	IT-DEPT		>
Connection Server: ROOT-DC01\B5_SQLSERVER Connection: BYTESHIELD\Administrator YT View connection properties Progress Ready	 Guest account enabled for Database role membership for: db_accessadmin db_backupoperator db_datawater db_ddladmin db_ddladmin db_denydat areader 	IT-DEPT.		>
Connection Server: ROOT-DC01\B5_SQLSERVER Connection: BYTESHIELD\Administrator YT View connection properties Progress Ready	 Guest account enabled for: Database role membership for: db_accessadmin db_backupoperator db_datawriter db_datawriter db_datawriter db_denydat are ader db_denydat awriter 	IT-DEPT IT-DEPT		3

Now we will let David Impersonate Kevin

Select a page General	🖵 Script 👻 😮 Help				
Server Roles User Mapping	Login name: David	1			
Securables	Securables:			19	Search
	Name			т	ype
	🚔 Kevin	💒 Kevin			
onnection	¢				_
Connection Server: ROOT-DC01\BS_SQLSERVER	< Permissions for Kevin Explicit Effective				
Connection Server: ROOT-DC01\BS_SQLSERVER Connection:	< Permissions for Kevin Explicit Effective Permission	Grantor	Grant	With Grant	Deny
onnection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator	< Permissions for Kevin Explicit Effective Permission Atter Cost of	Grantor	Grant	With Grant	Deny
onnection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator W Mew connection properties	< Permissions for Kevin Explicit Effective Permission Atter Control	Grantor	Grant	With Grant	Deny
Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator YTESHIELD\Administrator	Permissions for Kevin Explicit Effective Permission Atter Control Impersonate Impersonate	Grantor	Grant	With Grant	Deny
onnection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator W View.connection.properties	Permissions for Kevin Explicit Effective Permission Atter Control Impersonate View definition	Grantor Kevin	Grant	With Grant	Deny
onnection Server: ROOT-DC01\BS_SQLSERVER Connection: BYTESHIELD\Administrator W View connection properties	Permissions for Kevin Explicit Effective Permission Atter Control Impersonate Impersonate View definition	Grantor Kevin	Grant	With Grant	Deny

Creating SPN for SQL Server on ROOT-DC01

PS C:\Users\Administrator> setspn.exe -S "BS_SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433" "BYTESHIELD\Sql_Service" Checking domain DC=BYTESHIELD,DC=local

Registering ServicePrincipalNames for CN=Sql_Service,CN=Users,DC=BYTESHIELD,DC=local BS_SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433 Updated object

```
N=Sql_Service,CN=Users,DC=BYTESHIELD,DC=local
       BS SQLSERVER/ROOT-DC01.BYTESHIELD.local:1433
N=WIN10-CLIENT-02,CN=Computers,DC=BYTESHIELD,DC=local
       RestrictedKrbHost/WIN10-CLIENT-02
       HOST/WIN10-CLIENT-02
       RestrictedKrbHost/Win10-Client-02.BYTESHIELD.local
       HOST/Win10-Client-02.BYTESHIELD.local
N=WIN10-CLIENT-01, CN=Computers, DC=BYTESHIELD, DC=local
       MSSQLSvc/Win10-Client-01.BYTESHIELD.local:1433
       MSSQLSvc/Win10-Client-01.BYTESHIELD.local
       RestrictedKrbHost/WIN10-CLIENT-01
       HOST/WIN10-CLIENT-01
       RestrictedKrbHost/Win10-Client-01.BYTESHIELD.local
       HOST/Win10-Client-01.BYTESHIELD.local
N=WS01,CN=Computers,DC=BYTESHIELD,DC=local
       TERMSRV/WS01
       TERMSRV/WS01.BYTESHIELD.local
       WSMAN/WS01
       WSMAN/WS01.BYTESHIELD.local
       RestrictedKrbHost/WS01
       HOST/WS01
       RestrictedKrbHost/WS01.BYTESHIELD.local
       HOST/WS01.BYTESHIELD.local
```

On TRUSTED-DC03 Let's give justin.smith Sysadmin role for cross forest authentication on the SQL server



Sql Cross forest Authentication

Select User, Service Account, or Group		×
Select this object type:		-
User or Built-in security principal	(Object Types
From this location:		
BYTESHIELD.local		Locations
Enter the object name to select (<u>examples</u>):		
Justin Smith (Justin.Smith@BYTESHIELD.local)		Check Names
1		
Advanced	ОК	Cancel

Select a page				
🔑 General	LJ Sonpt 👻 🚱 Help			
Server Roles	Login name	BYTESHIELD Justin Smith	1	Search
Status	Windows authentication			
	SQL Server authentication			
	Palesword			
	Confirm password:			
	Specify aid password			
	Old password			
	C Enforce password policy			
	[v] Enforce passwort expra	ition		
	💬 Usermuit change panny	word at next login.		
	 Mapped to certificate 	4	~	
	 Mapped to asymmetric key 		1	
Connection	Map to Credential		~	Add
Connection	Mapped Credentials	Credential	F	
TRUSTED-DC03\TC_SQLSERVE				
Connection:				
View connection properties				
			/	
Program		<	>	Remove
Ready	Default database:	master	~	
14.4.5 V		orderfault >	<u> </u>	

Giving Justin.smith sysadmin on the Server

Login Properties - BYTESHIE	LD\Justin.Smith	-		\times
Select a page & General & Server Roles User Mapping & Securables & Status	Soript Help Server role is used to grant server-wide security privileges to a user. Server roles: bulk admin docreator diskadmin processadmin public securityadmin serveradmin setupadmin			
Connection Server: TRUSTED-DC03\TC_SQLSERVE Connection:				
sa V¥ Mew connection properties				
Progress				
C Ready				
	[ок	Car	ncel

Creating SPN for SQL Server on TRUSTED-DC03

PS C:\Users\Administrator> setspn.exe -S "TC_SQLSERVER/TRUSTED-DC03.TRUSTEDCORP.local:1433" "TRUSTEDCORP\TCSql_Service"
Checking domain DC=TRUSTEDCORP,DC=local

Registering ServicePrincipalNames for CN=TCSql_Service,CN=Users,DC=TRUSTEDCORP,DC=local TC_SQLSERVER/TRUSTED-DC03.TRUSTEDCORP.local:1433 Updated object

CN=TCSql_Service,CN=Users,DC=TRUSTEDCORP,DC=local TC_SQLSERVER/TRUSTED-DC03.TRUSTEDCORP.local:1433 CN=WS01,CN=Computers,DC=TRUSTEDCORP,DC=local TERMSRV/WS01 TERMSRV/WS01.TRUSTEDCORP.local WSMAN/WS01 WSMAN/WS01.TRUSTEDCORP.local RestrictedKrbHost/WS01 HOST/WS01 RestrictedKrbHost/WS01.TRUSTEDCORP.local HOST/WS01.TRUSTEDCORP.local

Unconstrained Delegation Setup, we are going to use Win10-Client-02 for unconstrained delegation and also make it a member of domain admins group because it is going to be admin Workstation

WIN10-C	LIENT-02 Pro	opertie	5			7	\times
General	Operating Sy	stem	Member Of	Delegation	Location	Managed By	Dial-In
Delega behalf	tion is a securi of another use	ty-sene r.	itive operatio	n, which allow	vs services	to act on	
O Do	not trust this co	ompute	r for delegatio	on			
Tru:	st this compute	r for de	legation to a	ny service (Ki	erberos only	0	
OTrue	st this compute	er for de	legation to a	pecified service	ces only		
	Use Kerberos	only	locotocol				
Sei	rvices to which	n This ac	count can p	resent delega	ied creden	timber	
S	ervice Type	User o	or Computer	Port		Service N	
						STERIOR IN S	
	Emanded			100			
	Expanded			Add	Be	move	
	Expanded			Add	Be	mave	
	Expanded			Add	Fie	move	
	Expanded			Add	File	mno Ne	

Constrained Delegation Setup, we are going to use Win10-Client-01 for constrained delegation

WIN10	O-CLIENT-01 Pro	operti	es					?	\times
Gene	ral Operating Sy	vstem	Member Of	Dele	gation	Location	Managed	Ву	Dial-in
Dele beha	egation is a securi alf of another use Do not trust this co Frust this compute	ty-sen: r. ompute er for d	sitive operatio er for delegatio elegation to a	n, whi on ny ser	ch allow vice (Ke	s services	to act on		
١	Trust this compute ● Use Kerberos ○ Use any authe Services to which	er for d only enticat h this a	elegation to s ion protocol ccount can p	pecifie resent	ed servic	es only	ntials:		
	Service Type	User	or Computer		Port		Service Ni		
	cifs Idap	ROO	T-DC01 T-DC01.BYT	E S			BYTESHII ForestDns		
	<						>		
l	Expanded				Add	R	emove		
			ок	0	Cancel	, A	pply		Help

Resource-based constrained delegation RBDC setup, we are going to create a group and name it RBDC group, this group will have write permission over WS01 and justin.smith with have full permission over the group, that will give our user ability to add himself to the group, james.brown is a member to the group

RBCD Group Properties	? ×	W501 Properties	? ×
Object Security General Members Member Of	Attribute Editor Managed By	General Operating System Member Of Location Managed By Object Sect Group or user names:	Delegation Password Replication unity Dial-in Attribute Editor
Members: Name Active Directory Domain Ser Sames Brown BYTESHIELD.local/Users	rvices Folder	Key Admins (BYTESHIELD\Key Admins) Key Admins (BYTESHIELD\Enterprise Key Admins (BYTESHIELD\Enterprise Administrators (BYTESHIELD\Administrators) Account Operators (BYTESHIELD\Administrators) Print Operators (BYTESHIELD\Administrators) Rec-Windows 2000 Compatible Access (BYTE ReCD Group (BYTESHIELD\RBCD Group)	se Key Admins) perators)) SHIELD\Pre-Windows 2000 C
	2 F	Permissions for RBCD Group Full control Read Write Create all child objects Delete all child objects Allowed to authenticate	Add Remove
Add Remove		For special permissions or advanced settings, click	Advanced. Advanced

Now Our user has full control over the Group, the user can add himself to the group



On TRUSTED-DC03 we going to make Clement to have ExtendedRight over Ruth.David

	ertific	ates	Member Of	Passwor	d Replica	ation	Dial-in	Objec
Remote	Deskt	top Se	rvices Profile	C	OM+	1	Attribute Ed	ditor
General	Add	ress	Account	Profile	Telepł	nones	Organi	ization
Security		En	vironment	Sess	sions	F	Remote cor	ntrol
Group or u	iser na	ames:						
St Even	one							~
	ATOR	OWN	FR					
SEL SEL E	:		211					
S. Authe	anticat	tod Lle	ore					
	TEM				-			
	Pot M	bite (C	lement White	OTRUST		locall		
		mine (C	TRUSTEDCO	BB\Domai	in Admine	a)		
Doma	ant Au		110312000	The Double	an Aurontis			~
					Add		Remov	/e
					Add		Remov	/e
Permission	is for (Clemer	nt White		Add	Nlow	Remov	/e
Permission	s for (Clemer	nt White		Add A	Nlow	Remov Deny	/e /
Permission Change Receive	passi as for (Clemer word	nt White		Add A [[Remov Deny	/e /
Permission Change Receive Reset p	as for (passi e as asswo	Clemer word	nt White		Add A [Remov Deny	/e
Permission Change Receive Reset p Send as	e passi e as asswo	Clemer word ord	nt White		Add A [[[Remov Deny	/e
Permission Change Receive Reset p Send as Read as	as for (passi asswo	Clemer word ord	nt White	_	۸dd ۹ ۱ ۱ ۱ ۱		Remov Deny	/e
Permission Change Receive Reset p Send as Read ad	as for (passue as asswo	Clemer word ord it restri	nt White	_	Add A [[[[]		Remov	/e
Permission Change Receive Reset p Send as Read ac Write ad	as for (passi e as asswo s ccoun	Clemer word ord t restri	nt White ctions ctions	-	Add A [[[[[] []			/e / ^
Permission Change Receive Reset p Send as Read ac Write ac	e as asswo ccoun	Clemer word ord t restri	nt White ctions ctions	l settings	Add A [[[[[[]]		Remov	/e
Permission Change Receive Reset p Send as Read ad Write ac For special	as for (passi asswo coun coun	Clemer word ord t restri	nt White ctions ctions s or advanced	l settings, c	Add Add [[[[]]]]]		Remov Deny C C C C C C C C C C C C C C C C C C C	d
Permission Change Receive Reset p Send as Read ad Write ad Write ad Por special Advanced	as for (passi asswo ccoun ccoun l perm	Clemer word ord trestri	nt White ctions ctions s or advanced	l settings, c	Add		Remov Deny C C C C C C C C C C C C C C C C C C C	d

While Michelle.Johnson will have Don not Require Kerberos preauthentication

selected

Published Ce Security Remote D	ntificates En Desktop Se	Member Of vironment rvices Profile	Passwor Sess C	d Replication ions OM+	Dial-in Remote c Attribute	Object ontrol Editor
General	Address	Account	Profile	Telephone	a Orga	nization
User logon i	name:					
Michelle.Jo	hnson		@TRU	STEDCORP	local	\sim
User logon a	name (pre-	Windows 2000	0):			
TRUSTED	CORP		Michelle	Johnson		
Unlock a	account					
Account op	account tions: inly Kerber iccount su	os DES encryp pports Kerbero pports Kerbero	tion types a AES 121 a AES 256	for this acco 8 bit encryptic 5 bit encryptic	unt m.	^
Account op	account tions: inly Kerber account su account su account su account su account su account su	os DES encryp pports Kerbero pports Kerbero erberos preaut	tion types s AES 12 s AES 250 henticatio	for this accor 8 bit encryptic 5 bit encryptic n	unt m.	د ۲
Account op	account tions: inly Kerberr iccount su iccount su iccou	os DES encryp pports Kerbero pports Kerbero erberos preaut	ntion types a AES 12 s AES 25 henticatio	for this acco 8 bit encryptic 5 bit encryptic n	unt m	< >

Michelle.johnson is a member of help desk user group while help desk user group has write privilege over StdBy Admins

elp Desk Proper	ties		?	\times
Object	Secu	rity	Attribute Edito	r
General	Members	Member Of	Manage	d By
Members:				
Name	Active Direc	tory Domain Servio	ces Folder	
👗 Michelle Jol	hn TRUSTEDO	ORP.local/Users		
Add	Remove			

General	Members	Member C	Уf	Managed I	Вy
Object	Secur	ity	Attrib	ute Editor	
aroup or user na	ames:				
SCREATOR	OWNER				-
🎎 Help Desk	(TRUSTEDCORP\	Help Desk)			
SELF					П
Authentica	ted Users				
SYSTEM					
📲 Domain Ad	mins (TRUSTEDCO	RP\Domain /	Admins)		~
		Ac	ld	Remove	
amissions for	Help Deek		Allow	Denv	
Eull control	holp beak				/
Pand					
neau					
Write					
Write Create all chil	d objects				
Write Create all chil	d objects				
Write Create all chil Delete all chil	d objects d objects				,
Write Create all chil Delete all chil or special perm	d objects d objects nissions or advanced	d settings, clic	k	Advanced	,
Write Create all chil Delete all chil or special perm dvanced.	d objects d objects hissions or advanced	d settings, clic	k	Advanced	
Write Create all chil Delete all chil or special perm dvanced.	d objects d objects nissions or advanced	d settings, clic	k	Advanced	
Write Create all chil Delete all chil or special perm dvanced.	d objects d objects iissions or advanced	d settings, clic	k	Advanced	

BYTESHIELD Domain User James Brown should be a member of Backup Operators of TRUSTEDCORP

ckup Operators Properties				ī	?	×
Object	Sec	curity	Д	ttribute E	ditor	
General	Members	Membe	er Of	Mana	aged By	,
Members:						
Name	Active Dire	ectory Domain	n Services	Folder		
👫 James.Brov	wn BYTESHI	ELD				
		1				
Add	Remove]				
Add	Remove]				