

Active Directory Felaketten Dönüş Prosedürü

Hasan Dimdik

İçerik

	Döküman Kontrolü	2
	Referans Dosyaları	. 2
	Döküman Kabulü	. 2
	Active Directory Takımı	3
	Birincil İrtibat Takımları/Kişileri	3
	Active Directory' nin Bağımlı Olduğu Katmanlar	. 3
	AD Entegrasyonları	. 3
	Active Directory FSMO Rollerinin Dağılımı	. 4
	Active Directory Mimarisi, Sunucuları vb	. 4
A	ctive Directory Kurtarma Prosedürü	5
Ye	edekten Geri Dönme Adımları	. 7
K	urtarma Sonrası Yapılacaklar 1	13
Μ	etadata Cleanup ve FSMO Role Seizing1	17
G	eçersiz FSMO Role Holder Düzeltme1	18
Va	arolan RID Havuzunu Geçersiz kılmak2	21

Merhabalar , umuyorum okuyacağınız döküman sizler için faydalı olacaktır. Okumaya başlamadan önce aşağıda oluşturduğum dökümanı kendi yapınıza uyarlarken yön vermesi amacıyla küçük örneklerle ve açıklamalarla içini doldurmaya çalıştım fakat test ortamı olması gereği ile tam da gerçeği yansıtmamaktadır. Kendi yapınızda çok daha farklı sistemler ,entegrasyonlar, bilinmeyen sistemler olacaktır. O yüzden ağadaki gibi bir döküman oluşturmak ve belirli periyotlarla güncellemek çok faydalı olacaktır.

Döküman Kontrolü

Döküman yazıldıktan sonra elbette belirli periyotlarda yenilenmesi gerekecektir. İlgili tabloda revize eden uzmanların bilgilerini girebilirsiniz.

Versiyon	Tarih	Yazan	Sebep
1	19/12/2024	Hasan Dimdik	İlk sürüm
1.1			
1.2			

Referans Dosyaları

Bu bölümde ilgili dökümana destek olan, atıfta bulunan dosyalar mevcut ise daha kolayca takip edilebilmesi açısından aşağıdaki tabloda tek tek girilebilir.

Döküman Başlığı	Referans Dökümanı	Versiyon	Tarih	

Döküman Kabulü

İlgili döküman hazırlanırken elbette bazı kriterler göz önünde bulundurulmalıdır ve ilgili birimlerin bu dökümanı okuyup onay vermeleri gerekmektedir. Siz dökümanı yazarken belki önemli bir kriteri kaçırmış olabilirsiniz veya döküman mükemmel bir şekilde yazılmıştır ama güvenlik riski içerebilir. O sebeple her ilgili departmanın okuması ve onay vermesi önem arz etmektedir.

İsim	İmza	Tarih

Active Directory Takımı

Elbette ilgili ürünü yöneten takım elemanları tek tek girilmelidir. Bu belki ilk başta göze garip gelebilir veya ben zaten ilgili takımı tanıyorum diyebilirsiniz fakat büyük şirketlerde durum bu şekilde olmayacaktır.

Uygulama	Uygulama Sahibi	Mail Adresi
Active Directory	Hasan Dimdik	hd@mshowto.org
Entra ID	Mustafa Kara	

Birincil İrtibat Takımları/Kişileri

Elbette Active Directory' i yöneten, ilgili servisi L1-L2-L3 seviyesinde yöneten departmanlar veya kişiler burada tanımlanmalıdır.

Rol/Servis/Bağımlılık	Kontaklar	E-Mail
Network	Emre Ozan	
Operasyon Ekibi	Ömer Taşkın	
Siber Güvenlik Ekibi	Mert Yeter	
İş Sürekliliği	Emre Aydın	

Active Directory' nin Bağımlı Olduğu Katmanlar

Active Directory servisinin bağlı olduğu birçok katman mevcut. Storage, network, firewall vb. Acil durumlarda, panik durumları da oluşabileceği için önemli asetlerin gözden kaçmaması açısından bu şekilde belirtilmesinde fayda vardır.

• Bağımlılıklar

- o Fiziksel Sunucular
- o Network
- o Storage
- o Sanallaştırma Katmanı

AD Entegrasyonları

Kritik noktalardan bir tanesi de Active Directory servisi ile entegrasyonu olan tüm uygulama sunucuları, donanımlar vb bu adımda tanımlanmalıdır.

Entegrasyon Listesi	Amaç
Uygulamalar	LDAP sorgusu vs
Donanımlar	LDAP sorgusu vs

Active Directory FSMO Rollerinin Dağılımı

Bu bölümde FSMO rollerine sahip domain controller bilgilerini girebilirsiniz.

Domain	FSMO Rolleri	Sunucu İsmi
hd.local	Schema Master	dc01
hd.local	Domain Namin Master	dc01
hd.local	PDC	dc02
hd.local	RID	dc02
hd.local	Infrastructre Master	dc03

Active Directory Mimarisi, Sunucuları vb.

- AD mimarisi (Bilgiler fikir vermek için yazılmıştır, tamamen uydurmadır 😊)
 - Active Directory Tier 0 katmanında konumlandırılmıştır.
 - o Windows Server 2019 işletim sistemi üzerinde çalışmaktadır
 - o Dimdik.local içerisinde üç adet fiziksel toplamda 10 dc bulunmaktadır.
 - Hd.local içerisinde iki tane dc bulunmaktadır ve Oracle üzerinde çalışmaktadır.
 - Hd.local ise üç farklı lokasyon da konumdırılmıştır ve buna göre de site lar yapılandırılmıştır.
 - o İki domain de Full mesh olarak yapılandırılmıştır.

HD.local Mimarisi

Buraya isteğe göre yapının grafiği eklenebilir.

AD Sunucu Havuzu

Active Directory sunucularının envanterinin tutulması, özelliklerinin belirtilmesi operasyonel anlamda da faydalı olacaktır.

Sunucu İsmi	IP Adresi	Server Rolü	Lokasyon	Sanal/Fiziksel	OS Bilgisi	CPU	Memory	HDD
DC01								
DC02								

Active Directory Kurtarma Prosedürü

Root Domain için Forest Kurtarma Adımları	Kontrol
Yeni sanal sunucu kurulumu (İşletim sistemi kurulu olmamalı)	
Son BMR yedeğinin kontrol edilmesi	
Recovery Mode içerisinde BMR yedeğinden restore işlemi	
Sunucunun restart edilmesi ve varsayılan admin ile yeniden oturum açılması(RID 500)	
Network ve Network kartlarının kontrol edilmesi	
RID 500 şifresinin resetlenmesi ve Enterprise, Domain, Schema Admin gruplarına üye olup olmadığının	
kontrolü	
Metadata cleanup	
Geçersiz FSMO rol sahipliklerinin düzeltilmesi	
RID havuzu numarasını yükseltme ve eskisini geçersiz kılma	
DC bilgisayar hesap şifresinin iki defa resetlenmesi	
KRBTGT hesabının iki defa resetlenmesi	

Yukarıdaki gibi prosedür hazırlamak zor zamanlarda hayat kurtarır. Gelelim işin Teknik tarafına. Başlamadan önce aşağıdaki maddeleri dikkatli olarak okumanızı tavsiye ederim

- Yeni sunucu, yedek alınan sunucu ile aynı özelliklere sahip olmalıdır
- Sadece BMR Backup desteklenmektedir. Diğer bir ifade ile üçüncü parti yazılımlar MS tarafından desteklenmemektedir.
- Alet çantanız içerisinde Fixfsmo.vbs(Fix Invalid FSMO RoleHolder) ve InvalidateRIDPool.ps1(Raise and Invalidate RID pool) scritleri olmalıdır.

Yapımı aşağıdaki tabloda görebilirsiniz. FSMO rollerim dc01 sunucumda ve sadece dc02 sunucumun yedeği alınıyor.Senaryom gereği tüm Domain Controller larımın ulaşılamaz hale geldiğini varsayacağız.

Hostname	IP	Backup	FSMO Rolleri
dc01	192.168.1.1		х
dc02	192.168.1.2	Х	
client	192.168.100		



Yedekten Geri Dönme Adımları

Ulaşılamaz hale gelen sunucumuz ile aynı sürüme sahip olacak şekilde iso muzu takıyoruz. **Repair your computer** seçiyoruz.

	🖆 Windows Setup	
	Windows Server• 2019	
	Install now	
	<u>R</u> epair your computer © 2013 Microsoft Corporation. Al rights reserved.	
*		

Troubleshooting tikliyoruz.

Cho	bose an option
I	Troubleshoot Reset your PC or see advanced options
ں ا	Turn off your PC
Y	

System Image Recovery tikliyoruz.

E	Adva	anced optior	าร	
	+	System Image Recovery Recover Windows using a specific system image file		
	C:\	Command Prompt Use the Command Prompt for advanced troubleshooting		

Eğer uyumsuz bir yedek seçtiyseniz aşağıdaki gibi bir hata alacaksınız. Burada küçük bir hatırlatma yapma gereği duyuyorum. <u>Yedekten geri döndüğünüz ortam eskisi ile aynı olmalı</u> <u>yani Hyper-V de alınan yedeği Vmware ortamına dönemezsiniz</u>.



ſ			
X	Ke-inage your computer	Select a system image backup Troubleshooting information for BMR: http://go.microsoft.com/fwink/p/Zinkid=225039 Use the latest available system image(recommended) Location: New Volume (C:) Date and time: 12/19/2024 9:56:16 AM (GMT-8:00) Computer: do2 Select a system image	
		<back next=""> Cancel</back>	

Advanced seçiyoruz.

둁 Re-image your computer	—
Choose additional restore options	è
Format and repartition disks Select this to delete any existing partitions and reformat all disks on this computer to match the layout of the system image.	Exclude disks
If you're unable to select an option above, installing the drivers for the disks you are restoring to might solve the problem.	Install drivers Advanced
< Back Nex	t > Cancel

Automatically restart the computer after the restore is complete kutucuğunu işaretlemiyoruz.

Re-image your computer
Choose additional restore options
Re-image Your Computer
 Automatically restart this computer after the restore is complete To make additional changes before restarting this computer, clear this check box. Automatically check and update disk error information This might take several minutes to complete. To check disks and update error information manually, clear this check box.
OK Cancel
Auvanced
< Back Next > Cancel

🍋 Re-image your computer		×
Re-image your computer	Your computer will be res image: Date and time: Computer: Drives to restore:	stored from the following system (19/2024 9:56: 16 AM (GMT-8:00)) dc02 \\?8faf1a2b-0000-0000-(
	< Ba	ck Finish Cancel

Re-image your comp	Uter Vour computer will be restored from the following system image: Date and time: '19/2024 9:56:16 AM (GMT-8:00) Computer: dc02 Drives to restore: 'V/V/wolume (8faf1a2b-0000-0000-4 Aur Computer aur Computer Il disks to be restored will be formatted and replaced with the spout and data in the system image. Yes No Yes No
	< Back Finish Cancel



Yedekten döndüğümüz sunucumuzu restart ediyoruz.

Re-image Your Computer Do you want to restart your computer now? Your computer has been restored. To start Windows in normal mode, restart your computer. Restart now Don't restart Close	Re-image Your Computer Do you want to restart your computer now? Your computer has been restored. To start Windows in normal mode, restart your computer. Restart now Don't restart Close
Do you want to restart your computer now? Your computer has been restored. To start Windows in normal mode, restart your computer. Restart now Don't restart Close	Do you want to restart your computer now? Your computer has been restored. To start Windows in normal mode, restart your computer. Restart now Don't restart Close Close
Your computer has been restored. To start Windows in normal mode, restart your computer. Restart now Don't restart Close	Your computer has been restored. To start Windows in normal mode, restart your computer. Restart now Don't restart
Restart now Don't restart Close	Restart now Don't restart Close
Close	Close

Domain admin hesabim ile oturum açıyorum.

Kurtarma Sonrası Yapılacaklar



ADUC, DSSITE ve DNS lerin kontrol edilmesini tavsiye ederim. Network ayarlarını yapınıza göre düzenlemeniz gerekmektedir. Net share i kontrol etmenizi de tavsiye ederim.

Active Directory Users and Computers altında yer alan SYSVOL **Subscription** in özellikler sekmesine gidiyorum.



MsDFSR-Enabled TRUE ve msDFSR-Options 1 olacak şekilde değiştiriyorum

	DNS Manager		—
File	Action View	Help	
•	Active Direct	SYSVOL Subscription Properties ? × General Object Security Attribute Editor	
	🗢 🔿 📶 🛅	Attributes:	DC Tuno Sito
	 Saved Qu Builti CafeA CafeA Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp Comp <li< td=""><td>Attribute Value * msDFSR-DeletedPath <not set=""> msDFSR-DeletedSize <not set=""> msDFSR-DfsLinkTarget <not set=""> msDFSR-Enabled TRUE msDFSR-Extension <not set=""> msDFSR-Flags <not set=""> msDFSR-MaxAgeInC <not set=""> msDFSR-OnDemand <not set=""> msDFSR-OnDemand <not set=""> msDFSR-OnDemand <not set=""> msDFSR-Options 1 msDFSR-ReadOnly FALSE msDFSR-Replication</not></not></not></not></not></not></not></not></not></td><td>on of the second s</td></li<>	Attribute Value * msDFSR-DeletedPath <not set=""> msDFSR-DeletedSize <not set=""> msDFSR-DfsLinkTarget <not set=""> msDFSR-Enabled TRUE msDFSR-Extension <not set=""> msDFSR-Flags <not set=""> msDFSR-MaxAgeInC <not set=""> msDFSR-OnDemand <not set=""> msDFSR-OnDemand <not set=""> msDFSR-OnDemand <not set=""> msDFSR-Options 1 msDFSR-ReadOnly FALSE msDFSR-Replication</not></not></not></not></not></not></not></not></not>	on of the second s
۲	> 🧰 NIDS > 🧮 TPM I	OK Cancel Apply Help	

Daha sonrasında DFS servisini restart ediyorum.

0			
🛋 Administrator: Command Pron	ıpt	_	[
Microsoft Windows [Version (c) 2018 Microsoft Corpora	10.0.17763.864] tion. All rights reserved.		
C:\Users\Administrator>sc	stop dfsr		
SERVICE_NAME: dfsr TYPE STATE WIN32_EXIT_CODE SERVICE_EXIT_CODE CHECKPOINT WAIT_HINT C:\Users\Administrator>sc	: 10 WIN32_OWN_PROCESS : 4 RUNNING (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN) : 0 (0x0) : 0 (0x0) : 0x0 : 0x0 : 0x0 : 0x0 : 0x0		
SERVICE_NAME: dfsr TYPE STATE WIN32_EXIT_CODE SERVICE_EXIT_CODE CHECKPOINT WAIT_HINT PID FLAGS	<pre>: 10 WIN32_OWN_PROCESS : 2 START_PENDING (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN) : 0 (0x0) : 0 (0x0) : 0x00 : 0x7d0 : 5640 :</pre>		

Sonrasında Event Viewer açıyorum ve DFS Replication altında **4602** ve**1206** event larının oluştuğunu doğruluyorum.

🛃 Event Viewer					- 🗆	×
File Action View Help						
🗢 🔿 🙍 🖬						
Event Viewer (Local)	DFS Replication	Number of events: 47			Actions	
 Event Viewer (Local) Custom Views Custom Views Windows Logs Applications and Services Log Active Directory Web Service DFS Replication Directory Service DNS Server Hardware Events Internet Explorer Key Management Service Microsoft OpenSSH Subscriptions 	DFS Replication Level i Information i Information i Information i Information General Details The DFS Replic Windows\SYS folder. No user command prov Additional Info Replicated Fold Log Name: Source:	Number of events: 47 Date and Time 12/18/2024 1:11:22 PM 12/18/2024 1:04:22 PM 12/18/2024 1:04:21 PM es - Event 4602, DFSR ation service successfully i VOL\domain. This membe action is required. To check mpt window and then type wirmation: der Name: SYSVOL Share DFS Replication DFSR	Source Event I DFSR 100 DFSR 460 DFSR 121 DFSR 121 nitialized the SYSVOL rr r is the designated print k for the presence of t "net share".	D Task ^ 6 Non 2 Non 0 Non eplicated fold ary membe he SYSVOL sl	Actions DFS Replication OPEN Saved L Create Custo Create Custo der at local path C: ^ r for this replicated hare, open a	×
	Level:	Information	Keywords:	Classic		
	User:	N/A	Computer:	dc01.hd.loo	cal	
< >>	OpCode: More Informatio	on: <u>Event Log Online Hel</u>	2			

🚼 Event V	/iewer				_
File Actio	on View Help				
 Event C W A A I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I<th>General Details The DFS Replication</th><th>Event 1206, DFSR</th><th>cted domain contr</th><th>roller dcrestore.hd.local to acces</th><th>×</th>	General Details The DFS Replication	Event 1206, DFSR	cted domain contr	roller dcrestore.hd.local to acces	×
> 📫 > 📫	 Log Name: Source: Event ID: Level: User: OpCode: More Information:	DFS Replication DFSR 1206 Information N/A <u>Event Log Online Help</u>	Logged: Task Category: Keywords: Computer:	12/18/2024 1:31:18 PM None Classic dcrestore.hd.local	•
	Сору				Close

Force synchronization for Distributed File System Replication (DFSR) replicated sysvol replication - Windows Server | Microsoft Learn

Metadata Cleanup ve FSMO Role Seizing

FSMO rolümün hangi dc de olduğnu kontrol ediyorum.



Doğal olarak eski dc lerime ulaşamadığım için fsmo rollerimi zorla almam gerekiyor. İlk olarak ulaşılamaz olan dc lerimi siliyorum.

Active Directory Users and Computers							
File Action View Help							
🗢 🔿 🙋 📷 🔏 🗉 🗙 🖾 🙆 🕞 🛛 📷 🗏 📚 🖆	1 🍸 🖻 🕯	<u>.</u>					
Active Directory Users and Computers [dc02.hd.local]	Name		Туре		DC Type	Site	Description
> Saved Queries	DC01		Computer		GC	Default-First-	Si
✓ jiii hd.local > □ Builtin	10C02		Computer		GC	Default-First-	Si
> 🖬 CafeAzure							
> 🚞 Computers							
🗸 🛅 Domain Controllers	I						
> 👰 DC01	Act	ive Directory I	Domain Services		\times		
✓ ▶ DC02							
DFSR-LocalSettings							
Domain System Volume		Are you	sure you want to delete the Con	mputer named 'DC0	1'?		
> ForeignSecurityPrincipals	4	•					
> 🦲 Keys							
> CostAndFound				Ves No			
> Managed Service Accounts							
> Program Data							
> System							
V Users							
👗 Administrator	11						

FSMO rollerini powershell ile hızlıca taşımak için aşağıdaki komut kullanılabilir

Move-ADDirectoryServerOperationMasterRole -Identity "Hedef DC" -OperationMasterRole 0,1,2,3,4 -force"

🔀 Administrator: Windows PowerShe	II. Contraction of the second s	-	×
vindows PowerShell Copyright (C) Microsoft Corpora	ation. All rights reserved.		^
PS C:\Users\Administrator.HD> N	Nove-ADDirectoryServerOperationMasterRole -Identity "dc02" -OperationMasterRole 0,1,2,3,4 -Force		
Move Operation Master Role Do you want to move role 'PDCEm [Y] Yes [A] Yes to All [N] No PS C:\Users\Administrator.HD>	mulator' to server 'dc02.hd.local' ? o [L] No to All [S] Suspend [?] Help (default is "Y"): A		
Administrator: Command Prom	pt	-	×
C:\Users\Administrator.HD)>dfsrdiag pollad		î
Operation Succeeded			
C:\Users\Administrator.HD	D>netdom query fsmo		
Schema master Domain naming master	dc01.hd.local		
PDC	dc01.hd.local		
RID pool manager	dc01.hd.local		
The command completed suc	ccessfully.		
C:\Users\Administrator.HD	Dentdom query fsmo		
Schema master	dc02.hd.local		
Domain naming master	dc02.hd.local		
RTD pool manager	dc02.hd.local		
The command completed suc	dc02.hd.local ccessfully.		
) C:\Users\Administrator.HD)>		

Not: Metadata cleanup ile ilgili detaylı yazıyı Mshowto github sayfasında Active Directory Migration konusunda içerisinde ele aldım.

Geçersiz FSMO Role Holder Düzeltme

Aşağıdaki linkten ilgili scripti DC mize kopyalıyoruz

Error when running the Adprep /rodcprep command in Windows Server 2008 - Windows Server | Microsoft Learn

fixfsmo.vbs DC=DomaindnsZones,DC=hd,DC=local komutunu cmd komut satırında çalıştrııyoruz ve FSMO Role Owner niteliğini ulaşılabilir dc ile değiştirmiş oluyoruz.

		 	_	
Administrator:	Windows PowerShell	-		×
PS C:\> cmd Microsoft Windo	ws [Version 10.0.17763.864]			^
(c) 2018 Micros	oft Corporation. All rights reserved.			
C:\>FIXFSMO.vbs				
C:\>FIXFSMO.vbs	DC=DomaindnsZones,DC=hd,DC=local			
C:\>FIXFSMO.vbs	DC=DomaindnsZones,DC=hd,DC=local			
C:\>				
	Windows Script Host X			
	DNS name: DomainDnsZones.hd.local			
I				
a				
Administ	rator: Windows PowerShell	 		
PS C:\> cmd				
Microsoft W	indows [Version 10.0.17763.864]			
(c) 2018 Mi	crosoft Corporation. All rights reserved.			
C:\>FIXFSMO).vbs			
C·\>ETXESMO	vbs DC=DomaindnsZones DC=bd DC=local			
C:\>FIXFSMO	.vbs DC=DomaindnsZones,DC=hd,DC=local			
IC:\>				
	Windows Seriet Hast			
1	Windows Script Host X			
	Using DC dc02.hd.local			
b				
2	ОК			
n				
	Mandau Barra Chall			
S C:\> cmd	: windows Powersneil			
licrosoft Wind	ows [Version 10.0.17763.864]			
(C) 2018 Micros	soft Corporation. All rights reserved.			
::\>FIXFSMO.vb	S			
::\>FIXFSMO.vb	s DC=DomaindnsZones,DC=hd,DC=local			
:\>FIXFSMO.vb	s DC=DomaindnsZones,DC=hd,DC=local			
::\>				
Windo	ows Script Host X			
infra 1 Settin	fsmo is CN=NTDS /gs\0ADEL:c56d48dd-4893-4341-a15a-1b253f9aeee6,CN=DC01,CN=			
Serve DC=1	s, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=hd			
,				
	ОК			

(c)	psoft Windows [Version 10.0.1//63.864] 2018 Microsoft Corporation. All rights reserved.		
::\>	FIXFSMO.vbs		
::\>	FIXFSMO.vbs DC=DomaindnsZones,DC=hd,DC=local		
::\>	FIXFSMO.vbs DC=DomaindnsZones,DC=hd,DC=local		
	Windows Script Host	×	
	Windows Script Host infra fsmo changed to:CN=NTDS Settings,CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites, N=Configuration,DC=hd,DC=local	×	

Varolan RID Havuzunu Geçersiz kılmak

rIDAvailablePool attribute ünü RID üzerindeki çakışmayı engellemek için değiştirmemiz gerekiyor .

Eski Hali



Yeni Hali



Aşağıdaki komut ile RID havuzunun hızlı bir şekilde güncellenmesini sağlamış oluyoruz.



Kaynak : AD Forest Recovery - Invalidating the RID Pool | Microsoft Learn

DCDiag /test:ridmanager /v komutu ile Domain Controller ın eski mi yeni mi RID havuzunu kullandığını görebilirsiniz. Yukarıda paylaştığım kaynağı dikkatlice okumanızı tavsiye ederim.

Bir sonraki adımda ise Domain Controller makina hesabını iki defa resetliyorum.



KRBTGT hesabını iki defa resetliyorum. Elbette kendi ortaminizda bu şekilde yapmadığınızdan eminim 😊

Manual Manua Manual Manua Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manua Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manua



Son olarak ise eski dc lerimin SRV bilgileri, DNS kayıtlarını siliyorum.

Daha sonrasında istemci makinam ile oturum açmayı denedim ve başarılı olduğunu gözlemledim. Aynı şekilde domaine yeni makina eklemeyi de denemenizi tavsiye ederim.



Umuyorum hiçbir zaman bu dökümanı pratikte uygulama gereği doğmaz. Olması halinde ise yukarıdaki adımlar hayat kurtarabilir. Umuyorum faydası olmuştur

Saygılarımla

Hasan DİMDİK

Security MVP

Cloud and Datacenter MVP