Active Directory Felaketten Dönüş Prosedürü

Hasan Dimdik

İçerik

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**
  - Fiziksel Sunucular
  - Network
  - Storage
  - 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.
    - Windows Server 2019 işletim sistemi üzerinde çalışmaktadır
    - 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.
    - 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

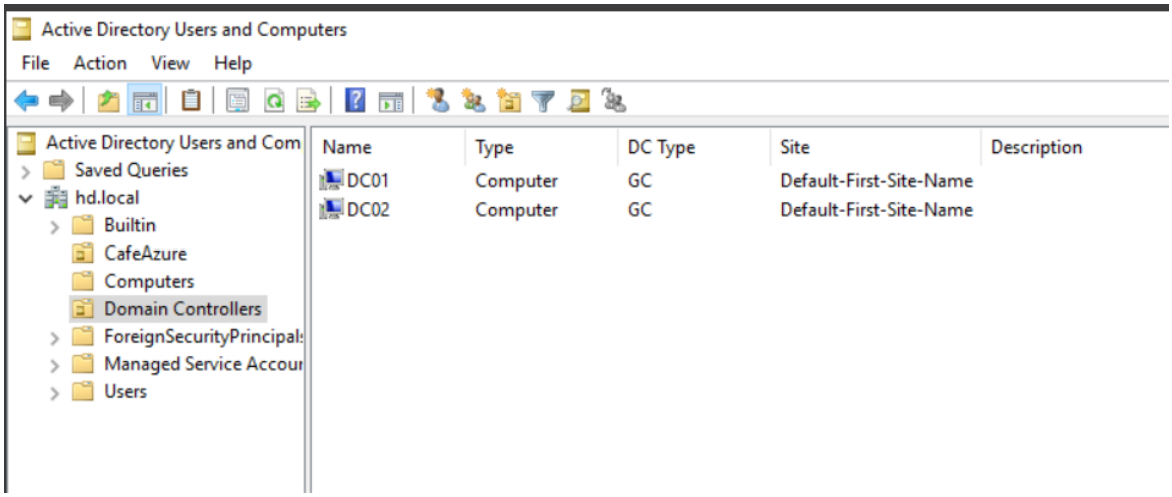
Root Domain için Forest Kurtarma Adımları	**Kontrol**
Yeni sanal sunucu kurulumu (İşletim sistemi kurulu olmamalı)	
Son BMR yedeğinin kontrol edilmesi	
Recovery Mode içerisinde BMR yedeğinden restore işlemi	
Sunucunun restart edilmesi ve varsayılan admin ile yeniden oturum açılması(RID 500)	
Network 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	

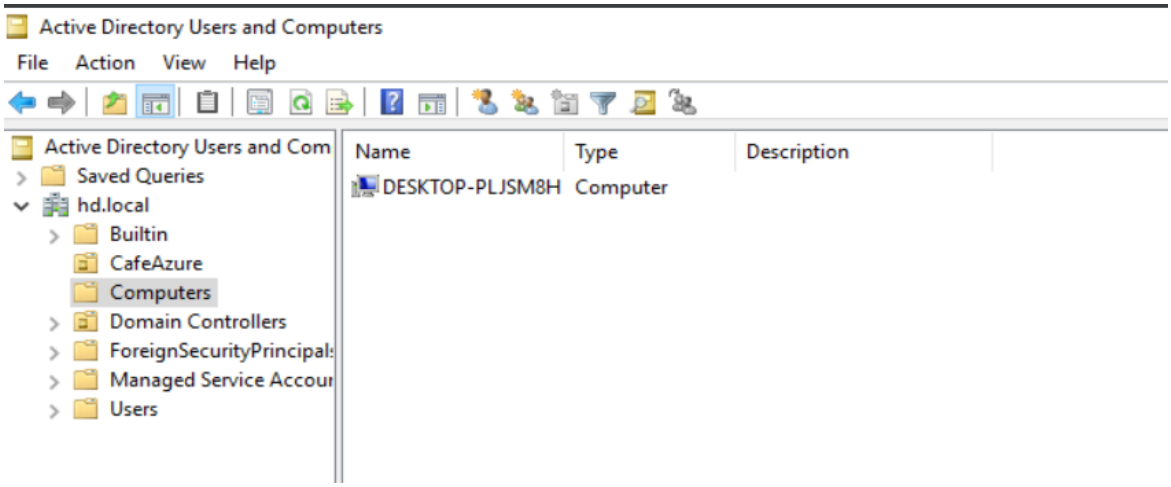
Yukarıdaki gibi prosedür hazırlamak zor zamanlarda hayat kurtarır. Gelelim işin Teknik tarafına. Başlamadan önce aşağıdaki maddeleri dikkatli olarak okumanızı tavsiye ederim

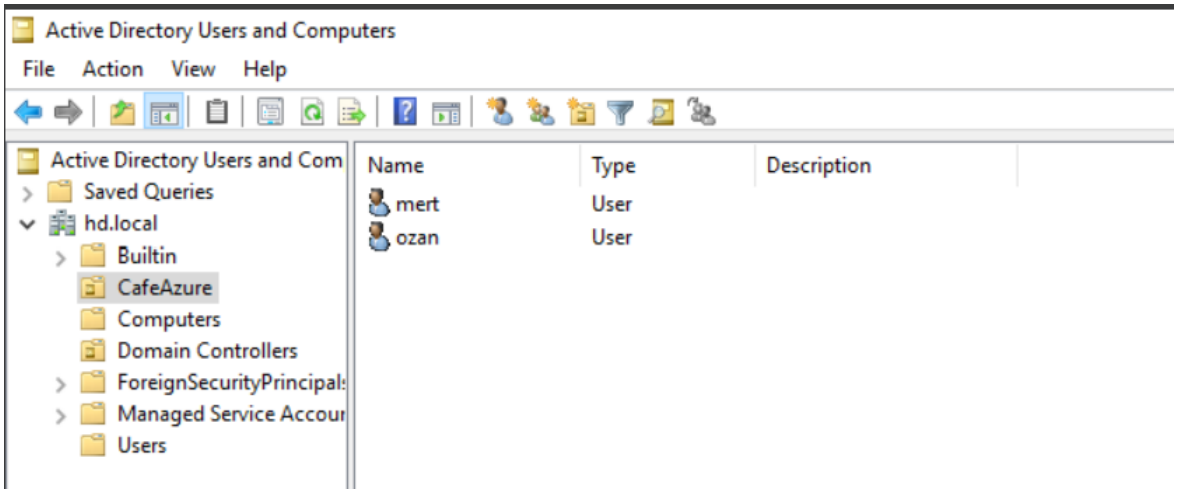
- Yeni sunucu, yedek alınan sunucu ile aynı özelliklere sahip olmalıdır
- Sadece BMR Backup desteklenmektedir. Diğer bir ifade ile üçüncü parti yazılımlar MS tarafından desteklenmemektedir.
- Alet çantanız içerisinde Fixfsmo.vbs(Fix Invalid FSMO RoleHolder) ve InvalidateRIDPool.ps1(Raise and Invalidate 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		x
dc02	192.168.1.2	x	
client	192.168.100		

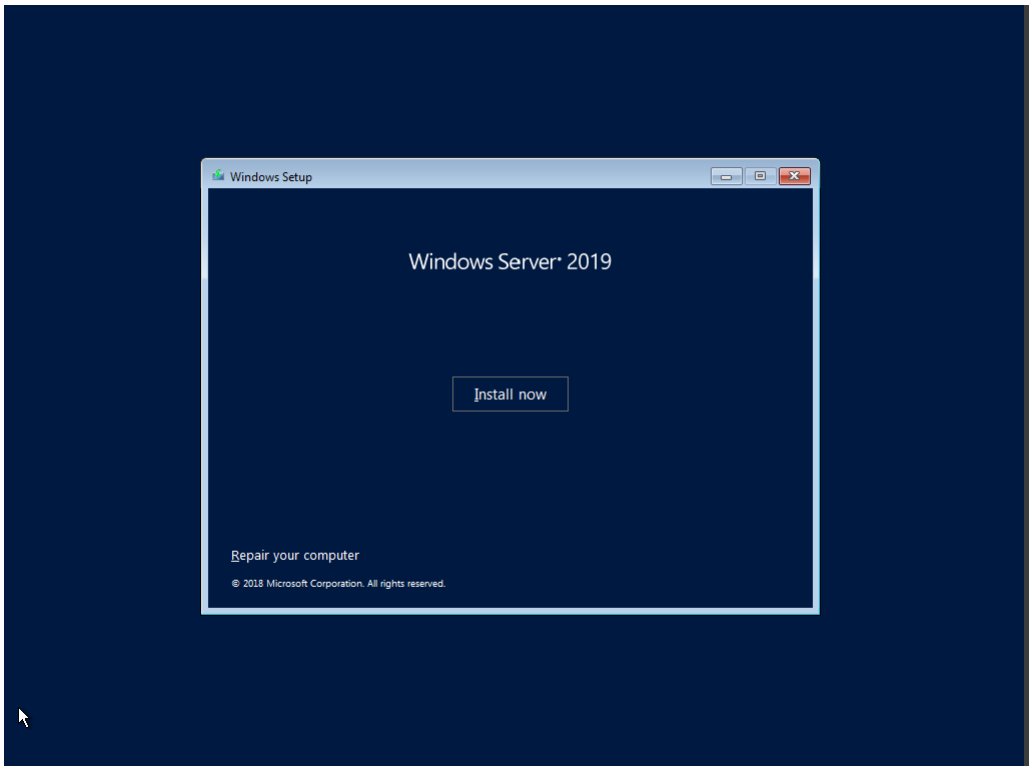

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
hd.local
Builtin
CafeAzure
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name Type DC Type Site Description
DC01 Computer GC Default-First-Site-Name
DC02 Computer GC Default-First-Site-Name


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
hd.local
Builtin
CafeAzure
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name Type Description
DESKTOP-PLJSM8H Computer

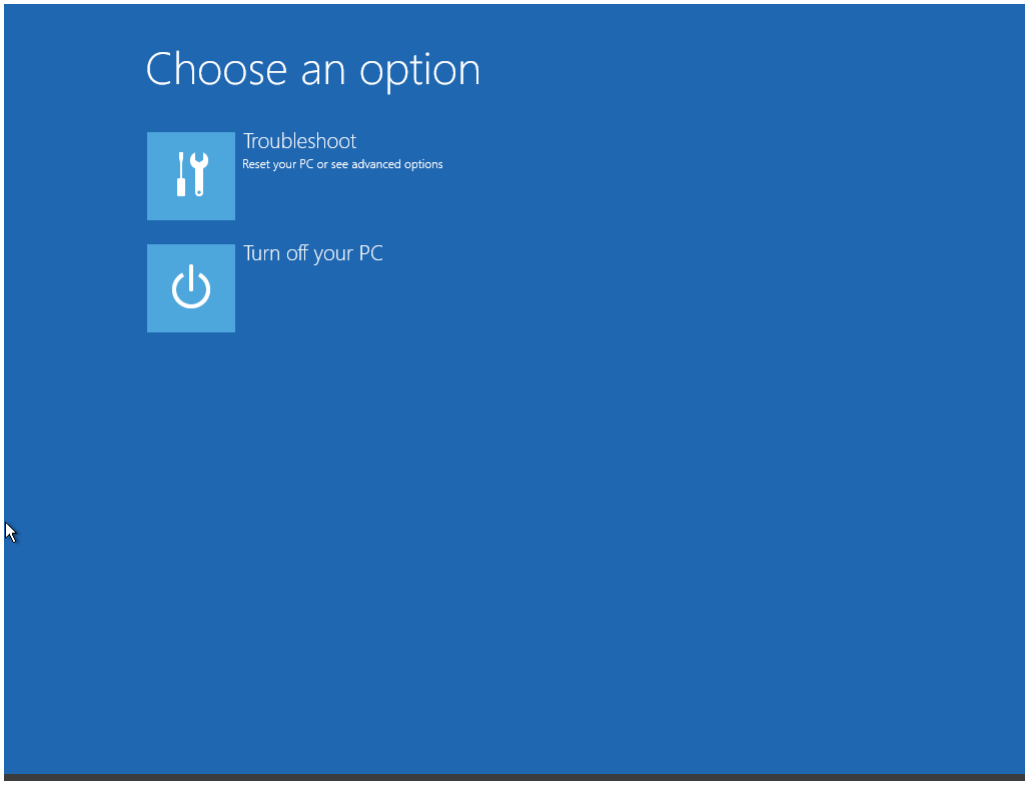

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
hd.local
Builtin
CafeAzure
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name Type Description
mert User
ozan User

Yedekten Geri Dönme Adımları

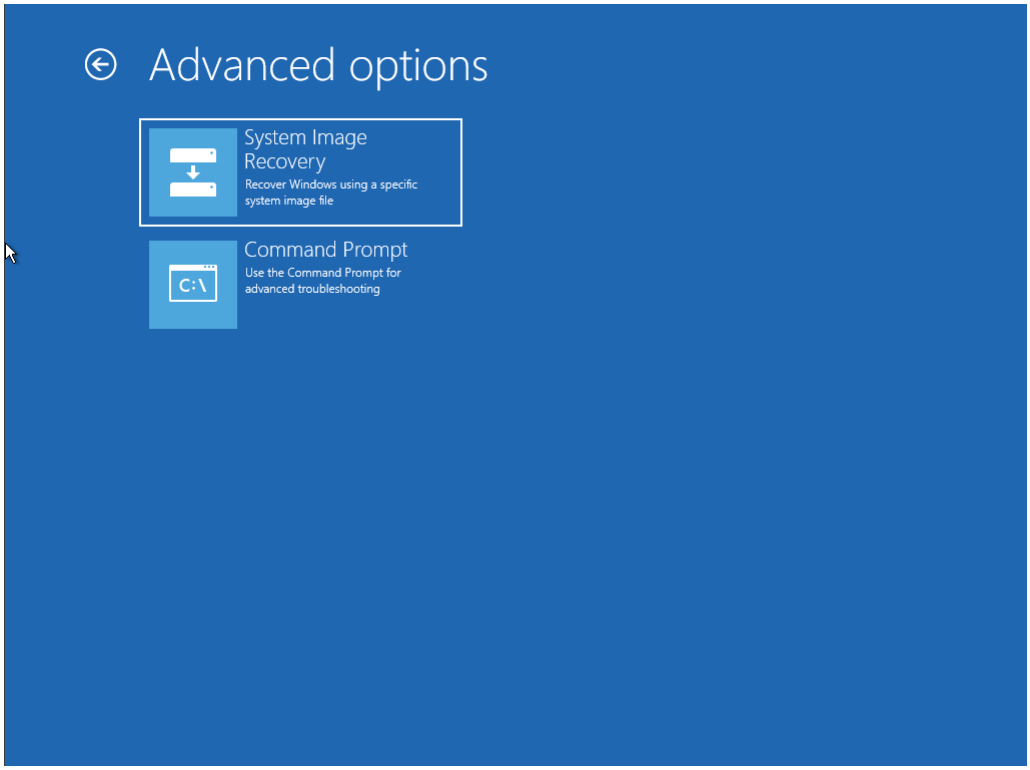
Ulaşılamaz hale gelen sunucumuz ile aynı sürüme sahip olacak şekilde iso muzu takıyoruz. **Repair your computer** seçiyoruz.



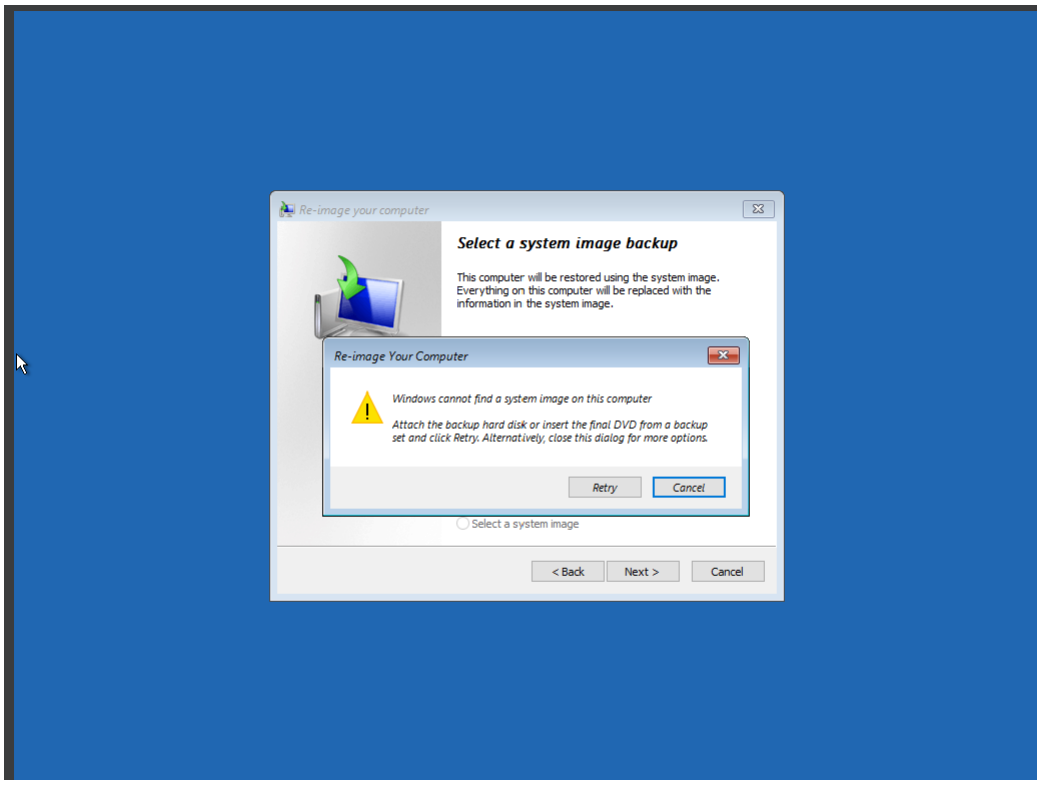
Troubleshooting tıklıyoruz.

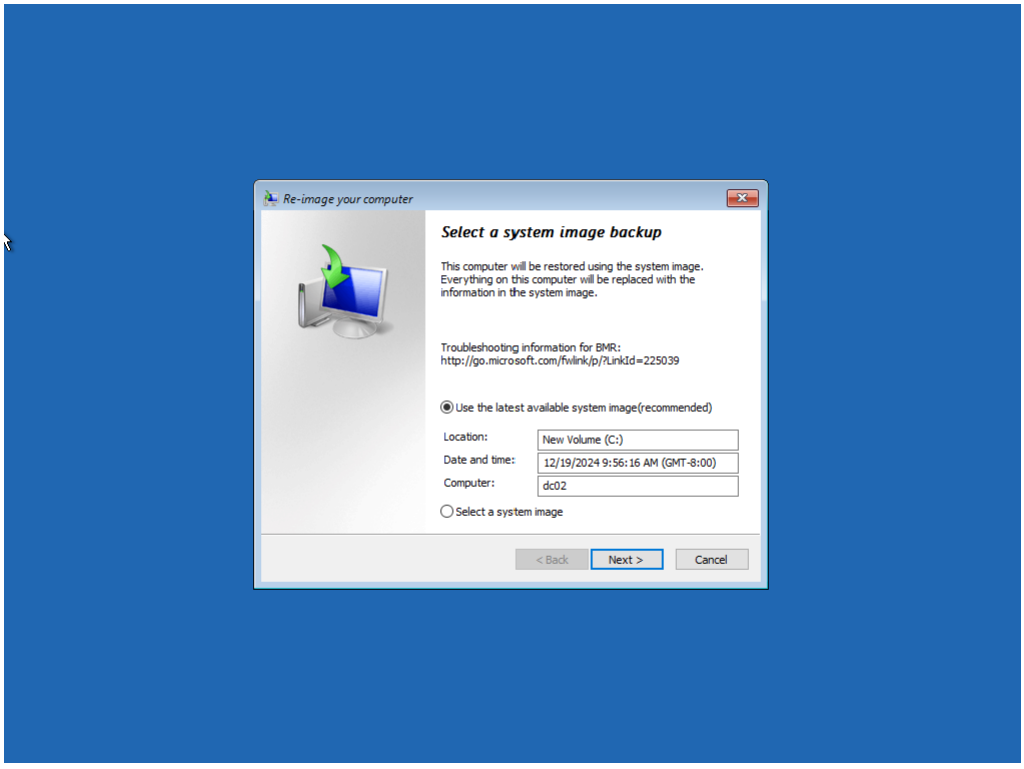


System Image Recovery tıklıyoruz.

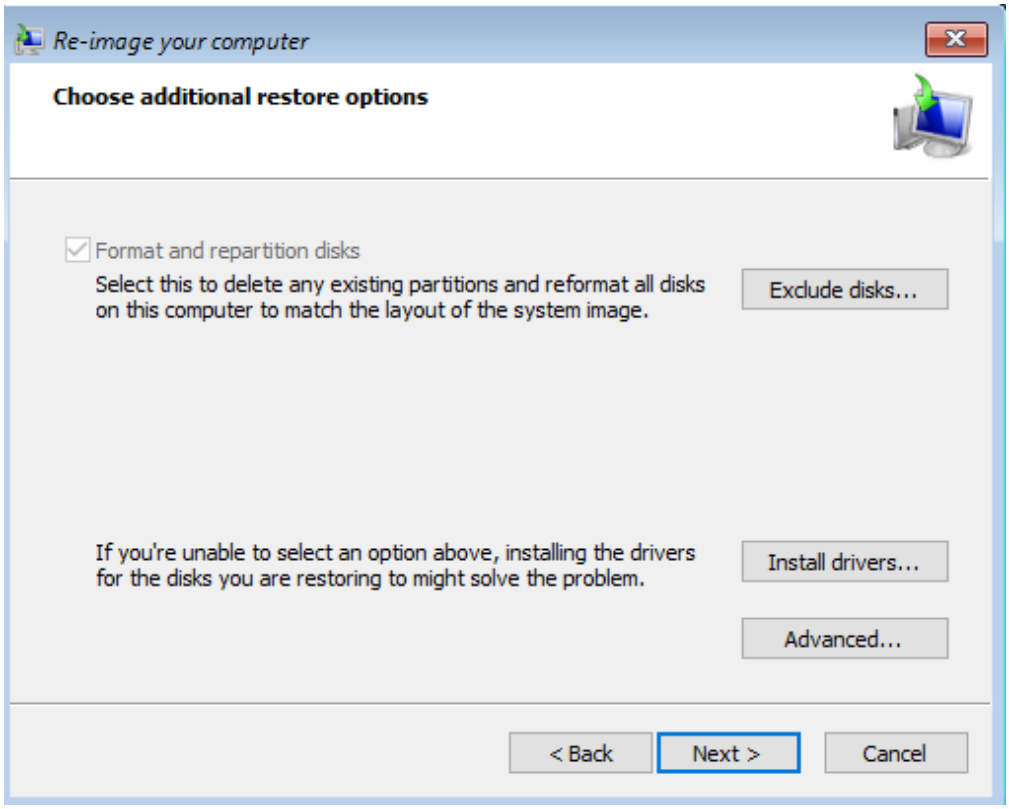


Eğer uyumsuz bir yedek seçtiyseniz aşağıdaki gibi bir hata alacaksınız. Burada küçük bir hatırlatma yapma gereği duyuyorum. **Yedekten geri döndüğünüz ortam eskisi ile aynı olmalı yani Hyper-V de alınan yedeği Vmware ortamına dönemezsiniz.**

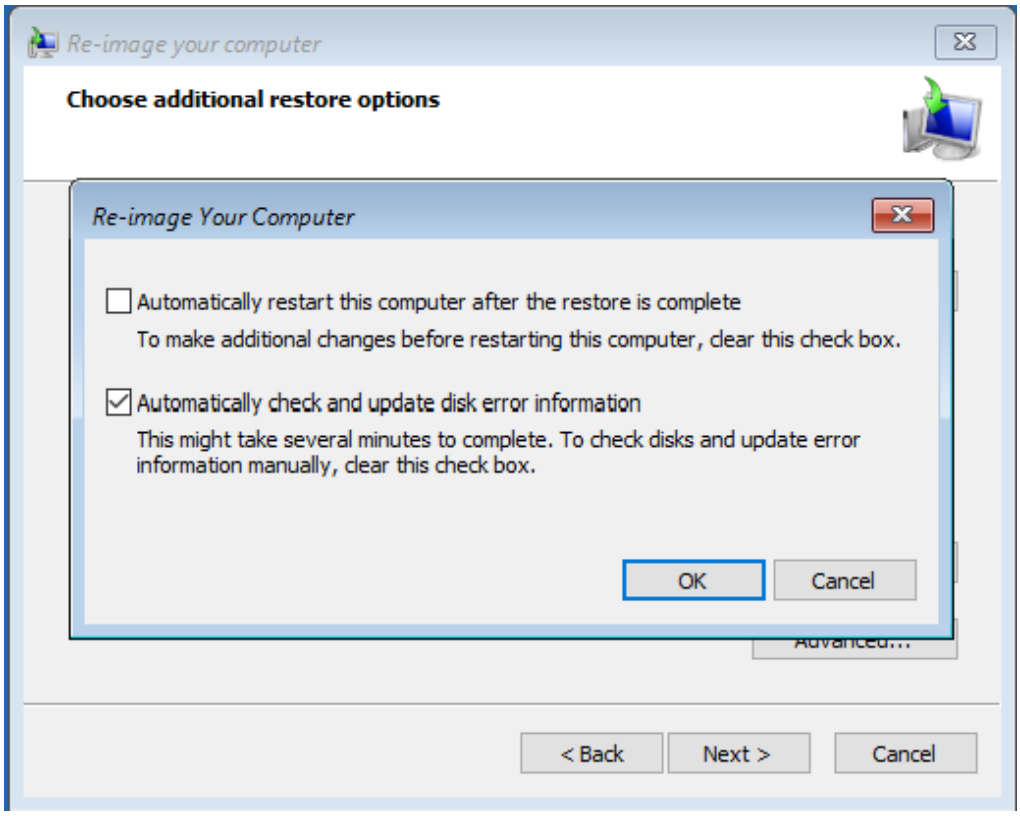


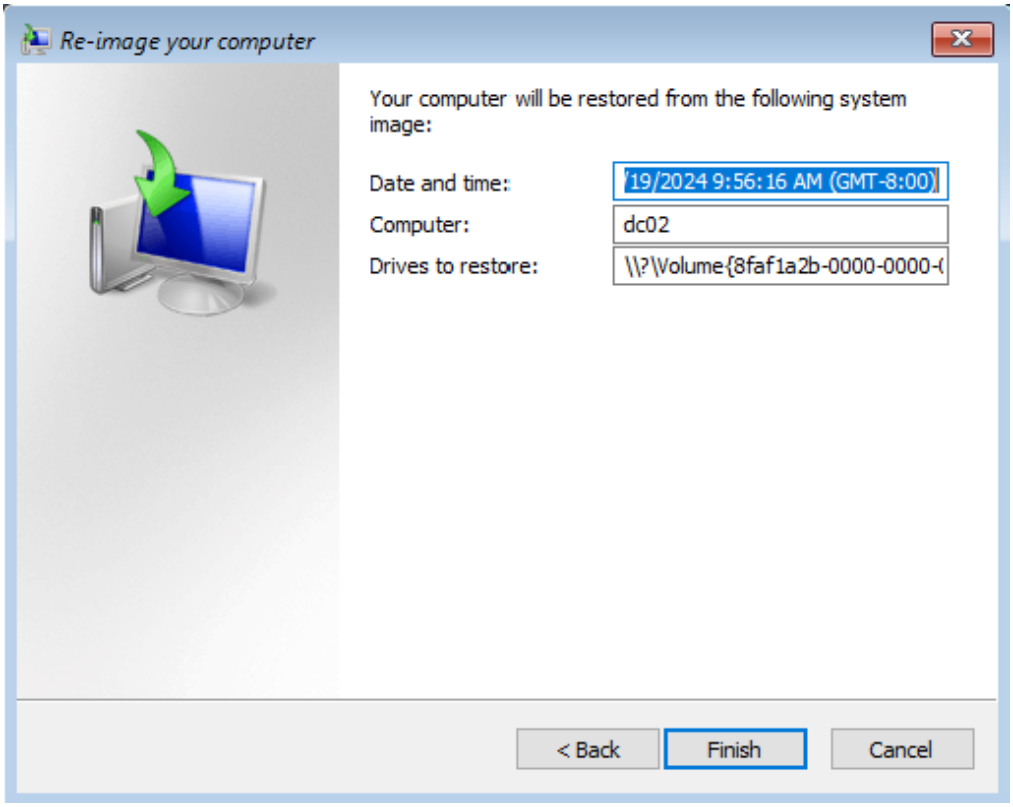


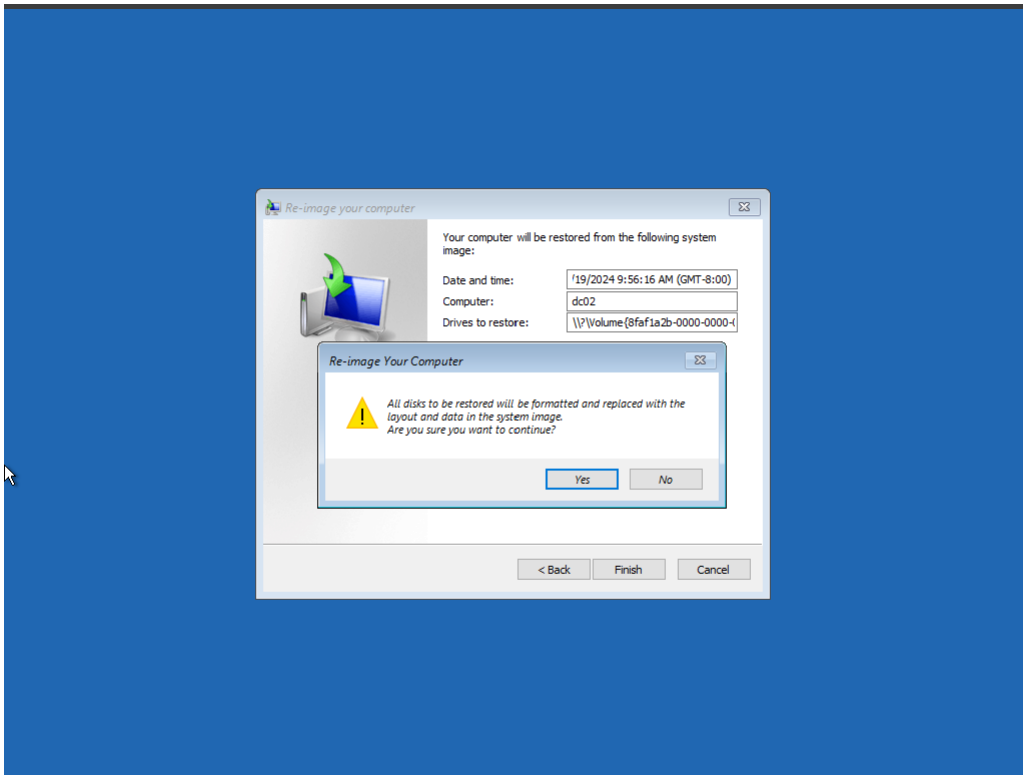
Advanced seçiyoruz.

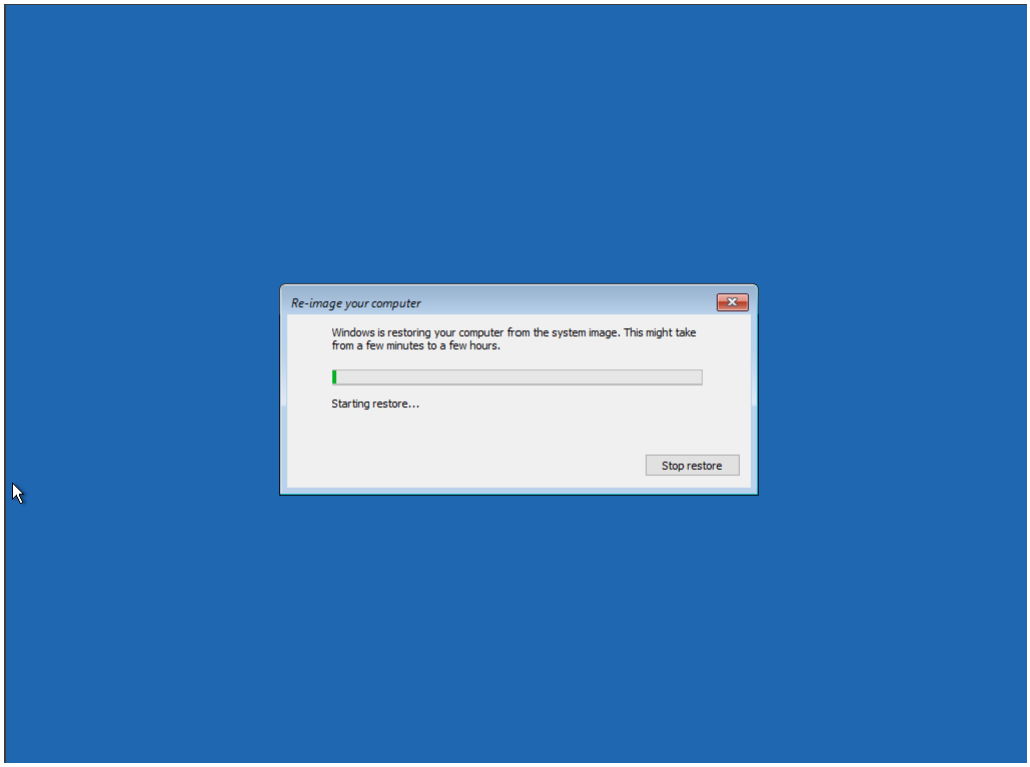


Automatically restart the computer after the restore is complete kutucuğunu işaretlemiyoruz.

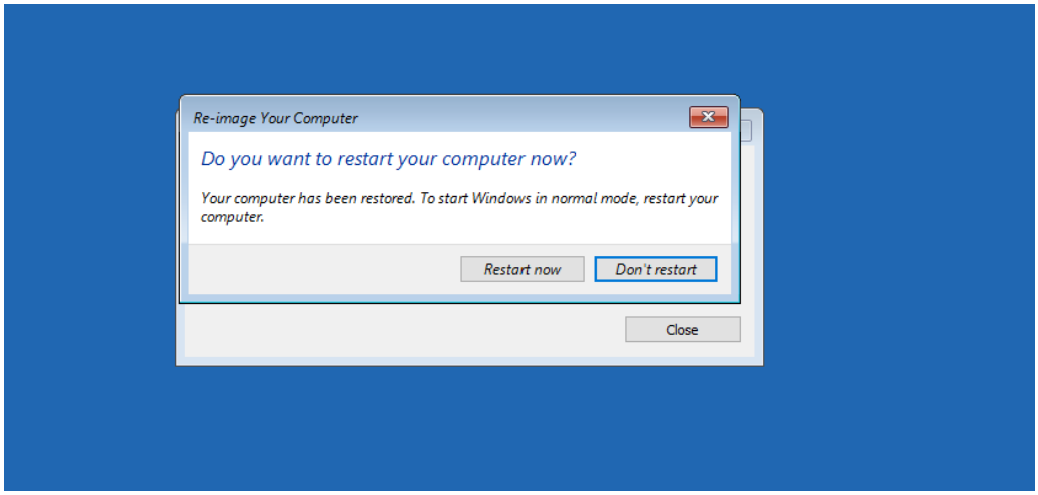



Re-image your computer
Your computer will be restored from the following system image:
Date and time:
'19/2024 9:56:16 AM (GMT-8:00)
Computer:
dc02
Drives to restore:
\\?\Volume{8faf1a2b-0000-0000-(
< Back
Finish
Cancel


Re-image your computer
Your 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:
\\?\Volume{8faf1a2b-0000-0000-(
Re-image Your Computer
All disks to be restored will be formatted and replaced with the layout and data in the system image.
Are you sure you want to continue?
Yes
No
< Back
Finish
Cancel

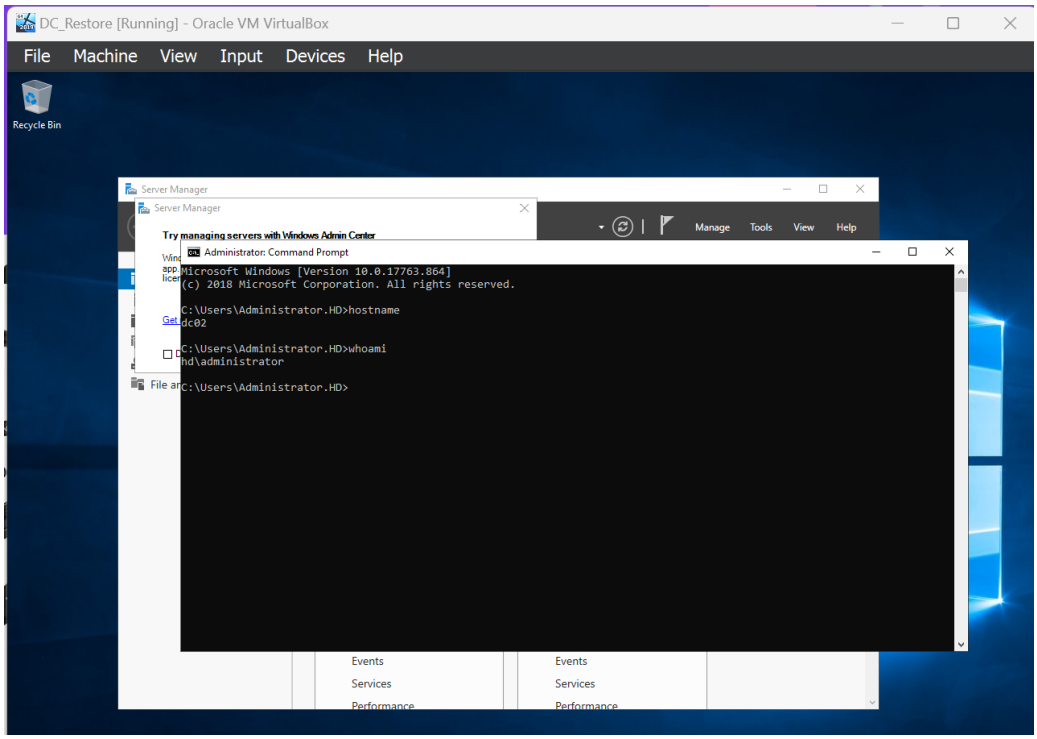


Yedekten döndüğümüz sunucumuzu restart ediyoruz.



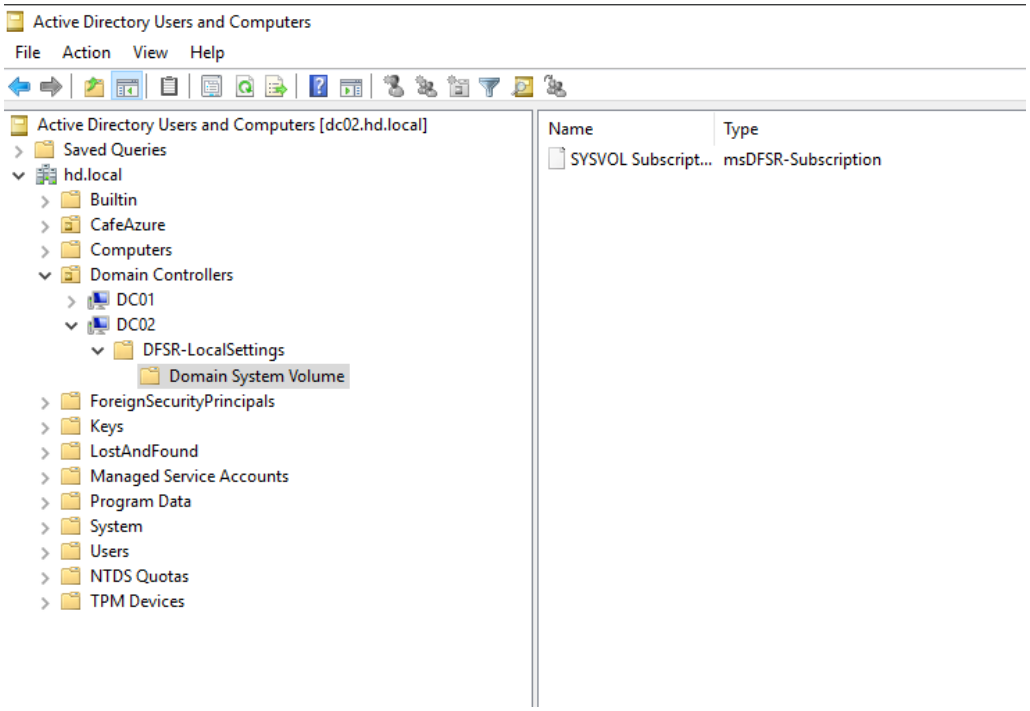
Domain admin hesabim ile oturum açıyorum.

Kurtarma Sonrası Yapılacaklar

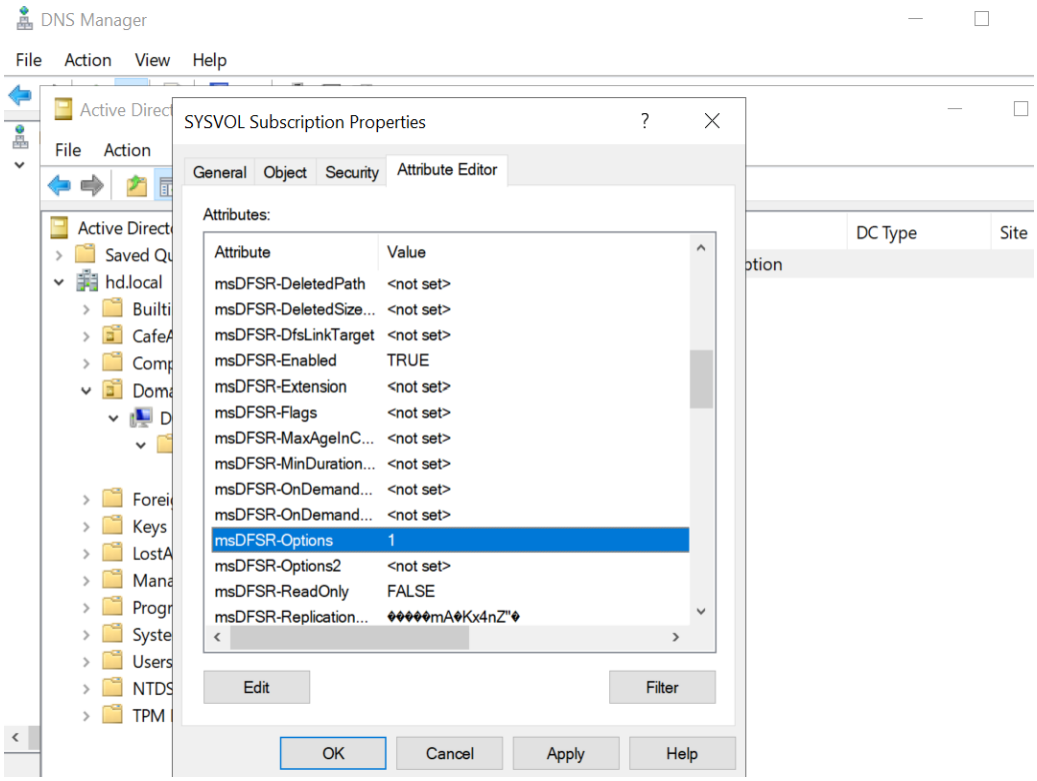


ADUC,DSSITE ve DNS lerin kontrol edilmesini tavsiye ederim. Network ayarlarını yapınıza göre düzenlemeniz gerekmektedir. Net share i kontrol etmenizi de tavsiye ederim.

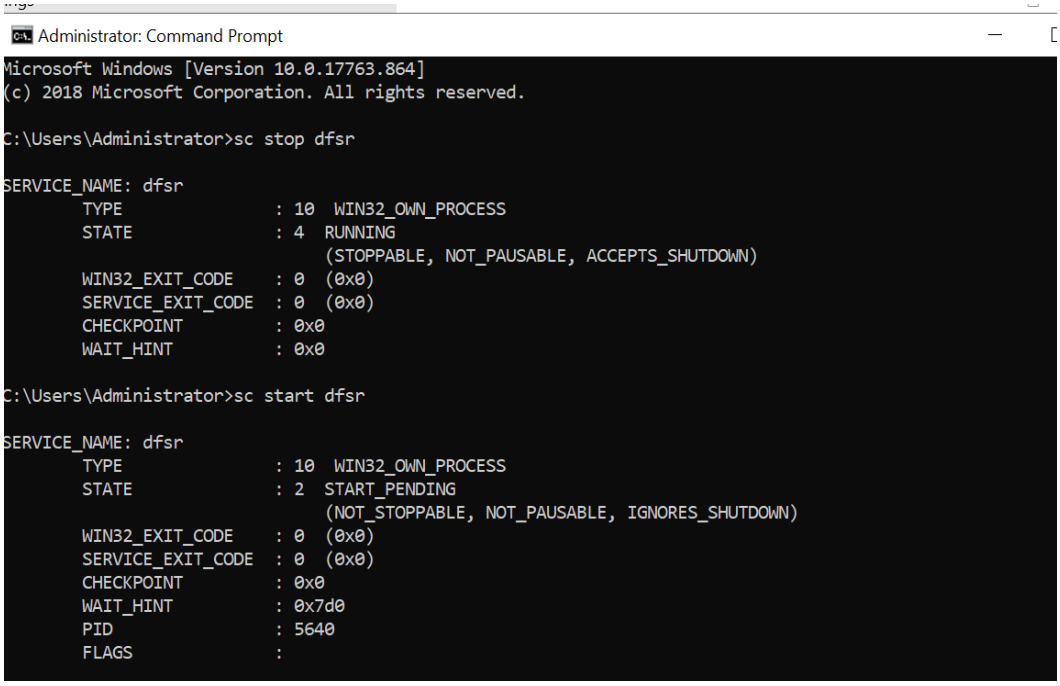
Active Directory Users and Computers altında yer alan SYSVOL **Subscription** in özellikler sekmesine gidiyorum.



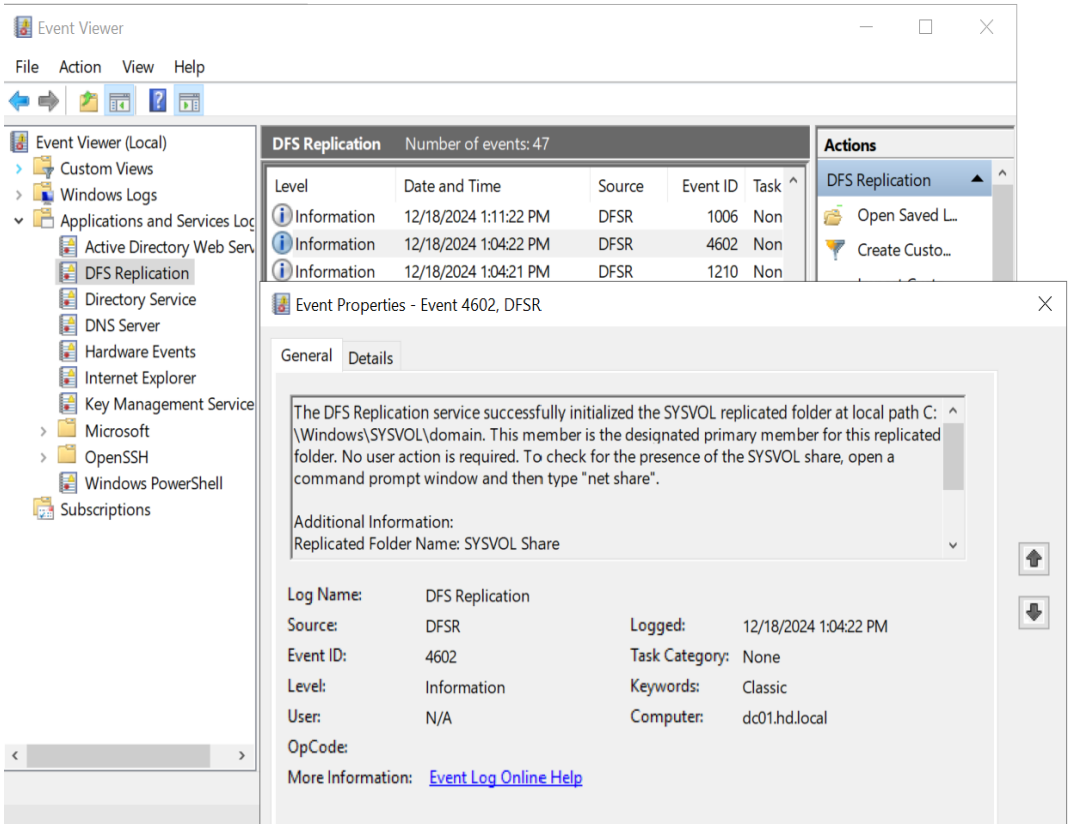
MsDFSR-Enabled TRUE ve **msDFSR-Options 1** olacak şekilde değiştiriyorum

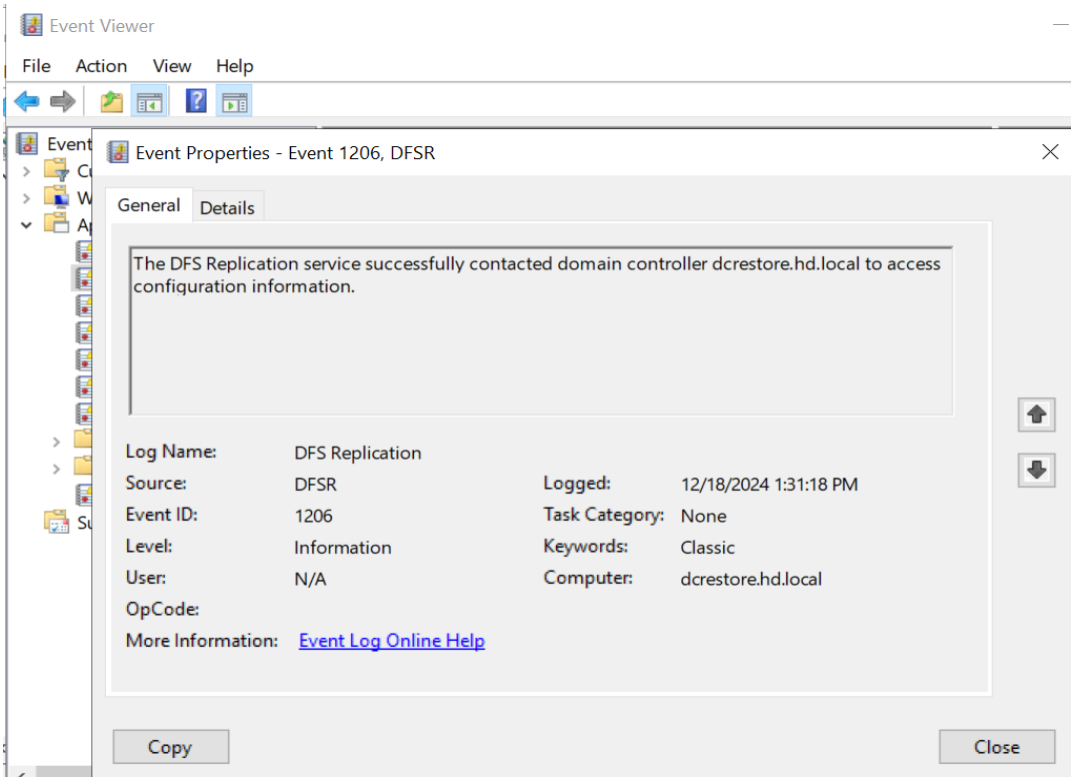


Daha sonrasında DFS servisini restart ediyorum.



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

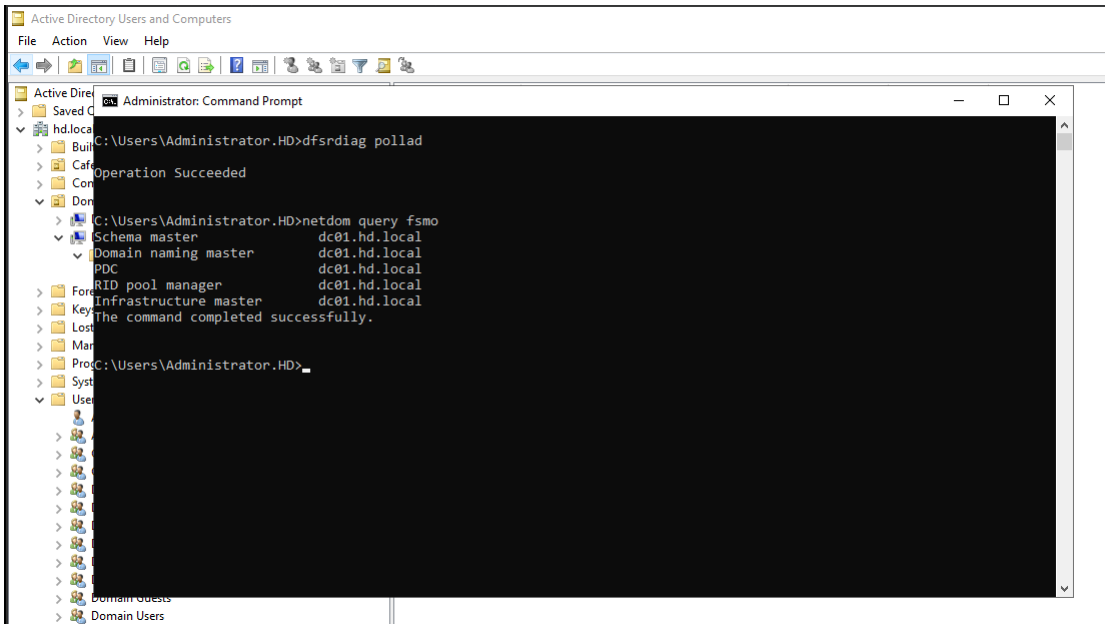




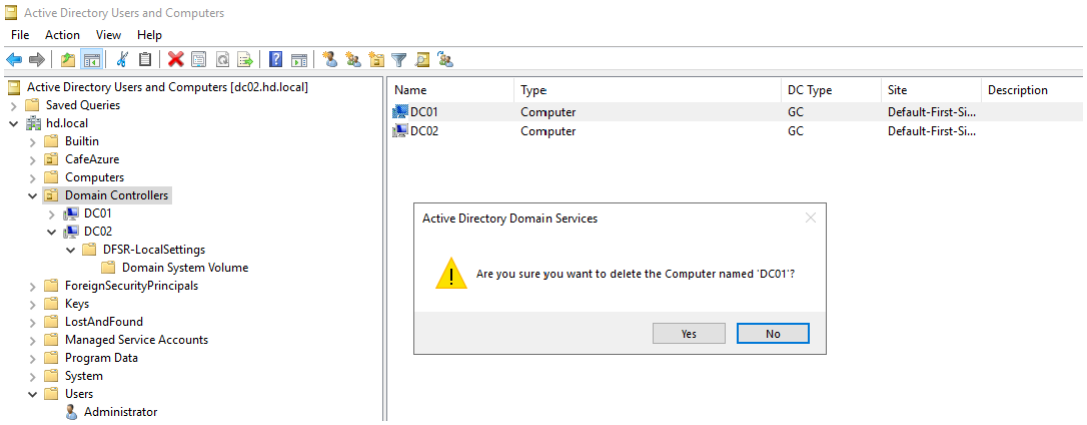
[Force synchronization for Distributed File System Replication (DFSR) replicated sysvol replication - Windows Server | Microsoft Learn]

Metadata Cleanup ve FSMO Role Seizing

FSMO rolümün hangi dc de olduğnu kontrol ediyorum.

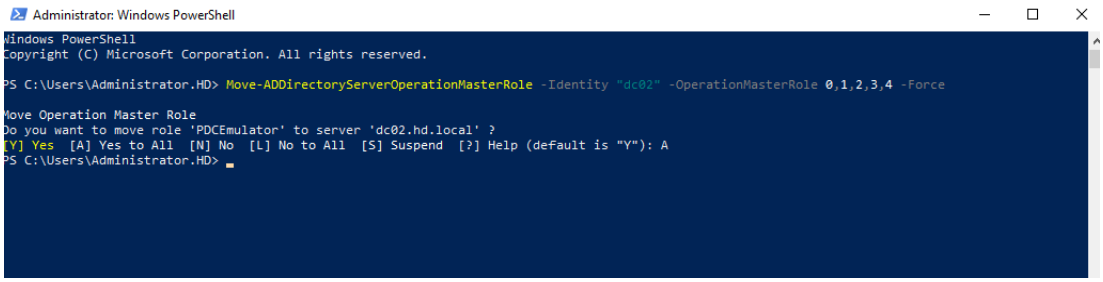


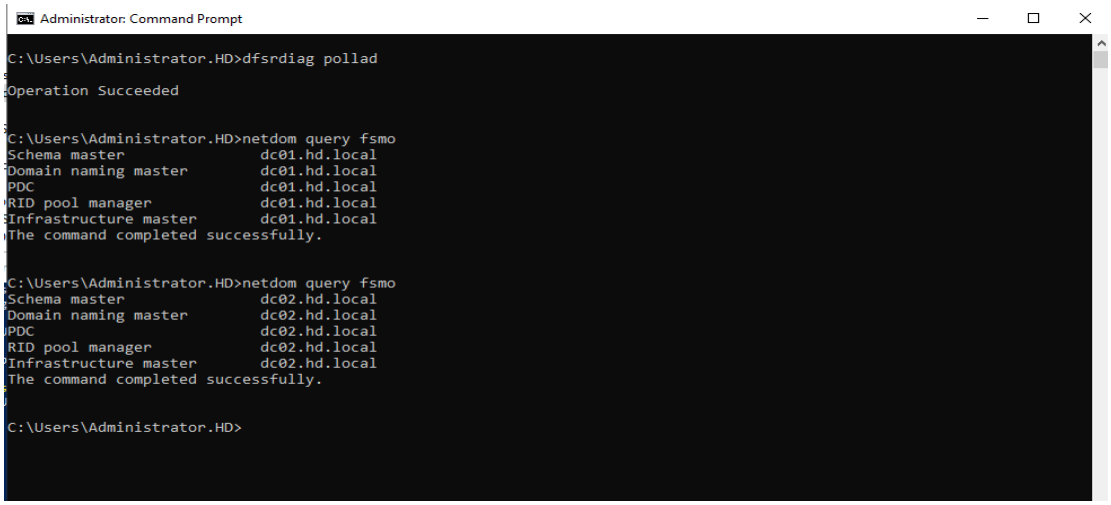
Doğal olarak eski dc lerime ulaşamadığım için fsmo rollerimi zorla almam gerekiyor. İlk olarak ulaşılamaz olan dc lerimi siliyorum.



FSMO rollerini powershell ile hızlıca taşımak için aşağıdaki komut kullanılabilir

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





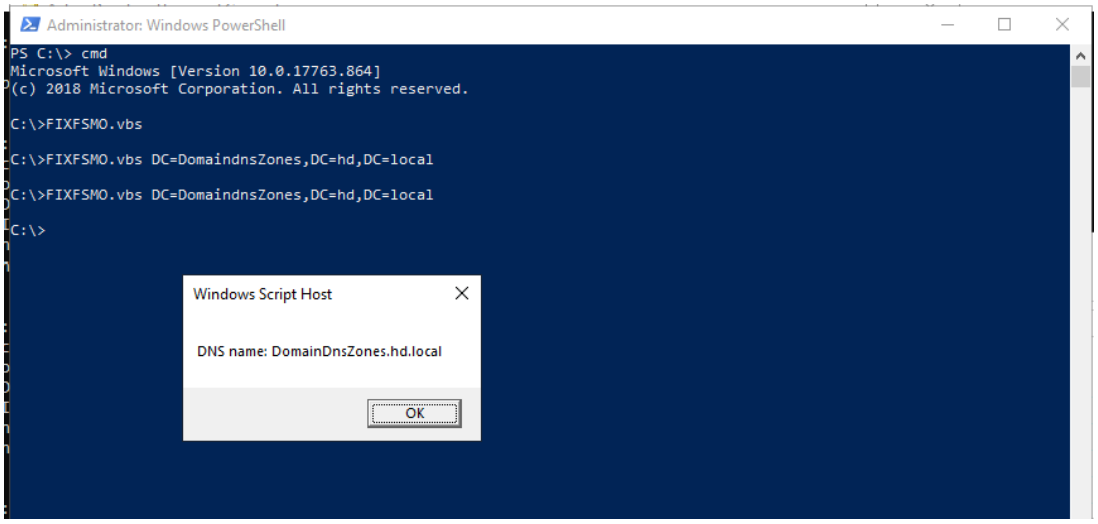
Not: Metadata cleanup ile ilgili detaylı yazıyı Mshowto github sayfasında Active Directory Migration konusunda içerisinde ele aldım.

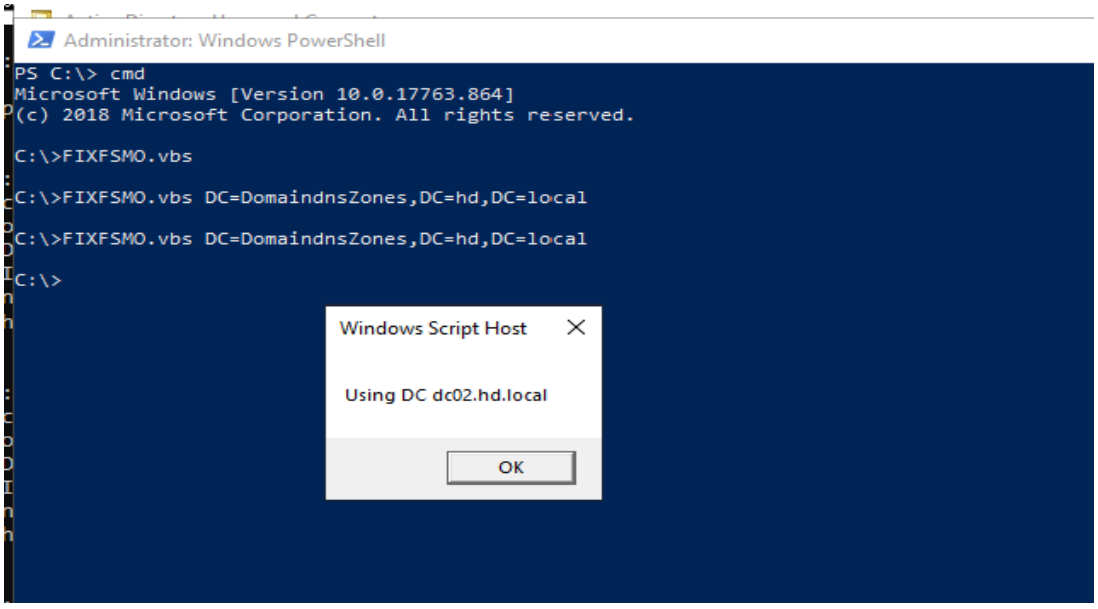
Geçersiz FSMO Role Holder Düzeltme

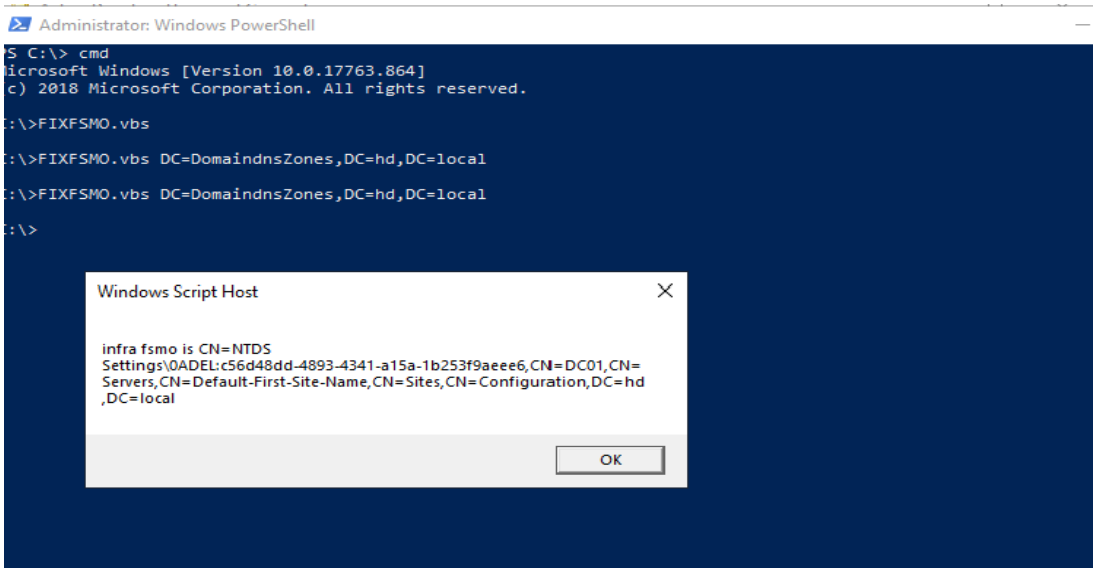
Aşağıdaki linkten ilgili scripti DC mize kopyalıyoruz

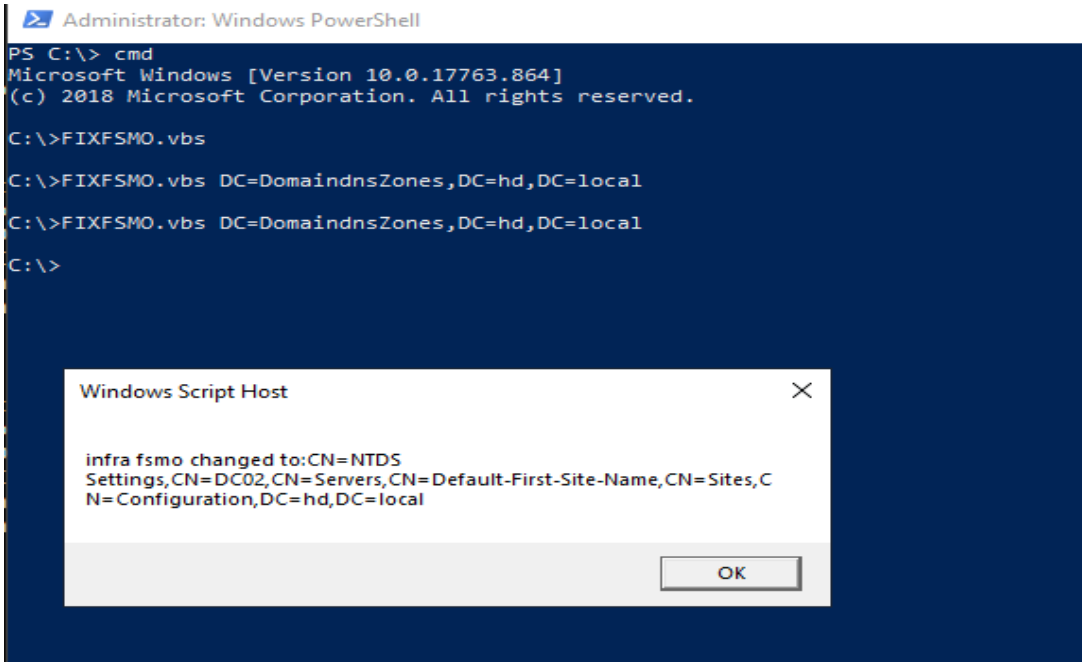
Error when running the Adprep /rodcprep command in Windows Server 2008 - Windows Server | Microsoft Learn

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


Administrator: Windows PowerShell
PS C:\> cmd
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft 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
DNS name: DomainDnsZones.hd.local
OK


Administrator: Windows PowerShell
PS C:\> cmd
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft 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
Using DC dc02.hd.local
OK

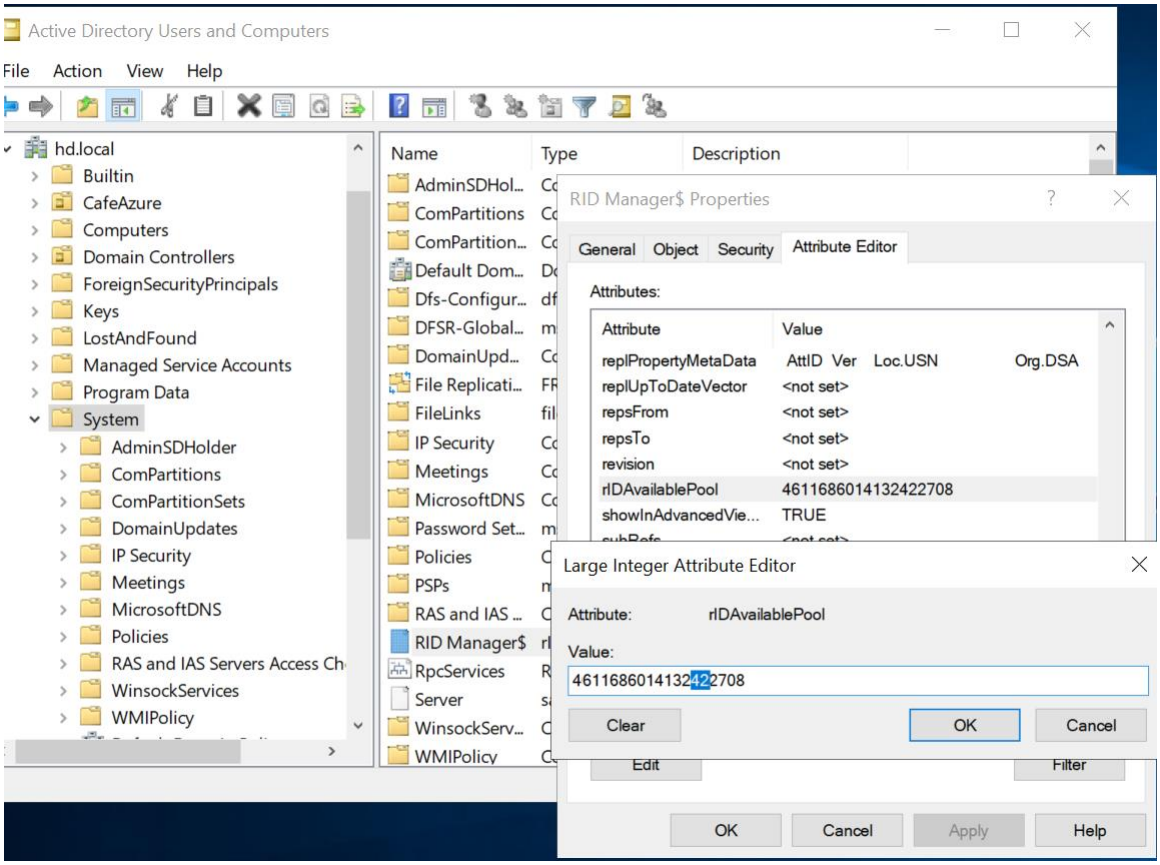

Administrator: Windows PowerShell
Windows Script Host
infra fsmo is CN=NTDS Settings\0ADEL:c56d48dd-4893-4341-a15a-1b253f9aeee6,CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=hd,DC=local
OK


Administrator: Windows PowerShell
PS C:\> cmd
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft 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
infra fsmo changed to:CN=NTDS
Settings,CN=DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,C
N=Configuration,DC=hd,DC=local
OK

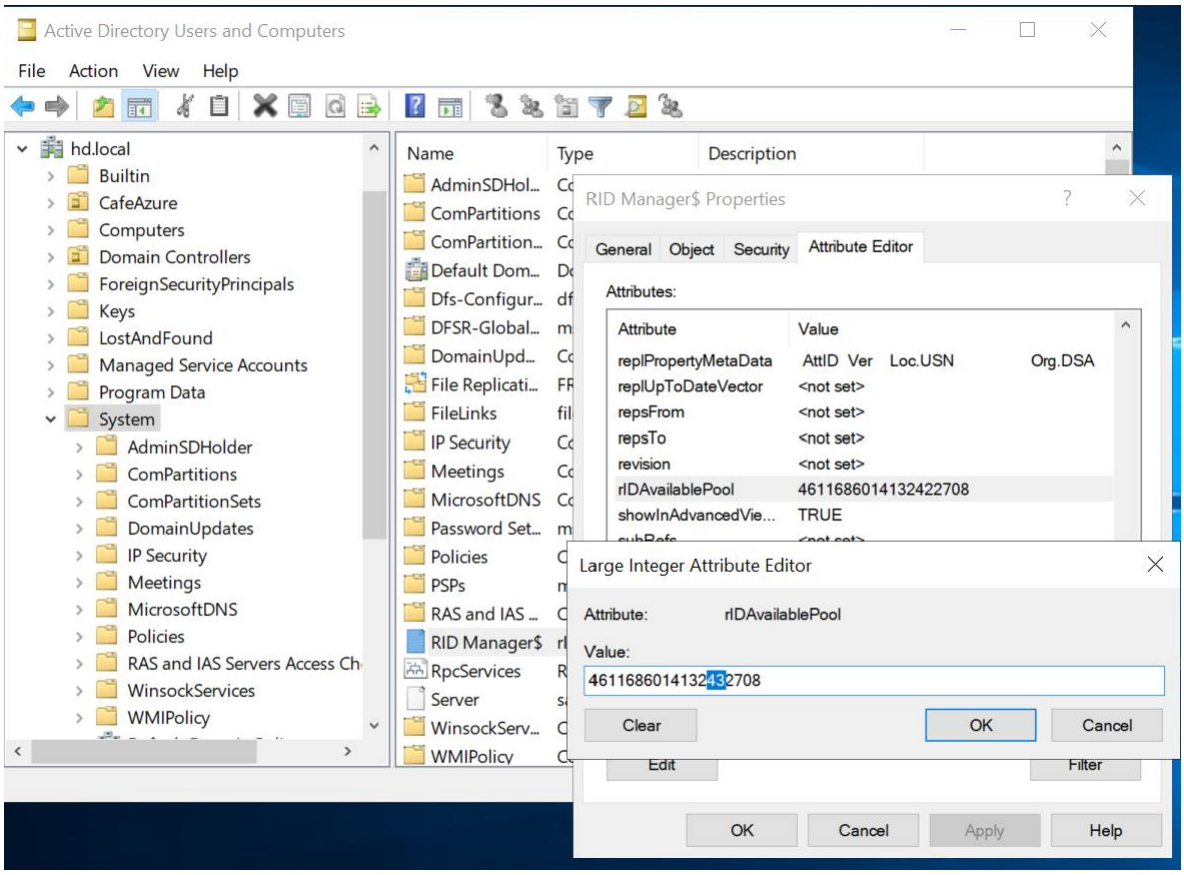
Varolan RID Havuzunu Geçersiz kılmak

rIDAvailablePool attribute ünü RID üzerindeki çakışmayı engellemek için değiştirmemiz gerekiyor .

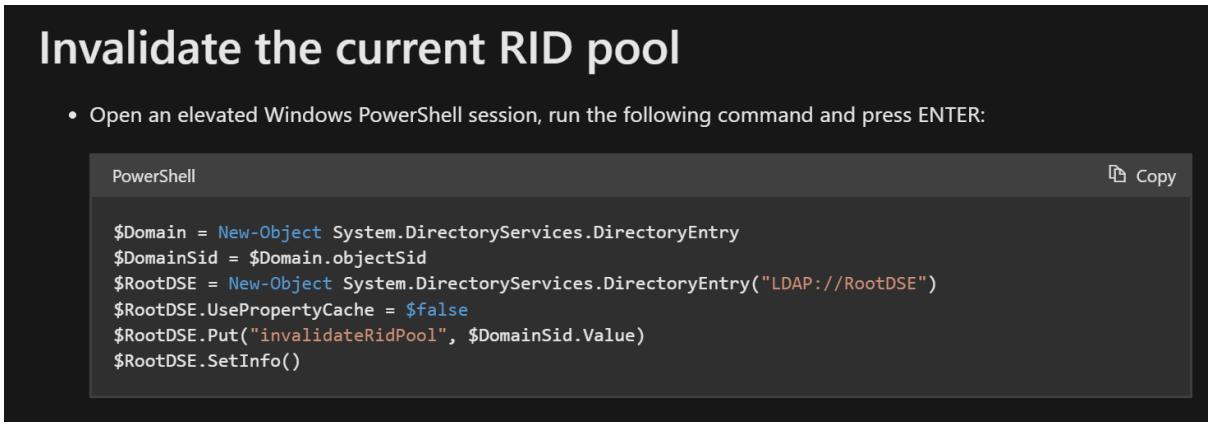
Eski Hali



Yeni Hali



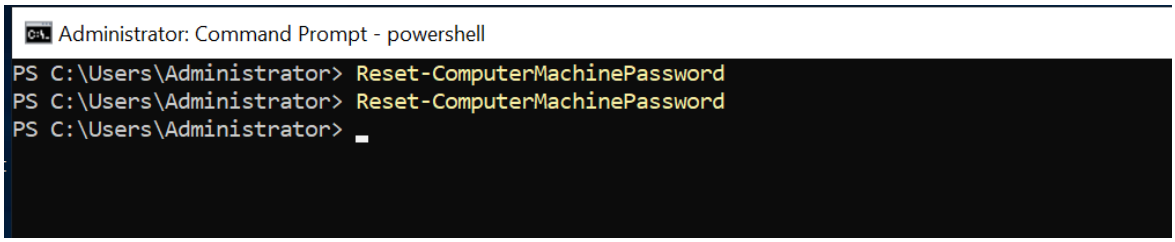
Aşağıdaki komut ile RID havuzunun hızlı bir şekilde güncellenmesini sağlamış oluyoruz.



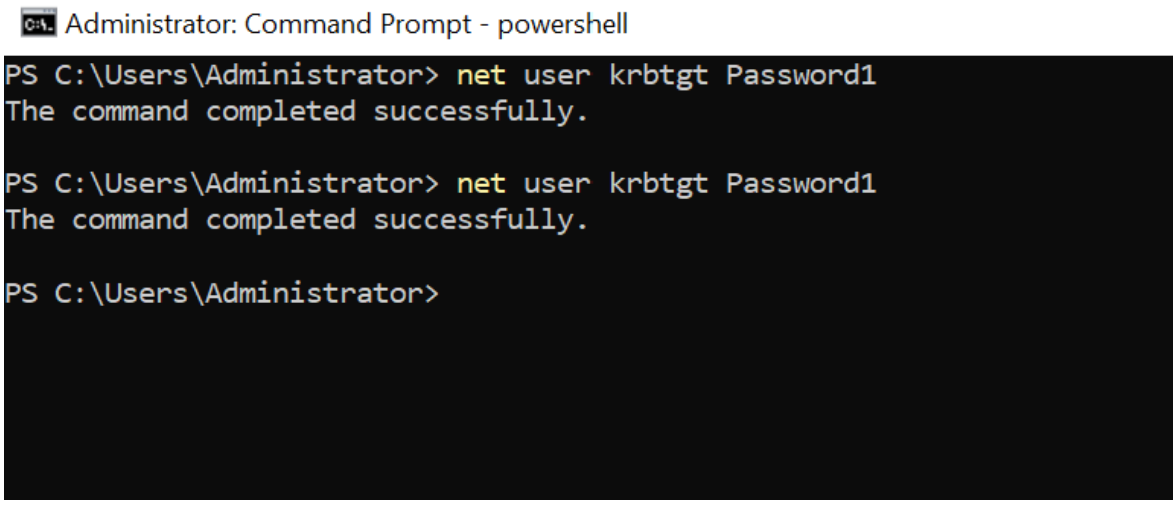
Kaynak : [AD Forest Recovery - Invalidating the RID Pool | Microsoft Learn]

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.

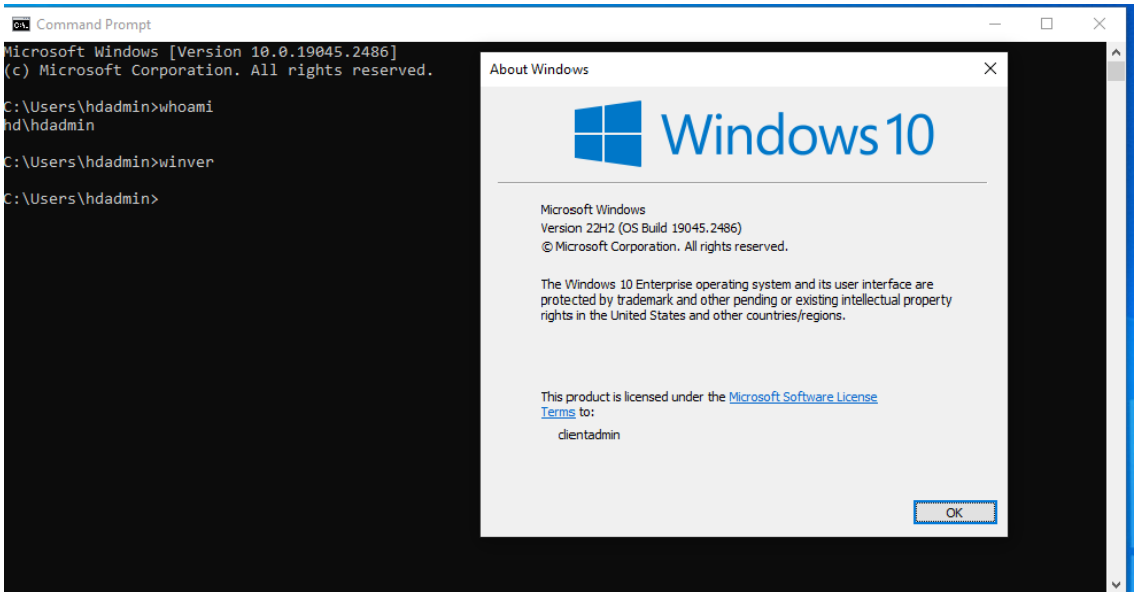


KRBTGT hesabını iki defa resetliyorum. Elbette kendi ortaminizda bu şekilde yapmadığınızdan eminim 😊



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