Zahid Mammadli

System Administration Project

1. **Layihəni Hyper V və ya Vmware Workstation üzərində hazırlaya bilərsiniz.**
2. **IP addresslər və Şəbəkə kartları barədə seçimlər sərbəstdir**
3. **Domain controller kimi fəaliyyət göstərəcək VM hazır edin.**
4. **DC daxilində qeyd olunan ardıcıllıqla OU, User, Group, Computer accountları yaradın Computer Accountlarını VM olaraq yaradın və Domainə qoşduqdan sonra qeyd olunan OU-lara daşıyın.**

OU

OU=S306,OU=SysAdm,OU=Students,OU=Users,OU=Root,DC=example,DC=local

OU=S307,OU=SysAdm,OU=Students,OU=Users,OU=Root,DC=example,DC=local

OU=IT,OU=Managers,OU=Staff,OU=Users,OU=Root,DC=example,DC=local

OU=Sales,OU=Managers,OU=Staff,OU=Users,OU=Root,DC=example,DC=local

OU=Red,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

OU=Green,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

OU=IT,OU=Staff,OU=Computers,OU=Root,DC=example,DC=local

OU=Sales,OU=Staff,OU=Computers,OU=Root,DC=example,DC=local

OU=Servers,OU=Computers,OU=Root,DC=example,DC=local

User

CN={Öz adınız},OU=S306,OU=SysAdm,OU=Students,OU=Users,OU=Root,DC=example,DC=local

CN={Random},OU=S307,OU=SysAdm,OU=Students,OU=Users,OU=Root,DC=example,DC=local

CN={Random},OU=IT,OU=Managers,OU=Staff,OU=Users,OU=Root,DC=example,DC=local

CN={Random},OU=Sales,OU=Managers,OU=Staff,OU=Users,OU=Root,DC=example,DC=local

Users Group

CN=S306-Users,OU=S306,OU=SysAdm,OU=Students,OU=Users,OU=Root,DC=example,DC=local

CN=S307-Users,OU=S307,OU=SysAdm,OU=Students,OU=Users,OU=Root,DC=example,DC=local

CN=IT-Users,OU=IT,OU=Managers,OU=Staff,OU=Users,OU=Root,DC=example,DC=local

CN=Sales-Users,OU=Sales,OU=Managers,OU=Staff,OU=Users,OU=Root,DC=example,DC=local

Computer

CN=E-red01,OU=Red,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

CN=E-green02,OU=Green,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

CN=E-IT04,OU=IT,OU=Staff,OU=Computers,OU=Root,DC=example,DC=local

CN=E-Sales03,OU=Sales,OU=Staff,OU=Computers,OU=Root,DC=example,DC=local

CN=E-FS01,OU=Servers,OU=Computers,OU=Root,DC=example,DC=local

CN=E-FS02,OU=Servers,OU=Computers,OU=Root,DC=example,DC=local

CN=E-BCK01,OU=Servers,OU=Computers,OU=Root,DC=example,DC=local

CN=E-BCK02,OU=Servers,OU=Computers,OU=Root,DC=example,DC=local

Computers Group

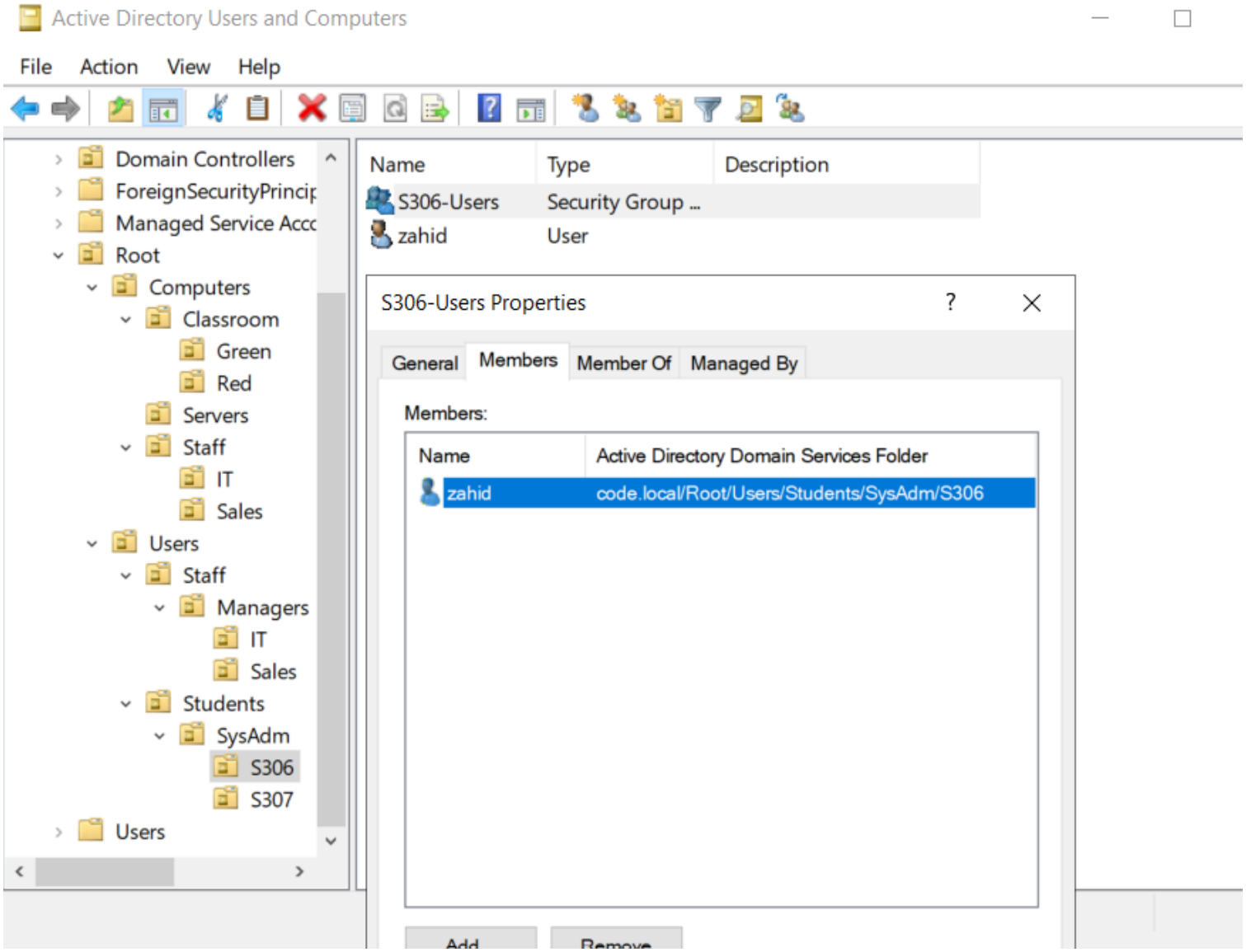
CN=Red-Computers,OU=Red,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

CN=Green-Computers,OU=Green,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

CN=IT-Computers,OU=IT,OU=Staff,OU=Computers,OU=Root,DC=example,DC=local

CN=Sales-Computers,OU=Sales,OU=Staff,OU=Computers,OU=Root,DC=example,DC=local

CN=Servers,OU=Servers,OU=Computers,OU=Root,DC=example,DC=local



5. Red, Green, Sales, Servers OU-larında olan computerlərdə Group Policy Vasitəsilə aşağıda qeyd olunanları tətbiq edin

- USB qosub işlətmək mümkün olmasın
- Interactive mesajlardan istifadə edərək maşın açılışında istifadəçilərə maşının istifadə qaydasına dair bəzi məlumatlar verin
- Maşınları sadəcə administrator yetkisinə sahib userlər söndürə (shutdown) bilsin
- Group policylər arxa planda hər 30 dəqiqədən bir (20+10) tətbiq olunsun

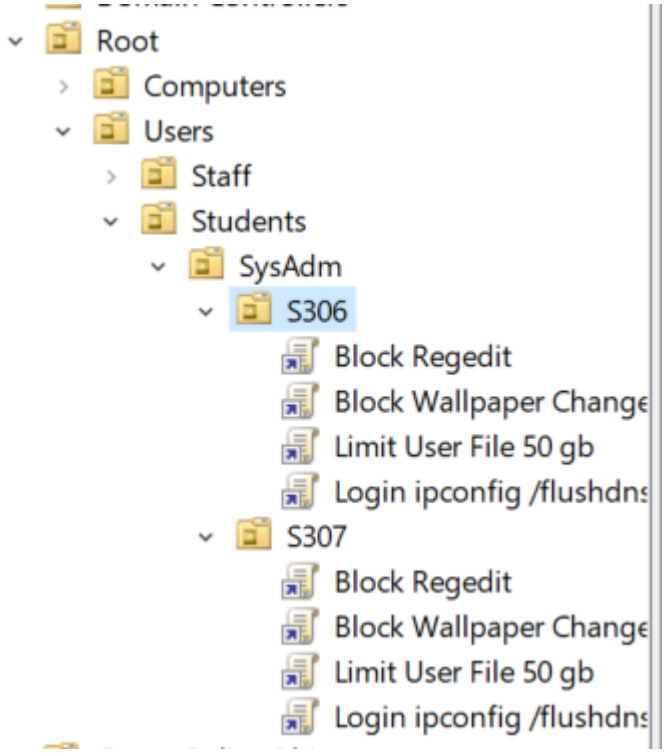
- 2 saatdan çox istifadə olunmayan kompyuterlərdə session-lar lock edilsin
- Cache-də sadəcə 1 istifadəçinin məlumatları saxlanılsın
- Şifrənin bitməyinə 4 gün qalmış istifadəçin ekranına bildiriş gəlsin
- Administrator accountunun username-ni dəyişin və təsadüfi bir ad verin
- Guest accountunun username-ni dəyişin və təsadüfi bir ad verin
- Varsayılan firewall rule-ları necədirsə bütün kompyuterlərdə eyni qaydada qalsın istifadəçilər (admin və ya user) bu qaydada local maşınlarda dəyişə bilməsinlər
- Istifadəçilərin maşınlara uğurlu və uğursuz loginləri audit olunsun
- Istifadəçilərin paylaşılmış folderlərə uğurlu və uğursuz bağlantısı audir olunsun
- Istifadəçilər pin yazaraq login ola bilsinlər
- Pin 42 gündən bir dəyişilsin, pinin max uzunluğu 8, minimum uzunlugu 4 olsun, kiçik herf və rəqəm mütləq iştirak etsin
- Daha öncə login olan userin məlumatları görünməsin
- 14 gündən çox istifadə olunmayan user profilləri (localdan) silinsin
-
- Biometric girişlər istifadə oluna bilsin
- Cortana istifadə oluna bilməsin
- Store applicationları blocklansın
- Powershell scriptləri local və digital signed olaraq execute oluna bilsin

GPO Settings Video:

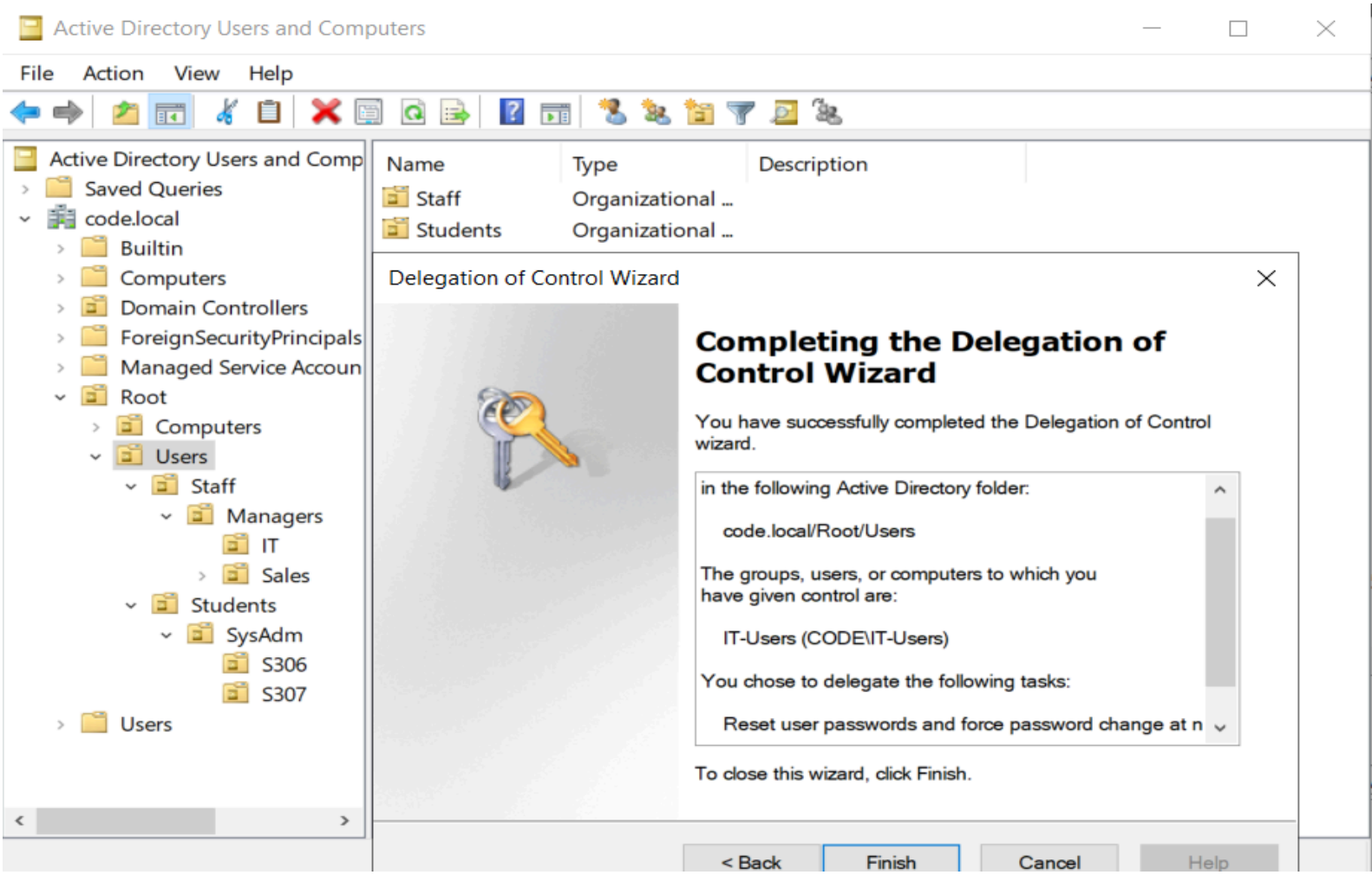
https://drive.google.com/file/d/1c6wix7r7WcVOe2R5PPbZGugxIP1sYPal/view?usp=share_link

6. S306, s307, sales OU-larında olan userlər üçün aşağıdaki policyləri tətbiq edin

- İstifadəçilər yeni şəkil tətbiq edə bilməsin
- Istifadəçilər regeditə daxil ola bilməsin
- Istifadəçi faylları 50 gb-ı keçməsin
- Istifadəçi logon etdiyi zaman ipconfig /flushdns komandası işə düşsün

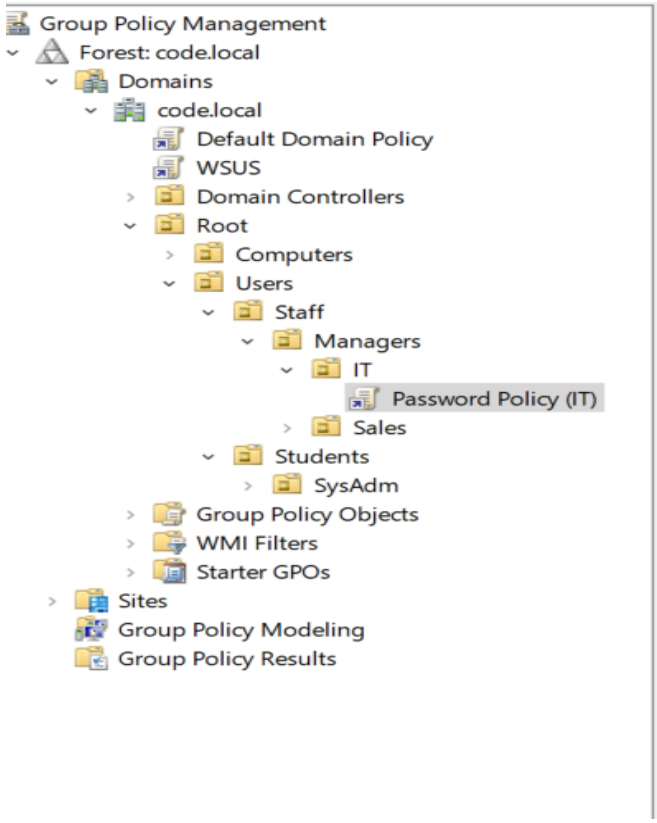


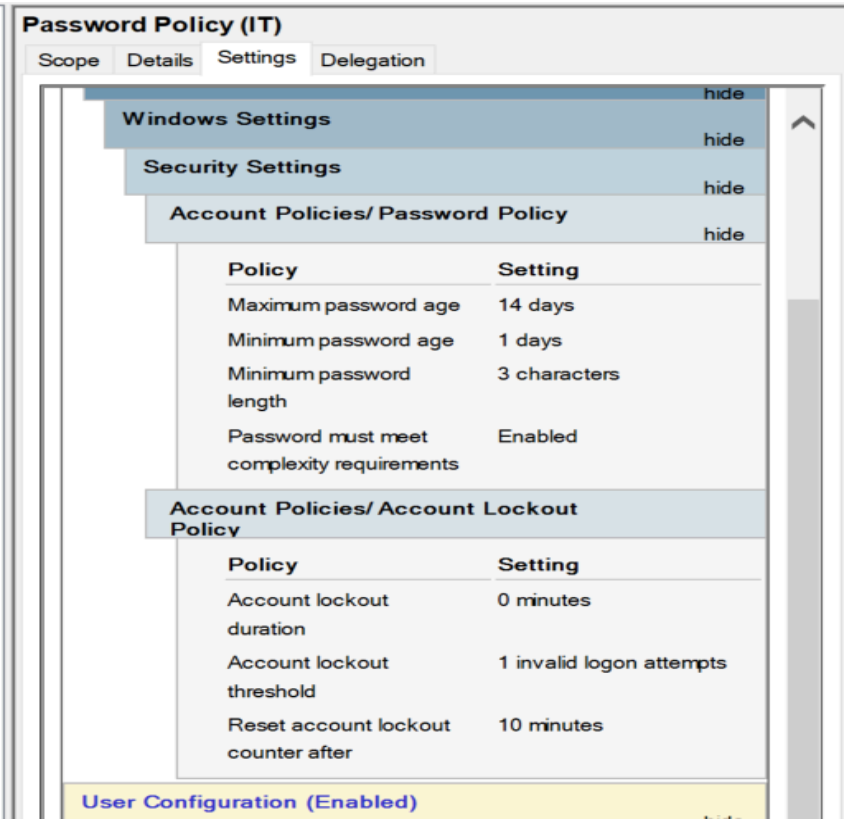
7. IT-Users qrupunda olan userlər Users OU-sunda olan bütün userlərin şifrəsini reset edə bilsin, domainə kompyuter üzv edə bilsin.



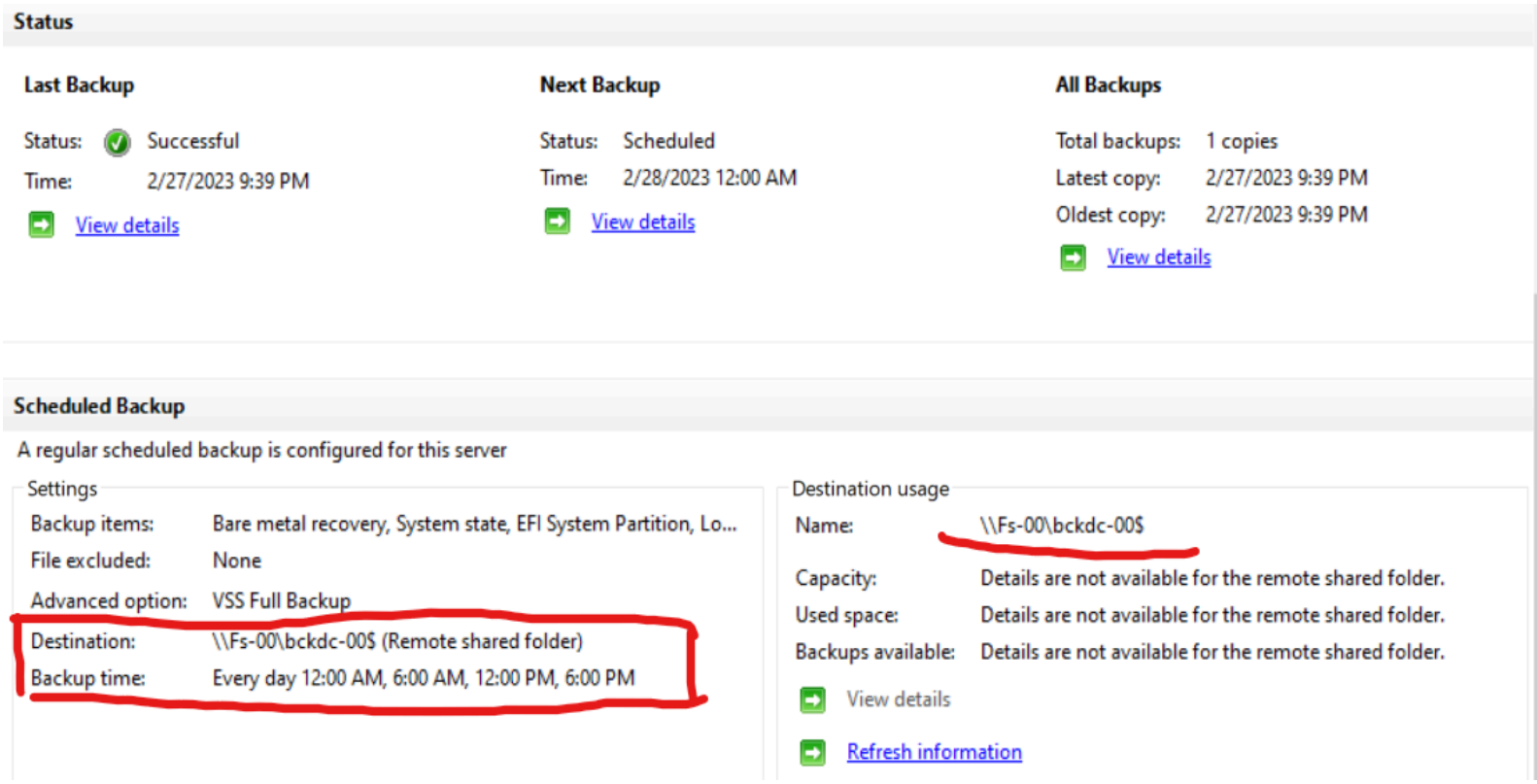
8. IT-Users qrupunda olan userlər üçün xüsusi password policy tətbiq edin:

Password minimal uzunluğu 3, minimal dəyişmə günü 1, maximum ömrü 14 gün, complex(enabled), 1 səhv yazılan şifrəylə account lock olsun, accountu yalnız domain admin bərpa edə bilsin.

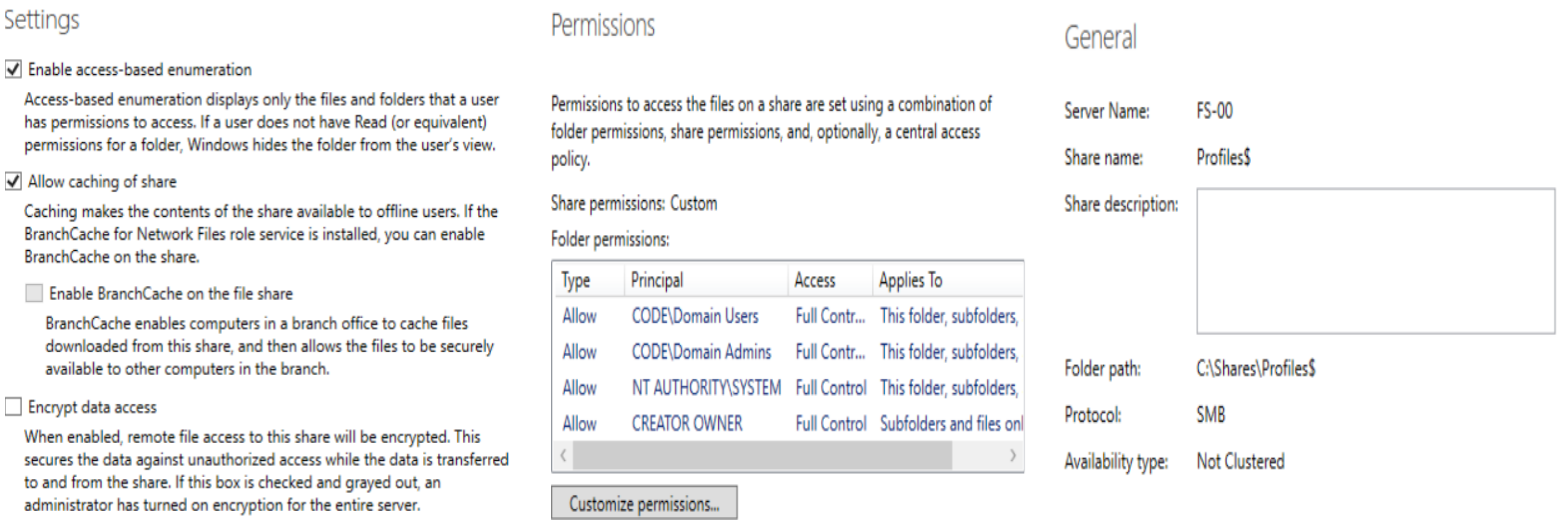




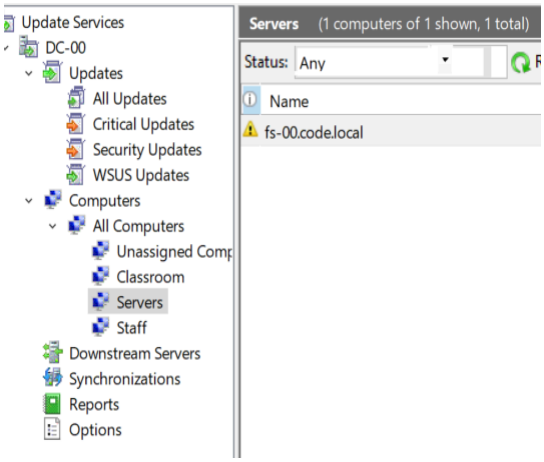
9. DC-dən E-B CK01 maşınına gündə 4 dəfə, 6 saatdan bir backup götürün. Backup Folderi gizli şəkildə paylaşılmış olsun. NTFS Permission olmayan userlər folderi görə bilməsin.

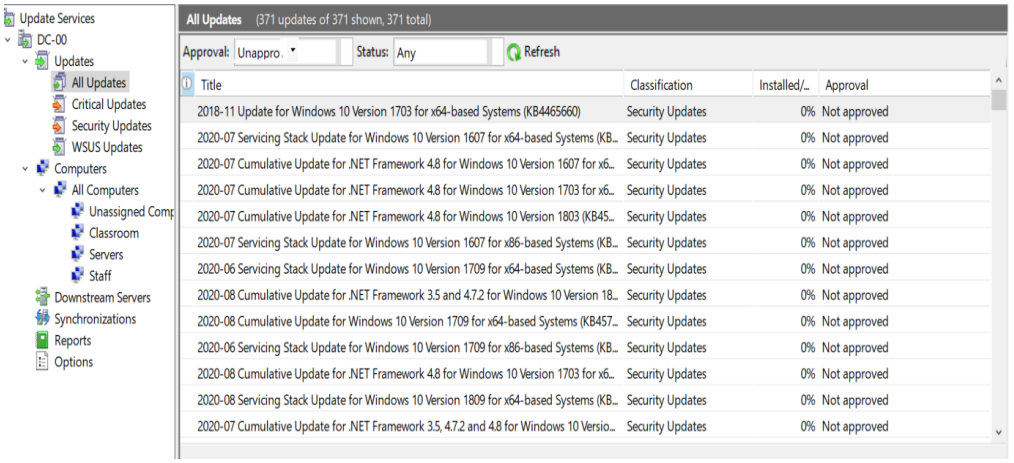


10. E-FS01 maşınında Profiles adlı Folder yaradıb gizli paylaşıma açın. Folder gizli şəkildə paylaşılmış olsun. NTFS Permission olmayan userlər folderi görə bilməsin.



11. WSUS Server Hazır edin. Windows 10 və Windows Serverlər üçün updatelər bir mərkəzdən idarə olunsun. WSUS daxilində OU adlarına uyğun kompyuter qrupları olsun və kompyuterlər uyğun qruplarda olsun.





12. DNS Serverdə olan Forward Lookup Zoneları (example.local) replicate edəcəyiniz bir DNS Server qurun.

13. Task Scheduler vasitəsilə (Group Policy daxilində və ya Hər maşında) aşağıdaki Taskları tətbiq edin - Red, Green, Sales kompyuterləri hər gün axşam 22:00 da hər bir halda sönsün

- E-BCK01 serverində olan DC Backupı axşam 10-dan səhər 7-yə qədər Google Drive-a Sync olunsun - Red, Green, Sales kompyuterlərinə hər hansı bir user login olduğu zaman google chrome işə düşsün və gmail.com, calendar.google.com səhifələri ayrı tablar açılsın

- Downloads və tmp(temp) folderlərində olan fayllar 14 gündən köhnədirsə avtomatik silinsin