

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 ardıcılıqla 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

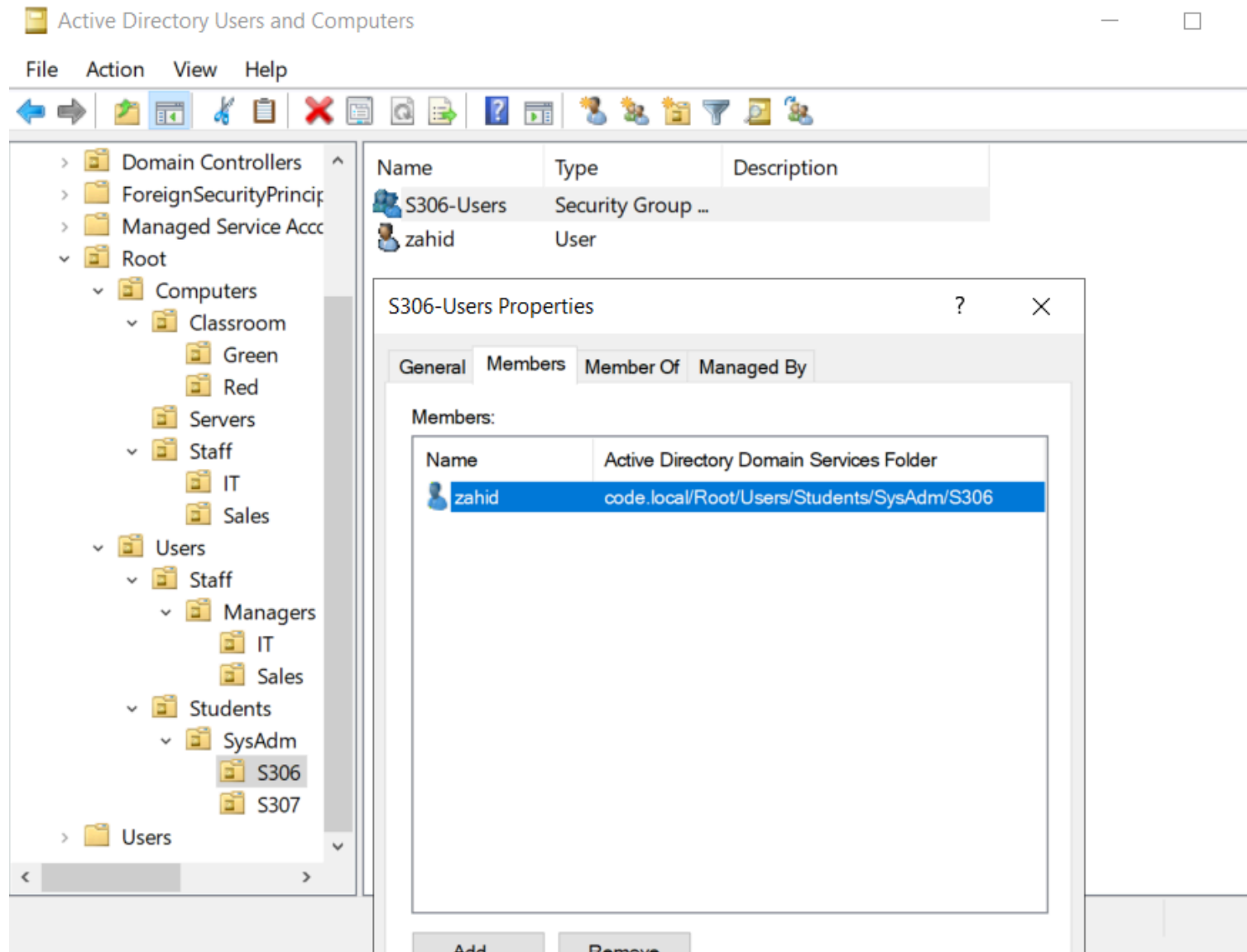
CN=Red-Computers,OU=Red,OU=Classroom,OU=Computers,OU=Root,DC=example,DC=local

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

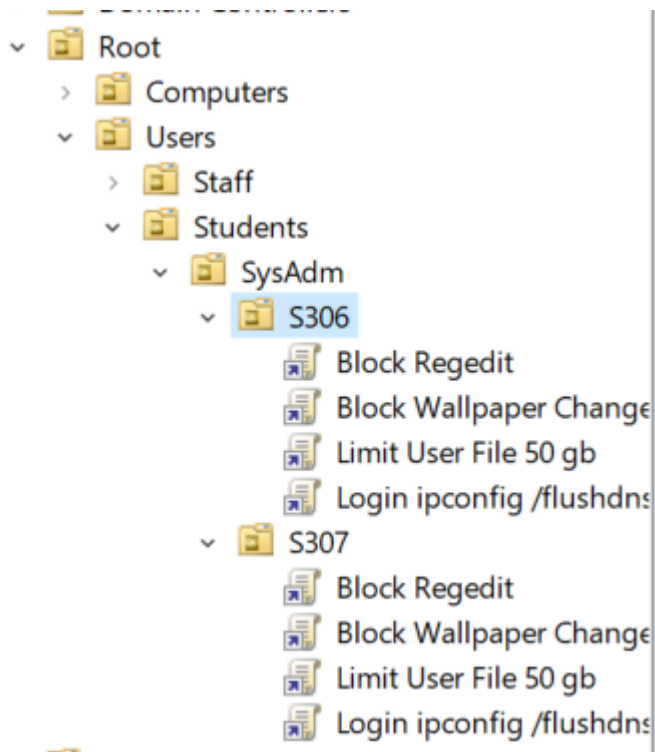
- 2 saatdan çox istifadə olunmayan kompyuterlərdə session-lar lock edilsin
- Cache-də sadəcə 1 istifadəçinin məlumatları saxlanılsın
- Şifrənin bitməyinə 4 gün qalmış istifadəçinin ekranına bildiriş gəlsin
- Administrator accountunun username-ni dəyişin və təsadüfi bir ad verin
- Guest accountunun username-ni 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
- İstifadəçilərin maşınlara uğurlu və uğursuz loginləri audit olunsun
- İstifadəçilərin paylaşılmış folderlərə uğurlu və uğursuz bağlantısı audir olunsun
- İstifadəçilər pin yazaraq login ola bilsinlər
- Pin 42 gündən bir dəyişilsin, pinin max uzunluğu 8, minimum uzunluğu 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:

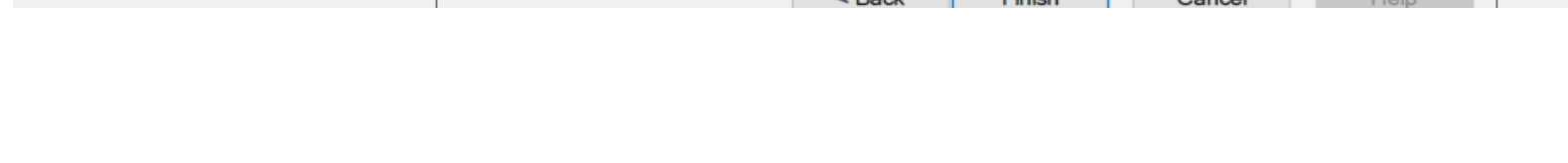
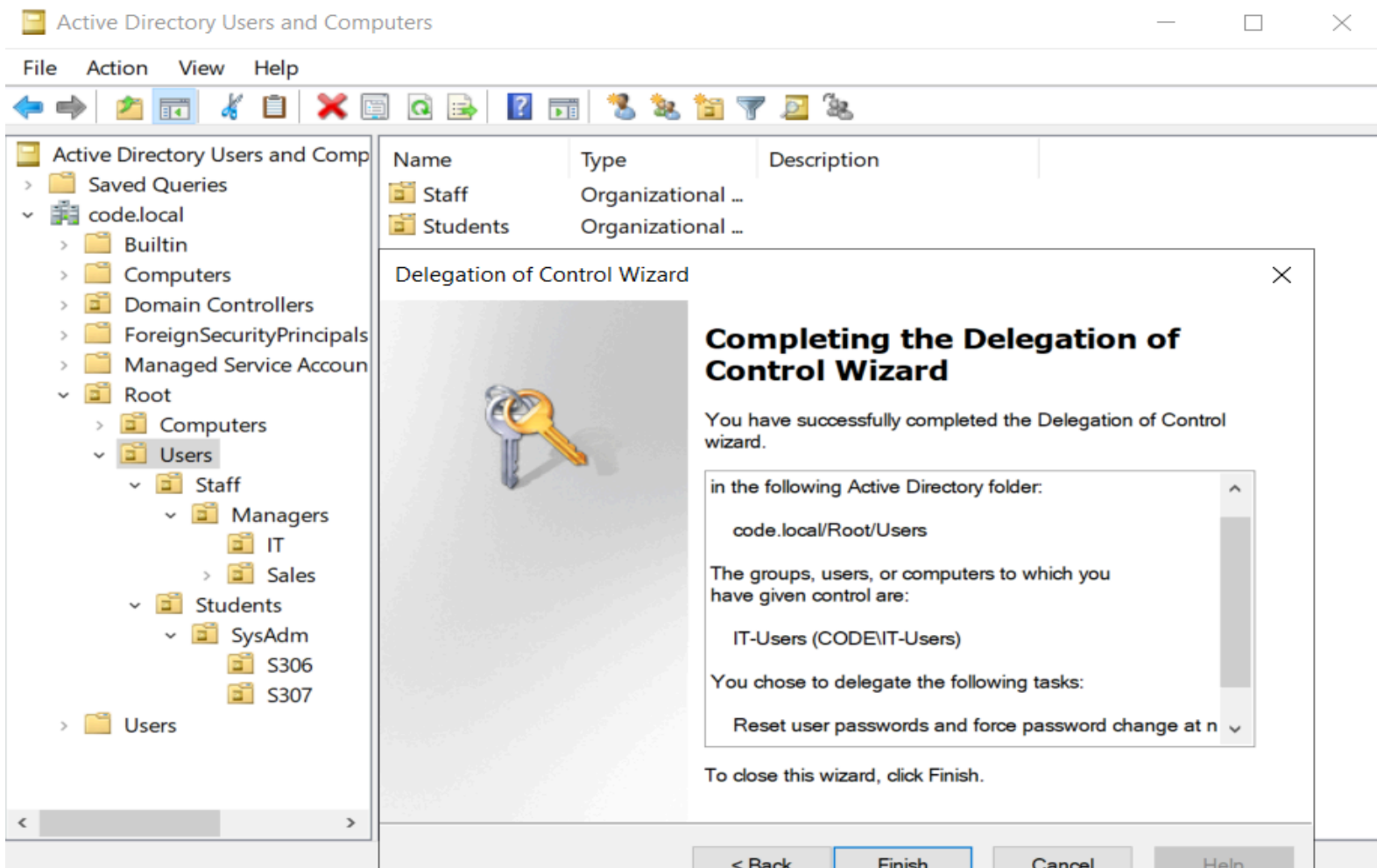
https://drive.google.com/file/d/1c6wix7r7WcVOe2R5PPbZGugxIP1sYPal/view?usp=share_link

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

- İstifadəçilər yeni şəkil tətbiq edə bilməsin
- İstifadəçilər regeditə daxil ola bilməsin
- İstifadəçi faylları 50 gb-ı keçməsin
- İstifadəçi 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.

The screenshot shows the Group Policy Management console. On the left, the tree view is expanded to 'Forest: code.local' > 'Domains' > 'code.local' > 'Users' > 'Staff' > 'Managers' > 'IT' > 'Password Policy (IT)'. The right pane shows the 'Password Policy (IT)' configuration page. The 'Settings' tab is selected. Under 'Account Policies/ Password Policy', the following settings are configured: Maximum password age: 14 days, Minimum password age: 1 days, Minimum password length: 3 characters, Password must meet complexity requirements: Enabled. Under 'Account Policies/ Account Lockout Policy', the following settings are configured: Account lockout duration: 0 minutes, Account lockout threshold: 1 invalid logon attempts, Reset account lockout counter after: 10 minutes. At the bottom, it says 'User Configuration (Enabled)'.

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.

Status

Last Backup

Status: Successful
Time: 2/27/2023 9:39 PM
[View details](#)

Next Backup

Status: Scheduled
Time: 2/28/2023 12:00 AM
[View details](#)

All Backups

Total backups: 1 copies
Latest copy: 2/27/2023 9:39 PM
Oldest copy: 2/27/2023 9:39 PM
[View details](#)

Scheduled Backup

A regular scheduled backup is configured for this server

Settings

Backup items: Bare metal recovery, System state, EFI System Partition, Lo...
File excluded: None
Advanced option: VSS Full Backup
Destination: \\Fs-00\bckdc-00\$ (Remote shared folder)
Backup time: Every day 12:00 AM, 6:00 AM, 12:00 PM, 6:00 PM

Destination usage

Name: \\Fs-00\bckdc-00\$
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.

[View details](#)
[Refresh information](#)

10. E-FS01 maşınında Profiles adlı Folder yaradıb gizli paylaşımına açın. Folder gizli şəkildə paylaşılmış olsun.

NTFS Permission olmayan userlər folderi görə bilməsin.

Settings

☒ **Enable access-based enumeration**
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☒ **Allow caching of share**
Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

☐ **Enable BranchCache on the file share**
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

☐ **Encrypt data access**
When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

Permissions

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Custom

Folder permissions:

Type	Principal	Access	Applies To
Allow	CODE\Domain Users	Full Contr...	This folder, subfolders,
Allow	CODE\Domain Admins	Full Contr...	This folder, subfolders,
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders,
Allow	CREATOR OWNER	Full Control	Subfolders and files onl

[Customize permissions...](#)

General

Server Name: FS-00

Share name: Profiles\$

Share description:

Folder path: C:\Shares\Profiles\$

Protocol: SMB

Availability type: Not Clustered

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.

Update Services

Update Services

- DC-00
 - Updates
 - All Updates
 - Critical Updates
 - Security Updates
 - WSUS Updates
 - Computers
 - All Computers
 - Unassigned Comp...
 - Classroom
 - Servers
 - Staff
 - Downstream Servers
 - Synchronizations
 - Reports
 - Options

Servers

(1 computers of 1 shown, 1 total)

Status: Any

Name
fs-00.code.local

All Updates

(371 updates of 371 shown, 371 total)

Approval: Unappro... Status: Any Refresh

Title	Classification	Installed/...	Approval
2018-11 Update for Windows 10 Version 1703 for x64-based Systems (KB4465660)	Security Updates	0%	Not approved
2020-07 Servicing Stack Update for Windows 10 Version 1607 for x64-based Systems (KB...	Security Updates	0%	Not approved
2020-07 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1607 for x6...	Security Updates	0%	Not approved
2020-07 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1703 for x6...	Security Updates	0%	Not approved
2020-07 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1803 (KB45...	Security Updates	0%	Not approved
2020-07 Servicing Stack Update for Windows 10 Version 1607 for x86-based Systems (KB...	Security Updates	0%	Not approved
2020-06 Servicing Stack Update for Windows 10 Version 1709 for x64-based Systems (KB...	Security Updates	0%	Not approved
2020-08 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows 10 Version 18...	Security Updates	0%	Not approved
2020-08 Cumulative Update for Windows 10 Version 1709 for x64-based Systems (KB457...	Security Updates	0%	Not approved
2020-06 Servicing Stack Update for Windows 10 Version 1709 for x86-based Systems (KB...	Security Updates	0%	Not approved
2020-08 Cumulative Update for .NET Framework 4.8 for Windows 10 Version 1703 for x6...	Security Updates	0%	Not approved
2020-08 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems (KB...	Security Updates	0%	Not approved
2020-07 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows 10 Versio...	Security Updates	0%	Not approved

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

13. Task Scheduler vasitəsilə (Group Policy daxilində və ya Hər maşında) aşağıdakı 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 tablalar açılsın

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