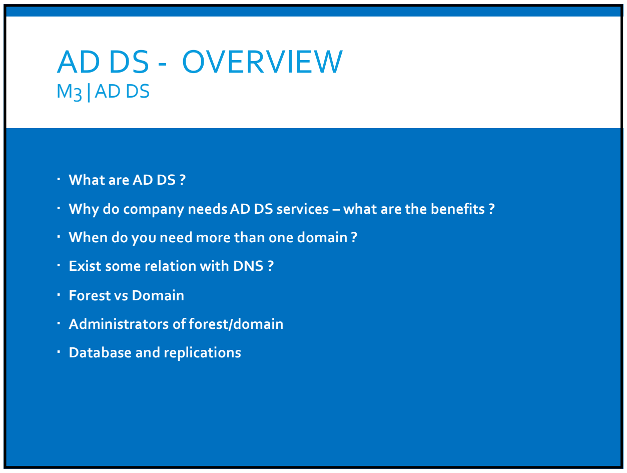
Module_4

AD DS and Group Policy

1

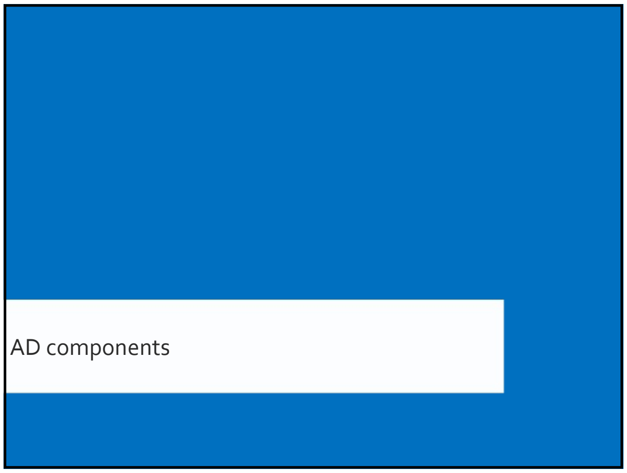


AD DS - OVERVIEW

M3 | AD DS

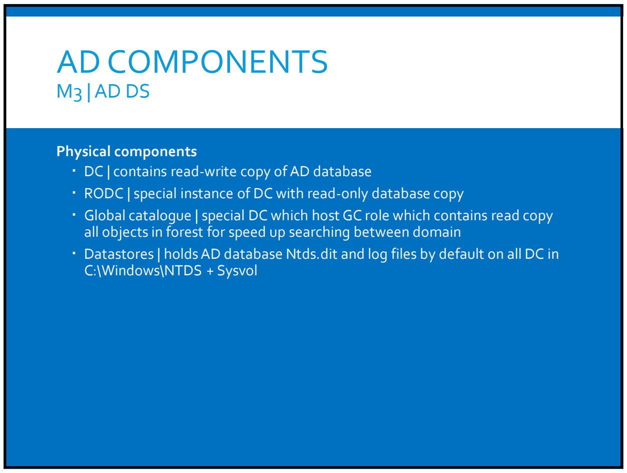
- What are AD DS ?
- Why do company needs AD DS services – what are the benefits ?
- When do you need more than one domain ?
- Exist some relation with DNS ?
- Forest vs Domain
- Administrators of forest/domain
- Database and replications

2



AD components

3



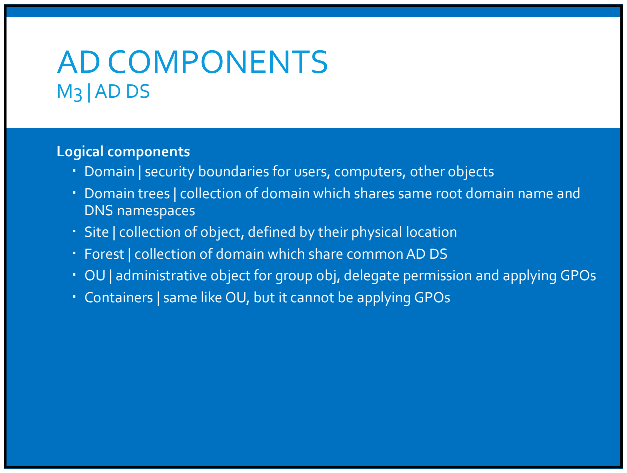
AD COMPONENTS

M3 | AD DS

Physical components

- DC | contains read-write copy of AD database
- RODC | special instance of DC with read-only database copy
- Global catalogue | special DC which host GC role which contains read copy all objects in forest for speed up searching between domain
- Datastores | holds AD database Ntds.dit and log files by default on all DC in C:\Windows\NTDS + Sysvol

4



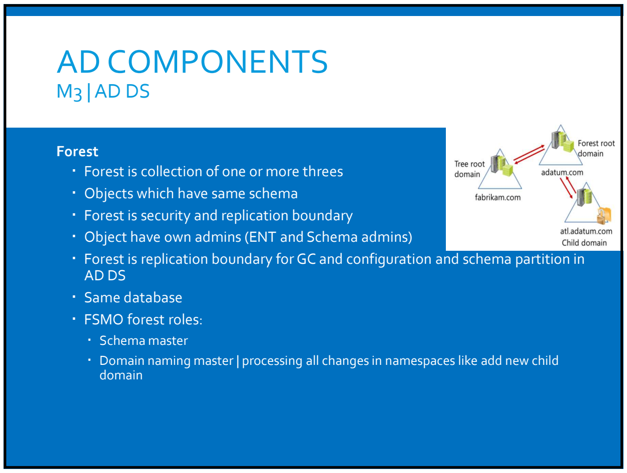
AD COMPONENTS

M3 | AD DS

Logical components

- Domain | security boundaries for users, computers, other objects
- Domain trees | collection of domain which shares same root domain name and DNS namespaces
- Site | collection of object, defined by their physical location
- Forest | collection of domain which share common AD DS
- OU | administrative object for group obj, delegate permission and applying GPOs
- Containers | same like OU, but it cannot be applying GPOs

5



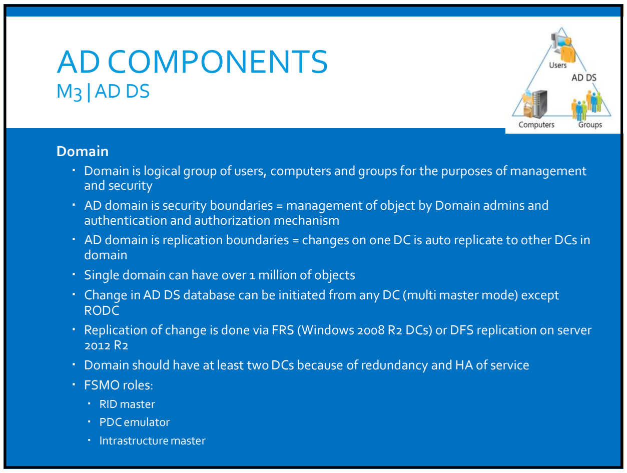
AD COMPONENTS

M3 | AD DS

Forest

- Forest is collection of one or more threes
- Objects which have same schema
- Forest is security and replication boundary
- Object have own admins (ENT and Schema admins)
- Forest is replication boundary for GC and configuration and schema partition in AD DS
- Same database
- FSMO forest roles:
  - Schema master
  - Domain naming master | processing all changes in namespaces like add new child domain

6



Users
AD DS
Computers
Groups

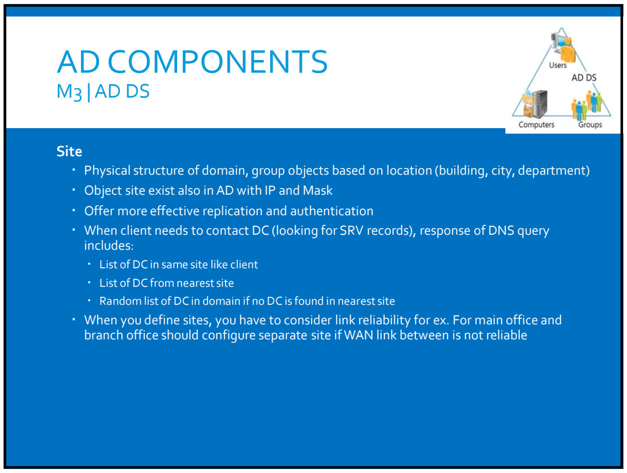
AD COMPONENTS

M3 | AD DS

Domain

- Domain is logical group of users, computers and groups for the purposes of management and security
- AD domain is security boundaries = management of object by Domain admins and authentication and authorization mechanism
- AD domain is replication boundaries = changes on one DC is auto replicate to other DCs in domain
- Single domain can have over 1 million of objects
- Change in AD DS database can be initiated from any DC (multi master mode) except RODC
- Replication of change is done via FRS (Windows 2008 R2 DCs) or DFS replication on server 2012 R2
- Domain should have at least two DCs because of redundancy and HA of service
- FSMO roles:
  - RID master
  - PDC emulator
  - Intrastructure master

7



Users
AD DS
Computers
Groups

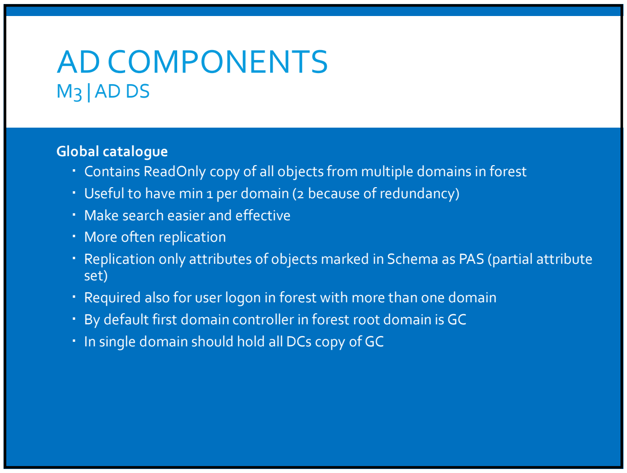
AD COMPONENTS

M3 | AD DS

Site

- Physical structure of domain, group objects based on location (building, city, department)
- Object site exist also in AD with IP and Mask
- Offer more effective replication and authentication
- When client needs to contact DC (looking for SRV records), response of DNS query includes:
  - List of DC in same site like client
  - List of DC from nearest site
  - Random list of DC in domain if no DC is found in nearest site
- When you define sites, you have to consider link reliability for ex. For main office and branch office should configure separate site if WAN link between is not reliable

8



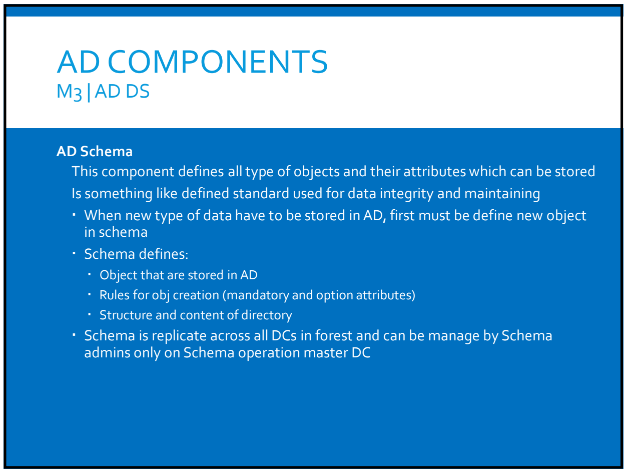
AD COMPONENTS

M3 | AD DS

Global catalogue

- Contains ReadOnly copy of all objects from multiple domains in forest
- Useful to have min 1 per domain (2 because of redundancy)
- Make search easier and effective
- More often replication
- Replication only attributes of objects marked in Schema as PAS (partial attribute set)
- Required also for user logon in forest with more than one domain
- By default first domain controller in forest root domain is GC
- In single domain should hold all DCs copy of GC

9



AD COMPONENTS

M3 | AD DS

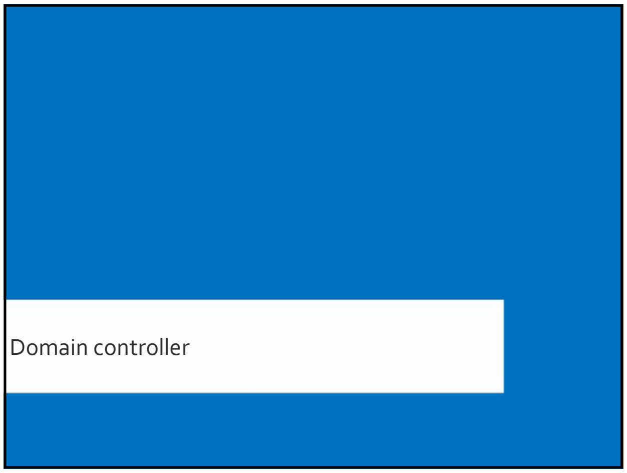
AD Schema

This component defines all type of objects and their attributes which can be stored

Is something like defined standard used for data integrity and maintaining

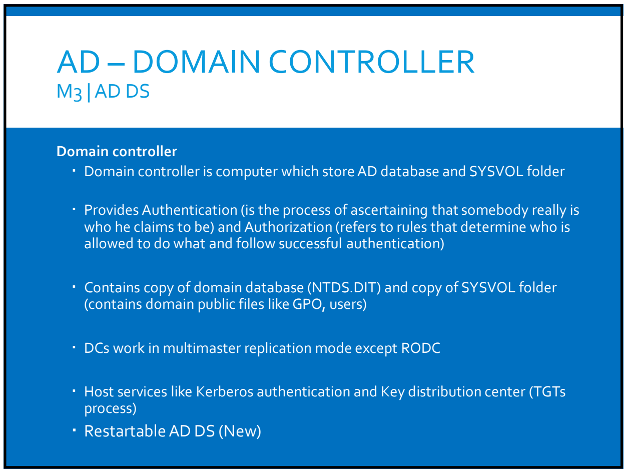
- When new type of data have to be stored in AD, first must be define new object in schema
- Schema defines:
  - Object that are stored in AD
  - Rules for obj creation (mandatory and option attributes)
  - Structure and content of directory
- Schema is replicate across all DCs in forest and can be manage by Schema admins only on Schema operation master DC

10



Domain controller

11



AD – DOMAIN CONTROLLER

M3 | AD DS

Domain controller

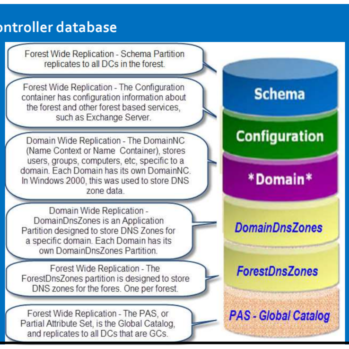
- Domain controller is computer which store AD database and SYSVOL folder
- Provides Authentication (is the process of ascertaining that somebody really is who he claims to be) and Authorization (refers to rules that determine who is allowed to do what and follow successful authentication)
- Contains copy of domain database (NTDS.DIT) and copy of SYSVOL folder (contains domain public files like GPO, users)
- DCs work in multimaster replication mode except RODC
- Host services like Kerberos authentication and Key distribution center (TGTs process)
- Restartable AD DS (New)

12

AD COMPONENTS

M3 | AD DS

Domain controller database



Forest Wide Replication - Schema Partition replicates to all DCs in the forest.

Forest Wide Replication - The Configuration container has configuration information about the forest and other forest based services, such as Exchange Server.

Domain Wide Replication - The DomainNC (Name Context or Name Container), stores users, groups, computers, etc, specific to a domain. Each Domain has its own DomainNC. In Windows 2000, this was used to store DNS zone data.

Domain Wide Replication - DomainDnsZones is an Application Partition designed to store DNS Zones for a specific domain. Each Domain has its own DomainDnsZones Partition.

Forest Wide Replication - The ForestDnsZones partition is designed to store DNS zones for the fores. One per forest.

Forest Wide Replication - The PAS, or Partial Attribute Set, is the Global Catalog, and replicates to all DCs that are GCs.

13

AD COMPONENTS

M3 | AD DS

Read only domain controller (RODC)

- More secure solution for branch office
- Contains Read-Only copy of AD objects but not all their attributes
- System critical attributes such pass are not replicated to RODC by default
- You also cannot change database on RODC
- Replication is one way only = from writable DC to RODC
- Do not cache any password by default (can be configure to cache pass via Pass replication policy)
- Lost of RODC cause lower impact from security view = only cached computer and user pass have to be reset
- Can be given admin privileges to manage RODC only (not other DCs)

14

DC ROLES

M3 | AD DS

Operation master roles

- **Schema master**
- **Domain naming master**

- **PDC emulator**
- **Intrastructure master**
- **RID mater**

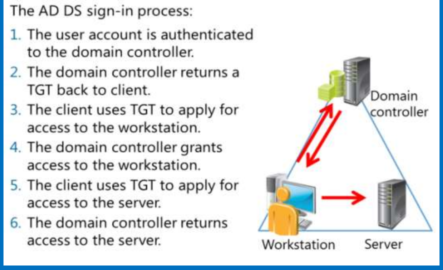
Global Catalogue roles

15

AD SSO PROCESS

M3 | AD DS

Sign-In Process



The AD DS sign-in process:

1. The user account is authenticated to the domain controller.
2. The domain controller returns a TGT back to client.
3. The client uses TGT to apply for access to the workstation.
4. The domain controller grants access to the workstation.
5. The client uses TGT to apply for access to the server.
6. The domain controller returns access to the server.

16

AD DC installation

17

DC INSTALLATION

M3 | AD DS

Pre-Requisites:

- Decision about Forest and domain level
- Physical or virtual system with Windows server 2016 installed
- Static IP configuration
- Administrator permission

Strong relation on following network services:

- DNS name space and DNS services

18

AD management of object(s)

19

AD OBJECTS

M3 | AD DS

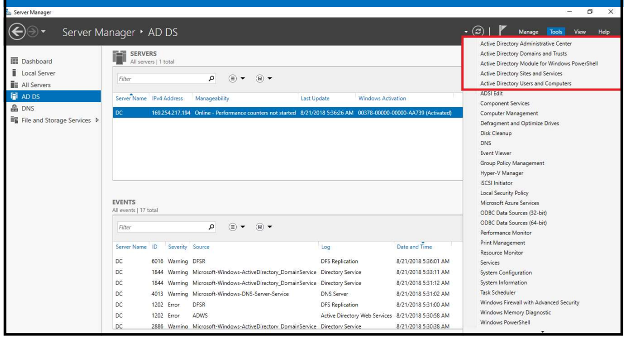
- Users
- Groups
- Computer
- Printers
- Containers
- OU
- Shared folders

Every object has GUID (128 bit identifier) and SID

20

AD OBJECTS – MGMT TOOLS

M3 | AD DS



SERVERS

All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC	169.254.217.194	Online - Performance counters not started	8/21/2018 5:36:26 AM	00378-00000-00000-AA739 (Activated)

EVENTS

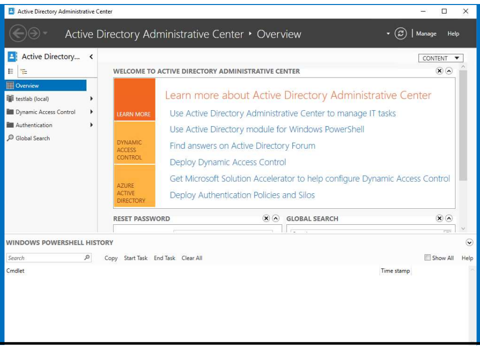
All events | 17 total

Server Name	ID	Severity	Source	Log	Date and Time
DC	6016	Warning	DFSR	DFS Replication	8/21/2018 5:36:01 AM
DC	1844	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	8/21/2018 5:33:11 AM
DC	1844	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	8/21/2018 5:31:12 AM
DC	4013	Warning	Microsoft-Windows-DNS-Server-Service	DNS Server	8/21/2018 5:31:02 AM
DC	1202	Error	DFSR	DFS Replication	8/21/2018 5:31:00 AM
DC	1202	Error	ADWS	Active Directory Web Services	8/21/2018 5:30:58 AM
DC	2886	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	8/21/2018 5:30:38 AM

21

AD OBJECTS – MGMT TOOLS

M3 | AD DS



WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER

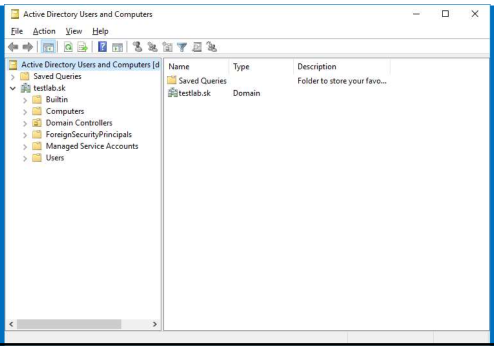
Learn more about Active Directory Administrative Center

- Use Active Directory Administrative Center to manage IT tasks
- Use Active Directory module for Windows PowerShell
- Find answers on Active Directory Forum
- Deploy Dynamic Access Control
- Get Microsoft Solution Accelerator to help configure Dynamic Access Control
- Deploy Authentication Policies and Silos

22

AD OBJECTS – MGMT TOOLS

M3 | AD DS

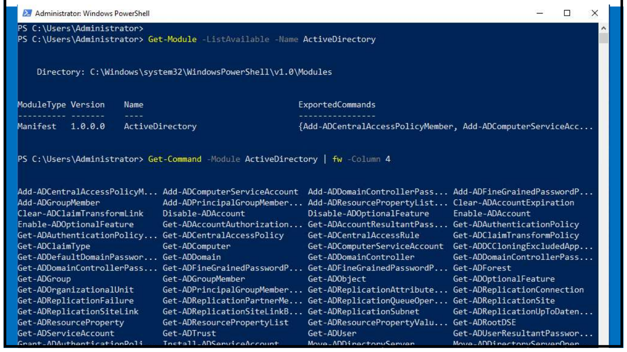


Name	Type	Description
Saved Queries		Folder to store your favo...
testlab.sk	Domain	

23

AD OBJECTS – MGMT TOOLS

M3 | AD DS



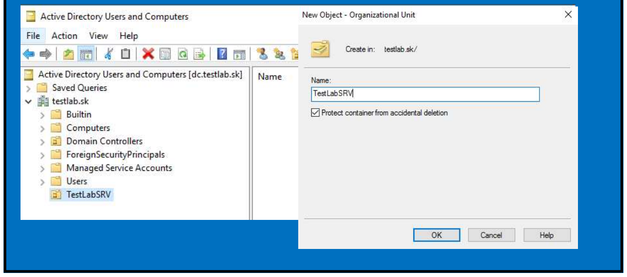
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-Module -ListAvailable -Name ActiveDirectory


    Directory: C:\Windows\system32\WindowsPowerShell\v1.0\Modules


ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Manifest   1.0.0.0    ActiveDirectory                     {Add-ADCentralAccessPolicyMember, Add-ADComputerServiceAcc...


PS C:\Users\Administrator> Get-Command -Module ActiveDirectory | fw -Column 4


Add-ADCentralAccessPolicyM... Add-ADComputerServiceAccount  Add-ADDomainControllerPass... Add-ADFineGrainedPasswordP...
Add-ADGroupMember             Add-ADPrincipalGroupMember... Add-ADResourcePropertyList... Clear-ADAccountExpiration
Clear-ADClaimTransformLink    Disable-ADAccount             Disable-ADOptionalFeature     Enable-ADAccount
Enable-ADOptionalFeature      Get-ADAccountAuthorization... Get-ADAccountResultantPass... Get-ADAuthenticationPolicy
Get-ADAuthenticationPolicy... Get-ADCentralAccessPolicy     Get-ADCentralAccessRule       Get-ADClaimTransformPolicy
Get-ADClaimType               Get-ADComputer                Get-ADComputerServiceAccount  Get-ADDCCloningExcludedApp...
Get-ADDefaultDomainPasswor... Get-ADDomain                  Get-ADDomainController        Get-ADDomainControllerPass...
Get-ADDomainControllerPass... Get-ADFineGrainedPasswordP... Get-ADFineGrainedPasswordP... Get-ADForest
Get-ADGroup                   Get-ADGroupMember             Get-ADObject                  Get-ADOptionalFeature
Get-ADOrganizationalUnit      Get-ADPrincipalGroupMember... Get-ADReplicationAttribute... Get-ADReplicationConnection
Get-ADReplicationFailure      Get-ADReplicationPartnerMe... Get-ADReplicationQueueOper... Get-ADReplicationSite
Get-ADReplicationSiteLink     Get-ADReplicationSiteLinkB... Get-ADReplicationSubnet       Get-ADReplicationUpToDaten...
Get-ADResourceProperty        Get-ADResourcePropertyList    Get-ADResourcePropertyValu... Get-ADRootDSE
Get-ADServiceAccount          Get-ADTrust                   Get-ADUser                    Get-ADUserResultantPasswor...
Grant-ADAuthenticationPoli... Install-ADServiceAccount      Move-ADDirectoryServer        Move-ADDirectoryServerOper...
```

24

AD OBJECTS – LOGICAL GROUPING

M3 | AD DS

- Containers
- Organizational Unit


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [dc.testlab.sk]
Saved Queries
testlab.sk
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
TestLabSRV
Name
New Object - Organizational Unit
OK
Cancel
Help

Create in: testlab.sk/

Name: TestLabSRV

☑ Protect container from accidental deletion

25

AD OBJECTS – COMPUTER

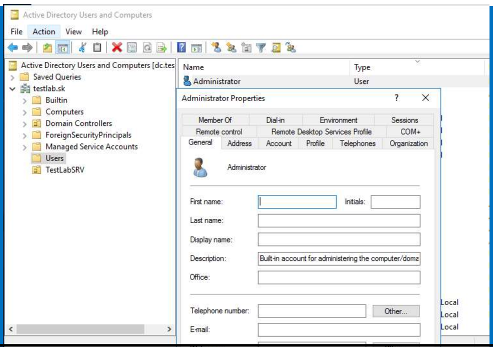
M3 | AD DS

- Containers
- Organizational Unit

26

AD OBJECTS – USERS

M3 | AD DS



Administrator User

Administrator

First name:

Initials:

Last name:

Display name:

Description: Built-in account for administering the computer/doma

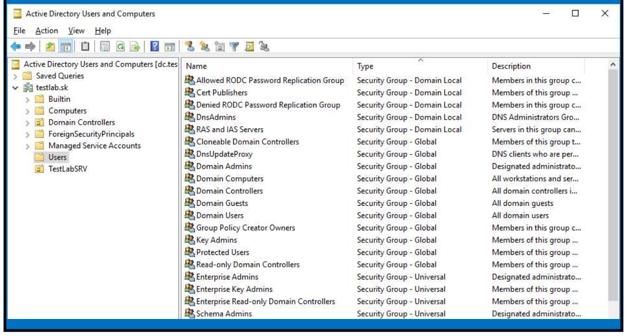
Office:

Telephone number:

E-mail:

27

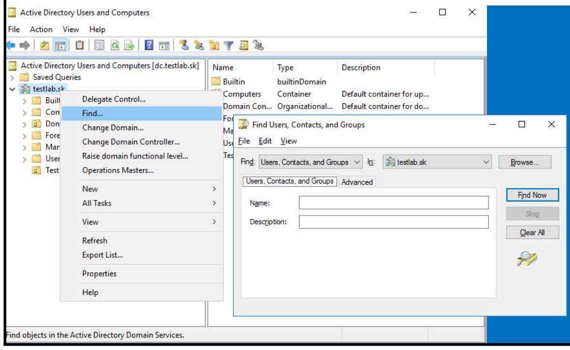
AD OBJECTS – GROUPS
M3 | AD DS



Name	Type	Description
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group c...
Cert Publishers	Security Group - Domain Local	Members of this group ...
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group c...
DnsAdmins	Security Group - Domain Local	DNS Administrators Gro...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Cloneable Domain Controllers	Security Group - Global	Members of this group t...
DnsUpdateProxy	Security Group - Global	DNS clients who are per...
Domain Admins	Security Group - Global	Designated administrato...
Domain Computers	Security Group - Global	All workstations and ser...
Domain Controllers	Security Group - Global	All domain controllers i...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Group Policy Creator Owners	Security Group - Global	Members in this group c...
Key Admins	Security Group - Global	Members of this group ...
Protected Users	Security Group - Global	Members of this group ...
Read-only Domain Controllers	Security Group - Global	Members of this group ...
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group ...
Schema Admins	Security Group - Universal	Designated administrato...

28

AD OBJECTS – SEARCHING
M3 | AD DS

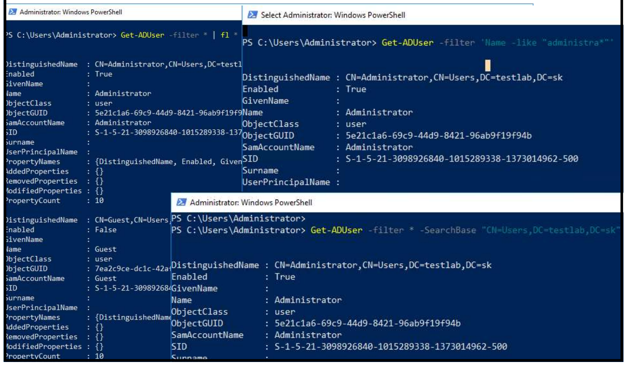


Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...

Find objects in the Active Directory Domain Services.

29

AD OBJECTS – POWERSHELL
M3 | AD DS


Administrator: Windows PowerShell
Select Administrator: Windows PowerShell
Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-ADUser -filter * | fl *

DistinguishedName  : CN=Administrator,CN=Users,DC=testl
Enabled            : True
GivenName          :
Name               : Administrator
ObjectClass        : user
ObjectGUID         : 5e21c1a6-69c9-44d9-8421-96ab9f19f9
SamAccountName     : Administrator
SID                : S-1-5-21-3098926840-1015289338-137
Surname            :
UserPrincipalName  :
PropertyNames      : {DistinguishedName, Enabled, Given
AddedProperties    : {}
RemovedProperties  : {}
ModifiedProperties : {}
PropertyCount      : 10

DistinguishedName  : CN=Guest,CN=Users,
Enabled            : False
GivenName          :
Name               : Guest
ObjectClass        : user
ObjectGUID         : 7ea2c9ce-dc1c-42a
SamAccountName     : Guest
SID                : S-1-5-21-30989268
Surname            :
UserPrincipalName  :
PropertyNames      : {DistinguishedName
AddedProperties    : {}
RemovedProperties  : {}
ModifiedProperties : {}
PropertyCount      : 10
```

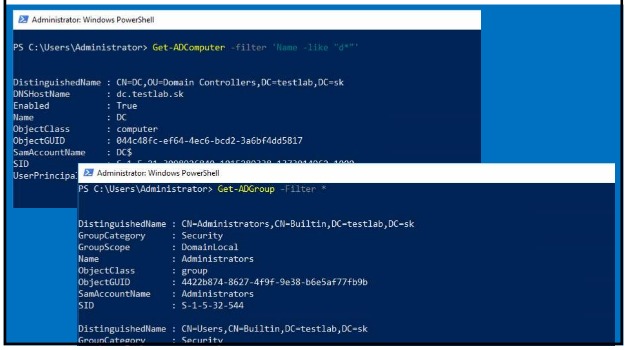
```
PS C:\Users\Administrator> Get-ADUser -filter 'Name -like "administra*"'


DistinguishedName : CN=Administrator,CN=Users,DC=testlab,DC=sk
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 5e21c1a6-69c9-44d9-8421-96ab9f19f94b
SamAccountName    : Administrator
SID               : S-1-5-21-3098926840-1015289338-1373014962-500
Surname           :
UserPrincipalName :
```

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -filter * -SearchBase "CN=Users,DC=testlab,DC=sk"


DistinguishedName : CN=Administrator,CN=Users,DC=testlab,DC=sk
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 5e21c1a6-69c9-44d9-8421-96ab9f19f94b
SamAccountName    : Administrator
SID               : S-1-5-21-3098926840-1015289338-1373014962-500
Surname           :
```

30

AD OBJECTS – POWERSHELL

M3 | AD DS



Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-ADComputer -filter 'Name -like "d*"'


DistinguishedName : CN=DC,OU=Domain Controllers,DC=testlab,DC=sk
DNSHostName       : dc.testlab.sk
Enabled           : True
Name              : DC
ObjectClass       : computer
ObjectGUID        : 044c48fc-ef64-4ec6-bcd2-3a6bf4dd5817
SamAccountName    : DC$
SID
UserPrincipa
```

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-ADGroup -Filter *


DistinguishedName : CN=Administrators,CN=Builtin,DC=testlab,DC=sk
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 4422b874-8627-4f9f-9e38-b6e5af77fb9b
SamAccountName    : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Users,CN=Builtin,DC=testlab,DC=sk
GroupCategory     : Security
```

31

Backup and restore

32

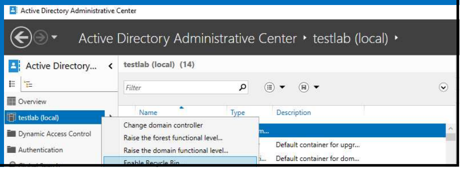
AD RESTORE

M3 | AD DS

Backup and restore AD

- System State backup is a backup of the AD DS
- System State backup captures the AD DS database and the SYSVOL, as well as all registry settings on the computer.

- **Non-authoritative Restore**
- **Authoritative Restore**

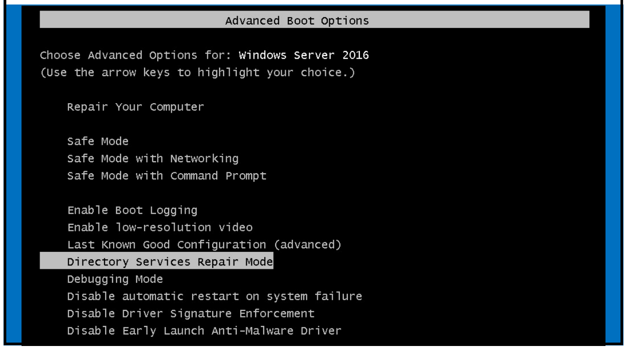


Active Directory Administrative Center
Active Directory Administrative Center ▸ testlab (local) ▸
Active Directory...
Overview
testlab (local)
Dynamic Access Control
Authentication
testlab (local) (14)
Filter
Name
Type
Description
Change domain controller
Raise the forest functional level...
Raise the domain functional level...
Enable Recycle Bin...
Default container for upgr...
Default container for dom...

33

AD RESTORE

M3 | AD DS



```
                         Advanced Boot Options

Choose Advanced Options for: Windows Server 2016
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video
    Last Known Good Configuration (advanced)
    Directory Services Repair Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement
    Disable Early Launch Anti-Malware Driver
```

34

GPO

35

GROUP POLICY PT1

M3 | AD DS

- Allow enforced settings by modify computer or user specific registry on domain based computer
- Can be applied on computer, user or both (it is set of settings)
- GPO is object containing modification of settings
- GPO templates are stored in SYSVOL
- For management is used GPMC

- (NEW) Preferences
  - Settings specify by Preferences can be change by user

36

GROUP POLICY PT2

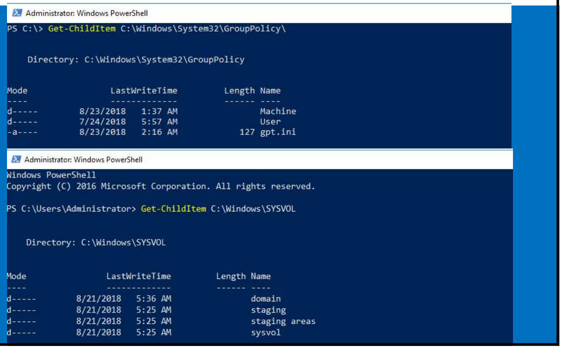
M3 | AD DS

- Used registry paths HKLM (computer settings) and HKCU (user settings)
- Not all policies can be applied to any version of windows OS and each new versions of OS bring new policies (older version of OS ignores new settings)
- All windows systems have local GPO which can be apply only on local computer
- Group policy storage: %SystemRoot%\SYSVOL\Domain\Policies\GPOGUID on DC

37

GROUP POLICY LOCATION

M3 | AD DS



Administrator: Windows PowerShell

```
PS C:\> Get-ChildItem C:\Windows\System32\GroupPolicy\


    Directory: C:\Windows\System32\GroupPolicy


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        8/23/2018   1:37 AM                Machine
d-----        7/24/2018   5:57 AM                User
-a----        8/23/2018   2:16 AM            127 gpt.ini
```

Administrator: Windows PowerShell

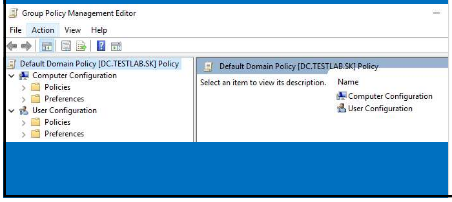
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ChildItem C:\Windows\SYSVOL


    Directory: C:\Windows\SYSVOL


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        8/21/2018   5:36 AM                domain
d-----        8/21/2018   5:25 AM                staging
d-----        8/21/2018   5:25 AM                staging areas
d-----        8/21/2018   5:25 AM                sysvol
```

38

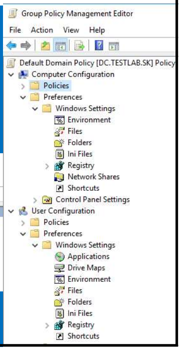
PREFERENCES

M3 | AD DS

- Domain based feature
- Very similar to group policy except:
  - Allowing change configuration by user
  - Refresh interval is same like for group policy
    - If configuration was change by user, refresh interval will have no impact



Select an item to view its description.

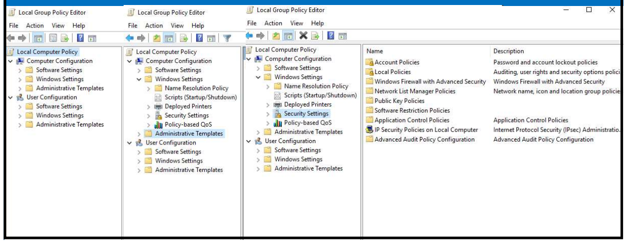


39

LOCAL GROUP POLICY

M3 | AD DS

- Gpedit.msc
- Used to configure clients which are not member of domain
- User and Computer parts available

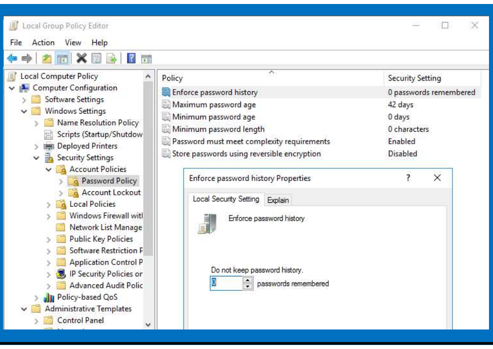


Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policie
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

40

EXAMPLE OF PASSWORD POLICY

M3 | AD DS



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Enforce password history Properties

Local Security Setting | Explain

Enforce password history

Do not keep password history.

0 passwords remembered

41

GROUP POLICY

M3 | AD DS

GPO processing order:

1. Local GPO
2. Site GPO
3. Domain GPO
4. OU GPO
5. Child OU GPO

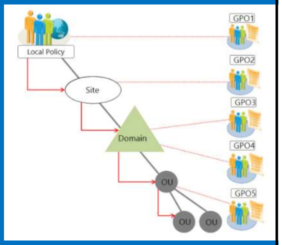
Enforced policy

Block inheritance

Security filtering

WMI filtering

Loopback processing



42

GROUP POLICY

M3 | AD DS

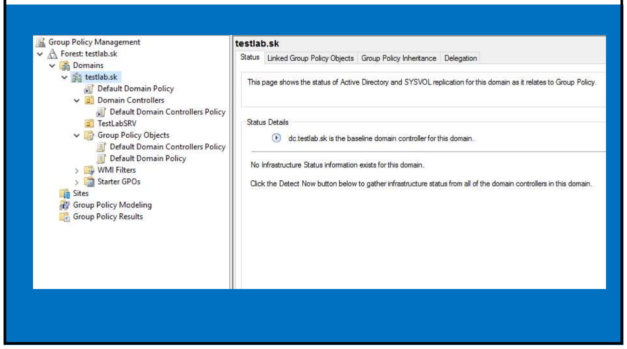
What can be manage by GPO

- Remote Group Policy update
  - **Invoke-GPUpdate**
  - **Get-GPPermissions**
  - **Set-GPPermissions**
- Group Policy infrastructure status
- Fast Startup
- New Group Policy starter GPOs
- Policy caching

43

GROUP POLICY MMC

M3 | AD DS



testlab.sk

This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

Status Details

dc.testlab.sk is the baseline domain controller for this domain.

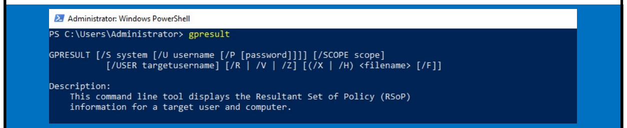
No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

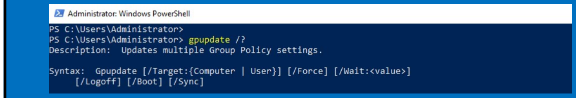
44

GROUP POLICY CMD

M3 | AD DS



```
PS C:\Users\Administrator> gpresult

GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope]
           [/USER targetusername] [/R | /V | /Z] [(/X | /H) <filename> [/F]]

Description:
    This command line tool displays the Resultant Set of Policy (RSoP)
    information for a target user and computer.
```

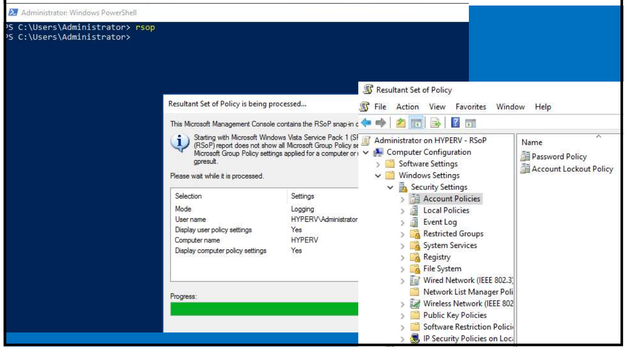


```
PS C:\Users\Administrator>
PS C:\Users\Administrator> gpupdate /?
Description:  Updates multiple Group Policy settings.

Syntax:  Gpupdate [/Target:{Computer | User}] [/Force] [/Wait:<value>]
     [/Logoff] [/Boot] [/Sync]
```

45

GROUP POLICY CMD

M3 | AD DS



Administrator: Windows PowerShell

```
PS C:\Users\Administrator> rsop
PS C:\Users\Administrator>
```

Resultant Set of Policy is being processed...

This Microsoft Management Console contains the RSoP snap-in c

Starting with Microsoft Windows Vista Service Pack 1 (SP (RSoP) report does not show all Microsoft Group Policy se Microsoft Group Policy settings applied for a computer or u gpresult.

Please wait while it is processed.

Selection	Settings
Mode	Logging
User name	HYPERV\Administrator
Display user policy settings	Yes
Computer name	HYPERV
Display computer policy settings	Yes

Progress:

Resultant Set of Policy

File Action View Favorites Window Help

- Administrator on HYPERV - RSoP
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3)
        - Network List Manager Poli
        - Wireless Network (IEEE 802
        - Public Key Policies
        - Software Restriction Polici
        - IP Security Policies on Loc

Name

- Password Policy
- Account Lockout Policy

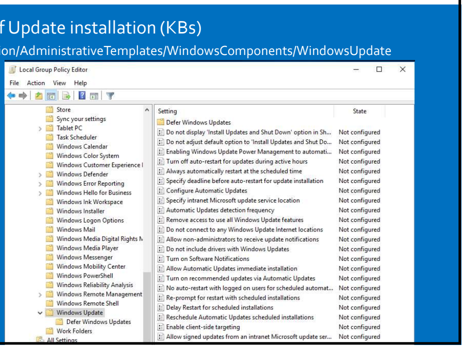
46

GROUP POLICY- REAL EXAMPLE

M3 | AD DS

Management of Update installation (KBs)

ComputerConfiguration/AdministrativeTemplates/WindowsComponents/WindowsUpdate



Local Group Policy Editor

File Action View Help

- Store
- Sync your settings
- Tablet PC
- Task Scheduler
- Windows Calendar
- Windows Color System
- Windows Customer Experience I
- Windows Defender
- Windows Error Reporting
- Windows Hello for Business
- Windows Ink Workspace
- Windows Installer
- Windows Logon Options
- Windows Mail
- Windows Media Digital Rights M
- Windows Media Player
- Windows Messenger
- Windows Mobility Center
- Windows PowerShell
- Windows Reliability Analysis
- Windows Remote Management
- Windows Remote Shell
- Windows Update
  - Defer Windows Updates
- Work Folders
- All Settings

Setting	State
Defer Windows Updates	
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured
Do not adjust default option to 'Install Updates and Shut Do...	Not configured
Enabling Windows Update Power Management to automati...	Not configured
Turn off auto-restart for updates during active hours	Not configured
Always automatically restart at the scheduled time	Not configured
Specify deadline before auto-restart for update installation	Not configured
Configure Automatic Updates	Not configured
Specify intranet Microsoft update service location	Not configured
Automatic Updates detection frequency	Not configured
Remove access to use all Windows Update features	Not configured
Do not connect to any Windows Update Internet locations	Not configured
Allow non-administrators to receive update notifications	Not configured
Do not include drivers with Windows Updates	Not configured
Turn on Software Notifications	Not configured
Allow Automatic Updates immediate installation	Not configured
Turn on recommended updates via Automatic Updates	Not configured
No auto-restart with logged on users for scheduled automat...	Not configured
Re-prompt for restart with scheduled installations	Not configured
Delay Restart for scheduled installations	Not configured
Reschedule Automatic Updates scheduled installations	Not configured
Enable client-side targeting	Not configured
Allow signed updates from an intranet Microsoft update ser...	Not configured

47

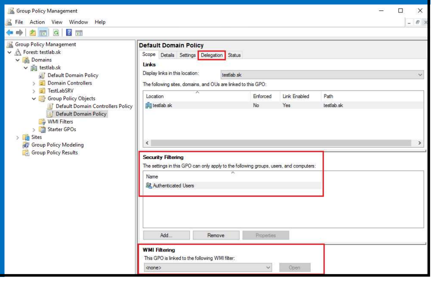
GROUP POLICY- FILTERING

M3 | AD DS

Security filtering

WMI filtering

Delegation



Group Policy Management

File Action View Window Help

- Group Policy Management
  - Forest: testlab.sk
    - Domains
      - testlab.sk
        - Default Domain Policy
        - Domain Controllers
        - TestLabSRV
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy
        - WMI Filters
        - Starter GPOs
    - Sites
  - Group Policy Modeling
  - Group Policy Results

Default Domain Policy

Scope Details Settings Delegation Status

Links

Display links in this location: testlab.sk

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
testlab.sk	No	Yes	testlab.sk

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

Add... Remove Properties

WMI Filtering

This GPO is linked to the following WMI filter:

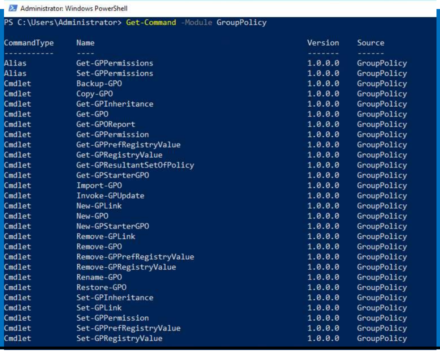
<none>

Open

48

GROUP POLICY- FILTERING

M3 | AD DS



Administrator: Windows PowerShell

```
PS C:\Users\Administrator> Get-Command -Module GroupPolicy

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           Get-GPPermissions                                  1.0.0.0    GroupPolicy
Alias           Set-GPPermissions                                  1.0.0.0    GroupPolicy
Cmdlet          Backup-GPO                                         1.0.0.0    GroupPolicy
Cmdlet          Copy-GPO                                           1.0.0.0    GroupPolicy
Cmdlet          Get-GPInheritance                                  1.0.0.0    GroupPolicy
Cmdlet          Get-GPO                                            1.0.0.0    GroupPolicy
Cmdlet          Get-GPOReport                                      1.0.0.0    GroupPolicy
Cmdlet          Get-GPPermission                                   1.0.0.0    GroupPolicy
Cmdlet          Get-GPPrefRegistryValue                            1.0.0.0    GroupPolicy
Cmdlet          Get-GPRegistryValue                                1.0.0.0    GroupPolicy
Cmdlet          Get-GPResultantSetOfPolicy                         1.0.0.0    GroupPolicy
Cmdlet          Get-GPStarterGPO                                   1.0.0.0    GroupPolicy
Cmdlet          Import-GPO                                         1.0.0.0    GroupPolicy
Cmdlet          Invoke-GPUpdate                                    1.0.0.0    GroupPolicy
Cmdlet          New-GPLink                                         1.0.0.0    GroupPolicy
Cmdlet          New-GPO                                            1.0.0.0    GroupPolicy
Cmdlet          New-GPStarterGPO                                   1.0.0.0    GroupPolicy
Cmdlet          Remove-GPLink                                      1.0.0.0    GroupPolicy
Cmdlet          Remove-GPO                                         1.0.0.0    GroupPolicy
Cmdlet          Remove-GPPrefRegistryValue                         1.0.0.0    GroupPolicy
Cmdlet          Remove-GPRegistryValue                             1.0.0.0    GroupPolicy
Cmdlet          Rename-GPO                                         1.0.0.0    GroupPolicy
Cmdlet          Restore-GPO                                        1.0.0.0    GroupPolicy
Cmdlet          Set-GPInheritance                                  1.0.0.0    GroupPolicy
Cmdlet          Set-GPLink                                         1.0.0.0    GroupPolicy
Cmdlet          Set-GPPermission                                   1.0.0.0    GroupPolicy
Cmdlet          Set-GPPrefRegistryValue                            1.0.0.0    GroupPolicy
Cmdlet          Set-GPRegistryValue                                1.0.0.0    GroupPolicy
```

49