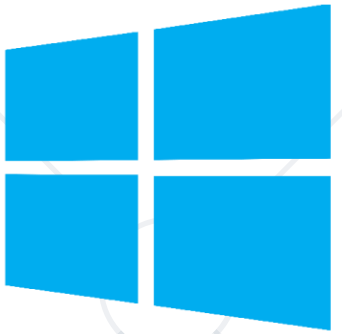


Additional Techniques in AD

Group Policies, Objects, and Preferences



Windows Server

SoftUni Team
Technical Trainers



SoftUni



Software University

<https://softuni.bg>

Have a Question?

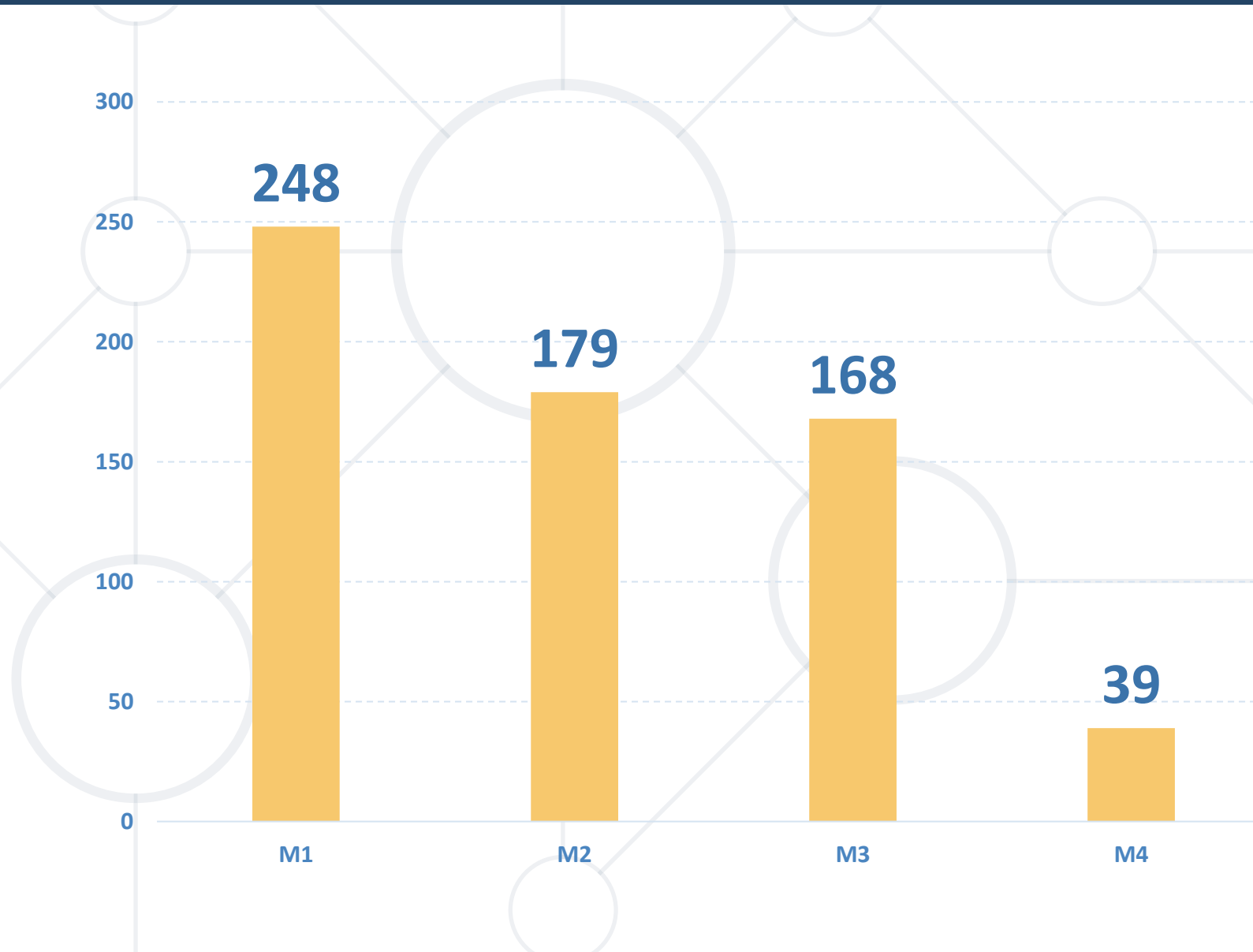
sli.do

#WSA

facebook.com/groups/

WindowsSystemAdministrationMarch2023/

Homework Progress



Submit M4
until 23:59:59
on 28.04.2023

Submit M4
until 23:59:59
on 05.05.2023



Previous Module (M4)

Quick overview

What We Covered

- File and Storage Services
- Remote Access and Management
- Print and Document Services



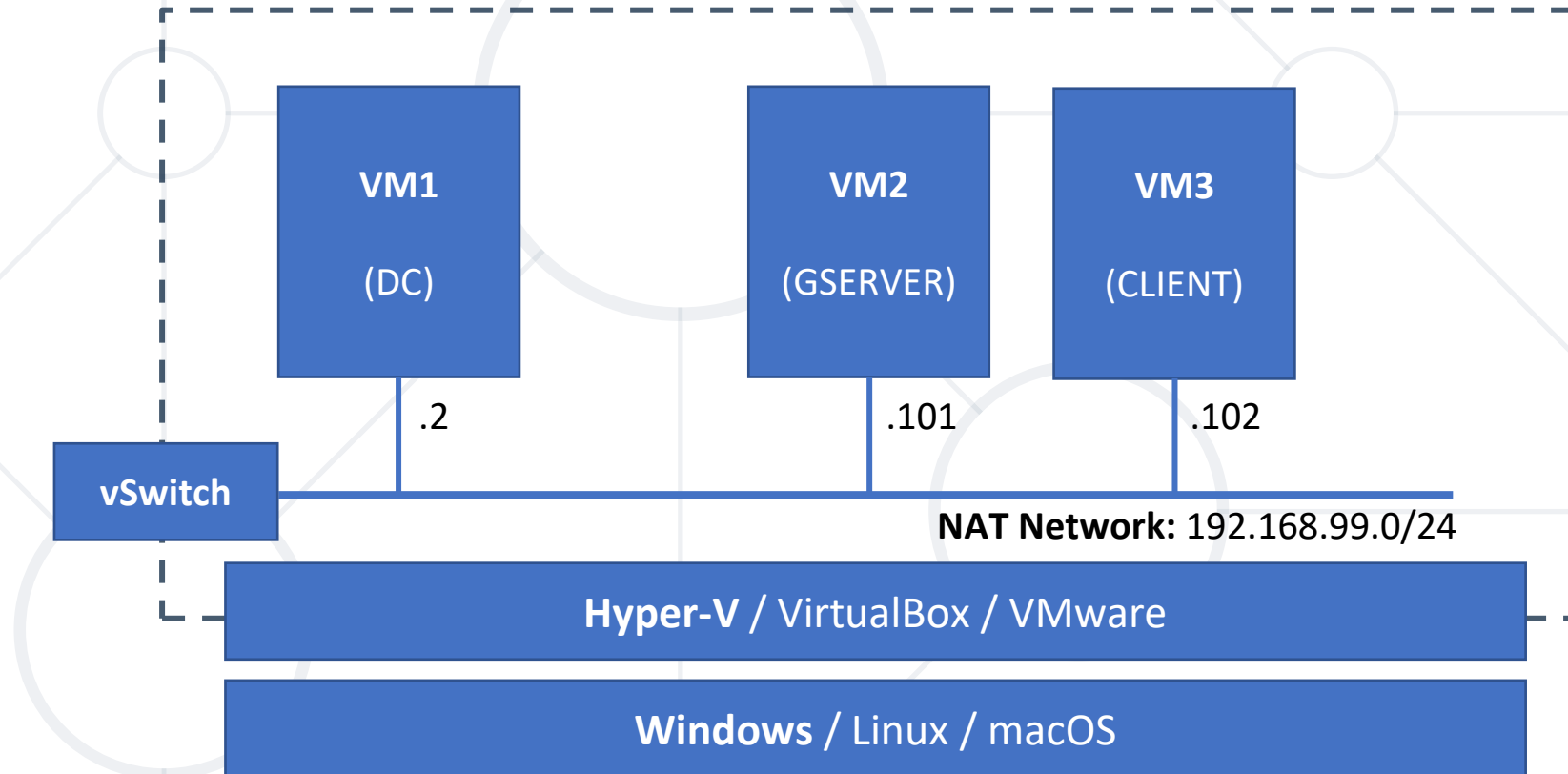
This Module (M5)

Topics

Table of Contents

1. Additional Features and Techniques
2. Group Policy Objects
3. Group Policy Preferences







Active Directory Next Steps

Additional Features and Tasks

- ADAC is newer than ADUC
- It is the tool recommended by Microsoft
- Both are rich in functions but aren't completely interchangeable
- Offers easy password reset and user search
- PowerShell based
 - Allows "reverse engineering"
 - Allows recipes creation

- Single Domain – Single Forest
- **Microsoft Recommended Approach**
 - Users go to Global Groups
 - Global Groups go to Domain Local Groups
 - Permissions are assigned to Domain Local Groups
- **Usual Situation**
 - Global Groups are treated as equivalent to Domain Local Groups
 - Global Groups are used for user categorization and permissions

- **Allowed Conversions**

- Domain Local Group, Global Group => Universal Group
- Universal Group => Domain Local Group, Global Group

- **Not Allowed Conversions**

- Domain Local Group ⇔ Global Group

- Can be done in **ADUC** or **ADAC**


- Can be done in PowerShell

```
PS C:\> Get-ADGroup "Help Desk" | Set-ADGroup -GroupScope Universal
```

- **Local System** (NT AUTHORITY\SYSTEM)
 - Privileges equal to a local user account member of the **local Administrators group**. A service under this account **accesses network resources using the computer's account credentials**. Additionally, it has **administrator level access** on the local machine.
- **Local Service** (NT AUTHORITY\LocalService)
 - Privileges equal to a local user account member of the **local Users group**. A service under this account **accesses network resources using null session** (without credentials). It should be used when no network access is required.
- **Network Service** (NT AUTHORITY\NetworkService)
 - Privileges equal to a local user account member of **the local Users group**. A service under this account **accesses network resources using the computer's account credentials**.

Service Accounts (AD Accounts)

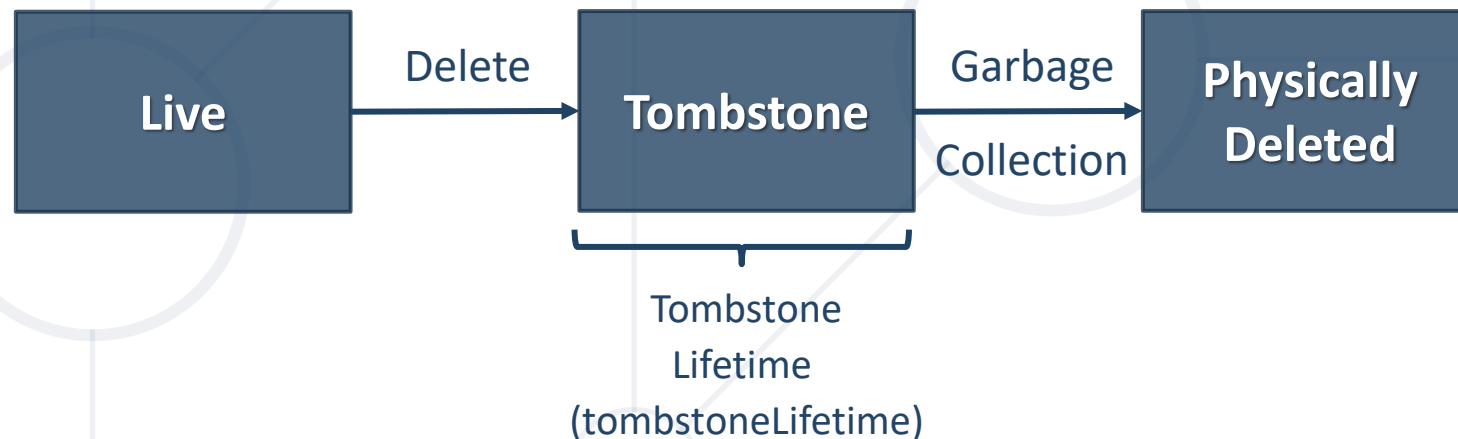
- Dedicated AD User Accounts
 - Issues with password and SPN management
- Managed Service Accounts (MSA)
 - Restricted to single computer
- Group Managed Service Accounts (gMSA)
 - Clients \geq Windows 8, DC \geq Windows Server 2012



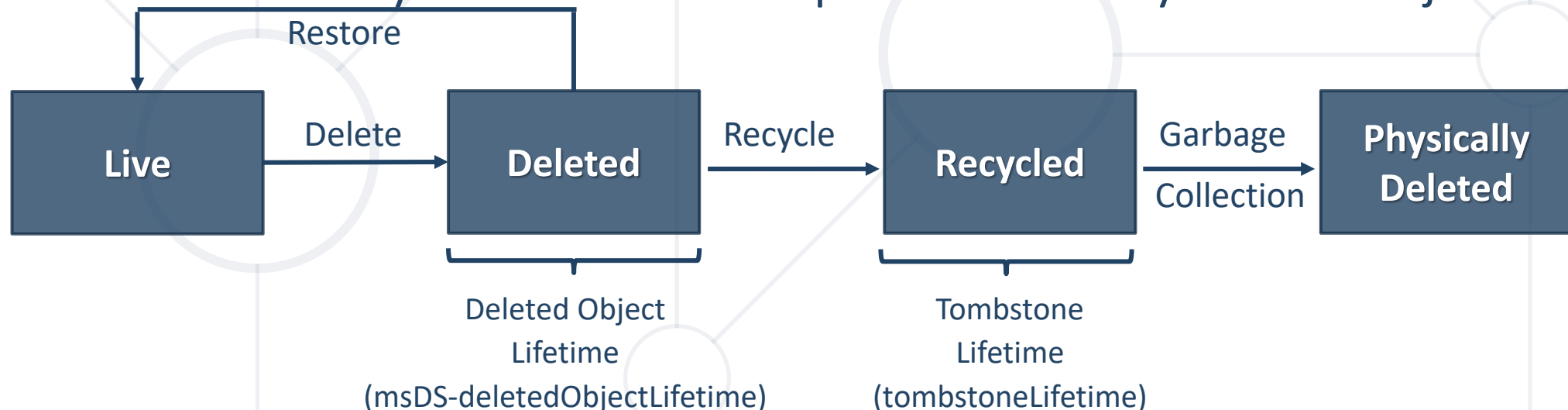
Automatic password management
Simplified SPN management

- Graphically
 - Provided by Microsoft (**ADUC**)
 - 3rd party tools
- On the command line
 - CMD Shell – LDIF Directory Exchange (**ldifde**)
 - CMD Shell – CSV Directory Exchange (**csvde**)
 - PowerShell – **Get-ADUser** + **Select-Object** + **Export-CSV**

- When an object is deleted, it becomes a tombstone
- Most of its attributes are striped off
- It stays in the partition's Deleted Objects container for the duration of the domain's **tombstoneLifetime** (if not set defaults to **60 days**)
- During the tombstone period the object is technically recoverable



- Introduced in the Windows Server 2008 R2 release
- It can be enabled via the ADAC or with PowerShell (**Enable-ADOptionalFeature**)
- Once enabled cannot be disabled because it changes the schema
- The majority of a deleted object's attributes are preserved for a period of time (if not set, equals to **tombstoneLifetime**)
- Increases the directory size and does not preserve already deleted objects



■ Default containers redirection

:: Redirect Users Container

```
C:\> redirusr "ou=Managed Users,dc=SULAB,dc=LOCAL"
```

:: Redirect Computers Container

```
C:\> redircmp "ou=Managed Computers,dc=SULAB,dc=LOCAL"
```

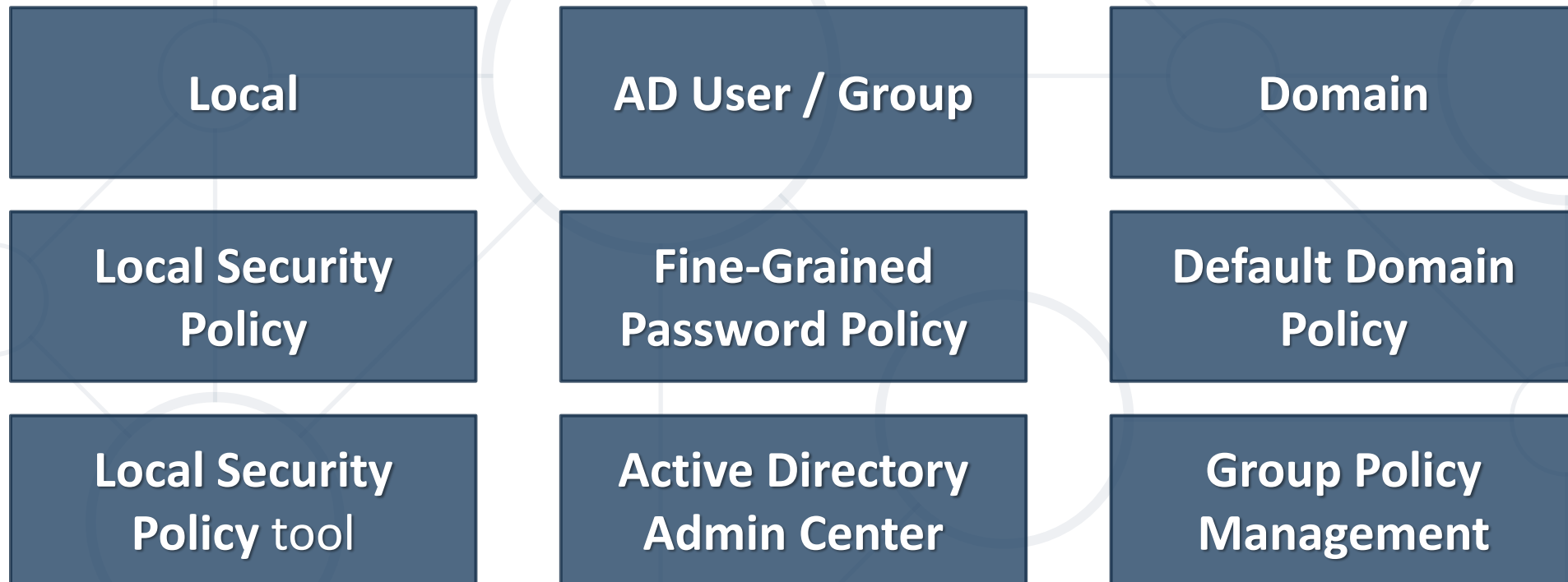
■ Check current state

Get domain attributes

```
PS C:\> Get-ADDomain
```

Get information about the default containers

```
PS C:\> Get-ADDomain | Select UsersContainer, ComputersContainer | FL
```





Practice: ADAC and More
Live Demonstration in Class



Group Policies 101

Control Your Environment

- **Group Policy** is a feature of the **Microsoft Windows NT** family of operating systems that **controls the working environment of user accounts and computer accounts**
- Group Policy provides **centralized management and configuration** of operating systems, applications, and users' settings in an Active Directory environment
- A set of Group Policy configurations is called a **Group Policy Object (GPO)**. A version of Group Policy called **Local Group Policy (LGPO** or **LocalGPO)** allows Group Policy Object management without Active Directory on standalone computers

- What is it?
 - Group of rules used to manage computers and users
- How is it created and operated?
 - Decide what and how will be configured
 - Create a named GPO
 - (Scoping) Link it to a **site, domain, or organizational unit**

Group Policy Objects (2)

- Can be used to manage
 - Windows and Application Settings
 - Software Deployment
 - Folder Redirection
 - Security Settings
 - Infrastructure Settings
- Two types – Local and Domain-based

- Used to apply settings to computer and its local users
- They are overridden by domain GPOs
- Multiple Local GPOs
 - Local Group Policy (applied to the computer)
 - Administrators Local Group Policy
 - Non-Administrators Local Group Policy
 - User-specific Local Group Policy

- Processing order
 - Local Group Policy
 - Administrators and Non-Administrators Local Group Policy
 - User-specific Local Group Policy
- Managed with **mmc.exe** (Microsoft Management Console)
 - Add snap-in Group Policy Object Editor
 - Specify Scope
- Not applicable to Security Groups

- Applicable to computer and user objects, part of AD domain
- Structure
 - Group Policy Container
 - Stored in the AD DS database
 - Defines fundamental attributes of the GPO
 - Group Policy Template
 - Collection of files and folders stored in the SYSVOL folder on all DCs
 - Contains the actual GPO settings

- Group Policy Management
 - Used for creation, linking, filtering, modeling and troubleshooting
- Group Policy Management Editor
 - Launched from within Group Policy Management
 - Used to view and configure available settings in the GPO
- PowerShell
 - **GroupPolicy** module
 - New-GPO, Get-GPO, Remove-GPO, Rename-GPO, ...

- Top-level
 - Computer Configuration (applied during startup and thereafter)
 - User Configuration (applied when user signs in and thereafter)
- Refreshed **every 90 to 120 minutes** [90 + RAND(30)]
- Applied policy settings need time to become effective
- Process can be forced
- **Good Practice is to separate GPOs for Computers and Users**

- **Software Settings**
 - Deploy, update, and remove software
- **Windows Settings**
 - Basic settings (Scripts, Security Settings, Folder Redirection)
- **Administrative Templates**
 - Registry settings that control user, computer, and applications

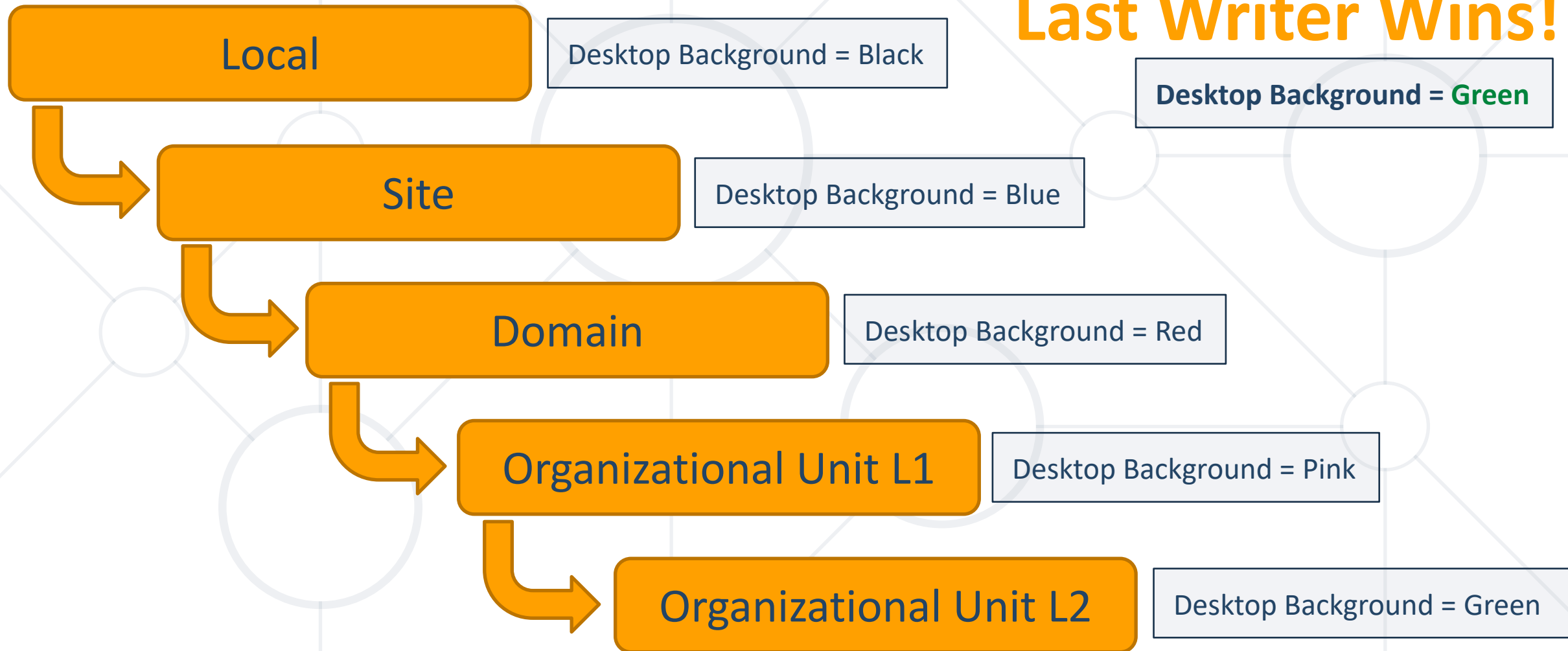
- **Domain Controllers**

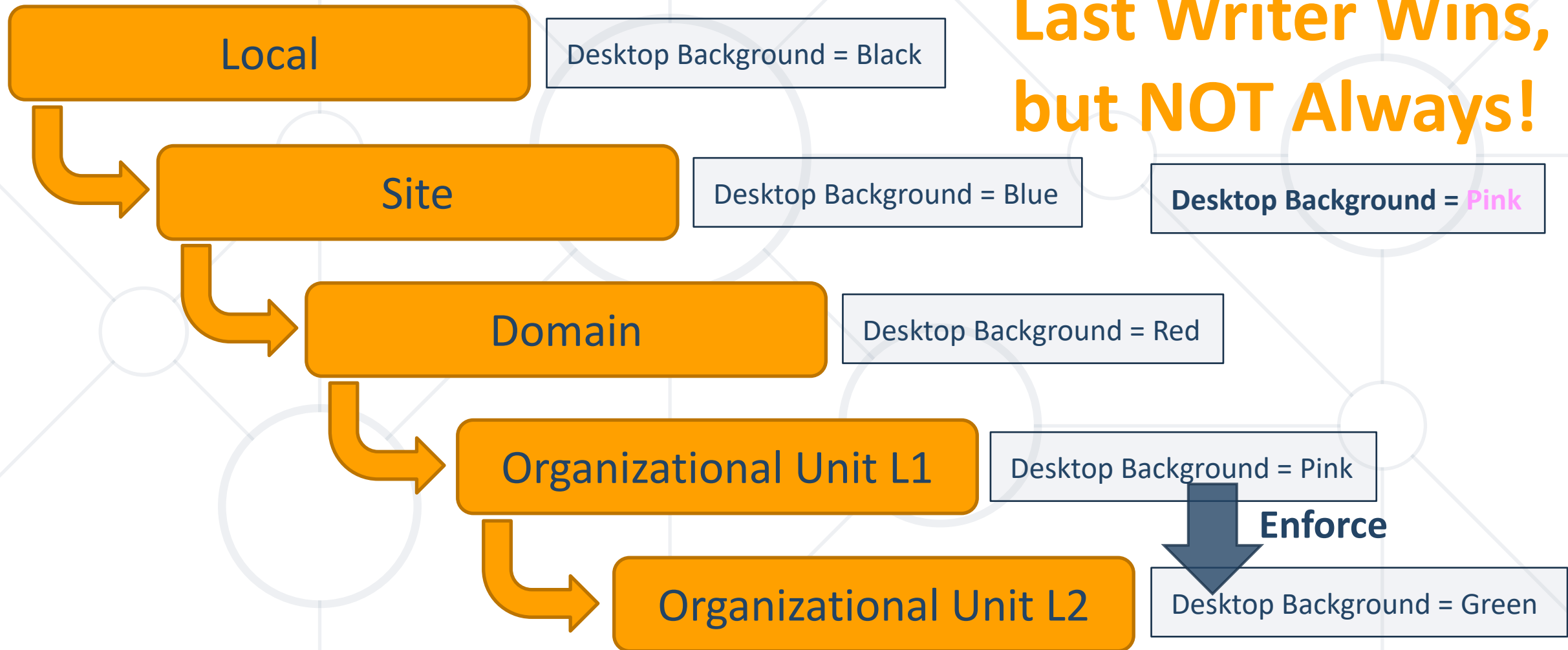
- Store and make available various GPOs

- **Client Computers**

- Responsible to connect, request, and apply GPOs
- Group Policy Client connects and downloads the required GPOs
- Local components (client-side extensions) process the GPO
- Registry policy, Scripts policy, Security policy, etc.

- Processing order and precedence
 - More than one GPO per OU are processed in order
 - GPOs with **lowest link order take precedence** (processed last)
- Inheritance
 - Child OUs inherit GPOs from parent (lowest precedence)
 - Inheritance could be **blocked** if desired
 - GPOs can be **enforced** to avoid blocking (highest precedence)
- Blocking and Enforcing should be minimized, **use filters instead**





■ Software Distribution

- Should be placed in a **shared folder**
- Only **MSI** files are supported
- **Assigned** software is automatically installed, while the **Published** software installation is initiated by the user
- Can be set on **Computer** (Assigned) or **User** (Assigned or Published) level
- **Upgrading, redeploying, and removal** actions are also available

■ Scripts Execution

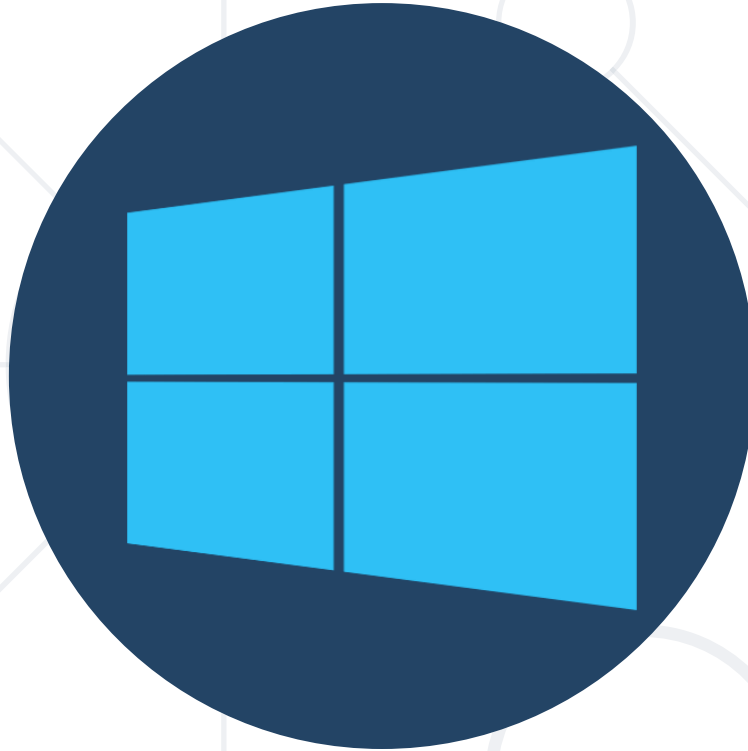
- Should be placed in a **shared folder**
- Can be set on **Computer** (**Startup/Shutdown**) or **User** (**Logon/Logoff**) level
- **PowerShell, VBScript, and other** are supported

- **Security Filtering**
 - By default, applies to **Authenticated Users**
 - Implement **Applies To Everyone But**
 - Implement **Applies To Only**
- **WMI Filtering**
 - Based on WMI Query
 - Example: **SELECT * FROM Win32_BIOS**



Practice: Group Policy Objects 101

Live Demonstration in Class



Group Policies 102

GPO Additional Tasks. Group Policy Preferences

- Starter GPO
 - We can install and use 3rd party starter GPOs or create our own
- Administrative Template Files
 - Stored on the DC in **.ADMX** and **.ADML**
- Central Store
 - **C:\Windows\SYSVOL\sysvol\wsa.lab\Policies**
- Manage GPOs
 - Backup and restore; export and import; duplication (copy)
- Migration Table
 - Transfer GPOs (users, groups, computers, paths) between domains

Force, Report, and Reset GPOs

- Force GPO Update

- CMD Shell

```
C:\> gpupdate /force
```

- PowerShell

```
PS C:\> Invoke-GPUUpdate -Force
```

- Report resulting GPO settings

```
C:\> gpresult /r
```

- Reset Default GPOs

```
C:\> dcgpofix
```


Group Policy Objects (GPO)

- Settings are strictly enforced
- Automatically refreshed on a periodic basis
- Disable its associated user interface item
- Don't change the original settings

Group Policy Preferences (GPP)

- Not strictly enforced
 - Can be automatically refreshed, but can also be applied only once
 - Preference folder is not available in the Local Group Policy
- Change the original setting in the registry



- **Create**
 - IF non-existing THEN create it
- **Replace**
 - IF non-existing THEN create it ELSE delete and create it
- **Delete**
 - IF existing THEN remove it
- **Update**
 - IF non-existing THEN create it ELSE modify it

- Coverage
 - Environment Variables
 - Network Drives
 - Files and Folders
 - Power Options
 - Registry Settings
 - Shortcuts, etc.
- Item-level Targeting (Targeting Editor)



Practice: Group Policy Objects 102

Live Demonstration in Class

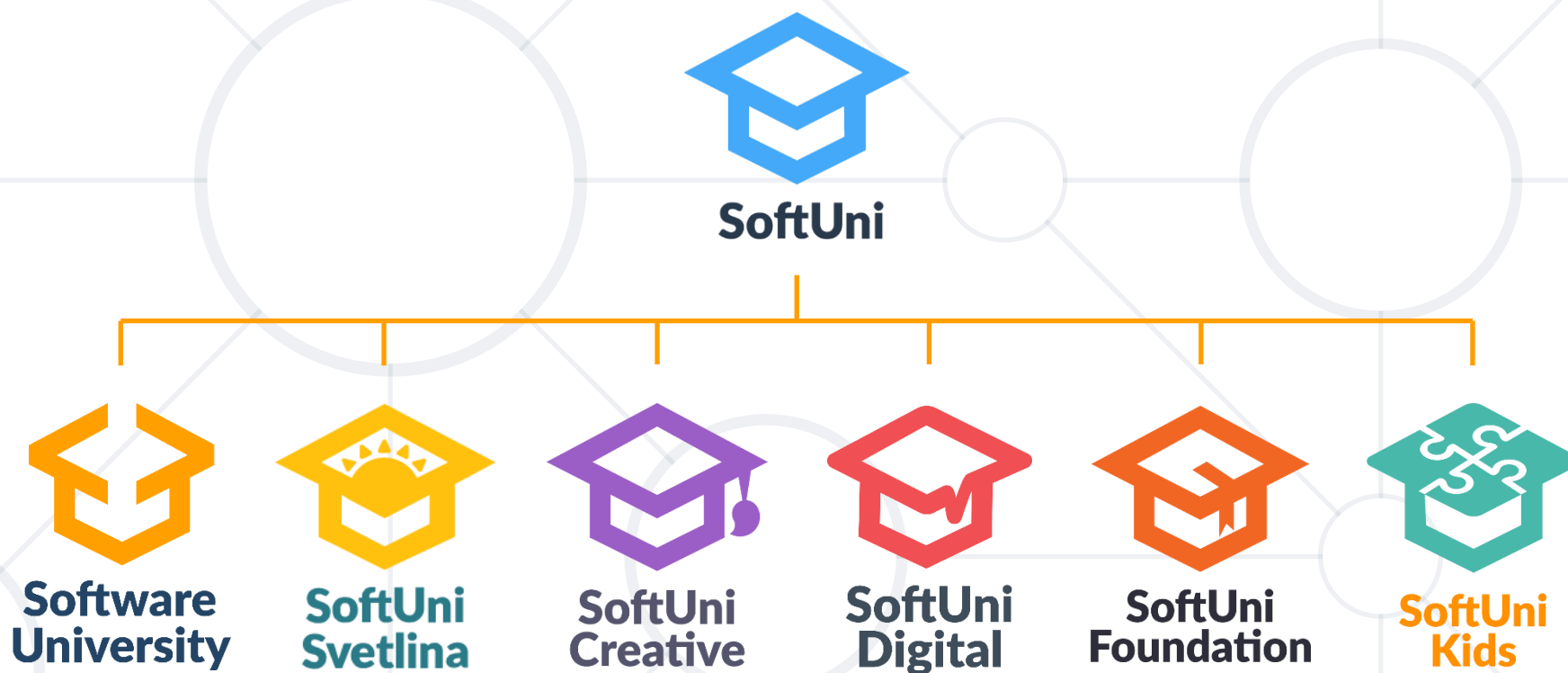
- There are rules for group conversion
- GPOs are used to centrally configure and manage
- GPOs can be linked to sites, domains, and OUs
- GPOs can be filtered with security or WMI filters
- GPOs can be blocked or enforced
- Preferences may apply drive mappings, desktop shortcuts, ...
- Preferences are applied in different way than policy settings



- GroupPolicy Module
<https://docs.microsoft.com/en-us/powershell/module/grouppolicy>
- Microsoft.PowerShell.Management Module
<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management>
- Group Policy Administrative Templates Catalog
<https://getadmx.com/>
- Configuring Group Policies using Windows PowerShell
<https://sid-500.com/2017/08/25/configuring-group-policies-by-using-windows-powershell>



Questions?



SoftUni Diamond Partners

SCHWARZ



Coca-Cola HBC
Bulgaria



Postbank

Решения за твоето утре



POKERSTARS



CAREERS



AMBITIONED

DXC
TECHNOLOGY



**SOFTWARE
GROUP**

Bosch.IO

INDEAVR
Serving the high achievers

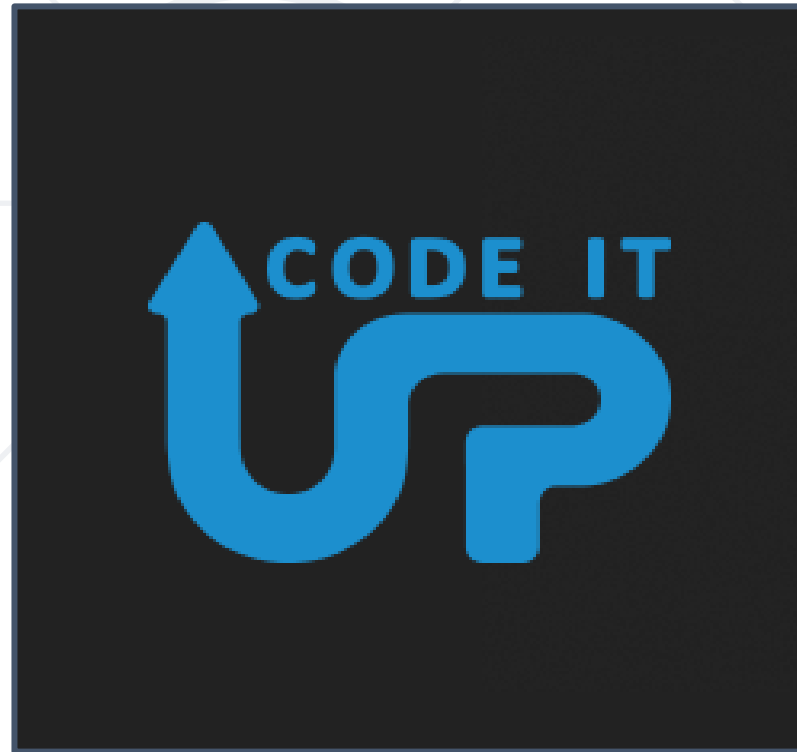
 **DRAFT
KINGS**



SmartIT

createX

**SUPER
HOSTING
.BG**



- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – <https://softuni.org>
- © Software University – <https://softuni.bg>



- Software University – High-Quality Education, Profession and Job for Software Developers

- softuni.bg, softuni.org

- Software University Foundation

- softuni.foundation

- Software University @ Facebook

- facebook.com/SoftwareUniversity

- Software University Forums

- forum.softuni.bg

