

0

Group Policy

Przegląd zasad grupy

 Zasady grupy udostępniają możliwości zarządzania ustawieniami konfiguracji dotyczącymi komputerów i użytkowników w środowisku usług Active Directory.

Funkcje konfiguracji zasad grupy

- Zarządzanie i instalacja oprogramowania.
- Skrypty.
- Ustawienia zabezpieczeń.
- Przekierowanie folderów.
- QoS.
- Ustawienia programu Internet Explorer.
- Szablony administracyjne.
- Preferencje.
- Drukarki.
- Blokowanie instalacji urządzeń.
- Ustawienia zarządzania zasilaniem.

Działanie zasad grupy

- Ustawienia zasad są konfigurowane jako obiekt zasad grupy (Group Policy Object – GPO).
- GPO zostają powiązane na różnych poziomach struktury AD (lokacji, domeny lub jednostek organizacyjnych).
- Hierarchia usług AD umożliwia dziedziczenie ustawień powiązanych z kontenerami na wyższym poziomie przez kontenery niższego poziomu.

Domyślna zasada kontrolerów domeny

- Podczas tworzenia pierwszej domeny w usługach AD powstają dwa obiekty GPO powiązane wewnątrz usług AD:
 - Domyślna zasada domeny (Default Domain Policy) – powiązana na poziomie domeny i używana do ustawiania domyślnych zasad zabezpieczeń i haseł dla całej domeny.
 - Domyślna zasada kontrolerów domeny (Default Domain Controllers Policy) – powiązana z jednostką organizacyjną kontrolery domeny (Domain Controllers) i używana do kontrolowania zabezpieczeń kontrolerów domeny.
- Można tworzyć dowolną liczbę obiektów GPO i łączyć je z różnymi miejscami struktury usług AD.

Lokalne obiekty zasad grupy

- Są tworzone w środowiskach komputerów klienckich lub autonomicznych.
- Komputery systemów Windows 2000, Windows Server 2003, Windows XP mogą zawierać tylko jeden LGPO dotyczący wszystkich logujących się użytkowników.
- Windows Vista, Windows 7 oraz Windows 2008 domyślnie tworzy jeden LGPO, ale istnieje możliwość używania obiektów LGPO dla wielu użytkowników.

Stosowanie obiektów zasad grupy



Zasady stosowania

- 1. Jeśli obiekt LGPO jest włączony, to jest zawsze przetwarzany w pierwszej kolejności.
- 2. W następnej kolejności są przetwarzane obiekty zasad grupy na poziomie lokacji (jeśli w obiekcie LGPO istnieją ustawienia sprzeczne z obiektem GPO1, ustawienia GPO1 zastąpią ustawienia LGPO).
- 3. W kolejnym kroku przetwarzane są wszystkie obiekty GPO domeny (wpływają na użytkowników i komputery tej określonej domeny. Jeśli istnieją ustawienia sprzeczne w lokacji lub LGPO, ustawienia domeny mają pierwszeństwo, zaś niesprzeczne są dziedziczone po obiektach GPO wyższych poziomów).
- Ostatnim etapem jest przetworzenie wszystkich obiektów GPO skojarzonych na poziomach jednostek organizacyjnych (jeśli istnieją ustawienia sprzeczne w domenie lokacji lub LGPO ustawienia dla jednostki organizacyjnej mają pierwszeństwo).

Składniki zasad grupy

- Obiekt zasad grupy korzystający z usług Active Directory w rzeczywistości składa się z dwóch składników:
 - 1. Składnik logiczny jest przechowywany w bazie danych usługi AD i jest nazywany kontenerem zasad grupy (Group Policy Container, GPC).
 - 2. Składnik fizyczny jest przechowywany w replikowanym folderze SYSVOL umieszczonym na każdym kontrolerze domeny i jest nazywany szablonem zasad grupy (Group Policy Template, GPT).

Kontener zasad grupy GPC

 Tworzony w bazie danych usług AD podczas tworzenia nowego obiektu GPO

🗢 🔿 🔁 📅 🔏 🗎 🕻 🖬 🔁 🧇 🤿	5 8 8 6	i 🍸 🔁 🐍	
Active Directory Users and Com 🔺 Name	Type	Description	
🗄 🚞 Saved Queries 🛛 📄 Machine	Container		
🖃 🏥 krakow.filemon.wszib.edu.p 🔰 🤗 _{User}	Container		
🕀 🧮 Builtin			
🕀 🚞 Computers			
🛨 🖬 Domain Controllers			
🕀 🧮 ForeignSecurityPrincipal			
🕀 🧮 LostAndFound			
🕀 🦳 Program Data			
🖃 🧮 System			
🕀 🚞 AdminSDHolder			
🕀 🚞 ComPartitions			
🕀 🚞 ComPartitionSets			
🕀 🚞 DomainUpdates			
🗉 🧮 IP Security			
🕀 🚞 Meetings			
🕀 🚞 MicrosoftDNS			
🖃 🧮 Policies			
🗉 🧮 RAS and IAS Server			
🗉 🦳 WMIPolicy			
🗉 📸 Default Domain Polic			
🗉 🧧 Dfs-Configuration			
🗉 🧰 DFSR-GlobalSetting:			
🗉 📇 File Replication Serv			
🗉 🧮 FileLinks 🔍 🚽			

Atrybuty GPC

GPC z	{31B2F340-016D-11D2-945F-00C04FB984F9} Properties ? × General Object Security Attribute Editor	ormacji
• Nazv	Attributes:	
 Scie: szab nazw 	Attribute Value dSCorePropagationD 0x0 = () extensionName <not set=""> flans 0</not>	owiedniego z tę samą
 Lista stron 	fSMORoleOwner <not set=""> gPCFileSysPath \\krakow.filemon.wszib.edu.pl\sysvol\krakov</not>	zerzeń po GPO.
 Num obieł używ 	gPCFunctionalityVersi 2 gPCMachineExtensio [{35378EAC-683F-11D2-A89A-00C04FBBCF. gPCUserExtensionNa [{25537BA6-77A8-11D2-9B6C-0000F808086 gPCWQLFilter www.setace.org	częścią GPC SPC i GPT i
 Stan Conf wyłą 	instanceType 0x4 = (WRITE) isCriticalSystemObject TRUE isDeleted <not set=""></not>	część User on
 Lista mają użytł 	IastKnownParent <not set=""> mS-DS-ConsistencyC <not set=""></not></not>	rupy, które lo których vienia GPO.
	Edit <u>Filter</u>	

Apply

Składniki szablonu zasad grupy

- Po skonfigurowaniu nowego obiektu GPO tworzony jest skojarzony z nim szablon GPT.
- Szablon GPT przechowywany jest w folderze %SystemRoot%\SYSVOL na każdym kontrolerze domeny.
- Szablon zasad grupy zawiera większość rzeczywistych ustawień obiektu GPO oraz kilka folderów i plików konfiguracji.

Składniki szablonu zasad grupy (Adm, GPT.ini)

- Adm w systemach różnych od Windows 7, Vista, 2008 Server zawiera kopię wszystkich plików szablonów administracyjnych z komputera, który został użyty do tworzenia obiektu GPO.
- Gpt.ini plik wykorzystywany do przechowywania numeru wersji szablonu GPT i nazwy wyświetlania skojarzonej z GPO.

Składniki szablonu zasad grupy (MACHINE)

- MACHINE zawiera wszystkie ustawienia konfiguracji komputera:
 - Registry.pol ustawienia rejestru wszystkich konfiguracji szablonów administracyjnych.
 - Applications informacje używane do instalacji oprogramowania zasad grupy.
 - Microsoft\WindowsNT\SecEdit zawiera plik GptTmpl.inf z ustawieniami zabezpieczeń.
 - \Scripts\Shutdown rzeczywiste pliki używane dla skryptów podczas zamykania komputera.
 - Scripts\Startup rzeczywiste pliki używane dla skryptów podczas uruchamiania komputera.

Składniki szablonu zasad grupy (USER)

- USER zawiera wszystkie ustawienia konfiguracji użytkownika:
 - Registry.pol zawiera ustawienia rejestru wszystkich konfiguracji szablonów administracyjnych.
 - Applications informacje do instalowania oprogramowania.
 - Documents&Settings informacje o zasadach przekierowania folderu skonfigurowanych w GPO.
 - Microsoft\IEAK informacje o ustawieniach programu IE.
 - \Scripts\Logon pliki dla skryptów logowania.
 - \scripts \Logoff pliki dla skryptów wylogowania.

Replikacja składników obiektu zasad grupy

- Kontener GPC jest replikowany jako część zwykłego procesu replikacji usług AD.
- Replikacja szablonu GPT jest zależna od poziomu funkcjonalnego domeny:
 - Na poziomie funkcjonalnym systemu Windows 2008, GPT jest replikowane za pomocą usługi DFS-R (Distributed File System Replication).
 - Domeny pracujące na poziomie Windows 2003 lub niższym korzystają z usługi FRS (File Replication Service)

Sposób przetwarzania obiektów GPO przez systemy klienckie

- Windows 7, Vista, Server 2008, zawierają usługę Group Policy Client Service (gpsvc), która przejęła zadania przetwarzania zasad grupy będące dotychczas częścią usługi Winlogon.
- Każdy system operacyjny Windows korzystający z zasad grupy zawiera składniki rozszerzenia po stronie klienta (CSE).
- CSE składają się z kilku bibliotek DLL wywoływanych przez mechanizm zasad grup, który używa informacji przekazanych przez GPT i GPC do określenia, które zasady mają być zastosowane do użytkownika lub komputera.

Interakcje mechanizmu zasad grupy klient - serwer



Implementowanie zasad grupy

- W systemach Windows 2008 Server zasadami grup zarządza się z konsoli GPMC (Group Policy Management Console).
- Składa się z kilku węzłów udostępniających różne poziomy funkcjonalności.
- Węzeł *Las* zawiera 4 kolejne węzły:
 - 1. Domeny udostępnia listy domen zarządzanych przez zasady grup.
 - 2. Lokacje udostępnia listę skojarzonych z lasem usług Active Directory.
 - Modelowanie zasad grup umożliwia tworzenie scenariuszy do stosowania i przetwarzania zasad grupy w danym środowisku.
 - Wyniki zasad grupy umożliwia korzystanie z programu kreatora wyników do określenia wyników przetwarzania zasad dla użytkowników i komputerów w środowisku AD.
- Po uruchomieniu GPMC domyślnie cała administracja ma miejsce na kontrolerze domeny.

Konsola GPMC

🛃 Group Policy Management			
🔣 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp			_ 8 ×
🗇 🔿 🙍 📊 🧕 👘		'	
Group Policy Management Forest: krakow.filemon.wszib.edu.pl Domains C R Policy Default Domain Policy niezaawansowani C Domain Controllers C Coup Policy Objects C C Policy Objects C Starter GPOs Starter GPOs C Sites Group Policy Modeling C Group Policy Results	Domains Contents	Current Domain Controller dns1.krakow.filemon.wszib.edu.pl	

Tworzenie obiektów GPO

- Składa się z dwóch kroków:
- Utworzenie obiektu GPO oraz skonfigurowanie go za pomocą odpowiednich zasad.
- Powiązanie obiektu GPO z domeną, lokacją lub kontenerem jednostki organizacyjnej.

Utworzenie obiektu GPO

 Prawy przycisk myszy na kontenerze GPO i opcja Nowy. Wpisujemy nazwę (srednio_zaawansowani).

🔜 Group Policy Management					
🔜 Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp				_ 8 ×	
🗢 🔿 🙍 🖬 📋 🙆 👘					
Group Policy Management	Group Policy Objects in k	rakow.filemo	n.wszib.edu.pl	1	
krakow.filemon.wszib.edu.pl E Default Domain Policy	Name A	GPO Status	WMI Filter	Modified	
niezaawansowani	Default Domain Controllers P	Enabled	None	2/15/2010	
Domain Controllers Group Policy Objects WMI Filters G Starter GPOs Sites G Group Policy Modeling Goup Policy Modeling	iezaawansowani	Enabled	None	2/15/2010	
Group Policy Results			🛃 New GPO		×
			<u>N</u> ame:		
			srednio_zaawanso	wani	
			<u>S</u> ource Starter GPC	D:	
			(none)		•
					OK Cancel

Powiązanie obiektu GPO

Drowny przywiek myczy po kontopor i wybioromy

🤜 Group Policy Management		
🔜 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp		_ _ 8 ×
🗇 🔿 🙋 📅 🙆 👔		
Group Policy Management A Forest: krakow.filemon.wszib.edu.pl D B Domains	Group Policy Objects in krakow.filemon.wszib.edu.p	»ı /)
🖃 🏥 krakow.filemon.wszib.edu.pl	Name 🔺 GPO Status WMI Filter	r Modified
 ➡ Default Domain Policy ➡ niezaawansowani ➡ Srednio_zaawansowani ➡ Domain Controllers ➡ Group Policy Objects ➡ WMI Filters ➡ Starter GPOs ➡ Sites ➡ Group Policy Modeling ➡ Group Policy Results 	Default Domain Controllers P Enabled None Default Domain Policy Enabled None Iniezaawansowani Enabled None Isrednio_zaawansowani Enabled None	2/16/2010 2/15/2010 2/15/2010 3/1/2010 1
	4 Group Policy obje	ect(s)

Powiązanie do użytkownika

🛃 Group Policy Management	
🔜 Eile Action View Window	Help
🔄 🔿 🙎 🖬	
Group Policy Management Group Policy Management Group Policy Management Group Policy Management Group Policy Noteling Group Policy Modeling Group Policy Modeling Group Policy Results	srednio_zaawansowani Scope Details Settings Delegation Links Display links in this location: krakow filemon.wszib.edu.pl ▼ The following sites, domains, and OUs are linked to this GPO: ▼ Image: Comparison of the state of the s
	,

Edycja obiektu GPO

📕 Group Policy Management Edito	r		<u>- 🗆 ×</u>
<u>File Action View H</u> elp			
🗢 🔿 🖄 📅 🖶 📋 🗮 🖉) 🗟 🛛 🖬 🔂 🗟	<mark>0 +</mark>	
 srednio_zaawansowani [dns1.kraki Computer Configuration Policies Preferences Veser Configuration Policies Preferences Vindows Settings Control Panel Settings Control Panel Settings Data Sources Devices Folder Options Local Users and Grain Network Options Network Options Printers Regional Options Scheduled Tasks Start Menuers 	Star Processing Abort rest of grou Process in user co Remove (if not ap Preference (apply Filtered directly: Filtered by ancest Disabled directly: Disabled by ancest Disabled by ancest No description pro	General Classic Cassic Common Start menu items: On't display this item Connect to Control Panel Object Display as a link Display as a menu Don't display this item Don't display this item Don't display this item Programs The Start menu contains shortcuts to the programs you use most often. Clearing the list of shortcuts does not delete the programs. Number of programs on Start menu: Present documents Select this option to provide quick access to the documents you opened most recently. Clearing this list does not delete the documents. Mumber of programs on Start menu: It ist my most recently opened documents OK Cancel Apply Help	
Start Menu			
pron c meno			

Składniki zarządzania zasadami

Ariin\/

🗐 Group Policy Management Editor	
Eile Action View Help	
Default Domain Policy [dns1.krakov] Default Domain Police	[dns1.krakow.filemon.wszib.edu.pl] Policy
 Policies Software Settings Windows Settings Scripts (Startup/Sh Security Settings Policy-based QoS Administrative Templat Preferences Windows Settings Control Panel Settings Software Settings<	otion. Name Computer Configuration User Configuration
Extended Standard	

Kontenery zasad grupy (1)

- Policies (User, Computer Configuration) zawierają kontenery Software Settings, Windows Settings oraz Administrative Templates. Konfigurują podstawowe ustawienia zasad grupy.
 - (CU)Policies\Software Settings konfiguracja wykorzystywana do dystrybucji programów.
 - (CU)Policies\Windows Settings\Scripts skrypty uruchamiania i zamykania systemów oraz logowania i wylogowania użytkowników.
 - (CU)Policies\Windows Settings\Security Settings ustawienia do skonfigurowania zabezpieczeń komputera (konfigurowalne na poziomie domeny lub kontenera).
 - (CU)Policies\Windows Settings\Policy-based QoS ustawienia priorytetów ruchu sieciowego dot. Użytkowników lub komputerów dla określonych aplikacji, adresów protokołów lub portów.

Kontenery zasad grupy (2)

- (U)Policies\Windows Settings\Folder Redirection – ustawienia, które przekierowują do udziału sieciowego foldery użytkownika (np. Documents).
- (U)Policies\Windows Settings\Remote Installation Services – opcja konfiguracji usługi RIS (Remote Installation Services).
- (U)Policies\Windows Settings\Internet Explorer Maintenance – zarządzanie konfiguracją IE.
- (UC)Policies\Administrative Templates schematy ustawień do konfigurowania ustawień systemów.

Kontenery zasad grupy (3)

- Preferences (User, Computer Configuration) – zawierają wskazówki odnoszące się do ustawień systemu Windows oraz Panelu Sterowania.
 - (CU)Preferences\Windows Settings konfiguracja ustawień systemu Windows (skróty, zmienne środowiskowe, rejestry, plik ini, mapowanie dysków (tylko U)...
 - (CU)Preferences\Control Panel Settings ustawienia panelu sterowania takie, jak kontrolowanie lokalnych grup i użytkowników, opcje folderów i in.

Modyfikowanie zakresu przetwarzania obiektu GPO

- Zakres modyfikacji obejmuje:
 - Modyfikowanie kolejności powiązania.
 - Wyłączanie lub powiązanie GPO.
 - Wymuszanie lub blokowanie powiązania obiektu GPO.
 - Filtrowanie stosowania GPO przy użyciu grup zabezpieczeń lub filtrów WMI (Windows Management Instrumentation).

Kolejności powiązań

- Podczas uruchamiania komputera lub logowania użytkownika ustawienia zasad są stosowane w następującej kolejności:
 - 1. Lokalne zasady grupy.
 - 2. Obiekty GPO przypisane na poziomie lokacji.
 - 3. Obiekty GPO przypisane na poziomie domeny.
 - 4. Obiekty GPO przypisane na poziomie jednostki organizacyjnej.

Modyfikacja kolejności powiązań

- Często do dowolnych poziomów usług AD jest powiązanych kilka obiektów GPO. W takim przypadku kolejność powiązania określa kolejność stosowania obiektów GPO.
- Powiązanie o najwyższym numerze będą przetwarzane jako pierwsze, a następnie przetwarzane będą powiązania o numerach niższych.
- Wszystkie niezgodne ustawienia zasad zostaną zastąpione przez ustawienia obiektu GPO skonfigurowanego dla ostatniego powiązania.

Przykład kolejności powiązań

Włączanie i wyłączanie przetwarzania zasad

Blokowanie i wymuszanie przetwarzania GPO

- Blokowanie może być stosowane, jeśli daną funkcjonalność chcemy zablokować i udostępnić wybranym użytkownikom:
 - 1. Tworzymy wówczas dla każdej z tych "grup" jednostki organizacyjne.
 - Definiujemy GPO, w którym funkcjonalność ta jest niedostępna i przypisujemy ją obu jednostkom organizacyjnym.
 - Blokujemy dziedziczenie zasad dla jednostki organizacyjnej, dla której funkcjonalność ta ma być dostępna.

Filtrowanie przetwarzania GPO za pomocą grup zabezpieczeń i WMI (Windows Management Instrumentations)

- Domyślnie po utworzeniu obiektu GPO, ustawienia zasad są stosowane do wszystkich uwierzytelnionych użytkowników.
- Istnieje możliwość wyspecyfikowania, do których użytkowników lub komputerów stosowany będzie obiekt GPO. W tym celu:
 - 1. Z listy Security Filtering usuwamy grupę użytkowników uwierzytelnionych.
 - 2. Dodajemy do listy odpowiednie konta.
- Specyficzne przetwarzanie GPO można zdefiniować dla określonych grup zabezpieczeń, użytkowników lub komputerów.
Filtrowanie zabezpieczeń

🛃 Group Policy Management	
🛃 Eile Action View Window	Help
Group Policy Management Group Policy Management Forest: krakow.filemon.wszib Domains Default Domain Pr niezaawansowani Srednio_zaawans Domain Controller Group Policy Obje WMI Filters Starter GPOs Sites Group Policy Modeling Group Policy Results	srednio_zaawansowani Scope Details Settings Delegation Links Display links in this location: krakow filemon.wszib.edu.pl The following sites, domains, and OUs are linked to this GPO: Location ^ Enforced Link Enabled Path Image: Readow filemon.wszib.edu.pl No Yes krakow filemon.wszib.edu.pl Security Filtering The gettings in this GPO can only apply to the following groups, users, and computers: Name ^ Add Remove Properties MMI Filtering This GPO is linked to the following <u>WMI filter:</u> Image: This GPO is linked to the following <u>WMI filter:</u>

Korzystanie z filtrów WMI

- Mogą zostać wykorzystane do precyzyjnego określania, do których komputerów powinny być stosowane ustawienia zasad grupy (np. mają zostać użyte do komputerów wyposażonych w co najmniej 512MB RAM).
- Funkcja WMI Filters jest obsługiwana w systemach Windows: XP, Server 2003, Vista, 7 oraz Server 2008. We wcześniejszych wersjach jest pomijana.

Scriptomatic Version 2.0 by The Microsoft Scripting Guys

Scriptomatic Version 2.0 by The Microsoft Scripting Guys		
WMI Namespace WMI Class		
root\CIMV2	_	
Run CIMv2 WMI Source Open Save Quit		
On Error Resume Next]	
	Languag	ge 🛛
Const wbemFlagReturnImmediately = &h10 Const wbemFlagForwardOnk = &h20		
const woeninagrof wardoniy - anzo	VBScript	•
arrComputers = Array("localhost")		
For Each strComputer In arrComputers	Perl	
WScript.Echo	JScript	0
WScript.Ecno "====================================	Buthon	
WScript.Echo "====================================	Fython	
	0.4.4.5	
Set objWMIService Administrator: C:\Windows\system32\cmd.exe		- 0 >
Set collems = objvv SupportsDiskQuotas:		
SupportsFileBasedCompression:		
For Each objitem in SystemCreationClassName: Win32_ComputerSystem		
WScript.Echo "Ac UolumeDirty:		
WScript.Echo "Av VolumeName: WScript.Echo "Bid UolumeSerria INumber:		
WScript.Echo "Ca		
WScript.Echo "Co Access: 0		
WScript.Echo "Co BlockSize:		
WScript.Echo "Co Caption: C: WScript.Echo "Co Caption: C:		
ConfigManagerErrorCode:		
Target Computers (cor ConfigManagerUserConfig:		
localhost CreationClassName: Win32_LogicalDisk Description: Local Fixed Disk		
DeviceID: C:		
DriveType: 3 EnnonCleaned:		
ErrorDescription:		
ErrorMethodology:		
Filesystem: MIFS FreeSpace: 36905172992		

Filtry WMI (2)

🛃 Group Policy Manageme	ent _	
🛃 Eile Action View Wit	indow Help	ð ×
🧢 🔿 🖄 🖬 🗐 🤇		
roup Policy Management Forest: krakow.filemon.wszib Domains krakow.filemon.wszib	WMI Filters in krakow.filemon.wszib.edu.pl D.edu.p Contents Delegation b.edu.p Name (Description Linked GPO Author ew WMI Filter X Name (Description X	=
Domain Contro Group Policy C WMI Filters Starter GPOs Sites	New WMI Filter Description: LDSpace > 100M	
Group Policy Modeling	Queries: Namespace: Namespace Provse Query: Query: Select * from Win32_LogicalDisk where FreeSpace > 104857600 AND Caption = "C:"	
	OK Cancel	

Filtry WMI (3)

Delegowanie administracji GPO

- Usługa AD umożliwia delegowanie zadań administracyjnych dotyczących zasad grup w obrębie organizacji.
- Możliwe są trzy sposoby delegowania:
 - 1. Delegowanie uprawnień do tworzenia, usuwania i modyfikowania obiektów GPO.
 - 2. Delegowania prawa do zarządzania powiązaniami zasad grup.
 - 3. Przekazanie użytkownikowi prawa do generowania informacji w wynikowym zestawie zasad RSoP (Resultant Set of Policy).

Delegowanie uprawnień – metoda 1

🧮 Group Policy Management		<u>- 0 ×</u>
🔣 Eile Action View Window Help		_ 8 ×
🗢 🔿 🖄 📰 📋 🙆 🔽 🖬		
Group Policy Management Forest: krakow.filemon.wszib.edu.pl Domains Krakow.filemon.wszib.edu.pl Forest: krakow.filemon.wszib.edu.pl Forest: krakow.filemon	Group Policy Objects in krakow.filemon.wszib.edu.pl Contents Delegation The following groups and users can create GPOs in this domain. Groups and users: Name Image: Contents Image: Contents Image: Contents Contents Image: Contents <td>Inh No No No</td>	Inh No No No

Delegowanie uprawnień – metoda 2

Active Directory Users and Computers	_ 🗆 🗵
Eile Action View Help	
← → 2 m = 0 → 2 m ≤ 2 m ≤ 2 m ≤ 2 × 2 ×	
Active Directory Users and Comput Saved Queries Saved Queries Builtin Builtin Builtin Computers Domain Controllers PoreignSecurityPrincipals Vusers Builtin Domain Controllers Domain Controllers Dours Vusers Delegation of Control Wizard Domain Controllers Domain Controllers Dours Vau can select common tasks or customize your own. Vau can select common tasks or customize your own. Delegate the following common tasks: Read all user information Modify the membership of a group Join a computer to the domain Manage Group Policy links Generate Resultant Set of Policy (Logging) Create, delete, and manage inetOrgPerson accounts	
< <tr> < Back Next > Cancel</tr>	Help

Delegowanie uprawnień – metoda 3

- Polega na przekazaniu użytkownikowi prawa do generowania informacji w wynikowym zestawie zasad RSoP.
- Konsola GPMC może być również używana do delegowania prawa do zarządzania powiązaniami GPO, modelowaniem zasad grupy i wynikami zasad grupy.

Implementowanie zasad grupy pomiędzy domenami

- Zasady grupy można wykorzystywać do wymuszania ustawień pomiędzy domenami i zaufanymi lasami.
- Utworzony obiekt GPO jest przechowywany tylko na kontrolerach domeny w domenie, w której zostały utworzone. Można je powiązać z dowolną lokacją domeną lub jednostką organizacyjną.
- Wady:
 - Powiązanie obiektu z kontenerem w innej domenie spowoduje spadek wydajności sieci.
 - 2. Jeśli użytkownicy jednej domeny muszą stosować obiekt GPO innej domeny to muszą oni mieć dostęp na poziomie odczytu do kontenera GPC w usługach AD i szablonu GPT w folderze SYSVOL.

Implementowanie zasad grupy pomiędzy lasami

- Zasady identyczne jak w implementacjach pomiędzy domenami.
- Wykorzystywane jeśli użytkownicy przemieszczają się pomiędzy lokalizacjami znajdującymi się w oddzielnych lasach.
- Możliwości:
 - 1. Udziały używane do dystrybucji oprogramowania mogą znajdować się w oddzielnych lasach.
 - 2. Skrypty logowania mogą znajdować się na kontrolerze domeny w innym lesie i mogą być z niego odczytywane.
 - 3. Foldery przekierowane i pliki profili mobilnych mogą znajdować się na kontrolerze w innym lesie.

Zarządzanie obiektami zasad grupy

- 1. Tworzenie kopii zapasowych i przywracanie obiektów zasad grupy.
- 2. Kopiowanie obiektów zasad grupy.
- 3. Importowanie ustawień obiektów zasad grupy.
- 4. Modelowanie i raportowanie wyników zasad grupy.

Tworzenie kopii

poszczególnych (

zestawu GPO.

Polega na kopiov

Administrator mu

wskazanego folde

obiektu GPO i up

folderze docelow

- Bezpieczeństwo i zarządzanie infrastrukturą AD silnie bazuje na zasadach grupy. Stąd istotne jest zaplanowanie i realizacia strategii kopii zapasowych Eterthered (March 1996)
- Kopni Zapacov yor
 Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.

Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.

To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.

Location:



	Vracania Windows Internet Explorer	nhiekte	ήνν GPO
💽 – 🌈 C:\Users\Ad	ministrator \AppData \Local \Microsoft \Windo	ws\Temporary Interne 🔽 🔸 🗙	Live Search
🔅 🌈 srednio_zaawa	nsowani		🟠 🔹 🔝 🔹 🖶 🔹 🔂 Page 🔹 🎯 Tç
ednio_zaawansowa	ni		
a collected on: 3/10/2010	9:35:22 AM		
neral			
Details			
Domain		krakow.filemon.wszib.edu	lq.t
Owner		KRAKOW\Domain Admin	15
Created		3/3/2010 7:48:18 PM	
Modified		3/5/2010 1:22:56 PM	
User Revisions		24 (AD), 24 (sysvol)	
Computer Revisio	Ins	0 (AD), 0 (sysvol)	
Unique ID		{F0DB6870-D6A2-4748-A	A670-7E3280061160}
GPO Status		Enabled	
Links			
Location	Enforced	Link Status	Path
krakow	No	Enabled	krakow.filemon.wszib.edu.pl
This list only inclu	ides links in the domain of the GPO.		
Security Filtering			
The settings in	this GPO can only apply to the follo	wing groups, users, and comput	ters:
Name			
KRAKOW\nowal	¢		
WMI Filtering			
WMI Filter Na	ne	LDS>100M	
Description		LDSpace > 100M	

🕞 🚯 🚭 Internet | Protected Mode: Off

🔍 100%

-

-		
	100	-
- 2		_
_		

Kopiowanie obiektów zasad grupy

- Funkcja wbudowana w konsolę GPMC.
- Dostarcza prostej metody migracji ustawień zasad grupy pomiędzy domenami.
- Wymagane prawa do odczytu dla obiektu GPO w domenie źródłowej oraz zapisu w docelowej.

Importowanie ustawień obiektu zasad grupy

- Wykorzystywana do kopiowania obiektu zasad grupy pomiędzy dwoma lokalizacjami, które nie są połączone.
- Polega na:
 - 1. Utworzeniu kopii zapasowej obiektów GPO w lokalizacji źródłowej.
 - 2. Utworzenie nowego obiektu GPO lub zastąpienie istniejącego poprzez zaimportowanie kopii w lokalizacji docelowej.

Modelowanie i raportowanie zasad grupy

- W systemie Windows Server 2008 dziennikowane są dane dotyczące przetwarzania zasad grupy (baza danych usługi WMI na komputerze lokalnym).
- Informacje zawierają listę, zawartość oraz informacje rejestrowania dla każdego przetwarzanego obiektu GPO i pozwalają określić w jaki sposób ustawienia zasad są stosowane do użytkowników i komputerów.
- Funkcja ta jest nazywana wynikowym zestawem zasad (Resultant Set of Policy, RSoP). Możliwe dwa tryby pracy:
 - 1. Rejestrowanie informacje o wynikach ogólnych ustawień (Group Policy Results).
 - 2. Planowanie metoda symulacji wyników ustawień zasad (Group Policy Modeling).

Modelowanie zasad grupy

- Umożliwia testowanie ustawień bazując na bieżącej infrastrukturze zasad grupy (przeniesienie użytkownika z jego politykami do innej jednostki organizacyjnej).
- Administrator musi posiadać uprawnienie Generate Resultant Set of Policy. Kontroler domeny w systemie co najmniej Windows 2003.
- Scenariusz testowy można uruchomić na dwa sposoby:
 - Z przestawki AD Users and Computers, prawy przycisk myszy na domenie, a z menu wybieramy All Tasks, a następnie RSoP Planning.
 - 2. Z konsoli GPMC, prawy przycisk myszy na Group Policy Modeling, a następnie Group Policy Modeling Wizard.

Wyniki zasad grupy

- Funkcja Group Policy Result jest wykorzystywana do raportowania blędów w ustawieniach GPO.
- Uruchamiana z przystawki AD Users and Computers lub konsoli GPMC.
- Wymagania:
 - Posiadanie uprawnień Read Group Policy Result.
 - Analizowany komputer musi pracować pod kontrolą systemu Windows: 2003, 2008, XP, Vista, 7.
 - Włączona musi być usługa WMI.
 - W przypadku monitorowania systemu zdalnego musi zostać na nim dopuszczone rozszerzenie Remote Administration.
 - Jeśli badane są ustawienia odnośnie użytkownika, to musiał on co najmniej raz być podłączonym do systemu.



gpresult.exe

 Program narzędziowy umożliwia wyświetlanie zasad grupy i wynikowego zestawu zasad (RSoP) dla komputera lub użytkownika.

gpresult.exe [/s komputer [/u domain\user] [/p password]]] [/scope {user|komputer}] [/user Nazwa] [/r|/v] [/x | /h plik [/f]]

gpupdate.exe

Program narzędziowy służący uaktualnianiu ustawień zasad grupy.



Profile użytkowników

- W Windows Server 2008, Vista i 7 wprowadzono zmiany w strukturze i nazewnictwie profili użytkowników (Documents and Settings -> Users).
- Profil użytkownika zawiera informacje, które mapują gałąź rejestru HKEY_CURRENT_USER i jest przechowywany w katalogu głównym profilu użytkownika jako plik NTUSER.DAT.
- Przechowuje ustawienia aplikacji i konfigurację środowiska pracy w folderach ukrytych i jawnych.
- Nowa struktura zapewnia przekierowania, co pozwala minimalizować ilość przesyłanych informacji.

Działanie profili lokalnych

- Profil lokalny zostaje utworzony na każdym komputerze, podczas pierwszego podłączania się użytkownika do systemu.
- Profil początkowy bazuje na ukrytym profilu nazwanym *Default* z katalogu %SystemDrive%\Users. W przypadku komputerów podłączonych do domeny sprawdzane jest czy nie istnieje wersja sieciowa domyślnego profilu użytkownika, która umieszczana jest na kontrolerach domeny w udziale NETLOGON.
- Profile użytkowników zostają skojarzone z identyfikatorami zabezpieczeń użytkowników dzięki czemu dwóch użytkowników o tej samej nazwie logowania nie będzie korzystać z tego samego profilu.

Działanie profili mobilnych

- Są przechowywane w udziałach sieci, dzięki czemu profil przemieszcza się wraz z użytkownikiem przez komputery domeny.
- Kiedy użytkownik o skonfigurowanym profilu mobilnym systemu Windows Server 2008, Vista, 7 loguje się po raz pierwszy, profil generowany jest na podstawie jednego z dwóch miejsc:
 - 1. Wstępnie skonfigurowany profil użytkownika znajdujący się w udziale NETLOGON (utworzony profil należy skopiować do udziału pod nazwą Default User.v2).
 - 2. Lokalny profil domyślny (jeśli w udziale NETLOGON profil Default User.v2 nie istnieje, to początkowe ustawienia pobierane są z profilu Default).
- Znaczniki czasów dla każdego pliku są wykorzystywane do synchronizacji wersji podczas odłączania się od systemu.

Konfigurowanie profili mobilnych

- Tworzymy udostępniony udział (%SystemRoot%\Profiles).
- Użytkownicy uwierzytelnieni powinni mieć pełny dostęp, grupa Users powinna mieć możliwość modyfikacji.
- Opcjonalnie tworzymy domyślny profil sieciowy i zapisujemy go w udziale NETLOGON pod nazwą Default User.V2. Grupa Wszyscy powinna mieć pełny dostęp.

Konfigurowanie profili mobilnych

- Wymaga przecho
- Każde k skonfigu została pobierau skojarzo

Profil obowiązkowy

- Używany wraz z profilem mobilnym do tworzenia zablokowanych, standardowych konfiguracji pulpitu dla grupy użytkowników.
- Polega na utworzeniu zwykłego profilu, a następnie skopiowaniu go do udziału NETLOGON (zakładka Profile w okienku Computer Properties). Kolejna czynność to zmiana nazwy NTUSER.DAT na NTUSER.MAN i skonfigurowanie pliku tylko do odczytu. W ostatnim kroku przypisujemy go wybranym użytkownikom.
- Zmiany wprowadzone w profilu obowiązkowym nie będą zapisywane.

Idea profilu superobowiązkowego

- Jeśli profil mobilny lub obowiązkowy nie jest dostępny, to system tworzy profil tymczasowy w oparciu o sieciowy profil Default lub profil lokalny. Podczas wylogowywania profil ten jest usuwany.
- Jeśli jednak wymagane jest, aby profil obowiązkowy był zawsze używany, to jeśli profile nie są dostępne, to zalogowanie nie będzie możliwe.
- Profile superobowiązkowe pozwalają zrealizować tę konfigurację.
- Każdy użytkownik, dla którego skonfigurowany został profil superobowiązkowy nie będzie mógł zapisywać ustawień na serwerze profili.

Konfigurowanie profilu superobowiązkowego

- 1. Tworzymy profil obowiązkowy.
- Zmieniamy nazwę folderu profilu użytkownika dodając rozszerzenie .man.V2
- Korzystając np. z konsoli AD Users and Computers, każdemu użytkownikowi, który ma mieć profil superobowiązkowy, na końcu ścieżki profilu dopisujemy rozszerzenie .man

Ustawienia profilu w zasadach grupy

- Znajdują się w następujących lokalizacjach:
 - 1. Computer Configuration\Policies\Admini strative Templates\System\User Profiles
 - 2. User Configuration\Policies\Administrativ e Templates\System\User Profiles

Atrybuty profilu w ustawieniach komputera

	리스
<u>File Action View H</u> elp	
Image: Section Server Man Section Server Man Image: Section Server Man Section Section Server Man Image: Section Server Man Section Sectio	ate ifigure ifigure ifigure ifigure ifigure ifigure ifigure ifigure ifigure ifigure ifigure ifigure
Image: Second	
Image: A standard	

17 setting(s)

Atrybuty profilu w ustawieniach użytkownika



Przekierowanie folderu

- Problemem profili mobilnych są potencjalnie duże ilości danych przechowywanych na pulpicie czy w folderze Documents.
- Zasady grupy umożliwiają przekierowanie wybranych folderów poza profil, co ogranicza obciążenie sieci.
- Pozwala również na instalowanie standardowego środowiska pulpitu, a nie używania obowiązkowych profili użytkowników (menu Start, Pulpit, uprawnienia tylko do odczytu).
- Przekierowanie jest logiczne. Wskazane foldery zostają skierowane do udziału sieci, gdzie może być archiwizowany centralnie.



Opcje miejsca docelowego (Target)

- Not Configured folder nie został przekierowany do udziału sieciowego.
- Basic jeśli zachodzi potrzeba utworzenia jednej lokalizacji, do której wszystkie foldery zostaną przekierowane.
- Advanced umożliwia konfigurowanie alternatywnych lokalizacji dla przekierowanych folderów w zależności od tego, do których grup zabezpieczeń usług AD należy dany użytkownik.

Ustawienia przekierowania folderu

- Oprócz konfigurowania lokalizacji docelowej, można skonfigurować dodatkowe ustawienia tych folderów. Należą do nici Documents Properties
 - Grant the user exclusive r użytkownikowi i kontu syst Administrator nie będzie n
 - Move the contents of folde ustawienie przenosi bieżą folderu do wskazanej loka
 - Also apply redirection poliprzekierowywanie folderóv wersjach systemu (Docurr

Documents Properties	<u>? ×</u>
Target Settings	
Select the redirection settings for Documents.	
Grant the user exclusive rights to Documents.	
\checkmark <u>M</u> ove the contents of Documents to the new location.	
Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems.	
Policy Removal	
$\textcircled{\begin{tabular}{ll} \bullet \\ \underline{ L} eave the folder in the new location when policy is removed. \end{tabular}}$	
 Redirect the folder back to the local <u>u</u>serprofile location when policy is removed. 	
OK Cancel <u>A</u> p	ply
Konfigurowanie przekierowania podstawowego

- Opcja Basic umożliwia określenie lokalizacji folderu docelowego z następującymi opcjami:
 - Redirect to the use katalogu Docuents
 - Create a folder for określenie ścieżki foldery.
 - Redirect to the foll użytkownika okreś przekierowanie kill wspólne menu Sta
 - Redirect to the loc domyślna jeśli nie

Documents Properties	
Target Settings	ala
You can specify the location of the Documents folder.	
Setting: Basic - Redirect everyone's folder to the same location	Nono
This folder will be redirected to the specified location.	wane
Target folder location	dego
Create a folder for each user under the root path	riiwe
Create a folder for each user under the root path Redirect to the following location Redirect to the local usermofile location	ru (np.
<u>B</u> rowse	
	ja
OK Cancel <u>A</u> pply	

Ustawienia przekierowania folderu (2)

- Policy Removal możliwość definiowania czynności na wypadek usunięcia zasady.
 - Leave the folder in the new location when policy is removed.
 - Redirect the folder back to the local userprofile when policy is removed.



Ustawienia przekierowania folderu (2)

Opcje zaawansowane – administrator

DQDZ Documents Properties folde człor

Documents Properties	💷 🖄 🔤 🔤	zacie
Target Settings	C lonal	zację
You can specify the location of the Docur	Specify Group and Location	? ×
Setting: Advanced - Specify locations for various	You can choose the target folder location fo security group.	ra
This folder will be redirected to different locations bas group membership of the users.	Security Group Membership	_
Security <u>G</u> roup Membership	Bro <u>w</u> se.	
Group Path Add Edit Bemove OK Ca	Target Folder Location Create a folder for each user under the root path Root Path: Browse	
	OK. Can	cel



Pliki trybu offline,a przekierowanie folderu

- Po wdrożeniu funkcji przekierowania folderu, wszystkie foldery przekierowane dostępne są w trybie offline.
- Po zalogowaniu się użytkownika, w obszarze powiadomień pojawia się komunikat informujący, że pliki trybu offline zostały skonfigurowane do przeprowadzenia synchronizacji.

Szablony administracyjne

🗐 Group Policy Management Editor		
<u>File Action View H</u> elp		
🗢 🔿 🙍 📑 📴 😽		
 Default Domain Policy [dns1.krakow.filemon.wszib.ed Computer Configuration Policies Software Settings Mindows Settings Administrative Templates: Policy definition Control Panel Network Printers System Windows Components All Settings Preferences Vindows Settings Software Settings Software Settings Software Settings Mindows Components Software Settings Software Settings Mindows Components All Settings Software Settings Software Settings Mindows Settings Mindows Settings Control Panel Administrative Templates: Policy definition Control Panel Add or Remove Programs Display Printers Programs Regional and Language Options Shared Folders Start Menu and Taskbar 	Select an item to view its description.	Setting I Hide "Set Program Access and Computer Defaults" page I Hide "Get Programs" page I Hide "Installed Updates" page I Hide "Programs and Features" page I Hide the Programs Control Panel I Hide "Windows Features" I Hide "Windows Marketplace"
	Extended Standard	
7 setting(s)	<u></u> /	

Działanie plików szablonów (do Windows Server 2003)

- Są używane aby udostępnić ustawienia zasad dla każdego elementu z węzła Administrative Templates.
- Do wersji Server 2003 było to pięć plików adm w folderze %SystemRoot%\Inf.
- Pilki zawierają wpisy definiujące opcje dostępne w szablonie.
- Podstawowe pliki: System.adm, Inetres.adm, Wmplayer.adm, Conf.adm, Wuau.adm.

Działanie plików szablonów



Zarządzanie plikami szablonów odnoszących się do domeny (1)

- Zalecane jest utworzenie w katalogu SYSVOL kontrolera domeny centralnego archiwum plików ADMX. Będzie on replikowany automatycznie, co zapewni dostęp do aktualnych wersji na pozostałych kontrolerach.
- Czynności:
 - Na kontrolerze domeny tworzymy folder: %SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitio ns.
 - 2. W folderze PolicyDefinitions tworzymy foldery dla każdego języka wymaganego w domenie.

Zarządzanie plikami szablonów odnoszących się do domeny (1)

3. Korzystając z komputera klienckiego (7, 2008) skopiować wszystkie pliki ADMX do folderu PolicyDefinitions:

copy %systemroot%\PolicyDefinitions*
%logonserver%\sysvol\%userdnsdomain%\Policies\Poli
cyDefinitions

4. Jak poprzednio, skopiować wszystkie pliki ADML do odpowiednich podfolderów:

copy %systemroot%\PolicyDefinitions\[MUIculture]* %logonserver%\sysvol\%userdnsdomain%\Policies\Poli cyDefinitions\[MUIculture]

 Po skonfigurowaniu centralnego archiwum w folderze SYSVOL narzędzie GPM będzie odczytywać pliki wyłącznie z niego ignorując lokalne.

Używanie skryptów do zarządzania środowiskiem użvtkownika

📕 Group Policy Management Editor	
<u>Eile Action View H</u> elp	
🗢 🔿 🙍 📑 🛛 🖬	
Default Domain Policy [dns1.krakow.filemon.wszib.edu.pl] Policy	utdown)
Elect an item to view its descr	ription. Name
Startup Properties	Startup
Script Scripts	Shutdown
Preferences	
🖂 🕵 User Configurati	
Policies Name Parameters	
E Software Up	
E Windows Down	
Rem	
a Scrip	
⊕ Secu Add Ad	
Edit.	
E Administi	
Preferences	
To view the script files stored in this Group Policy Object, proce	
the button below.	
<u>S</u> how Files	
OK Cancel Apply	

Używanie skryptów w praktyce

- Tworzymy skrypty, a następnie kopiujemy je do kontrolerów domeny. Lokalizacja dowolna – muszą być jednak dostępne dla systemów klienckich:
 - %SystemRoot%\SYSVOL\sysvol\domainname\ GlobalPolicyGUID\Machine\Scripts
 - 2. %SystemRoot%\SYSVOL\sysvol\domainname\ GlobalPolicyGUID\User\Scripts
 - 3. %SystemRoot%\SYSVOL\sysvol\domainname\ Scripts
- Tworzymy lub modyfikujemy obiekt GPO dla zlokalizowania folderu Scripts:
 - Computer Configuration\Policies\Windows Settings
 - User Configuration\Policies\Windows Settings

Instalowanie oprogramowania przy użyciu zasad grupy

- Zarządzanie oprogramowaniem opiera się na technologii Microsoft Windows Installer. Składa się ona z:
 - Pliku pakietu instalacyjnego oprogramowania (msi) – posiada bazę danych zawierającą wszystkie instrukcje konieczne do dodania lub usunięcia pakietu.
 - Usługi Windows Installer (Msiexec.exe) zarządza wykonaniem rzeczywistej instalacji (dll do odczytu pliku msi oraz dokonuje wpisów do rejestru, utworzenia katalogów, skrótów, itd.).

Instalowanie aplikacji (1)

- Możliwe ogłaszanie dostępności lub udostępnianie aplikacji do zainstalowania.
- Administrator kopiuje pliki instalacyjne oprogramowania do udziału sieciowego dostępnego dla wszystkich użytkowników. Konieczne prawo odczytu dla użytkowników lub komputerów.
- Decyzja, czy aplikacja będzie ogłaszana dla użytkowników czy dla komputerów.
- Modyfkacja lub utworzenie nowego obiektu GPO:
 - Computer Configuration\Policies\Software Settings aplikacje będą instalowane po następnym uruchomieniu komputera.
 - User Configuration\Policies\Software Settings aplikacje będą instalowane po następnym zalogowaniu się użytkownika.

Instalowanie aplikacji (2)

- Opcje ogłaszania aplikacji dla klientów:
 - 1. Przypisanie aplikacji wskazanie komputera lub użytkownika.
 - 2. Publikowanie aplikacji tylko dla użytkowników.
- Przypisanie do komputera skutkuje jej zainstalowaniem przy ponownej inicjalizacji systemu.
- Przypisanie do użytk ogłaszana przy nast dodaje się ją do mer Get Programs aplika aplikacja nie jest ins wywołania (uruchom
- Publikowanie dla uż Panelu sterowania v

ļ	<u>kownika nowoduja ża anlikacja jast</u>	
1	Deploy Software	×
יו	Select deployment method:	
6	C <u>P</u> ublished	
5		
r	C Ad <u>v</u> anced	
2	Select this option to Assign the application without modifications.	-
V	/	
	OK Cancel]

Procedura ogłaszania (1)

- Dla ogłoszenia aplikacji za pomocą zasad grupy należy:
 - Skopiować pliki instalacji do udziału sieciowego. Skonfigurować uprawnienia tak, aby wszyscy użytkownicy i komputery mieli uprawnienia do odczytu.
 - 2. Za pomocą konsoli GPMC utworzyć nowy obiekt lub zmodyfikować istniejący. Odpowiednio go powiązać.
 - Jeśli aplikacja jest ogłaszana dla użytkowników w edytorze GPM rozwinąć kontener User Configuration\Policies\Software Settings, kliknąć prawym przyciskiem myszy pozycję Software Installation, przycisk New, a następnie opcję Package.
 - Jeśli aplikacja jest ogłaszana dla kont komputerów, należy rozwinąć kontener w obiekcie GPO Computer Configuration\Policies\Software Settings, kliknąć prawym przyciskiem myszy pozycję Software Installation, przycisk New, a następnie opcję Package.

Procedura ogłaszania (1)

E Onen				XII	
🗐 Group Policy Management Editor					
<u>File Action View H</u> elp					
🗢 🔿 🔰 📊 🗐 🤒 👔 1	•				
🗐 Na potrzeby instalacji [dns1.krakov 🛛 Na	ame 🔺	Version	Deployment state	Source	
🖻 👰 Computer Configuration	Microsoft Visual Studio	9.0	Assigned	\\dns1\WETLOGON\VStudio_2008\vs	
Policies					
Software Settings					
🕀 🧮 Administrative Templat					
Preferences					
E 🐒 User Configuration					
)]	

Używanie zasad grupy do dystrybucji aplikacji, które nie są instalowane za pomocą technologii Windows

- Wymagane jest utworzenie pliku (zap) za pomocą pakietu aplikacji ZAW (Zero Administration for Windows).
- Plik zap jest plikiem tekstowym zawierającym instrukcje instalowania aplikacji. W większości przypadków jego zawartość jest następująca:

[Application] FriendlyName = "applicationname" SetupCommand = ""\\servername\sharename\installappliation.exe""

Plik zap

- Wartość atrybutu *FriendlyName* to napis, który zostanie wyświetlony w Panelu sterowania programu Dodaj usuń programy.
- Wartość atrybutu SetupCommand to ścieżka dostępu do programu instalacyjnego. Można posługiwać się notacją UNC lub zasobem sieciowym.
- Jeśli program instalatora wymaga przełączników, podajemy je po znaku ".

SetupCommand = " <u>\\servername\sharename\installappliation.exe</u>" /parametr

Instalacia

旦.	One	n				XI		
]	Group Policy Management Edito	r					
S	Eile	e <u>A</u> ction <u>V</u> iew <u>H</u> elp						
- Q	4	🔿 🔊 📰 🔄 🐼 😹						
		Instalacia zan [dos 1 krakow filemo	Namo é	Versien	Deployment state	L Courses		
Fa		Computer Configuration	Word Reader	0.0	Published	Vdns1WETLOG	DN\Word_Reader\kk	
	<u> </u>	🕀 📔 Policies						
93	L	Preferences						
1		Subser Configuration						
		Contracts Contracts						
E		Software installatic						
B		Windows Settings						
8								
8								
F								
	브							

. [

Ograniczenia plików zap

- Aplikacje dystrybuowane za pomocą plików zap nie mogą być przypisywane do komputerów lub użytkowników i nie mogą być aktualizowane przez aplikację rozszerzenia.
- Instalacja uruchamia typowy plik instalacyjny aplikacji, co oznacza, że nie można dostosowywać instalacji.
- Instalacja musi być przeprowadzana przez administratora lokalnego.
- Jeśli aplikacja nie działa, gdyż został usunięty lub uszkodzony jeden z jej plików, użytkownik będzie musiał uruchomić ręcznie oryginalną procedurę instalacji.
- Aplikacje instalowane plikami zap nie będą mogły być w prosty sposób aktualizowane.

Modyfikowanie właściwości pakietów oprogramowania

General Deployment Categories Security Deployment type Published Cassigned 	etu istnieje owania jego
Deployment options Image: Constant of the second secon	Advanced Deployment Options: Ignore language when deploying this package Make this 32-bit X86 application available to Win64 machines. Include QLE class and product information. Advanced diagnostic information: Product code: {0000000-0000-0000-000000000000} Deployment Count: 0 Script name: "\\dns1\NETLOGON\Word_Reader \KKopy.exe"

Aktualizowanie istniejącego pakietu

📕 Group Policy Management Editor		
<u>File A</u> ction <u>V</u> iew <u>H</u> elp		
🗢 🔿 🙍 🗔 💷 🧟 😖		
🗐 Instalacja zap [dns1.krakow.filemon.wszib.edu.pl] 🛛 Na	ime 🔺 Version Deployment state Source	lego dia
Computer Configuration	Microsoft Visual Studio 2008 Professional Edition - ENIL (2) Pro 2 X	ISD
□ □ Policies □ □ □ □ Software Settings □ □		
Software installation	General Add Upgrade Package	lі
Windows Settings Administrative Templates: Policy definition		bolitvk
	Choose a package from	[
E 🕵 User Configuration		
	Browse	VmV
		ynny
Administrative Templates: Policy definit Preferences	- Package to upgrade	dce
	Microsoft Vieual Studio 2008 Professional Edition - ENU	
	Add.	wym. W
	M HEdn	l
		plikacja
	 Uninstall the existing package, then install the upgrade package 	
	<u>P</u> ackage can upgrade over the existing package	vvCj.
	OK Cancel	
,	OK Cancel Apply	

Usuwanie oprogramowania zainstalowanego za pomocą zasad grup

- Funkcja Software installation może również zostać użyta do odinstalowania uprzednio zainstalowanych aplikacji i programów.
- Istnieją trzy możliwości usuwania oprogramowania za pomocą zasad grup:
 - 1. Usunięcie oprogramowania jako etap wstępny instalowania nowej wersji programu.
 - 2. Usuwanie oprogramowania jeśli komputer lub użytkownik są przenoszeni poza jurysdykcję administratora.
 - 3. Usuwanie oprogramowania jeśli usuwany jest pakiet oprogramowania.

Usuwanie oprogramowania z pakietem

- Dostępne jeśli z obiekru GPO usuwany jest pakiet oprogramowania.
- Administrator może określić w jaki sposób zarządzać oprogramowaniem.
- Prawy przycisk myszy na pakiecie, następnie All tasks i Remove. Dostępne możliwości to:
 - Natychmiast odinstaluj oprogramowanie od użytkowników i z komputerów.
 Remove Software
 - 2. Zezwalaj użytkownikom r oprogramowania, ale unio Oprogramowanie zostani komputer zostanie ponov ponownie się zaloguje.



Preferencje zasad grupy

- Zestaw rozszerzeń po stronie klienta dołączonych do systemu Windows Server 2008 umożliwiających centralne konfigurowanie i zarządzanie ustawieniami systemu operacyjnego i aplikacji.
- Wiele z nich do tej pory mogła być konfigurowana skryptami, jak np. mapowanie dysku sieciowego.
- Preferencje zasad grupy mają w zamierzeniu wyeliminować skrypty logowania.

Preferencje zasad, a ustawienia zasad grupy

- Wymuszanie ustawień po skonfigurowaniu ustawienia zasad grupy jest ono wymuszane na użytkownikach i komputerach przypisanych do GPO. Jeśli konfigurowane są preferencje zasad grupy, konfiguracja nie jest ściśle wymuszana i pozwala użytkownikom zmieniać ustawienia,
- Wskazywanie docelowych obiektów ustawień jednym z ograniczeń ustawień zasad grupy jest brak możliwości filtrowania poszczególnych ustawień zasad wewnątrz obiektu GPO. Stąd tworzenie specyficznych obiektów GPO odnoszących się do ustawienia zasady, a następnie stosowanie obiektu GPO przy użyciu filtrowania WMI. Funkcje preferencji umożliwiają określenie wartości docelowej na poziomie elementu.

Podsumowanie

Funkcja	Ustawienie zasady	Preferencje
Wymuszania	 Ustawienia są wymuszane. Interfejs użytkownika zostaje wyłączony. Ustawienia są odświeżane. Wymagane funkcje i aplikacje korzystające z zasad grupy. 	 •Ustawienia nie są wymuszane. •Interfejs użytkownika nie jest wyłączany. •Ustawienia mogą być stosowane tylko raz lub odświeżane okresowo. •Nie są wymagane funkcje i aplikacje korzystające z zasad grupy.
Obsługa lokalnych zasad grupy	Obsługiwane	Nie są obsługiwane
Wskazywanie obiektów docelowych i filtrowanie	Tylko na poziomie GPO (WMI)	Obsługa określania wartości na poziomie elementu

Ustawienia systemu Windows

🗐 Group Policy Management Editor						
<u>File Action View H</u> elp						
🗢 🔿 🙍 🖬 🗄 🗐 🗰 🙆 👔	T 🗟 🔕 🕇					
 Instalacja zap [dns 1.krakow.filemon.wszib.edu.pl] 	🔊 Files		Name	Order	Action	Source
 Windows Settings Environment Files Folders Ini Files Registry Network Shares Shortcuts Shortcuts Ocntrol Panel Settings Wiser Configuration Policies Preferences Windows Settings 	Processing	۲	There are no it	ems to sho	Action w in this viev	v.
Applications Drive Maps Environment Files Folders Ini Files Registry Shortcuts Control Panel Settings	Description No policies selected Preferences Extended	×	 ∕			Þ
Files						

Ustawienia panelu sterowania



Opcje preferencji zasad grupy

New File Properties	5		2	<u><</u>				
General Common	1			akci	e wykc	nywar	ne poo	lczas
Action:	New File Proper	ties			× no		, kozoć	ć
	General Comm	1 Targeting B	Editor		EIIU		N9209	
<u>S</u> ource file(s): <u>D</u> estination File:	Options com	<u>N</u> ew Item ▼	Add <u>C</u> ollection Item address range is 0.0.0	Options -	* * 👗 🛍 (🖺 🗕 🗙 Delete	❷ <u>H</u> elp	
	Apply o							
		<u>b</u> etween An IP Address processing co	0.0.0.0 s Range targeting iter omputer's IP address i	<u>a</u> nd allows a pre s within the ra	0.0.0.0 ference item to be ange specified in th	applied to comput e targeting item. <i>{</i>	ers or users on Additional inform	y if the nation
							ОК	Cancel