Infrastruktura od zera

Udziały NTFS i drukarki dla małej firmy; domena, DNS, DHCP i GPO są w książce Active Directory, DNS i DHCP.

- Udziały i uprawnienia NTFS na serwerze plików
- Serwer wydruku i drukarki z GPO

Udziały i uprawnienia NTFS na serwerze plików

Poziom: podstawy **Dotyczy: Windows Server 2019+, SMB 3.x** **Czas: ~30 min**

Serwer plików udostępnia foldery po sieci jako udziały, a każdy udział ma swój własny, osobny komplet uprawnień od uprawnień samego folderu na dysku. Uczymy się, jak nadawać oba komplety naraz przez model AGDLP, zamiast wpisywać pojedyncze konta w dwóch miejscach. Tu wracamy za każdym razem, kiedy ktoś ma dostęp do udziału i mimo to nie może otworzyć pliku.

Skróty użyte na tej stronie (5)

Skrót	Co znaczy
ACL	Access Control List: lista, kto ma jakie prawa do pliku lub zasobu
AGDLP	Account, Global, Domain Local, Permission: skrócona nazwa modelu zagnieżdżania grup w Active Directory, od kont przez grupy globalne i lokalne w domenie aż do faktycznego uprawnienia
DFS	Distributed File System: usługa łącząca udziały z wielu serwerów pod jedną wspólną ścieżką sieciową
NTFS	New Technology File System: system plików Windows z wbudowanymi uprawnieniami ACL na poziomie pliku i folderu
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy

Fiszka

ZMIENIA SYSTEM

Utworzenie udziału z uprawnieniami: New-SmbShare

```
New-SmbShare -Name "NazwaUdzialu" -Path "SciezkaFolderu" -FullAccess
"GrupaPelnaKontrola" -ChangeAccess "GrupaZmiana" -ReadAccess "GrupaOdczyt"
```

Tworzy nowy udział sieciowy i od razu nadaje uprawnienia udziału trzem grupom naraz, bez osobnego wywołania `Grant-SmbShareAccess` dla każdej z nich.

Przykład:

```
New-SmbShare -Name "Ksiegowosc" -Path "D:\Dane\Ksiegowosc" -FullAccess "ZIELONA\Domain Admins" -ChangeAccess "ZIELONA\DL_Ksiegowosc_RW" -ReadAccess "ZIELONA\DL_Ksiegowosc_RO"
```

TYLKO ODCZYT

Sprawdzenie uprawnień udziału: Get-SmbShareAccess

```
Get-SmbShareAccess -Name "NazwaUdzialu"
```

Przykład:

```
Name        ScopeName AccountName                AccessControlType AccessRight
----        --------- -----------                ----------------- -----------
Ksiegowosc  *         ZIELONA\DL_Ksiegowosc_RW    Allow             Change
Ksiegowosc  *         ZIELONA\DL_Ksiegowosc_RO    Allow             Read
Ksiegowosc  *         ZIELONA\Domain Admins       Allow             Full
```

ZMIENIA SYSTEM

Dołożenie kolejnego uprawnienia udziału: Grant-SmbShareAccess

```
Grant-SmbShareAccess -Name "NazwaUdzialu" -AccountName "NazwaGrupyLubUzytkownika" -AccessRight Change -Force
```

Dokłada jedno uprawnienie na poziomie udziału, nie ruszając tych, które już tam są. `-Force` pomija pytanie o potwierdzenie, przydatne w skryptach.

TYLKO ODCZYT

Odczyt uprawnień NTFS z konsoli: icacls

```
icacls "SciezkaFolderu"
```

Pokazuje wpisy listy kontroli dostępu wprost na folderze, razem z flagami dziedziczenia w nawiasach obok każdego konta.

Przykład:

```
D:\Dane\Ksiegowosc ZIELONA\DL_Ksiegowosc_RW:(OI)(CI)(M)
                   ZIELONA\DL_Ksiegowosc_RO:(OI)(CI)(RX)
                   BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files
```

NTFS = New Technology File System: system plików Windows z wbudowanymi uprawnieniami ACL na poziomie pliku i folderu

ZMIENIA SYSTEM

Nadanie uprawnienia NTFS z dziedziczeniem: icacls /grant

```
icacls "SciezkaFolderu" /grant "NazwaGrupy:(OI)(CI)M"
```

> (gdzie `(OI)` to Object Inherit, `(CI)` to Container Inherit, a `M` to skrót nadawanego uprawnienia, tu Modify)

Flagi `(OI)(CI)` razem sprawiają, że uprawnienie spływa też na wszystkie podfoldery i pliki utworzone w środku po nadaniu go, nie tylko na sam folder, na którym stoimy. Bez nich nowy plik dorzucony do folderu tydzień później dostanie inne uprawnienia niż reszta.

NTFS = New Technology File System: system plików Windows z wbudowanymi uprawnieniami ACL na poziomie pliku i folderu · **CI** = Continuous Integration: automatyczne budowanie i testowanie kodu po każdej zmianie; w ITIL także configuration item, czyli element konfiguracji: każdy składnik usługi zapisany w CMDB

TYLKO ODCZYT

Odczyt uprawnień przez PowerShell: Get-Acl

```
Get-Acl -Path "SciezkaFolderu" | Format-List
```

Zwraca ten sam komplet uprawnień co `icacls`, ale jako obiekt PowerShella, wygodny do porównywania skryptem albo do skopiowania na inny folder przez `Set-Acl`.

ZMIENIA SYSTEM

Zapis uprawnień przez PowerShell: Set-Acl

```
Set-Acl -Path "SciezkaFolderu" -AclObject $AclDoSkopiowania
```

Najczęściej łączymy z wcześniejszym `Get-Acl` na innym, już poprawnie skonfigurowanym folderze, żeby skopiować gotowy komplet uprawnień zamiast klikać go ręcznie w każdym nowym miejscu.

ZMIENIA SYSTEM

Ukrycie niedostępnych elementów: Set-SmbShare -FolderEnumerationMode

```
Set-SmbShare -Name "NazwaUdzialu" -FolderEnumerationMode AccessBased
```

Włącza Access-Based Enumeration na już istniejącym udziale. Domyślnie po utworzeniu udziału ten tryb jest wyłączony, więc każdy zalogowany użytkownik widzi wszystkie podfoldery udziału, nawet te, do których nie ma żadnego prawa.

TYLKO ODCZYT

Podgląd otwartych plików na udziale: Get-SmbOpenFile

```
Get-SmbOpenFile
```

Przykład:

```
FileId SessionId Path                                ClientComputerName ClientUserName
------ --------- ----                                ------------------ --------------
17     3         D:\Dane\Ksiegowosc\Faktury2026.xlsx   10.20.20.54
ZIELONA\halina.kowalska
```

ZMIENIA SYSTEM

Zamknięcie otwartego pliku: Close-SmbOpenFile

```
Close-SmbOpenFile -FileId NumerFileId -SessionId NumerSessionId -Force
```

Przydatne, kiedy plik został otwarty na udziale i zablokowany, a osoba, która go otworzyła, już dawno wyszła z biura albo ma zawieszoną aplikację.

Z życia wzięte

Z ŻYCIA WZIĘTE

Piątek, 15:40, dwa dni przed zamknięciem miesiąca. Pani Halina prosi Tomka o pilny dostęp do zapisu w folderze Wspólne dla nowej praktykantki z księgowości. Tomek nadaje jej grupie `Full` na poziomie udziału przez `Grant-SmbShareAccess` i uznaje sprawę za załatwioną, ale praktykantka wciąż dostaje błąd przy zapisie pliku. Dopiero po telefonie do drugiego administratora Tomek przypomina sobie, że na poziomie NTFS ten folder wciąż ma dla jej grupy tylko odczyt, a przy udziale i NTFS liczy się zawsze bardziej restrykcyjne z dwóch.

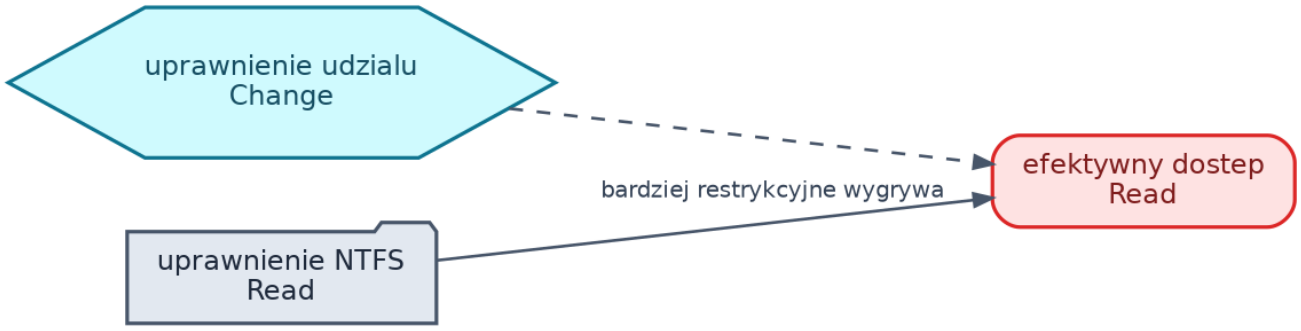
Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: uprawnienia udziału (share permissions). Osobny komplet uprawnień, który dotyczy wyłącznie dostępu przez sieć, do konkretnej ścieżki sieciowej w postaci `\\NazwaSerwera\NazwaUdzialu`. Ustawiamy je przez `New-SmbShare`, `Grant-SmbShareAccess` albo kartę Udostępnianie we właściwościach folderu.

Pojęcie: uprawnienia NTFS. Komplet uprawnień zapisany bezpośrednio w systemie plików, na samym folderze i jego zawartości, niezależnie od tego, czy ktoś dociera do niego przez sieć, czy loguje się lokalnie na serwer. Ustawiamy je przez `icacls`, `Get-Acl` / `Set-Acl` albo kartę Zabezpieczenia.

Z tego, że istnieją dwa niezależne komplety uprawnień, wynika reguła, która najczęściej zaskakuje: przy dostępie przez sieć liczy się zawsze bardziej restrykcyjne z dwóch. Użytkownik z `Full Control` na udziale i `Read` na NTFS w praktyce tylko czyta. Użytkownik z `Read` na udziale i `Full Control` na NTFS też tylko czyta, bo udział go dalej nie wpuści.



Uprawnienie udziału razem z uprawnieniem NTFS: efektywny dostęp to zawsze ich przecięcie, nie suma (kliknięcie otwiera pełny rozmiar)

Pojęcie: dziedziczenie (inheritance). Mechanizm, dzięki któremu uprawnienie nadane na folderze nadrzędnym automatycznie obejmuje też podfoldery i pliki utworzone w nim później, bez ręcznego powtarzania wpisu w każdym miejscu. Flagi `(OI)` i `(CI)` w `icacls` włączają dziedziczenie osobno dla plików i osobno dla podfolderów.

Pojęcie: jawna odmowa (explicit deny). Wpis ACL mówiący wprost, że danemu kontu czy grupie czegoś nie wolno, w odróżnieniu od zwykłego braku wpisu zezwalającego. Jawna odmowa wygrywa zawsze, niezależnie od tego, ile innych grup danej osoby ma gdzie indziej `Allow`, dlatego stawiamy ją tylko wtedy, gdy naprawdę nie ma innego sposobu wykluczenia jednej osoby z szerszej grupy.

Pojęcie: właściciel (owner). Konto albo grupa zapisana w ACL jako twórca obiektu, z prawem zmiany uprawnień nawet wtedy, gdy sam sobie odbierze dostęp do odczytu. Domyślnym właścicielem nowego folderu jest konto, które go utworzyło, ale grupa `BUILTIN\Administrators` zawsze może przejąć własność z powrotem poleceniem `takeown` albo przez `icacls /setowner`.

Pojęcie: model AGDLP. Kolejność zagnieżdżania kont w grupach przy nadawaniu uprawnień w domenie: konta użytkowników (**A**ccount) trafiają do grupy globalnej (**G**lobal), grupa globalna trafia do grupy lokalnej domeny (**D**omain **L**ocal), a dopiero grupie lokalnej domeny nadajemy uprawnienie (**P**ermission) na zasobie. W Zielonej konto `halina.kowalska` trafia do `GG_Ksiegowosc`, `GG_Ksiegowosc` trafia do `DL_Ksiegowosc_RW`, a to `DL_Ksiegowosc_RW` stoi w ACL folderu `\\fs01\Ksiegowosc`.



Model AGDLP na przykładzie księgowości Zielonej: konto w grupie globalnej, grupa globalna w grupie lokalnej domeny, uprawnienie na zasobie (kliknięcie otwiera pełny rozmiar)

Sens tego zagnieżdżenia widać przy zmianie zespołu: kiedy pani Halina przechodzi z magazynu do księgowości, wystarczy zmienić jej członkostwo w grupach globalnych, bez dotykania ani jednego ACL na żadnym serwerze plików. Gdyby uprawnienia stały wprost na koncie użytkownika, każda taka zmiana wymagałaby przeszukania wszystkich udziałów w firmie.

> **Pojęcie: Access-Based Enumeration (ABE).** Tryb udziału, w którym użytkownik w ogóle nie widzi w oknie Eksploratora plików i folderów, do których nie ma żadnego prawa dostępu, zamiast widzieć je i dostawać odmowę dopiero po kliknięciu. Włączamy go przez `Set-SmbShare -FolderEnumerationMode AccessBased`, zwykle na udziałach zbiorczych typu `\\fs01\Wspolne`, gdzie różne działy mają w środku własne podfoldery.

Krótko o DFS Namespaces: gdy udziałów działowych robi się więcej niż kilka i leżą na różnych serwerach, Distributed File System pozwala złożyć je pod jedną wspólną ścieżką, w Zielonej `\\ad.zielona.example\pliki`, tak że użytkownik nie musi wiedzieć, na którym fizycznie serwerze leży dany folder. Przestrzeń nazw Zielonej, jej foldery i cele opisuje strona fs01 od środka: maszyna na hvclu01, wolumeny, udziały działów i przestrzeń nazw DFS.

Częste błędy

Objaw	Przyczyna	Co robimy
Użytkownik ma `Full Control` na udziale, a i tak nie może zapisać pliku	uprawnienia NTFS na folderze są bardziej restrykcyjne niż uprawnienia udziału	sprawdzamy `icacls` albo `Get-Acl` na folderze, nie tylko `Get-SmbShareAccess` na udziale
Nowy plik w folderze ma inne uprawnienia niż reszta zawartości	uprawnienie nadane `icacls /grant` bez flag `(OI)(CI)`	powtarzamy `/grant` z pełnym zapisem `(OI)(CI)Uprawnienie`, tak żeby objęło też przyszłą zawartość

Objaw	Przyczyna	Co robimy
Użytkownik będący w kilku grupach nie ma dostępu, mimo że jedna z grup ma `Allow`	w ACL stoi jawna odmowa dla innej grupy, do której też należy	szukamy wpisu `Deny` przez `icacls` na całej ścieżce w górę drzewa katalogów, nie tylko na docelowym folderze
Użytkownik widzi w Eksploratorze foldery innych działów, choć nie ma do nich dostępu	Access-Based Enumeration wyłączone na udziale	włączamy `Set-SmbShare -FolderEnumerationMode AccessBased`
Zmiana uprawnień NTFS nie daje żadnego efektu dla dostępu przez sieć	udział wciąż ma dla tej samej grupy uprawnienie `Read`, mimo zmiany na NTFS	sprawdzamy oba komplety naraz, `Get-SmbShareAccess` i `icacls`, i podnosimy ten, który jest niżej

Ćwiczenia

1. Grupa `DL_Magazyn_RO` ma na udziale `\\fs01\Magazyn` uprawnienie `Change`, a na samym folderze na dysku, w NTFS, tylko `Read`. Jaki efektywny dostęp będzie mieć użytkownik z tej grupy, łączący się przez sieć?

Odpowiedź

Tylko odczyt. Przy dostępie przez sieć liczy się zawsze bardziej restrykcyjne z dwóch kompletów uprawnień, udziału i NTFS. Nazwa grupy `DL_Magazyn_RO` sugeruje zresztą, że taki stan jest zamierzony, tylko uprawnienie udziału zostało nadane przez pomyłkę zbyt szeroko.

1. Dlaczego w modelu AGDLP uprawnienie do folderu nadajemy grupie lokalnej domeny, a nie od razu grupie globalnej, skoro grupa globalna i tak trafia do grupy lokalnej domeny?

Odpowiedź

Bo grupa lokalna domeny reprezentuje sam zasób (konkretny udział, konkretne uprawnienie), a grupa globalna reprezentuje zespół ludzi, niezależnie od tego, do jakich zasobów akurat ma dostęp. Rozdzielenie tych dwóch warstw pozwala dodać zespołowi dostęp do nowego zasobu jedną zmianą w grupie lokalnej domeny, bez ruszania definicji samego zespołu, i odwrotnie: zmienić skład zespołu bez dotykania żadnego ACL.

Powiązane: fs01 od środka: maszyna na hvclu01, wolumeny, udziały działów i przestrzeń nazw DFS · Audyt dostępu do plików na fs01 i kwartalny przegląd uprawnień z właścicielami działów · Skrypty audytowe Active Directory · Storage Spaces i warstwy magazynu · Wolumeny współdzielone klastra (CSV)

Źródła: New-SmbShare, PowerShell SmbShare module, Microsoft Learn · Grant-SmbShareAccess, PowerShell SmbShare module, Microsoft Learn · Set-SmbShare, PowerShell SmbShare module, Microsoft Learn · Get-SmbOpenFile, PowerShell SmbShare module, Microsoft Learn · Close-SmbOpenFile, PowerShell SmbShare module, Microsoft Learn · icacls, Windows Commands, Microsoft Learn · Active Directory security groups, Microsoft Learn

Serwer wydruku i drukarki z GPO

Poziom: podstawy **Dotyczy: Windows Server 2019+ (rola Print Services), Windows 10/11**

Czas: ~25 min

Serwer wydruku instaluje drukarkę raz, a udostępnia ją całej firmie, zamiast każdego komputera z osobna. Uczymy się dokładać drukarki z konsoli, wypychać je przez GPO na stacje i wiemy, dlaczego zwykły użytkownik od kilku lat sam już nie zainstaluje sterownika. Tu wracamy, kiedy ktoś w firmie nie może wydrukować albo prosi o nową drukarkę na dziale.

ZAŁOŻENIA SCENARIUSZA

magazyn jest w sieci centrali (VLAN 30 za `fw01`), więc serwer wydruku w VLAN 10 drukuje na drukarkę etykiet 10.20.30.81 bezpośrednio przez `fw01`, a rezerwacje adresów obsługują `dc01` i `dc02` (patrz DHCP: adresy dla biura i magazynu z przełączaniem awaryjnym). Przy osobnej lokalizacji ruch do drukarki idzie tunelem do `rtr-mag01`: IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy.

Skróty użyte na tej stronie (6)

Skrót	Co znaczy
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
TCP/IP	zestaw protokołów internetu: IP przenosi pakiety między adresami, TCP pilnuje, żeby dane doszły w całości i w kolejności
UNC	Upper Non-Critical: górny próg ostrzegawczy czujnika w BMC
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie

Fiszka

◫◫ ZMIENIA SYSTEM

Instalacja roli serwera wydruku: Install-WindowsFeature

```
Install-WindowsFeature -Name Print-Services -IncludeManagementTools
```

Dokłada na serwerze rolę Print Services razem z konsolą zarządzania drukowaniem. Bez tej roli serwer wciąż może udostępniać pojedynczą drukarkę, ale nie zobaczymy jej w jednym miejscu razem z resztą floty.

◫◫ ZMIENIA SYSTEM

Dodanie sterownika drukarki: Add-PrinterDriver

```
Add-PrinterDriver -Name "NazwaSterownika"
```

Instaluje na serwerze sterownik, który musi już być wcześniej dostarczony do magazynu sterowników Windows (przez `pnputil` albo Windows Update). Nazwę sterownika sprawdzamy wcześniej poleceniem `Get-PrinterDriver` na komputerze, który tę samą drukarkę ma już zainstalowaną lokalnie.

Przykład:

```
Add-PrinterDriver -Name "HP Universal Printing PCL 6"
```

◫◫ ZMIENIA SYSTEM

Dodanie portu drukarki: Add-PrinterPort

```
Add-PrinterPort -Name "NazwaPortu" -PrinterHostAddress "AdresIpDrukarki"
```

Tworzy standardowy port TCP/IP wskazujący na adres sieciowy fizycznej drukarki. Serwer wydruku łączy się przez ten port, kiedy faktycznie wysyła zadanie do urządzenia.

Przykład:

```
Add-PrinterPort -Name "IP_10.20.20.71" -PrinterHostAddress "10.20.20.71"
```

◫◫ **TCP/IP** = zestaw protokołów internetu: IP przenosi pakiety między adresami, TCP pilnuje, żeby dane doszły w całości i w kolejności

◫◫ ZMIENIA SYSTEM

Dodanie i udostępnienie drukarki: Add-Printer -Shared

```
Add-Printer -Name "NazwaDrukarki" -DriverName "NazwaSterownika" -PortName "NazwaPortu" -Shared -ShareName "NazwaUdostepnienia"
```

Łączy sterownik i port w jedną widoczną drukarkę i od razu udostępnia ją w sieci pod podaną nazwą. Bez `-Shared` drukarka istnieje tylko lokalnie na serwerze, niewidoczna dla innych komputerów.

Przykład:

```
Add-Printer -Name "Ksiegowosc-Faktury" -DriverName "HP Universal Printing PCL 6" -PortName "IP_10.20.20.71" -Shared -ShareName "Ksiegowosc-Faktury"
```

◫◫ TYLKO ODCZYT

Lista drukarek na serwerze: Get-Printer

```
Get-Printer
```

Przykład:

```
Name                ComputerName DriverName                    PortName    Shared
----                ------------ ----------                    --------    ------
Ksiegowosc-Faktury               HP Universal Printing PCL 6    IP_10.20.20.71 True
Magazyn-Etykiety                 Zebra ZPL Driver              IP_10.20.30.81 True
```

◫◫ TYLKO ODCZYT

Lista zadań w kolejce drukarki: Get-PrintJob

```
Get-PrintJob -PrinterName "NazwaDrukarki"
```

Przykład:

```
Id DocumentName          SubmittedTime          JobStatus     UserName
-- ------------          -------------          ---------     --------
```

```
41 Faktura_2026_09_0182   28.09.2026 14:02:11    Printing      ZIELONA\halina.kowalska
42 Faktura_2026_09_0183   28.09.2026 14:02:19    Paused        ZIELONA\halina.kowalska
```

◫◫ OSTROŻNIE · NIEODWRACALNE

Usunięcie zawieszonego zadania: Remove-PrintJob

```
Remove-PrintJob -PrinterName "NazwaDrukarki" -ID NumerZadania
```

Usuwa jedno konkretne zadanie z kolejki, na przykład zawieszone po zniknięciu drukarki z sieci w trakcie druku.

◫◫ ZMIENIA SYSTEM

Restart usługi bufora wydruku: Restart-Service Spooler

```
Restart-Service -Name Spooler -Force
```

Zatrzymuje i uruchamia ponownie usługę Print Spooler. Typowe lekarstwo, kiedy kolejka drukarki utknęła na jednym zadaniu i żadne inne zadanie nie chce ruszyć dalej, nawet po usunięciu tego zawieszonego.

◫◫ TYLKO ODCZYT

Wdrożenie drukarki przez GPO

Preferencje zasad grupy wypychają gotową, udostępnioną drukarkę na stacje robocze bez logowania się na każdą z osobna:

```
Edytor zarządzania zasadami grupy
  → Konfiguracja użytkownika
  → Preferencje
  → Ustawienia Panelu sterowania
  → Drukarki
  → Nowa → Drukarka udostępniona
```

W polu Ścieżka UNC wpisujemy pełną ścieżkę sieciową drukarki, na przykład `\\fs01\Ksiegowosc-Faktury`, a w zakładce Wspólne warto włączyć docelowanie na poziomie

elementu, żeby ta sama polityka rozdzielała różne drukarki do różnych grup zabezpieczeń.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **UNC** = Upper Non-Critical: górny próg ostrzegawczy czujnika w BMC

Z życia wzięte

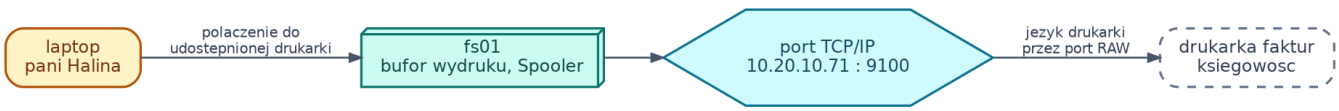
Z ŻYCIA WZIĘTE

Poniedziałek, 6:10 rano, start zmiany w Swarzędzu. Marek dzwoni, że nie może wydrukować etykiet wysyłkowych, choć wczoraj wieczorem wszystko działało. Okazuje się, że drukarka etykiet dostała w nocy nowy adres z serwera DHCP, bo rezerwacja adresu wygasła po awarii `dc01`, a port TCP/IP na serwerze wydruku wciąż wskazuje na stary adres. Po dodaniu trwałej rezerwacji w DHCP i poprawieniu adresu w `Add-PrinterPort` etykiety znowu się drukują, a Marek ma jeszcze pół godziny zapasu przed pierwszą wysyłką.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: serwer wydruku. Komputer albo serwer, na którym stoi rola Print Services, trzymająca sterowniki i kolejki wszystkich udostępnionych drukarek w firmie w jednym miejscu. Stacja robocza łączy się do drukarki przez ten serwer, zamiast łączyć się bezpośrednio do fizycznego urządzenia w sieci.



Droga zadania wydruku: laptop łączy się do udziału drukarki na serwerze, serwer wysyła dane przez port TCP/IP do fizycznej drukarki (kliknięcie otwiera pełny rozmiar)

Ta sama trasa działa też bez osobnego serwera wydruku: stacja robocza może połączyć się bezpośrednio do drukarki po adresie IP, sama trzymając sterownik i kolejkę lokalnie. W Zielonej wybieramy serwer wydruku tam, gdzie z jednej drukarki korzysta więcej niż kilka osób, żeby aktualizacja sterownika wymagała jednej zmiany na serwerze, a nie osobnej wizyty przy każdym komputerze.

> **Pojęcie: Point and Print.** Mechanizm, dzięki któremu stacja robocza, łącząc się po raz pierwszy do udostępnionej drukarki na serwerze, sama pobiera od niego brakujący sterownik, zamiast prosić osobę przy komputerze o ręczną instalację. Przez wiele lat Point and Print pozwalał na to każdemu zalogowanemu użytkownikowi, bez podnoszenia uprawnień.

Luka PrintNightmare (`CVE-2021-34527`) pokazała, że ten sam mechanizm dawał się wykorzystać do zdalnego uruchomienia dowolnego kodu z uprawnieniami systemowymi, bo stacja ufała sterownikowi z serwera bez dodatkowej weryfikacji. Microsoft odpowiedział aktualizacjami z lipca i sierpnia 2021 roku, opisanymi w biuletynie `KB5005010`, które trwale zmieniły domyślne zachowanie Windows w tym miejscu.

> **Pojęcie: Point and Print Restrictions.** Zasada grupy (`Computer Configuration → Administrative Templates → Printers → Point and Print Restrictions`) kontrolująca, czy i kiedy stacja robocza może pobrać albo zaktualizować sterownik drukarki od serwera bez podnoszenia uprawnień do administratora. Od aktualizacji z sierpnia 2021 roku o ostatecznym zachowaniu decyduje jednak osobny wpis rejestru, który nadpisuje tę zasadę.
>
> **Pojęcie: RestrictDriverInstallationToAdministrators.** Wartość rejestru `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint\RestrictDriverInstallationToAdministrators`, domyślnie ustawiona na `1` od aktualizacji z sierpnia 2021 roku. Ustawiona na `1`, wymusza uprawnienia administratora przy instalacji dowolnego sterownika drukarki, sygnowanego czy nie, i to niezależnie od tego, co mówi zasada Point and Print Restrictions.

Dla zwykłego użytkownika w Zielonej oznacza to, że pierwsze podłączenie do już wcześniej znanej, zaktualizowanej drukarki działa bez pytania, bo sterownik trafił na stację wcześniej przez GPO albo Windows Update. Ale zupełnie nowa drukarka, z nowym sterownikiem, którego stacja jeszcze nie zna, wymaga dziś podniesienia uprawnień, więc instalujemy ją przez serwer wydruku i wdrożenie GPO opisane w Fiszce, nie licząc na to, że pracownik zrobi to sam przy swoim koncie.

Częste błędy

Objaw	Przyczyna	Co robimy
Zadania w kolejce stoją, żadne nie drukuje się dalej	usługa Print Spooler zawiesiła się na jednym uszkodzonym zadaniu	`Remove-PrintJob` na zawieszonym zadaniu, w razie potrzeby `Restart-Service Spooler -Force`
Etykiety albo faktury drukują się na złej drukarce po restarcie sieci	drukarka dostała z DHCP inny adres IP niż ten w `Add-PrinterPort`	ustawiamy trwałą rezerwację adresu w DHCP dla adresu MAC drukarki, poprawiamy port na aktualny adres
Stacja robocza pyta o hasło administratora przy podłączaniu znanej od dawna drukarki	`RestrictDriverInstallationToAdministrators` ustawione na `1` blokuje też aktualizację już istniejącego sterownika	aktualizujemy sterownik na serwerze wydruku i wypychamy go GPO, zamiast liczyć na samodzielną instalację przez użytkownika
Nowa drukarka nie pojawia się na stacjach mimo wdrożonego GPO	preferencja GPO wskazuje złą ścieżkę UNC albo docelowanie na poziomie elementu wyklucza tę grupę użytkowników	sprawdzamy ścieżkę UNC w preferencji i wynik `gpresult /r` na stacji testowej
`Add-Printer -Shared` kończy się błędem o braku sterownika	sterownik nie został wcześniej dodany przez `Add-PrinterDriver`	sprawdzamy `Get-PrinterDriver`, w razie braku dokładamy sterownik, dopiero potem tworzymy drukarkę

□□ Ćwiczenia

1. Marek zgłasza, że drukarka etykiet w Swarzędzu działała wieczorem, a rano przestała. Jakie są dwie najbardziej prawdopodobne przyczyny do sprawdzenia w pierwszej kolejności, zanim zaczniemy grzebać w sterownikach?

Odpowiedź

Po pierwsze zawieszone zadanie w kolejce blokujące usługę Print Spooler, sprawdzane przez `Get-PrintJob` i naprawiane `Remove-PrintJob` albo restartem usługi. Po drugie zmiana adresu IP drukarki po stronie DHCP, jeśli adres nie ma trwałej rezerwacji, sprawdzana przez porównanie adresu w `Add-PrinterPort` z aktualnym adresem urządzenia.

1. Dlaczego po aktualizacjach z sierpnia 2021 roku zwykły użytkownik w firmie bez zmiany żadnej zasady GPO i tak nie zainstaluje już samodzielnie nowego, nieznanego sterownika drukarki?

Odpowiedź

Bo od tamtych aktualizacji o tym decyduje domyślnie ustawiona na `1` wartość rejestru `RestrictDriverInstallationToAdministrators`, która nadpisuje zasadę Point and Print Restrictions i wymaga uprawnień administratora przy instalacji każdego sterownika, niezależnie od tego, czy administrator w ogóle skonfigurował jakąkolwiek zasadę GPO dotyczącą drukowania.

Powiązane: Diagnostyka systemu · Skrypty audytowe Active Directory

Źródła: Add-PrinterDriver, PowerShell PrintManagement module, Microsoft Learn · Add-PrinterPort, PowerShell PrintManagement module, Microsoft Learn · Add-Printer, PowerShell PrintManagement module, Microsoft Learn · KB5005010: Restricting installation of new printer drivers, Microsoft Support · KB5005652: Manage new Point and Print default driver installation behavior (CVE-2021-34481), Microsoft Support