Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt

Poziom: zaawansowany

Dotyczy: Active Directory na dc01, dc02 i dc03 (propozycja), Windows Server 2022 i 2025, Windows 11, Protected Users, gMSA i dMSA, NTLM, Kerberos, LDAP, SMB, Graylog, PingCastle, Purple Knight

Czas: ~60 min

Kto przejmie Active Directory, przejmuje całą firmę: pocztę, pliki, kopie i wszystkie serwery, które ufają domenie. Ta strona zbiera to, co w Zielonej robimy, żeby to przejęcie było trudne: rozdzielamy konta i maszyny na warstwy, pilnujemy kont uprzywilejowanych, wyłączamy stare protokoły, wysyłamy zdarzenia do Grayloga i raz na kwartał sprawdzamy domenę narzędziem z zewnątrz. Wracamy tu przy każdym nowym koncie administracyjnym, po każdym Patch Tuesday z poprawkami dla kontrolerów i przed wizytą audytora.

Skróty użyte na tej stronie (27)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
AES	Advanced Encryption Standard: powszechny szyfr blokowy, którym szyfrują dane karty DESFire i wiele innych systemów, w naszych przykładach z kluczem 128 bitów
dMSA	delegated Managed Service Account: rodzaj konta usługowego z Windows Server 2025, który przejmuje rolę istniejącego konta usługi; luka BadSuccessor załatana w sierpniu 2025
EAP-TLS	EAP z TLS: uwierzytelnianie certyfikatem użytkownika albo urządzenia zamiast hasła
GB	Gigabyte: miliard bajtów, jednostka pojemności pamięci i plików, tu najczęściej rozmiar modelu albo pamięci karty graficznej

Skrót	Co znaczy
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
gMSA	group Managed Service Account: konto usługi, któremu Windows sam zmienia hasło
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
IAKerb	Initial and Pass Through Authentication Using Kerberos: rozszerzenie, w którym serwer pośredniczy w logowaniu Kerberos klienta bez bezpośredniego dostępu do kontrolera; jeden z zamienników NTLM
KDC	Key Distribution Center: serwer Kerberosa wydający bilety logowania
KDCSVC	nazwa usługi centrum dystrybucji kluczy Kerberos na kontrolerze domeny, źródło zdarzeń 201 do 209 o użyciu RC4
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
LDAPS	LDAP szyfrowany TLS, zwykle port 636
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol w wersji 2: metoda sprawdzania hasła w sieci, używana wewnątrz PEAP
NTLM	NT LAN Manager: starszy od Kerberos sposób logowania w sieciach Windows przez wyzwanie i odpowiedź, podatny na przekazywanie i użycie skrótu hasła; Microsoft zapowiedział jego domyślne wyłączenie
NTLMv1	pierwsza wersja NTLM, łamana w godzinach; usunięta z Windows 11 24H2 i Windows Server 2025
PAW	Privileged Access Workstation: osobna stacja administracyjna bez poczty i przeglądarki internetowej, z której zarządzamy kontrolerami i serwerami
RC4	stary szyfr strumieniowy, używany kiedyś w biletach Kerberos; od 2026 roku domyślnie zastępowany przez AES
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy
SMBv1	pierwsza wersja protokołu udostępniania plików Windows, bez szyfrowania i z poważnymi lukami; nie instaluje się domyślnie od Windows 10 1709 i Windows Server 2019
SPN	Service Principal Name: nazwa usługi zapisana na koncie w AD, po której Kerberos wie, dla jakiego konta wydać bilet do tej usługi
TGT	Ticket Granting Ticket: główny bilet Kerberos wydawany przez kontroler domeny po zalogowaniu, na jego podstawie komputer dostaje bilety do konkretnych usług
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii

Skrót	Co znaczy
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Komendy wykonujemy w PowerShellu z modułem `ActiveDirectory`, kontem administracyjnym warstwy 0 (`nazwa_usera.t0`), z osobnej stacji administracyjnej, a nie ze zwykłego komputera biurowego. Odczyty działają z każdego konta domenowego z prawem odczytu katalogu.

TYLKO ODCZYT

Lista członków grup uprzywilejowanych: Get-ADGroupMember -Recursive

```
"Domain Admins","Enterprise Admins","Schema Admins","Administrators","Account
Operators","Backup Operators","Server Operators","DnsAdmins" | ForEach-Object {
    $grupa = $_
    Get-ADGroupMember -Identity $grupa -Recursive | Select-Object
@{n='Grupa';e={$grupa}}, SamAccountName, objectClass
}
```

Rozwija grupy zagnieżdżone, więc pokazuje każdego, kto naprawdę ma uprawnienia, także przez grupę w grupie. Wynik porównujemy co miesiąc z listą zatwierdzoną w GLPI.

Przykład:

```
Grupa             SamAccountName       objectClass
-----             --------------       -----------
Domain Admins     Administrator        user
Domain Admins     jan.kowalski.t0      user
Enterprise Admins Administrator        user
Backup Operators  svc-stary-backup     user
DnsAdmins         jan.kowalski.t0      user
```

Wiersz `svc-stary-backup` w Backup Operators to konto po starym programie kopii: członkowie tej grupy mogą zrobić kopię bazy katalogu z kontrolera, więc konto trafia do wyłączenia.

□□ **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

□□ TYLKO ODCZYT

Konta oznaczone jako uprzywilejowane: Get-ADUser -Filter adminCount

```
Get-ADUser -Filter 'adminCount -eq 1' -Properties adminCount, LastLogonDate,
PasswordLastSet, Enabled | Select-Object SamAccountName, Enabled, LastLogonDate,
PasswordLastSet
```

Atrybut `adminCount` dostaje każde konto, które kiedykolwiek było w grupie chronionej. Po usunięciu z grupy atrybut zostaje, więc lista pokazuje też byłych administratorów, którym trzeba przejrzeć uprawnienia.

□□ ZMIENIA SYSTEM

Dodanie konta do Protected Users: Add-ADGroupMember

```
Add-ADGroupMember -Identity "Protected Users" -Members nazwa_usera.t0
```

Konto w Protected Users loguje się tylko przez Kerberos z AES, bez NTLM, bez delegowania i bez poświadczeń zapisanych w pamięci podręcznej, a jego bilet TGT żyje 4 godziny. Dodajemy najpierw jedno konto i sprawdzamy przez dzień, czy wszystko działa.

□□ **AES** = Advanced Encryption Standard: powszechny szyfr blokowy, którym szyfrują dane karty DESFire i wiele innych systemów, w naszych przykładach z kluczem 128 bitów · **NTLM** = NT LAN Manager: starszy od Kerberos sposób logowania w sieciach Windows przez wyzwanie i odpowiedź, podatny na przekazywanie i użycie skrótu hasła; Microsoft zapowiedział jego domyślne wyłączenie · **TGT** = Ticket Granting Ticket: główny bilet Kerberos wydawany przez kontroler domeny po zalogowaniu, na jego podstawie komputer dostaje bilety do konkretnych usług

□□ ZMIENIA SYSTEM

Zablokowanie delegowania konta: Set-ADUser -AccountNotDelegated

```
Set-ADUser -Identity nazwa_usera.t0 -AccountNotDelegated $true
```

Ustawia flagę „Konto jest poufne i nie może być delegowane”. Dla kont warstwy 0 robimy to zawsze, także gdy są w Protected Users, bo flaga działa również na kontrolerach starszych

niż Windows Server 2012 R2 i w scenariuszach, których Protected Users nie obejmuje.

ZMIENIA SYSTEM

Czasowe uprawnienia administratora domeny: Add-ADGroupMember -MemberTimeToLive

```
Add-ADGroupMember -Identity "Domain Admins" -Members nazwa_usera.t0 -MemberTimeToLive
(New-TimeSpan -Hours LiczbaGodzin)
```

Privileged Access Management jest w lesie Zielonej włączony, więc członkostwo w Domain Admins może wygasnąć samo. Na co dzień konta `.t0` nie są w Domain Admins, tylko w grupach z wąsko delegowanymi prawami; do pracy, która naprawdę wymaga Domain Admins, dostają członkostwo na kilka godzin. Bilet Kerberos jest wtedy ważny najwyżej do końca członkostwa. Mechanizm opisuje strona Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu.

TYLKO ODCZYT

Konta z SPN, podatne na Kerberoasting: Get-ADUser -Filter ServicePrincipalName

```
Get-ADUser -Filter 'ServicePrincipalName -like "*"' -Properties ServicePrincipalName,
PasswordLastSet, 'msDS-SupportedEncryptionTypes' | Select-Object SamAccountName,
PasswordLastSet, 'msDS-SupportedEncryptionTypes', ServicePrincipalName
```

Każde zwykłe konto użytkownika z nazwą usługi (SPN) jest celem: dowolny użytkownik domeny może poprosić o bilet do tej usługi i łamać hasło offline. Takie konta zamieniamy na gMSA albo dajemy im hasło dłuższe niż 25 znaków i szyfrowanie AES.

Przykład:

```
SamAccountName PasswordLastSet      msDS-SupportedEncryptionTypes ServicePrincipalName
-------------- ---------------      ----------------------------- --------------------
krbtgt         14.03.2024 10:12:40                                {kadmin/changepw}
svc-optima     02.02.2019 09:00:11
{MSSQLSvc/sql01.ad.zielona.example:1433}
```

`krbtgt` jest na liście zawsze. `svc-optima` z hasłem z 2019 roku i bez ustawionych typów szyfrowania to pierwszy kandydat do zamiany na gMSA.

SPN = Service Principal Name: nazwa usługi zapisana na koncie w AD, po której Kerberos wie, dla jakiego konta wydać bilet do tej usługi · **gMSA** = group Managed Service Account: konto usługi, któremu Windows sam zmienia hasło · **AES** = Advanced Encryption Standard: powszechny szyfr blokowy, którym szyfrują dane karty DESFire i wiele innych systemów, w naszych przykładach z kluczem 128 bitów

TYLKO ODCZYT

Komputery z delegowaniem bez ograniczeń: Get-ADComputer -Filter TrustedForDelegation

```
Get-ADComputer -Filter 'TrustedForDelegation -eq $true -and PrimaryGroupID -ne 516' -
Properties TrustedForDelegation | Select-Object Name
```

Delegowanie bez ograniczeń pozwala serwerowi działać w imieniu każdego, kto się do niego zaloguje, także administratora domeny. Kontrolery domeny (grupa podstawowa 516) mają je z założenia, więc je pomijamy; każdy inny wynik to serwer do przestawienia na delegowanie ograniczone.

ZMIENIA SYSTEM

Wyłączenie SMBv1 na serwerze: Set-SmbServerConfiguration

```
Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol, RequireSecuritySignature
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
Uninstall-WindowsFeature FS-SMB1
```

Pierwsze polecenie pokazuje stan, drugie wyłącza SMBv1 w usłudze serwera, trzecie usuwa składnik z systemu (wymaga restartu). Na Windows 11 to samo robi `Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`.

SMBv1 = pierwsza wersja protokołu udostępniania plików Windows, bez szyfrowania i z poważnymi lukami; nie instaluje się domyślnie od Windows 10 1709 i Windows Server 2019

TYLKO ODCZYT

Sprawdzenie blokady poświadczeń NTLMv1: reg query BlockNtlmv1SSO

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0" /v BlockNtlmv1SSO
```

Na Windows 11 24H2 i nowszym oraz Windows Server 2025 brak wartości oznacza od aktualizacji z 13 października 2026 tryb wymuszania (1). Wartość 0 to tryb audytu, ustawiany tylko czasowo, gdy coś w sieci wciąż potrzebuje MS-CHAPv2.

Przykład:

```
ERROR: The system was unable to find the specified registry key or value.
```

Komunikat o braku wartości jest tu dobrą wiadomością: obowiązuje zachowanie domyślne, czyli blokada.

NTLMv1 = pierwsza wersja NTLM, łamana w godzinach; usunięta z Windows 11 24H2 i Windows Server 2025 · **MS-CHAPv2** = Microsoft Challenge Handshake Authentication Protocol w wersji 2: metoda sprawdzania hasła w sieci, używana wewnątrz PEAP · **reg** = registry: narzędzie wiersza poleceń do odczytu i zmiany rejestru Windows, na przykład reg query · **HKLM** = HKEY_LOCAL_MACHINE: gałąź rejestru Windows z ustawieniami całego komputera, a nie pojedynczego użytkownika

TYLKO ODCZYT

Zdarzenia RC4 w Kerberos na kontrolerze: Get-WinEvent KDCSVC

```
Get-WinEvent -FilterHashtable @{LogName='System'; ProviderName='Microsoft-Windows-Kerberos-Key-Distribution-Center'; Id=201,202,203,204,205,206,207,208,209} -MaxEvents 50 -ErrorAction SilentlyContinue | Select-Object TimeCreated, Id, Message
```

Zdarzenia 201 do 209 opisują konta i klientów, którzy wciąż polegają na RC4. Od aktualizacji z kwietnia 2026 domyślne szyfrowanie kont bez ustawionego `msDS-SupportedEncryptionTypes` to wyłącznie AES; zdarzenia 203, 204, 208 i 209 oznaczają żądania już zablokowane. Nazwę dostawcy zdarzeń sprawdzamy w podglądzie zdarzeń na naszym kontrolerze, bo dokumentacja podaje skrót KDCSVC.

RC4 = stary szyfr strumieniowy, używany kiedyś w biletach Kerberos; od 2026 roku domyślnie zastępowany przez AES · **KDCSVC** = nazwa usługi centrum dystrybucji kluczy Kerberos na kontrolerze domeny, źródło zdarzeń 201 do 209 o użyciu RC4 · **AES** = Advanced Encryption Standard: powszechny szyfr blokowy, którym szyfrują dane karty DESFire i wiele innych systemów, w naszych przykładach z kluczem 128 bitów

TYLKO ODCZYT

Zdarzenia niepodpisanych połączeń LDAP: Get-WinEvent 2887 i 2889

```
Get-WinEvent -FilterHashtable @{LogName='Directory Service'; Id=2887,2889} -MaxEvents 20
| Select-Object TimeCreated, Id, Message
```

Zdarzenie 2887 to dobowe podsumowanie: ile połączeń LDAP bez podpisu przyjął kontroler. Zdarzenie 2889 z adresem i kontem klienta pojawia się po włączeniu szczegółowego dziennika poleceniem z następnej fiszki.

LDAP = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)

ZMIENIA SYSTEM

Włączenie szczegółowego dziennika LDAP: reg add 16 LDAP Interface Events

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics" /v "16 LDAP Interface
Events" /t REG_DWORD /d 2 /f
```

Na tydzień przed wymuszeniem podpisywania LDAP. Po zebraniu listy klientów wracamy do wartości 0, bo dziennik szybko rośnie.

LDAP = Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) · **reg** = registry: narzędzie wiersza poleceń do odczytu i zmiany rejestru Windows, na przykład reg query · **HKLM** = HKEY_LOCAL_MACHINE: gałąź rejestru Windows z ustawieniami całego komputera, a nie pojedynczego użytkownika

TYLKO ODCZYT

Odczyt zasad audytu: auditpol /get

```
auditpol /get /category:*
```

Pokazuje, które kategorie zaawansowanego audytu są włączone na kontrolerze. Porównujemy z tabelą w sekcji „Audyt i Graylog”.

auditpol = audit policy: odczyt i zmiana zaawansowanych zasad audytu Windows

TYLKO ODCZYT

Kontrola domeny narzędziem PingCastle: PingCastle.exe --healthcheck

```
.\PingCastle.exe --healthcheck --server NazwaDomeny
```

Uruchamiamy zwykłym kontem domenowym, z katalogu, do którego rozpakowaliśmy program pobrany ze strony producenta. Wynikiem jest raport HTML z oceną i listą reguł; licencję wersji bezpłatnej opisujemy niżej.

HTML = HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce

Z życia wzięte

Z ŻYCIA WZIĘTE

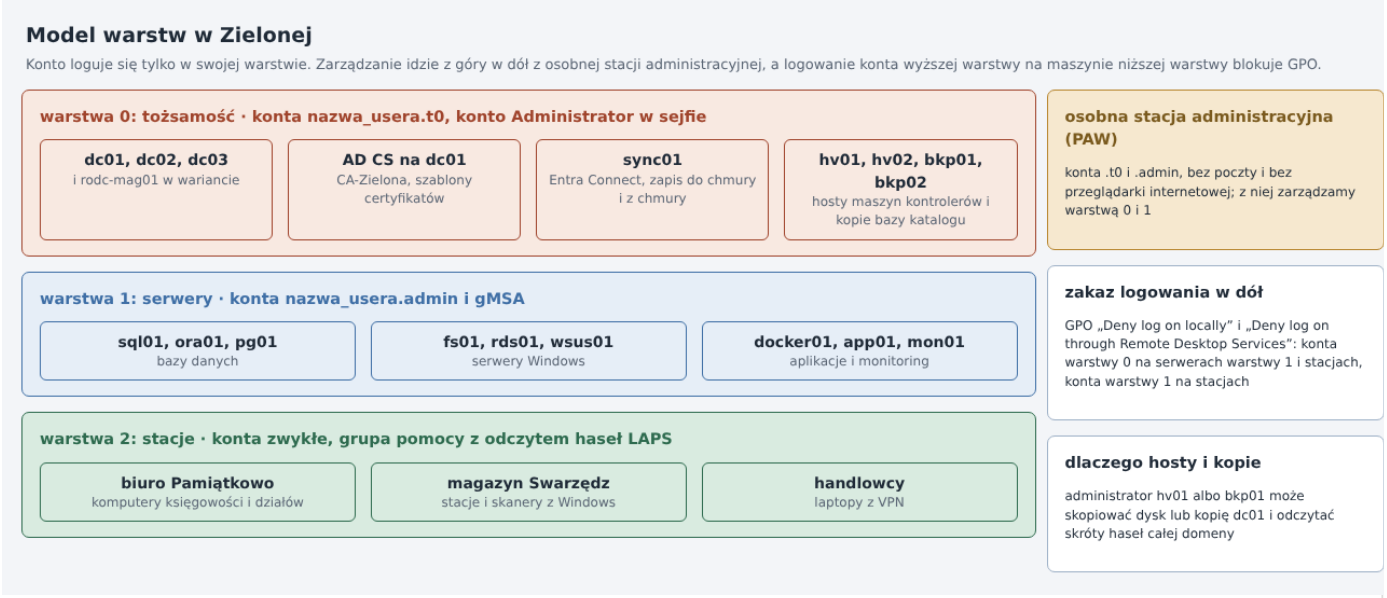
Środa, 14:00. Pan Wojtek, audytor, kładzie na stole wydruk z pytaniem: „Ile osób w firmie może jutro wyłączyć wszystkie komputery?”. Tomek liczy członków Domain Admins i dochodzi do siedmiu: dwóch administratorów, konto `Administrator`, konto programu kopii sprzed lat, Ola „na chwilę” od 2023 roku, dostawca WMS i konto `zbigniew.admin`, założone, gdy pan Zbigniew chciał sam zainstalować drukarkę. Po miesiącu na liście zostaje konto `Administrator` w sejfie, a dwa konta `.t0` dostają członkostwo tylko na czas pracy.

Jak to działa

Rozwiń: jak to działa pod spodem

Model warstw

Pojęcie: model warstw (tiering). Podział maszyn i kont według tego, jak wielką władzę dają. Konto z wyższej warstwy nigdy nie loguje się na maszynę z niższej warstwy, bo tam napastnik mógłby przechwycić jego poświadczenia. Microsoft opisuje dziś szerszy Enterprise Access Model, ale dla firmy z jedną domeną trzy klasyczne warstwy wystarczają.



Rysunek 1. Trzy warstwy Zielonej: warstwa 0 z kontrolerami, AD CS na dc01, sync01, hostami hv01 i hv02 oraz serwerami kopii; warstwa 1 z serwerami aplikacji i baz; warstwa 2 ze stacjami i laptopami; konta logują się tylko w swojej warstwie, a zarządzanie idzie z góry w dół z osobnych stacji (kliknięcie otwiera pełny rozmiar)

Warstwa	Co do niej należy w Zielonej	Konta	Gdzie wolno się logować
0: tożsamość	`dc01`, `dc02`, `dc03`, `rodc-mag01`, AD CS na `dc01` (`CA-Zielona`), docelowo urząd główny offline `ca-root01` z nośnikami jego kopii i urząd wydający `ca01`, `conn01` z Certificate Connector dla Intune, `acme01` ze step-ca (jeśli powstanie: warstwa 0 bez ograniczenia nazw, warstwa 1 z ograniczeniem do `*.zielona.example`), `sync01` z Entra Connect, `hv01` i `hv02` (na nich stoją kontrolery), `bkp01` i `bkp02` (trzymają kopie bazy katalogu), konsola zapory `fw01` z logowaniem domenowym	`nazwa_usera.t0`, konto `Administrator` w sejfie	kontrolery, serwery warstwy 0 i osobna stacja administracyjna

Warstwa	Co do niej należy w Zielonej	Konta	Gdzie wolno się logować
1: serwery	`sql01`, `ora01`, `fs01`, `docker01`, `pg01` i pozostałe serwery aplikacji	`nazwa_usera.admin`, konta gMSA	serwery warstwy 1, osobna stacja administracyjna
2: stacje	komputery biura, magazynu, laptopy handlowców, skanery z Windows	konta zwykłe, grupa pomocy z prawem odczytu LAPS	stacje i laptopy

Dwie rzeczy w tej tabeli zaskakują zawsze. Pierwsza: `hv01` i `hv02` są w warstwie 0, bo administrator hosta Hyper-V może skopiować dysk maszyny `dc01` i wyciągnąć z niego całą bazę katalogu. Druga: `bkp01` i `bkp02` są w warstwie 0 z tego samego powodu, co opisuje strona Kopia i odtwarzanie Active Directory: stan systemu, restic, kosz AD i DSRM. AD CS na kontrolerze domeny jest dopuszczalny w małej firmie, ale źle skonfigurowany szablon certyfikatu pozwala zwykłemu użytkownikowi uzyskać certyfikat administratora; szablony sprawdzamy w raporcie PingCastle i narzędziem Locksmith. Przeniesienie urzędu na osobny serwer warstwy 0 to już zaplanowana praca: projekt nowej hierarchii opisuje strona Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA, a kolejność zmian strona Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona.

Rozdział warstw egzekwujemy GPO z prawami użytkownika: „Deny log on locally” i „Deny log on through Remote Desktop Services” dla grupy kont warstwy 0 na wszystkich serwerach warstwy 1 i stacjach, a dla grupy kont warstwy 1 na stacjach. Dla dwuosobowego zespołu osobna stacja administracyjna (PAW, Privileged Access Workstation) może być jednym dodatkowym laptopem bez poczty i przeglądarki internetowej; wybór sprzętu i miejsca jest do decyzji autora.

Konta uprzywilejowane

> **Pojęcie: konto uprzywilejowane.** Konto, które może zmienić bezpieczeństwo innych kont albo maszyn: członek Domain Admins, Enterprise Admins, Schema Admins, Administrators na kontrolerze, a także Backup Operators, Server Operators, Account Operators i DnsAdmins, bo każda z tych grup daje drogę do przejęcia domeny.

Zasady w Zielonej:

1. Każdy administrator ma trzy konta: zwykłe do poczty i pracy biurowej, `.admin` do serwerów i `.t0` do warstwy 0. Hasła są różne, a konta `.t0` mają klucz sprzętowy albo

co najmniej hasło dłuższe niż 20 znaków.
2. Domain Admins jest na co dzień pusta poza wbudowanym kontem `Administrator`, którego hasło leży w sejfie i w Vaultwardenie. Konta `.t0` dostają członkostwo czasowe przez `-MemberTimeToLive`.
3. Grupy Account Operators, Server Operators, Print Operators i Backup Operators mają być puste. Nowe zadania delegujemy na jednostkach organizacyjnych, jak opisuje strona Struktura OU Zielonej i delegowanie uprawnień.
4. Zmiana członkostwa w grupie uprzywilejowanej daje zdarzenie w Graylogu i alarm w ciągu minuty.
5. Dostawca WMS i inni zewnętrzni nie mają kont w warstwie 0. Gdy potrzebują dostępu do `ora01`, dostają konto warstwy 1 na czas pracy.

> **Pojęcie: AdminSDHolder.** Obiekt w katalogu z wzorcowymi uprawnieniami dla kont w grupach chronionych. Co godzinę proces SDProp nadpisuje uprawnienia tych kont wzorcem, żeby nikt nie mógł ich po cichu zmienić. Skutek uboczny: konto usunięte z grupy chronionej zachowuje `adminCount = 1` i wyłączone dziedziczenie uprawnień, dopóki ich ręcznie nie przywrócimy.

Protected Users

> **Pojęcie: Protected Users.** Grupa wprowadzona w Windows Server 2012 R2, której członkowie dostają twarde ograniczenia po stronie komputera i kontrolera: brak NTLM, brak DES i RC4 w Kerberos, brak delegowania, brak zapamiętanych poświadczeń, bilet TGT ważny 4 godziny.

Kogo dodajemy	Kogo nie dodajemy
konta `.t0` obu administratorów	konta usługowe i konta komputerów (to nie zadziała i zepsuje usługi)
konta `.admin` po teście	jedno konto awaryjne warstwy 0, które musi działać, gdy Kerberos zawiedzie
konto pana Zbigniewa, jeśli dostanie jakiekolwiek uprawnienia administracyjne	konta, które logują się do aplikacji obsługujących tylko NTLM (najpierw znajdujemy takie aplikacje w audycie NTLM)

Konto w Protected Users nie zaloguje się do komputera, który nie widzi kontrolera, bo nie ma zapisanych poświadczeń. Dla administratora to zaleta, ale dla handlowca w hotelu byłoby przeszkodą, dlatego zwykłych kont do tej grupy nie dodajemy.

Konta usługowe: gMSA i dMSA

> **Pojęcie: gMSA (group Managed Service Account).** Konto usługi, którego hasło ustala i zmienia sam kontroler domeny, co 30 dni, z długim losowym ciągiem. Nikt go nie zna, więc nie da się go złamać z biletu Kerberos ani wpisać w skrypt. Zakładanie opisuje strona Konta usługowe MSA i gMSA.

> **Pojęcie: dMSA (delegated Managed Service Account).** Nowy rodzaj konta w Windows Server 2025, który przejmuje rolę istniejącego zwykłego konta usługi i pozwala je wyłączyć bez przepisywania usługi od zera. W maju 2025 badacze opisali nadużycie nazwane BadSuccessor: użytkownik z prawem tworzenia obiektów w jakiejkolwiek jednostce organizacyjnej mógł przez dMSA przejąć uprawnienia dowolnego konta. Microsoft załatał je w sierpniu 2025 (CVE-2025-53779).

W Zielonej zamieniamy konta usługowe na gMSA, zaczynając od kont z SPN (Optima, aplikacje Java na `app01`). dMSA rozważymy, gdy w domenie będą kontrolery z Windows Server 2025, a do tego czasu sprawdzamy w raporcie PingCastle, komu delegowano prawo tworzenia obiektów w jednostkach organizacyjnych.

Stare protokoły: NTLM, RC4, SMBv1, LDAP bez podpisu

> **Pojęcie: NTLM.** Starszy od Kerberos sposób logowania w sieciach Windows, w którym serwer sprawdza znajomość hasła przez wyzwanie i odpowiedź. Jego słabości są znane od lat: przechwycony skrót hasła pozwala logować się bez znajomości hasła (pass the hash), a połączenie można przekazać do innego serwera (relay). Wersja pierwsza, NTLMv1, łamie się w godzinach.

> **Pojęcie: podpisywanie LDAP i powiązanie kanału (LDAP signing i channel binding).** Podpisywanie sprawia, że nikt po drodze nie zmieni zapytania LDAP ani odpowiedzi. Powiązanie kanału łączy uwierzytelnienie z konkretnym połączeniem TLS, więc przechwycone logowanie nie zadziała w innym połączeniu LDAPS.

Mechanizm	Stan u Microsoftu w październiku 2026	Co robimy w Zielonej
NTLMv1	usunięty z Windows 11 24H2 i Windows Server 2025; od aktualizacji z 13 października 2026 na tych systemach domyślnie blokowane są poświadczenia pochodne NTLMv1 dla logowania jednokrotnego (`BlockNtlmv1SSO`), co może zatrzymać Wi-Fi i VPN z MS-CHAPv2 na komputerach bez Credential Guard	GPO „Network security: LAN Manager authentication level” ustawione na „Send NTLMv2 response only. Refuse LM & NTLM” w całej domenie; VPN handlowców i tak używa EAP-TLS z certyfikatem
NTLM w ogóle	według planu Microsoftu ze stycznia 2026: najpierw rozszerzony audyt (dostępny w Windows Server 2025 i Windows 11 24H2, a od października 2026 także w poprawkach dla Windows Server 2022 i 2019), potem w 2026 roku rozwiązania blokujące przejście (IAKerb i lokalny KDC, w czerwcu 2026 w wersji zapoznawczej dla Insiderów), a w następnej dużej wersji Windows Server NTLM wyłączony domyślnie; daty tej wersji Microsoft nie podał	włączamy audyt NTLM w domenie („Network security: Restrict NTLM: Audit NTLM authentication in this domain”), zbieramy zdarzenia w Graylogu i listujemy aplikacje; blokady nie włączamy przed końcem listy
RC4 w Kerberos	aktualizacje od 13 stycznia 2026 dodały zdarzenia audytu KDCSVC 201 do 209; od kwietnia 2026 domyślne typy szyfrowania kont bez ustawionego `msDS-SupportedEncryptionTypes` to tylko AES; od lipca 2026 tryb audytu usunięto	sprawdzamy zdarzenia 201 do 209 na kontrolerach, konta z SPN przestawiamy na AES albo gMSA, keytaby dla linuksów generujemy z kluczami AES
SMBv1	nie jest instalowany domyślnie od Windows 10 1709 i Windows Server 2019	sprawdzamy fiszką na każdym serwerze; stary skaner sieciowy, który wymagał SMBv1, dostaje skanowanie na FTP albo do poczty
podpisywanie SMB	według dokumentacji Windows 11 24H2 Pro, Enterprise i Education wymaga podpisu w obu kierunkach, Windows Server 2025 wymaga podpisu połączeń wychodzących, a kontrolery od dawna wymagają podpisu połączeń do siebie	nie wyłączamy; urządzenia NAS i drukarki ze skanowaniem do udziału testujemy przed wymianą systemów
podpisywanie LDAP	nowe wdrożenia Windows Server 2025 wymagają podpisu domyślnie; przy aktualizacji ustawienia zostają takie, jakie były	dziennik 2887 i 2889, lista klientów, potem GPO „Domain controller: LDAP server signing requirements” na „Require signing”

Mechanizm	Stan u Microsoftu w październiku 2026	Co robimy w Zielonej
powiązanie kanału LDAP	w nowych wdrożeniach Windows Server 2025 domyślnie „When supported” z włączonym audytem	GPO „Domain controller: LDAP server channel binding token requirements” najpierw „When supported”, po przeglądzie zdarzeń 3039 do 3041 „Always”

Kolejność w Zielonej jest zawsze ta sama: audyt, lista zależności, poprawka albo wymiana klienta, wymuszenie w pilotażu, wymuszenie wszędzie. Każdy krok jest zmianą w GLPI z planem wycofania, a wymuszenia nie robimy w zakazie zmian od 15 listopada do 6 stycznia.

> ⚠ Aplikacje, które najczęściej psują się po wymuszeniu podpisu LDAP, to te, które łączą się z AD prostym powiązaniem na porcie 389: w Zielonej Gitea, NetBox, Graylog i GLPI mają logowanie z AD. Przed wymuszeniem przestawiamy je na LDAPS (port 636) z certyfikatem `CA-Zielona`, opisanym na stronach logowania z AD w każdej z tych książek.

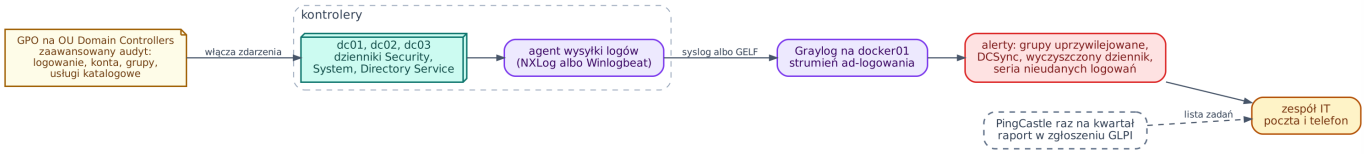
Konto krbtgt

> **Pojęcie: krbtgt.** Ukryte konto, którego kluczem kontroler podpisuje każdy bilet TGT w domenie. Kto zna ten klucz, może wystawić sobie bilet dowolnego użytkownika (golden ticket), a zmiana haseł użytkowników tego nie zatrzyma.

Hasło `krbtgt` zmieniamy dwa razy, z przerwą dłuższą niż najdłuższy czas życia biletu (domyślnie 10 godzin), bo kontroler pamięta poprzednie hasło. Robimy to raz w roku, po odejściu każdej osoby z dostępem do warstwy 0 i zawsze po podejrzeniu włamania. Microsoft udostępnia do tego skrypt `New-KrbtgtKeys.ps1` w repozytorium na GitHubie, który najpierw sprawdza replikację i pozwala wykonać próbę bez zmian. Przed pierwszym użyciem czytamy jego aktualny opis.

Audyt i Graylog

Kontrolery wysyłają dziennik zabezpieczeń do Grayloga agentem opisanym na stronie Wysyłka logów z hostów, do strumienia `ad-logowania` ze strony Graylog: codzienna praca z logami. Żeby zdarzenia w ogóle powstały, GPO podpięte do jednostki `Domain Controllers` włącza zaawansowany audyt.



Rysunek 2. Droga zdarzeń bezpieczeństwa: GPO z zaawansowanym audytem włącza zdarzenia na dc01, dc02 i dc03, agent wysyła dziennik Security, System i Directory Service do Grayloga na docker01, strumień ad-logowania i alerty powiadamiają zespół, a raport PingCastle raz na kwartał uzupełnia obraz (kliknięcie otwiera pełny rozmiar)

Zdarzenie	Co znaczy	Alarm w Graylogu
4624, 4625	udane i nieudane logowanie	seria nieudanych logowań (już jest na stronie o Graylogu)
4740	zablokowane konto	każde na koncie `.t0`
4728, 4732, 4756	dodanie do grupy globalnej, lokalnej, uniwersalnej	każde dla grup uprzywilejowanych
4720, 4726	utworzenie i usunięcie konta	raport dzienny
4768, 4769, 4771	bilet TGT, bilet do usługi, nieudane uwierzytelnienie wstępne Kerberos	bilety z szyfrowaniem RC4 (typ 0x17)
4776	uwierzytelnienie NTLM na kontrolerze	raport tygodniowy do audytu NTLM
4662 z prawami replikacji	ktoś pobiera dane katalogu jak kontroler (DCSync)	każde, gdy konto nie jest kontrolerem
5136	zmiana obiektu katalogu (wymaga audytu zmian usług katalogowych)	zmiany GPO i obiektu AdminSDHolder
4794	próba ustawienia hasła DSRM	każde
1102	wyczyszczenie dziennika zabezpieczeń	każde
2887, 2889, 3039 do 3041	LDAP bez podpisu i powiązanie kanału	raport tygodniowy do czasu wymuszenia
KDCSVC 201 do 209	RC4 w Kerberos	raport tygodniowy

Zakres audytu na kontrolerach (zaawansowane zasady audytu): logowanie konta (Credential Validation, Kerberos Authentication Service, Kerberos Service Ticket Operations), zarządzanie kontami (User Account Management, Security Group Management), dostęp do usług katalogowych (Directory Service Access, Directory Service Changes), logowanie i wylogowanie, zmiana zasad. Sukces i porażka dla każdej z nich. Dziennik zabezpieczeń na kontrolerach

powiększamy do co najmniej 1 GB, żeby lokalna historia przetrwała kilka dni przerwy w Graylogu.

Narzędzia sprawdzające: PingCastle, Purple Knight i Locksmith

Raz na kwartał uruchamiamy narzędzie, które patrzy na domenę oczami napastnika i porównuje ją z listą znanych słabości. Wynik nie zastępuje audytu, ale daje listę zadań i liczbę, którą widać z kwartału na kwartał.

Narzędzie	Kto rozwija	Co sprawdza	Licencja (informacyjnie, sprawdzamy u producenta)
PingCastle	Netwrix (dawniej projekt Vincenta Le Toux)	konta uprzywilejowane, delegowanie, szablony AD CS, stare protokoły, zaufania; raport HTML z punktacją	według strony Netwrix wydanie Community jest bezpłatne do sprawdzania własnego środowiska, bez wsparcia; audyt cudzych firm i funkcje dodatkowe wymagają licencji komercyjnej
Purple Knight	Semperis	wskaźniki narażenia i wskaźniki włamania w AD, w nowszych wersjach także w Entra ID (do potwierdzenia w aktualnej wersji)	według Semperis narzędzie bezpłatne; warunki pobrania i użycia czytamy przy pobieraniu
Locksmith	Jake Hildreth, moduł PowerShell z galerii	tylko AD CS: urzędy i szablony w lesie, każdy błąd z numerem ESC; użycie i poprawki opisuje strona Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza	bezpłatny moduł w galerii PowerShell; licencję sprawdzamy w repozytorium projektu (do potwierdzenia)

Wszystkich trzech narzędzi używamy z osobnej stacji administracyjnej, zwykłym kontem domenowym, a raporty trzymamy w zgłoszeniu GLPI z ograniczonym dostępem: raport to gotowa mapa słabości domeny.

Częste błędy

Objaw	Przyczyna	Co robimy
Po dodaniu konta do Protected Users administrator nie może zalogować się do starej konsoli zapory	konsola uwierzytelnia przez NTLM albo zapisuje poświadczenia	konto `.t0` bez Protected Users tylko do tej konsoli albo, lepiej, konsola z logowaniem przez RADIUS i certyfikat
Usługa przestała działać po zmianie typu szyfrowania na AES	hasło konta ustawiono, zanim domena miała klucze AES, więc konto ich nie ma	jednorazowa zmiana hasła konta usługi, a docelowo gMSA
Wi-Fi z PEAP-MSCHAPv2 przestało łączyć się samo po aktualizacji z października 2026	domyślne wymuszenie `BlockNtlmv1SSO` na komputerach bez Credential Guard	docelowo EAP-TLS z certyfikatem; czasowo `BlockNtlmv1SSO = 0` w GPO dla grupy komputerów z datą zakończenia
Gitea przestała logować użytkowników AD po wymuszeniu podpisu LDAP	proste powiązanie bez TLS na porcie 389	przestawienie Gitea na LDAPS 636 z zaufanym certyfikatem `CA-Zielona`
Konto usunięte z Domain Admins nadal nie dziedziczy uprawnień jednostki	`adminCount = 1` i wyłączone dziedziczenie po AdminSDHolder	czyścimy `adminCount` i włączamy dziedziczenie na koncie po upewnieniu się, że nie należy już do żadnej grupy chronionej
Graylog nie pokazuje zdarzeń 4728 i 5136	zaawansowany audyt nie jest włączony w GPO dla `Domain Controllers`	`auditpol /get /category:*`, poprawka GPO, `gpupdate /force` na kontrolerze
Raport PingCastle pokazuje konto z delegowaniem bez ograniczeń	stary serwer wydruku albo aplikacja ustawiona tak przed laty	przestawiamy na delegowanie ograniczone do konkretnej usługi albo wyłączamy delegowanie

□□ Ćwiczenia

1. Dlaczego `hv01` i `hv02` są w warstwie 0, skoro nie są kontrolerami domeny?

Odpowiedź

Bo stoją na nich maszyny `dc01` i `dc02`. Administrator hosta może zatrzymać maszynę, skopiować jej dysk i odczytać bazę katalogu ze skrótami haseł wszystkich kont. Każdy system, który daje dostęp do danych kontrolera, ma tę samą wartość co kontroler.

1. Ola potrzebuje przez jedno popołudnie zmienić GPO dla komputerów swojego zespołu. Co robimy, zamiast dodać ją do Domain Admins?

Odpowiedź

Najlepiej delegujemy jej prawo edycji jednego konkretnego GPO i linkowania na jednostce z komputerami zespołu. Jeśli to jednorazowe, robimy zmianę sami albo dajemy członkostwo czasowe w grupie z wąskim prawem przez `-MemberTimeToLive` na kilka godzin, z wnioskiem w GLPI. Domain Admins nie jest potrzebne do edycji jednego GPO.

1. Po aktualizacji z 13 października 2026 laptopy w magazynie przestały łączyć się z Wi-Fi bez wpisywania hasła. Gdzie szukamy przyczyny i co robimy od razu, a co docelowo?

Odpowiedź

W dzienniku Microsoft-Windows-NTLM/Operational na laptopie szukamy zdarzenia 4025: to wymuszenie `BlockNtlmv1SSO`, które blokuje logowanie jednokrotne z MS-CHAPv2 na komputerach bez Credential Guard. Od razu, na ograniczony czas i tylko dla tych komputerów, wracamy do trybu audytu wartością 0 w GPO. Docelowo przestawiamy Wi-Fi magazynu na EAP-TLS z certyfikatem albo włączamy Credential Guard.

1. Pan Wojtek pyta, jak udowodnimy, że nikt nie dodał się po cichu do Domain Admins w ostatnim kwartale. Co pokazujemy?

Odpowiedź

Zapytanie w Graylogu o zdarzenia 4728, 4732 i 4756 dla grup uprzywilejowanych z całego kwartału, razem z alertami, które te zdarzenia wywołały, oraz zgłoszenia w GLPI dla każdego zamierzonego dodania (członkostwa czasowe). Do tego miesięczne porównania wyniku `Get-ADGroupMember -Recursive` z listą zatwierdzoną.

Powiązane: Projekt lasu i domeny Zielonej: lokacje, podsieci, FSMO, poziomy funkcjonalne i nazewnictwo · Zasady haseł i blokady konta: polityka domeny i PSO · Windows LAPS: hasło lokalnego administratora w Active Directory · Konta usługowe MSA i gMSA · Skrypty audytowe Active Directory · Graylog: codzienna praca z logami · Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu

Źródła: (odczyt 19.10.2026) · Microsoft Support, KB5066470 „Upcoming changes to NTLMv1 in Windows 11, version 24H2 and Windows Server 2025” (`BlockNtlmv1SSO`, audyt od sierpnia 2025 i listopada 2025, wymuszenie domyślne od aktualizacji z 13.10.2026, zdarzenia 4024 i 4025, tylko bez Credential Guard) · Microsoft 365 Message Center MC1508562 (15.10.2026, wpływ na MS-CHAPv2) · Microsoft Tech Community, „Advancing Windows security: disabling NTLM by default” (29.01.2026) oraz securityweek.com, „Microsoft moves closer to disabling NTLM” (02.02.2026: trzy etapy, NTLM wyłączony domyślnie w następnej dużej wersji) · it-connect.tech, IAKerb i LocalKDC w wersji zapoznawczej (02.06.2026) i „Windows Server October 2026 updates explained in detail” (15.10.2026, rozszerzony audyt NTLM dla Windows Server 2022 i 2019) · vinfrastructure.it, „NTLM

v1 is being removed in recent Windows versions” (styczeń 2026) · Microsoft Support, KB5073381 „How to manage Kerberos KDC usage of RC4” (CVE-2026-20833: zdarzenia KDCSVC 201 do 209, etapy 13.01.2026, 14.04.2026, lipiec 2026) · Microsoft Learn, „LDAP signing” (domyślne ustawienia Windows Server 2025, zdarzenia 2886 do 2889 i 3039 do 3041) · Microsoft Learn, „Event ID 2887” i „Event ID 2889” (LDAP signing) · Microsoft Learn, „Control SMB signing behavior” (wymagania podpisu w Windows 11 24H2 i Windows Server 2025) · Microsoft Learn, „Protected Users Security Group”, „Securing privileged access: Enterprise access model”, „AdminSDHolder”, „Appendix B: Privileged Accounts and Groups in Active Directory” · helpnetsecurity.com, „Microsoft fixes BadSuccessor Kerberos vulnerability (CVE-2025-53779)” (13.08.2025) · netwrix.com, porównanie wydań PingCastle (Community do własnego środowiska) · semperis.com, komunikaty o Purple Knight (bezpłatne narzędzie od marca 2021) · github.com/microsoft/New-KrbtgtKeys.ps1

Revision #3
Created 2026-10-18 22:59:59 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:43 UTC by Tomasz Konieczny