ManageEngine
ADAudit Plus

Przewodnik po inspekcji usługi Active Directory

Spis treści

Wstęp

Zabezpieczenie usługi Active Directory pozwala chronić konta użytkownika, systemy firmy, oprogramowanie i inne najważniejsze składniki infrastruktury IT organizacji przed nieupoważnionym dostępem.

ADAudit Plus to rozwiązanie do prowadzenia inspekcji zmian w czasie rzeczywistym i analizowania zachowań użytkowników, które pomaga zabezpieczyć usługę Active Directory.

Z ADAudit Plus można prowadzić inspekcję trzech głównych kontekstów Active Directory:

- nazywania domen (w tym użytkowników, komputerów, grup, jednostek organizacyjnych i innych obiektów),
- schematów (i wszystkich obiektów schematów),
- konfiguracji (w tym stron, podsieci, DNS AD i innych obiektów).

ADAudit Plus pozwala prowadzić inspekcję kontrolerów domeny w poniższych wersjach systemu operacyjnego:

- Windows Server 2003/2003 R2,
- Windows Server 2008/2008 R2,
- Windows Server 2012/2012 R2,
- Windows Server 2016,
- Windows Server 2019.

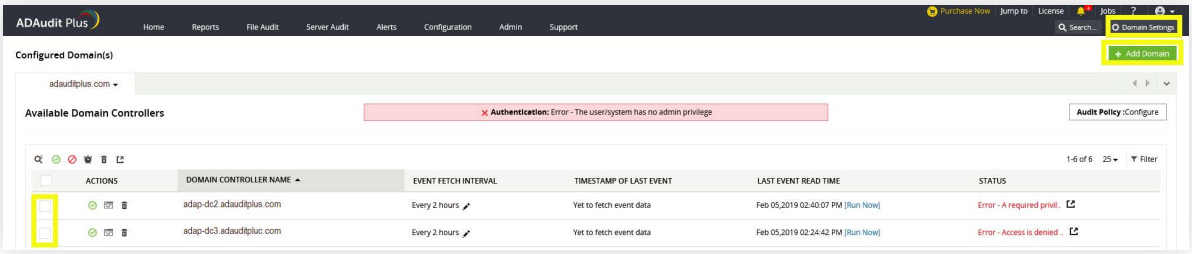
Ten przewodnik pomoże Ci skonfigurować rozwiązanie ADAudit Plus i środowisko usługi Active Directory na potrzeby prowadzenia inspekcji w czasie rzeczywistym.

1. Konfiguracja domen usługi Active Directory i kontrolerów domeny w ADAudit Plus

1.1 Konfiguracja automatyczna

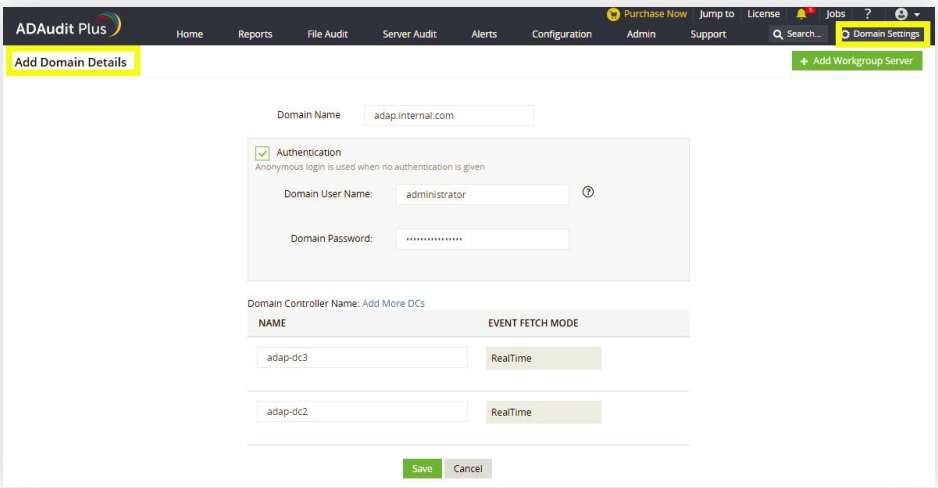
Po zainstalowaniu, ADAudit Plus automatycznie wykrywa domenę lokalną i uruchomione na niej kontrolery.

Zaloguj się do konsoli internetowej ADAudit Plus → Domain Settings → Wybierz odpowiednie kontrolery domeny, klikając pola wyboru.



1.2 Konfiguracja ręczna

Dodawanie domeny: Zaloguj się do konsoli internetowej ADAudit Plus → Domain Settings → Add Domain → Wprowadź wymagane szczegóły.



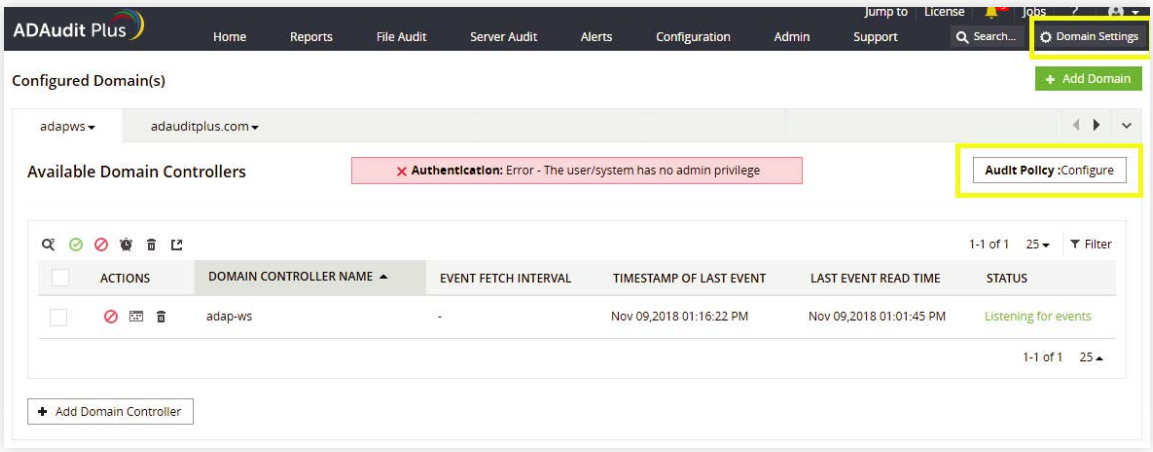
2. Konfiguracja zasad inspekcji

Zasady inspekcji należy skonfigurować, aby wydarzenia były rejestrowane w chwili aktywności.

2.1 Konfiguracja automatyczna

ADAudit Plus pozwala automatycznie skonfigurować wymagane zasady inspekcji na potrzeby inspekcji Active Directory.

Uwaga: jeśli nie chcesz podawać poświadczeń administratora domeny, skonfiguruj konto usługi z minimalną liczbą uprawnień wymaganych do automatycznej konfiguracji zasad inspekcji, wykonując poniższe kroki.



2.2 Konfiguracja ręczna

2.2.1 Konfiguracja zaawansowanych zasad inspekcji

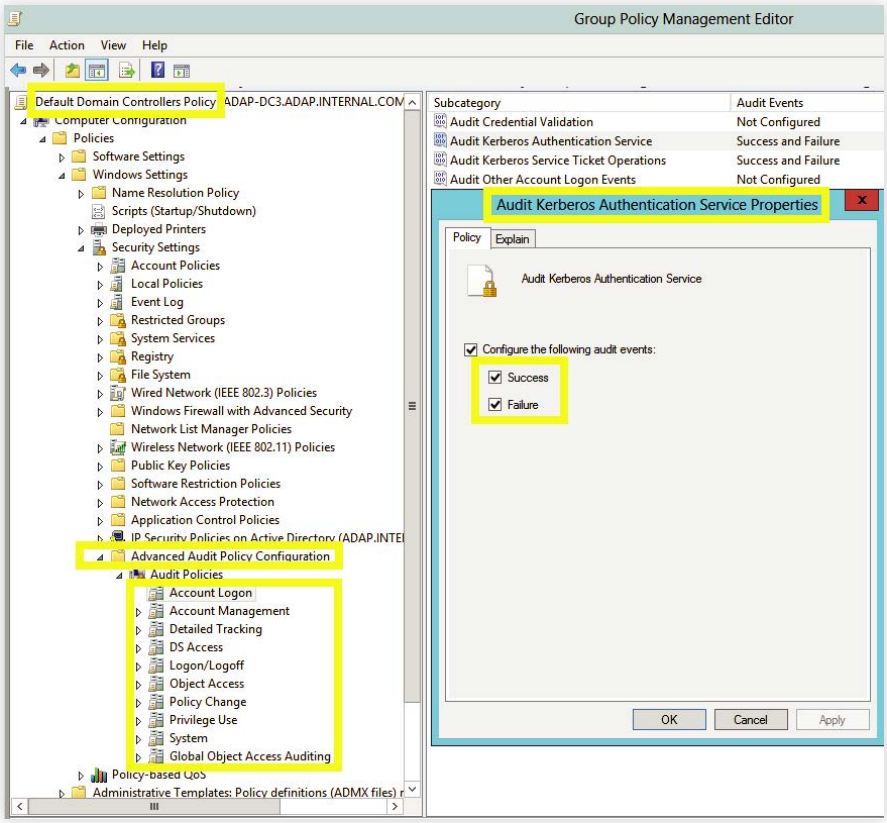
Zaawansowane zasady inspekcji pomagają administratorom zyskać szczegółową kontrolę nad tym, które aktywności są rejestrowane w dziennikach, co pozwala ograniczyć nadmierną ilość informacji. Zaleca się, aby zaawansowane zasady inspekcji zostały skonfigurowane na kontrolerach domeny uruchomionych na systemach Windows Server 2008 i jego nowszych wersjach.

i Zaloguj się do dowolnego komputera z **Group Policy Management Console (GPMC)** używając poświadczeń administratora domeny → Otwórz GPMC → Kliknij **Default Domain Controllers Policy** → **Edit.**

ii W obszarze **Group Policy Management Editor** → **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policy** i kliknij dwukrotnie odpowiednie ustawienie zasad.

iii Przejdź do prawego okienka → Kliknij prawym przyciskiem myszy wybraną podkategorię, a następnie kliknij **Properties** → Wybierz **Success, Failure** lub obie opcje zgodnie z informacjami w poniższej tabeli.

Cateogory	Sub Category	Audit Events
Account Logon	• Audit Kerberos • Authentication Service	✓ Success and Failure
Account Management	• Audit Computer Account • Management • Audit Distribution Group • Management • Audit Security Group • Management	✓ Success
	• Audit User Account • Management	✓ Success and Failure
Detailed Tracking	• Audit Process Creation • Audit Process Termination	✓ Success
DS Access	• Audit Directory Services • Changes • Audit Directory Service Access	✓ Success
Logon /Logoff	• Audit Logon • Audit Network Policy Server	✓ Success and Failure
	• Audit Other Logon/Logoff • Events • Audit Logoff	✓ Success
Object Access	• Audit Other Object • Access Events	✓ Success
Policy Change	• Audit Authentication • Policy Change • Audit Authorization Policy • Change	✓ Success
System	• Audit Security State Change	✓ Success



Obraz z następującymi informacjami: Account Logon category → Audit Kerberos Authentication Service subcategory → Skonfigurowano opcję Success i Failure.

Uwaga: aby włączyć inspekcję zdarzeń NTLM, zaloguj się do konsoli internetowej ADAudit Plus → Kliknij kartę Support → Kliknij More pod obszarem Support Information → Kliknij Enable/Disable Configuration settings pod obszarem Configuration → Włącz inspekcję NTLM.

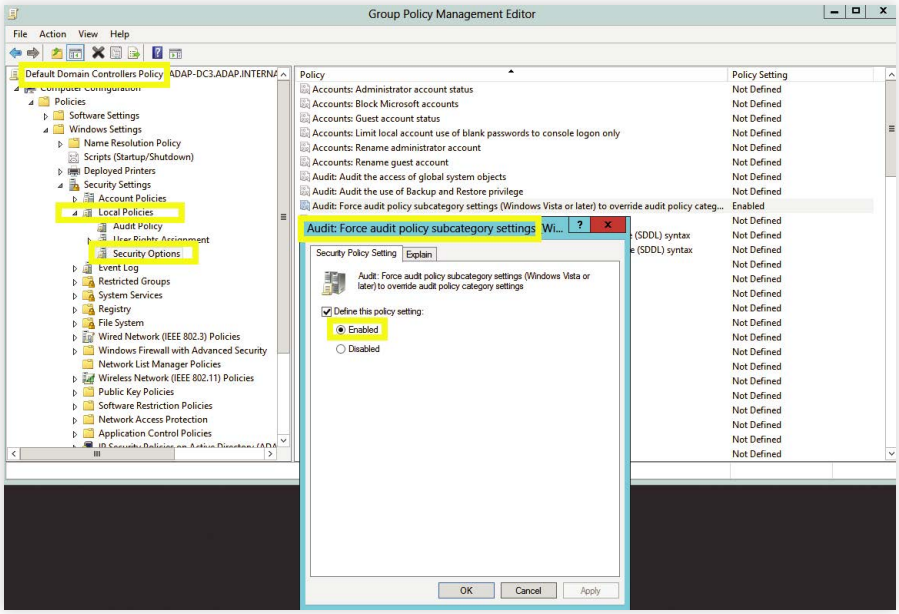
2.2.2 Egzekwowanie zaawansowanych zasad inspekcji

Jeśli korzystasz z zaawansowanych zasad inspekcji, sprawdź czy są nadrzędne wobec starszych wersji zasad inspekcji.

i Zaloguj się do dowolnego komputera z Konsolą zarządzania zasadami grupy (GPMC) używając poświadczeń administratora domeny → **Otwórz GPMC** → Kliknij **Default Domain Controllers Policy** → **Edit.**

ii W obszarze **Group Policy Management Editor** → **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** **Security Options.**

iii Przejdź do prawego okienka → **Right-click on Audit: Force audit policy subcategory settings** → **Properties** → **Enable.**



2.2.3 Konfiguracja starszych wersji zasad inspekcji

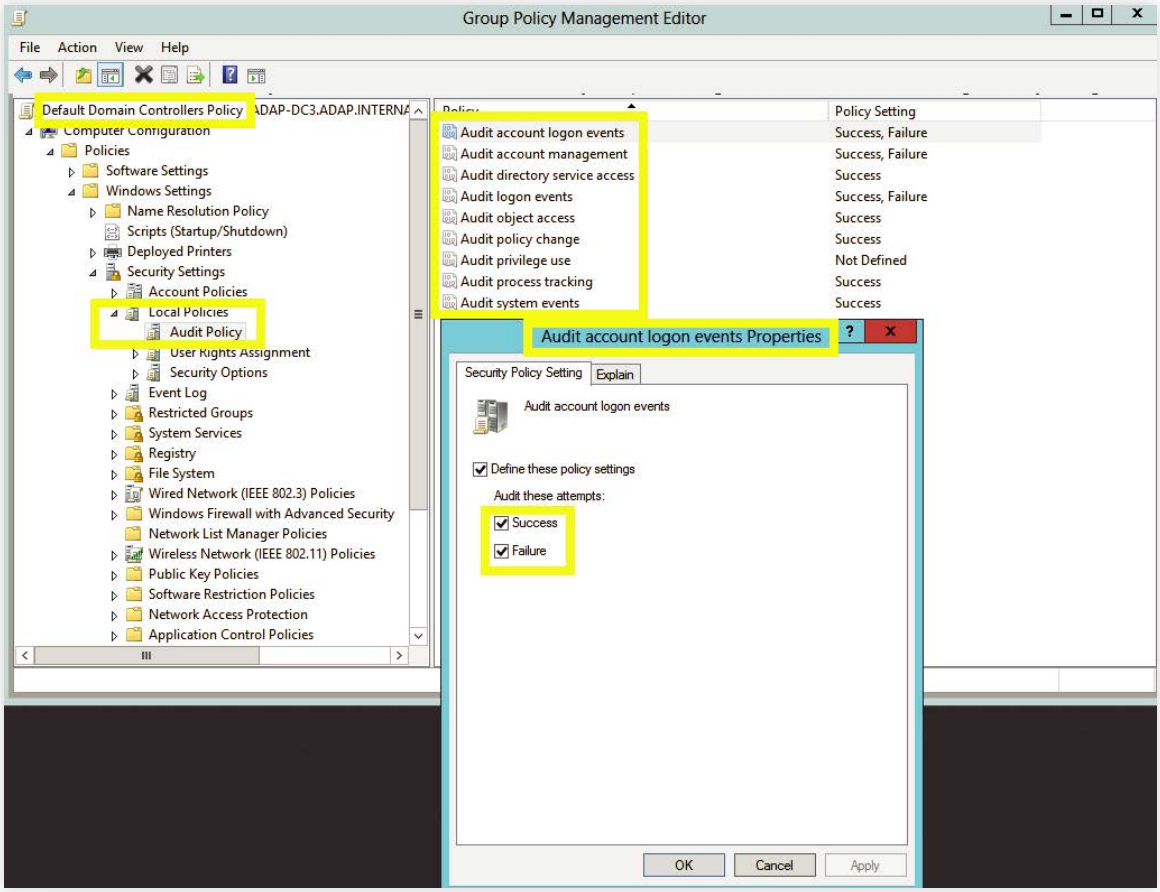
Zaawansowanych ustawień inspekcji nie można skonfigurować na systemach Windows Server 2003 i na wcześniejszych wersjach. Dlatego w przypadku tych systemów należy skonfigurować starsze wersje zasad inspekcji.

i Zaloguj się do dowolnego komputera z **Group Policy Management Console (GPMC)** używając poświadczeń administratora domeny → Otwórz GPMC → Kliknij Right click on Default Domain Controllers Policy → Edit.

ii W **Group Policy Management Editor** → **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → Kliknij dwukrotnie **Audit Policy.**

iii Przejdź do prawego okienka → Kliknij prawym przyciskiem myszy wybraną zasadę, a następnie kliknij Properties →Wybierz Success, Failure lub obie opcje zgodnie z informacjami w poniższej tabeli.

Category	Audit Events
Account Logon	✓ Success and Failure
Audit Logon / Logoff	✓ Success and Failure
Account Management	✓ Success
Directory Service Access	✓ Success
Process Tracking	✓ Success
Object Access	✓ Success
System Events	✓ Success



Obraz z następującymi informacjami: Kategoria Audit account logon events → Skonfigurowano opcję Success i Failure.

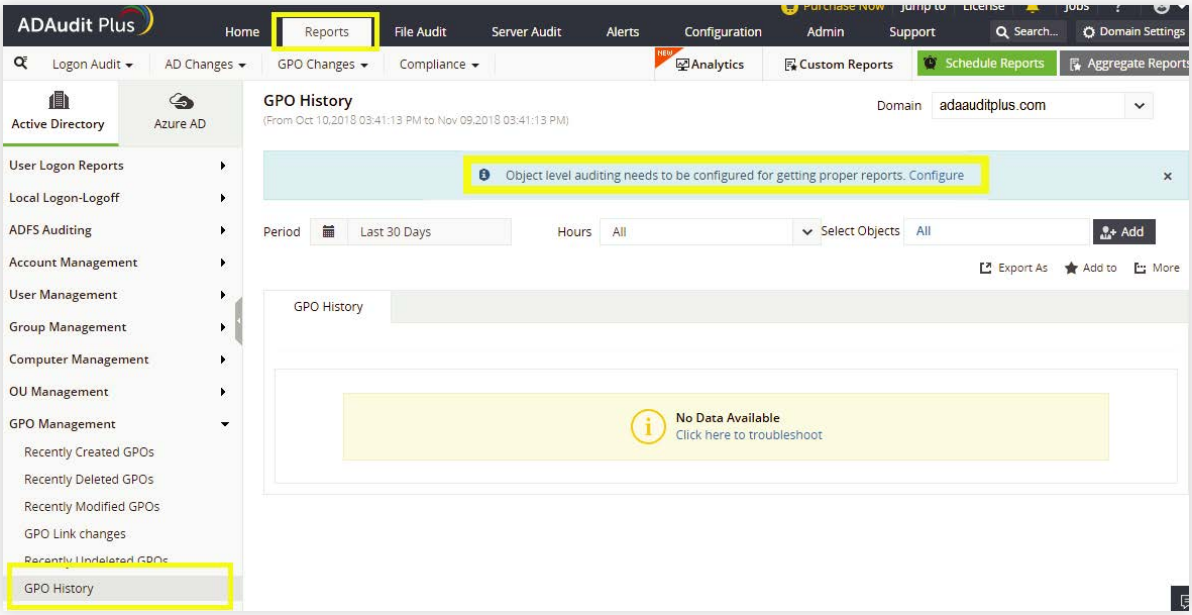
3. Konfiguracja inspekcji na poziomie obiektu

Konfiguracja inspekcji na poziomie obiektu pozwala rejestrować wydarzenia, gdy pojawi się aktywność związana z obiektem usługi Active Directory.

3.1 Konfiguracja automatyczna

ADAudit Plus może automatycznie skonfigurować poziom inspekcji wymaganego obiektu.
Uwaga: automatyczna konfiguracja inspekcji na poziomie obiektu jest przeprowadzana bez zgody użytkownika.

Aby automatycznie zainicjować konfigurację inspekcji na poziomie obiektu, zaloguj się do konsoli internetowej ADAudit Plus → Reports → GPO Management → GPO History → Object level auditing needs to be configured for getting proper reports: Configure.



3.2 Konfiguracja ręczna

3.2.1 Konfiguracja inspekcji dla jednostki organizacyjnej, obiektu zasad grupy, użytkownika, grupy, komputera i obiektów kontaktów

i Zaloguj się do dowolnego komputera z Active Directory Users and Computers, korzystając z poświadczeń administratora domeny → Otwórz ADUC.
Kliknij View i sprawdź, czy zostały włączone Advanced Features. Zostaną wyświetlone zaawansowane ustawienia zabezpieczeń wybranych obiektów dla Active Directory Users and Computers.

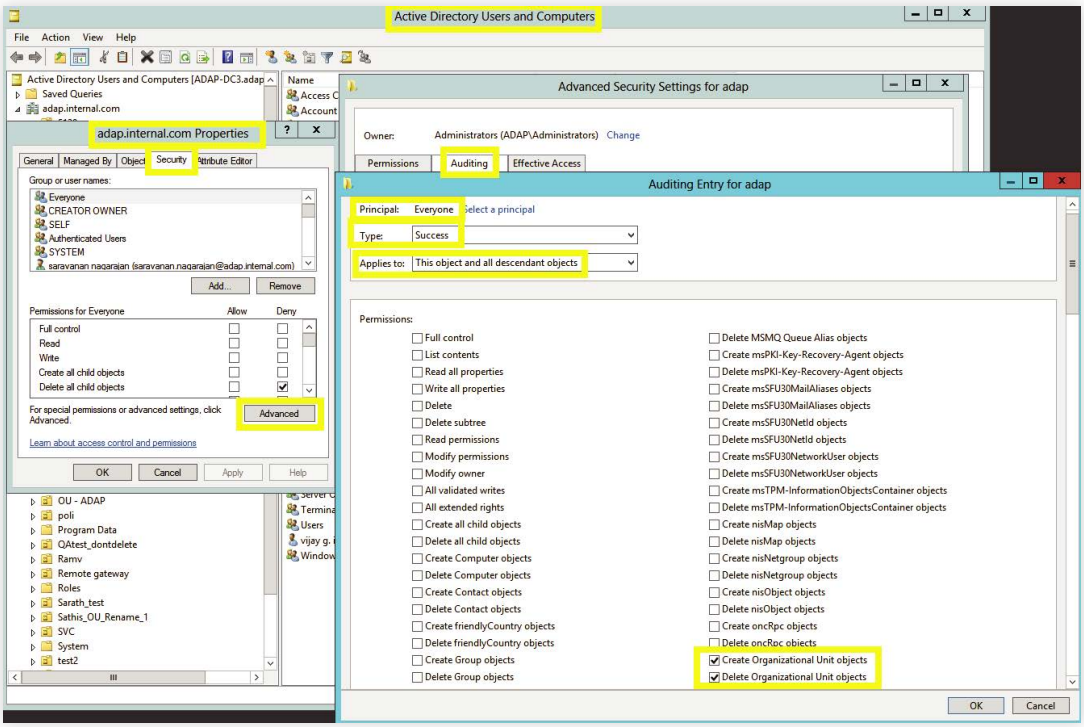
ii Kliknij prawym przyciskiem myszy domenę → Properties → Security → Advanced → Auditing → Add.

iii W oknie Auditing Entry → Select a principal: Everyone → Type: Success → Wybierz odpowiednie uprawnienia zgodnie z poniższą tabelą.

Uwaga: za pomocą opcji Wyczyść wszystko usuń wszystkie uprawnienia i właściwości przed wyborem odpowiednich uprawnień.

Auditing Entry number	Auditing Entry for	Access	Apply onto	
			Windows Server 2003	Windows Server 2008 and above
1&2	OU	• Create Organizational Unit objects • Delete Organizational Unit objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete Modify Permissions	Organizational Unit objects	Descendant Organizational Unit objects
3&4	GPO	• Create groupPolicy Container Objects • Delete groupPolicy Container Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions	groupPolicy Container objects	Descendant groupPolicy Container objects
5&6	User	• Create User Objects • Delete User Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions • All Extended Rights	User objects	Descendant User objects
7&8	Group	• Create Group Objects • Delete Group Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions • All Extended Rights	Group objects	Descendant Group objects

9&10	Computer	• Create Computer Objects • Delete Computer Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions • All Extended Rights	Computer objects	Descendant Computer objects
11&12	Contact	• Create Contact Objects • Delete Contact Objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions	Contact objects	Descendant Contact objects



Obraz z następującymi informacjami: Auditing numer 1.

Uwaga: należy włączyć wszystkie 12 pozycji poddanych inspekcji.

3.2.2 Konfiguracja inspekcji dla obiektów kontenera

i Zaloguj się do dowolnego komputera z przystawką **Active Directory Service Interfaces** Otwórz konsolę ADSI Edit → Kliknij prawym przyciskiem myszy ADSI Edit → Connect to.

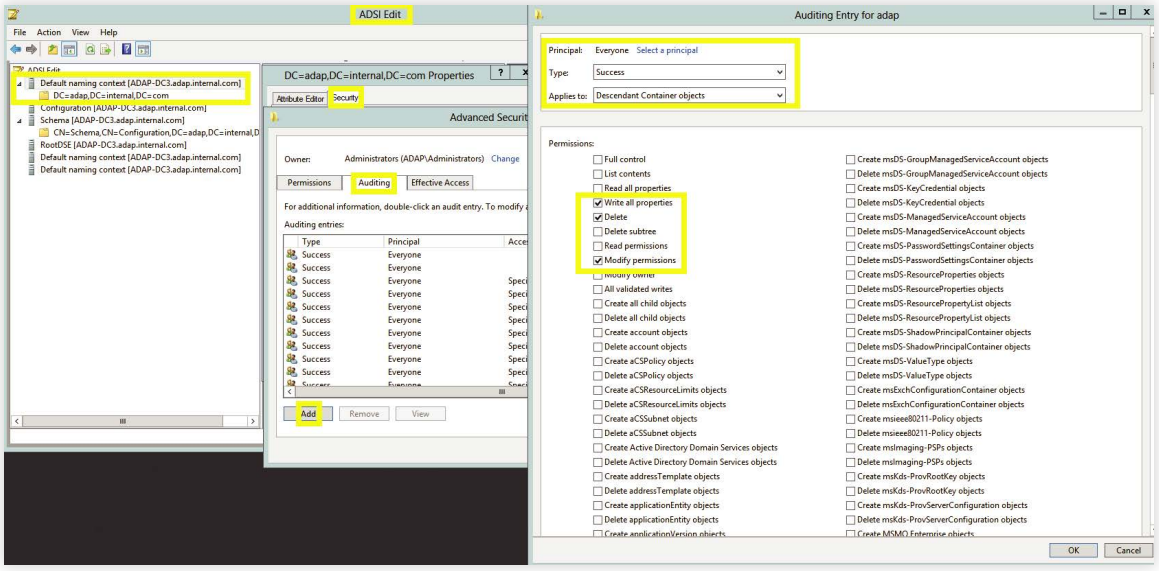
ii W oknie **Connection Settings** → W obszarze **Select a Well-Known Naming Context** → Wybierz **'Default Naming Context'.**

iii Przejdź do lewego okienka → Kliknij **Default naming context** → Kliknij prawym przyciskiem myszy nazwę wyróżniającą domeny → Wybierz **Properties** → **Security** → **Advanced Auditing** → **Add.**

iv W oknie **Auditing Entry** → **Select a principal: Everyone** → **Type: Success** → Wybierz odpowiednie uprawnienia zgodnie z poniższą tabelą.

Uwaga: za pomocą opcji Wyczyść wszystko usuń wszystkie uprawnienia i właściwości przed wyborem odpowiednich uprawnień.

Auditing Entry	Access	Apply onto	
		Windows Server 2003	Windows Server 2008 and above
Container	• Write All Properties • Delete • Modify Permissions	Container objects	Descendant Container objects



3.2.3 Konfiguracja inspekcji dla obiektów ustawień hasła

i Zaloguj się do dowolnego komputera z przystawką **Active Directory Service Interfaces** → → Otwórz konsolę ADSI Edit → Kliknij prawym przyciskiem myszy ADSI Edit → Connect to.

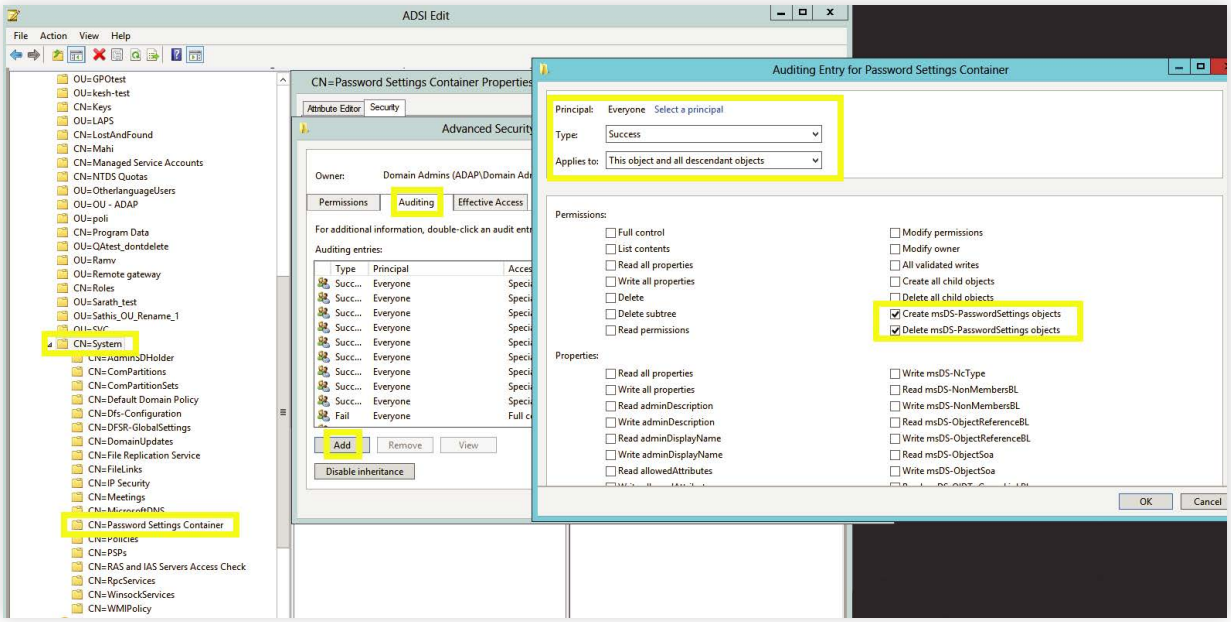
ii W oknie Connection Settings → W obszarze Select a Well-Known Naming Context → Wybierz 'Default Naming Context'.

iii Przejdź do lewego okienka → Kliknij Domyślny kontekst nazewnictwa → Rozwiń domenę Rozwiń kontener System → Kliknij prawym przyciskiem myszy Password Settings Container → Properties → Security → Advanced → Auditing → Add.

iv W oknie Auditing Entry → Select a principal: Everyone → Type: Success → Wybierz odpowiednie uprawnienia zgodnie z poniższą tabelą.

Uwaga: za pomocą opcji Wyczyść wszystko usuń wszystkie uprawnienia i właściwości przed wyborem odpowiednich uprawnień.

Auditing Entry number	Auditing Entry for	Access	Apply onto	
			Windows Server 2003	Windows Server 2008 and above
1&2	Password Settings Container	◦ Create msDS-Password Settings objects ◦ Delete msDS-Password Setting objects	Not Applicable	This object and all descendant objects
		◦ Write All Propertie ◦ Delete ◦ Modify Permissions	Not Applicable	Descendant msDS-PasswordSettings objects



Obraz z następującymi informacjami: Auditing Entry numer 1.

Uwaga: Należy włączyć obie pozycje do inspekcji.

3.2.4 Konfiguracja inspekcji dla obiektów konfiguracji

i Zaloguj się do dowolnego komputera z przystawką **Active Directory Service Interfaces** Otwórz konsolę ADSI Edit → Kliknij prawym przyciskiem myszy ADSI Edit → Connect to.

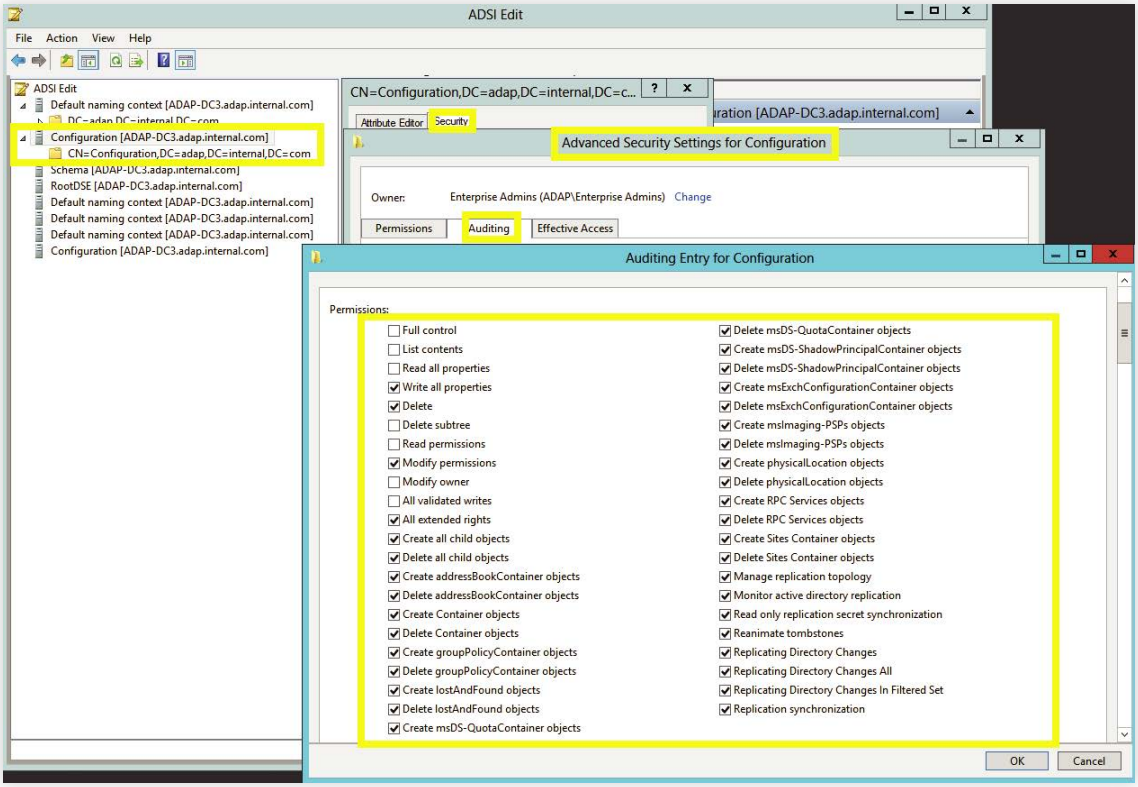
ii W oknie Connection Settings → W obszarze Select a Well-Known Naming Context → Wybierz Configuration.

iii Przejdź do lewego okienka → Kliknij Configuration → Kliknij prawym przyciskiem myszy Configuration naming context → Wybierz Properties → Security → Advanced → Auditing → Add.

iv W oknie Auditing Entry → Select a principal: Everyone → Type: Success → Wybierz odpowiednie uprawnienia zgodnie z poniższą tabelą.

Uwaga: za pomocą opcji Wyczyść wszystko usuń wszystkie uprawnienia i właściwości przed wyborem odpowiednich uprawnień.

Auditing Entry for	Access	Apply onto	
		Windows Server 2003	Windows Server 2008 and above
Configur-ation	• Create All Child objects • Write All Properties • Delete All child objects • Delete • Modify Permissions • All Extended Rights	This object and all child objects	This object and all



3.2.5 Konfiguracja inspekcji dla obiektów schematu

i Zaloguj się do dowolnego komputera z przystawką Active Directory Service Interfaces → Otwórz konsolę ADSI Edit → Kliknij prawym przyciskiem myszy ADSI Edit → Connect to.

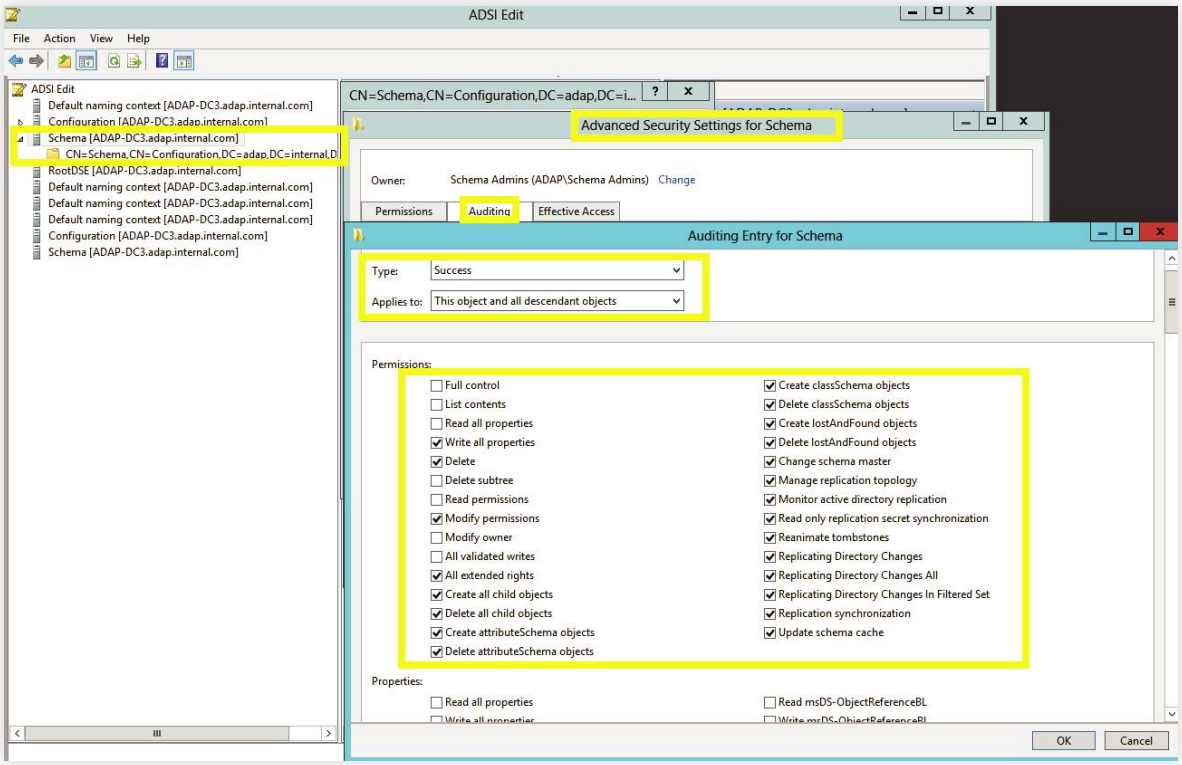
ii W oknie Connection Settings → W obszarze Select a Well-Known Naming Context → Wybierz schemat

iii Przejdź do lewego okienka → Kliknij schemat → Kliknij prawym przyciskiem myszy Schema naming context → Wybierz Properties → Security → Advanced → Auditing → Add.

iv W oknie Auditing Entry → Select a principal: Everyone → OK → Type: Success → Wybierz odpowiednie uprawnienia zgodnie z poniższą tabelą.

Uwaga: za pomocą opcji Wyczyść wszystko usuń wszystkie uprawnienia i właściwości przed wyborem odpowiednich uprawnień.

Auditing Entry for	Access	Apply onto	
		Windows Server 2003	Windows Server 2008 and above
Schema	• Create All Child objects • Write All Properties • Delete All child objects • Delete • Modify Permissions • All Extended Rights	This object and all child objects	This object and all descendant objects



3.2.6 Konfiguracja inspekcji dla obiektów DNS

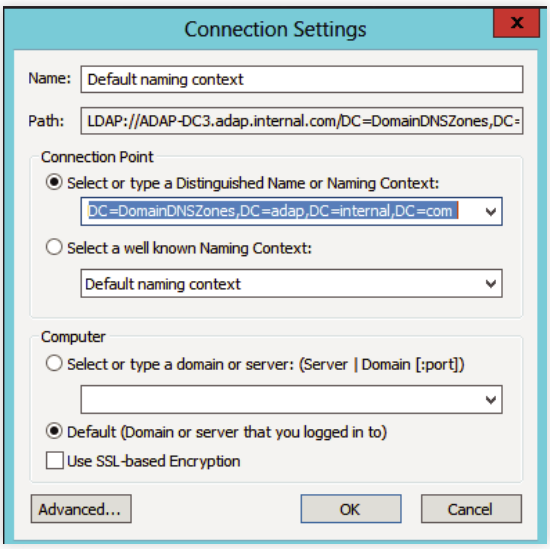
i Zaloguj się do dowolnego komputera z przystawką Active Directory Service Interfaces → Otwórz, typ uruchamiania adsiedit.msc → OK → Kliknij prawym przyciskiem myszy ADSI Edit → Connect to.

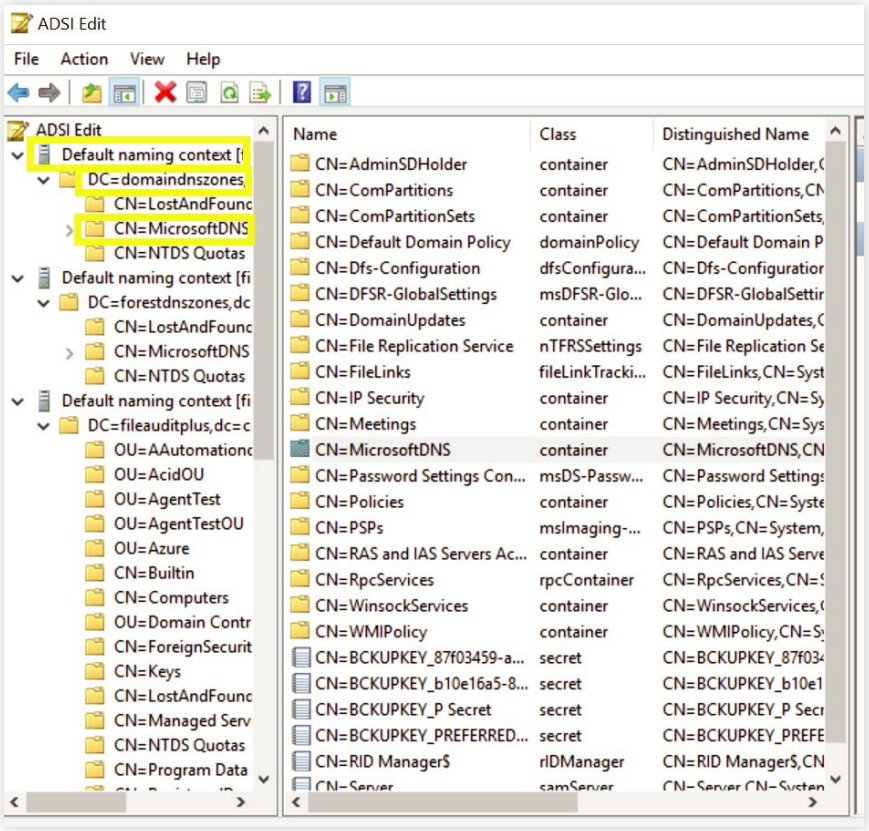
ii W oknie Connection Settings → W obszarze Select or type a Distinguished Name or Naming Context.

- Wprowadź DC=adap, DC=internal, DC=com jako nazwę wyróżniającą. (Ta partycja jest zazwyczaj domyślnie załadowana w Adsiedit)

- Wprowadź DC=DomainDNSZones, DC=adap, DC=internal, DC=com jako nazwę wyróżniającą.

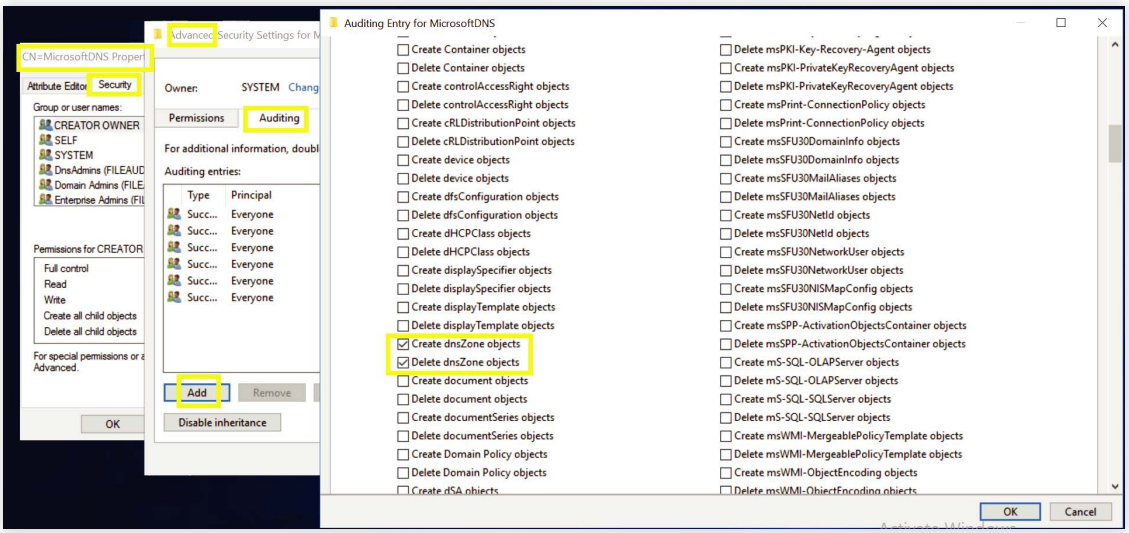
- Wprowadź DC=ForestDNSZones, DC=adap, DC=internal, DC=com jako nazwę wyróżniającą.





iii Przejdź do lewego okienka → Kliknij Default naming context → Kliknij prawym przyciskiem myszy DomainDNSZone naming context → Wybierz properties → Security → Advanced Auditing → Add.

iv W oknie Auditing Entry → Select a principal: Everyone → OK → Type: Success → Wybierz odpowiednie uprawnienia zgodnie z poniższą tabelą.

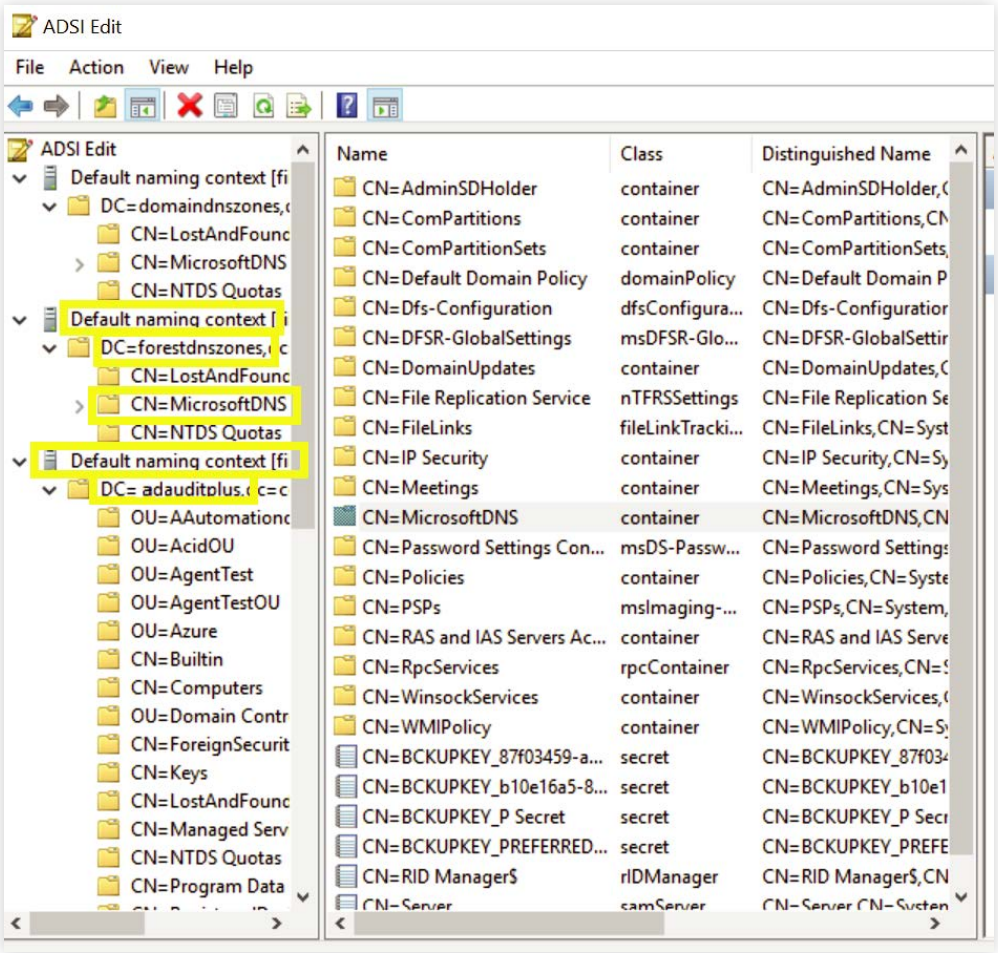


Uwaga: za pomocą opcji Wyczyść wszystko usuń wszystkie uprawnienia i właściwości przed wyborem odpowiednich uprawnień.

Auditing Entry number	Auditing Entry for	Access	Apply onto	
			Windows Server 2003	Windows Server 2008 and above
1&2	DNS Zones	• Create DNS Zones objects • Delete DNS Zones objects	This object and all child objects	This object and all descendant objects
		• Write All Properties • Delete • Modify Permissions	DNS Zone objects	Descendant DNS Zone objects
3&4 Permissions	DNS Nodes	• Create DNS Nodes objects • Delete DNS Nodes objects	This object and all child objects	Descendant DNS Zone objects
		• Write All Properties • Delete • Modify Permissions	DNS Node objects	Descendant DNS Node objects

Uwaga: Należy ukończyć wszystkie Auditing Entries.

Uwaga: Powtórz kroki iii. i iv. dla 2 pozostałych kontekstów nazewnictwa.



4. Konfiguracja ustawień dziennika zdarzeń

Ustawienie wartości progowej rozmiaru dziennika zdarzeń pomaga zapobiec utracie danych inspekcji. Jeśli rozmiar dziennika zdarzeń nie został określony w systemie, starsze wydarzenia zostaną zastąpione.

i Zaloguj się do dowolnego komputera z **Group Policy Management Console** (GPMC) używając poświadczeń administratora domeny → Otwórz GPMC → Kliknij Default Domain Controllers Policy → Edit.

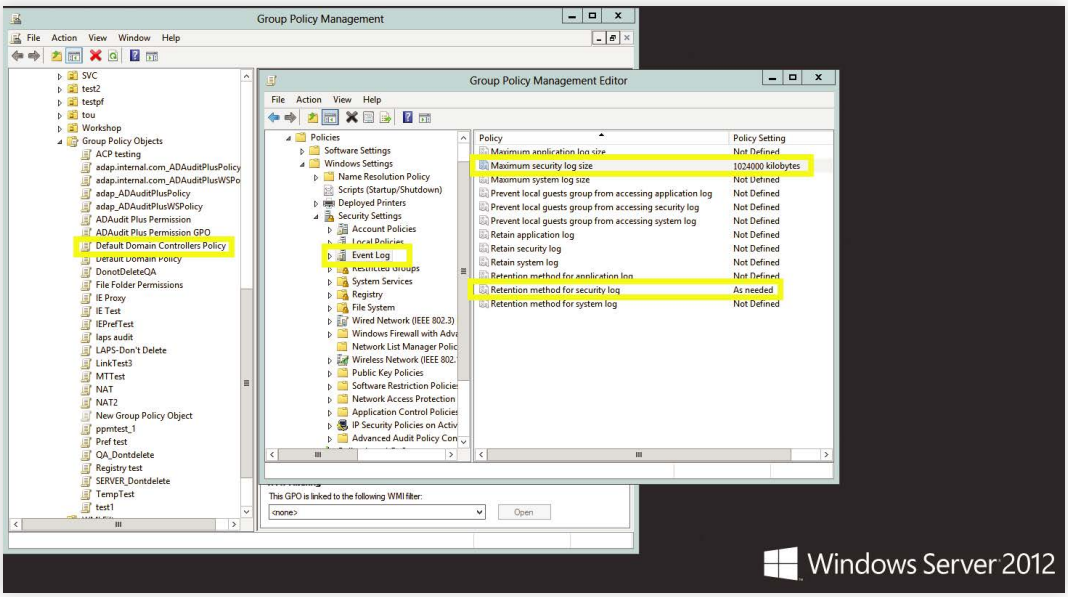
ii W obszarze Group Policy Management Editor → Computer Configuration → Policies → Windows Settings → Security Settings → Event Log.

iii Przejdź do prawego okienka → Kliknij prawym przyciskiem myszy Retention method for security log → Properties → Zastąp wydarzenia zgodnie z potrzebą.

iv Przejdź do prawego okienka → Kliknij prawym przyciskiem myszy Maximum security log size → Ustaw rozmiar zgodnie z informacjami w poniższej tabeli.

Uwaga: sprawdź, czy dzienniki zdarzeń zabezpieczeń mają wystarczająco miejsca na dane z co najmniej 12 godzin.

Role	Operating System	Size
Domain Controller	Windows Server 2003	512 MB
Domain Controller	Windows Server 2008 and above	1024 MB



5. Rozwiązywanie problemów — FAQ

i **Sprawdzanie konfiguracji danych zasad inspekcji i ustawień dziennika zabezpieczeń:**
Zaloguj się do dowolnego komputera z Group Policy Management Console (GPMC) używając poświadczeń administratora domeny → Otwórz GPMC → Kliknij prawym przyciskiem myszy Group Policy Results → Group Policy Results Wizard → Wybierz komputer i użytkownika (bieżącego użytkownika) → Sprawdź, czy dane ustawienia zostały skonfigurowane.

ii **Aby sprawdzić, czy wymagane ustawienia inspekcji na poziomie obiektu zostały skonfigurowane:**
Wykonaj instrukcje podane w kroku 3.2 w tym dokumencie.

iii **Aby zweryfikować, czy dane zdarzenia są rejestrowane:**
Zaloguj się do dowolnego komputera za pomocą poświadczeń administratora domeny → Otwórz obszar Run → Wpisz eventvwr.msc → Kliknij prawym przyciskiem myszy Event Viewer → Połącz się z komputerem docelowym → Sprawdź, czy wydarzenie związane ze skonfigurowanymi zasadami inspekcji są rejestrowane.

Na przykład: zakończona powodzeniem konfiguracja Kerberos Authentication Service Success advanced audit policy powinna zakończyć się zarejestrowaniem wydarzenia o identyfikatorze 4768.