Del 4 – Authentication Policy Silos

Tier0-skydd för domänkontrollant
GreenTyre Recycling AB

Datum: 2026-02-28

Upprättad av: Julian Rieger – IT-säkerhetskonsult

Kurs: IAM – Identity and Access Management

Domän: mylab.local (Windows Server 2019)

DC-namn: WIN2019VM

1. Inledning

Authentication Policy Silos är en avancerad säkerhetsfunktion i Active Directory Domain Services (AD DS) som introducerades i Windows Server 2012 R2. Funktionen möjliggör strikt kontroll över VAR privilegierade konton får autentisera, en central del i en Tier-modell för administrativ åtkomst.

I GreenTyre Recycling AB:s miljö innebär detta att Tier0-administratörskontot DA_Admin enbart kan logga in på domänkontrollanten (WIN2019VM). Försök att logga in på vanliga klientdatorer nekas av KDC:n (Key Distribution Center) innan autentiseringen ens påbörjas.

2. Bakgrund – Tier-modellen och Authentication Policy Silos

Microsofts Tier-modell (Enterprise Access Model) delar upp administrativ åtkomst i tre nivåer för att förhindra att ett kompromitterat konto på en lägre nivå kan eskalera privilegier till en högre:

Nivå	Objekt som skyddas	Exempel på konton
Tier 0	AD DS, domänkontrollanter, PKI	DA_Admin, Schema Admins
Tier 1	Servrar, applikationer	Serveradministratörer
Tier 2	Klientdatorer, användare	Helpdesk, vanliga admins

Authentication Policy Silos är den tekniska mekanismen som tvingar fram Tier-separationen ett Tier0-konto nekas fysiskt att autentisera mot Tier1- eller Tier2-enheter, även om kontot råkar ha lösenordet kompromitterat.

3. Labbmiljö

Komponent	Detaljer
Domänkontrollant (DC)	WIN2019VM – Windows Server 2019, mylab.local
Domännivå	Windows Server 2016 (kompatibel med silos)
Klientdator	Windows 11 – domänansluten till mylab.local
Tier0-konto	DA_Admin – medlem i Domain Admins och Tier0_Admins

4. Konfiguration

4.1 Del 1 – Skapa DA_Admin

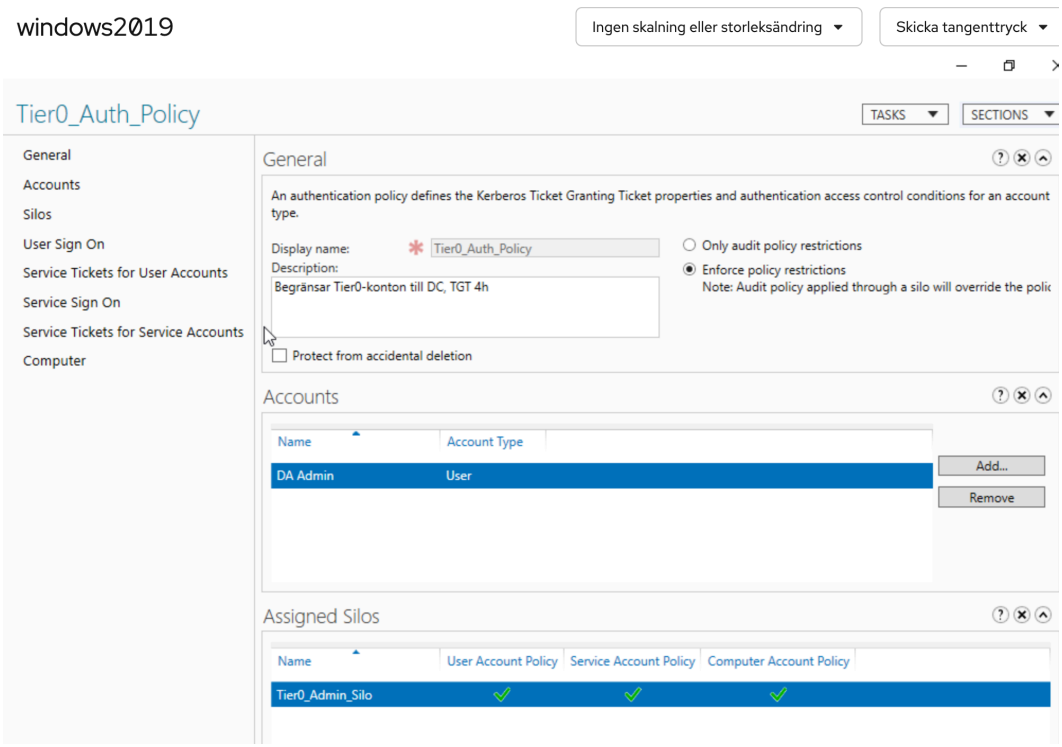
Ett dedikerat Tier0-administratörskonto skapades separerat från det vanliga administratörskontot, i enlighet med principen om minsta privilegium och Tier-separation:

Egenskap	Värde
Namn	DA Admin
SamAccountName	DA_Admin
OU	OU=admins, OU=IT, DC=mylab,
Gruppmedlemskap	Domain Admins, Tier0_Admins

4.2 Del 2 – Skapa autentiseringspolicy (Tier0_Auth_Policy)

En autentiseringspolicy skapades i Active Directory Administrative Center (ADAC) med två Kerberos-krav som begränsar Tier0-kontots autentisering:

Kerberos-krav	Inställning	Syfte
Krav 1: TGT-livstid	240 minuter (4 timmar)	Kortare livstid på Kerberos-biljetten — standardvärde är 10 timmar. Minimerar risken vid en kompromitterad biljett.
Krav 2: Silo-tillhörighet	Enforce-läge aktiverat	KDC:n nekar autentisering om kontot eller datorn inte är med i silon.

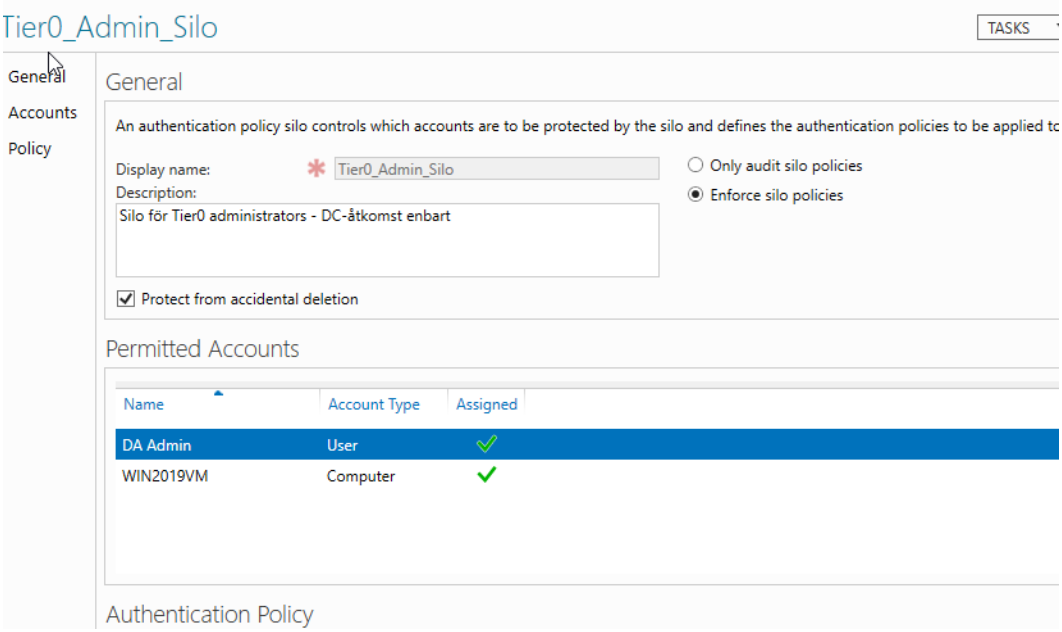


Figur 1 – Tier0_Auth_Policy i Active Directory Administrative Center

4.3 Del 3 – Skapa silo (Tier0_Admin_Silo)

Silon skapades och konfigurerades med användare och datorer som tillsammans bildar det betrodda Tier0-segmentet:

Objekt	Typ	Roll i silon
DA_Admin	Användare	Tier0-administratörskonto – enda kontot som får logga in på DC
WIN2019VM	Dator	Domänkontrollant – enda maskinen DA_Admin får logga in på
Tier0_Auth_Policy	Policy	Kerberos-policy med TGT 4h och silo-enforcement



Figur 2 – Tier0_Admin_Silo i ADAC med DA_Admin och WIN2019VM som medlemmar

4.4 Del 4 – Aktivera Enforce-läge

Silon sattes i Enforce-läge (till skillnad från Audit-läge som enbart loggar). I Enforce-läge nekar KDC:n aktivt autentiseringsförfrågningar som bryter mot silons regler. I produktionsmiljö rekommenderas att Audit-läge testas under minst en vecka innan Enforce aktiveras.

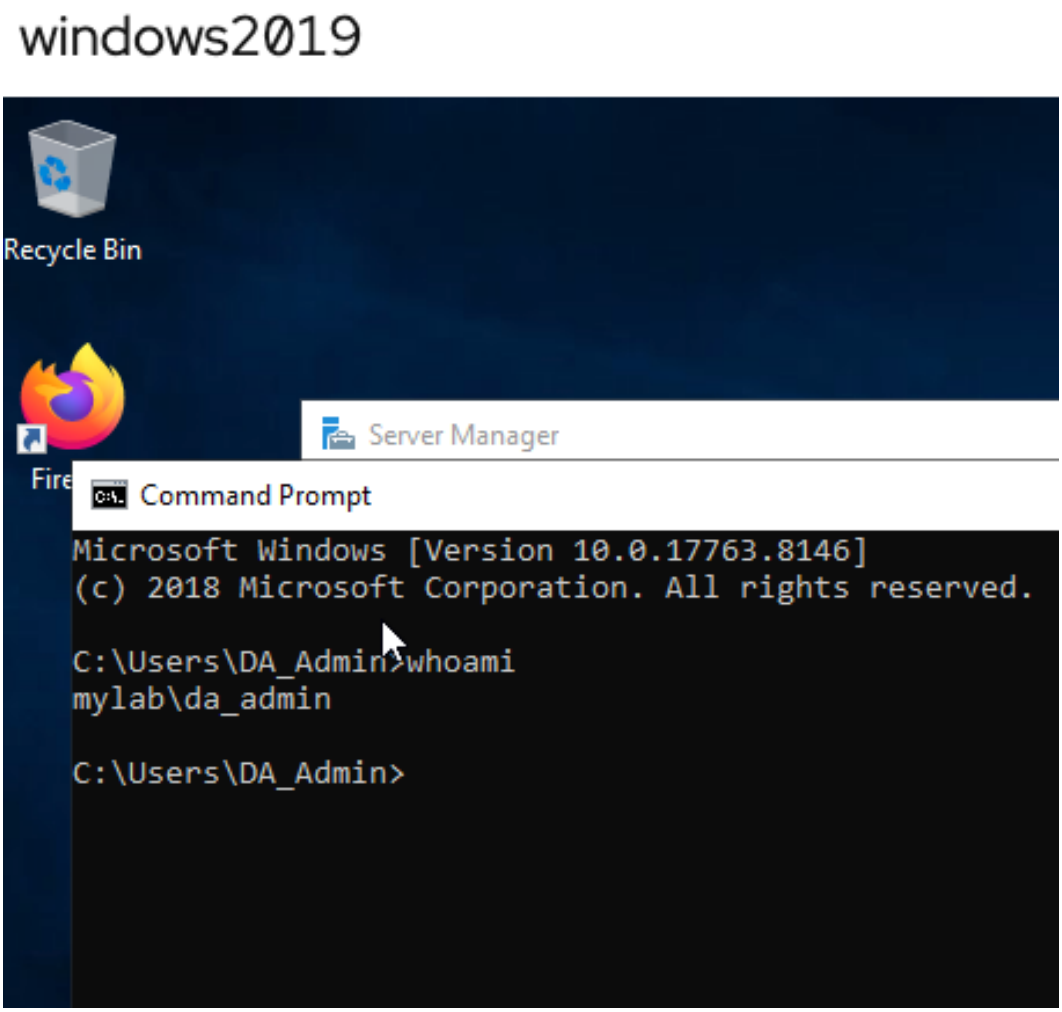
Läge	Beteende
Audit-läge	Loggar autentiseringshändelser i Security Event Log men nekar inte åtkomst. Används för att verifiera konfigurationen innan produktionssättning.
Enforce-läge	KDC:n nekar aktivt autentisering som bryter mot silons regler. Händelse 4820 loggas vid nekad autentisering.

5. Testresultat (Del 5)

Inloggningstester genomfördes för att verifiera att silon fungerar korrekt. Testerna utfördes via RDP mot domänkontrollanten samt via inloggning på den domänanslutna Windows 11-klienten.

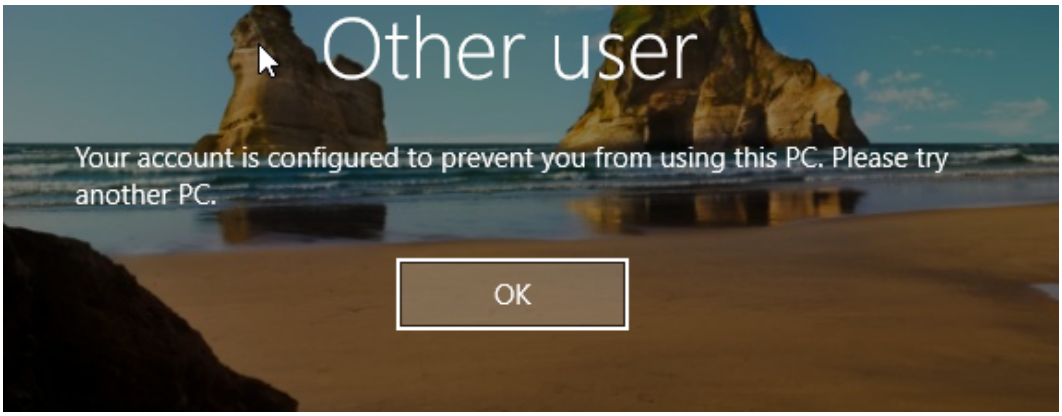
Scenario	Konto	Maskin	Förväntat / Resultat
Test 1 – Tier0 på DC	DA_Admin (i silo)	WIN2019VM (i silo)	**TILLÅTEN – Inloggning lyckas**
Test 2 – Tier0 på klient	DA_Admin (i silo)	Windows 11 (ej i silo)	**NEKAD – Kerberos-fel**

Screenshot nedan visar DA_Admin inloggad på DC (WIN2019VM). PowerShell-kommandot whoami bekräftar kontot:



Figur 3 – DA_Admin (mylab\da_admin) inloggad på WIN2019VM (DC)

Screenshot nedan visar nekad inloggning när DA_Admin försöker logga in på Windows 11-klienten som inte är med i silon:

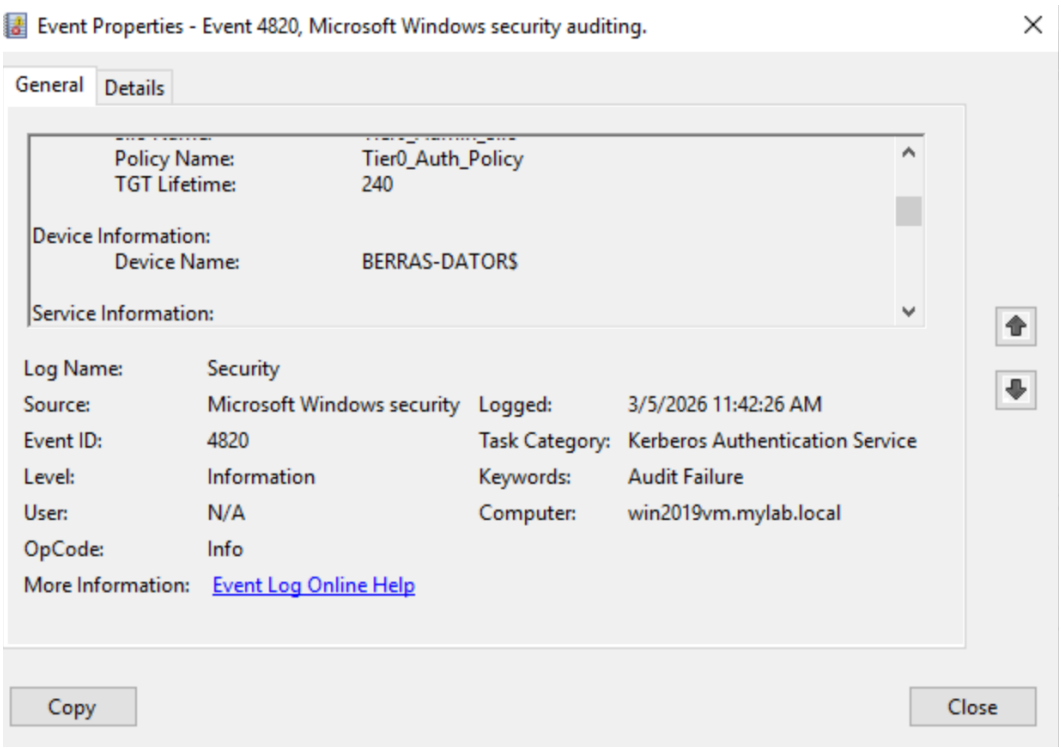


Figur 4 – DA_Admin nekas inloggning på Windows 11-klienten

6. Verifiering via händelseloggen

Autentiseringshändelser relaterade till Authentication Policy Silos loggas i Windows Security Event Log. Relevanta Event ID:n:

Event ID	Händelse	Innebörd
4820	Kerberos TGT nekad – silo	Autentisering nekad pga silo-regelbrott (Enforce-läge)
4821	Kerberos TGT nekad – policy	Autentisering nekad pga policybrott
4822	NTLM nekad – silo	NTLM-autentisering nekad för silo-konto
4626	Silo-tilldelning	Konto tilldelat silo vid inloggning (Audit-läge)



Figur 5 – Security Event Log med silo-relaterade händelser

7. Koppling till NIS2 och ISO 27001

Krav/Kontroll	Källa	Hur labben uppfyller kravet
Art. 21.2(a) – Åtkomstkontroll	NIS2	Tier0-konton begränsas strikt till DC via silo-enforcement
Art. 21.2(b) – Minsta privilegium	NIS2	DA_Admin kan inte användas på klientdatorer – minimerar attackyta
Kontroll 8.2 – Privilegierad åtkomst	ISO 27002:2022	Privilegierade konton isoleras i Tier0-silo med kortare TGT-livstid
Kontroll 5.3 – Segregation of duties	ISO 27002:2022	Tier0-administratörer är tekniskt separerade från Tier1/2-miljöer

8. Slutsats och reflektion

Authentication Policy Silos är ett kraftfullt verktyg för att implementera Tier-separation i Active Directory. Labben visar att det går att tekniskt tvinga fram att Tier0-konton (DA_Admin) enbart kan autentisera mot domänkontrollanten, och nekas på alla andra enheter.

- Tier0-separation: DA_Admin är fysiskt begränsad till DC – även om lösenordet kompromitteras kan angriparen inte logga in från en vanlig klientdator

- Kortare TGT-livstid: 4 timmar istället för standardmässiga 10 timmar minskar fönstret för pass-the-ticket-attacker
- Händelseloggning: Alla nekade försök loggas med Event ID 4820 för forensisk granskning
- NIS2-efterlevnad: Uppfyller krav på åtkomstkontroll och minsta privilegium för kritisk infrastruktur