Microsoft Windows domēns - lietotāju kontu bloķēšana pēc vairākiem neveiksmīgiem pieslēgšanās mēģinājumiem

1. Domēna kontrolierī (DC) atrodam Group Policy Management sadaļu un tajā rediģējam "Default Domain Policy" grupu politikas objektu (GPO).



Spiežam uz Start/Windows logo un uzreiz rakstam jeb meklēšanas laukā (ikona ar lupu) ievadam group policy un izvēlamies "Group Policy Management"

	🥱   🚩 Manage Tools View Help
	Active Directory Administrative Center
	Active Directory Domains and Trusts
	Active Directory Module for Windows PowerShell
	Active Directory Sites and Services
	Active Directory Users and Computers
	ADSI Edit
	Component Services
	Computer Management
	Defragment and Optimize Drives
	Disk Cleanup
	DNS
	Event Viewer
	Group Policy Management
	iSCSI Initiator
	Local Security Policy
	Microsoft Azure Services
	ODBC Data Sources (32-bit)
	ODBC Data Sources (64-bit)
	Performance Monitor
	Print Management
Servers	Recovery Drive
I Derverb	Registry Editor
anageabil	Resource Monitor
ents	Services
	System Configuration
ervices	System Information
erformanc	Task Scheduler
A results	Windows Defender Firewall with Advanced Security
	Windows Memory Diagnostic
	Windows PowerShell
	Windows PowerShell (x86)
	Windows PowerShell ISE
	Windows PowerShell ISE (x86)
	Windows Server Backup

**CERT.LV** 

Šis ir vēl viens variants, kā atvērt "Group Policy Management" - Server Manager -> Tools un izvēlēties "Group Policy Manegement"

## Group Policy Management Help File File Action View Window 📅 🖺 💢 🗖 | ? (= K Group Policy Management Def ✓ A Forest: lab.local Sco ✓ Call Domains Lin lab.local × 🟥 Dis 🛒 Default Domain Policy Domain Controllers The > Microsoft Exchange Security Groups L ✓ Group Policy Objects 1 Default Domain Controllers Policy Default Domain Policy Edit... > 📑 WMI Filters GPO Status > > 🧊 Starter GPOs > 📑 Sites Back Up... 👸 Group Policy Modeling Restore from Backup... 🕞 Group Policy Results Import Settings... Save Report... View > New Window from Here Copy Delete Se Rename The Refresh N Help 8

CERT.LV

Atrodam Group Policy Objects -> Default Domain Policy un uzspiežot ar labo peles klikšķi izvēlamies Edit

 Rediģējam esošo "Default Domain Policy" - kad domēna lietotājs mēģina pieslēgties iekārtai (arī attālināti ar Remote Desktop) tiek skaitīti secīgi neveiksmīgas pieslēgšanās mēģinājumi (šeit piemērs ir ar 10 reizēm) un, kad definētais limits ir sasniegts, lietotāja konts tiek īslaicīgi bloķēts (šajā piemērā tas ir uz 15 minūtēm) vai arī līdz brīdim, kad sistēmas Administrators lietotāju atbloķē (skatīt 5. punktu).



Atveram Computer Configuration- > Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

Izvēlamies sekojošas vērtības (tās, protams, var pielāgot sava uzņēmuma/organizācijas vajadzībām):

Account lockout duration – 15

Account lockout threshold - 10

Reset account lockout counter after - 15

3. Pārliecināmies, ka tikko rediģētie uzstādījumi ir saglabājušies un ka politika ir piesaistīta visam domēnam (vai pēc nepieciešamības, piemēram, pakārtota tikai konkrētam Organizational Unit). Jāpiemin, ka domēna politika ņems virsroku pār lokālo iekārtas politiku, t.i. gadījumā, ja uz iekārtas ir arī lokālie lietotāju konti, tad šī politika attieksies arī uz tiem.

Group Policy Management		
File Action View Window Help		
Group Policy Management     A Forest: lab.local     Bomains     Iab.local     J Default Domain Policy     J ⊆ Domain Controllers     J ⊆ Domain Controllers     J ⊆ Group Policy Objects     J ⊆ WMI Filters     J ⊆ Starter GPOs	Default Domain Policy Scope Details Settings Delegation	
	Default Domain Policy Data collected on: 01.06.2021 12:29:31	
	General	
	Details	
	Links	
Group Policy Modeling	Security Filtering	
	Delegation	
	Computer Configuration (Enabled)	
	Policies	
	Windows Settings	
	Security Settings	
	Account Policies/Password Policy	
	Account Policies/Account Lockout Policy	
	Policy	Setting
	Account lockout duration	15 minutes
	Account lockout threshold	10 invalid logon attempts
	Reset account lockout counter after	15 minutes
	Account Policies /Kachame Policy	

Atgriežamies pie Group Policy Management paneļa un redzam, ka Default Domain Policy GPO ir piesaistīts visam domēnam. Uzklikšķinot uz šīs politikas un labajā pusē izvēloties Settings, varam vēlreiz apskatīt izveidotos GPO uzstādījumus un pārliecināties, ka viss ir korekti.

III Tieši šāds pieslēgšanās mēģinājumu skaits un bloķēšanas ilgums lietotāju kontiem tiek rekomendētas no Microsoft puses (*Windows security baselines*). Vairāk informācijas par šiem un arī citiem ar drošību saistītiem iestatījumiem, pieejama šeit: <u>https://www.microsoft.com/en-</u> <u>us/download/details.aspx?id=55319</u>

4. Pēc politikas uzstādīšanas un izplatīšanas (piemēram ar gpupdate/force), domēna lietotāji, mēģinot pieslēgties Windows sistēmai ar vairāk nekā 10 secīgiem neveiksmīgiem mēģinājumiem, redzēs kādu no šiem vai citu līdzīgu paziņojumu (atkarīgs no OS versijas):



Paziņojums par bloķētu lietotāja kontu Windows 10/Windows Server2016/ Windows Server2019 operētājsistēmā

CER	T.LV	_∧_
	Ite referenced account is currently locked out and may not be logged on to.	
	Stradows <sup>-7</sup> Professional	

Paziņojums par bloķētu lietotāja kontu Windows 7 operētājsistēmā



Paziņojums par bloķētu lietotāja kontu, ja izmanto Windows Remote Desktop programmatūru, lai pieslēgtos sistēmai attālināti

CERT.LV

5. Lietotāja konts atbloķēsies, kā arī neveiksmīgo mēģinājumu skaits *nonullēsies* automātiski pēc 15 minūtēm ( šīs vērtības tika norādītas šīs instrukcijas otrajā punktā). Gadījumā, ja ir nepieciešams kontu atbloķēt nekavējoties, sistēmas administratoram ir pieejama šāda opcija. To var izdarīt, aktīvajā direktorijā atrodot vajadzīgo lietotāju un ieliekot ķeksīti pie "Unlock account" (šo var darīt arī izmantojot Powershell).

Active Directory Users and Computers -										
File Action View Help										
🗢 🔿 🖄 📰 🖌 🛅	] 🙆 🗟   🛛 🖬   🖏	2 🕯 🎙	7 🗾 🗿							
Active Directory Users and Com	Name	Type		Desc	Description					
> 📔 Saved Queries <ul> <li>Iab.local</li> </ul>	Janis Properties				?	×				
> 📔 Builtin	Member Of	Dial-in	Envi	ronment	Sessions	to				
> 📋 Computers	Remote control	Remote D	Desktop Services Profile		COM+					
> 📓 Domain Controllers	General Address	Account	Profile	Telephones	Organizatio	on [				
> ForeignSecurityPrincipal:	User logon name:					· · · ·				
Managed Service Accourt Missage & Euclosupe Service	ianis		7							
Ilsers	Microsoft Exchange Secu									
	User logon name (pre-\	Windows 2000	U):			ıe				
	LADU		Janis							
	Logon Hours	Log On To	D			Þ				
	Unlock account. Th	nis account is	currently lo	cked out on th	is Active	Þ				
	Directory Domain C	ontroller.				an				
	Account options:					P				
	User must chang	Ulear must change password at part logon								
	User cannot cha	User cannot change password at next logon								
	Password never expires									
□ Store password using reversible encryption ✓										
< >	Account expires									
	Never									
	O End of:	otutdiopa 20	21 and-	1 :51:5		Pe				
		etuntulena, 20	iz i. yaua	r. julijs						
BPA results						B				
	OK		ancel	Apply	Help					

Lietotāja atbloķēšana, izmantojot AD grafisko interfeisu - ieliekot ķeksi pie "Unlock acccount"

## PAPILDUS IETEIKUMS:

Rekomendējam Windows domēnā ieslēgt arī auditācijas pierakstus, kas ir attiecināmi uz lietotāju kontu bloķēšanos. To var izdarīt, veidojot jaunu GPO vai arī izmantojot jau esošu politiku un izvēloties **Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Logon/Logoff:** Audit Account Lockout -Failure.



CERT.LV

Tiks reģistrēti tikai Failure notikumi, t.i. neveiksmīgie pieslēgšanās mēģinājumi, kamēr konts ir bloķēts. Šie notikumi Windows žurnālierakstos tiek apzīmēti ar EventID:4625 (par šo EventID vairāk var lasīt šeit: <u>https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625</u>)

!!! CERT.LV ir izstrādājusi rekomendācijas auditēšanas iestatījumiem Windows domēna infrastruktūrā, ar kurām varat iepazīties šeit: <u>https://cert.lv/lv/2020/04/rekomendacijas-auditesanas-iestatijumiem-</u> <u>windows-domena-infrastruktura</u>