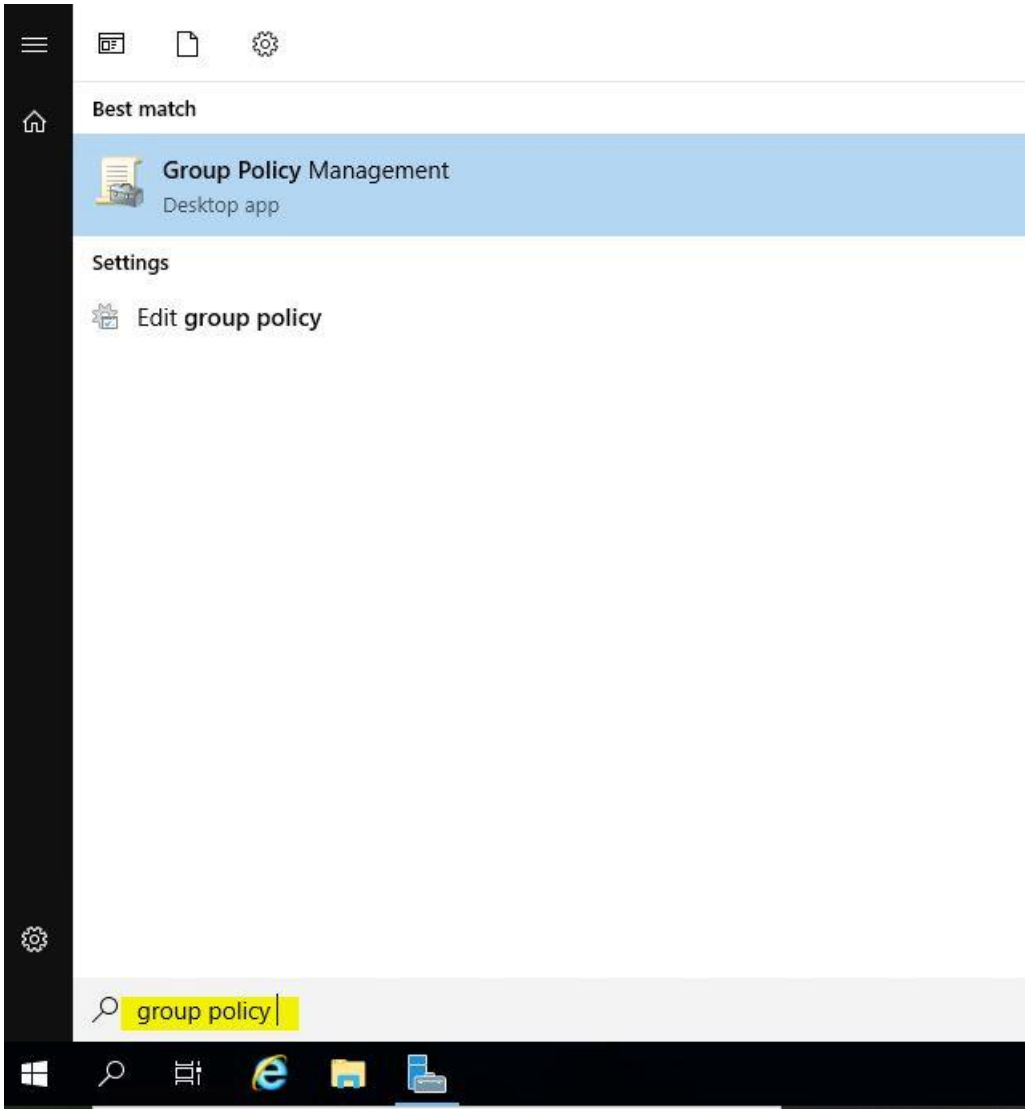
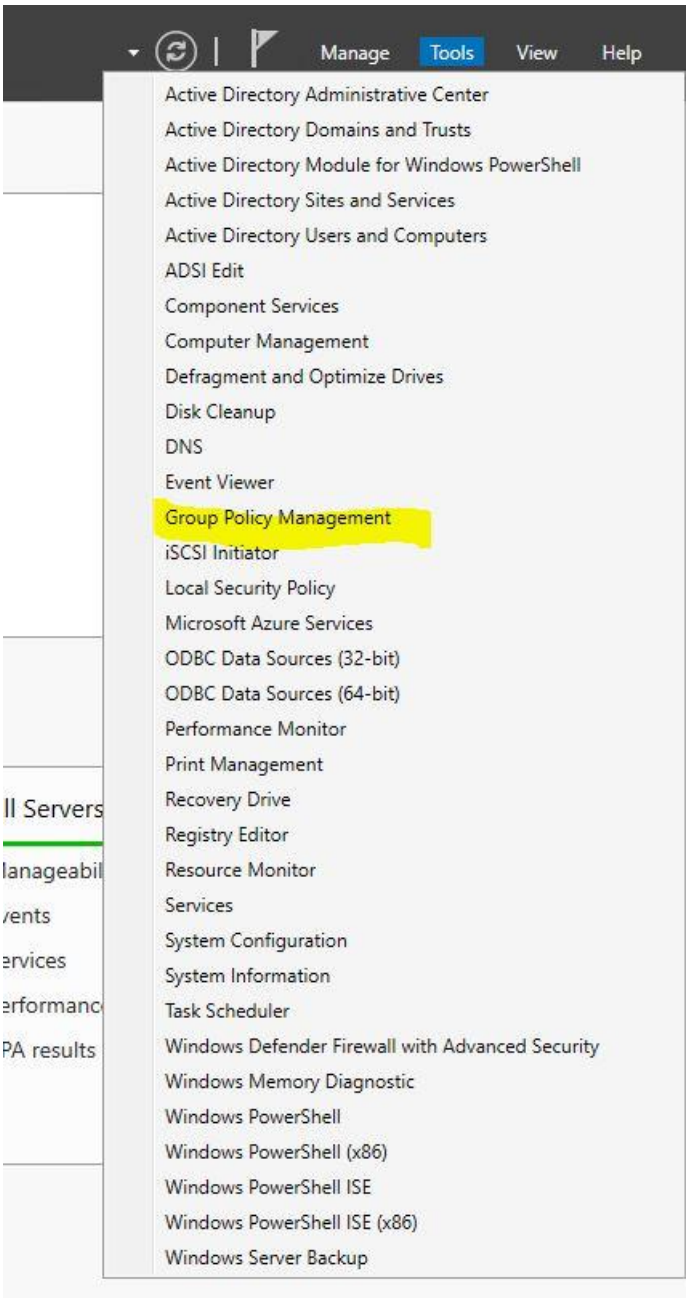
Microsoft Windows domēns - lietotāju kontu bloķēšana pēc vairākiem neveiksmīgiem pieslēgšanās mēģinājumiem

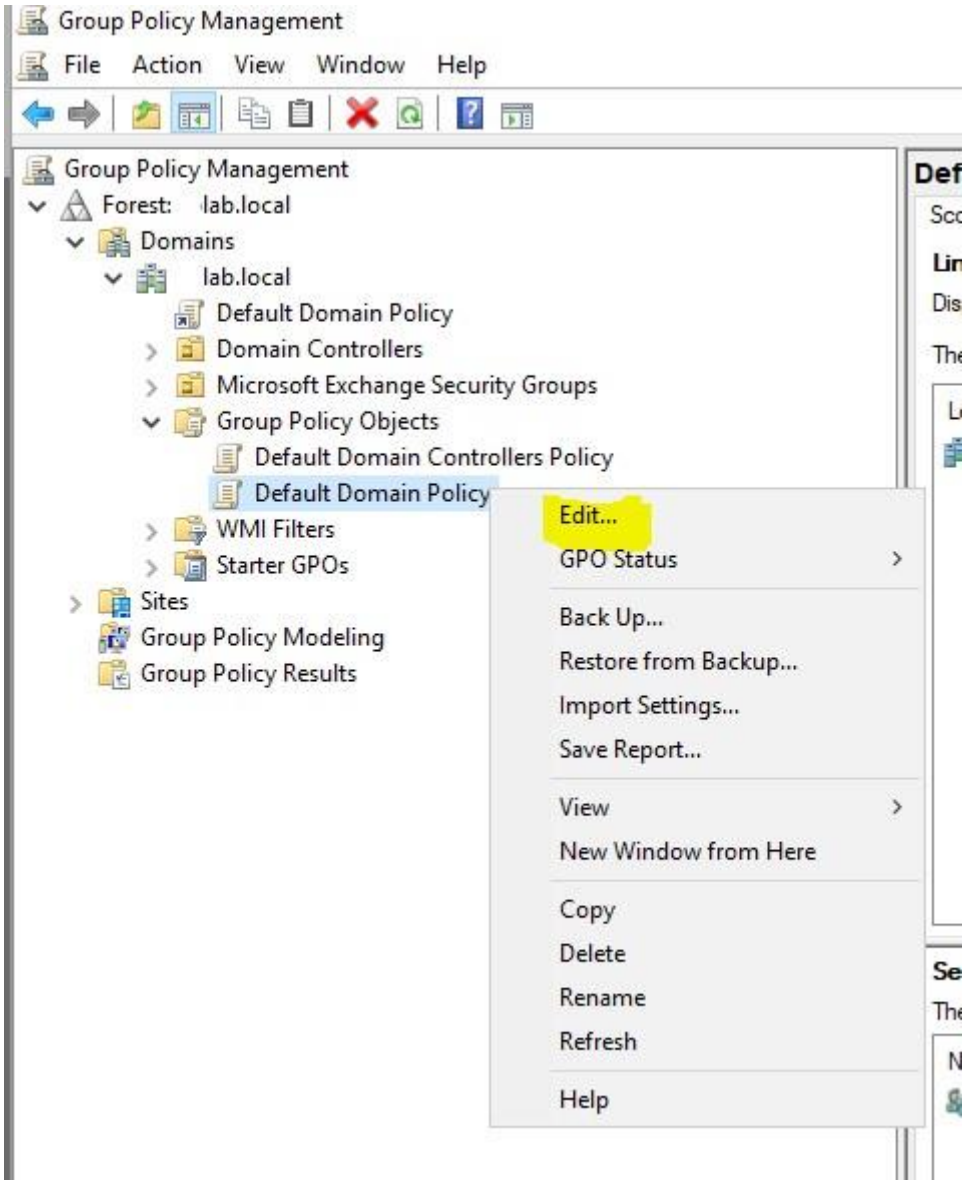
1. Domēna kontrolierī (DC) atrodam Group Policy Management sadaļu un tajā rediģējam "Default Domain Policy" grupu politikas objektu (GPO).



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

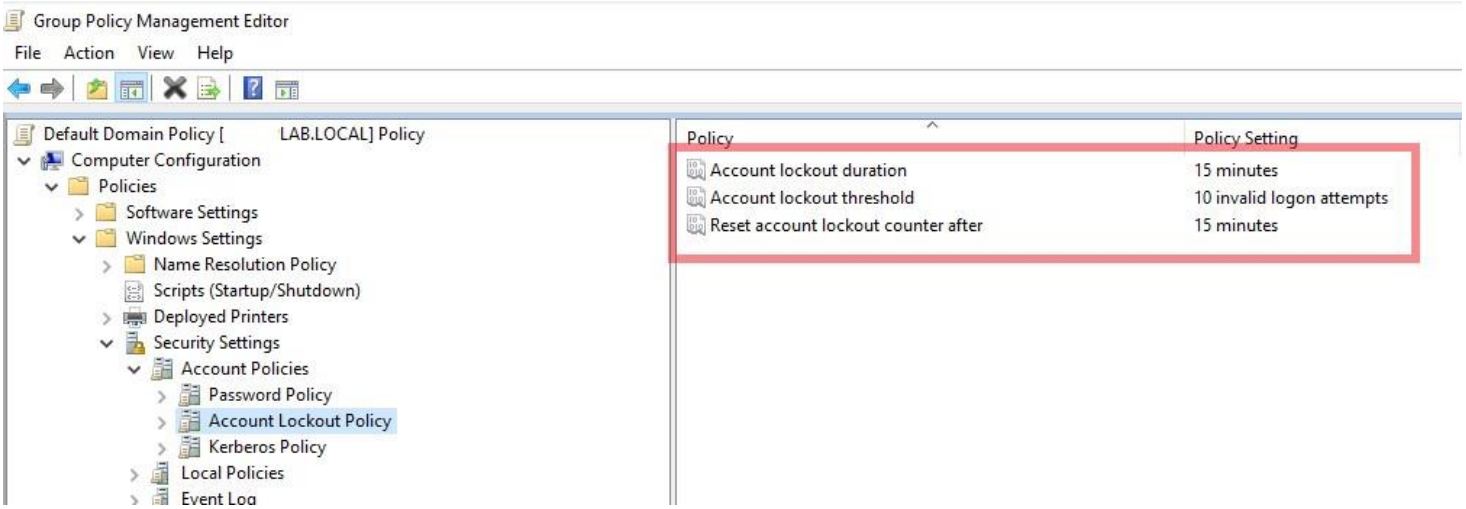


Šis ir vēl viens variants, kā atvērt “Group Policy Management” - Server Manager -> Tools un izvēlēties “Group Policy Manegement”



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

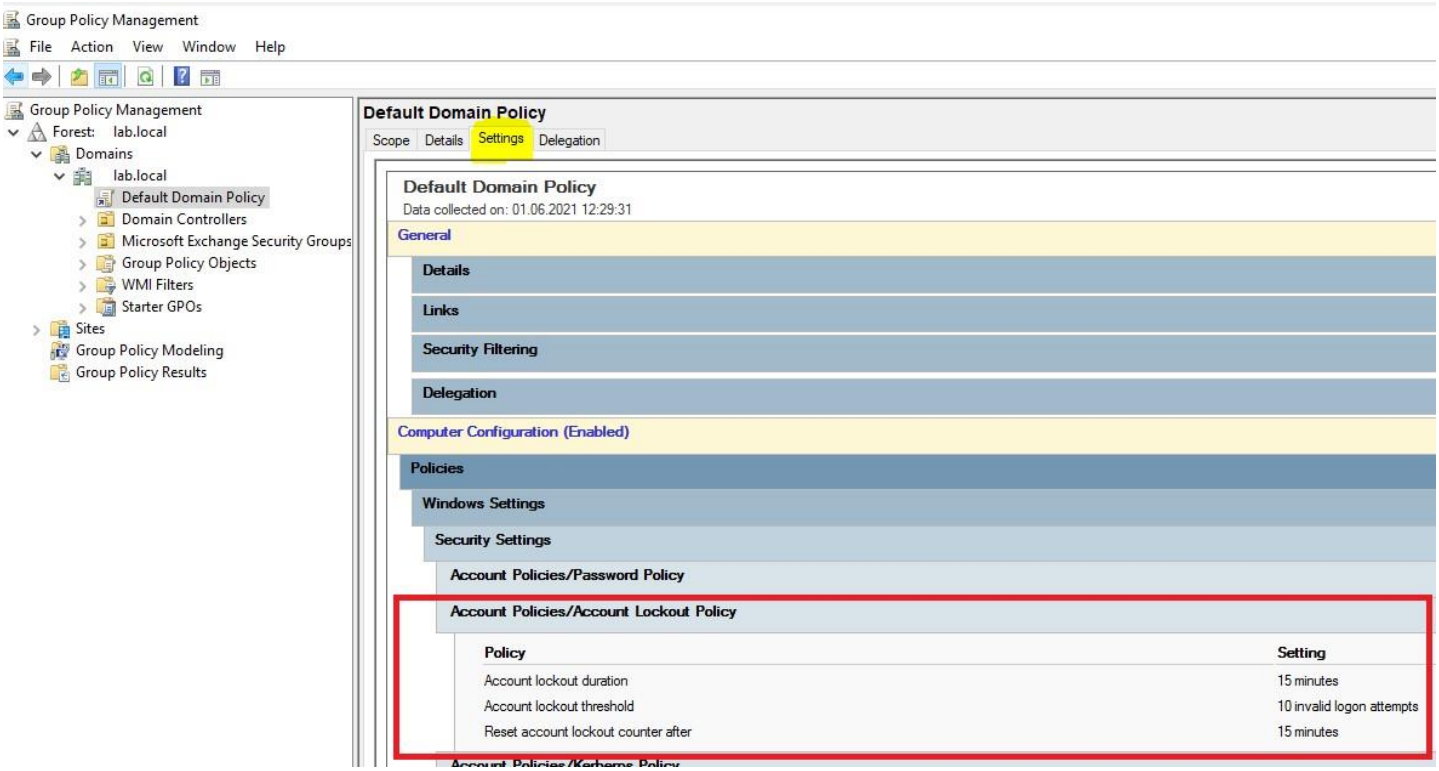
2. Rediģējam esošo "Default Domain Policy" - kad domēna lietotājs mēģina pieslēgties iekārtai (arī attālināti ar Remote Desktop) tiek skaitīti secīgi neveiksmīgas pieslēgšanās mēģinājumi (šeit piemērs ir ar 10 reizēm) un, kad definētais limits ir sasniegts, lietotāja konts tiek īslaicīgi bloķēts (šajā 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.

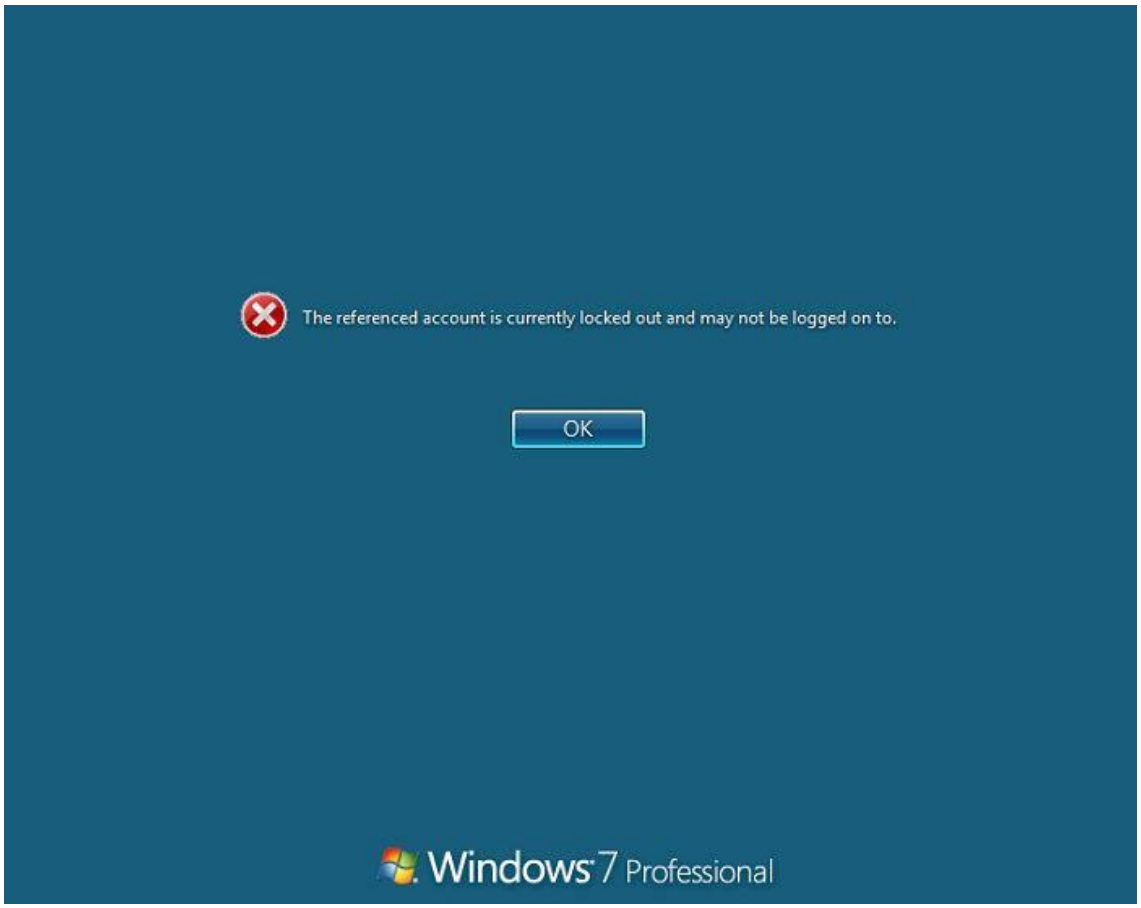


Atgriežamies pie `Group Policy Management` paneļa un redzam, ka `Default Domain Policy` GPO ir piesaistīts visam domēnam. Uzklikšķinot uz šīs politikas un labajā pusē izvēloties `Settings`, varam vēlreiz apskatīt izveidotos GPO uzstādījumus un pārliecināties, ka viss ir korekti.

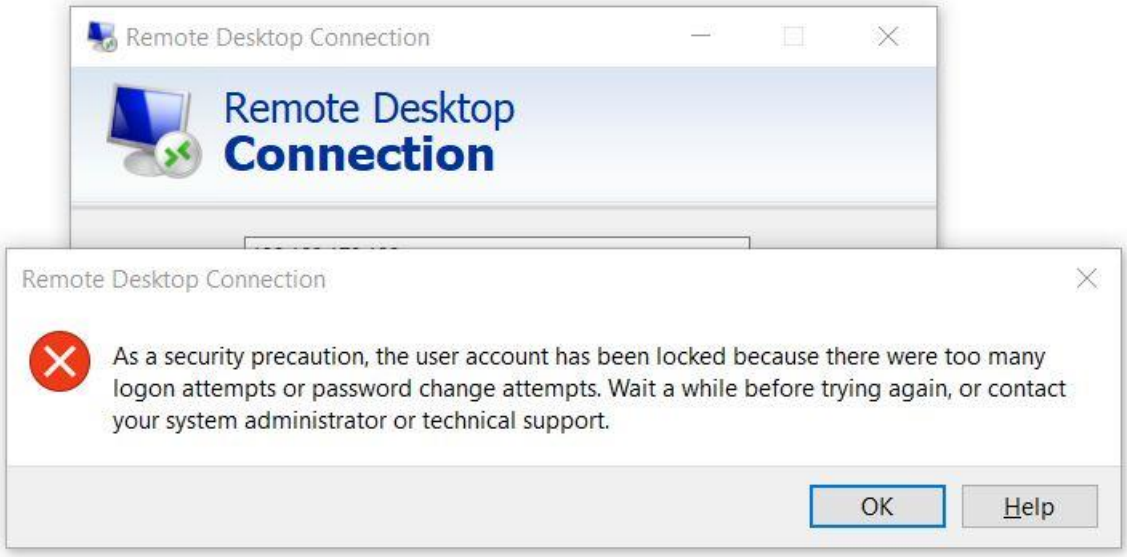
!!! Tieši šāds pieslēgšanās mēģinājumu skaits un bloķēšanas ilgums lietotāju kontiem tiek rekomendētas no Microsoft puses (*Windows security baselines*). Vairāk informācijas par šiem un arī citiem ar drošību saistītiem iestatījumiem, pieejama šeit: https://www.microsoft.com/en-us/download/details.aspx?id=55319

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

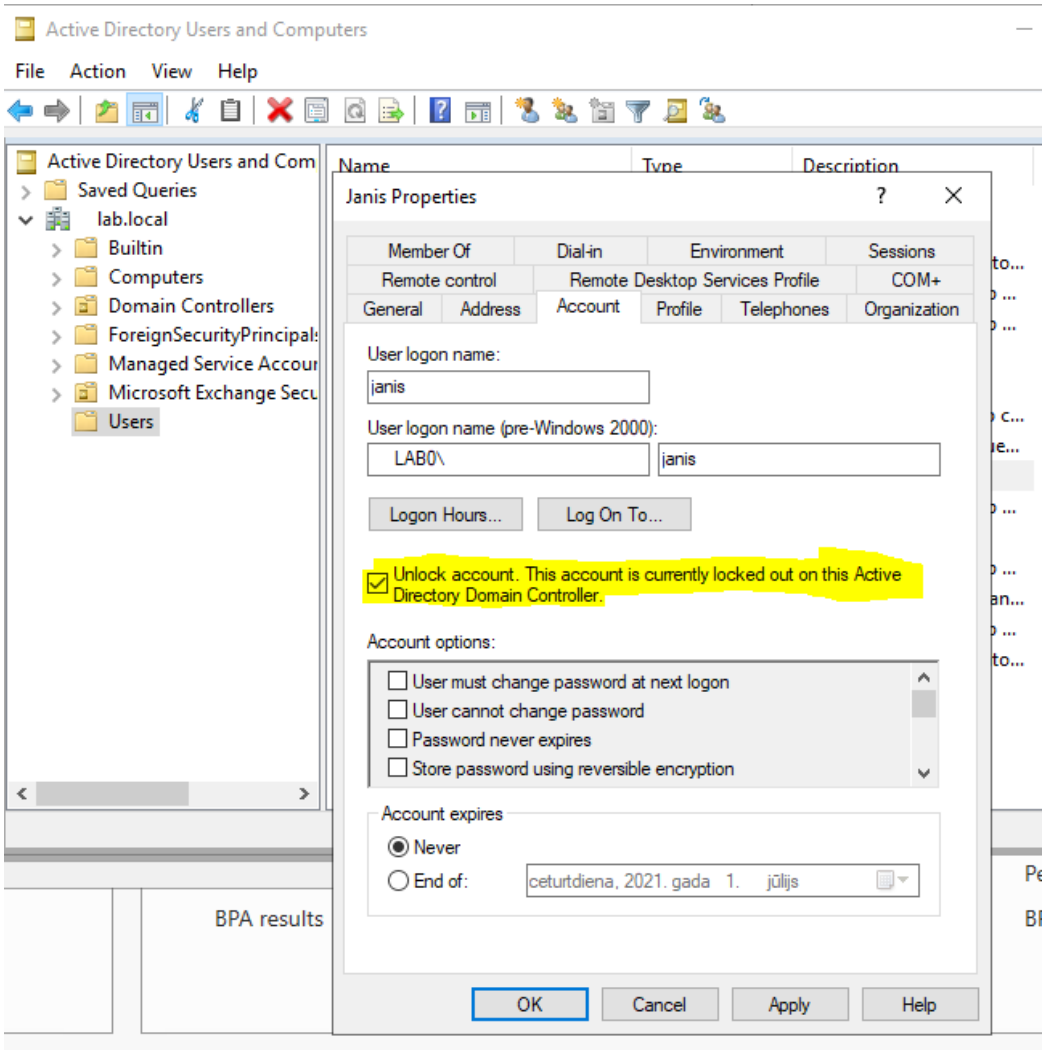


Paziņojums par bloķētu lietotāja kontu Windows 7 operētājsistēmā



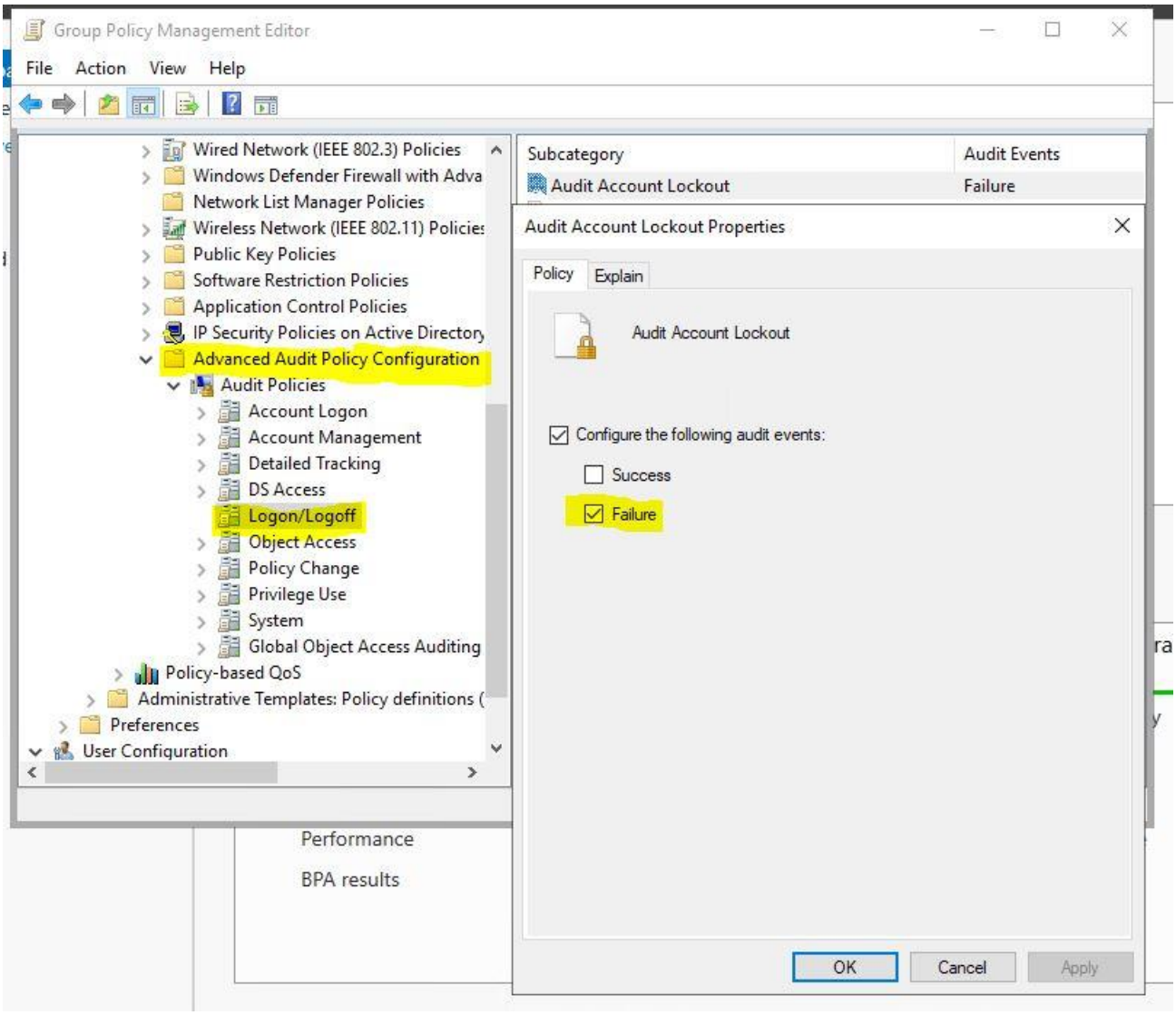
Paziņojums par bloķētu lietotāja kontu, ja izmanto Windows Remote Desktop programmatūru, lai pieslēgtos sistēmai attālināti

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).



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.`



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: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625)

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