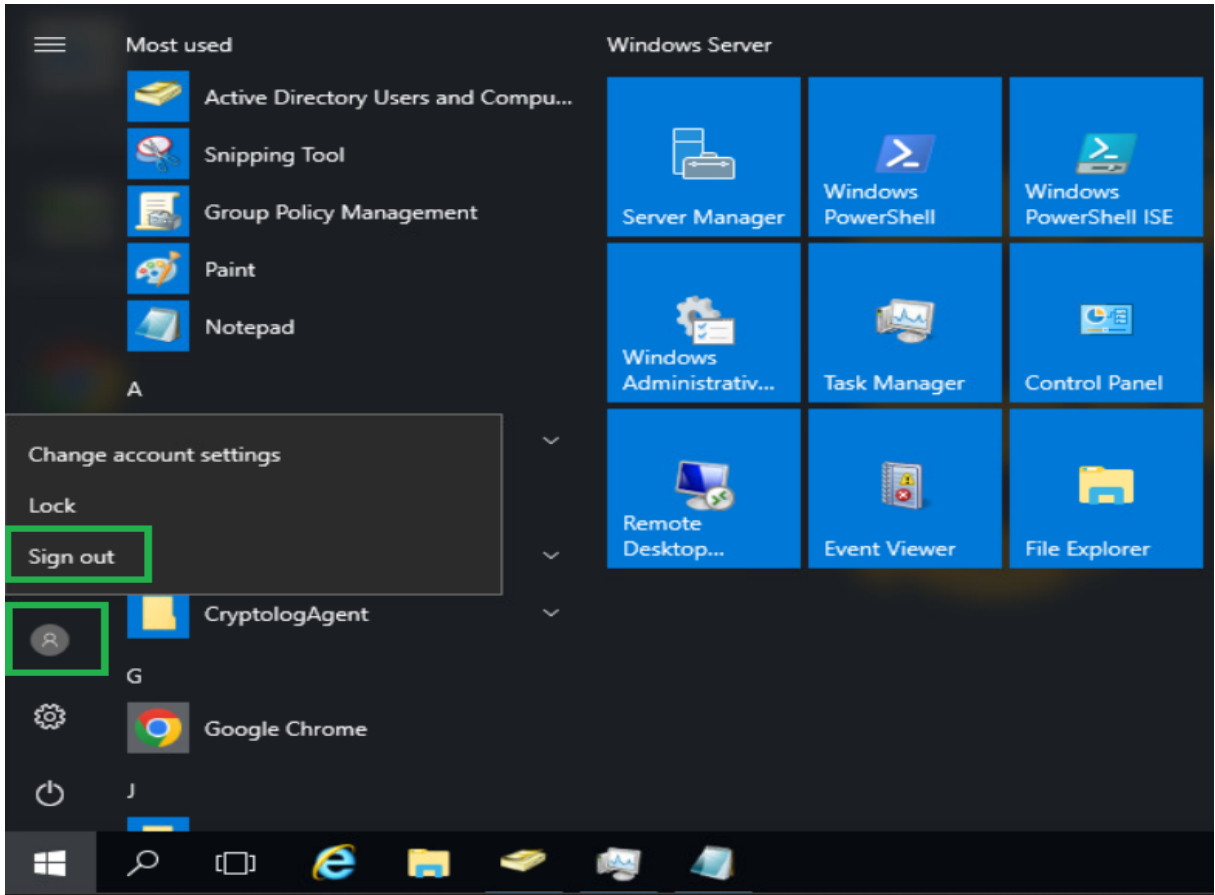


RDS Session Time Limits Ayarları

Çoğu firmada eksik gördüğüm bir konuya değinmek istiyorum bugün. Büyük bir çoğunluğumuz bir sunucuya "RDP" ile bağlandığımızda üst köşedeki çarpı butonuna basıp öyle çıkış yapıyoruz.



Peki ne yapmamız gerekiyor, Çarpı butonuna basmak yerine sing out olmamız gerekiyor.



Bunu yapmadığımız taktirde başımıza neler gelebilir biraz bahsedeyim. Sunucumuzdan görev yöneticisini açıp daha sonrasında “Users” kısmına geldiğimizde bazı kullanıcıların açık olduğunu görüyoruz. Aslında bu kullanıcılar “Sing out” olmak yerine üst tarafta bulunan çarpı butonuna bastıkları için oturumları kapanmıyor ve bu durum sunucunun performansını ve güvenliğini etkilemiş oluyor. Güvenlik kısmına değinmek istiyorum, elbette dışardan destek aldığımız firma olabilir veya şirketimizde çalışan bir personel olabilir hiç fark etmez. Saldırgan eğer isterse daha yetkili bir kullanıcının powershell’ini çalıştırabilir hatta yeni kullanıcı oluşturup veya kendisini domain admin yapabilir. Bunu yapabilmesi için bazı tool’lar var ve bu saldırıyı gerçekleştirebilmek için saldırganın local admin olması yeterlidir. Saldırı nasıl yapıldığına şuanlık değinmeyeceğim isteyen olursa benimle iletişim geçebilir.

Task Manager

File Options View

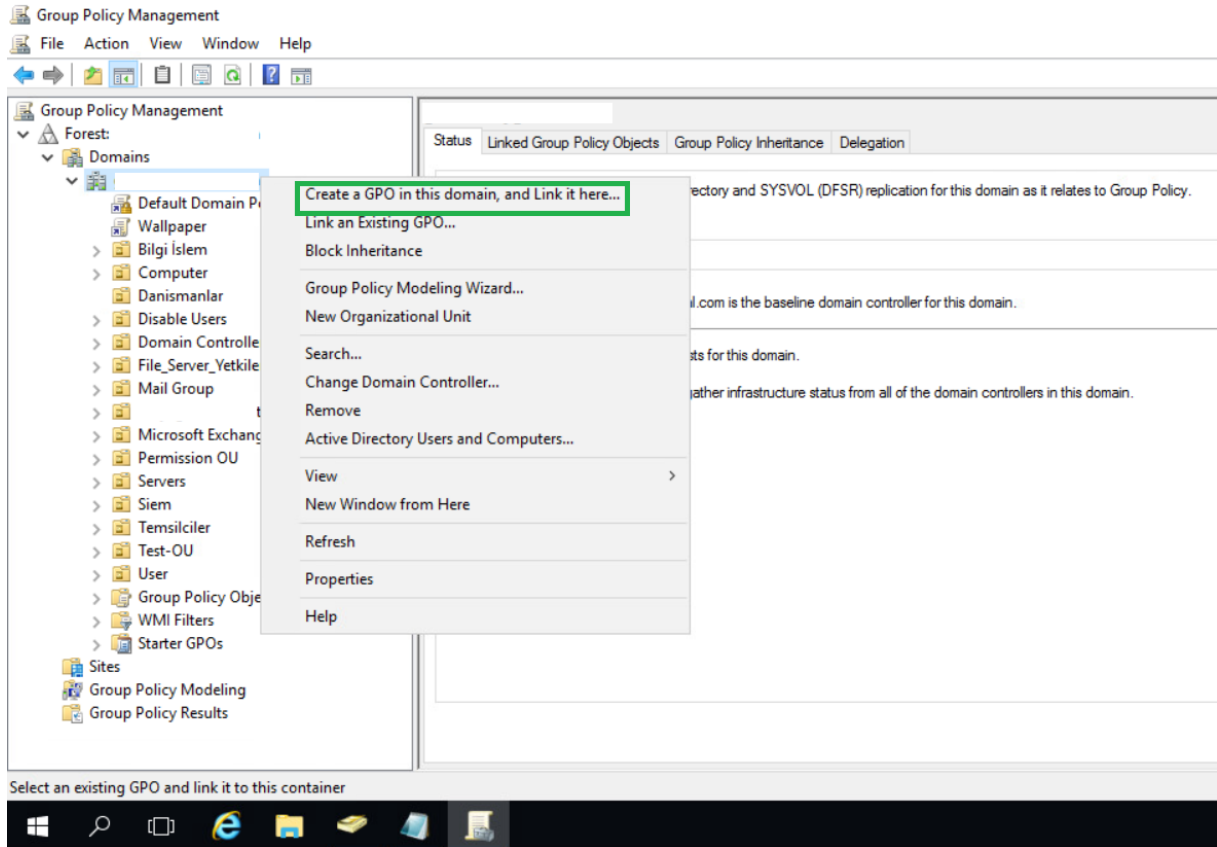
Processes Performance **Users** Details Services

User	Status	17% CPU	69% Memory
> do	Disconnected	0%	203.6 MB
> fatih.bulbul (22)		0.2%	236.3 MB
> m	Disconnected	0%	279.9 MB
> nu	Disconnected	0%	199.0 MB
> oz	Disconnected	0%	368.5 MB

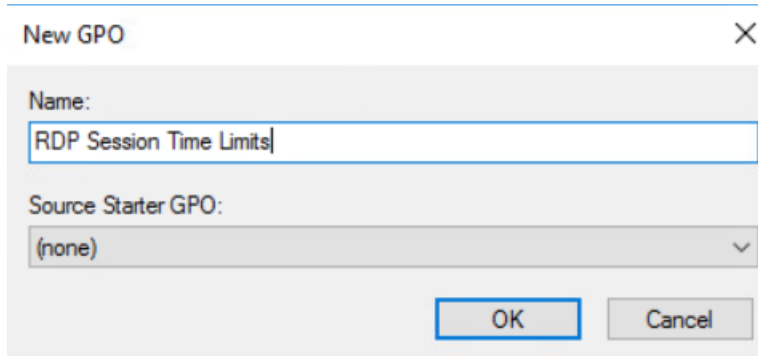
Fewer details

Disconnect

Gelelim güvenliğin sağlanmasına, öncelikle group policy açalım ve bir adet policy oluşturalım.

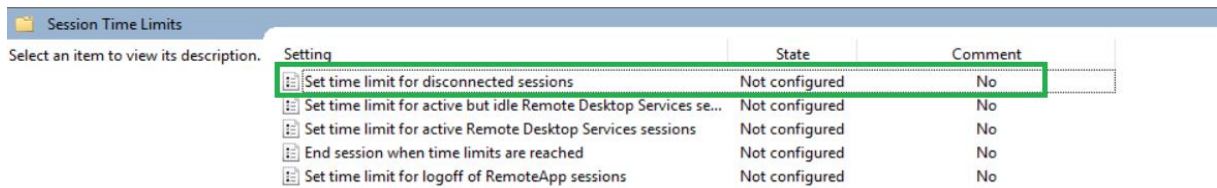


Oluşturmuş olduğum policy'nin ismini "RDP Session Time Limits" veriyorum siz istediğinizi verebilirsiniz.



Oluşturduğumuz policy'de sağ tıklayıp edit diyelim ve belirtmiş olduğum dizine gelelim.

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits



En üst seçenekte belirttiğim gibi “Set time limit for disconnected sessions” seçelim. Seçtiğimiz seçenek şuna yarıyor. Kullanıcı “RDP” bağlantısını üst köşeden çarpıya bastıktan sonra kaç dk sonra kullanıcının hesabı sing out olmasını istediğimiz belirlediğimiz kısım.

Set time limit for disconnected sessions

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: End a disconnected session 1 minute

Help: This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. You can use this policy setting to specify the maximum amount of time that a disconnected session remains active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session. When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server. If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select Never. If you have a console session, disconnected session time limits do not apply.

OK Cancel Apply

Resimde görüldüğü gibi kuralı “Enabled” edip süre olarak 1 dk seçtim. Yani kullanıcı oturumdan çıktıktan 1 dk sonra oturumu otomatikman sing out olacak. Bir başka seçeneğide göz atalım 2. sırada bulunan “Set time limit for active ut idle Remote Desktop Services sessions” seçiyorum.

Session Time Limits			
Select an item to view its description.			
Setting	State	Comment	
Set time limit for disconnected sessions	Not configured	No	
Set time limit for active but idle Remote Desktop Services se...	Not configured	No	
Set time limit for active Remote Desktop Services sessions	Not configured	No	
End session when time limits are reached	Not configured	No	
Set time limit for logoff of RemoteApp sessions	Not configured	No	

Bu seçenek ise şuna yarıyor. Kullanıcı üst köşeden oturumu kapatmayıp ama herhangi bir işlem’de yapmadığı zaman kaç dk sonra sing out olunmasını belirlediğimiz ekran. Kısaca özetlemek gerekirse sunucuda bir işlem oldu ve giriş yaptım, işlem bittikten sonra oturumu kapatmayıp alt sekmeye aldığımı farz edelim. Bu durumlar için kullanılır.

Set time limit for active but idle Remote Desktop Services sessions

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: Idle session limit: 30 minutes

Help: This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected.

If you enable this policy setting, you must select the desired time limit in the Idle session limit list. Remote Desktop Services will automatically disconnect active but idle sessions after the specified amount of time. The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. If you have a console session, idle session time limits do not apply.

If you disable or do not configure this policy setting, the time limit is not specified at the Group Policy level. By default, Remote Desktop Services allows sessions to remain active but idle for an unlimited amount of time.

If you want Remote Desktop Services to end instead of disconnect a session when the time limit is reached, you can

OK Cancel Apply

Yukarıda görüldüğü üzere “Enabled” seçip süreyi’de 30 dk olarak belirledim. Buradaki süreyi çok kısa tutmanızı tavsiye etmem çünkü. Belki o sırada kullanıcı bir uygulama indiriyordur veya bir kurulum yaparken beklemesi gerekti diyelim bu gibi kazalar yaşanmaması için 30 dk belittim.

Fatih Bülbül