

1. Yukarıdaki topolojiyi sanal ortamda oluşturunuz.
2. İstanbul.com ve Ankara.com iki ayrı forest yapısında olacak şekilde gerekli kurulumları yapınız.
3. Tüm makineler kendi yapılarındaki Active Directory Domain’lerinin üyesi olsunlar.
4. Her iki yapıda da DNS, DHCP, WINS ve RRAS servislerini hazır hale getiriniz.
5. RAS’lar arasında Site2Site VPN Yapınız. (L2TP - IPsec)
6. ISTCL’ları istanbul.com içerisine dahil ediniz.
7. İstanbul.com yapısına bir adet Server 2008R2 daha ekleyerek bu sunucuyu DC olarak yapılandırıp sigorta.istanbul.com isimli child domaini kurunuz.
8. Ankara.com yapısına bir adet server 2008R2 daha ekleyerek bu sunucuyu DC olarak yapılandırıp yatirim.net isimli bir tree domain oluşturunuz.
9. İstanbul.com ve ankara.com root domain’leri arasında karşılıklı isim çözümlemesini sağlayarak Forest Trust yapılandırınız.
10. İstanbul.com DC’sinde OU dizaynı yapınız. (Personel: Satis-Pazarlama-Muhasebe) ayrıca her OU’nun içerisine 3 adet user oluşturunuz. Departmanlara ilişkin grupları oluşturunuz.
11. FS’lar üzerinde dosya paylaşımları oluşturunuz.
12. Personel klasörünü oluşturup paylaşıma açınız. Altına satis, pazarlama ve muhasebe klasörlerini oluşturunuz.
13. Personel’e tüm personel girebilsin okuyabilsin, dosya ekleyip kendi eklediği dosyaları silebilsin. Başkalarının eklediklerini silemesin.
14. Muhasebe’ye sadece muhasebeciler, satis’a sadece satiscılar, pazarlama’ya sadece pazarlamacılar girebilsin. Dosya ekleyebilsin ve sadece kendi ekledikleri dosyaları silebilsinler.
15. İstanbul’daki Pazarlama Personeli, ANKFS içerisinde açılan Evrak isimli paylaşım için en güvenli ve efektif şekilde yetkilendirilsin. AGUDLP hak atama stratejisini hayata geçiriniz.
16. Her iki Forest’taki WINS’lere kayıtların gelmesini sağlayınız.
17. WINS’leri Push&Pull partner şeklinde ayarlayınız.
18. İstanbul.com yapısındaki domain controller’ın system state backup’ını alınız.
19. FS’ler üzerindeki dosya paylaşımlarının Pazartesi Full, Salı-Çarş,Perş incremential, Cuma Differential, Cmrts ve Pazar Inremential olacak şekilde her gün 02:00’ye backup schedule ediniz.
20. Istanbul.com root DC’deki Personel OU’sunu siliniz.
21. Bu OU’yu geri getirebilmek için Authorative Restore yapınız.
22. RAS’ın üzerindeki Demand Dial Interface’lerdeki TCP paketlerinin sayısını izleyiniz.
23. DC üzerine 1 saat içinde gelen Kerberos Authentication isteklerinin sayısını tespit ediniz.
24. RAS’ın İşlemci, RAM ve HDD, NIC kullanımını inceleyen bir monitoring ekranı oluşturunuz. Bu monitoring işlemlerini 2sn’de bir örnekleme yapacak şekilde sonradan incelenebilecek halde raporlanmasını sağlayınız.
25. İstanbul.com’daki FS içerinde Profil isimli bir klasör oluşturunuz. Bu klasörü gizli paylaşıma açınız. Tüm kullanıcıların profillerini client’ların localinde değil FS üzerindeki bu paylaşımda kendi kullanıcı isimlerine ait klasörlerde tutmalarını sağlayınız.
26. Ankara.com ve istanbul.com’daki DNS sunucularda Aging ve Scavenging işlemlerini aktif hale getiriniz.
27. İstanbul.com yapısını kapatınız. Ankara.com yapısına iki adet daha DC ekleyiniz.
28. Active Directory master rollerini ankara.com’daki 3 DC üzerine dağıtınız. 1. ve 2. DC’ler GC tutsunlar ve DNS Server olsunlar. 3. DC sadece DNS Server olsun.
29. Schema Master ve Domain Naming master DC1’de, PDC Emulator ve RID Master DC2’de, Infrastructure Master ise DC3’te olsun.
30. DC2’yi siliniz.
31. DC2 ve DC3 üzerindeki master Rollerini DC1’e aktarınız.
32. Temel yapıdaki 6 makine açık olsun.
33. Istanbul yapısındaki DHCP içerisinde Scope Option’larını düzenleyiniz.
34. DHCP içerisinde 3 adet scope oluşturunuz. (192.168.10.0 / 20.0 / 30.0) Bu üç scope için de Time Server 192.168.1.1 olsun. Her scope’un default gateway’ı kendi bloğunun kullanılabilir son IP adresi olsun. Her scope için IP adresleri 4 günlüğüne kiralansın ancak 2. Scope için 2 saatliğine kiralansın. 2. Scope’taki bu değişiklik scope ayarlarından değil DHCP scope option’larından yapılsın.
35. Custom Scope Option’ları oluşturunuz.
36. FS üzerine DHCP kurarak sistemdeki iki DHCP arasında 80/20 kuralını uygulayınız.
37. RAS’ların arasına 2 adet 2 interface’li Telecom’u simule edecek RAS ekleyiniz.
38. LAN Segment’lerini bu RAS’lara göre düzenleyiniz.
39. Static Route ile Ankara ve Istanbul’u görüştürünüz.
40. Static Route’ları silip RIPv2 ile Ankara ve Istanbul’u görüştürünüz.
41. RIPv2’yi silip OSPF ile Ankara ve Istanbul’u görüştürünüz.
42. Ankara yapısını kapatınız. CL4 isimli WAN’da olacak bir client ekleyiniz.
43. İç Yapıdaki FS’a doğrudan RDP ile erişebilsin.
44. ISTRAS üzerinde NAT yapılandırınız RDP bağlantısını kuramadığınızı gözlemleyiniz. NAT üzerinde port yönlendirerek (PAT) tekrar FS’a RDP ile erişilmesini sağlayınız.
45. Ankara.com yapısının iç subnet’ini ikiye bölünüz.
46. ANKRAS’a bir ethernet kartı daha ekleyerek bu iki subnet’in görüşmesini sağlayınız.
47. İkinci subnet’e 2 adet client ekleyiniz.
48. Bu client’ların otomatik TCP/IP yapılandırması alması için RelayAgent yapılandırınız.
49. İkinci subnet’ten sunucuların olduğu birinci subnet’e RDP ile erişilmesini engelleyiniz.
50. Bu işlemlerin ardından istanbul.com iç yapısında group policy konfigurasyonu yapılacaktır. Açık olacak makineler istanbul.com yapısındaki ISTDC, ISTFS, ISTCL1 ve ISTCL2 makineleri olacaktır.
51. Group Policy Aracılığı ile sistemdeki makinelerin açılmadan önce mutlaka group policy’leri almasını sağlayan bir ayarlama yapınız.
52. Sistemdeki kullanıcıların şifrelerini minimum 8 karakter ve komplekslik olacak şekilde ayarlaryınız.
53. Kullanıcılar şifrelerini en fazla 60 gün kullanabilsinler.
54. Kullanıcılar son kullandıkları 3 şifreyi tekrar kullanamasınlar.
55. Kullanıcılar 4 kere yanlış şifre girdiklerinde hesapları kitlensin. Kullanıcıların hesaplarını admin tekrar açmak zorunda kalmasın hesaplar 10 dakika sonra otomatik tekrar aktif hale gelsin.
56. Sistemdeki client’lar üzerinde logon işlemlerinin olay görüntüleyiciye (eventvwr) hem başarılı hem de başarısız olarak loglanmasını sağlayınız.
57. Kullanıcıların hangi Policy sebebiyle Domain Controller’lara oturum açamadıklarını tespit ediniz. Aynı policy’i kullanıcıların file server’a interaktif oturum açamamaları için uygulayınız.
58. ISTCL1’in localinde Local\_Backup isimli bir kullanıcı yaratınız. Bu kullanıcı hesabının local’deki dosyaları ntbackup ile yedekleyebilmesi için gerekli GPO yetkileriniz veriniz.
59. Client bilgisayarların local’indeki Guest kullanıcısının durumunu disable ediniz.
60. Domain yapısında LocalAdmin isimli bir kullanıcı oluşturarak bu kullanıcı hesabını tüm client bilgisayarların local admin grubuna merkezi bir şekilde üye ediniz.
61. Bu işlemin ardından Client bilgisayarların localindeki administrator account’unum ismini “olduser” yapınız ve bu hesabı da disable hale getiriniz.
62. Client bilgisayarlara local olarak oturum açan kullanıcılar varsa bunların CD-ROM ve Floppy’leri kullanmasını yasaklayınız.
63. Client bilgisayarlara oturum açarken CTRL+ALT+DEL tuşlarına basmak gerekmesin.
64. Client bilgisayarlar açıldığında kullanıcılar log-on olmadan önce “Bu bilgisayarların şirkete ait olduğunu... ” belirten yasal bir uyarı ile karşılaşsınlar.
65. Local bilgisayarlardaki log-on cache’inin sayısı 2 olsun.
66. LDAP Signing ve SMB Signing işlemlerinin ne amaçlı kullanıldıklarını ve çalışma mekanizmalarını açıklayınız.
67. Sistemdeki tüm sunucu ve local makineler için tüm event loglarının boyutlarını 100mb olarak ayarlayınız. Bu event loglarının 100mb sınırına ulaşıldığında otomatik bir şekilde birbirinin üzerine yazılmasını engelleyiniz. Makinelerdeki event log’ların ancak admin tarafından temizlenebilmesini sağlayınız.
68. Sistemdeki Client makinelerde Messenger servisinin her zaman kapalı olmasını ve netlogon servisinin de her zaman açık olmasını GPO ile kesinleştiriniz.
69. Local Admin’lerin bilgisayarda Remote Desktop uygulamasının portunu değiştirmesini engelleyiniz.
70. Active Directory’de Log\_User isimli bir kullanıcı oluşturunuz. Sistemdeki tüm sunucuların c:\ sürücüsünün altındaki perflogs klasöründe bu kullanıcının read yetkisinin olmasını sağlayınız.
71. Sistemdeki sertifikaların son kullanıcılar ve kullanıcı bilgisayarları tarafından otomatik alınmasını sağlayan group policy’leri kontrol ediniz.
72. Client bilgisayarlarda solitaire ve mspaint uygulamalarının çalışmasını yasaklayınız.
73. Client bilgisayarlar üzerine admin aracılığı ile Windows Live Messenger uygulamasını yükleyiniz.
74. Live Messenger uygulamasının client bilgisayarlarda kullanımını yasaklayınız.
75. IPsec teknolojisi ve kullanım modları hakkında bilgi veriniz.
76. Sistemdeki client makinelerin USB flash bellekleri ve USB harddisk’leri kullanmalarını engelleyiniz. Ancak yaptığınız bu kısıtlama USB klavye ve mouse’ları etkilemesin.
77. Client Bilgisayarların Internet Explorer’larında options altında Security, Connections ve Advanced tablarını görmelerini engelleyiniz.
78. Kullanıcıların bilgisayarlarında Internet Explorer browserlarında video izlemelerini engelleyiniz. Böylelikle bir kısım video paylaşım sitelerini yasaklayınız.
79. Sistemdeki kullanıcılar 16 bit yapısında hazırlanmış bazı eski uygulamaları kullandıklarını tespit ettiniz. Bu uygulamaların çalışmasını engelleyiniz.
80. Client Makinelere IIS kurulmasını engelleyiniz.
81. Domain’e dahil tüm bilgisayarlar için Microsoft Security Center aktif olsun.
82. Client bilgisayarlarda oluşturulan Schedule Task’ların silinmesini engelleyiniz.
83. ISTFS’i Terminal Server olark değerlendiriniz. Terminal Server’a iki client’tan da remote desktop ile ulaşıldığını teyid ediniz. Terminal Server’lara sadece pazarlama grubu üyelerinin ulaşabilmesini ayarlayınız. Pazarlama user’larıyla her iki client’a da oturum açınız.
84. Kullanıcılar Remote Desktop yaptıklarında performans gereği ile bağlandıkları terminal server’ın wallpaper’ını göremesinler. Bağlantıda kullanılacak renk derinliği de 16bit olsun.
85. Terminal Server’a eş zamanlı en fazla 20 kişi RDP ile oturum açabilsin.
86. Pazarlama Kullanıcıları Terminal Server’a oturum açtıklarında ekranlarına wordpad(excel ya da muhasebe programı da olabilir.) otomatik olarak açılsın.
87. File Server’ın içine Pazarlama kullanıcılarının ortak kullanacakları bir paylaşım oluşturunuz. Paylaşıma ilişkin gerekli yetkilendirmeleri yapınız. Bu paylaşıma remote desktop ile ulaşan pazarlama kullanıcıların bu paylaşımı home directory olarak kullanmalarını sağlayınız.
88. Terminal Servis kullanıcıların bilgi güvenliği amacıyla clipboard redirection yapmasını dolayısıyla terminal server’dan kendi makinelerine kopyalama yapmasını engelleyiniz.
89. Terminal Server’da session’a ait temp dosyası kullanılmasın.
90. Terminal Server yapısının bir Network Load Balancer (NLB) cluster ortamında olduğunu düşünürseniz, kullanıcıların bağlantı koptuğunda ,her zaman bağlantılarının devam ettiği terminal server’a bağlanmaları için session directory ayarını yapınız.
91. Kullanıcılar Termninal Server’a en fazla 8 saat bağlı kalabilsinler.
92. Kullanıcıların Disconnect oldukları session’lar 30 dk. İçerisinde otomatik olarak kapatılsın.
93. Kullanıcıların bağlanıp iş yapmadıkları remote desktop session’ları bir saat içerisinde otomatik olarak kapatılmasını sağlayınız.
94. Client Bilgisayarlardan update’lerin kaldırılmasını engelleyiniz.
95. Windows Messenger uygulamasının çalışmasını engelleyiniz.
96. Windows Movie Maker Uygulamasının çalışmasını engelleyiniz. Ancak bu grup policy’nin Pazarlama Kullanıcılarından birine uygulanmasını engelleyiniz.
97. Sistemde FS üzerine WSUS 3.0 kurulumu yapınız.
98. Sistemdeki bilgisayarları tüm update’lerini WSUS üzerinden almaları için GPO ile yapılandırınız.
99. Kullanıcı bilgisayarlarında otomatik update’leri GPO ile aktif duruma getiriniz.
100. Client’larda media player’ın masaüstünde kısayol oluşturmasını ve update almasını engelleyiniz.
101. Sunucularda oturum açıldığında “Manage your server” ekranı görülmesin.
102. CD-ROM’a takılan uygulamaların kendini otomatik olarak başlatmasını tüm client makinelerde engelleyiniz.
103. Roaming Profile’a sahip olan kullanıcılar Client’lara oturum açtıklarında ekledikleri veriler, oturum kapatılırken local makinelerden güvenlik gereği silinsin.
104. Bilgisayarlar için uygulanan startup script’lerinin senkron çalışmasını sağlayınız.
105. Bilgisayarlara acrobat reader uygulamasını merkezi bir şekilde GPO aracılığıyla assing metodunda yükleyiniz.
106. Kullanıcılara winrar uygulamasını GPO aracılığyla publish ediniz. İsteyen kullanıcılar yükleyebilsinler.
107. FS içerisinde muhasebe isimli bir paylaşım açınız. Mushasebe kullanıcıları için gerekli yetkilendirmeleri yapınız.
108. Muhasebe kullanıcılarına bir log-on script’i uygulayarak bu paylaşımın kullanıcılar oturum açtıklarında map’lenmesini sağlayınız.
109. Kendiniz bir script yazarak sadece satış kullanıcılarına oturum açma sırasında uygulayınız. Bu script ISTANBUL A.S. sistemine hosgeldiniz şeklinde bir yazı ile kullanıcıları karşılasın.
110. Client bilgisayarlarda disk kotası uygulayarak disklerin 1500mb’lik bölümününün kullanılmasını sağlayınız.
111. Domain Controller üzerine group policy yönetimini kolaylaştırmak için GPMC (Group Policy Management Console) yükleyiniz.
112. Group Policy’ler için slowlink detection’un algılanmasını sağlayınız. Bu Policy’nin de aşağıdaki hiç bir OU’dan ezilememesini sağlayınız.
113. Sistemdeki tüm makinelerde RSoP datası üretmesini bu bilgileri görmesini engelleyiniz. Ancak IT OU’su altındaki bilgisayarlarda bu veri incelenebilsin.
114. Loopback processing mode’un ne amaçla kullanıldığını ve mode’larını belirtiniz.
115. Loopback Processing Mode’u “Merge Mode” olarak ayarlayınız.
116. Virüslerden korunmak amacıyla sistem içerisindeki client’larda System Restore’u kapatınız.
117. Kullanıcıların karşılaştıkları Windows hatalarını Microsoft’a göndermeleri yerine, administrator’un incelemesi için FS içerisinde Hatalar isimli bir klasöre göndermelerini sağlayınız.
118. Hatalı yüklemeleri engellemek için kullanıcı bilgisayarlarında print driver’larının download edilmesini engelleyiniz.
119. DNS yapısında reverse zone oluşturunuz. Bu reverse zone yapısına GPO desteği ile PTR record’larının oluşturulmasını sağlayınız.
120. Client bilgisayarlardaki Offline Cache boyutunun default diskin %15’i kadar olmasını sağlayınız.
121. Offline file yapısındaki hatırlatıcı balonların 20 saniye aralıklarla görülmesini sağlayınız.
122. QoS teknolojisini ve işlevini açıklayınız.
123. BITS (backgroud intelligent transfer service) sisteminin işlevini açıklayınız ve sistem için aktif olmayan işlerin time out süresini 3 gün olarak yapılandırınız.
124. Bilgisayara local olarak tanıtılmış printer’ların kullanıcılar tarafından paylaştırılmasını engelleyiniz.
125. Sadece Muhasebe kullanıcıların hesap makinesi kullanmalarını yasaklayınız.
126. FS içerinde bir belgeler isimli bir paylaşım oluşturarak satıs personelinin bu paylaşım altında sadece belgelerim’lerinin içine kaydettiklerini merkezi bir şekilde açılan bu paylaşım altında kendi isimleri ile tutulmasını sağlayınız.
127. Tüm ISTANBUL A.S. çalısanlarının Internet Explorer’larının başlığında “ISTANBUL IT DEPARTMENT” yazısının çıkmasını sağlayınız.
128. Sirket çalışanlarının bilgisayarlarında 192.168.1.254:8080 şekline proxy konfigürasyonu yapılmasını sağlayınız.
129. Tüm kullanıcıların IE ana sayfalarında sirketin web sitesi olsun.
130. Tüm kullanıcıların netmeeting ile chat yapmasını ve dosya alış verişinde bulunmasını engelleyiniz.
131. Satış kullanıcılarında internet explorer options’da connections tabının görülmesini engelleyiniz.
132. Pazarlama personelinin ağ paylaşımlarının üstüne tıkladığında “Map network drive” seçeneğini görmelerini engelleyiniz.
133. Muhasebe ve Pazarlama personelleri bilgisayarım’larının içerisinde A/B/C/D sürücülerini göremesinler ve bu sürücülerin içeriğine hiç bir şekilde erişemesinler.
134. Muhasebe çalışanlarının bilgisayarlarında CD yazıcı varsa, CD yazma özelliğini kullanamasınlar.
135. Tüm personel Bilgisayarlarında çöp kutusunun maksimum boyutu harddiskin %12’si olsun.
136. Muhasebe Personelinin Windows Arayüzünden, başlat çubuğundan Belgelerimini, RUN seçeneğini ve arama seçeneğini kaldırın.
137. Satış personelinin başlat menüsünden Ağ Bağlantıları seçeneğini kaldırın.
138. Muhasebe Personelinin bilgisayarını kapatmak için shutdown system ikonuna hiç bir şekilde erişememesini sağlayınız.
139. Yine Muhasebe Personelinin Start Menu ve Taskbar’ı değiştirememesini sağlayınız.
140. Tüm Personel için Başlat çubuğunda sık kullanılan programların görülmesini engelleyiniz.
141. Satış personeli için Başlat şubuğundan saati kaldırınız ve notification area’nın görülmesini engelleyiniz.
142. Pazarlama Personeli masaüstünde Bilgisayarım, Ağ Bağlantılarım ve Çöp Kutusu ikonlarını kesinlikle göremesin.
143. Satış Personelinin Belgelerim klasörünün yerini (path’ini) değiştirmesini engelleyiniz.
144. ISTANBUL A.S. için bir wallpaper hazırayınız ve tüm şirket personeli bu wallpaper’i kullansın.
145. Muhasebe personelinin control panel’e erişmesini engelleyiniz.
146. Pazarlama personeli control panel’de program ekle/kaldır’ı göremesin.
147. Tüm kullanıcılar için güvenlik sebebiyle, 2 dakikalık bir süre içerisinde ekran koruyucu devreye girsin.
148. Muhasebe kullanıcıları içinde ekran koruyucu 1 dakika sonra devreye girsin ve şifre korumalı olsun.
149. Muhasebe kullanıcılarının bilgisayarlarına tanıtılmış printer’ları silmelerini engelleyiniz.
150. Satış kullanıcıların güvenlik sebebiyle sistem yöneticisinin kendisine vereceği haricinde VPN bağlantısı oluşturmasını engelleyiniz.
151. Pazarlama kullanıcılarının CMD arayüzüne ulaşmalarını engelleyiniz.
152. Muhasebe kullanıcılarının bilgisayarlardaki local profillerinde veri tutmalarını engellemek için profil büyüklüklerini 25mb olarak ayarlayınız.
153. Satış Personelleri için oturum açıkken CTRL+ALT+DEL tuşlarına basıldığında LockComputer, Task Manager ve Logoff seçeneklerine erişmelerini engelleyiniz.
154. Sistemdeki deployment policy’lerinin bilgisayarların disklerinde 4gb’dan fazla yer varsa işlemesini sağlayınız.
155. Sistemdeki uygulama kurulumu policy’lerinden birinin bilgisayarların işletim sistemi eğer Windows XP ise uygulanmasını sağlayınız.
156. Sistemdeki tüm group policy’lerin yedeklerini en iyi yöntemle alınız.