

SQL Change Guard Kullanım Kılavuzu

Sürüm: 1.0

Kapsam: Kurulum, yapılandırma, günlük kullanım, denetim

Hedef okuyucu: Ürünü ilk kez kullanan herkes

Bölüm 0. Giriş ve Terimler	19
0.1 SQL Change Guard nedir	19
0.2 Üç odak alanı	20
0.3 Kimler kullanır	20
0.4 Terimler sözlüğü	20
Bölüm 1. Mimari ve Bileşenler	22
1.1 Genel görünüm	22
1.2 Bileşenler ve görevleri	23
1.3 Desteklenen veritabanı türleri	23
1.4 Worker işleri	24
1.5 Ölçekleme ve dağıtım	25
1.6 Ölçülmüş kapasite ve boyutlandırma	26
Bu tablo nasıl okunmalı ve önerilen sunucu	26
Depolama planlaması	27
Eş zamanlı kullanım ve ekip büyüklüğü	27
Sunucu sayısı	28
Sınırların özeti	28
Bölüm 2. Kurulum	30
2.1 Ön koşullar	30
2.2 Kurulum adımları	30
2.3 Veritabanının oluşturulması	31
2.4 appsettings.json alan alan	32
2.4.1 ConnectionStrings	34
2.4.2 Database:EvidenceLedger ve Evidence:Ledger	34
2.4.3 Auth	34
2.4.4 Jwt	37
2.4.5 Security (şifreleme anahtarları)	38
2.4.6 License	38
2.4.7 Mail	39

2.4.8 Ldap.....	39
2.4.9 Diğer ayarlar	41
2.4.10 SIEM (SOC entegrasyonu)	46
2.4.11 Sso (kurum hesabıyla giriş)	49
2.5 Worker tarafı appsettings.json	52
2.6 İlk yönetici ve ilk giriş	53
2.7 Kurulum doğrulama kontrol listesi.....	53
2.8 Sık karşılaşılan kurulum hataları.....	54
Bölüm 3. Lisans	55
3.1 Lisans dosyası nedir.....	55
3.2 Lisans içeriği	55
3.3 Modüller.....	55
3.4 Sunucu limiti.....	56
3.5 Veritabanı türlerinin lisanstan gelmesi	56
3.6 Lisans durumları ve sistem davranışı	57
3.7 Lisans yükleme adımları	57
3.8 Lisans hata mesajları	57
Bölüm 4. Roller, Yetkiler ve Hiyerarşi	59
4.1 Roller ve sayısal değerleri.....	59
4.2 Kimlik ile hiyerarşi ayrı kavramlardır	60
4.3 Denetçi rolünün özel durumu	60
4.4 Rol yetki matrisi.....	60
4.5 Yetki anahtarları	62
4.6 Arayüz gizlemesi güvenlik değildir	63
4.7 Kullanıcı yaşam döngüsü	63
Yetki değişikliği ne zaman etkili olur	64
4.8 LDAP kullanıcıları ile yerel kullanıcıların farkı.....	65
Kurum hesabıyla (SSO) giriş yapan kullanıcılar	66
Rolün kaynağı: kurum hesabı (SSO) ve izin (LDAP) birlikte	69

Kişi kurum hesabıyla ya da dizinle giremiyorsa	70
4.9 Şifre politikası ve BCrypt	72
Hash nedir	72
Salt nedir	72
Neden BCrypt seçildi	72
4.10 Kullanıcılar ekranı	73
4.11 Roller ekranı	74
4.12 Toplu kullanıcı aktarımı	75
Dosya nasıl hazırlanır	75
Doğrulama ve hata bildirimi.....	75
Aktarılan hesap giriş yapamaz.....	76
Denetim izi	76
Bölüm 5. Güvenlik ve Şifreleme Modeli.....	76
5.1 Üç farklı ihtiyaç, üç farklı yöntem.....	76
5.2 Sunucu şifreleri: AES-256-GCM.....	76
Simetrik şifreleme nedir.....	76
GCM neden seçildi	77
Nerede kullanılır.....	77
5.3 Neyin nerede korunduğu	77
5.4 Denetim kaydı: append-only defter	77
Defter nedir	77
Özet ve dış tanık	78
Neden gizli anahtar yok.....	78
5.5 Veritabanı seviyesi yazma kaydı	78
Yazma kaydında neden mühür yok	79
Kurulumda yapılması gereken.....	79
5.6 Sır maskeleyme	79
Bölüm 6. Sunucu Tanımları	80
6.1 Bu ekran ne işe yarar	80

6.2 Alan alan açıklama	81
6.3 Bağlantı testi.....	86
6.4 Otomatik çalıştırma: arka planda ne oluyor.....	86
Zincir.....	86
Şartlar	87
Zaman nasıl hesaplanır	87
Kayıt kime yazılır	88
6.5 Maskeleye rejimi.....	88
6.6 Çoklu sunucu kuralı	89
6.7 Sunucu silme ve pasife alma	89
6.8 Hedefteki oturum adı ve oturum yoklaması	90
Bölüm 7. Parametreler	90
7.1 Bu ekran ne işe yarar.....	91
7.2 Ekrandaki alanlar	91
7.3 Genel grubu.....	91
DefaultQueryTimeout	91
MaxQueryTimeout.....	91
ExecutionDelaySeconds	92
RejectOnError.....	92
7.4 Görevler Ayrılığı grubu	92
RequesterCanSelfApproveExecute.....	92
ApproverCanExecute.....	93
RequireDistinctApproverPerStep	93
EmergencyMinimumRole.....	93
7.5 Ayar Onayı grubu.....	94
SettingsApprovalPolicy.....	94
7.6 ITSM Bilet grubu.....	94
ChangeTicketRequired	94
ChangeTicketRegex	94

EmergencyTicketRequired	95
EmergencyTicketRegex	95
Geri alma talebinde bilet	96
RequestTicketRegex	96
ITSM entegrasyonu parametreleri	96
7.7 Sorgu Sonucu grubu	98
QrFileRetentionDays	98
QrRequesterCanDownload	98
QrDownloadMinimumRole	98
QrDeliveryMode.....	98
QrMaxRowCount.....	99
QrOutputFormat	100
QrCsvThresholdRowCount	100
QrExcelAutoFitMaxRows.....	101
7.8 Hassas Veri grubu	101
QrMaskingEnabled.....	101
QrSensitiveDataPolicy	101
QrSensitiveDetectionSampleSize	102
QrSensitiveDetectionThresholdPct	102
QrSensitiveDetectionSampleMode.....	102
QrSensitiveDetectionTimeBudgetSeconds	103
QrColumnPreviewEnabled	103
UnmaskedColumnRequestPolicy	103
UnmaskedColumnApproverRole.....	103
7.9 E-posta Onayı grubu.....	104
QrEmailApprovalPolicy.....	104
QrEmailApproverRole	104
QrEmailAutoApproveUsers	104
7.10 Parametre değişikliği ne zaman devreye girer	104

7.11 SIEM grubu	106
Eşikle susturulamayan olaylar	107
Kapsam daraltması SOC'a duyurulur	108
Bölüm 8. Ayar Değişikliği Onayı (Dört Göz)	108
8.1 Ne işe yarar	108
8.2 Kapsam	108
Kontrol ayarı ne demektir	108
8.3 Akış	109
8.4 Onayın komutu tekrar oynatması ne demektir	110
8.5 Kim onaylar	110
8.6 Kilitlenme kapısı	111
8.7 Ayar Onayları ekranı	111
8.8 Bu ekrandaki mesajlar	111
Bölüm 9. Kritik Nesneler, SQL Standartları ve Hassas Veri	113
9.1 Kritik Nesneler	113
Ne işe yarar	113
Alanlar	113
Eşleşme mantığı	113
Kritik nesne tespit edilince ne değişir	113
9.2 SQL Standartları	114
Ne işe yarar	114
Alanlar	114
İhlalde ne olur	115
Örnek standartlar	115
9.3 Hassas Veri Desenleri	116
Ne işe yarar	116
Alanlar	116
Doğrulayıcılar neden vardır	117
Kısmi maskeleye örneği	117

9.4 Hassas Kolon Kataloğu	117
Ne işe yarar	117
Alanlar	117
9.5 Aday Kolonlar (öğrenme döngüsü)	118
Aday nasıl oluşur	118
Kolonlar	118
Onaylanırsa ne olur	119
Bölüm 10. Onay Politikaları	120
10.1 Politika nedir	120
10.2 Politika alanları	120
10.3 Politika eşleştirme (kapsam)	120
Priority ne işe yarar	121
10.4 Politika seçim akışı	121
Birden çok politika eşleşirse ne olur	122
Hiçbiri eşleşmezse ne olur	122
Tüm adımlar atlanırsa ne olur	122
10.5 Adım alanları ve davranışları	123
Adım nasıl karar verir	123
Örnek politika	124
10.6 Görevler ayrılığı (SoD) kuralları	124
Rol atlama izi	125
10.7 Kilitlenme senaryoları	125
10.8 Acil durum uygunluğu	125
Bölüm 11. Değişiklik Talebi Uçtan Uca	126
11.1 Durum makinesi	126
Geçiş matrisi	126
11.2 Talep oluşturma ekranı	128
Ön koşul: sunucunun onay politikası olmalı	129
11.3 Betik editörü ve ayrıştırma	130

Ayrıştırma ne zaman çalışır	130
Ayrıştırma neyi üretir	130
Ayrıştırma hatası	131
Etkilenen nesneler ve fark karşılaştırması.....	131
11.4 Talep detay ekranı	132
Üst bilgi alanları.....	132
Betikler ve nesneler tablosu.....	133
Onay adımları tablosu	133
Çalıştırma sonucu.....	134
Denetim / olay listesi.....	134
11.5 Düğmeler ve aktiflik koşulları.....	134
11.6 Çalıştırma akışı	135
Zamanlanmış çalıştırma	136
Çalıştırmayı iptal etme	137
Çökme kurtarma	137
Onay zinciri: kaydedilen, onaylanan ve çalışan aynıdır	137
11.7 Kısmi başarı ve geri alma.....	138
11.8 Geri alma (rollback) talepleri	138
Geri alma betiği nasıl üretilir.....	139
Yeniden kurmanın kapsamı	139
Ekranı gördüğünüz iki farklı uyarı.....	140
Eksik geri alma betiğinin sonuçları.....	140
11.9 Çalıştırmayı başlatan kişi (attribution)	141
11.10 Acil durum geçersiz kılma (Emergency Override)	141
11.11 Talep listesi ekranı	141
Bölüm 12. Risk Bandı.....	143
12.1 Amaç ve ilke	143
12.2 Band nedir.....	143
12.3 Band nasıl belirlenir	143

12.4 Skor nasıl hesaplanır (kayıt için)	144
12.5 Somut örnek: band High ve üç High bulgu	144
Aynı örneğin varyasyonları	145
12.6 Skor açıklaması (ScoreExplain)	146
12.7 Asla atlanamaz (NeverSkip) kuralları	146
12.8 Risk bandı nerede görünür.....	147
12.9 Bandın kararlara etkisi.....	147
Bölüm 13. Sorgu Sonucu (Query Result) Akışı	148
13.1 Ne işe yarar	148
13.2 Sorgu tipleri	148
13.3 Sorgu sonucu talebi oluşturma	148
Kolon önizlemesi	149
E-posta onay adımı.....	150
Maskesiz kolon onay adımı	150
13.4 Çalıştırma anında arka planda ne oluyor	150
Maskeleme kararı nasıl verilir	151
Kayıt ne tutar	152
13.5 Sonuç dosyası ve teslim	153
İndirme yetkisi.....	153
13.6 Bu akıştaki özel kurallar	154
13.7 Sonuç dosyasının biçimi ve satır sınırı	155
13.8 Ölçülmüş maliyet ve performans	155
Bölüm 14. Sandbox	157
14.1 Ne işe yarar	157
14.2 Nasıl çalışır	157
14.3 Sonucun akışa etkisi	158
14.4 Bilinen sınırlar	158
14.5 Sandbox istek ve pencere olayları	159
Bölüm 15. Sürüm Paketi	159

15.1 Ne işe yarar	159
15.2 Paket alanları.....	159
15.3 Çalıştırma modları	159
15.4 Paket içeriği ve sıralama.....	160
15.5 Tekil talep akışından farkları.....	160
15.6 Kısıtlar.....	161
15.7 Paket çalıştırmada pencere	162
Bölüm 16. Nesne Geçmişi (DDL History)	162
16.1 Ne işe yarar	162
16.2 Ekran akışı	162
16.3 Denetim değeri	163
Bölüm 17. Denetim Kaydı ve Bütünlük	165
17.1 Denetim kaydında ne tutulur	165
17.2 Ne tutulmaz.....	165
17.3 Olay adlandırma kuralı	165
17.4 Eski ve yeni değer sözleşmesi	168
17.5 Kural seti anlık görüntüsü ("o gün neydi")	169
17.6 Defter Durumu	169
Betik Bütünlüğü Doğrula	170
17.7 Yazma kaydının kapsam özeti	170
17.8 Kanıtın kurum dışına teslimi.....	170
17.9 Zaman damgası (isteğe bağlı).....	171
17.10 Denetim Kaydı ekranı	173
17.11 Kanıt paketi: denetim kayıtlarını ham haliyle teslim etme	173
17.12 SOC entegrasyonu (SIEM)	175
Ne zaman gönderilir	175
Teslim kaldığı yerden devam eder.....	175
Nabız	176
Ne gönderilir, ne gönderilmez.....	176

17.13 SOC'a giden mesaj nasıl okunur	176
Örnek bir mesaj.....	176
Öncelik sayısı ve local0.....	177
Ciddiyet nasıl belirlenir	178
Kapsam daraltıldığında SOC'a düşen mesaj	180
17.14 Yürütme ve sandbox pencere olayları.....	181
17.15 Pencere olaylarının SIEM'e taşınması	184
17.16 Kanıt defteri ve kanıt yazma sınırı	185
17.17 Defter özeti.....	185
17.18 Dönem paketi.....	186
Bölüm 18. Denetim Dosyası (Evidence Dossier)	187
18.1 Ne işe yarar	187
18.2 Kim üretir	187
18.3 Dosya içeriği	187
18.4 Sorgu sonucu verisi neden girmez	188
18.5 Dışa aktarmanın kendisi denetlenir	189
18.6 Dosya nasıl doğrulanır	189
Doğrulama başarısız olursa ne anlama gelir	190
Sisteme hiç girmeden doğrulama	190
Paketin içindeki doğrulama betiği.....	191
18.7 Çok uzun betikler ve PDF	192
18.8 Kararları verenlerin oturumu	192
18.9 Denetçi bu dosyayla neyi ispatlayabilir	193
18.10 Yürütme pencereleri ve istisnalar	195
Bölüm 19. Kontrol Paneli (Dashboard).....	195
19.1 Zaman ayrımı.....	195
19.2 Aralık kartları	196
19.3 Şimdi kartları	196
19.4 Çalıştırma başarı oranı	196

19.5 Grafikler ve listeler	197
19.6 İstisnalar kartı	197
19.7 Rol bazında farklar	198
19.8 Boş veri durumu	198
19.9 Panodaki açıklama işaretleri	199
19.10 Worker göstergesi ve kesinti kaydı	199
Kesinti denetim kaydına yazılır	200
Bölüm 20. Raporlar	200
20.1 Genel kurallar	200
20.2 Ortak parametreler	201
20.3 Change Governance grubu	201
20.4 Object & Structure grubu	204
20.5 Access & Authorization grubu	204
Expected Access Principals raporu	205
20.6 Data & Privacy grubu	206
20.7 Configuration & Compliance grubu	207
20.8 Rapor okuma önerileri	207
20.9 Dışa aktarma	208
Bölüm 21. Bildirimler ve E-posta	209
21.1 Hangi olayda kime bildirim gider	209
21.2 Transaction içinde e-posta gönderilmez	209
21.3 E-posta Kaynakları ekranı	209
21.4 Bildirim Kayıtları ekranı	210
Bölüm 22. ITSM Entegrasyonu ve Bilet Numarası	211
22.1 Ne işe yarar	211
22.2 Alanlar	211
22.3 Zorunluluk ve biçim kontrolü	211
22.4 Bilet listesine kayıt ne zaman eklenir	213
22.5 ITSM entegrasyonu	213

22.6 Kayıt türleri.....	214
22.7 ITSM'deki durum nasıl okunur	214
22.8 Talep kaydedilirken.....	215
22.9 Çalıştırmadan hemen önce	215
22.10 ITSM'e ulaşılamazsa	217
22.11 ITSM'e yazılan notlar	217
22.12 ITSM ekranı	217
22.13 Kurulum.....	218
22.14 Dikkat edilmesi gerekenler.....	218
Bölüm 23. Tarih ve Saat Modeli	219
23.1 Saklama: her zaman UTC.....	219
23.2 Neden UTC saklanır	219
23.3 Gösterim.....	219
23.4 Somut örnek.....	220
23.5 Filtrelerde yerel gün sınırı	220
Bölüm 24. Dil ve Yerelleştirme	221
24.1 Arayüz dili.....	221
24.2 API mesajlarının dili.....	221
24.3 Rapor çıktıları	221
24.4 Genel kabul görmüş terimler	221
Bölüm 25. Bakım ve İşletme.....	222
25.1 Bakım Görevleri ekranı.....	222
25.2 Varsayılan bakım görevleri	222
25.3 Bakım kayıtları	223
25.4 Tanılama ekranı	223
25.5 Worker izleme	223
25.6 Yedekleme önerileri	224
25.7 Çökme kurtarma eşiği	224
Eşik neden var	225

Değeri nasıl seçmelisiniz	225
Kurtarmada yürütme penceresi	226
25.8 SIEM teslimini izleme	226
Sık karşılaşılan durumlar	226
25.9 SOC bağlantısını toplayıcı olmadan doğrulama	227
Bölüm 26. Sorun Giderme	228
26.1 Uyarı ve hata mesajları sözlüğü	228
Yetki mesajları	228
Durum mesajları	229
Görevler ayrılığı mesajları	230
Geri alma mesajları	230
Sürüm paketi ve sandbox mesajları	231
Ayar onayı mesajları	232
Sunucu ve lisans mesajları	232
Talep içeriği mesajları	233
Çalıştırma günlüğü notları	233
26.2 Sık karşılaşılan senaryolar	234
Giriş yapılamıyor	234
Sunucuya bağlanılamıyor	234
Talep çalışmıyor	235
Worker çalışmıyor	235
Rapor boş geliyor	235
E-posta gitmiyor	236
Bölüm 27. Yönetişim Kontrolleri ve Şeffaflık	237
27.1 Eksik yönetim adımı göstergesi	237
27.2 İzole deneme zorunluluğu	237
27.3 Geri alma planının bütünlüğü	238
27.4 Engellenen görevler ayrılığı girişimleri	239
27.5 Acil değişiklik gözden geçirme	239

27.6 Maskesiz kolon onayının risk bandına etkisi	240
27.7 İlk girişte parola değiştirme.....	241
27.8 Yönetişim kurulum kontrolü ekranı.....	241
Satırın sütunları	241
Beklenen sütununda tire ne demek.....	242
Üç durum ve ne yapmanız gerektiği.....	242
Ekranın üstündeki sayaçlar.....	242
Örnek: bilet numarası biçimi satırı	242
Ekrandaki bütün satırlar ve ne anlama geldikleri.....	243
DAM ve SIEM eşleşmesi beyanları	251
27.9 Kural motorunun kapsamı ve sınırı	251
27.10 Kapalı düğmeler ve sebepleri.....	251
27.11 Talep kopyalama.....	252
Bölüm 28. Ekler	253
28.1 Enum sözlüğü	253
Roller (enmRole)	253
Talep durumu (ChangeRequestStatus)	253
Talep tipi (QueryType).....	254
Veritabanı tipi (DatabaseType).....	254
Risk bandı (RiskTier)	255
Sürüm paketi çalıştırma modu (ReleaseExecutionMode).....	255
Onay adımı durumu	255
Sunucu ortamı	255
Maskeleye rejimi.....	256
Maskeleye politikası kaydı	256
Maskeleye gerekçe tipleri	256
Aday kolon durumu.....	256
Ayar değişikliği durumu.....	257
Lisans durumu	257

28.2 Parametre hızlı referansı	257
28.3 Yetki anahtarları hızlı referansı.....	260
28.4 UTC saklama notu	261
28.5 Kurulum kontrol listesi	261
28.6 İlk yapılandırma kontrol listesi	262
28.7 Denetim hazırlığı kontrol listesi.....	262

Bölüm 0. Giriş ve Terimler

0.1 SQL Change Guard nedir

SQL Change Guard, veritabanlarına kendi üzerinden yapılan müdahaleleri kayıt altına alan, onaya bağlayan ve kanıtını üreten bir yönetim (governance) uygulamasıdır.

Kurumların çoğunda değişiklik yönetimi zaten kuruludur: iş bir bilet sistemine kaydedilir, gerekiyorsa değişiklik kurulunda görüşülür, onay orada verilir ve uygulama tarafındaki değişiklikler dağıtım hattından geçer. SQL Change Guard bu düzenin yerine geçmez, ona bağlanır: ITSM kaydının numarası talebe bağlanır, talep kaydedilirken ve çalıştırmadan hemen önce ITSM'de doğrulanır ve yapılan iş ITSM kaydına not olarak yazılır (Bölüm 22).

Bu düzenin tamamı değişikliği anlatan kayıt üzerinde çalışır. Çalışacak olan SQL metninin kendisi zincirin dışında kalır ve üç yerde kopma olur:

1. Betiğin ne yaptığı sistematik olarak çözümlenmez. Betik bilete eklenmiş olsa bile onu okuyan gözdür; hangi nesneye dokunulduğu, filtresiz bir güncelleme bulunup bulunmadığı veya kritik bir tabloya girilip girilmediği okuyan kişinin dikkatine kalır ve neyin kontrol edildiği geriye kalan kayıta görünmez.
2. Onaylanan metin ile çalışan metnin aynı metin olduğunu gösteren bir kayıt genellikle yoktur. Onaydan sonra betikte yapılan tek karakterlik bir düzeltmeyi bilet sistemi görmez.
3. Üretimden veri okuma bu zincirin dışında kalır. Değişiklik tarafı olgun kurumlarda bile bir liste talebi çoğu zaman bilet açılmadan karşılanır; kimin hangi gerekçeyle hangi kolonları aldığı ve sonucun kime teslim edildiği tek bir yerde toplanmaz.

SQL Change Guard bu üç noktaya çalışır. Betik metin olarak değil, veritabanının kendi dilbilgisiyle ayrıştırılır; hangi nesneye ne yapıldığı betiğin kendisinden çıkarılır, kural setine göre risk bandı hesaplanır ve gereken onay adımları oluşur (Bölüm 9, 10, 12). Onaylanan betiği uygulamanın kendisi çalıştırır ve betiğin parmak izi saklanır; böylece onaylanan metin ile çalışan metnin aynı olduğu gösterilebilir (Bölüm 11). Üretimden veri okuma ayrı bir talep türüdür: hassas kolonlar maskelenir, sonuç ekranda gösterilmez ve şifreli paketle teslim edilir (Bölüm 13). Her adım, veritabanı motorunun güncelleme ve silmeyi reddettiği append-only bir denetim kaydına yazılır (Bölüm 17) ve tek bir talebin tüm yaşam döngüsü imzalı bir kanıt dosyası olarak dışa aktarılabilir (Bölüm 18).

Ürünün sınırları baştan bilinmelidir. ITSM ile bağlantı okuma ve not yazmaktan ibarettir: ürün ITSM'de kayıt açmaz ve kaydın durumunu değiştirmez (Bölüm 22). Ürün canlı veritabanı trafiğini izlemez, bu yüzden ürün dışından yapılmış bir değişikliği kendiliğinden bildiremez; gösterebileceği şey sunucudaki tanımın kayıtle uyuşmadığıdır (Bölüm 16.3). Kural motoru yalnız betikten okunabilen şeyi söyler; hedef veritabanının o anki durumunu gerektiren kontroller kapsam dışındadır (Bölüm 27.9). Aynı sebeple nesne bağımlılığı çözümlemesi de yapılmaz: betiğin dokunduğu nesneler listelenir, ancak değiştirilen bir prosedürü hangi nesnelerin çağırdığı gösterilmez.

0.2 Üç odak alanı

Ürün üç başlıkta çalışır. Kılavuz boyunca hangi bölümün hangi başlığa hizmet ettiği belirtilir.

Odak alanı	Anlamı	Kılavuzdaki bölümler
Database Change Governance	Veritabanı yapısını değiştiren işlerin yönetimi. Kim ne değiştirdi, kim onayladı, ne zaman çalıştı.	10, 11, 12, 14, 15, 16
Production Query Governance	Canlı ortamdan veri okuma işlerinin yönetimi. Kim hangi sorguyu çalıştırdı, sonuç kime gitti.	13
Data Governance & Compliance	Kişisel ve hassas verinin korunması, denetim kanıtı üretimi.	9, 13, 17, 18, 20

Ürünün genel konumlandırması Database Operations Governance başlığıdır: veritabanı operasyonlarının yönetişimi.

0.3 Kimler kullanır

Rol	Kılavuzda öncelikli bölümler
Geliştirici	11, 12, 14, 22, 26
Veritabanı yöneticisi	6, 11, 12, 15, 25, 26
Değişiklik yöneticisi	10, 11, 19, 20
Bilgi işlem yöneticisi	2, 3, 7, 8, 25
Denetçi	17, 18, 20, 23
Sistem yöneticisi	2, 3, 4, 5, 6, 7, 8, 9, 25

0.4 Terimler sözlüğü

Kılavuz boyunca kullanılan terimler. Her biri ilgili bölümde ayrıntılı anlatılır.

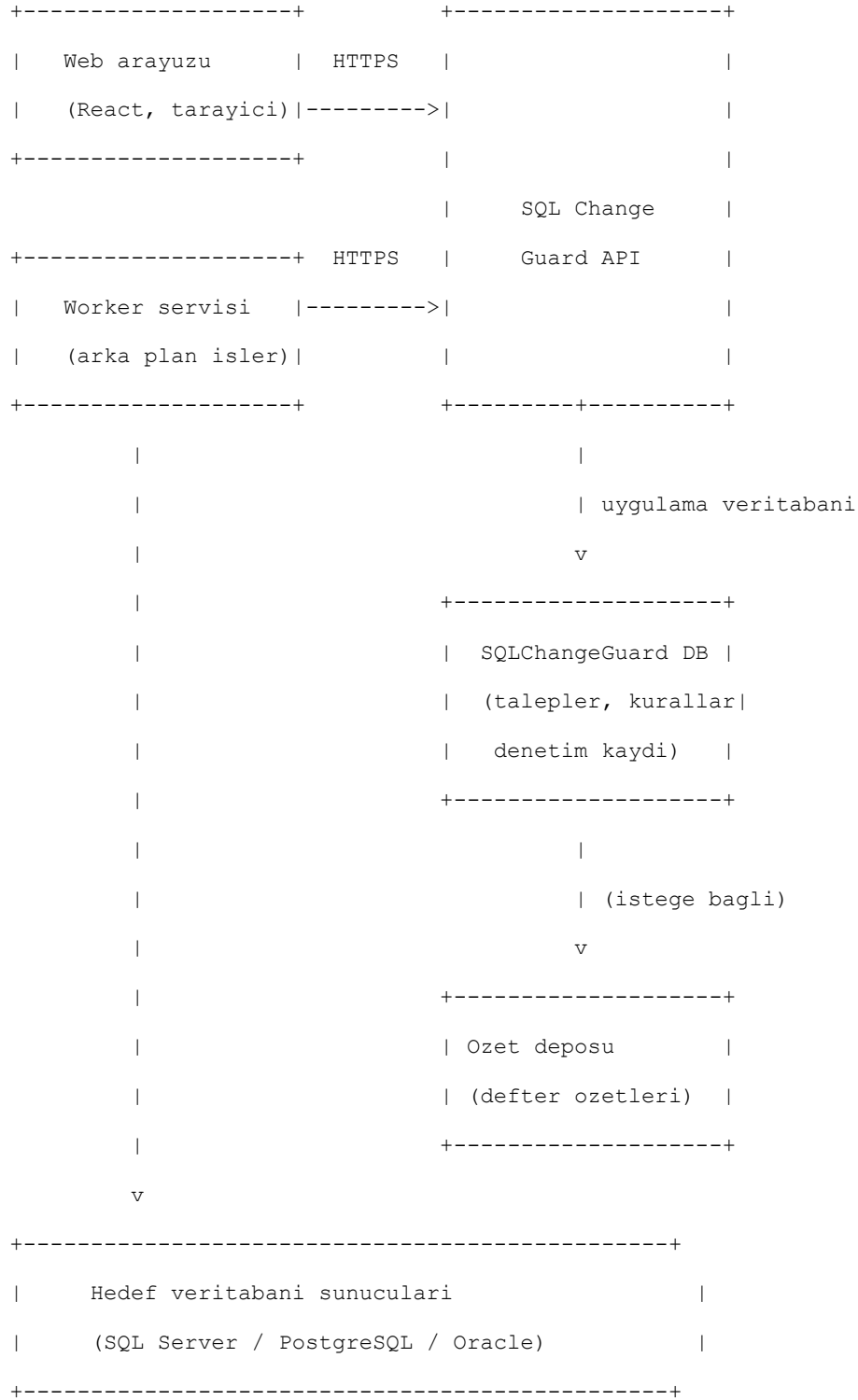
Terim	Açıklama
Talep (Change Request)	Bir veya birden çok SQL betiğinin, bir veya birden çok hedef sunucuda çalıştırılması için açılan kayıt. Kısaltması CR.
Sorgu Sonucu (Query Result)	Canlı ortamdan veri okumak için açılan talep türü. Sonuç şifreli bir dosya olarak teslim edilir. Kısaltması QR.

Terim	Açıklama
Rollback talebi	Bir değişiklik talebini geri almak için ona bağlı olarak açılan talep.
Betik (Script)	Talebin içindeki tek bir SQL metni. Bir talep birden çok betik taşıyabilir.
Ayrıştırma (Parse)	Betiğin metin olarak değil, yapı olarak çözümlenmesi. Hangi nesneye hangi işlemin yapıldığı buradan çıkar.
SQL standardı	Betikte aranan bir kural. Örnek: "xp_cmdshell çağırısı var mı".
Kritik nesne	Kurumun özel olarak işaretlediği veritabanı nesnesi. Bu nesneye dokunan talep farklı davranır.
Risk bandı (Band)	Talebin risk seviyesi. Beş kademe: Info, Low, Medium, High, Critical.
Risk skoru (iç değer, gösterilmez)	İç değerlendirme sırasında hesaplanan sayısal karşılık. Hiçbir ekranda, raporda veya denetim dosyasında gösterilmez. Kullanıcıyı ve denetçiyi ilgilendiren tek ölçü risk bandıdır; kararı da band belirler.
Onay politikası	Hangi durumda kaç kişinin, hangi rolle onay vereceğini tanımlayan kural seti.
Onay adımı	Politikanın ürettiği tek bir onay isteği.
Dört göz (Four eyes)	Bir işlemin en az iki farklı kişi tarafından tamamlanması ilkesi.
Görevler ayrılığı (SoD)	Talebi açan, onaylayan ve çalıştıran kişilerin ayrı olması ilkesi.
Acil durum talebi (Emergency)	Normal onay yolunun kısaltıldığı, gerekçesi zorunlu talep. Ayrı bir talep türü değildir: talep üzerindeki acil durum işaretidir ve talep yalnız acil durum politikasına eşlenir.
Sandbox	Betiğin canlıya girmeden önce bir test sunucusunda denenmesi.
Sürüm paketi (Release Package)	Birden çok talebin sıralı biçimde birlikte çalıştırılması.
Denetim kaydı (Audit log)	Sistemde olan olayların kaydı. Veritabanı motoru bu kayıtların güncellenmesini ve silinmesini reddeder.
Denetim dosyası (Evidence Dossier)	Tek bir talebin tüm yaşam döngüsü kanıtını içeren ZIP paketi.
Maskeme	Sorgu sonucundaki hassas değerlerin okunamaz hale getirilmesi.
Worker	Zamanlanmış işleri arka planda yürüten Windows servisi.

Bölüm 1. Mimari ve Bileşenler

1.1 Genel görünüm

Sistem dört ana parçadan oluşur. Bunlar birbirinden bağımsız kurulabilir.



1.2 Bileşenler ve görevleri

Bileşen	Ne yapar	Çalışmazsa ne olur
API	Tüm iş kuralları burada çalışır. Yetki kontrolü, onay akışı, risk hesabı, denetim yazımı.	Hiçbir ekran çalışmaz.
Web arayüzü	Kullanıcının gördüğü ekranlar. İş kuralı içermez, her isteği API'ye sorar.	Kullanıcı ekranlara erişemez, ancak arka plan işleri devam eder.
Worker servisi	Zamanlanmış çalıştırma, sunucu bağlantı kontrolü, bildirim gönderimi, defter özeti ve kanıt yazma sınırı kontrolü, bakım işleri.	Hiçbir talep çalışmaz. Ekrandaki Çalıştır düğmesi işi worker kuyruğuna verir ve çalıştırmayı worker yapar; bu yüzden elle başlatılan talepler de bekler ve Çalışıyor durumunda kalır. E-posta gitmez, sunucu bağlantı durumu güncellenmez.
Uygulama veritabanı	Talepler, kurallar, kullanıcılar, denetim kaydı.	Sistem tümüyle durur.
Dış özet deposu	API'nin defter özetlerini (imza açıksa imzalı) yazdığı klasör (Evidence:Ledger:DigestOutputPath). Veritabanı yöneticisinin değiştiremeyeceği bir yerde durmalıdır; bu depoyu (WORM paylaşım gibi) kurum sağlar.	Defter çalışmaya devam eder, ancak hiçbir kayıt dış özetle kapsamaz ve bağımsız doğrulamanın dayanağı oluşmaz.
Hedef sunucular	Değişikliklerin ve sorguların gerçekten çalıştığı veritabanları.	Sadece o sunucuya ait talepler çalışmaz.

1.3 Desteklenen veritabanı türleri

DatabaseType değerleri:

Değer	Tür
1	SQL Server
2	Oracle
3	PostgreSQL

İki ayrı yerde kullanılır ve karıştırılmamalıdır:

1. Uygulamanın kendi veritabanı: her zaman SQL Server'dır, seçenek yoktur.

2. Hedef sunucular: Her sunucu tanımının kendi türü vardır. Aynı kurulum aynı anda SQL Server, Oracle ve PostgreSQL sunucularını yönetebilir.

Hangi hedef türlerinin kullanılabileceği lisanstan gelir. Ayrıntı: Bölüm 3.

1.4 Worker işleri

Worker servisi Quartz zamanlayıcısı ile çalışır. Her iş kendi periyoduna sahiptir ve periyotlar API tarafındaki appsettings.json içindeki Workers bölümünden okunur.

İş	Ne yapar	Ayar anahtarı	Varsayılan
MainWorkJob	Sırayla dört şey yapar: (1) zamanı gelmiş sürüm paketlerini çalıştırır, (2) kuyruğa alınmış talepleri çalıştırır, (3) bekleyen sandbox işlerini çalıştırır, (4) zamanı gelmiş talepleri çalıştırır.	Workers:MainWorkSeconds	30 saniye
ConnectionCheckJob	Tanımlı sunuculara bağlanmayı dener, durum bilgisini günceller.	Workers:ConnectionCheckSeconds	60 saniye
NotificationJob	Kuyruktaki e-posta ve bildirimleri gönderir.	Workers:NotificationFlushSeconds	60 saniye
MaintenanceJob	Bakım görevlerini (MaintenanceTasks tablosu) zamanına göre çalıştırır.	Workers:MaintenanceSeconds	30 saniye
TableWriteLogCoverageJob	Veritabanı seviyesi yazma kaydının kapsam özetini (satır sayısı, numara aralığı) kanıt defterine yazar.	Workers:TableWriteLogCoverageSeconds	86400 saniye (günde bir)
HeartbeatJob	Worker servisinin ayakta olduğunu API'ye bildirir.	Kod içinde sabit periyot	-
LedgerDigestJob	Defter özeti turunu başlatır: API özeti alır, imzalar (imza açıksa), özet klasörüne (Evidence:Ledger:DigestOutputPath) yazar ve geri yükleme ile çatal (eski yedeğe dönüş) kontrolünü yapar.	Evidence:Ledger:DigestIntervalMinutes	60 dakika
EvidenceBoundaryJob	Kanıt yazma sınırını denetler; bozulursa durum değiştiren işlemleri durdurur.	Evidence:Ledger:BoundaryCheckMinutes	15 dakika

Açma ve kapama bayrakları:

Bayrak	Etkisi
Workers:MainWorkEnabled	false ise talep alıřtırma tmyle durur. Zamanlanmış talepler de, ekrandan elle bařlatılanlar da alıřmaz; ikisini de worker yrtr.
Workers:ConnectionCheckEnabled	false ise sunucu baėlantı durumu gncellenmez.
Workers:MaintenanceEnabled	false ise bakım grevleri alıřmaz.
Workers:TableWriteLogCoverageEnabled	false ise yazma kaydının gnlk kapsam zeti deftere yazılmaz.

MainWorkJob aynı anda iki kez alıřmaz. Bir tur bitmeden yeni tur bařlamaz. Bu, aynı talebin iki kez alıřtırılmasını engelleyen ilk katmandır. İkinci katman veritabanı seviyesindedir: bir talebi alıřtırmaya bařlamadan nce worker o talebi "sahiplenir"; bařka bir worker aynı talebi sahiplenemez.

1.5 lkleme ve daėıtım

Bileřen	Ka kopya alıřtırılabilir	Dikkat edilmesi gereken
API	Birden ok kopya alıřtırılabilir. Oturum bilgisi jetonun iinde tařınır, sunucu tarafında oturum durumu tutulmaz.	İstek sınırlama sayaları kopya bazındadır ve IP adresi bařına uygulanır. İki kopya varsa aynı adres iin etkin sınır iki katına ıkar. Kopya sayısı kaydetme hızını artırmaz; sebebi blm 1.6'da aıklanmıřtır.
Web arayz	Birden ok kopya alıřtırılabilir.	Her kopyanın adresi AllowedOrigins listesinde bulunmalıdır.
Worker	Tek kopya alıřtırılmalıdır.	Bir talebin sahiplenilmesi veritabanı seviyesinde atomiktir, yani iki worker aynı talebi aynı anda alamaz. Ancak worker'lar arasında kiralama (lease) mekanizması yoktur: yarım kalmıř alıřtırmaların toparlanması yalnızca zaman eřiėine dayanır. Bkz. 25.7.
Uygulama veritabanı	Tek veritabanı.	Yksek eriřilebilirlik gerekiyorsa veritabanı sunucusu seviyesinde zlr (yk devretme kmesi gibi).

Kapasite ile ilgili pratik notlar:

- Bir talebin alıřma sresi hedef sunucudaki betiėin sresine baėlıdır; uygulama tarafında bir st sınır MaxQueryTimeout parametresidir.

- Worker turları üst üste binmediği için, çok uzun süren bir talep aynı turdaki diğer işleri bekletir. Uzun süren bakım işlerini yoğun olmayan saatlere zamanlamanız önerilir.
- Rapor sorguları ayrı bir zaman aşımına tabidir (Reports:QueryTimeoutSeconds) ve uygulama veritabanı üzerinde çalışır. Çok geniş tarih aralıklarında rapor almak uygulama veritabanını yorar.

1.6 Ölçülmüş kapasite ve boyutlandırma

Aşağıdaki değerler tahmin değildir; gerçek talepler uçtan uca akıştan geçirilerek ölçülmüştür ve ölçüm beş kez tekrarlanmıştır. Tablonun nasıl okunacağı ve önerilen sunucu, hemen altındaki başlıkta anlatılmıştır.

Ölçü	Değer
Talep kaydetme süresi, ortalanca	0,1 ile 0,6 saniye
Talep kaydetme süresi, p95	0,2 ile 0,7 saniye
Tek kullanıcı için saniyede kaydedilen talep	2 ile 9
Talep başına veritabanı büyümesi	yaklaşık 57 KB

Aralık, ölçüm makinesinin o anda başka ne yaptığına bağlıdır. Makine boştayken kaydetme onda bir saniye, makine yoğunken yarım saniye civarındadır. Kullanıcı açısından ikisi de anlık kabul edilir.

Bu tablo nasıl okunmalı ve önerilen sunucu

Yayınlanan değerler ölçülen değerlerdir ve alt sınırdır. Ölçüm, uygulama ile veritabanının aynı makinede çalıştığı dört çekirdekli, 8 GB bellekli bir dizüstü bilgisayarda yapılmıştır. Ayrılmış bir sunucuda değerlerin bundan kötü olması beklenmez. Sunucu üzerinde ayrıca ölçüm yapılmadığı için bu belgede tahmini bir sunucu değeri yayınlanmaz: yazan her rakam gerçekten ölçülmüştür.

Önerilen asgari kurulum:

Bileşen	Asgari	Not
Uygulama sunucusu (API ve Worker)	4 çekirdek, 8 GB bellek, 20 GB disk	Web arayüzü de aynı sunucuda durabilir.
Uygulama veritabanı sunucusu	4 çekirdek, 16 GB bellek, SSD	Beş yıllık saklama için 10 GB mertebesinde veri alanı yeterlidir.
Ağ	Uygulama sunucusu ile veritabanı sunucusu aynı yerel ağda olmalıdır	Sebebi aşağıda.

Uygulama ile veritabanı arasındaki ağ mesafesi, işlemci seçiminden daha çok fark yaratır. Tek bir talep kaydı yüz civarında veritabanı gidiş dönüşü yapar. Aradaki gecikme 0,3 milisaniye ise bunların toplamı otuz milisaniyedir ve fark edilmez. Aynı gecikme 5 milisaniye olursa (farklı veri merkezi veya VPN arkası) yalnızca bu yüzden kaydetme süresine yarım saniye eklenir. Veritabanı sunucusu uygulama sunucusuna ağ olarak yakın tutulmalıdır.

Depolama planlaması

Talep başına 57 KB üzerinden:

Günlük talep	Yıllık büyüme
20	yaklaşık 400 MB
50	yaklaşık 1 GB
100	yaklaşık 2 GB

Bu rakam ham büyümedir. Kurulumla gelen bakım görevleri yalnız süresi dolan jetonları, 90 günden eski bildirim kayıtlarını ve sorgu sonucu dosyalarını siler; talepleri ve denetim kayıtlarını arşivlemez. Denetim kayıtları defter tablosunda durduğu için silinemez.

Talep başına yazılan satır sayısı ilk bakışta beklenenden fazladır, çünkü her değişiklik talebi kendi geri alma talebini de doğurur ve veritabanı denetim izi her yazma işlemini ayrı satırda saklar.

Eş zamanlı kullanım ve ekip büyüklüğü

Kaydetme işlemi talebin satırlarını ve denetim olayını tek transaction içinde yazar. Aynı anda kaydeden kullanıcı sayısı arttıkça veritabanındaki kilit beklemesi artar ve kaydetme süresi uzar.

Ölçülen davranış, beş turun toplamı:

Tam olarak aynı anda kaydeden kişi	Denenen	Kullanıcıya hata dönen
1	40	0
2	80	0
4	160	3
8	320	4

İki kişiye kadar hiç hata yoktur. Dört ve sekiz kişi tam olarak aynı anda kaydettiğinde her yüz istekten bir ile ikisi kullanıcıya hata döner. Böyle bir durumda kaydet düğmesine yeniden basmak yeterlidir; kayıp veri olmaz, yarım kayıt oluşmaz.

Sistem genelinde ölçülen kaydetme tavanı saniyede yaklaşık 20 taleptir. Bu değer tek bir makinede ölçülmüştür ve kurulum kabulünde kurumun donanımında yeniden ölçülür. API'yi birden çok kopya çalıştırmak kaydetme hızını artırmaz, çünkü sınırı belirleyen nokta uygulamada değil veritabanındadır. Birden çok kopya okuma tarafındaki yükü paylaştırır.

Kaç kişilik ekibi kaldırır. Ekip büyüklüğü pratikte sınır değildir. Birkaç yüz kişilik bir ekip desteklenir. Sınırı belirleyen şey ekip mevcudu değil, ekibin gerçekte kaç değişiklik yazdığıdır. Saniyede 20 kaydetme, sekiz saatlik bir iş gününde yüz binlerce kaydetme demektir; kurumsal veritabanı değişiklik hacmi bu mertebede değildir. Dört kişinin tam olarak aynı saniyede kaydetme basması, ancak günlük talep sayısı binleri bulduğunda sıradan hale gelir. Günde elli talep üreten bir ekipte aynı anda kaydetme durumu haftada bir mertebesinde. Yoğun sürüm saatlerinde taleplerin gün içine yayılması bu ihtimali daha da azaltır.

Sunucu sayısı

Yönetilen sunucu sayısı kaydetme hızını etkilemez. Sınırı belirleyen şey bağlantı sağlık kontrolüdür: worker altmış saniyede bir tanımlı aktif sunucuları yoklar (varsayılan olarak aynı anda en çok sekiz sunucu); erişilemeyen bir sunucu, bağlantı zaman aşımı dolana kadar bu yuvalardan birini meşgul eder.

Ortam	Önerilen sunucu sayısı
Yerel ağdaki sunucular	100 ve üzeri
Uzak veya bulut sunucular	30 ile 40

Erişilemeyen sunucular turu uzatır. Kullanımdan kalkan sunucuları pasif duruma almak, sağlık kontrolünün zamanında tamamlanmasını sağlar.

Sınırların özeti

Sınır	Değer	Sınırı belirleyen
Ekip büyüklüğü	birkaç yüz kişi	Ekip mevcudu değil, günlük talep sayısı
Aynı anda kaydeden kişi	2 kişiye kadar hatasız; 4 ve 8 kişide yüz istekte 1 ile 2 tekrar	Veritabanı yazma kilitleri
Sistem geneli kaydetme tavanı	saniyede yaklaşık 20 talep	Veritabanı yazma kilitleri
Günlük talep	5.000 talepte sistemin meşgul olduğu süre oranı yüzde 2	Yukarıdaki tavan
Yönetilen sunucu	yerel ağda 100 ve üzeri, uzak veya bulutta 30 ile 40	Bağlantı sağlık kontrolü turu
Depolama	talep başına yaklaşık 57 KB	Ölçüldü

Bu deęerler talep kaydetme yolu iin, yeni kurulmuř bir veritabanında llmřtr. Uzun sre biriken veride liste ve rapor sorguları veri hacmine baęlı hale gelir; geniř tarih aralıklı raporları yoęun olmayan saatlerde almanız nerilir.

Bölüm 2. Kurulum

Bu bölüm sıfırdan kurulum içindir. Sıra önemlidir. Kurulumdan önce hazırlanacaklar, IIS ve Windows servisi kurulumu, veritabanı yöneticisinin elle kurduğu veritabanı ve entegrasyonların (LDAP, SSO, ITSM, SIEM) ayrıntılı kurulumu iki ayrı belgededir: Kurulum Ön Hazırlık Listesi ve Kurulum ve İşletim Kılavuzu.

2.1 Ön koşullar

Gereksinim	Açıklama
Uygulama sunucusu donanımı	En az 4 çekirdek, 8 GB bellek, 20 GB disk. API, Worker ve web arayüzü aynı sunucuda çalışabilir.
Veritabanı sunucusu donanımı	En az 4 çekirdek, 16 GB bellek, SSD. Beş yıllık saklama için 10 GB mertebesinde veri alanı yeterlidir.
Ağ yakınlığı	Uygulama sunucusu ile uygulama veritabanı sunucusu aynı yerel ağda olmalıdır. Sebebi bölüm 1.6'da açıklanmıştır.
.NET 10 çalışma zamanı	API ve Worker bu sürümle derlenir (net10.0).
SQL Server 2022 veya üzeri	Uygulama veritabanı için. Denetim kayıtları SQL Server 2022 ile gelen append-only defter (ledger) tablosunda tutulur; defter bütün sürümlerde vardır.
Windows sunucu	Worker Windows servisi olarak çalışır. Denetim dosyası PDF üretimi de Windows yazı tiplerini kullanır.
Ağ erişimi	API ve Worker sunucularından hedef veritabanı sunucularına erişim gerekir: talepleri ve bağlantı sağlık kontrolünü Worker yürütür, bağlantı testi ve kolon önizlemesi API üzerinden yapılır. SQL Server için 1433, Oracle için 1521, PostgreSQL için 5432 varsayılan portlardır.
SMTP sunucusu	Bildirim e-postaları için. Zorunlu değildir, kapatılabilir.
Servis hesabı	Worker servisinin çalışacağı hesap. Uygulama veritabanına ve QR dosya klasörüne yazma yetkisi olmalıdır.

2.2 Kurulum adımları

Kurulum şu sırayla yapılır:

1. Veritabanını oluşturun

|

v

2. API appsettings.json dosyasını düzenleyin

|

v

3. API'yi baslat (sema ve varsayılan veri otomatik oluşur)

|

v

4. Lisans dosyasını yükle

|

v

5. İlk yönetici ile giriş yap, şifreyi değiştir

|

v

6. Sunucuları tanımla

|

v

7. Kullanıcıları ekle

|

v

8. Parametreleri ve onay politikalarını ayarla

|

v

9. Worker servisini baslat

|

v

10. Doğrulama kontrol listesini uygula

2.3 Veritabanının oluşturulması

Boş bir veritabanı oluşturmanız yeterlidir. Tablolar, saklı yordamlar ve varsayılan veriler API ilk açıldığında otomatik kurulur.

Bunu sağlayan ayar:

```
"Database": {  
  "AutoMigrate": true  
}
```

AutoMigrate true iken API açılışta şu dosyaları sırayla uygular:

Dosya	İçerik
001_Tables.sql	Tüm tablolar ve indeksler

Dosya	İçerik
002_SeedData.sql	Roller, varsayılan yönetici, parametreler, SQL standartları, rapor tanımları, bakım görevleri
003_StoredProcedures.sql	Rapor saklı yordamları
004_TableWriteLogs.sql	Veritabanı seviyesi yazma kaydı ve tetikleyicileri

Betikler tekrar çalıştırılabilir biçimde yazılmıştır. Var olan kayıt tekrar eklenmez, sizin yaptığınız değişiklikler ezilmez.

AutoMigrate false yapılırsa ürün şemaya dokunmaz: veritabanı yöneticisi bu betikleri uygular, ardından API klasöründeki DbScripts\DbSchemaVersions.ps1 yardımcısının ürettiği kayıt dosyasını çalıştırır. API açılışta eksik ya da değişmiş betik görürse adını söyler ve açılmaz. Sıkı değişiklik kontrolü olan kurumlarda bu tercih edilir. Adımlar Kurulum ve İşletim Kılavuzu Bölüm 3.2'dedir.

2.4 appsettings.json alan alan

Aşağıdaki tablo API tarafındaki appsettings.json dosyasının tüm bölümlerini açıklar. Sırlar bu dosyaya yazılmaz; nasıl verildikleri hemen aşağıda anlatılır.

Sırlar nereden okunur: Ürün, bağlantı dizesi ve şifreleme anahtarı gibi gizli değerleri ortam değişkeninden okur. Yapılandırma dosyasındaki karşılıkları boş bırakılır. Yapılandırma şu sırayla okunur ve her adım bir öncekini ezer: appsettings.json, appsettings.<Ortam>.json, ortam değişkenleri, komut satırı. Ortam değişkeninin adı, ayar yolundaki iki nokta üst üste karakterinin çift alt çizgi ile değiştirilmesiyle bulunur. Örnek: Jwt:SigningKey ayarı Jwt__SigningKey değişkeninden gelir, Security:ServerPasswordKey ayarı Security__ServerPasswordKey değişkeninden gelir.

Neden dosyaya yazılmaz: Yapılandırma dosyası çoğu kurumda kaynak kontrolünde durur ve yedeklere girer. Orada duran bir sır, depoya erişebilen herkesin eline geçer. Bunun en ağır sonucu kanıt imzalama özel anahtarındadır: anahtarı bilen biri kurum adına imzalı kanıt dosyası üretebilir.

Zorunlu beş sır. Bunlar tanımlı değilse ürün çalışmaz: ConnectionStrings:Default (uygulamanın kendi veritabanı), Jwt:SigningKey (oturum jetonu imza anahtarı), Security:ServerPasswordKey (sunucu parolalarının şifrlenmesi), Security:QrZipPasswordKey (sorgu sonucu paketinin şifrlenmesi), Workers:ApiKey (worker servisinin API'ye kimlik kanıtı).

Koşullu sırlar. Yalnız ilgili özellik kullanılıyorsa gerekir: Mail:Password (bildirim e-postası), Ldap:BindPassword (dizin ile kimlik doğrulama), Evidence:Signing:Keys (kanıt dosyalarını, paketleri ve defter özetini imzalayan anahtar), Evidence:Timestamp:ProxyPassword (zaman

damgası sunucusuna vekil sunucu üzerinden çıkılıyorsa), Sso:Providers:N:ClientSecret (kurum hesabıyla girişte OIDC istemci sırrı) ve Sso:Providers:N:SpCertificatePassword (SAML imza sertifikasının parolası). N, kimlik sağlayıcısının listedeki sıra numarasıdır; ilk sağlayıcı 0'dır. Örnek: Sso__Providers__0__ClientSecret. Kullanılmayan bir özelliğin sırrının tanımsız olması eksiklik değildir. Kanıt imzalama anahtarı tanımlı değilse ürün çalışmaya devam eder ve kanıt dosyaları imzasız üretilir; bu eksiklik hem dosyanın kendisinden hem de Yönetişim Kurulum Kontrolü ekranından görülür.

Kanıt imzalama anahtarı hakkında iki nokta. Birincisi: ürün genelinde tek bir anahtar çifti kullanılır ve özel anahtar yalnız API'de durur. Worker zincir mühürlerini API'ye imzalatır, defter özetini ise API kendisi alır ve imzalar; API'den aldığı yapılandırmadan özel anahtar çıkarılır. İkincisi: anahtarlar bir halka içinde tutulur (Evidence:Signing:Keys altında kimlikli olarak). İmza yalnız Evidence:Signing:ActiveKeyId ile belirtilen anahtarla atılır, doğrulama halkadaki her anahtarla yapılabilir. Anahtar değiştirildiğinde eskisinin açık kısmı halkada bırakılmalıdır; geçmiş kanıt dosyalarının doğrulanabilirliği buna bağlıdır.

Worker yapılandırmasını API üzerinden aldığı için o çağrı veritabanı bağlantı dizelerini (paylaşım açaksa), Security anahtarlarını, posta ve SIEM ayarlarını taşır; kanıt imzalama özel anahtarını taşımaz. API ile worker ayrı makinelerdeyse aradaki bağlantının şifreli olması gerekir. Ürün bunu zorlayamaz; bu bir güvenlik duvarı veya ters vekil karardır. Ancak Yönetişim Kurulum Kontrolü ekranı, çağrının şifresiz ve uzak bir adresten geldiğini tespit ederse uyarı gösterir.

Örnek tanımlama (Windows, kalıcı sistem değişkeni). Yönetici komut isteminde: setx /M ConnectionStrings__Default "Server=SQLSRV01;Database=SQLChangeGuard;UserId=scg;Password=...;TrustServerCertificate=True" ve setx /M Jwt__SigningKey "en az 32 karakterlik rastgele değer". Değişkenler tanımlandıktan sonra API ve worker servisleri yeniden başlatılmalıdır; yapılandırma yalnız süreç açılırken okunur. Bir değişkeni kaldırmak için setx kullanılmaz, çünkü boş değer yazar: reg delete "HKLM\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\Environment" /F /V Jwt__SigningKey komutu kullanılır.

Doğrulama: Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranındaki Sır yerleşimi grubu, yukarıdaki sırların her biri için değer nereden geldiğini gösterir. Kurum hesabıyla giriş için tanımlı her kimlik sağlayıcısının sırrı ayrı bir satırdır. Üç durum vardır: ortam değişkeni, yapılandırma dosyası, tanımsız. Beklenen değer ortam değişkenidir. Ekran sırların kendisini hiçbir zaman göstermez, yalnızca nereden geldiklerini söyler.

2.4.1 ConnectionStrings

Anahtar	Ne işe yarar	Örnek
ConnectionStrings:Default	Uygulamanın kendi kayıt veritabanının bağlantı metni.	Server=SQLSRV01;Database=SQLChangeGuard;UserId=scg;Password=...;TrustServerCertificate=True

Uygulamanın kendi kayıt veritabanı SQL Server üzerinde çalışır. PostgreSQL ve Oracle yönetilen hedef veritabanlarıdır; onların bağlantı bilgileri burada değil, Sunucular ekranındaki kayıtlarda tutulur.

Yanlış verilirse: API açılışta bağlanamaz ve günlük dosyasına bağlantı hatası yazar. Hiçbir ekran açılmaz.

2.4.2 Database:EvidenceLedger ve Evidence:Ledger

Kanıt defteri ve defter özeti ayarları. Defterin nasıl çalıştığı Bölüm 5.4, 17.16 ve 17.17'de anlatılır.

Anahtar	Ne işe yarar
Evidence:Ledger:DigestOutputPath	API'nin defter özetlerini (imza açıksa imzalı) yazdığı klasör. Kurumun değiştirilemez deposu olmalıdır: WORM paylaşım, nesne kilidi açık depolama ya da veritabanı yöneticisinin yazamadığı bir paylaşım. Var olan bir dosyanın üstüne yazılmaz. Boş bırakılırsa hiçbir kayıt dış özetle kapsamaz.
Evidence:Ledger:DigestIntervalMinutes	Özetin alınma aralığı, dakika. Varsayılan 60, en az 5.
Evidence:Ledger:DigestStaleAfterIntervals	Kaç aralık boyunca özet gelmezse Yönetişim Kurulum Kontrolü ekranının uyaracağı. Varsayılan 2.
Evidence:Ledger:BoundaryCheckMinutes	Kanıt yazma sınırının denetlenme aralığı, dakika. Varsayılan 15.
Database:EvidenceLedger	Kanıt tablosunun append-only defter olarak kurulması. Varsayılan true; false yalnız entegrasyon testleri içindir. Üretimde false yapılırsa hazırlık ekranı uyarır ve değişiklik App.ControlRelaxed olarak kaydedilir.

Özet klasörüne API uygulama havuzu hesabı yalnız yeni dosya yazabilmeli ve okuyabilmelidir; değiştirme ve silme yetkisi verilmez. Worker hesabına bu klasörde izin gerekmez. Veritabanı yöneticisinin bu klasöre yazma yetkisi olmamalıdır. Ayrıntı: Bölüm 17.17.

2.4.3 Auth

Anahtar	Ne işe yarar	Varsayılan	Örnek etki
Auth:Mode	Üründe kaydı olmayan bir kişi şifre ekranından	Local	

Anahtar	Ne işe yarar	Varsayılan	Örnek etki
	girmeye çalıştığında hangi yolla doğrulanacağı. Local: yalnız üründe açılmış hesaplar girer. Ldap: kaydı olmayan kişi kurum dizinine sorulur; doğrulanırsa hesap açılır. Hesap izin grubunun eşlendiği rolle açılır. Eşlenen grubu yoksa Ldap:RoleSource Manual iken hesap erişimsiz (NoAccess) açılır ve rolünü yönetici verir; Directory iken hesap açılmaz. Kaydı olan kullanıcıda bu ayar kullanılmaz; hesabın kendi kimlik doğrulama tipi (Yerel, LDAP, Kurum hesabı) geçerlidir. Kurum hesabıyla (SSO) gelen yeni kişileri bu ayar değil Sso:AutoProvision belirler.		
Auth:AccountLockoutMaxAttempts	Kaç hatalı şifre ya da iki adımlı doğrulama kodu denemesinden sonra hesap kilitlenir. İkisi aynı sayaca sayılır.	5	5 iken beşinci yanlış denemede hesap kilitlenir.
Auth:AccountLockoutMinutes	Kilit süresi (dakika).	15	15 iken kilitlenen hesap 15 dakika sonra kendiliğinden açılır.
Auth:Password:MinLength	En az şifre uzunluğu.	6	
Auth:Password:RequireUppercase	Büyük harf zorunlu mu.	false	
Auth:Password:RequireDigit	Rakam zorunlu mu.	true	true iken "şifre" reddedilir, "şifre1" kabul edilir.
Auth:Password:HistoryCount	Son kaç şifre tekrar kullanılamaz. 0 = kontrol yok.	0	3 iken kullanıcı son üç şifresinden birini tekrar seçemez.

Anahtar	Ne işe yarar	Varsayılan	Örnek etki
Auth:Password:ExpiryDays	Şifre kaç günde bir değişmeli. 0 = süresiz.	0	90 iken 90 gün sonra kullanıcı şifre değiştirmeye zorlanır.
Auth:Password:ResetTokenExpiryMinutes	Şifre sıfırlama bağlantısının geçerlilik süresi.	30	
Auth:Password:ResetBaseUrl	Şifre sıfırlama e-postasındaki bağlantının kök adresi. Web arayüzünün adresi yazılır.	http://localhost:5173	Yanlış yazılırsa kullanıcı e-postadaki bağlantıya tıkladığında hatalı sayfaya gider.
Auth:MaxSessionHours	Bir oturumun ilk girişten itibaren en uzun süresi (saat). Jeton yenileme bu süreyi uzatmaz; süre dolunca kullanıcı yeniden giriş yapar. 0 sınırsız demektir.	12	12 iken sabah 08:00'de giren kullanıcı en geç 20:00'de yeniden giriş yapar.
Auth:MfaTicketMinutes	Şifre doğrulandıktan sonra iki adımlı doğrulama kodunun girilebileceği süre (dakika).	5	5 iken kod 5 dakika içinde girilmezse kullanıcı şifre adımına döner.
Auth:MfaTicketMaxAttempts	Tek bir girişte en fazla kaç hatalı kod denenebilir.	5	5 iken beşinci hatalı koddan sonra kullanıcı şifre adımına döner.
Auth:LocalLoginAllowedUsers	Şifre ekranından girebilecek yerel hesapların listesi. Boş liste bütün yerel hesapların girebileceği anlamına gelir. Liste doluysa yalnız listedeki yerel hesaplar şifreyle girer; diğerlerine "Bu hesapla şifre ile giriş kapalı" denir ve şifre hiç denenmez. Kurum hesabıyla giriş açıkken bu listeye yalnız acil durum hesapları yazılır. LDAP ve kurum hesapları bu listeden etkilenmez.	boş (bütün yerel hesaplar)	["admin"] iken yalnız admin şifreyle girer. Bu hesabın her girişi kurum hesabıyla giriş açıkken LoginBreakGlass olayı olarak denetim izine yazılır ve SOC'a alarm olarak gider.

2.4.4 Jwt

Kullanıcı giriş yaptığında verilen erişim jetonunun ayarları.

Anahtar	Ne işe yarar	Varsayılan
Jwt:Issuer	Jetonu üreten tarafın adı.	SCG
Jwt:Audience	Jetonu kullanacak tarafın adı.	SCG-Clients
Jwt:AccessTokenMinutes	Erişim jetonunun ömrü (dakika). Süre dolunca yenileme jetonu ile yenilenir.	120
Jwt:RefreshTokenHours	Yenileme jetonunun ömrü (saat). Bu da dolarsa kullanıcı yeniden giriş yapar. Yenileme oturumun toplam süresini uzatmaz; üst sınır Auth:MaxSessionHours ayarıdır.	48
Jwt:SigningKey	Jetonun imza anahtarı. Üretimde mutlaka değiştirin.	(dosyada boş; Jwt__SigningKey ortam değişkeni ile verilir)

SigningKey neden önemlidir: jeton, bu anahtarla imzalanır. Anahtarı bilen biri istediği kullanıcı adına geçerli jeton üretebilir, yani parola bilmeden sisteme girebilir. En az 32 karakter, rastgele üretilmiş bir değer kullanın.

Anahtar değiştirilirse: o anda açık olan tüm oturumlar geçersiz olur ve herkes yeniden giriş yapar. Veri kaybı olmaz.

Oturumun toplam süresi: Erişim jetonunun süresi dolunca uygulama yenileme jetonuyla yeni bir jeton alır. Yenileme oturumu uzatmaz: oturumun başladığı an yeni jetona taşınır ve ilk girişin üzerinden Auth:MaxSessionHours kadar süre geçince yenileme reddedilir, kullanıcı yeniden giriş yapar. Böylece dizinde kapatılan bir hesabın açık oturumu da en geç bu sürede kapanır. Erişim jetonu ve yenileme jetonu bu tavanın ötesine geçmez: tavana yakın yapılan son yenilemede iki jetonun bitişi de oturumun bitişine kırılır ve oturum kaydındaki bitiş tarihi oturumun gerçek sonunu gösterir. Tarayıcı sekmesi uzun süre açık kalsa, sayfa yenilense ya da yeni bir sekme açılrsa da oturum, yenileme jetonu geçerli olduğu sürece devam eder. Sekmeler aynı oturumu paylaşır; bir sekmede alınan yeni jeton diğerlerine de geçer, bir sekmede yapılan çıkış hepsini kapatır. Reddedilen her yenileme, sebebiyle birlikte SessionRefreshRejected olayı olarak denetim kaydına yazılır: Revoked (harcanmış bir jetonun yeniden kullanılması), Expired, SessionLifetimeExceeded, NoAccess ya da SsoDisabled.

Çıkış yapıldığında yenileme jetonu sunucuda iptal edilir ve çıkış denetim kaydına kullanıcının adıyla yazılır. Yenileme jetonları, şifre sıfırlama bağlantıları ve iki adımlı doğrulama biletleri veritabanında açık metin olarak değil, tek yönlü özet (SHA-256) olarak saklanır; veritabanını okuyabilen biri bunlarla oturum açamaz.

2.4.5 Security (şifreleme anahtarları)

Anahtar	Ne işe yarar	Kaybolursa ne olur
Security:ServerPasswordKey	Sunucu tanımlarındaki veritabanı şifrelerinin diskte şifrlenmesi için kullanılan AES-256 anahtarı. 32 baytlık, base64 kodlu değer.	Kayıtlı sunucu şifreleri çözülemez. Her sunucu tanımına şifre yeniden girilmelidir.
Security:QrZipPasswordKey	Sorgu sonucu ZIP paketlerinin parolalarının şifrlenmesi için kullanılan AES-256 anahtarı.	Eski sonuç dosyalarının parolaları görüntülenemez.

Bu anahtarları nasıl üretirsiniz: 32 baytlık rastgele bir değeri base64 olarak kodlayın. PowerShell ile:

```
$bytes = New-Object byte[] 32  
[System.Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bytes)  
[Convert]::ToBase64String($bytes)
```

Bu anahtarların appsettings.json içinde düz metin durması yerine ortam değişkeni ile verilmesi gerekir; kullanıcı sırları (user secrets) yalnız geliştirme ortamında okunur.

Anahtar rotasyonu tuzağı: ServerPasswordKey değiştirilirse eski şifrelenmiş değerler yeni anahtarla çözülemez. Anahtar değiştirmeden önce tüm sunucu şifrelerinin yeniden girileceğini planlayın.

2.4.6 License

Anahtar	Ne işe yarar	Varsayılan
License:LicensePath	Lisans dosyasının yolu.	license.scglicense
License:PublicKeyPem	Lisans imzasının doğrulandığı açık anahtar. Değiştirilmez.	Ürünle gelir
License:ExpiryWarningDays	Lisans bitişine kaç gün kala uyarı verilsin.	30

ExpiryWarningDays 30 iken, lisansın bitmesine 29 gün kaldığında lisans durumu "Expiring" olur ve arayüzde uyarı görünür. Sistem çalışmaya devam eder.

2.4.7 Mail

Anahtar	Ne işe yarar	Not
Mail:Enabled	E-posta gönderimi açık mı.	false ise hiç e-posta gitmez, kayıt yine tutulur.
Mail:SmtpHost	SMTP sunucu adresi.	
Mail:SmtpPort	SMTP portu.	587 yaygın kullanımdır.
Mail:Username, Mail:Password	SMTP kimlik bilgileri.	
Mail:FromAddress, Mail:FromName	Gönderen adresi ve görünen adı.	
Mail:EnableSsl	Şifreli bağlantı kullanılsın mı.	Üretimde true olmalıdır.
Mail:DevMode	true ise tüm e-postalar gerçek alıcı yerine tek bir test adresine gider.	Üretimde mutlaka false yapın.
Mail:DevOverrideEmail	DevMode açıkken kullanılacak test adresi.	

Üretim kurulumunda en sık yapılan hata: DevMode true bırakmak. Bu durumda talep sahiplerine hiç e-posta ulaşmaz, hepsi test kutusuna düşer.

2.4.8 Ldap

Kurum dizini (LDAP ya da Active Directory) ile şifre doğrulama. Kişi giriş ekranına kurum kullanıcı adını ve şifresini yazar; ürün şifreyi saklamaz, dizine sorar. Ldap:Host boş bırakılırsa dizin kullanılmaz. Hatalı değer sessizce kullanılmaz: güvenli bir varsayılan kullanılır ve hata Yönetişim Kurulum Kontrolü ekranında gösterilir; girişi imkânsız kılan bir hata varsa (BaseDn boş, bağlanma biçiminin istediği alan bilgisi ya da servis hesabı yok, kullanıcı süzgecinde {user} yok) dizine hiç gidilmez.

Anahtar	Ne işe yarar
Ldap:Host	Dizin sunucusunun adı, örnek dc01.kurum.local. Boş bırakılırsa dizin kullanılmaz.
Ldap:Port	Bağlantı noktası. Yazılmazsa Ldaps için 636, StartTls ve None için 389.
Ldap:Security	Bağlantının şifrlenmesi. Ldaps (varsayılan, önerilen): baştan şifreli bağlantı. StartTls: şifresiz porta bağlanıp şifreliye geçer. None: şifresiz; kişilerin şifresi ağda açık gider, yalnız bilinçli olarak ve test için.
Ldap:BaseDn	Kişilerin arandığı dizin yolu, örnek DC=kurum,DC=local. Bu yolun dışındaki kişi bulunamaz. Zorunludur.

Anahtar	Ne işe yarar
Ldap:BindDn, Ldap:BindPassword	Yalnız okuma yetkili servis hesabının tam adı ve şifresi. SearchDn biçimi ve dizin eşitlemesi için zorunludur. Şifre bir sırdır, üretimde Ldap__BindPassword ortam değişkeniyle verilir.
Ldap:Domain	Active Directory alan adı, örnek KURUM. DownLevel biçiminde zorunludur. Kişi farklı bir alan adı yazarsa (BASKA\ali) şifre hiç denenmez.
Ldap:TimeoutSeconds	Dizin çağrısının zaman aşımı (saniye), 2 ile 60 arası. Varsayılan 10.
Ldap:AllowUntrustedCertificate	true iken dizin sunucusunun sertifikası doğrulanmaz. Yalnız kendinden imzalı sertifikalı test ortamı içindir; üretimde false olmalıdır, aksi halde araya giren biri kendini dizin gibi gösterip şifreleri toplayabilir.
Ldap:BindFormat	Şifrenin dizine hangi adla doğrulatılacağı. DownLevel: KURUM\kullanıcı (Active Directory, Ldap:Domain gerekir). Upn: kullanıcı@kurum.local (Active Directory, Ldap:UpnSuffix gerekir). SearchDn: önce servis hesabıyla kişi aranır, sonra bulunan tam adla doğrulanır (OpenLDAP gibi genel dizinler).
Ldap:UpnSuffix	Active Directory UPN soneki, örnek kurum.local. Upn biçiminde zorunludur.
Ldap:UserFilter	Kişiyi bulan arama süzgeci. {user} yazılan kısa adla değişir; özel karakterler kaçışlanır. Tam olarak bir kişi döndürmelidir. Varsayılan: (&(objectClass=user)(sAMAccountName={user})). OpenLDAP örneği: (&(objectClass=inetOrgPerson)(uid={user})).
Ldap:IdentityAttribute	Kişinin değişmeyen kimliğini tutan öznitelik. Active Directory: objectGUID (varsayılan). OpenLDAP: entryUUID. Hesap ilk girişte bu değere bağlanır; kullanıcı adı değişse ya da aynı adla yeni biri açılrsa bile hesap yanlış kişiye geçmez.
Ldap:EmailAttribute, Ldap:DisplayNameAttribute	E-posta (varsayılan mail) ve görünen ad (varsayılan displayName) öznitelikleri. Dizinde e-postası olmayan kişiye hesap açılmaz.
Ldap:GroupMatch	Rol eşlemede grubun hangi adıyla karşılaştırılacağı. Dn (varsayılan, önerilen): tam adla; başka klasördeki aynı adlı grup eşleşmez. Cn: kısa adla; farklı klasörlerdeki aynı adlı gruplar ayırt edilmez.
Ldap:NestedGroups	true (varsayılan) iken iç içe gruplar da sayılır: A grubu B grubunun içindeyse A üyesi B üyesi de sayılır. En fazla 10 seviye ve 500 grup okunur.
Ldap:RoleSource	Dizin hesabının rolünün kaynağı; Sso:RoleSource ile aynı kural. Manual (varsayılan): dizin grubu yalnız ilk açılışta rol

Anahtar	Ne işe yarar
	verir; eşlenen grubu olan kişi o rolle, olmayan erişimsiz (NoAccess) açılır. Sonrasında rolü yönetici Kullanıcılar ekranından yönetir; dizindeki grup değişikliği rolü değiştirmez. Directory: rol her girişte ve her eşitlemede izin grubundan hesaplanır; eşlenen grubu olmayan kişiye hesap açılmaz ve rol ekrandan elle değiştirilemez (SystemManager hariç). İki modda da yeni kişinin grupları dizinden okunamazsa hesap açılmaz; kişi tekrar dener.
Ldap:Sync:Enabled	true iken izin eşitlemesi düzenli aralıklarla yapılır: Worker zamanın geldiğini API'ye bildirir, eşitlemeyi API yapar (Worker dizine bağlanmaz). Dizinde bulunamayan ya da kapalı hesap erişimsiz (NoAccess) bırakılır ve oturumları kapanır, hesap silinmez. Varsayılan false; üretimde açık olması önerilir.
Ldap:Sync:IntervalMinutes	iki eşitleme arası en az süre (dakika), 15 ile 1440 arası. Varsayılan 60.
Ldap:Sync:AbortRatio, Ldap:Sync:AbortMinCount	Güvenlik sınırı. Bir eşitlemede erişimi kapatılacak hesap sayısı AbortMinCount değerinden (varsayılan 5) az değilse ve oran AbortRatio değerini (varsayılan 0.2, yüzde 20) aşıyorsa eşitleme hiçbir değişiklik yapmaz ve Ldap.SyncAborted olayını yazar.
Workers:DirectorySyncPollSeconds	Worker'ın API'ye eşitleme zamanının gelip gelmediğini sorma aralığı (saniye). Varsayılan 300. Worker dizine bağlanmaz; izin ayarları yalnız API'de durur.

LDAP kullanıcıları ile yerel kullanıcıların farkı Bölüm 4.8'de anlatılır. Kurum hesabıyla (SSO) giriş yapan kullanıcılar da aynı bölümdedir; bağlantı ayarları Bölüm 2.4.11'dedir.

Ayar değişikliğinin izi: Bu bölüm ve Auth:Mode yapılandırma dosyasında durur. API her açılışta bu ayarların şifre içermeyen özetini son kayıtlarla karşılaştırır; fark varsa eski ve yeni hali Ldap.ConfigurationChanged olayıyla denetim izine yazılır ve SOC'a alarm olarak gider.

2.4.9 Diğer ayarlar

Anahtar	Ne işe yarar	Varsayılan
Display:TimeZone	Belgelerde ve sunucu tarafında üretilen çıktılarda saatlerin gösterileceği saat dilimi.	Europe/Istanbul
AllowedOrigins	Web arayüzünün çalıştığı adresler. Buraya yazılmayan adresten gelen istek reddedilir.	localhost adresleri

Anahtar	Ne işe yarar	Varsayılan
Mfa:Enabled	İki adımlı doğrulamanın ana anahtarı. Kapalıysa hiçbir kullanıcı iki adımlı doğrulama kuramaz ve girişte kod istenmez. Açık olması tek başına kod zorunlu kılmaz; ayrıntı aşağıda.	true
Mfa:Method	Yöntem. Totp mobil doğrulayıcı uygulaması demektir.	Totp
Mfa:Issuer	Doğrulayıcı uygulamada görünecek ad.	SQLChangeGuard
Mfa:EnforceEnrollment	Kaydolmanın zorunlu olup olmadığı. Kapalıyken kaydolmak kullanıcının tercihidir. Açıkken kaydolmamış kullanıcı giriş yapar ama oturumu yalnız kurulum adımına yarar.	false
ForwardedHeaders:KnownProxies	Ürün bir ters vekil (yük dengeleyici) arkasındaysa o vekilin IP adresleri. Yalnız bu adreslerden gelen X-Forwarded-For başlığı işlenir ve denetim kaydına gerçek istemci IP adresi yazılır.	boş (başlık okunmaz)

İki adımlı doğrulama nasıl devreye girer: Ana anahtar açık olsa bile kod, yalnızca kendi hesabında iki adımlı doğrulamayı kurmuş kullanıcılardan istenir. Kurulum kullanıcı bazındadır ve kullanıcının kendisi tarafından yapılır. Ana anahtar kapatılırsa mevcut kurulumlar da devre dışı kalır. Yani ana anahtarın açık olması, kurumdaki herkesin iki adımlı doğrulama kullandığı anlamına gelmez; kaç kullanıcının kurduğunu Ayarlar > Tanılama ekranındaki MFA kayıt oranı satırından görebilirsiniz.

Dizin (LDAP) hesapları da iki adımlı doğrulama kurabilir. Dizin şifreyi doğrular ama ikinci faktör sunmaz; kod, dizin şifresi doğrulandıktan sonra ürün tarafından istenir. Kaydolma zorunlu tutulduğunda LDAP hesapları da kurulum adımından geçer.

Kaydolmayı zorunlu kılmak: Mfa:EnforceEnrollment açıldığında, iki adımlı doğrulamayı henüz kurmamış bir kullanıcı giriş yapabilir ancak o oturum yalnızca kurulum adımına yarar. Kullanıcı parolasını doğruladıktan sonra ekranda doğrudan kurulum adımı açılır: karekod, elle girilebilir anahtar ve altı haneli doğrulama kodu alanı. Kod doğrulanana kadar başka hiçbir işlem çalışmaz; kural arayüzde değil sunucuda uygulanır, yani adres çubuğundan başka bir ekrana gidilse de istekler reddedilir. Kod doğrulandığı anda oturum normale döner, yeniden giriş yapmak gerekmez. Bu ayar yalnız ana anahtar açıkken anlamlıdır. Ana anahtar kapalıyken zorunluluk bayrağı tek başına hiçbir şey yapmaz; aksi halde kullanıcılar kuramayacakları bir kurulumla yönlendirilir ve kilitlenirdi. Ayarın açık olup olmadığı Ayarlar > Tanılama ekranında MFA kaydı zorunlu satırında görünür. Kod adımının güvenliği: Kod ekranına yalnız şifresini (ya da izin şifresini) doğrulamış kişi gelebilir. Şifre doğrulanınca sunucu o girişe özel, tek kullanımlık ve kısa ömürlü bir bilet üretir	Sorgu sonucu ZIP dosyalarının yazılacağı klasör.	C:\SCG\QrFiles
--	---	-----------------------

(Auth:MfaTicketMinutes); kod ancak bu biletle birlikte kabul edilir. Yalnız kullanıcı adı ve kod bilinerek giriş yapılamaz. Bir biletle en fazla Auth:MfaTicketMaxAttempts kez hatalı kod denenebilir; sonra kullanıcı şifre adımına döner. Hatalı kodlar hatalı şifre ile aynı kilit sayacına sayılır ve hesabı kilitleyebilir. Kabul edilmiş bir kod, geçerlilik süresi dolmamış olsa bile ikinci kez kabul edilmez. Başarılı ve başarısız her kod denemesi gerçek kullanıcı adıyla ve bağlantının IP adresiyle denetim kaydına yazılır (MfaSuccess, MfaFailed). Ters vekil arkasında çalışmak: Denetim kayıtlarındaki IP adresi bağlantının kendisinden okunur; istemcinin gönderdiği X-Forwarded-For başlığına güvenilmez, çünkü o başlığı herkes yazabilir. Ürün bir ters vekil ya da yük dengeleyici arkasında çalışıyorsa vekilin IP adresi ForwardedHeaders:KnownProxies listesine yazılır. Yalnız bu listedeki vekillerden gelen başlık işlenir ve kayda gerçek istemci adresi düşer. Liste boşsa bütün kayıtlarda vekilin adresi görünür. QueryResult:OutputPath		
---	--	--

QueryResult:MaxMailAttachmentMB	E-posta ekinin en büyük boyutu. Bunu aşan dosya eklenmez, kullanıcı arayüzden indirir.	10
Reports:QueryTimeoutSeconds	Rapor sorgularının zaman aşımı.	500
RateLimiting:PermitPerMinute	Dakikada izin verilen istek sayısı.	60
RateLimiting:QueueLimit	Sıraya alınacak istek sayısı.	10
Workers:ApiKey	Worker servisinin API'ye kimliğini kanıtladığı anahtar. Worker tarafındaki WorkerApi:Key ile aynı olmalıdır.	(dosyada boş; Workers__ApiKey ortam değişkeni ile verilir)
Workers:WorkerErrorMailTo	Worker beklenmedik hata verirse bildirimin gideceği adres.	
Workers:StaleExecutionRecoveryMinutes	Çökme kurtarma eşiği (dakika). Bu süreden uzun süredir sahiplenilmiş kalan çalıştırma ölü kabul edilir. Hedefte commit olmadığı kesin olan talep Approved durumuna döner; commit olmuş olabilecek talep Uzlaştırma bekliyor (ReconciliationRequired) durumuna alınır ve yeniden çalıştırılmaz. Ayrıntı: Bölüm 25.7.	120

QueryResult:OutputPath klasörüne worker servis hesabının yazma yetkisi olmalıdır. Yetki yoksa sorgu çalışır ama dosya oluşturulamaz ve talep detayında paketleme hatası görünür.

2.4.10 SIEM (SOC entegrasyonu)

Ürün, yönetim olaylarını kurumun SOC toplayıcısına aktarabilir. Bu bölüm bağlantı bilgisini taşır: hangi adrese, hangi protokolle ve hangi biçimde gönderileceğini. Gönderimin kapsamı burada değil, Ayarlar ekranındaki parametrelerden yönetilir (Bölüm 7.11).

Ayrım bilinçlidir. Adres, port ve sertifika bir kurulum bilgisidir; kurulumu yapan kişi bilir ve nadiren değişir. Kapsam ise bir kontroldür: neyin SOC'a gittiğini belirler, değişmesi denetim kaydına düşmelidir ve dört göz kuralına tabi olmalıdır. İkisi aynı yerde tutulsaydı, kapsamı daraltmak için dosyaya erişmek yeterli olurdu ve bu değişiklik hiçbir yerde görünmezdi.

Bu bölüm worker tarafına ayrıca yazılmaz. Worker aynı ayarları API üzerinden alır. İki ayrı yerde tutulsaydı API ile worker farklı uçlara yazabilir ve bunu hiçbir şey söylemezdi.

Anahtar	Ne işe yarar	Kurulumla gelen değer
Siem:Endpoints[].Name	Uç adı. Teslim işareti bu adla tutulur. Kuruludan sonra değiştirilirse o uç yeni sayılır ve işareti sıfırdan başlar, yani geçmiş olayların tamamı yeniden gönderilir.	SOC
Siem:Endpoints[].Type	Syslog asıl hedeftir. File seçeneği her satıra bir olay gelecek şekilde dosyaya yazar; toplayıcısı olmayan kurumlar ve kurulum denemesi için kullanılır.	File
Siem:Endpoints[].Host	Toplayıcının adresi.	127.0.0.1
Siem:Endpoints[].Port	Toplayıcının portu. Şifreli syslog için yaygın değer 6514'tür.	6514

Anahtar	Ne işe yarar	Kurulumla gelen değer
Siem:Endpoints[].Protocol	Tls, Tcp veya Udp. Tls önerilir. UDP tek pakete sığmayan mesajı kaybeder ve kaybettiğini söylemez; yalnız kurum ısrar ederse kullanın.	Tls
Siem:Endpoints[].Format	Rfc5424Json, Rfc5424Sd, Cef, Leef veya Json. Toplayıcıya göre seçilir: ArcSight için Cef, QRadar için Leef, diğerlerinin çoğu için Rfc5424Json.	Json
Siem:Endpoints[].Facility	Syslog tesis adı. Toplayıcıda kaynağı ayırt etmek için kullanılır.	local0
Siem:Endpoints[].TlsServerCertificateThumbprint	Boş bırakılırsa sistemin güven zinciri kullanılır. Doldurulursa toplayıcının sertifikası bu parmak iziyle karşılaştırılır ve tutmazsa bağlantı reddedilir. Kendi imzalı sertifika kullanan toplayıcılar için doldurun.	(boş)
Siem:Endpoints[].FilePath	Yalnız Type değeri File iken kullanılır. Dosyanın yolu.	logs/siem-events.jsonl
Siem:Endpoints[].BatchSize	Bir turda en fazla kaç olay gönderilir. Toplayıcı uzun süre kapalı kalırsa birikmiş kayıtlar bu büyüklükte gruplar halinde akar.	200
Siem:Endpoints[].PollSeconds	Uç tanımında saklanır, zamanlamayı belirlemez. Gönderim aralığı worker tarafındaki Workers:SiemPumpSeconds	10

Anahtar	Ne işe yarar	Kurulumla gelen değer
	anahtarından gelir ve bütün uçlar aynı turda taranır.	
Siem:Endpoints[].Heartbeat Minutes	Uç tanımında saklanır, zamanlamayı belirlemez. Nabız aralığı ürün genelinde beş dakikadır.	5
Siem:AppLogQueueSize	Ürünün kendi günlüğü için bellek kuyruğu kapasitesi. Dolarsa en eski kayıt düşürülür ve sayaç artar.	10000
Siem:AppLogMinLevel	Bu seviyenin altındaki ürün günlüğü SOC'a gitmez. Information göndermek SOC'u ürünün ayrıntılarıyla boğar.	Warning
Workers:SiemPumpSeconds	Gönderim yoklamasının aralığı (saniye). Bir denetim kaydının SOC'a ulaşması varsayılan değerde en fazla on saniye sürer. Sıfır veya negatif değer yok sayılır ve 10 kullanılır; üst sınır 3600 saniyedir.	10
Workers:SiemLeaseSeconds	Uç ve akış başına tek yazıcı kirasının süresi (saniye). Worker birden fazla kopya çalıştırılırsa ikinci kopya bu süre dolmadan aynı akışa yazmaz.	60

Birden fazla uç tanımlanabilir. Her uç kendi teslim işaretini tutar; biri erişilemez olduğunda diğeri etkilenmez.

Kurulumla gelen değer File olarak gelir; böylece ürün kurulur kurulmaz, ortada bir toplayıcı olmadan da gönderimin çalıştığı görülebilir. Kurum toplayıcısına bağlanırken Type değeri Syslog yapılır ve adres, port, protokol ile biçim doldurulur.

2.4.11 Sso (kurum hesabıyla giriş)

Kurum hesabıyla giriş (tek oturum açma, SSO) açıkken kullanıcı şifresini ve çok faktörlü doğrulamasını kurumun kendi giriş sayfasında girer; şifre ürüne hiç gelmez. Ürün iki standart protokolü destekler: OIDC (Microsoft Entra ID, Keycloak, Okta) ve SAML 2.0 (AD FS, Entra ID, Keycloak). Kimliği doğrulanan kişi değişmeyen kimliğiyle bulunur ya da açılır, grubu bir role eşlenir ve ürün kendi oturumunu başlatır. Varsayılan olarak kapalıdır. Değişiklikten sonra API yeniden başlatılır.

Anahtar	Ne işe yarar	Varsayılan
Sso:Enabled	true iken giriş ekranında her kimlik sağlayıcısı için "... ile giriş yap" düğmesi görünür. false iken kurum hesabı tipindeki hesaplar giremez ve API yeniden başlatıldığı anda bu hesapların açık oturumları da kapanır (örnek: kimlik sağlayıcısının güvenliğinden şüphe edildiğinde); yerel ve LDAP giriş etkilenmez.	false
Sso:ApiBaseUrl	API'nin tarayıcıdan görünen adresi. Kimlik sağlayıcısına bildirilen geri dönüş adresi bundan kurulur. Adres istekten türetilmez; ters vekil arkasında da doğru adres üretilir.	http://localhost:5204
Sso:FrontendBaseUrl	Web arayüzünün adresi. Giriş bitince tarayıcı bu adrese döner. Dönüş adresi yalnız buradan okunur; saldırganın	http://localhost:5173

Anahtar	Ne işe yarar	Varsayılan
	yönlendirme adresi vermesi mümkün değildir.	
Sso:AutoProvision	true iken üründe hesabı olmayan kişi ilk girişinde otomatik açılır. false iken hesabı önce yönetici Kullanıcılar ekranında Kurum hesabı tipiyle, aynı kullanıcı adıyla açar.	true
Sso:RoleSource	Idp: rol her girişte kimlik sağlayıcısındaki gruptan yeniden hesaplanır; gruptan çıkarılan kişi bir sonraki girişinde rolünü kaybeder ve açık oturumları kapanır. Manual: grup yalnız ilk açılışta rol belirler, sonrasını yönetici yönetir.	Idp
Sso:MaxSessionHours	Kurum hesabıyla açılan oturumun en uzun süresi (saat). Auth:MaxSessionHours ile birlikte küçük olanı uygulanır. Kimlik sağlayıcısında kapatılan hesabın üründeki oturumu en geç bu sürede biter.	10
Sso:SignOutFromIdp	true iken üründen çıkan kullanıcı kimlik sağlayıcısından da çıkarılır (yalnız OIDC).	false
Sso:LoginTimeoutMinutes	Giriş düğmesine basıldıktan sonra kimlik sağlayıcısından	10

Anahtar	Ne işe yarar	Varsayılan
	dönmek için tanınan süre (dakika).	
Sso:ExchangeCodeSeconds	Dönüşten sonra arayüzün oturumla takas ettiği tek kullanımlık kodun ömrü (saniye). Kod yalnız girişi başlatan tarayıcıda geçerlidir.	120
Sso:ClockSkewMinutes	Kimlik sağlayıcısının cevabındaki süre kontrolünde kabul edilen saat farkı (dakika).	5
Sso:Providers	Kimlik sağlayıcıları listesi. Her biri giriş ekranında ayrı bir düğmedir. Alanları aşağıdaki tabloda.	boş

Her kimlik sağlayıcısının alanları:

Anahtar	Ne işe yarar
Name	Değişmeyen ad. Kullanıcının bağlı kimliği ve rol eşlemeleri bu adla tutulur; kurulumdan sonra değiştirilmez. Yalnız harf, rakam, tire ve alt çizgi içerir.
DisplayName	Giriş düğmesinde görünen ad.
Protocol	Oidc ya da Saml.
RequireHttpsMetadata	Üstveri adresinin HTTPS olması zorunlu mu. Üretimde her zaman true olmalıdır.
Authority, ClientId, ClientSecret, Scopes	OIDC için sağlayıcının adresi, uygulama kaydında verilen istemci kimliği ve istemci sırrı. İstemci sırrı ortam değişkeniyle verilmelidir.

Anahtar	Ne işe yarar
IdpMetadataUrl, SpEntityId, SpCertificatePath, SpCertificatePassword, SignAuthnRequests	SAML için kimlik sağlayıcısının üstveri adresi, ürünün SAML kimliği ve isteğe bağlı imza sertifikası. Sertifika parolası ortam değişkeniyle verilmelidir.
SubjectClaim	Kişiyi eşleştiren değişmeyen kimlik. Entra ID: oid, Keycloak ve Okta: sub, SAML: NameID (kalıcı biçimde olmalıdır). E-posta ya da kullanıcı adı yazılmaz, çünkü değişebilirler.
UsernameClaim, EmailClaim	Yeni açılan hesabın kullanıcı adı ve e-postası.
GroupsClaim	Rol eşleymesinde okunan bilgi. Entra ID'de uygulama rolleri (roles) önerilir.
RequireMfaClaim, MfaClaim, MfaClaimValue	true iken kimlik sağlayıcısı çok faktörlü doğrulama yapıldığını bildirmezse giriş reddedilir. Üretimde true önerilir.

Kimlik sağlayıcısı tarafına girilecek adresler (geri dönüş adresi, çıkıştan sonra dönüş adresi, SAML uygulama kimliği ve üstveri adresi) Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında kopyalanabilir biçimde gösterilir. Aynı ekrandaki Bağlantıyı test et düğmesi kimlik sağlayıcısının üstverisine ulaşıp ulaşılamadığını gösterir. Hatalı tanımlanan sağlayıcı kullanılmaz ve Yönetişim Kurulum Kontrolü ekranında Kurum hesabı ayar hataları satırında görünür.

Hangi grubun hangi rolü alacağı bu dosyada değil, Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranındaki Grup ile rol eşlemesi tablosunda yönetilir (Bölüm 4.8).

Ayar değişikliğinin izi: Bu bölüm yapılandırma dosyasında durduğu için ekrandan değişmez. Dosyada yapılan bir değişikliğin (kurum hesabıyla girişi kapatmak, MFA denetimini kaldırmak, rolün kaynağını değiştirmek, Auth:LocalLoginAllowedUsers listesini değiştirmek gibi) izi yine de kalır: API her açılışta bu ayarların özetini son kayıtla karşılaştırır ve fark varsa eski ve yeni halini Sso.ConfigurationChanged olayıyla denetim izine yazar. Olay SOC'a kontrol değişikliği olarak gider ve User Access Changes raporunda görünür. Özete sırlar yazılmaz; yalnız tanımlı olup olmadıkları yazılır. Aynı ayarla yeniden başlatmak kayıt üretmez.

2.5 Worker tarafı appsettings.json

Worker'ın kendi dosyası kısadır:

Anahtar	Ne işe yarar
WorkerApi:BaseUrl	API adresi. Worker durum bilgisini buraya bildirir.
WorkerApi:Key	API tarafındaki Workers:ApiKey ile aynı olmalıdır.
Serilog:MinimumLevel	Günlük ayrıntı seviyesi.

İki anahtar birbirini tutmazsa worker açılışta yapılandırmasını API'den alamaz; 3 saniye arayla 10 denemeden sonra durur ve hiçbir iş çalışmaz. Arayüzde worker "çevrimdışı" görünür. Worker uygulama veritabanına kendi hesabıyla bağlanacaksa bu dosyada ConnectionStrings:Worker değeri (ya da ConnectionStrings__Worker ortam değişkeni) verilir; boşsa bağlantı dizesi API'den gelir.

2.6 İlk yönetici ve ilk giriş

Kurulumda hiç kullanıcı yoksa tek bir yönetici hesabı oluşturulur:

Alan	Değer
Kullanıcı adı	admin
Başlangıç şifresi	admin123
Rol	SystemManager (35)

Sistem ilk girişte bu şifreyi değiştirmeye zorlar: parola değiştirilene kadar oturum yalnız parola değiştirme işlemine izin verir, başka hiçbir istek çalışmaz. Kontrol sunucu tarafındadır, arayüz atlansa bile geçerlidir. Bu hesap üretim kopyasında tek başına gelir; başka hiçbir örnek kullanıcı oluşturulmaz.

Yerel hesaplar (admin dahil) giriş ekranına yalnız kullanıcı adıyla girer: admin. KURUM\admin ya da admin@kurum.com gibi alan adlı ya da e-posta sonekli yazımda şifre denenmez ve "yalnız kullanıcı adıyla girin" mesajı çıkar; bu deneme hatalı giriş sayılmaz ve hesabı kilitlemez. Alan adı ve sonek yalnız dizin (LDAP) hesaplarında kullanılır ve orada Ldap:Domain ile Ldap:UpnSuffix ayarlarına göre denetlenir.

2.7 Kurulum doğrulama kontrol listesi

Aşağıdakilerin hepsi sağlanıyorsa kurulum başarılıdır:

- [] API adresine tarayıcıdan erişiliyor ve giriş ekranı açılıyor.
- [] admin hesabıyla giriş yapılabiliyor ve şifre değiştirildi.
- [] Ayarlar > Lisans ekranında lisans durumu geçerli görünüyor.

[] Ayarlar > Sunucular ekranında en az bir sunucu tanımlı ve bağlantı testi başarılı.

[] Ayarlar > Tanılama ekranındaki kontroller yeşil.

[] Worker servisi çalışıyor ve arayüzde çevrimiçi görünüyor.

[] Test amaçlı bir talep açılıp onaylanabiliyor.

[] Denetim Kaydı ekranında bu işlemlerin kaydı görünüyor.

2.8 Sık karşılaşılan kurulum hataları

Belirti	Olası sebep	Çözüm
API açılmıyor, günlükte bağlantı hatası var	ConnectionStrings:Default yanlış veya veritabanı yok	Bağlantı metnini ve veritabanı erişimini kontrol edin.
Ekranlar açılıyor ama her istek yetkisiz dönüyor	Jwt:SigningKey değiştirilmiş, eski oturum açık	Çıkış yapıp yeniden giriş yapın.
Web arayüzü API'ye erişemiyor	AllowedOrigins içinde arayüz adresi yok	Arayüz adresini listeye ekleyin ve API'yi yeniden başlatın.
Yazma işlemleri 402 hatası veriyor	Lisans süresi dolmuş veya geçersiz	Geçerli lisans dosyası yükleyin. Ayrıntı: Bölüm 3.6.
E-posta gitmiyor	Mail:Enabled false veya DevMode true	Ayarları düzeltin, Bildirim Kayıtları ekranından sonucu izleyin.
Zamanlanmış talep çalışmıyor	Worker durmuş veya MainWorkEnabled false	Servisi başlatın, bayrağı true yapın.
Sorgu sonucu dosyası oluşmuyor	QueryResult:OutputPath yok veya yazma yetkisi yok	Klasörü oluşturun, servis hesabına yazma yetkisi verin.
Sunucu şifresi çözülüyor hatası	Security:ServerPasswordKey değişmiş	Eski anahtarı geri koyun veya sunucu şifrelerini yeniden girin.

Bölüm 3. Lisans

3.1 Lisans dosyası nedir

Lisans, .scglicense uzantılı imzalı bir dosyadır. İçinde müşteri adı, geçerlilik tarihleri, açık modüller, izin verilen sunucu sayısı ve izin verilen veritabanı türleri bulunur.

Dosya dijital imzalıdır. İmza, License:PublicKeyPem ayarındaki açık anahtar ile doğrulanır. İçeriği elle değiştiren bir dosya imza doğrulamasından geçmez ve geçersiz sayılır.

3.2 Lisans içeriği

Alan	Ne işe yarar	Boş bırakılırsa
CustomerName	Müşteri adı. Arayüzde gösterilir.	-
Edition	Sürüm adı. Bilgi amaçlıdır.	Core
MaxInstances	İzin verilen en fazla yönetilen sunucu sayısı. Yalnız aktif sunucular sayılır; lisansla üretim dışı sunucular ücretsiz işaretliyse (varsayılan) yalnız Production ortamındaki aktif sunucular sayılır. Bkz. 3.4.	0 yazılırsa sınırsız
DatabaseTypes	İzin verilen hedef veritabanı türleri.	Boş liste = hepsi açık
Modules	Açık modüller.	Boş liste = hepsi açık
GracePeriodDays	Lisans bittikten sonra kaç gün daha çalışılabilir.	7
ValidFrom, ValidTo	Geçerlilik aralığı.	-
IssuedAt	Üretim tarihi.	-

Ürün tek bir biçimde satılır: bütün modüller açıktır. Fiyat, kapsama giren üretim veritabanı sunucusu sayısına bağlıdır; modüller ayrı ayrı satın alınmaz ve kullanıcı sayısı sınırsızdır. Lisans dosyasındaki modül listesi teknik bir alandır: boş bırakıldığında bütün modüller açık gelir, yani standart kurulumda bu alana dokunulmaz.

3.3 Modüller

Altı opsiyonel modül vardır. Çekirdek işlevler (talep açma, onay akışı, çalıştırma, denetim kaydı, kullanıcı ve rol yönetimi, LDAP girişi) modülden bağımsız her zaman açıktır.

Modül	Açıkken gelen özellikler	Kapalıyken ne olur
QueryGovernance	Sorgu sonucu talebi açma, hassas veri maskeleyme, şifreli sonuç teslimi, sonuç dosyası indirme.	Sorgu sonucu talebi kaydedilemez ve çalıştırılmaz, indirme düğmesi gizlenir.
Sandbox	Talebi test sunucusunda deneme.	Sandbox düğmesi gizlenir, sandbox komutu reddedilir.
RollbackRecovery	Otomatik geri alma betiği üretimi, sunucu bazında geri alma zorunluluğu, Oracle otomatik geri alma.	Geri alma üret düğmesi gizlenir. Ayrıca "Rollback Zorunlu" kuralı etkisizleşir: otomatik üretim yokken talep çalıştırmanın kilitlenmemesi için zorunluluk uygulanmaz. Sunucu tanımındaki bayrak görünmeye devam eder ama çalıştırmayı engellemez.
ScheduledExecution	Talebi ileri bir tarihe zamanlama, sunucu bazında otomatik çalıştırma.	Zamanla düğmesi gizlenir, onaydan sonra otomatik zamanlama yapılmaz.
ReleasePackages	Sürüm paketi oluşturma ve çalıştırma.	Sürüm paketi ekranındaki işlemler reddedilir.
InsightsReporting	Yönetim raporları ve Nesne Geçmişi ekranı.	Raporlar ve nesne geçmişi açılmaz.

Önemli ilke: Kapalı modülün geçmiş verisi okunabilir kalır. Örneğin sürüm paketi modülü kapatılırsa eski paketler listede görünmeye devam eder, yalnızca yeni işlem yapılamaz. Veri rehin alınmaz.

Modül kapalıyken ilgili düğme arayüzde gizlenir, gri gösterilmez. Bunun sebebi, kullanıcının yapamayacağı bir işlemi denemeye çalışıp hata mesajı almasının anlamsız olmasıdır.

3.4 Sunucu limiti

MaxInstances değeri, limite sayılan sunucuların sayısı ile karşılaştırılır. Yalnızca aktif sunucular sayılır; pasif sunucular sayılmaz. Lisansta üretim dışı sunucular ücretsiz işaretliyse yalnızca üretim ortamındaki aktif sunucular sayılır ve test, geliştirme, hazırlık ortamları sınırsızdır. Limit dolduğunda yeni sunucu eklenemez, mevcut sunucular çalışmaya devam eder.

Örnek: MaxInstances 3 iken limite sayılan üç sunucu varsa dördüncüyü ekleme denemesi hata verir. Bir sunucuyu pasife almak yer açar; silmek şart değildir. Pasif sunucu limite sayılmaz ama kullanılamaz da: yeni taleplerde seçilemez.

3.5 Veritabanı türlerinin lisanstan gelmesi

Sunucu tanımı ekranındaki veritabanı türü listesi lisanstan doldurulur. Lisansta DatabaseTypes boşsa üç tür de seçilebilir. Örneğin lisansta yalnızca SqlServer varsa:

- Yeni sunucu eklerken listede yalnızca SQL Server görünür.

- Daha önce eklenmiş bir Oracle sunucusu varsa o sunucuda çalıştırma, bağlantı testi ve sandbox işlemleri engellenir. Kayıt silinmez, yalnızca kullanılamaz.

3.6 Lisans durumları ve sistem davranışı

Durum	Anlamı	Sistem davranışı
Valid	Geçerli.	Her şey normal çalışır.
Trial	Deneme lisansı.	Her şey çalışır, tüm modüller açık kabul edilir.
Expiring	Bitişe ExpiryWarningDays günden az kaldı.	Her şey çalışır, arayüzde uyarı görünür.
GracePeriod	Süre doldu ama ek süre içinde.	Her şey çalışır, uyarı görünür.
Expired	Süre ve ek süre doldu.	Kısıtlı mod.
Invalid	İmza doğrulanamadı veya dosya bozuk.	Kısıtlı mod.
Missing / NoLicense	Lisans dosyası yok.	Kısıtlı mod.

Kısıtlı mod ne demektir: Tüm yazma işlemleri (POST, PUT, PATCH, DELETE) reddedilir ve 402 kodu ile "lisans geçersiz veya süresi dolmuş" hatası döner. İstisna üç uçtur: giriş işlemleri, lisans işlemleri ve API dokümantasyonu. Yani sisteme girip yeni lisans yükleyebilirsiniz, ama başka hiçbir kayıt oluşturamaz veya değiştiremezsiniz. Okuma işlemleri çalışmaya devam eder, mevcut verilerinizi görebilirsiniz.

3.7 Lisans yükleme adımları

1. Ayarlar ekranını açın.
2. Lisans sekmesine geçin. Bu sekmeyi görmek için rolünüzde lisans yönetimi yetkisi olmalıdır.
3. Mevcut durum kartında müşteri adı, bitiş tarihi ve kalan gün sayısı görünür.
4. Lisans dosyasını seçin veya içeriğini yapıştırın.
5. Kaydedin. Uygulama imzayı doğrular ve lisansı yeniden yükler.

Yükleme başarılıysa durum kartı hemen güncellenir. Uygulamayı yeniden başlatmak gerekmez.

3.8 Lisans hata mesajları

Mesaj	Sebebi	Çözüm
Lisans geçersiz veya süresi dolmuş	Kısıtlı modda yazma denemesi yapıldı	Geçerli lisans yükleyin.
İmza doğrulanamadı	Dosya değiştirilmiş veya başka bir kuruma ait	Doğru dosyayı tedarikçinizden isteyin.

Mesaj	Sebep	Çözüm
Sunucu limiti aşıldı	MaxInstances doldu	Kullanılmayan sunucu tanımını silin veya lisansı yükseltin.
Bu modül lisans kapsamında değil	Kapalı bir modülün işlemi çağrıldı	Modülü lisansınıza ekletin.

Bölüm 4. Roller, Yetkiler ve Hiyerarşi

4.1 Roller ve sayısal değerleri

Sistemde sekiz rol vardır. Rol kimlikleri beşer artar.

Kimlik (Id)	Rol adı	Hiyerarşi seviyesi	Kısa açıklama
0	NoAccess	0	Erişimi yok. Hesap açık ama hiçbir şey yapamaz.
5	Viewer	5	Yalnızca kontrol panelini görür.
10	Auditor	10	Denetçi. İzler, kanıt üretir ve doğrular. Değişiklik akışına giremez.
15	Requester	15	Talep açar.
20	RequestManager	20	Talep açar ve onaylar.
25	DbAdmin	25	Veritabanı yöneticisi. Çalıştırır ve tüm ayarları yönetir.
30	ChangeManager	30	Değişiklik yöneticisi. DbAdmin ile aynı yetkilere sahiptir, hiyerarşide üsttedir. Teknik taraftaki en üst onay seviyesidir; kurumun değişiklik kurulu (CAB) değildir.
35	SystemManager	35	Sistem yöneticisi. En üst seviye. Rol tanımı düzenlenemez.

Neden beşer artıyor: İleride iki rolün arasına yeni bir rol gerekirse aradaki boş sayılardan biri seçilir ve hiçbir kullanıcı kaydı kaydırılmaz. Ardışık numaralarda (4 ile 5 arasında) bu mümkün olmaz.

ChangeManager ile kurumun değişiklik kurulu (CAB) aynı şey değildir. CAB, kurumun ITSM sisteminde (ServiceNow, Jira gibi) bir değişikliğin yapıp yapılmayacağına ve ne zaman yapılacağına karar verir. Üründeki ChangeManager ise o değişikliği yapan betiği ve veriyi onaylar: onay politikalarında "en az şu rol onaylar" diye tanımlanan üst seviye adımlarda ve ürünün bazı yetki eşiklerinde kullanılır. Örnek: başkasının sorgu sonucu dosyasını indirebilmek için gereken en düşük rol (QrDownloadMinimumRole) ve sonucun gönderileceği e-posta adresini onaylayan rol (QrEmailApproverRole) kurulumda ChangeManager'dır.

Bu rol, CAB'ı yöneten kişiye değil, teknik tarafta son sözü söyleyecek kişiye verilir; çoğu kurumda bu DBA ekip lideridir. Kurum isterse CAB'ı yöneten kişiye de bu rol verilebilir; böylece yüksek riskli işlerde betiği de görür ve onaylar. Bu bir zorunluluk değildir.

4.2 Kimlik ile hiyerarşi ayrı kavramlardır

Bu kılavuzun teknik ekiplerce en dikkatli okunması gereken maddesidir.

Her rolün iki sayısı vardır:

- Kimlik (Id): Kullanıcı kayıtlarında saklanan numara.
- Seviye (Level): Hiyerarşide nerede durduğunu belirten numara.

Bu ikisi bugün aynı değerlerdedir, ancak aynı kavram değildir. Bir rol kimlik olarak listenin sonuna eklenip hiyerarşide ortaya yerleştirilebilir. Denetçi rolü tam olarak bu sebeple ayrı yönetilir: izleme yetkisi Viewer'dan genişler, ancak değişiklik akışında hiçbir yetkisi yoktur.

Yetki karşılaştırması rolün kimlik numarasına değil, hiyerarşideki seviyesine bakar. Bu ayrım sayesinde listeye sonradan eklenen bir rol, sırf numarası büyük diye kendiliğinden yetki kazanmaz.

Tanımsız bir rol değeri gelirse seviye 0 kabul edilir. Yani tanımsız rol yetki kazanmaz.

4.3 Denetçi rolünün özel durumu

Denetçi onay akışında onaylayan olarak seçilemez. Denetleyen kişi onaylayan konumuna geçerse görevler ayrılığı bozulur, çünkü kendi onayladığı işi denetlemiş olur.

Denetçinin yapabildikleri: raporları görmek, kontrol panelini görmek, denetim kayıtlarını görmek, tüm talepleri görmek, bildirim kayıtlarını görmek, denetim dosyası dışa aktarmak.

Denetçinin yapamadıkları: talep açmak, onaylamak, çalıştırmak, sandbox çalıştırmak, herhangi bir ayarı değiştirmek, sürüm paketi yönetmek.

4.4 Rol yetki matrisi

Aşağıdaki tablo varsayılan rol tanımlarını gösterir. Roller ekranından değiştirilebilir; SystemManager rolü düzenlenemez.

Yetki	NoAccess	Viewer	Auditor	Requester	RequestManager	DbAdmin	ChangeManager	SystemManager
Talep ekleme	-	-	-	Evet	Evet	Evet	Evet	Evet
Çalıştırma	-	-	-	-	-	Evet	Evet	Evet
Onaylama	-	-	-	-	Evet	Evet	Evet	Evet
Sandbox	-	-	-	-	-	Evet	Evet	Evet

Yetki	NoAccess	Viewer	Auditor	Requester	RequestManager	DbAdmin	ChangeManager	SystemManager
Rapor görme	-	-	Evet	-	Evet	Evet	Evet	Evet
Kontrol paneli	-	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Denetim kaydı görme	-	-	Evet	-	-	Evet	Evet	Evet
Sürüm paketi yönetimi	-	-	-	-	-	Evet	Evet	Evet
Tüm talepleri görme	-	-	Evet	Evet	Evet	Evet	Evet	Evet
Sunucu yönetimi	-	-	-	-	-	Evet	Evet	Evet
Kullanıcı yönetimi	-	-	-	-	-	Evet	Evet	Evet
Rol yönetimi	-	-	-	-	-	Evet	Evet	Evet
Parametre yönetimi	-	-	-	-	-	Evet	Evet	Evet
Onay politikası yönetimi	-	-	-	-	-	Evet	Evet	Evet
SQL standardı yönetimi	-	-	-	-	-	Evet	Evet	Evet
Kritik nesne yönetimi	-	-	-	-	-	Evet	Evet	Evet
ITSM bilet yönetimi	-	-	-	-	-	Evet	Evet	Evet
Hassas kolon yönetimi	-	-	-	-	-	Evet	Evet	Evet

Yetki	NoAccess	Viewer	Auditor	Requester	RequestManager	DbAdmin	ChangeManager	SystemManager
Hassas desen yönetimi	-	-	-	-	-	Evet	Evet	Evet
E-posta kaynağı yönetimi	-	-	-	-	-	Evet	Evet	Evet
Bakım yönetimi	-	-	-	-	-	Evet	Evet	Evet
Bildirim kayıtları görme	-	-	Evet	-	-	Evet	Evet	Evet
Lisans yönetimi	-	-	-	-	-	Evet	Evet	Evet
Tanımlama kullanımı	-	-	-	-	-	Evet	Evet	Evet
Denetim dosyası dışa aktarma	-	-	Evet	-	-	Evet	Evet	Evet

Talep ekleme yetkisi olan roller aynı zamanda sorgu sonucu talebi de açabilir.

4.5 Yetki anahtarları

Her yetki bir anahtar ile temsil edilir ve giriş jetonuna yazılır. Ekranların ve düğmelerin görünürlüğü bu anahtarlara bakar.

Anahtar	Açtığı işlem
cr.add	Talep ve sorgu sonucu talebi açma
qr.add	Sorgu sonucu talebi açma
cr.execute	Talep çalıştırma
cr.sandbox	Sandbox çalıştırma
cr.approve	Onaylama, reddetme, zamanlama, manuel işaretleme
cr.seeall	Başkalarının taleplerini görme
report.view	Raporlar ekranı

Anahtar	Açtığı işlem
dashboard.view	Kontrol paneli
audit.view	Denetim kaydı ekranı
audit.evidenceexport	Denetim dosyası dışa aktarma
rp.manage	Sürüm paketi yönetimi
settings.servers ve diğer settings.* anahtarları	İlgili ayar sekmesi

4.6 Arayüz gizlemesi güvenlik değildir

Bir düğmenin gizlenmesi kullanıcının o işlemi yapmasını engellemez. Web arayüzü tarayıcıda çalışır ve kullanıcı isterse doğrudan API'ye istek gönderebilir.

Bu yüzden her işlem iki kere kontrol edilir:

1. Arayüz, düğmeyi gösterip göstermeyeceğine karar verir.
2. API, isteği aldığı anda aynı kuralı bağımsız olarak tekrar uygular.

İkinci kontrol asıl güvenliktir. Birinci kontrol yalnızca kullanıcı deneyimi içindir.

4.7 Kullanıcı yaşam döngüsü

İşlem	Davranış
Kullanıcı ekleme	Kullanıcı adı ve e-posta benzersiz olmalıdır. Yerel ve dizin (LDAP) hesaplarında kullanıcı adı kısa addır: alan adı (KURUM\ali) ya da e-posta soneki (ali@kurum.com) içeremez, çünkü giriş ekranı yazılan adı kısa ada indirerek arar ve bu biçimde kaydedilen hesap hiç giriş yapamaz. Ekran bu durumda kısa adı önerir. Kurum hesabında (SSO) ad kimlik sisteminden geldiği gibi kalır (örnek: ali@kurum.com). Aynı nedenle adı alan adı ya da sonek içeren bir kurum hesabı yerel ya da dizin tipine çevrilemez.
Kullanıcı silme	Kayıt fiziksel olarak silinmez, silindi olarak işaretlenir (yumuşak silme). Geçmiş taleplerdeki adı korunur.
Silinmiş kullanıcı ile aynı adda ekleme	Yeni kayıt oluşturulmaz, eski kayıt canlandırılır. Böylece aynı kişi aynı geçmişe geri döner. Ekran kaydetmeden önce uyarır ve kapatılmış hesabın e-postasını gösterir: o hesabın geçmişteki talepleri, onayları ve denetim kayıtları canlandırılan hesaba ait görünür. Yönetici "Aynı kişi, geri aç" demeden hesap geri açılmaz; farklı bir kişiye başka bir kullanıcı adı seçilir. Dört göz onayı açıksa uyarı onaya gönderilmeden önce çıkar. Geri açma denetim izine User.Reactivate olayıyla yazılır.

İşlem	Davranış
Son sistem yöneticisini silme	Engellenir. Sistemde en az bir sistem yöneticisi kalmalıdır.
Kendini silme	Engellenir.
Dört göz kilitlenme kapısı	Ayar onayı açıkken, bir ekranın yetkisine sahip son ikinci kişiyi silmek engellenir. Aksi halde o ekrandaki değişiklikler hiç onaylanamaz hale gelirdi.
Hesap kilidi	Ardışık hatalı şifre ya da iki adımlı doğrulama kodu denemesi sonrası hesap geçici kilitlenir. Yönetici elle de açabilir.

Yetki değişikliği ne zaman etkili olur

Bir kullanıcının rolü değiştiğinde, hesabı kapatıldığında ya da rolün yetki matrisi güncellendiğinde değişiklik beklemeden etkili olur. Bunu iki mekanizma birlikte sağlar.

1. Yüksek etkili işlemlerde yetki veritabanından okunur. Aşağıdaki işlemlerde yetki, kullanıcının elindeki oturum anahtarından değil doğrudan veritabanından doğrulanır:

- Talebi çalıştırma
- Çalıştırmayı zamanlama
- Talep onaylama
- Ayar değişikliğini onaylama ve reddetme

Yetkisi çekilmiş ya da hesabı kapatılmış bir kullanıcı, oturumu hâlâ açık görünse bile bu işlemleri yapamaz.

2. Oturum kapatılır. Rol değiştiğinde, hesap kapatıldığında, kimlik doğrulama tipi değiştiğinde, rolün yetki matrisi güncellendiğinde veya şifre sıfırlandığında (yönetici tarafından ya da e-postadaki bağlantıyla) etkilenen kullanıcıların oturumları hemen kapanır: açık pencere bir sonraki tıklamada giriş ekranına döner. Bunu her kullanıcı için tutulan bir oturum sürümü sağlar; oturum anahtarı üretildiği andaki sürümü taşır ve her istekte veritabanıyla karşılaştırılır. Kullanıcı kendi şifresini değiştirdiğinde diğer bütün oturumları kapanır, şifreyi değiştirdiği oturum kesintisiz devam eder.

İptal denetim izine de yazılır: kullanıcı bazlı iptal User.SessionsRevoked, rol bazlı iptal Role.SessionsRevoked olayıdır. Kayıt, iptal sebebini ve kaç oturumun kapatıldığını taşır.

Rol ya da rol yetkisi değiştiğinde kullanıcı yeniden giriş yapar ve yeni yetkileriyle devam eder. Böylece yetkinin hem çekilmesi hem verilmesi hemen geçerli olur; kullanıcı eski yetkilerini taşıyan bir oturumla çalışmaya devam edemez.

4.8 LDAP kullanıcıları ile yerel kullanıcıların farkı

Konu	Yerel kullanıcı	LDAP kullanıcısı
Şifre nerede	SQL Change Guard veritabanında, BCrypt özeti olarak; geri çözülemez.	Kurum dizininde. Uygulama şifreyi saklamaz.
Şifre değiştirme	Uygulama içinden.	Kurum dizininden.
Rol	Uygulama içinden atanır.	Ldap:RoleSource Manual iken ilk açılışta izin grubundan gelir (eşlenen grup yoksa erişimsiz), sonrasında uygulama içinden atanır. Directory iken izin grubundan gelir ve her girişte ve eşitlemede yeniden hesaplanır.
Hesap kilidi	Uygulama yönetir.	Uygulama yanlış izin şifrelerini de sayar ve hesabı kilitler. Uygulamanın eşiği dizininkinden küçük tutulmalıdır.
İki adımlı doğrulama	Uygulama içinden kurulur; şifreden sonra kod istenir.	Uygulama içinden kurulur; izin şifresinden sonra kod istenir.
Hesabın açılması	Yönetici Kullanıcılar ekranından açar.	Yönetici açar ya da Auth:Mode Ldap iken ilk girişte açılır. Dizinde e-postası olmayan kişiye hesap açılmaz.
Kişinin tanınması	Kullanıcı adıyla.	Dizindeki değişmeyen kimlikle (objectGUID ya da entryUUID). Kullanıcı adı değişse de kişi kendi hesabıyla girer; aynı adla yeni biri eski hesaba geçemez.
İşten ayrılma	Yönetici hesabı kapatır.	Dizinde kapatılan ya da silinen kişinin erişimi izin eşitlemesinde kapanır ve açık oturumları biter.

Grup ile rol eşlemesi: Dizin hesaplarının eşlemeleri kurum hesabı eşlemeleriyle aynı tabloda, Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında "Dizin (LDAP)" sağlayıcısıyla tanımlanır. Değer grubun dizindeki tam adıdır, örnek CN=DBA-Ekibi,OU=Gruplar,DC=kurum,DC=local; boşluk ve büyük küçük harf farkı önemli değildir. Birden fazla grup eşleşirse en yüksek rol verilir. SystemManager eşlemeyle hiçbir durumda verilmez. Grubun değerini bilmiyorsanız kişi bir kez girmeyi denesin; Denetim Günlükleri'ndeki LdapLoginDenied kaydı dizinden gelen grupları (ReceivedGroups) listeler.

Rolün kaynağı izin iken (Ldap:RoleSource = Directory): Kişi gruptan çıkarılırsa bir sonraki girişinde ya da eşitlemede yeni rolünü alır ve eski rolüyle açık oturumları hemen kapanır. Grup bilgisi okunamazsa var olan rol düşürülmez, giriş reddedilir. Kullanıcılar ekranında rol elle yalnız

SystemManager yapılabilir ya da SystemManager rolü geri alınabilir. Bir kişiyi dizin ekibini beklemeden üründe hemen durdurmak gerekirse Kullanıcılar ekranından hesabı silin: açık oturumları hemen kapanır ve dizin şifresi doğru olsa da giremez. Hesap gerekirse aynı adla yeniden eklenir; geçmiş kayıtlar korunur.

Dizin eşitlemesi: Ldap:Sync:Enabled açıkken Worker, dizin hesaplarını servis hesabıyla dizinde arar. Bulunamayan ya da dizinde kapalı olan hesap erişimsiz bırakılır ve oturumları kapanır; e-posta dizinden güncellenir. Toplu kapatma güvenlik sınırını aşarsa ya da dizine ulaşamazsa hiçbir değişiklik yapılmaz. Sistemi yönetecek son SystemManager hesabı kapatılmaz. Eşitleme Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranındaki Şimdi eşitle düğmesiyle de çalıştırılabilir; aynı ekrandaki Bağlantıyı test et düğmesi dizine ulaşıp ulaşılamadığını gösterir.

Hatalı şifre: Hesabı olan kişide yanlış dizin şifresi yerel hesaptaki gibi sayılır ve hesap kilitlenir. Üründe hesabı olmayan bir ad için de aynı sayıda hatalı denemeden sonra aynı süre dizine gidilmez; var olan ve olmayan adlar aynı cevabı alır. Dizine ulaşamazsa sayaç artmaz. SystemManager hesabı ürün tarafından kalıcı olarak kilitlenmez; bu hesaplarda da aynı sınır bellekte uygulanır, böylece yöneticinin dizin şifresi ürün ekranından sınırsız denenemez.

Denetim izi: Dizin girişiyle açılan hesap User.CreatedFromDirectory, dizinden güncellenen rol ya da e-posta User.SyncedFromDirectory, eşitlemede erişimi kapatılan hesap User.DisabledInDirectory, kural gereği ret LdapLoginDenied, eşitleme sonucu Ldap.SyncCompleted ya da Ldap.SyncAborted olarak yazılır.

Kurum hesabıyla (SSO) giriş yapan kullanıcılar

Kurum hesabıyla giriş açıkken giriş ekranında şifre alanlarının altında "... ile giriş yap" düğmesi görünür. Kullanıcı düğmeye basar, kurumun giriş sayfasında kendi kurum hesabıyla girer ve ürüne geri döner. Kullanıcılar ekranında bu hesapların kimlik doğrulama tipi Kurum hesabı olarak görünür.

Konu	Kurum hesabı kullanıcısı
Şifre nerede	Kurumun kimlik sisteminde. Ürün şifreyi hiç görmez ve saklamaz.
Şifre değiştirme ve sıfırlama	Kurumun kimlik sisteminden. Üründe şifre sıfırlama düğmesi bu hesaplarda yoktur.
Rol	Kimlik sağlayıcısındaki gruptan, Grup ile rol eşlemesi tablosuna göre verilir. Birden fazla grup eşleşirse en yüksek rol verilir.

Konu	Kurum hesabı kullanıcısı
İki adımlı doğrulama	Kurumun kimlik sisteminde yapılır. Ürün içinden kurulmaz; ürünün kaydolma zorunluluğu bu hesapları etkilemez.
Hesabı kapatma	Kurumun kimlik sisteminde kapatılan hesap yeniden giremez. Açık oturumu en geç Sso:MaxSessionHours sonunda biter.
Şifre ekranından giriş	Yapılamaz. Şifre ekranına kullanıcı adı yazılırsa "Bu hesap kurum hesabıyla giriş yapar" mesajı gelir ve hatalı giriş sayacı artmaz.

Kişinin bulunması: Ürün kişiyi kimlik sağlayıcısının verdiği değişmeyen kimlikle bulur, e-posta ya da kullanıcı adıyla değil. İlk girişte kişi, aynı kullanıcı adıyla önceden açılmış bir Kurum hesabı tipindeki hesaba bağlanır. Yerel ya da LDAP tipindeki bir hesaba kendiliğinden bağlanmaz; bu durumda giriş reddedilir ve yöneticinin hesabın tipini Kurum hesabı yapması gerekir. Böylece kimlik sağlayıcısında aynı adı alan biri üründeki yerel yönetici hesabını ele geçiremez.

Grup ile rol eşlemesi: Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranında her satır bir kimlik sağlayıcısı, bir grup (ya da uygulama rolü) değeri ve bir rolden oluşur. Değer kimlik sağlayıcısının gönderdiği metinle aynı yazılır; büyük küçük harf farkı gözetilmez. Hiçbir eşlemeye uymayan kişi erişim almaz. Kimlik sağlayıcısının hangi değeri gönderdiğini bilmiyorsanız kişi bir kez kurum hesabıyla girmeyi denesin: giriş reddedilir ve Denetim Günlükleri'ndeki SsoLoginDenied kaydında gelen grup değerleri (ReceivedGroups) yazar. Eşlemeye bu değer aynen yazılır. SystemManager rolü eşlemeyle hiçbir durumda verilmez; yalnız Kullanıcılar ekranından elle verilir. Eşlemeyi değiştirmek için Kullanıcılar ekranının yetkisi gerekir; ayar değişikliği onayı açıksa değişiklik ikinci bir kişinin onayından geçer. Rolün kaynağı ldp iken bir eşleme değiştirildiğinde ya da silindiğinde, o kimlik sağlayıcısına bağlı ve eşlemenin rolündeki kişilerin açık oturumları hemen kapanır; kişi yeniden girdiğinde yeni eşlemeye göre rol alır. Böylece silinen bir eşlemenin verdiği yetkiyle çalışmaya devam edilemez.

Rolün kaynağı ldp iken (Sso:RoleSource) rol her girişte yeniden hesaplanır. Kişi kurumda gruptan çıkarılırsa bir sonraki girişinde yeni rolünü alır ve eski rolüyle açık oturumları hemen kapanır. Bu modda Kullanıcılar ekranında kurum hesabının rolü elle yalnız SystemManager yapılabilir ya da SystemManager rolünden alınabilir. Kimlik sağlayıcısı grup bilgisini hiç göndermezse var olan hesabın rolü düşürülmez, giriş reddedilir; yeni kişinin hesabı açılmaz.

Bağlı kimlikler: Kullanıcılar ekranında kurum hesabının düzenleme penceresi, bağlı kurum kimliklerini (kimlik sağlayıcısı, değişmeyen kimlik, son giriş) gösterir. Bağlı kaldır düğmesi bağlı siler ve açık oturumları kapatır. Kullanıcı bir sonraki kurum hesabıyla girişinde yeniden bağlanır.

Acil durum hesabı: Kimlik sağlayıcısına ulaşılamazsa ürüne girilebilmesi için en az bir yerel, şifreli ve SystemManager rolünde hesap tutulur. Auth:LocalLoginAllowedUsers listesine yalnız bu hesaplar yazılır; diğer yerel hesaplar şifre ekranından giremez. Acil durum hesabının her girişi LoginBreakGlass olayı olarak denetim izine yazılır ve SOC'a alarm olarak gider.

Acil durum hesabının kullanımı: Her SystemManager bu listeye yazılmaz. Günlük yönetim işini yapan yöneticiler kurum hesabıyla girer; onlara SystemManager rolü Kullanıcılar ekranından elle verilir. Listeye yalnız acil durum için ayrılmış bir ya da iki yerel SystemManager hesabı yazılır.

Önerilen düzen:

Hesap	Tipi ve rolü	Listede mi	Kim kullanır
acil.yonetici	Yerel, SystemManager	Evet	Günlük işte kimse kullanmaz; yalnız kimlik sağlayıcısı çalışmazken
acil.yonetici2	Yerel, SystemManager	Evet	Yedek; ilk hesap kilitlenirse ya da şifresi kaybolursa
ahmet.yilmaz	Kurum hesabı, SystemManager (elle verilmiş)	Hayır	Günlük yönetim işi
Diğer kullanıcılar	Kurum hesabı	Hayır	Günlük kullanım

Bu düzende yapılandırma dosyasındaki değer şöyledir: "Auth": { "LocalLoginAllowedUsers": ["acil.yonetici", "acil.yonetici2"] }. Liste yapılandırma dosyasında durur; değişiklik API yeniden başlatılınca geçerli olur ve Sso.ConfigurationChanged olayıyla denetim izine yazılır.

Acil durum hesabı için önerilen kurallar:

1. Hesap bir kişiye değil göreve aittir. Adı kişi adı olmaz (acil.yonetici gibi) ve günlük işte kullanılmaz.
2. Şifre uzun ve karmaşıktır. Kurumun kasasında ya da şifre kasası uygulamasında saklanır; iki parçaya bölünüp iki ayrı kişide tutulabilir. Her kullanımdan sonra değiştirilir.
3. Her giriş LoginBreakGlass olarak denetim izine yazılır; SIEM bağlıysa güvenlik ekibine alarm gider. Güvenlik ekibi o anda gerçekten bir kesinti olup olmadığını doğrular.
4. Hesabın çalıştığı belirli aralıklarla (örnek üç ayda bir) denetlenir. Bu deneme de denetim izine yazıldığı için denetimde kanıt olur.

5. Hesap sayısı az tutulur. Her yerel hesap kurumun kimlik politikasının (iki adımlı doğrulama, hesap kapatma) dışında kalır.

Kurulumla gelen admin hesabı: Acil durum hesabı olarak kullanılacaksa listede kalır ve şifresi yukarıdaki kurallarla saklanır. Kullanılmayacaksa önce acil.yonetici gibi yeni yerel SystemManager hesapları açılır ve listeye yazılır; admin listeden ancak bundan sonra çıkarılır. Listedeki yerel bir SystemManager kalmazsa kimlik sağlayıcısı çalışmadığında hiçbir yönetici giremez; Kurulum Kontrolü'ndeki "Acil durum hesabı" satırı bu durumda uyarı verir.

Başka yerel hesaplar: Kimlik sağlayıcısında kaydı olmayan kişiler (örnek dış danışman) ya da geçiş dönemi için yerel bir hesap geçici olarak listeye eklenebilir ve iş bitince listeden çıkarılır. Kurum hesabı olan kişilere "her ihtimale karşı" ayrıca yerel hesap açılmaz: kişinin iki kimliği olur ve işten ayrıldığında kurum hesabı kapatılsa da yerel hesabı açık kalır. Kimlik sağlayıcısı çalışmazken bir kişinin işi aksamamalıysa yönetici acil durum hesabıyla girer ve o kişiyi geçici olarak yerel hesaba çeker (Kişi kurum hesabıyla ya da dizinle giremiyorsa bölümü).

Denetim izi: Başarılı giriş SsoLoginSuccess, teknik doğrulama hatası SsoLoginFailed, kural gereği ret (hesap bağlı değil, rol eşlenmedi, MFA bildirilmedi gibi) SsoLoginDenied olarak yazılır. Hesabın kimlik sağlayıcısıyla açılması User.CreatedFromIdp, rolünün ya da e-postasının güncellenmesi User.SyncedFromIdp, kimlik bağı User.ExternalIdentityLinked ve User.ExternalIdentityUnlinked, eşleme değişiklikleri SsoRoleMapping.Create, SsoRoleMapping.Update ve SsoRoleMapping.Delete olaylarıdır.

Oturum numarası: Her başarılı giriş bir oturum numarası alır. Numara giriş kaydına (LoginSuccess, MfaSuccess, SsoLoginSuccess, LoginBreakGlass) ve oturumun kimlik bilgisine yazılır: parolanın doğrulandığı yer, kimlik sağlayıcısının adı, MFA ve acil durum girişi. Bu bilgi oturum boyunca değişmez, yenilemede de taşınır. LDAP'ta kişi "KURUM\ayse" ya da "ayse@kurum.local" yazarak girse de giriş kaydı hesabın kayıtlı adıyla (ayse) yazılır. Talep üzerindeki kararlar bu bilgiyi karar anında dondurur (Bölüm 18.8).

Rolün kaynağı: kurum hesabı (SSO) ve dizin (LDAP) birlikte

Kurum hesabında Sso:RoleSource, dizinde Ldap:RoleSource aynı kuralla çalışır. Gruptan modu (Idp, Directory) rolü her girişte gruptan hesaplar. Elle modu (Manual) grubu yalnız hesap ilk açılırken kullanır; sonrasında rolü yönetici Kullanıcılar ekranından yönetir.

Kişi ilk kez girdiğinde:

Durum	SSO Idp	LDAP Directory	SSO Manual	LDAP Manual
Eşlenmiş grubu var	O rolle açılır, girer	Aynı	O rolle açılır, girer	Aynı
Eşlenmiş grubu yok	Hesap açılmaz	Aynı	Erişimsiz (NoAccess) açılır; rolü yönetici verir	Aynı
Gruplar okunamadı	Hesap açılmaz	Hesap açılmaz; kişi tekrar dener	Erişimsiz açılır	Hesap açılmaz; kişi tekrar dener

Hesap açıldıktan sonra gruptan modunda kişi gruptan çıkarılınca bir sonraki girişte rolü düşer ve açık oturumları kapanır; rol Kullanıcılar ekranında kilitlidir (yalnız SystemManager verilir geri alınabilir). Elle modunda grup değişikliği rolü değiştirmez ve yönetici rolü serbestçe değiştirir.

Gruplar okunamazsa iki elle modun farkı: dizinde ürün grupları kendisi okur ve okuma hatasını kesin olarak tanır; bu yüzden hesabı açmaz, kişi tekrar dener ve izin düzelince doğru rolle açılır. Kurum hesabında gruplar kimlik sisteminden hazır gelir; grup bilgisi hiç gelmezse ürün bunun "kişinin grubu yok" mu yoksa bir kurulum eksikliği mi olduğunu ayırt edemez ve kişiyi grubu yok sayar. İki davranış da kimseye fazladan yetki vermez. Entra ID'de çok gruplu kişiler için grup yerine uygulama rolü kullanılması önerilir.

Kişi kurum hesabıyla ya da dizinle giremiyorsa

Önce nedeni bulun: Denetim Günlükleri'nde SsoLoginDenied, SsoLoginFailed ya da LdapLoginDenied kaydı nedeni ve gelen grupları yazar.

Durum	Kalıcı çözüm	Yerel hesap geçici çözüm olarak uygun mu?
Kimlik sistemi ya da izin çalışmıyor	Kimlik sistemini ya da dizini düzeltin; bu sırada yöneticiler acil durum hesabıyla girer	Yalnız işi aksamaması gereken birkaç kişi için, geçici
Kişinin grubu bir role eşlenmemiş (gruptan modu)	Kişiyi doğru gruba ekleyin ya da grubu eşleyin	Önerilmez: rol grubun dışında verilmiş olur
Gruplar okunamıyor	Dizin sorununu giderin; Entra ID'de uygulama rolü kullanın	Sorun giderilene kadar geçici

Durum	Kalıcı çözüm	Yerel hesap geçici çözüm olarak uygun mu?
Kişi kimlik sisteminde ya da dizinde kapatılmış veya kilitlenmiş	Kurumun kararıdır; kimlik ekibiyle konuşun	Hayır: yerel hesap bu kararı deler
"Kurum hesabına bağlı olmayan bir hesap var" mesajı	Hesabın tipini Kurum hesabı yapın	Gerek yok
Kurum hesabının iki adımlı doğrulaması kayboldu	Kimlik sisteminde sıfırlatın	Hayır
Dizin hesabının ürün MFA'sı kayboldu	Kullanıcılar > MFA Sıfırla	Gerek yok
Hesap üründe hatalı şifre yüzünden kilitli	Süre dolar ya da yönetici kilidi açar	Gerek yok

Kurum ya da dizin hesabını yerel hesaba çekmek için bağı önce kaldırmanız gerekmez: Kullanıcılar ekranında kimlik doğrulama tipini Yerel yapın ve kaydedin (kişinin açık oturumları kapanır), sonra Şifre Sıfırla ile geçici bir şifre verin. Kişi ilk girişte şifresini değiştirir; ürünün iki adımlı doğrulaması zorunluysa kurar. Auth:LocalLoginAllowedUsers doluysa kişi listeye eklenmeden şifreyle giremez. Kimlik sistemiyle bağ kayıta kalır ama kullanılmaz; geçici geçişte bırakın, kalıcı geçişte Bağlı kaldır ile silebilirsiniz. Kullanıcı adı alan adı ya da e-posta biçimindeyse (örnek ayse@kurum.com) hesap yerel tipe çevrilemez; kişiye kısa adla ve farklı bir e-postayla ayrı bir yerel hesap açılır.

Yerel hesabın sonuçları: Yönetici tipi değiştirirken rolü de değiştirebilir, yani rol grubun dışında verilebilir. Kimlik sisteminde ya da dizinde yapılan kapatma yerel hesabı kapatmaz ve dizin eşitlemesi yerel hesaplara dokunmaz; kişi ayrılırsa yerel hesap elle kapatılmalıdır. Şifre ve iki adımlı doğrulama üründe tutulur. Ayrı yerel hesap açılırsa kişinin iki hesabı olur, geçmişi bölünür ve görevler ayrılığı iki hesap arasında çalışmaz; bu yol yalnız çevirme mümkün değilse kullanılmalı ve iş bitince yerel hesap silinmelidir.

Bunu görünür kılan kontroller: tip ve rol değişikliği dört göz onayı açıksa onaya düşer ve denetim izine User.Update olarak eski ve yeni değerlerle yazılır; kurum hesabıyla giriş açıkken her yerel giriş LoginBreakGlass olarak yazılır ve SIEM açıksa alarm olur; Kurulum Kontrolü'ndeki "Şifre ile giriş yalnızca acil durum hesaplarında" satırı izin listesi boşken uyarı verir; User Access Changes raporu değişikliği listeler. Sorun giderilince tipi yeniden Kurum hesabı ya da LDAP yapın: ürün

yerel şifreyi siler, kişi bir sonraki girişini eskisi gibi yapar ve gruptan modunda rolü yeniden gruptan hesaplanır.

SystemManager kurum hesabıyla ya da dizinle girebilir. SystemManager rolü eşlemeyle hiçbir zaman verilmez, çünkü bir gruba üye eklemek ürünün tam yöneticisini yaratmamalıdır; ama yönetici bir kurum ya da dizin hesabına Kullanıcılar ekranından elle SystemManager verebilir. Elle verilen SystemManager'a girişler ve eşitleme dokunmaz. Kimlik sistemi ya da dizin çökerse kimse giremeyeceği için en az bir yerel SystemManager (acil durum hesabı) her zaman bulunmalıdır; Kurulum Kontrolü'ndeki "Acil durum hesabı" satırı bunu denetler.

4.9 Şifre politikası ve BCrypt

Hash nedir

Bir metni geri döndürülemez biçimde sabit uzunlukta bir değere çeviren işleme özet (hash) denir. Şifreler veritabanında düz metin olarak tutulmaz, özetleri tutulur. Kullanıcı giriş yaptığında girdiği şifrenin özeti hesaplanır ve kayıttaki özetle karşılaştırılır.

Veritabanını ele geçiren biri özetleri görür, şifreleri göremez.

Salt nedir

Aynı şifreyi kullanan iki kullanıcının özeti aynı çıkarsa, saldırgan bir tanesini çözdüğünde diğerini de çözer. Bunu engellemek için her şifreye rastgele bir ek değer (salt) karıştırılır. Böylece aynı şifre farklı kullanıcılarda farklı özet üretir.

Neden BCrypt seçildi

SQL Change Guard kullanıcı şifreleri için BCrypt kullanır.

Özellik	Düz SHA-256	BCrypt
Hız	Çok hızlı. Saniyede milyarlarca deneme yapılabilir.	Kasıtlı olarak yavaş.
Salt	Ayrıca eklemek gerekir.	Kendi içinde üretir ve saklar.
Ayarlanabilir maliyet	Yok.	Var (iş faktörü).
Şifre saklamaya uygunluk	Uygun değil.	Uygun.

İş faktörü nedir: BCrypt'in kaç tur döneceğini belirleyen sayıdır. Bir artırmak süreyi iki katına çıkarır. Donanım hızlandıkça bu sayı artırılarak aynı koruma seviyesi korunur.

SHA-256'nın hızlı olması normal şartlarda iyi bir özelliktir, ama şifre saklamada zayıftır: saldırgan da o hızda deneme yapabilir. BCrypt kasıtlı olarak yavaştır; kullanıcı girişinde fark edilmeyen bir gecikme, milyarlarca deneme yapmaya çalışan saldırgan için aşılabilir bir maliyete dönüşür.

SHA-256 üründe başka amaçlarla da kullanılır: betik parmak izi, kanıt paketlerinin dosya özetleri ve kanıt defterinin özeti. Orada amaç şifre saklamak değil, içeriğin değişmediğini kanıtlamaktır ve hız bir zayıflık değildir. Ayrıntı: Bölüm 5.4.

4.10 Kullanıcılar ekranı

Ekran: Ayarlar > Kullanıcılar

Yetki: settings.users

Alan	Ne işe yarar	Zorunlu	Notlar
Domain Kullanıcı Adı	Kullanıcının giriş adı. Talep, onay ve denetim kayıtlarında bu ad görünür.	Evet	Benzersizdir. Silinmiş bir kullanıcıyla aynı ad girilirse eski kayıt canlandırılır.
E-posta	Bildirimlerin gideceği adres.	Evet	Benzersizdir. Sorgu sonucu e-posta onayında da kullanılır.
Rol	Kullanıcının rolü.	Evet	Bölüm 4.1.
Yönetici	Kullanıcının doğrudan yöneticisi.	Hayır	Onay adımının rolünü karşılıyorsa adım bu kişiye atanır ve bildirim önce ona gider.
Kimlik Doğrulama Tipi	Yerel hesap mı, dizin hesabı mı.	Evet	Bölüm 4.8.
Şifre / Yeni Şifre	Yerel hesaplarda şifre.	Yerel hesapta evet	Dizin hesaplarında görünmez. Şifre politikası Bölüm 2.4.3'teki ayarlardan gelir.
Kilitli	Hesabın kilitli olup olmadığı.	-	Hatalı giriş denemeleri sonucu otomatik oluşur.

Ekrandaki işlemler:

İşlem	Ne yapar
Kilidi aç	Kilitlenmiş hesabı süre dolmadan açar.
Şifre sıfırla	Yerel hesaba yeni şifre atar.

İşlem	Ne yapar
CSV içe aktar	Toplu kullanıcı ekler. Dosyadaki her satır tek tek doğrulanır; hatalı satırlar sonuç özetinde bildirilir.
Sil	Yumuşak silme yapar. Bölüm 4.7'deki koruma kuralları uygulanır.

Dört göz kuralı açıkken bu ekrandaki değişiklikler de onaya düşer. Bölüm 8.

4.11 Roller ekranı

Ekran: Ayarlar > Roller

Yetki: settings.roles

Her rol için Bölüm 4.4'teki yetkiler tek tek açılıp kapatılabilir. Üç kural vardır:

1. SystemManager rolü düzenlenemez. Aksi halde biri en üst rolün yetkisini kısıtlayıp sistemi yönetilemez hale getirebilirdi.
2. Denetçi rolüne onaylama veya çalıştırma yetkisi verilemez. Görevler ayrılığı gereğidir.
3. Rolün hiyerarşi seviyesi ekrandan değiştirilmez. Seviye ürün tanımının parçasıdır.

4.12 Toplu kullanıcı aktarımı

Ekran: Ayarlar > Kullanıcılar > CSV içe aktar

Yetki: settings.users

Kurumun kullanıcı listesi tek tek girilmek yerine bir dosyadan yüklenebilir. Aktarım, tek tek kullanıcı eklemenin kestirme yolu değildir: aynı roller, aynı yetki kontrolü, aynı denetim izi geçerlidir. Dört göz kuralı açıksa aktarım da onaya düşer ve onaylanana kadar hiçbir kullanıcı oluşmaz.

Dosya nasıl hazırlanır

Ekrandaki Şablon indir düğmesi bir Excel dosyası verir. Şablonun Kullanıcılar sayfasında beş kolon vardır ve başlık satırı değiştirilmemelidir:

DomainUsername, Email, Role, AuthType, ManagerUsername

Rol ve kimlik doğrulama tipi kolonları açılır liste ile doldurulur. Rol listesi ürünün tanıdığı rollerin tamamıdır, Denetçi rolü de bu listededir. Dosya doldurulduktan sonra Farklı Kaydet ile CSV UTF-8 biçiminde kaydedilir ve ekrandan yüklenir.

Doğrulama ve hata bildirimi

Her satır tek tek doğrulanır. Bir satırda bile hata varsa hiçbir kullanıcı oluşturulmaz ve hatalar satır numarasıyla birlikte ekranda listelenir. Bu bilinçli bir tercihtir: yarısı yüklenmiş bir kullanıcı listesi, hiç yüklenmemiş bir listeden daha zor düzeltilir.

Kontrol edilenler: zorunlu alanlar, e-posta biçimi, rolün ve kimlik doğrulama tipinin geçerliliği, kullanıcı adının ve e-postanın hem dosya içinde hem sistemde benzersizliği, yerel ve izin hesaplarında kullanıcı adının kısa ad olması (alan adı ya da e-posta son eki içermemesi), yönetici zincirinde döngü olmaması. Kapatılmış bir hesapla aynı kullanıcı adı da toplu aktarımla açılmaz; hesabı geri açmak yönetici kararıdır ve tek tek yapılır.

Yönetici alanına yazılan kişinin ya aynı dosyada ya da sistemde zaten kayıtlı olması gerekir. Kullanıcılar parça parça yükleniyorsa, yöneticisi önceki dosyayla gelmiş kişiler doğrudan bağlanır. Kapatılmış bir hesap yönetici olarak seçilemez: listede görünmeyen bir kişiye bağlı kullanıcılar oluşur ve onay adımı kimseye düşmez.

Bir dosya en fazla 500 satır içerebilir.

Aktarılan hesap giriş yapamaz

Şablonda parola kolonu yoktur. Bu bilinçli bir tercihtir: dosya elden ele dolaşırken parola taşımaz ve yöneticinin bildiği bir parola oluşmaz. Sonuç olarak aktarılan yerel hesap parolasız açılır ve kullanıcı giriş yapamaz.

Bu durum kullanıcı listesinde Parola yok rozetiyle gösterilir. Hesabı kullanıma açmak için satırdaki Şifre sıfırla işlemiyle geçici bir parola verilir; kullanıcı ilk girişte kendi parolasını koymak zorundadır. Dizin (LDAP) hesaplarında parola üründe tutulmadığı için bu rozet çıkmaz, o hesaplar aktarımdan hemen sonra kullanılabilir.

Denetim izi

Aktarım, her kullanıcı için tek tek eklemeye aynı kaydı yazar: User.Create olayı, hesabın kimliği ve kaydın tam görüntüsü. Böylece "bu hesabı kim, ne zaman, hangi rolle açtı" sorusunun cevabı hesabın hangi yoldan açıldığına bağlı değildir.

Bunun yanında toplu işin kendisi de User.BulkImport olayıyla kaydedilir ve hangi kullanıcıları kapsadığını yazar. İki kayıt birlikte, aynı dakikada açılan hesapların tesadüf olmadığını gösterir.

Bölüm 5. Güvenlik ve Şifreleme Modeli

5.1 Üç farklı ihtiyaç, üç farklı yöntem

İhtiyaç	Kullanılan yöntem	Neden
Kullanıcı şifresi saklamak	BCrypt	Geri döndürülmemeli, kırılması pahalı olmalı.
Sunucu şifresi ve sonuç paketi parolası saklamak	AES-256-GCM	Uygulamanın bu değerleri geri okuyabilmesi gerekir.
Denetim kaydındaki değişikliği fark ettirmek	Append-only defter (SQL Server ledger) ve imzalı dış özet	Geri okumak gerekmez, yalnızca doğrulamak gerekir.

Temel ayrım şudur: bir değeri geri okumanız gerekiyorsa şifreleme, yalnızca doğrulamanız gerekiyorsa özet kullanılır.

5.2 Sunucu şifreleri: AES-256-GCM

Simetrik şifreleme nedir

Aynı anahtarla hem şifreleyip hem çözebildiğiniz yönteme simetrik şifreleme denir. AES bunun en yaygın örneğidir. 256, anahtar uzunluğunun bit cinsinden değeridir.

GCM neden seçildi

AES'in birden çok çalışma kipi vardır. GCM kipi şifrelemeye ek olarak bir doğrulama etiketi üretir. Şifreli metin sonradan değiştirilirse çözme işlemi hata verir, sessizce bozuk veri dönmez.

Klasik kiplerde (örneğin CBC) saldırgan şifreli metni bozabilir ve uygulama bunu fark etmeden anlamsız bir sonuç üretebilir. GCM'de değiştirilmiş şifreli metin doğrulama etiketinden geçmez ve çözme hata verir.

Nerede kullanılır

Veri	Nerede tutulur	Anahtar
Sunucu tanımındaki veritabanı şifresi	Servers.SqlPassword sütunu	Security:ServerPasswordKey
Sorgu sonucu ZIP parolası	ChangeRequests.QrZipPassword sütunu	Security:QrZipPasswordKey

Anahtarlar veritabanında değil, yapılandırmada durur. Böylece yalnızca veritabanına erişen biri bu değerleri çözemez.

Anahtar değişirse: Eski değerler çözülemez. Sunucu şifrelerinin yeniden girilmesi gerekir. Bu yüzden anahtar değişimi planlı yapılmalıdır.

5.3 Neyin nerede korunduğu

Veri	Durum
Kullanıcı şifresi	BCrypt özeti olarak saklanır. Geri okunamaz.
Sunucu veritabanı şifresi	AES-256-GCM ile şifreli saklanır. Arayüzde hiçbir zaman gösterilmez.
Sorgu sonucu ZIP parolası	AES-256-GCM ile şifreli saklanır. Yalnızca yetkili kullanıcıya gösterilir.
Sorgu sonucu verisi	Şifreli ZIP içinde diskte tutulur, saklama süresi dolunca silinir.
Denetim kaydı	Açık metin olarak append-only defter tablosunda tutulur; veritabanı motoru güncelleme ve silmeyi reddeder.
Günlük dosyaları	Şifre ve parola alanları maskelenir.

5.4 Denetim kaydı: append-only defter

Defter nedir

Denetim kayıtları SQL Server'ın append-only ledger (defter) tablosunda tutulur (evidence.AuditLogs). Veritabanı motoru bu tablodaki bir kaydın değiştirilmesini ya da

silinmesini sysadmin dahil herkes için reddeder. Tabloyu düşürmek mümkündür, ancak düşürme defterin kendi geçmişinde iz bırakır ve ürün bunu yakalar (Bölüm 17.16).

Özet ve dış tanık

Motor kayıtları bloklar halinde birbirine bağlar ve istendiğinde o ana kadarki bütün defteri kapsayan tek bir özet üretir. Worker saatte bir özet turunu başlatır; API özeti alır, imza açıksa kurumun özel anahtarıyla imzalar ve kurumun değiştirilemez deposuna yazar (Bölüm 17.17). Veritabanı dosyasına doğrudan müdahale ya da eski bir yedeğe dönüş, dışarı yazılmış özetle karşılaştırıldığında ortaya çıkar.

Her turda API geri yükleme geçmişini ve dış depodaki son özetle sürekliliği kontrol eder; bir sorun bulursa Ledger.RestoreDetected ya da Ledger.ForkDetected olayını yazar. Bağımsız tam doğrulamayı ise kurum ya da denetçi yapar: yedek bir kopyaya geri yüklenir ve sys.sp_verify_database_ledger yordamı değiştirilemez depodaki özetlerle çalıştırılır. Adımlar Denetçi Kiti belgesindedir.

Neden gizli anahtar yok

Kayıtların bütünlüğü bir gizli anahtara dayanmaz. Doğrulama için gereken her şey (özet dosyaları, açık anahtar, veritabanı kopyası) denetçiye verilebilir ve kuruma ait hiçbir sır paylaşılmaz. Özet dosyalarının imzası yalnızca dosyanın hangi kurulumdan çıktığını gösterir.

5.5 Veritabanı seviyesi yazma kaydı

Denetim kaydının yanında ikinci bir iz daha tutulur: TableWriteLogs. Bu iz ürünün kendi veritabanındaki tablolar içindir; yönettiğiniz hedef veritabanlarındaki tabloları kapsamaz. İzlenen her tabloda ekleme, güncelleme ve silme olduğunda satırın eski ve yeni hali buraya yazılır. Kaydı veritabanı tetikleyicileri yazar.

İkisi ayrı işlere bakar:

	Denetim kaydı (AuditLogs)	Yazma kaydı (TableWriteLogs)
Ne saklar	Uygulamadan geçen yönetim olayları	Veritabanındaki ham yazma hareketi
Kim yazar	Uygulama	Veritabanı tetikleyicisi
Uygulamayı atlayan değişikliği görür mü (tetikleyici açıkken)	Hayır	Evet
Mühür	Append-only defter ve dış özet	Yok, aşağıya bakınız

Yazma kaydında değişikliği yapan veritabanı girişi de saklanır. Biri doğrudan SQL ile kayıt üzerinde değişiklik yaparsa, hangi girişin yaptığı buradan görülür.

Yazma kaydında neden mühür yok

Denetim kaydı append-only defterde durur: veritabanı motoru değiştirmeyi ve silmeyi reddeder ve defterin özeti dışarı yazılır. Denetim kanıtı orada durur.

Yazma kaydı defter tablosu yapılmaz: her yazımda satırın eski ve yeni halini sakladığı için hacmi büyüktür ve zamanla temizlenmesi gerekebilir; defter tablosundan satır silinemez. Bunun yerine iki gerçek kontrol kullanılır.

Kurulumda yapılması gereken

1. Yazma kaydına yalnız ekleme yetkisi verin. Uygulama hesabının bu tabloyu değiştirmesi veya silmesi gerekmez:

```
GRANT INSERT ON dbo.TableWriteLogs TO [uygulama_hesabi];  
DENY UPDATE, DELETE ON dbo.TableWriteLogs TO [uygulama_hesabi];
```

Bu adım kurulumla bırakılmıştır, çünkü hesap adı kuruma göre değişir. Uygulandığında uygulama hesabı yazma kaydındaki satırları değiştiremez ve silemez.

2. Günlük kapsam özetini açık tutun. Worker her gün yazma kaydının kapsam özetini (satır sayısı ve numara aralığı) kanıt defterine TableWriteLog.CoverageRecorded olayı olarak yazar. Olay değiştirilemediği için toplu silme sonradan görünür. Bu, worker çalıştığı sürece kendiliğinden olur (Workers:TableWriteLogCoverageEnabled).

Geriye kalan tek durum, veritabanında değiştirme yetkisi olan birinin tek bir satırı yerinde düzenlemesidir. Bunu veritabanı içinde hiçbir yöntem engelleyemez; çözümü birinci maddedeki yetki ayarıdır.

5.6 Sır maskeleyme

Denetim kaydına ve günlüklere yazılan bilgilerde şifre, parola ve bağlantı metni gibi alanlar maskelenir. Amaç, denetim izini okuma yetkisi olan bir kişinin bu izden gizli bilgi toplayamamasıdır.

Bölüm 6. Sunucu Tanımları

Ekran: Ayarlar > Sunucular

Yetki: settings.servers

6.1 Bu ekran ne işe yarar

Talep ve sorguların çalıştırılacağı hedef veritabanı sunucuları burada tanımlanır. Bir sunucu tanımı yoksa hiçbir talep açılmaz, çünkü talep en az bir hedef sunucu seçmek zorundadır.

6.2 Alan alan açıklama

Tabloda yer almayan iki alan daha vardır. Sunucu sertifikasını doğrula (varsayılan kapalı): açıkken hedefin TLS sertifikası doğrulanır; SQL Server'da sertifikaya koşulsuz güvenilmez, PostgreSQL'de tam doğrulama (VerifyFull) yapılır. Kapalıyken bağlantı şifreli olabilir ama hedefin kimliği doğrulanmaz; üretim hedeflerinde açılması önerilir. İzole deneme zorunlu: Sandbox modülü lisanslıysa görünür ve bu sunucudaki	Ne işe yarar	Zorunlu	Geçerli değerler	Varsayılan	Boş bırakılırsa	Değiştirince ne olur
---	--------------	---------	------------------	------------	-----------------	----------------------

talepler için sandbox denemesini zorunlu kılar. Alan						
Sunucu Adı	Sistem içinde bu sunucuyu tanımlayan ad. Taleplerde ve raporlarda bu ad görünür.	Evet	Serbest metin	-	Kaydedilmez, hata verir	Eski taleplerdeki sunucu adı metin olarak saklandığı için geçmiş kayıtlar eski adı gösterir.
Host	Sunucunun ağ adresi veya adı.	Evet	Ad veya IP	-	Kaydedilmez	Yeni bağlantılar yeni adrese gider.
Port	Bağlantı portu. Veritabanı tipini değiştirdiğinizde otomatik güncellenir.	Hayır	Sayı	SQL Server 1433, Oracle 1521, PostgreSQL 5432	Varsayılan kullanılır	
Veritabanı Tipi	Hedefin türü. Liste lisansa göre daralır.	Evet	SQL Server, Oracle, PostgreSQL	SQL Server	-	Betik ayrıştırma ve çalıştırma davranışı tümüyle değişir.
Veritabanı Adı	Bağlanılacak veritabanı. PostgreSQL için gereklidir. SQL Server'da bağlantı bu veritabanında açılır; betikteki USE ifadesi bunu ezer. Oracle için servis adıdır ve genelde host içinde verilir.	Türe bağlı	Serbest metin	Boş	SQL Server'da varsayılan veritabanı kullanılır	
Ortam	Sunucunun hangi ortama	Evet	Production, Staging,	Production	-	Politika eşleşmesi

	ait olduđu. Onay politikası seçimini doğrudan etkiler.		Development, Test			değişir, yeni talepler farklı onay adımları alabilir.
SQL Kullanıcı Adı	Hedef sunucuya bağlanılacak hesap.	Evet	Serbest metin	-	Bağlantı kurulamaz	
SQL Şifre	Hesabın şifresi. Şifreli saklanır, hiçbir ekranda geri gösterilmez.	Yeni kayıta evet	Serbest metin	-	Düzenlemede boş bırakılırsa mevcut şifre korunur	
Aktif	Sunucunun kullanımda olup olmadığı.	-	Açık / Kapalı	Açık	-	Kapatılırsa yeni taleplerde seçilemez.
CR Otomatik Çalıştırma	Onaylanan değişiklik talepleri bu sunucuda otomatik çalışsın mı. Zamanlama modülü gerektirir.	-	Açık / Kapalı	Kapalı	-	Bkz. 6.4
QR Otomatik Çalıştırma	Onaylanan sorgu sonucu talepleri bu sunucuda otomatik çalışsın mı.	-	Açık / Kapalı	Kapalı	-	Bkz. 6.4
Rollback Zorunlu	Bu sunucuda çalıştırma yapılabilmesi için geri alma betiğinin oluşturulmuş olması şartı.	-	Açık / Kapalı	Kapalı	-	Açıldığında geri alma betiği olmayan talepler çalıştırılmaz.
Otomatik Rollback	Talep onaylandığında geri alma betiği otomatik üretilsin mi.	-	Açık / Kapalı	Kapalı	-	

SSL Zorunlu	Yalnızca PostgreSQL için görünür. Bulut PostgreSQL servislerinde gereklidir.	-	Açık / Kapalı	Kapalı	-	
Maskeleme	Bu sunucudan dönen sorgu sonuçlarında hassas veri tespitinin nasıl yapılacağı.	Evet	Tam (katalog + desen), Yalnız içerik	Tam	-	Bkz. 6.5
Muafiyet gerekçesi	Maskeleme "Tam" dışında seçildiyse yazılı gerekçe.	Tam dışında evet	Serbest metin	Boş	Kaydedilmez, hata verir	Denetim kaydına yazılır.

6.3 Bağlantı testi

Sunucu düzenleme ekranında bağlantı testi düğmesi vardır. Test, girilen bilgilerle sunucuya bağlanmayı dener ve sonucu hemen gösterir.

Test sonuçlarının anlamı:

Sonuç	Anlamı	Ne yapmalı
Başarılı	Bağlantı kuruldu.	-
Kimlik doğrulama hatası	Kullanıcı adı veya şifre yanlış.	Bilgileri kontrol edin.
Sunucuya ulaşılamıyor	Ağ, host adı veya port hatalı ya da güvenlik duvarı engelliyor.	Ağ erişimini kontrol edin.
Veritabanı bulunamadı	Veritabanı adı yanlış.	Adı kontrol edin.
Bu veritabanı tipi lisans kapsamında değil	Lisans bu türe izin vermiyor.	Bölüm 3.5.

Worker servisi ayrıca ConnectionCheckJob ile düzenli aralıklarla tüm aktif sunuculara bağlanmayı dener ve durumu günceller. Bu sayede bir sunucu erişilemez hale geldiğinde talep çalıştırılmadan önce fark edilir.

6.4 Otomatik çalıştırma: arka planda ne oluyor

Bu, kılavuzun en çok soru alan konularından biridir. Adım adım anlatalım.

Zincir

Talep onaylandı

|

v

Otomatik zamanlama kontrolü (ApplyAutoSchedule)

|

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

|

Sartlar saglanmiyor

|

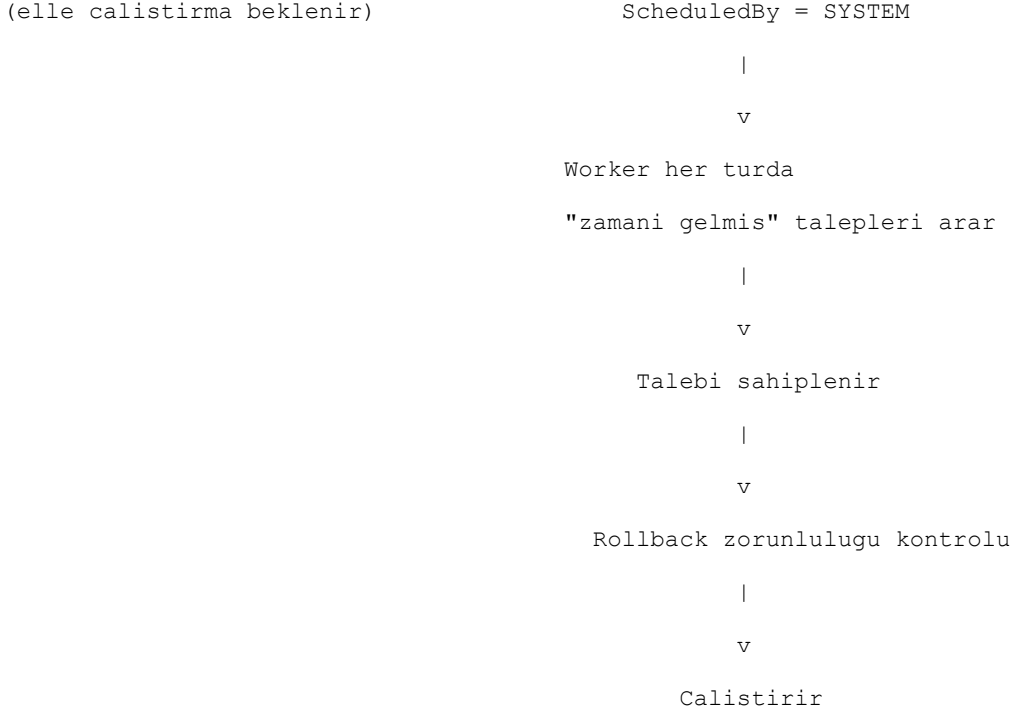
Sartlar saglanıyor

|

ScheduledAt bos kalir

|

ScheduledAt hesaplanir



Şartlar

Otomatik zamanlama yalnızca aşağıdakilerin hepsi doğruysa yapılır:

1. Zamanlama modülü lisanslı.
2. Talebin risk bulgularından hiçbiri "asla atlanamaz" (NeverSkip) işaretli değil.
3. Talep bir rollback talebi değil.
4. Talep aktif bir sürüm paketi içinde değil.
5. Talebin tüm hedef sunucularında ilgili otomatik çalıştırma bayrağı açık. Değişiklik talepleri için CR bayrağı, sorgu sonucu talepleri için QR bayrağı bakılır.
6. Değişiklik talebi ise ve talebin sunucusunda "Rollback Zorunlu" açıksa, geri alma betiği oluşturulmuş olmalı.

Şartlardan biri sağlanmazsa talep onaylı durumda bekler ve birinin elle çalıştırmasını bekler. Daha önce sistem tarafından konmuş bir zamanlama varsa temizlenir.

Zaman nasıl hesaplanır

Sıralama şudur:

1. Kullanıcı talepte belirli bir çalıştırma tarihi verdiyse (RequestedExecutionDate) o kullanılır.
2. Vermediyse ve gecikme dakikası verdiyse (ScheduleDelayInMinutes), onay anı + o dakika kullanılır.
3. Hiçbiri yoksa onay anının kendisi kullanılır.

Sonra ExecutionDelaySeconds parametresi devreye girer: hesaplanan zaman, "şu an + ExecutionDelaySeconds" değerinden erken ise o değere çekilir.

Somut örnek: ExecutionDelaySeconds 300 (5 dakika). Bir talebi saat 14:00'te onayladınız ve talepte özel bir tarih yok.

- Hesaplanan zaman: 14:00

- En erken izin verilen zaman: 14:05

- Sonuç: çalıştırma zamanı 14:05 olur.

Worker 14:05'ten önce bu talebi almaz. Bu bekleme süresi bilinçlidir: yanlışlıkla verilen bir onaydan sonra talebi iptal etmek için insan zamanı bırakır.

Aynı parametre elle zamanlamada da alt sınır olarak çalışır, ancak orada en az 30 saniye uygulanır: ExecutionDelaySeconds 10 girilse bile elle zamanlamada en erken 30 saniye sonrası seçilebilir.

Kayıt kime yazılır

Otomatik zamanlamada düğmeye basan bir kişi yoktur. Bu yüzden:

- ScheduledBy = SYSTEM

- ExecutionRequestedBy = SYSTEM

Alan boş bırakılsaydı raporu okuyan kişi "yazılmayı mı unuttular" diye düşünürdü. Kararın sahibi açıkça SYSTEM olarak yazılır.

6.5 Maskeleye rejimi

Rejim	Ne yapar	Ne zaman kullanılır
Tam (Strict)	Hem sınıflandırma kataloğuna (kolon adı) hem veri desenlerine bakar.	Gerçek veri barındıran her ortam. Varsayılan budur.
Yalnız içerik (ContentOnly)	Kolon adına bakmaz, yalnızca değerlere bakar.	Sentetik (üretilmiş) veri barındıran test ortamları.

Sunucu seviyesinde "kapalı" seçeneği bilinçli olarak yoktur. Maskelemeyi tümüyle kapatmak yalnızca genel QrMaskingEnabled parametresi ile mümkündür ve bu bir kontrol değişikliği sayılır.

Yalnız içerik rejimi kendini doğrular: Bu rejimde kolon adına bakılmaz, ama değer bazlı kontrol çalışmaya devam eder. Sunucuya gerçek veri yüklenirse kimlik numarası, kart numarası ve IBAN gibi doğrulanabilir alanlar yine yakalanır ve maskelenir. Yani "test ortamı" diye açılan muafiyet, ortama gerçek veri girdiği anda kendiliğinden dar bir korumaya döner.

Bu rejimde açık kalan alanlar: ad, adres, tanı gibi belirli bir deseni olmayan bilgiler. Ekranda bu uyarı açıkça gösterilir.

Rejim "Tam" dışında seçildiğinde yazılı gerekçe zorunludur ve teslim anında kayda dondurulur. Sunucu sonradan "Tam" moduna çevrilse bile o teslimin hangi rejimle yapıldığı kanıtta kalır.

6.6 Çoklu sunucu kuralı

Birden çok sunucu yalnız sorgu sonucu (QueryResult) talebinde seçilebilir; değişiklik ve geri alma talepleri tek sunucuya gider ve bu kural sunucu tarafında da uygulanır. Sebebi sunucular arasında dağıtık transaction olmamasıdır: ilk sunucu commit edip ikincisi düşerse yarım değişiklik kalırdı. Sunucu adları tek alanda, noktalı virgül ile ayrılarak saklanır:

PROD-SQL01 ; PROD-SQL02 ; PROD-SQL03

Bunun sonuçları:

- Talep listelerinde ve raporlarda sunucu sütunu birden çok ad içerebilir.
- Onay politikası çözümlemesi her sunucu için ayrı yapılır ve en katı sonuç uygulanır.
- Otomatik çalıştırma için tüm sunucularda bayrağın açık olması gerekir.
- Sorgu sonucu taleplerinde her sunucu kendi maskeleye rejimiyle değerlendirilir; canlı sunucu maskelenirken test sunucusu açık kalabilir.
- Sunucu adına göre filtre yapan raporlarda tam eşleşme değil, liste içinde arama yapılır.

6.7 Sunucu silme ve pasife alma

İşlem	Etkisi
Pasife alma	Yeni taleplerde seçilemez. Mevcut talepler etkilenmez. Lisans sayımına girmez (Bölüm 3.4).
Silme	Kayıt tablodan çıkar, lisans sayımında yer açılır. Geçmiş taleplerde sunucu adı metin olarak saklandığı için kayıtlar bozulmaz.

6.8 Hedefteki oturum adı ve oturum yoklaması

Ürün, hedef veritabanına açtığı her bağlantıya bir ad verir. Böylece veritabanı yöneticisi ve veritabanı etkinlik izleme (DAM) aracı, bir oturumun ürüne ait olup olmadığını ve hangi işe ait olduğunu görebilir. Ad bağlantıya verilir, betiğin metnine dokunulmaz.

Ad biçimi: SQL Change Guard/<Rol>/<Numara>. Örnek: SQL Change Guard/Execute/123. Ad en fazla 63 karakterdir ve yalnız ASCII harf, rakam, boşluk, eğik çizgi, tire ve alt çizgi içerir. Oracle'da ad bağlantı açıldıktan sonra atanır: rol MODULE alanına, numara ACTION alanına, tam ad CLIENT_IDENTIFIER alanına yazılır.

Rol	Ne zaman	Havuz	Pencere
Execute	Değişiklik talebi çalışırken	Kapalı	Açar
Query	Sorgu sonucu talebi, sunucu başına	Kapalı	Açar
Release	Sürüm paketi, AllOrNothing kipi (tek bağlantı)	Kapalı	Açar
Sandbox, SandboxRelease	Talebin ya da paketin izole denemesi	Kapalı	Açar
Health	Worker'ın bağlantı sağlık kontrolü	Açık	Açmaz
Preview, Definition, Test	Kolon önizlemesi, nesne tanımı okuma, bağlantı deneme	Açık	Açmaz

Kimlik taşıyan beş rolde bağlantı havuzu kapalıdır: iş bitince oturum kapanır. Health, Preview, Definition ve Test rollerinde havuz açıktır; bağlantı bir süre boşta açık kalabilir. Bu normaldir ve bu bağlantılar betik çalıştırmaz.

Bağlantı açıldıktan sonra ürün hedefe tek bir okuma sorgusu atar ve oturum numarasını ile hedefin gördüğü istemci adresini öğrenir (SQL Server: oturum numarası ve istemci adresi; PostgreSQL: süreç numarası ve istemci adresi; Oracle: SID, denetim oturum numarası ve istemci adresi). Bu iki bilgiyi istemci değil sunucu söyler, bu yüzden sahtelenemez. Sorgu başarısız olursa alanlar boş kalır, iş devam eder ve Worker günlüğüne uyarı yazılır.

Uygulama adı bir etikettir: bağlanan taraf kendi söyler. Ad tek başına kanıt sayılmaz; hesap, hedefin gördüğü adres, oturum numarası ve pencere zamanı birlikte aranır.

Bölüm 7. Parametreler

Ekran: Ayarlar > Parametreler

Yetki: settings.params

7.1 Bu ekran ne işe yarar

Sistem davranışını belirleyen tekil ayarlar burada tutulur. Her parametrenin bir anahtarı, bir değeri ve bir grubu vardır. Ekranda parametreler gruplara göre listelenir.

7.2 Ekrandaki alanlar

Alan	Anlamı
Anahtar (Key)	Parametrenin sistem içindeki adı. Değiştirilmez.
Değer (Value)	Etkin değer.
Açıklama	Parametrenin ne yaptığı.
Kontrol tipi	Değerin ekranda nasıl girileceği: Numeric (sayı), Boolean (açık/kapalı), Text (metin), Combo (listeden seçim).
Seçenekler	Combo tipindeki parametrenin geçerli değerleri.
Grup	Ekrandaki başlık.
Kontrol ayarı rozeti	Bu parametre bir kontrolün sertliğini doğrudan belirliyorsa gösterilir. Bkz. Bölüm 8.

7.3 Genel grubu

DefaultQueryTimeout

- Ne işe yarar: Yeni açılan taleplerde sorgu zaman aşımı alanının başlangıç değeri ve alt sınırı.
- Değer: Saniye cinsinden sayı.
- Varsayılan: 30
- Nerede okunur: Talep editörü ekranı ve talep kaydetme komutu.
- Örnek: 30 iken yeni bir talep açtığınızda zaman aşımı alanı 30 gelir. Elle 10 yazarsanız kayıt sırasında 30'a yükseltilir.
- Boş veya 0 ise: 30 kabul edilir.
- Geçmiş etkiler mi: Hayır, yalnızca yeni taleplerde geçerlidir.

MaxQueryTimeout

- Ne işe yarar: Bir talebe verilebilecek en yüksek zaman aşımı.
- Değer: Saniye cinsinden sayı.
- Varsayılan: 3600 (1 saat)
- Nerede okunur: Talep kaydetme ve sürüm paketi kaydetme komutları.

- Örnek: 3600 iken kullanıcı 7200 girerse değer 3600'e düşürülür.
- Neden vardır: Çok uzun süren bir betik hedef sunucuda kilit tutar ve diğer işleri bekletir. Üst sınır bu riski sınırlar.

ExecutionDelaySeconds

- Ne işe yarar: Onaydan sonra çalıştırmaya kadar geçecek en az süre.
- Değer: Saniye cinsinden sayı.
- Varsayılan: 300 (5 dakika)
- Nerede okunur: Onay komutu, onay akışı servisi, elle zamanlama komutu.
- Örnek: Bölüm 6.4'te ayrıntılı anlatıldı. 300 iken 14:00'te onaylanan talep en erken 14:05'te çalışır.
- 0 ise: Bekleme uygulanmaz, otomatik çalıştırma onay anında devreye girer. Elle zamanlamada yine 30 saniye alt sınır geçerlidir.
- Neden vardır: Yanlış verilen onaydan dönmek için zaman bırakır.

RejectOnError

- Ne işe yarar: Çalıştırma hata verdiğinde talep otomatik reddedilsin mi.
- Değer: true / false
- Varsayılan: true
- Nerede okunur: Zamanlanmış çalıştırma servisi.
- Örnek: true iken gece çalışan bir talep hata alırsa durumu Rejected olur ve bir daha denenmez. false iken talep Approved durumuna geri döner ve tekrar denenebilir.
- Kontrol ayarı mı: Evet.
- Hangisini seçmeli: Sıkı kontrol isteyen kurumlarda true tercih edilir; başarısız bir işin sessizce tekrar denenmesi istenmez.

7.4 Görevler Ayrılığı grubu

Bu gruptaki parametreler kurum genelindeki varsayılanlardır. Bir onay politikası bunları sunucu veya ortam bazında değiştirebilir. Etkin değerler, onay akışı kurulurken talebe dondurulur; sonradan yapılan değişiklikler karara bağlanmış talepleri yeniden yazmaz.

RequesterCanSelfApproveExecute

- Ne işe yarar: Talebi açan kişi kendi talebini onaylayıp çalıştırabilir mi.
- Değer: true / false
- Varsayılan: true

- Nerede okunur: Onaylama, çalıştırma, zamanlama ve manuel işaretleme kontrolleri.
- Örnek: false iken bir geliştirici kendi açtığı talebi onaylamak isterse "talep sahibi kendi talebini onaylayamaz" mesajını alır ve düğme pasif görünür.
- Kontrol ayarı mı: Evet.

ApproverCanExecute

- Ne işe yarar: Bir talebi onaylayan kişi aynı talebi çalıştırabilir mi.
- Değer: true / false
- Varsayılan: true
- Nerede okunur: Çalıştırma ve zamanlama kontrolleri.
- Örnek: false iken talebi onaylayan yönetici çalıştır düğmesini pasif görür; başka bir yetkilinin çalıştırması gerekir.
- Neden vardır: Onaylayan ile uygulayanın ayrılması yaygın bir denetim beklentisidir.
- Kontrol ayarı mı: Evet.

RequireDistinctApproverPerStep

- Ne işe yarar: Aynı kişi bir talepte birden çok onay adımını kapatabilir mi.
- Değer: true / false
- Varsayılan: false
- Örnek: İki adımlı bir politikada, false iken yeterli role sahip tek kişi iki adımı da kapatabilir. true iken ikinci adım için farklı bir kişi gerekir. Gerçek dört göz kuralı budur.
- Kontrol ayarı mı: Evet.

EmergencyMinimumRole

- Ne işe yarar: Acil durum talebi açabilmek için gereken en düşük rol.
- Değer: Rol adı.
- Varsayılan: Requester
- Örnek: ChangeManager yapılırsa geliştiriciler acil durum talebi açamaz; yalnızca değişiklik yöneticisi ve üstü açabilir.
- Neden vardır: Acil durum ilan etmek bir yetkidir. Herkeste olursa normal onay yolu kolayca aşılr.
- Kontrol ayarı mı: Evet.

7.5 Ayar Onayı grubu

SettingsApprovalPolicy

- Ne işe yarar: Ayar ekranlarında dört göz kuralının kapsamı.
- Değerler:
 - Disabled: Değişiklikler anında uygulanır.
 - ControlSettingsOnly: Yalnızca bir kontrolü zayıflatan veya güçlendiren değişiklikler onay bekler.
 - All: Bu ekranlardaki her değişiklik onay bekler.
- Varsayılan: Disabled
- Kontrol ayarı mı: Evet. Kapatmak da onay ister; açmak hemen uygulanır, çünkü politika kapalıyken yakalama zaten çalışmaz.
- Ayrıntı: Bölüm 8.

7.6 ITSM Bilet grubu

ChangeTicketRequired

- Ne işe yarar: Değişiklik bileti numarasının hangi taleplerde zorunlu olduğu. Değişiklik bileti, işin dayandığı değişiklik kayıdır ve dış sistemden (ITSM) gelir.
- Değer: Always (bilet her talepte zorunlu) / ExceptEmergency (acil olmayan taleplerde zorunlu, acil taleplerde istenmez) / Never (zorunlu değil)
- Varsayılan: Always
- Örnek: Always iken bilet numarası girilmeden talep kaydedilemez. ExceptEmergency, kurumda iki akışın birlikte yaşadığı durum içindir: planlı değişiklik ITSM'de başlar ve biletyle gelir, gece yarısındaki acil müdahale ise ürünün kendisinde başlar ve o anda henüz bir değişiklik kaydı yoktur. Bu seçenek olmasaydı ya kural her yerde gevşetilir ya da nöbetçi alana uydurma bir numara yazardı; ikincisi boş bırakmaktan daha zararlıdır, çünkü denetimde doğrulanamayan bir numara kayıt varmış izlenimi verir.
- Kontrol ayarı mı: Evet.

ChangeTicketRegex

- Ne işe yarar: Bilet numarasının biçim kontrolü.
- Değer: Düzenli ifade (regular expression). Boş bırakılabilir.
- Varsayılan: ^CHG\d{7}\$ (ServiceNow değişiklik kaydı biçimi, örnek CHG0012345)
- Örnek: Varsayılan değerde CHG0012345 kabul edilir, 0012345 ve CHG12345 reddedilir.
- Boş bırakılırsa: Biçim kontrolü yapılmaz, herhangi bir metin kabul edilir.

- Kendi kurumunuz için: Kurulum değeri ServiceNow biçimidir. Aynı biçimi kullanıyorsanız değeri Parametreler ekranında bir kez kaydedin; kurulum kontrolü satırı düzene geçer. Jira kullanıyorsanız anahtarlar proje önekiyle gelir (örnek OPS-123), ^OPS-\d+\$ yazabilirsiniz. Numaralarınız farklıysa kendi deseninizi yazın ya da boş bırakın.

EmergencyTicketRequired

- Ne işe yarar: Acil taleplerde olay (incident) numarasının zorunlu olup olmadığı.
- Değer: Always (zorunlu), Never (zorunlu değil)
- Varsayılan: Never
- Olay numarası nedir: Aciliyeti doğuran arıza kaydının numarasıdır ve değişiklik biletinden farklı bir kayıttır. Biri arızayı anlatır (ödeme servisi durdu), diğeri müdahaleyi (bozuk indeks yeniden oluşturulacak). Denetçi iki ayrı soru sorar: bu değişiklik neden gece yarısı onay kısaltılarak yapıldı, ve bu değişiklik hangi kayda dayanıyor. Birincinin cevabı olay kaydıdır.
- Örnek: Always iken acil talep, olay numarası girilmeden kaydedilemez. Acil olmayan taleplerde bu alan hiç sorulmaz.
- Varsayılan neden Never: Acil yol, kurumun bilinçli olarak benimsemediği bir veri girişi kuralı yüzünden kilitlenmemelidir. Karar verilmediği sürece ayar sessizce kapalı kalmaz; Tanılama ekranındaki kurulum kontrolü listesinde "Karar verin" olarak görünür.
- Kontrol ayarı mı: Evet. Gevşetilmesi denetimde "bu acil değişiklik hangi arızaya dayanıyor" sorusunu cevapsız bırakır.

EmergencyTicketRegex

- Ne işe yarar: Olay numarasının biçim kontrolü.
- Değer: Düzenli ifade (regular expression). Boş bırakılabilir.
- Varsayılan: ^INC\d{7}\$ (ServiceNow olay kaydı biçimi, örnek INC0012345)
- Kendi kurumunuz için: Olay numarası biçimi kurumdan kuruma değişir (ServiceNow'da INC0012345, Jira'da OPS-123). Kurulum değeri ServiceNow biçimidir. Aynı biçimi kullanıyorsanız değeri bir kez kaydedin, farklıysa kendi deseninizi yazın ya da boş bırakın. Boş bırakmak geçerli bir karardır: olay numarası biçim kontrolü olmadan kabul edilir.
- Örnek: Varsayılan değerde INC0012345 kabul edilir, 12345 ve INC-12345 reddedilir.
- Değişiklik biletinden bağımsızdır: iki numara ayrı kayıtlardır ve biçimleri genelde farklıdır. Olay numarası, değişiklik biletinin desenine uymak zorunda değildir.

- Dikkat: Çalıştırılmayan bir desen yazılırsa kaydetme reddedilir. Doğrudan veritabanına yazılmış bozuk bir desen ise kullanıcıyı kilitlemez, biçim kontrolü o istekte uygulanmaz ve durum günlüğe yazılır; kurulum kontrolü listesi bunu "Dikkat" olarak gösterir.

Geri alma talebinde bilet

Geri alma talebi izlenebilirliğini kaynağından alır: hangi talebi geri aldığı kayıtlıdır ve bileti de kaynaktan miras gelir. Bu yüzden kaynağa bağlı bir geri alma talebinde ayrıca bilet numarası istenmez. Aksi halde, biletsiz açılabilen acil bir değişiklik çalıştırıldıktan sonra otomatik geri alma üretimi kurala takılır ve en riskli değişiklikte güvenlik ağı kurulamazdı. Kaynağa bağlı olmayan bir talep bu muafiyetten yararlanamaz.

RequestTicketRegex

- Ne işe yarar: Veri çıkarma talebi bir hizmet talebine dayanıyorsa (ItsmQueryResultTicketKind = Request) numaranın biçim kontrolü. ITSM kapalıyken de geçerlidir.
- Değer: Düzenli ifade (regular expression). Boş bırakılırsa veri çıkarma talebinin numarası ChangeTicketRegex ile kontrol edilir; ayrı bir hizmet talebi biçimi kullanmıyorsanız boş bırakın.
- Varsayılan: ^RITM\d{7}\$ (ServiceNow hizmet talebi biçimi, örnek RITM0010001)
- Örnek: ^RITM\d{7}\$ yazıldığında RITM0010001 kabul edilir, CHG0030001 reddedilir.
- Kontrol ayarı mı: Evet.

ITSM entegrasyonu parametreleri

Aşağıdaki parametreler ITSM entegrasyonunun davranışını belirler. Hepsi kontrol ayarıdır. Nasıl çalıştıkları Bölüm 22'de örneklerle anlatılır. Bağlantı bilgileri (hangi ITSM, adres, hesap) bu ekranda değil, appsettings.json dosyasındaki Itsm bölümündedir.

Anahtar	Değerler	Varsayılan	Ne yapar
ItsmEnabled	true / false	false	Ana anahtar. Kapalıyken ürün ITSM'e gitmez.
ItsmVerifyOnSave	Block / Warn / Off	Block	Talep kaydedilirken kural ihlalinde (kapanmış, bulunamayan, yanlış türde kayıt) ne olacağı.

Anahtar	Değerler	Varsayılan	Ne yapar
ItsmExecuteGate	Block / Off	Block	Çalıştırmadan hemen önce değişiklik kaydının hazır olması aranır mı.
ItsmEnforceWindow	true / false	false	Çalıştırma ITSM'deki planlanan zaman aralığında olmalı mı.
ItsmVerifyIncident	Block / Warn / Off	Warn	Acil talepteki olay numarası ITSM'de nasıl doğrulanır.
ItsmQueryResultTicketKind	Request / Change / None	Request	Veri çıkarma talebi hangi kayda dayanır.
ItsmUnavailablePolicy	AllowAndRecord / Block	AllowAndRecord	ITSM'e ulaşılamazsa işlem sürer mi. Acil talep her durumda geçer.
ItsmReadyStates	Durum adları (; ile)	Scheduled;Implement	Hazır sayılan durumlar.
ItsmClosedStates	Durum adları (; ile)	Review;Closed;Cancelled;Cancelled;Resolved;Closed Complete;Closed Incomplete;Closed Skipped	Kapanmış sayılan durumlar.
ItsmApprovedValues	Değerler (; ile)	Approved	ITSM onay alanında onaylandı sayılan değerler.
ItsmWriteBackEnabled	true / false	true	ITSM kaydına not yazılır mı.
ItsmWriteBackEvents	Olay adları (; ile)	Talep olayları	Hangi talep olaylarının not olarak yazılacağı.

7.7 Sorgu Sonucu grubu

QrFileRetentionDays

- Ne işe yarar: Sonuç ZIP dosyalarının diskte kaç gün tutulacağı.
- Değer: Gün sayısı.
- Varsayılan: 1
- Nerede uygulanır: Bakım görevi (QR Dosya Temizleme).
- Örnek: 1 iken bugün üretilen dosya yarın silinir. Silme işlemi denetim kaydına yazılır ve Veri Erişim raporunda görünür.
- Kontrol ayarı mı: Evet.
- Neden kısa tutulur: Canlı veri içeren dosyanın diskte kalma süresi ne kadar kısaysa risk o kadar azdır.

QrRequesterCanDownload

- Ne işe yarar: Talebi açan kişi kendi sonuç dosyasını indirebilir mi.
- Değer: true / false
- Varsayılan: true
- Örnek: false yapılırsa sorgu sonucunu isteyen kişi dosyayı indiremez; yalnızca aşağıdaki rol eşiğini geçen kişiler indirebilir. Bu, veriyi isteyen ile veriye erişen kişiyi ayırmak isteyen kurumlar içindir.
- Kontrol ayarı mı: Evet.

QrDownloadMinimumRole

- Ne işe yarar: Talebi açan kişi dışındakiler için indirme yetkisinin alt sınırı.
- Değer: Rol adı.
- Varsayılan: ChangeManager
- Örnek: ChangeManager iken bir DbAdmin başkasının sonuç dosyasını indiremez, çünkü hiyerarşide altıdır.
- Kontrol ayarı mı: Evet.

QrDeliveryMode

- Ne işe yarar: Sonuç dosyasının ve onu açan ZIP parolasının hangi kanaldan teslim edileceği. Bu değer kurum TAVANIDIR: talep daha sıkı bir biçim seçebilir, daha gevşegini seçemez.

- Değer: PortalOnly, AttachmentPortalPassword veya AttachmentAndPassword. Ekranda listeden seçilir.

- Varsayılan: AttachmentPortalPassword

- PortalOnly: E-postada ne dosya ne parola gider; yalnızca "sonucunuz hazır" bildirimi gönderilir. Dosya da parola da portalden alınır. En sıkı seçenektir.

- AttachmentPortalPassword: ZIP e-postaya eklenir, parola e-postada YAZMAZ, portalden alınır. Varsayılan budur.

- AttachmentAndPassword: ZIP ve parolası aynı e-postada gider. En gevşek seçenektir ve yazılı gerekçe ister.

- Neden varsayılan parolayı e-postadan çıkarır: Şifreli ZIP'in koruduğu durum (posta kutusunun ele geçmesi, e-postanın yanlış kişiye gitmesi, arşivin okunması) tam da parolanın aynı e-postada durduğu durumdur. Parola yanındaysa şifreleme koruma sağlamaz.

- Gerekçe hangi durumda istenir: Uygulanacak biçim AttachmentAndPassword ise. Talep biçim seçmemişse kurum tavanı uygulanacağı için gerekçe yine istenir.

- Parolayı portalden görme: Yazılı gerekçe zorunludur ve gerekçesiz istek reddedilir. Her görüntüleme denetim kaydına yazılır.

- Uygulanan biçim nasıl belirlenir: Talebin seçimi ile kurum tavanının SIKI olanı geçerlidir. Kurum tavanı talep kaydedildikten sonra sıkılaştırılmışsa eski talep de yeni kurala uyar.

- Teslim anında dondurulur: Uygulanan biçim teslim kaydına yazılır ve sonradan yeniden hesaplanmaz. Böylece kurum ayarı daha sonra değişse bile geçmiş bir teslimin raporu ve denetim dosyası değişmez.

- Kontrol ayarı mı: Evet. Gevşetilmesi dört göz onayına düşer ve denetim kaydına ayrı bir olay olarak yazılır.

QrMaxRowCount

- Ne işe yarar: Bir sorgu sonucu talebinin teslim edebileceği en fazla satır sayısı.

- Değer: Satır sayısı.

- Varsayılan: 1000000

- Nerede uygulanır: Sonuç okunurken. Sınıra ulaşıldığı anda okuma durdurulur.

- Örnek: Sınır 1000000 iken 1.200.000 satır döndüren bir talep çalıştırılmaz. Talep başarısız olur, sebebi çalıştırma günlüğüne yazılır, paket üretilmez ve e-posta gönderilmez.

- Neden okuma sırasında uygulanır: Önce hepsini okuyup sonra reddetmek ne zamanı ne belleği kurtarır. Ölçümde 2 milyon satırlık bir sonuç, reddedilmeden önce 1,1 GB bellek dolduruyordu. Sınır okuma sırasında uygulandığı için bellekte sınırdan fazla satır hiçbir zaman tutulmaz; maskeleme ve dosya yazımı hiç çalışmaz.

- Excel ile ilişkisi: Sonuç Excel olarak yazılacaksa geçerli sınır, bu değer ile Excel biçiminin kendi sınırı olan 1.048.575 veri satırından küçük olanıdır. Bu ikinci sınır bir tercih değil,.xlsx dosya biçiminin kuralıdır ve değiştirilemez.

- Kontrol ayarı mı: Evet. Değeri yükseltmek, tek bir onaylı talebin daha fazla canlı veriyi kurum dışına taşıyabilmesi demektir.

QrOutputFormat

- Ne işe yarar: Sonuç paketindeki veri dosyasının biçimi.

- Değer: Auto, ExcelOnly veya CsvOnly. Ekranda listeden seçilir.

- Varsayılan: Auto

- Auto: Satır sayısı QrCsvThresholdRowCount değerinin altındaysa Excel, üstündeyse CSV yazılır.

- ExcelOnly: Her zaman Excel yazılır. Geçerli satır sınırı, Excel biçiminin 1.048.575 satırlık tavanı ile kesişir.

- CsvOnly: Her zaman CSV yazılır. Excel satır tavanı devreye girmez, yalnızca QrMaxRowCount geçerlidir.

- CSV biçimi: Ayraç noktalı virgüldür ve dosya UTF-8 işaretiyle yazılır. Böylece dosya Türkçe Excel'de hem doğru sütunlara ayırır hem de Türkçe karakterler bozulmadan açılır.

- Güvenlik notu: Eşittir, artı, eksi veya @ işaretiyle başlayan METİN hücreleri, dosya Excel'de açıldığında formül olarak çalışmasın diye etkisizleştirilir. Değer kaybolmaz, yalnızca çalışması engellenir. Sayı, tarih ve mantıksal değerler bundan etkilenmez; negatif sayılar sayı olarak kalır ve toplanabilir.

- Kontrol ayarı mı: Hayır. Biçim, kimin neye erişebildiğini ya da ne kadar verinin dışarı çıktığını değiştirmez. Paket her iki biçimde de aynı şifreli ZIP içinde ve aynı maskeleme ile teslim edilir.

QrCsvThresholdRowCount

- Ne işe yarar: Auto biçiminde Excel ile CSV arasındaki geçiş noktası.

- Değer: Satır sayısı.

- Varsayılan: 500000

- Örnek: 500000 iken 400.000 satırlık sonuç Excel, 600.000 satırlık sonuç CSV olarak yazılır. Tam 500.000 satırda Excel yazılır, çünkü eşik "bundan fazlaysa" anlamına gelir.

- Birinci sınır: Değer QrMaxRowCount değerinden büyük olamaz. Büyük olsaydı hiçbir zaman devreye giremezdi: sonuç zaten üst sınırdan kesildiği için eşik üstüne hiç çıkmazdı ve ayar sessizce anlamsız kalırdı.

- İkinci sınır: Değer Excel'in 1.048.575 satırlık tavanının üstüne çıkamaz, çıkarılırsa tavanda uygulanır. Aksi halde tavan ile eşik arasında kalan sonuçlar CSV'ye gitmez, Excel'e yazılmaya çalışılır ve dosya yazımının en sonunda başarısız olurdu.

- Kontrol ayarı mı: Hayır.

QrExcelAutoFitMaxRows

- Ne işe yarar: Excel dosyasında sütun genişliklerinin içeriğe göre ayarlanacağı en fazla satır sayısı.

- Değer: Satır sayısı.

- Varsayılan: 50000

- Örnek: 50000 iken 20.000 satırlık bir dosyada sütunlar içeriğe göre genişletilir; 200.000 satırlık bir dosyada bu adım atlanır ve sütunlar varsayılan genişlikte kalır.

- Neden eşik var: Genişlik ayarı yazı tipi ölçümü yapar ve ölçümde Excel yazım süresinin yaklaşık üçte birini tek başına harcamıştır. Yalnızca görünümü etkiler, verinin kendisini değiştirmez.

- Kontrol ayarı mı: Hayır.

7.8 Hassas Veri grubu

QrMaskingEnabled

- Ne işe yarar: Maskeleyen ana anahtarı.

- Değer: true / false

- Varsayılan: true

- Kapatılırsa: Hiç tespit ve maskeleye yapılmaz. Ancak her teslim yine kayda yazılır ve uygulanan politika MaskingOff görünür. Denetçinin "maskeleye kapalıyken gönderilmiş sonuç" durumunu görebildiği tek yer burasıdır.

- Kontrol ayarı mı: Evet.

QrSensitiveDataPolicy

- Ne işe yarar: Maskeleye açıkken davranış.

- Değerler:

- AutoMask: Tespit edilen hassas kolonlar maskelenir. Onaylı istisnalar açık kalır.

- WarnOnly: Hiçbir şey maskelenmez, tespit sonucu yalnızca kayda yazılır.

- Varsayılan: AutoMask

- Örnek: WarnOnly, yeni kurulumda desenlerin doğru çalışıp çalışmadığını görmek için kısa süreli kullanılır. Kalıcı kullanımı korumayı ortadan kaldırır.

- Bilinmeyen bir değer yazılırsa: Güvenli tarafta kalınır, maskeleye uygulanır.

- Kontrol ayarı mı: Evet.

QrSensitiveDetectionSampleSize

- Ne işe yarar: Her kolondan kaç satır örnek alınıp desen taraması yapılacağı.

- Varsayılan: 1000

- Örnek: 1000 iken 500 bin satırlık bir sonuçta her kolondan 1000 hücre incelenir. Sayıyı büyütmek doğruluğu artırır, süreyi uzatır.

- Kontrol ayarı mı: Evet.

QrSensitiveDetectionThresholdPct

- Ne işe yarar: Örneklenen hücrelerin yüzde kaçını eşleşirse kolon hassas sayılır.

- Değer: 0-100 arası sayı.

- Varsayılan: 20

- Örnek: 1000 satır örneklenip eşik 20 iken, 200 hücrede kimlik numarası deseni bulunursa kolon hassas kabul edilir ve maskelenir. 150 hücrede bulunursa kabul edilmez.

- Düşürülürse: Daha çok kolon maskelenir, yanlış pozitif artar.

- Yükseltirirse: Daha az kolon maskelenir, kaçırma riski artar.

- Kontrol ayarı mı: Evet.

QrSensitiveDetectionSampleMode

- Ne işe yarar: Örnek satırların nasıl seçileceği.

- Değerler: Random, Sequential

- Varsayılan: Random

- Örnek: Sıralı veride ilk 1000 satır aynı bölgeye ait olabilir ve temsil etmeyebilir. Random tüm sonuca yayılmış seçim yapar.

- Kontrol ayarı mı: Evet.

QrSensitiveDetectionTimeBudgetSeconds

- Ne işe yarar: Tüm tespit turunun toplam süre bütçesi.

- Varsayılan: 10

- Bütçe aşılsa: Kalan kolonlar "taranmadı" olarak işaretlenir ve maskelenir. Güvenli taraf her zaman kazanır.

- 0 ise: Sınır yoktur.

- Kontrol ayarı mı: Evet.

QrColumnPreviewEnabled

- Ne işe yarar: Sorgu sonucu talebi kaydedilirken hedef sunucudan kolon listesi alınsın mı.

- Varsayılan: true

- Ne yapar: Sorguyu çalıştırmaz. Yalnızca "bu sorgu hangi kolonları döndürür" diye sorar, tek satır veri okumaz.

- Neden önemlidir: Önizleme, takma ad (alias) kullanılan kolonların gerçek kaynağını öğrenir. SELECT TCKN AS Kod yazıldığında kolon adı Kod görünür ama kaynak kolon TCKN'dir. Bu bilgi olmadan maskeleyme atlatılabilirdi.

- Sunucu cevap veremezse: Talep yine kaydedilir.

UnmaskedColumnRequestPolicy

- Ne işe yarar: Kullanıcı belirli kolonların maskelenmeden gelmesini isteyebilir mi.

- Değerler:

- RequireApproval: İstenen kolonlar listelenir, ayrı bir onay adımı eklenir. Onaylanan kolonlar maskelenmez.

- AllowWithReason: Ek onay adımı yoktur, gerekçe yazılır ve otomatik onaylı sayılır.

- Disabled: Özellik kapalıdır, editörde ilgili alanlar gizlenir ve varsa liste temizlenir.

- Varsayılan: RequireApproval

- Kontrol ayarı mı: Evet.

- Bağımlılık: QrMaskingEnabled kapalıysa bu ayar Disabled gibi davranır. Maskelenecek bir şey yokken maskesiz isteme onayı istemek, onay mekanizmasını lastik damgaya çevirirdi.

UnmaskedColumnApproverRole

- Ne işe yarar: Maskesiz kolon isteğini kim onaylar.

- Varsayılan: SystemManager

- Kontrol ayarı mı: Evet.

7.9 E-posta Onayı grubu

QrEmailApprovalPolicy

- Ne işe yarar: Sorgu sonucunun gönderileceği e-posta adresleri onaydan geçsin mi.

- Değerler: RequireApproval, Disabled

- Varsayılan: RequireApproval

- Örnek: RequireApproval iken daha önce onaylanmamış bir adrese sonuç göndermek istendiğinde talebe ek bir onay adımı eklenir. Amaç, canlı verinin kurum dışı bir adrese sessizce gitmesini engellemektir.

- Kontrol ayarı mı: Evet.

QrEmailApproverRole

- Ne işe yarar: E-posta adresi onayını kim verir.

- Varsayılan: ChangeManager

- Kontrol ayarı mı: Evet.

QrEmailAutoApproveUsers

- Ne işe yarar: Sistemde kayıtlı kullanıcılara ait adresler otomatik onaylı sayılsın mı.

- Değerler: True / False

- Varsayılan: True

- Örnek: True iken bir kullanıcının kendi kurumsal adresine sonuç göndermesi ek onay istemez; kurum dışı bir adres eklerse onay adımı devreye girer.

- Kontrol ayarı mı: Evet.

7.10 Parametre değişikliği ne zaman devreye girer

Durum	Davranış
Yeni açılan talepler	Yeni değer hemen geçerlidir.
Onay akışı henüz kurulmamış talepler	Yeni değer geçerlidir.
Onay akışı kurulmuş talepler	Görevler ayrılığı ayarları talebe dondurulmuştur, eski değerlerle devam eder.
Tamamlanmış talepler	Etkilenmez.
Maskeleme tespit ayarları	Her teslimde o anki değerler kullanılır ve kayda dondurulur.

7.11 SIEM grubu

Bu grup, yönetim olaylarının SOC toplayıcısına gönderilme kapsamını belirler. Bağlantı bilgisi burada değil appsettings dosyasındadır (Bölüm 2.4.10); bu ekranda yalnızca neyin gideceği yönetilir.

Dördü de kontrol ayarıdır. Sebebi açıktır: bunların değişmesi, kurumun kendini SOC'tan gizleyebileceği tek yoldur. Akışı kapatmak, eşiği yükseltmek veya ana anahtarı kapatmak, dışarıdan görünen izi susturur. Betik metni bayrağı ise ters yönde bir kontroldür; açılması iş verisinin SOC'a çıkmasına yol açabilir. İkisi de aynı listeye girer, çünkü ikisi de neyin dışarı çıktığını belirler.

Parametre	Ne işe yarar ve ne girilir	Varsayılan
SiemEnabled	Ana anahtar. Kapalıyken hiçbir olay gönderilmez. Kurulumda açık (true) gelir. Gönderim için appsettings içinde en az bir uç tanımlı olmalıdır (Bölüm 2.4.10); uç tanımlı değilse Yönetişim Kurulum Kontrolü ekranı bunu eksik olarak gösterir.	true
SiemStreams	Gönderilecek akışlar, noktalı virgülle ayrılır. Dört akış vardır: Audit denetim izidir, Anchor defter özeti olaylarıdır (özet yayımı, özet hatası, geri yükleme, çatal), AppLog ürünün kendi günlüğüdür, Heartbeat nabızdır. Boş bırakılırsa dördü de gönderilir. Örnek bir daraltma: Audit;Anchor;Heartbeat	Audit;Anchor;AppLog;Heartbeat
SiemMinSeverity	Bu ciddiyetin altındaki olaylar gönderilmez. Info, Notice, Warning, Error ve Alert değerlerinden biri girilir. SIEM	Notice

Parametre	Ne işe yarar ve ne girilir	Varsayılan
	lisansları hacme göre fiyatlandığı için kapsamı daraltmak meşrudur; ancak beş sınıf olay bu eşikten etkilenmez ve her koşulda gönderilir (aşağıda).	
SiemIncludeScriptText	Betiğin tam metni SOC'a gitsin mi. Varsayılan kapalıdır, çünkü bir betik iş verisi içerebilir. Kapalıyken yalnız betiğin özeti gönderilir; özet, betiğin onaylanan metinle aynı metin olduğunu göstermeye yeter. Açmadan önce SOC'un veri sınıflandırma kurallarını kontrol edin.	false

Eşikle susturulamayan olaylar

SiemMinSeverity ne olursa olsun aşağıdaki beş sınıf gönderilir. İlk dördü, risk modelindeki asla atlanamaz (NeverSkip) kuralının SOC tarafındaki karşılığıdır.

Acil müdahale olayları. Acil durum geçersiz kılma, adım atlama ve benzeri hareketler. Onayı kaldırmaz, kısaltır; izi kalmalıdır.

Yetki reddi ve başarısız kimlik doğrulama. Reddedilen bir işlem, izin verilen bir işlem kadar önemlidir; saldırı belirtisi çoğu zaman reddedilen isteklerde görünür.

Kontrol zayıflatma olayları. Onay politikası, SQL standardı, kritik nesne listesi, parametre, rol, sunucu, lisans ve ayar onayı değişiklikleri ile kullanıcı açma, silme, rol değiştirme ve oturum iptali. SOC için en değerli olaylar bunlardır, çünkü ürünün içinden bakıldığında olağan görünürler.

Defter özeti olayları. Özet yayımı, özet hatası, geri yükleme ve çatal. Kanıtın dış tanığıdır ve hacmi saatte birkaç mesajdır; düşük ciddiyette olsalar bile atlanamazlar. Geri yükleme ve çatal ayrıca alarm seviyesindedir.

Nabız. Ciddiyeti bilerek düşüktür, çünkü bir olay değil bir yaşam işaretidir ve SOC panosunda olayların arasında görünmemelidir. Eşikle susturulabilir olsaydı işe yaramazdı: varsayılan eşik

zaten nabız seviyesinin üstündedir, yani nabız hiçbir kurulumda gönderilmezdi. Nabız kapatmanın meşru yolu SiemStreams parametresinden Heartbeat akışını çıkarmaktır; o yol denetim izine düşer ve SOC'a duyurulur, yani kapatma görünür olur.

Kapsam daraltması SOC'a duyurulur

Bu dört parametreden biri değiştiğinde, değişiklik yürürlüğe girmeden önceki yapılandırmayla SOC'a ayrı bir olay gönderilir. Sıra böyle olmak zorundadır: yeni yapılandırmayla duyurulsaydı, akışı kapatan bir değişiklik kendi duyurusunu da susturabilirdi.

Dört göz kuralı açıkken bu akış bozulmaz. Onay gerektiren değişiklik ilk kaydetmede uygulanmaz; onaylandığı anda uygulanır ve duyuru o anda çıkar.

Bölüm 8. Ayar Değişikliği Onayı (Dört Göz)

8.1 Ne işe yarar

Ayar ekranlarındaki değişikliklerin tek kişinin elinden çıkmamasını sağlar. Bir kullanıcı ayarı değiştirdiğinde değişiklik hemen uygulanmaz, bekleyen kayıt olarak saklanır ve başka bir kullanıcının onayını bekler.

Bu neden gereklidir: onay politikalarını, kritik nesne listesini veya maskeleye ayarını tek kişi kapatabiliyorsa, bütün kontrol sistemi o kişinin insafına kalmış demektir.

8.2 Kapsam

SettingsApprovalPolicy parametresi kapsamı belirler:

Değer	Kapsam
Disabled	Yakalama yoktur, her değişiklik anında uygulanır.
ControlSettingsOnly	Yalnızca bir kontrolü zayıflatan veya güçlendiren değişiklikler beklemeye düşer.
All	Kapsamdaki ekranlardaki her değişiklik beklemeye düşer.

Kapsamdaki ekranlar: sunucular, kullanıcılar, roller, parametreler, onay politikaları, SQL standartları, kritik nesneler, hassas kolonlar, hassas veri desenleri, aday kolonlar, e-posta kaynakları, bakım görevleri, ITSM biletleri.

Kontrol ayarı ne demektir

ControlSettingsOnly kapsamında beklemeye düşecek parametreler kod içinde sabit bir liste ile belirlenir. Bu liste veritabanında tutulmaz. Sebebi şudur: sınıflandırmanın kendisi düzenlenebilir olsaydı, biri önce parametreyi "kontrol değil" olarak işaretleyip sonra korumayı onaysız kapatabilirdi.

Kontrol ayarı sayılan parametreler:

SettingsApprovalPolicy, QrMaskingEnabled, QrSensitiveDataPolicy, QrSensitiveDetectionThresholdPct, QrSensitiveDetectionSampleSize, QrSensitiveDetectionSampleMode, QrSensitiveDetectionTimeBudgetSeconds, UnmaskedColumnRequestPolicy, UnmaskedColumnApproverRole, QrDeliveryMode, QrRequesterCanDownload, QrDownloadMinimumRole, QrFileRetentionDays, QrMaxRowCount, QrEmailApprovalPolicy, QrEmailApproverRole, QrEmailAutoApproveUsers, RequesterCanSelfApproveExecute, ApproverCanExecute, RequireDistinctApproverPerStep, EmergencyMinimumRole, RejectOnError, ChangeTicketRequired, EmergencyTicketRequired, ChangeTicketRegex, EmergencyTicketRegex, RequestTicketRegex, bütün ITSM entegrasyonu parametreleri (ItsmEnabled, ItsmVerifyOnSave, ItsmExecuteGate, ItsmEnforceWindow, ItsmVerifyIncident, ItsmQueryResultTicketKind, ItsmUnavailablePolicy, ItsmReadyStates, ItsmClosedStates, ItsmApprovedValues, ItsmWriteBackEnabled, ItsmWriteBackEvents), kurum beyanları (WorkerEndpointNetworkRestricted, TargetAccountDedicated, DamAllowlistMaintained) ve SIEM grubu (SiemEnabled, SiemStreams, SiemMinSeverity, SiemIncludeScriptText).

Ayrıca onay politikaları, SQL standartları, kritik nesneler, hassas kolonlar ve desenler ile sunucu kontrol bayrakları da her zaman kontrol değişikliği sayılır.

8.3 Akış

Kullanıcı ayarı değiştirir ve kaydeder

|

v

Politika Disabled mi? ---evet---> Degisiklik ANINDA uygulanir

| hayir

v

ControlSettingsOnly ve degisiklik kontrol degil mi? ---evet---> ANINDA uygulanir

| hayir

v

Kullanıcının o ekran yetkisi var mi? ---hayir---> Handler kendi hatasini verir

| evet

v

Onaylayacak baska kimse var mi? ---hayir---> ANINDA uygulanir (uyari gunluge yazilir)

| evet

v

Aynı kayıt için bekleyen talep var mi? ---evet---> HATA: zaten bekleyen bir talep var

| hayir

v

Bekleyen kayıt oluşturulur

Canlı kayda DOKUNULMAZ, eski değer yururlukte kalır

Denetim kaydına "SettingChange.Requested" yazılır

|

v

Baska bir kullanıcı onaylar veya reddeder

|

+-----+

|

ONAY

|

RED

|

Komut aynen tekrar oynatılır

Hicbir şey uygulanmaz

(doğrulamalar, lisans limiti,
eşzamanlılık kontrolü dahil)

Istenen değerler denetim
kaydında kalır

|

Basarili -> Approved

|

Rejected

Basarisiz -> Failed

8.4 Onayın komutu tekrar oynatması ne demektir

Onay verildiğinde sistem, kullanıcının başlangıçta gönderdiği komutu saklandığı yerden çıkarır ve aynen yeniden çalıştırır.

Bunun faydası: doğrulamalar, lisans limitleri, eşzamanlılık kontrolü ve denetim kaydı, ilk gönderimde nasıl çalışıyorsa onay anında da aynen çalışır. Bu mantık ikinci kez yazılmaz, dolayısıyla iki yol arasında fark oluşamaz.

Bunun bir sonucu vardır: onay anında koşullar değişmişse komut başarısız olabilir. Örneğin sunucu limiti bu arada dolmuşsa onay "Failed" olarak kapanır ve sebebi kayda yazılır.

Kayıt üzerindeki oluşturan ve değiştiren alanları talep edene yazılır, çünkü değişiklik onun eseridir. Onaylayanın izi ayrı alanda ve denetim kaydında tutulur.

8.5 Kim onaylar

Ayrı bir "ayar onaylayıcısı" rolü yoktur. Onaylayan kişi o ekranın kendi yetkisine sahip olmalıdır. Sunucu değişikliğini sunucu yetkisi olan biri onaylar.

Değişmez kural: Kimse kendi talebini onaylayamaz veya reddedemez. Bu kural politikadan bağımsız olarak her zaman geçerlidir.

8.6 Kilitlenme kapağı

Bir ekranın yetkisine yalnızca tek kişi sahipse, o kişinin yaptığı değişikliği onaylayacak kimse yoktur ve değişiklik sonsuza kadar bekler. Bu durumda sistem değişikliği doğrudan uygular ve günlüğe uyarı yazar.

Bu bilinçli bir tercihtir: kural zaten uygulanamıyorsa sistemi kilitlemek yerine durumu görünür kılmak daha doğrudur. Kalıcı çözüm, her ekran yetkisine en az iki kullanıcı atamaktır.

Aynı sebeple kullanıcı silme işlemi de bu durumu kontrol eder ve son ikinci yetkiliyi silmeyi engeller.

8.7 Ayar Onayları ekranı

Ekran: Ayarlar > Ayar Onayları

Kolon	Ne gösterir
Ekran	Hangi ekrana ait değişiklik (sunucu, parametre, politika vb.).
İşlem	Ekleme, güncelleme veya silme.
Kayıt	Değişikliğin okunabilir özeti; özet yoksa değiştirilecek kaydın anahtarı.
Talep eden	Değişikliği isteyen kullanıcı.
Talep zamanı	İstek zamanı.
Durum	Bekliyor, Onaylandı, Reddedildi, Başarısız.
İşlemler	Satırın sonundaki Detay düğmesi. Mevcut değer ile istenen değeri yan yana açar.
Karar veren (ayrı sütun değildir)	Onaylayan veya reddeden kullanıcı. Durum sütununun altında, karar zamanıyla birlikte küçük yazıyla görünür.
Gerekçe (ayrı sütun değildir)	Red gerekçesi veya başarısızlık sebebi. Detay penceresinde görünür.

Satırın sonundaki Detay düğmesi mevcut değer ile istenen değeri yan yana gösterir. Listenin üstündeki düğmelerle Bekliyor, Onaylandı, Reddedildi ve Başarısız kayıtları arasında geçiş yapılır.

Reddetme işleminde gerekçe zorunludur.

8.8 Bu ekrandaki mesajlar

Mesaj	Sebebi	Ne yapmalı
Değişiklik onaya gönderildi	Kayıt beklemeye alındı.	Yetkili bir meslektaşınızdan onay isteyin.
Bu kayıt için zaten bekleyen bir değişiklik var	Aynı kayda ikinci bir istek gönderildi.	Önce mevcut isteği sonuçlandırın.

Mesaj	Sebep	Ne yapmalı
Bu talep zaten karara bağlanmış	Başka biri sizden önce onayladı veya reddetti.	Listeyi yenileyin.
Kendi talebinizi onaylayamazsınız	Dört göz kuralı.	Başka bir yetkiliye onaylatın.
Yetkiniz yok	O ekranın yetkisine sahip değilsiniz.	Yetki talep edin.
Değişiklik uygulanamadı	Onay anında komut hata verdi.	Gerekçeyi okuyun, sorunu giderip yeniden isteyin.

Bölüm 9. Kritik Nesneler, SQL Standartları ve Hassas Veri

9.1 Kritik Nesneler

Ekran: Ayarlar > Kritik Nesneler

Yetki: settings.critical

Ne işe yarar

Kurumun "bu nesneye dokunulursa özel dikkat gerekir" dediği veritabanı nesnelerinin listesidir. Örnek: müşteri tablosu, bakiye tablosu, yetkilendirme prosedürü.

Alanlar

Alan	Ne işe yarar	Zorunlu	Örnek
Veritabanı Adı	Nesnenin bulunduğu veritabanı. Boş bırakılabilir; boş bırakılırsa bütün veritabanları kapsanır.	Hayır	MusteriDB
Nesne Tipi	Tablo, prosedür, görünüm, fonksiyon, tetikleyici.	Evet	Table
Şema Adı	Nesnenin şeması. Boş bırakılabilir; boş bırakılırsa bütün şemalar kapsanır.	Hayır	dbo
Nesne Adı	Nesnenin adı.	Evet	Musteri
Erişim Kontrolü	Bu nesne üzerindeki yetki değişiklikleri izlensin mi.	-	Açık
Şema Değişikliği	Bu nesnenin yapısını değiştiren işlemler izlensin mi.	-	Açık

Eşleşme mantığı

Eşleşme dört alanın birlikte karşılaştırılmasıyla yapılır: veritabanı, nesne tipi, şema, nesne adı. Aynı dörtlü iki kez tanımlanamaz.

Karşılaştırma büyük-küçük harf duyarsızdır. dbo.Musteri ile DBO.MUSTERI aynı nesnedir.

Kritik nesne tespit edilince ne değişir

1. Talep ayrıştırıldığında ilgili ifade "kritik nesne" olarak işaretlenir. Talep detayındaki nesne tablosunda kritik sütunu işaretli görünür.

2. CriticalObjectDrop standardı devreye girebilir. Bu standardın önem derecesi Critical'dır ve "asla atlanamaz" işaretlidir.

3. Risk bandı Critical'a çıkar.

4. Onay politikasında bu standarda bağlı bir adım varsa o adım kilitlenir ve hiçbir kural ile atlanamaz.

5. Otomatik çalıştırma devre dışı kalır; talep onaylansa bile bir insanın çalıştır düğmesine basması gerekir.

Önemli kural: Kritiklik kararı talep ayrıştırıldığı anda kaydedilir. Kataloğu sonradan düzenlemeniz geçmiş talepleri yeniden yazmaz. Denetimde "o gün ne biliyorduk" sorusunun cevabı bu şekilde korunur.

9.2 SQL Standartları

Ekran: Ayarlar > SQL Standartları

Yetki: settings.standards

Ne işe yarar

Betiklerde aranan kuralların listesidir. Kurulumla birlikte 88 standart gelir. Her biri açılıp kapatılabilir, önem derecesi değiştirilebilir. İsimlendirme kuralları ifade biçimine göre ayrı satırlarda durur: CREATE, ALTER ve CREATE OR REPLACE için ayrı anahtarlar vardır. Bunlar tek bir kuralın parçalarıdır. Temel anahtar güncellediğinizde aktiflik, örnek ve önem derecesi diğer biçimlere de aktarılır; listede o satırlar hangi kuralı izlediklerini yazar. Bu birliktelik olmasaydı kural sessizce delinirdi: Oracle ve PostgreSQL sunucularında nesneler neredeyse her zaman CREATE OR REPLACE ile yazılır, yani yalnız CREATE biçimi açık olsaydı kural o sunucularda hiç uygulanmazdı.

Alanlar

Alan	Ne işe yarar	Değerler
Aktif	Kural çalışsın mı.	Açık / Kapalı
Standart Anahtarı	Kuralın sistem içindeki adı. Onay politikası adımları bu anahtara bağlanır.	Örnek: XpCmdShellUsage
Başlangıç metni	Bazı kurallarda aranan metin.	
Hata Mesajı	Kural tetiklendiğinde kullanıcıya gösterilen açıklama.	
Önem Derecesi (Tier)	Kuralın risk seviyesi.	0=Info, 1=Low, 2=Medium, 3=High, 4=Critical
Asla Atlanamaz (NeverSkip)	Tetiklenirse otomatik çalıştırma yapılmaz ve buna bağlı onay adımı atlanamaz.	Açık / Kapalı
Kayıd Engeller	Tetiklenirse talep hiç kaydedilemez.	Açık / Kapalı
Engellenen Talep Tipleri	Kuralın hangi talep tiplerinde kaydı engelleyeceği.	
Üst Sınır (MaxValue)	Sayısal kurallarda eşik değeri.	

Alan	Ne işe yarar	Değerler
Veritabanı Tipi	Kuralın hangi veritabanlarında geçerli olduğu. Noktalı virgülle ayrılır. Boş ise hepsi.	1;3 = SQL Server ve PostgreSQL

İhlalde ne olur

Üç farklı sonuç vardır:

Durum	Sonuç
Kural tetiklendi, "Kaydı Engeller" kapalı	Talep kaydedilir. Bulgu risk hesabına girer, bandı yükseltebilir.
Kural tetiklendi, "Kaydı Engeller" açık	Talep kaydedilmez. Kullanıcı hata mesajını görür ve betiği düzeltmek zorundadır.
Kural tetiklendi, "Asla Atlanamaz" açık	Talep kaydedilir, ancak otomatik çalıştırma yapılmaz ve ilgili onay adımı kilitlenir.

Örnek standartlar

Anahtar	Ne kontrol eder	Önem	Asla atlanamaz
CriticalObjectDrop	Kritik nesnenin silinmesi (DROP).	Critical	Evet
XpCmdShellUsage	xp_cmdshell çağrısı. İşletim sistemi komutu çalıştırır.	Critical	Evet
LinkedServerUsage	Dış veri kaynağı erişimi (bağlı sunucu, OPENROWSET, veritabanı bağlantısı).	High	Evet
DynamicSqlUsage	Dinamik SQL kullanımı. Enjeksiyon riski taşır ve çalışan sorgu denetimde görünmez.	High	Hayır
TempTableUsage	Geçici tablo kullanımı.	Medium	Hayır
WaitForDelayUsage	WAITFOR DELAY kullanımı. Bağlantıyı bloke eder.	Medium	Hayır
DeprecatedTypeUsage	Kullanımdan kaldırılmış veri tipleri.	Medium	Hayır

Anahtar	Ne kontrol eder	Önem	Asla atlanamaz
IdentityFunctionUsage	@@IDENTITY kullanımı. Tetikleyici zincirinde yanlış değer döndürebilir.	Medium	Hayır
RequireTryCatch	Prosedür gövdesinde hata yakalama bloğu yok.	Low	Hayır
PrintStatementInObject	Nesne gövdesinde PRINT ifadesi.	Low	Hayır
OrderByPosition	ORDER BY 1, 2 gibi konum bazlı sıralama.	Info	Hayır

Tam liste Ayarlar > SQL Standartları ekranındadır.

9.3 Hassas Veri Desenleri

Ekran: Ayarlar > Hassas Veri Desenleri

Yetki: settings.patterns

Ne işe yarar

Sorgu sonucundaki değerlerin içinde hassas veri arayan kurallardır. Kolon adına değil, değer kendisine bakar.

Alanlar

Alan	Ne işe yarar	Örnek
Ad	Desenin adı.	TCKN
Regex	Aranan biçim.	11 haneli sayı
Maskeleme Biçimi	Tam maskeleme veya kısmi maskeleme.	PartialMask
Sağda Bırakılacak Karakter	Kısmi maskelemede açık kalacak karakter sayısı.	4
Doğrulayıcı	Biçim eşleşmesinden sonra çalışan algoritma.	TcknChecksum, Luhn, IbanMod97
Sayısal Kolonlara Uygulanır	Sayı ve tarih kolonları da metne çevrilip taransın mı.	Kapalı
Kategori	Sektör veya konu etiketi.	Finance, Health
Yerleşik	Ürünle gelen desen mi.	
Etkin	Desen çalışsın mı.	

Doğrulayıcılar neden vardır

Yalnızca biçime bakmak yanlış pozitif üretir. 11 haneli her sayı kimlik numarası değildir; sipariş numarası da 11 hane olabilir.

Bu yüzden desen eşleşmesi tek başına yeterli değildir. Doğrulayıcı tanımlıysa algoritmanın da geçmesi gerekir:

Doğrulayıcı	Ne yapar
TcknChecksum	Kimlik numarasının kontrol basamağı hesabını doğrular.
Luhn	Kredi kartı numaralarında kullanılan kontrol algoritmasıdır.
IbanMod97	IBAN'ın 97'ye bölüm kontrolünü yapar.

Sonuç: 11 haneli bir sipariş numarası kimlik kontrolünden geçemez ve maskelenmez. Böylece hem gereksiz maskeleye hem de "bu kolonu açın" talepleri azalır.

Kısmi maskeleye örneği

PartialMask ve sağda 4 karakter ayarıyla 12345678901 değeri *8901 olarak görünür. Tam maskelemede değer tümüyle yıldızla değiştirilir.

9.4 Hassas Kolon Kataloğu

Ekran: Ayarlar > Hassas Kolonlar

Yetki: settings.qrsensitive

Ne işe yarar

Kolon adına göre çalışan sınıflandırma kataloğudur. Veri değerine bakılmaz; bu yüzden sınıflandırma yapmak için kimsenin ham veriyi görmesi gerekmez.

Alanlar

Alan	Ne işe yarar	Değerler
Kolon Adı	Aranan ad.	
Eşleşme Biçimi	Exact tam eşleşme, Contains içinde geçme, Regex düzenli ifade.	
Şema Adı	Kural yalnızca bu şemada geçerli olsun. Boş ise her şema.	
Tablo Adı	Kural yalnızca bu tabloda geçerli olsun. Boş ise her tablo.	

Alan	Ne işe yarar	Değerler
Veritabanı Tipi	Kural yalnızca bu türde geçerli olsun. Boş ise hepsi.	
Sınıflandırma	Denetçi etiketi.	KVKK-Kimlik, PCI-Kart
Maskeleme Biçimi	Tam veya kısmi. Boş ise tam maskeleme.	
Sağda Bırakılacak Karakter	Kısmi maskelemede.	
Aktif	Kural çalışsın mı.	

Aynı kolon adı farklı kapsamlarda tanımlanabilir. Tekillik kapsamla birlikte sağlanır.

Sunucunun maskeleme rejimi "Yalnız içerik" ise bu katalog o sunucu için devre dışı kalır; yalnızca desenler çalışır.

9.5 Aday Kolonlar (öğrenme döngüsü)

Ekran: Ayarlar > Aday Kolonlar

Yetki: settings.qrsensitive

Aday nasıl oluşur

Bir sorgu sonucunda desenle yakalanan ama katalogda olmayan bir kolon bulunursa aday kaydı oluşur veya var olan adayın görülme sayısı artar.

Bu tabloda hiçbir veri değeri tutulmaz. Yalnızca kolon adı, tablo adı, şema adı, sunucu adı ve eşleşen desenin adı saklanır.

Kolonlar

Kolon	Ne gösterir
Kolon Adı	Sonuçtaki kolon adı.
Kaynak Şema / Tablo / Kolon	Kolonun gerçek kaynağı. Takma ad kullanılmışsa asıl ad burada görünür.
Sunucu	Hangi sunucuda görüldü.
Tespit Edilen Desen	Hangi desen eşleşti.
Görülme Sayısı	Kaç teslimde karşılaşıldı. Sık görülenler üstte listelenir.
İlk / Son Görülme	Tarihler.
Durum	New karar bekliyor, Accepted kataloğa alındı, Ignored yok sayıldı.

Kolon	Ne gösterir
Karar veren / Karar zamanı	

Onaylanırsa ne olur

Aday kabul edildiğinde hassas kolon kataloğuna eklenir. Bundan sonra o kolon adına göre de yakalanır, yani değer desenine uymayan satırlarda bile maskelenir.

Bu döngü sayesinde katalog kullanıldıkça zenginleşir; kurumun kendi veri yapısını elle taramasına gerek kalmaz.

Bölüm 10. Onay Politikaları

Ekran: Ayarlar > Onay Politikaları

Yetki: settings.approvals

10.1 Politika nedir

Politika, "hangi durumda kimin onayı gerekir" sorusunun cevabını tutan kural setidir. Bir politikanın içinde sıralı adımlar vardır ve her adım bir rol ister.

Birden çok politika bulunmasının sebebi, farklı ortamların farklı sertlik gerektirmesidir. Canlı ortamda üç onay isterken test ortamında hiç onay istemeyebilirsiniz.

10.2 Politika alanları

Alan	Ne işe yarar	Boş bırakılırsa
Ad	Politikanın adı. Talebe kalıcı iz olarak yazılır.	Zorunlu
Açıklama	Serbest açıklama.	-
Aktif	Politika kullanımda mı.	Pasif politika hiç eşleşmez.
Acil Durum Politikası	Bu politika yalnızca acil durum talepleri için mi.	Kapalı ise yalnızca normal talepler eşleşir.
Talep sahibi kendi talebini onaylayabilir	Kurum varsayılanını bu politika kapsamında değiştirir.	Boş ise kurum parametresi kullanılır.
Onaylayan çalıştırabilir	Aynı şekilde.	Boş ise kurum parametresi kullanılır.
Her adım farklı onaylayan	Aynı şekilde.	Boş ise kurum parametresi kullanılır.

Önemli: Acil durum talebi yalnızca acil durum politikasına, normal talep yalnızca normal politikaya eşleşir. Bu iki küme birbirine karışmaz.

10.3 Politika eşleştirme (kapsam)

Politikalar doğrudan talebe bağlanmaz. Arada bir eşleştirme kaydı vardır ve bu kayıt kapsamı belirler:

Alan	Anlamı
Sunucu	Belirli bir sunucu. Boş ise sunucu bazlı değil.
Ortam	Production, Staging, Test, Development. Boş ise ortam bazlı değil.
Talep Tipi	Change, QueryResult, Rollback. Boş ise her tip.

Alan	Anlamı
Öncelik (Priority)	Aynı kapsamda birden çok politika varsa hangisinin önce deneneceği. Büyük sayı önce gelir.

Priority ne işe yarar

Aynı kapsam katmanında birden çok politika tanımlıysa, önce yüksek öncelikli olan denir. Eşitlik durumunda politika kimliği küçük olan önce gelir; bu, sonucun her zaman aynı çıkmasını sağlar.

Öncelik yalnızca aynı katman içinde karşılaştırılır. Farklı katmanlar arasında öncelik değil, özgüllük belirleyicidir.

10.4 Politika seçim akışı

Bu akış, talep kaydedildiğinde onay adımları oluşturulurken çalışır. Talebin her sunucusu için ayrı ayrı yürütülür.

Talebin her sunucusu için:

|

v

1. Bu sunucuya OZEL ve tam bu talep tipine ait esleme var mı?

evet -> adaylar bunlar, önceliğe göre sırala

hayır -> devam

v

2. Bu sunucuya OZEL ve tip belirtilmemiş esleme var mı?

evet -> adaylar bunlar

hayır -> devam

v

3. Sunucunun ORTAMINA ait ve tam bu talep tipine ait esleme var mı?

evet -> adaylar bunlar

hayır -> devam

v

4. Sunucunun ORTAMINA ait ve tip belirtilmemiş esleme var mı?

evet -> adaylar bunlar

hayır -> devam

v

5. GENEL (sunucu ve ortam belirtilmemiş) ve tam bu tipe ait esleme var mı?

evet -> adaylar bunlar

hayir -> devam

v

6. GENEL ve tip belirtilmemis esleme

|

v

Adaylar oncelik sirasiyla denenir.

Ilk "en az bir aktif adim ureten" aday kazanir.

|

v

Sunucular arasi karsilastirma:

- Once en kritik ORTAM kazanir (Production > Staging > Test > Development > tanimsiz)

- Ayni ortam seviyesinde daha COK aktif adim iceren kazanir

Birden çok politika eşleşirse ne olur

Yukarıdaki sıra tek bir katman seçer. O katmandaki adaylar öncelik sırasıyla denenir ve en az bir aktif adım üreten ilk aday kazanır.

Bu davranışın sebebi şudur: yüksek öncelikli bir politikanın adımları koşullara bağlı olabilir ve hiçbiri tetiklenmeyebilir. O politika kazansaydı, aslında onay isteyecek olan düşük öncelikli politika sessizce devre dışı kalırdı.

Hiçbiri eşleşmezse ne olur

Politikası olmayan bir sunucuya talep açılmaz. Kaydetme reddedilir ve hangi sunucunun kapsam dışında kaldığı hata mesajında yazar. Sebebi şudur: politika eşleşmezse onay adımı üretilmez, adımı olmayan bir talebi kimse onaylayamaz ve talep çıkışı olmayan bir duruma girerdi.

Geri alma talepleri bu kuralın dışındadır. Geri alma bir kurtarma işlemidir; politika kapsamı dışında kalsa bile kaydedilir, çünkü burada engellenirse kaynak değişikliğin onayı sırasında otomatik geri alma da üretilmez ve olay anında geri alınacak bir şey kalmaz. Politika eşleşmediğinde ürün kaynak değişikliğin onay gereksinimini yansıtır: değişikliği onaylamaya yetkili rol, geri almayı da onaylar.

Kurulum önerisi: En az bir genel politika tanımlayın. Aksi halde kapsam dışında kalan sunuculara hiç talep açılmaz.

Tüm adımlar atlanırsa ne olur

Politika eşleşti ama koşullar nedeniyle tüm adımlar atlandıysa talep yine otomatik onaylanır. Ancak bu durumda atlanan adımlar gerekçeleriyle birlikte kaydedilir. Talep detayında ve denetim dosyasında "hangi adım neden atlandı" görünür.

Bu iki durumu ayırt etmenin yolu: uygulanan politika adı doluysa politika eşleşmiş ama adımlar atlanmıştır, boşsa hiç politika eşleşmemiştir.

10.5 Adım alanları ve davranışları

Her politika adımı için aşağıdaki alanlar tanımlanır.

Alan	Ne işe yarar	Ne set edersen nasıl davranır
Sıra (StepOrder)	Adımın kaçınıcı sırada olduğu.	Adımlar bu sıraya göre oluşturulur. Aynı politikada aynı sıra iki kez kullanılamaz.
Adım Adı	Ekranda görünen ad.	Örnek: "Yönetici Onayı".
Onaylayan Rol	Adımı kapatabilecek en düşük rol.	DbAdmin yazarsanız DbAdmin ve üstü onaylayabilir.
Band En Az (TriggerIfBandAtLeast)	Risk bandı bu değere eşit veya üstündeyse adım devreye girer.	3 (High) yazarsanız adım yalnızca High ve Critical taleplerde çalışır.
Band En Fazla (SkipIfBandAtMost)	Risk bandı bu değere eşit veya altındaysa adım atlanır.	1 (Low) yazarsanız Info ve Low taleplerde adım atlanır.
Tetikleyen Standartlar (TriggerIfStandardKeys)	Bu standartlardan biri tetiklenmişse adım devreye girer. Noktalı virgülle ayrılır.	XpCmdShellUsage;LinkedServerUsage yazarsanız adım yalnızca bu bulgular varsa çalışır.
Talep Sahibi Rolü En Az (SkipIfRequesterRoleAtLeast)	Talebi açan kişinin rolü bu seviyede veya üstündeyse adım atlanır.	ChangeManager yazarsanız değişiklik yöneticisinin açtığı taleplerde bu adım atlanır.
Kilitli Adım (IsNonSkippable)	Adım hiçbir kural ile atlanamaz.	Açıksa band, rol ve diğer tüm atlama kuralları geçersizdir.

Adım nasıl karar verir

Bir adım için sıralı olarak şu kontroller yapılır:

1. Adım KILITLI mi (IsNonSkippable)?
evet -> ATLANMAZ, karar biter
2. Adımı tetikleyen bir standart NeverSkip
isaretili ve tetiklendi mi?
evet -> ATLANMAZ, karar biter
3. Adım bir TETIKLEME adımı mi
(standart anahtarı veya band esigi var)?
evet ve hicbiri eslesmedi -> ATLANIR ("kosul olusmadi")
evet ve eslesti -> asagidaki 5 ve 6 UYGULANMAZ
4. Talep sahibinin rolu esigi asiyor mu?
evet -> ATLANIR ("talep sahibi rolu")
5. Talep sahibinin rolu, adimin onaylayan

rolüne esit veya ustunde mi?	evet -> ATLANIR ("sahip rolu")
6. Band, atlama esiginin altinda mi?	evet -> ATLANIR ("dusuk band")
7. Hicbiri degilse	-> ADIM AKTIF, onay bekler

Dikkat edilmesi gereken nokta: 3. adımda koşulu eşleşen bir tetikleme adımı, 5 ve 6 numaralı kurallarla atlanamaz. Yani "yüksek riskte devreye gir" diye tanımlanmış bir adım, talep sahibinin rolü adımın onaylayan rolünü karşılıyor diye atlanmaz; aksi halde riskli işi yapan kişinin kıdemi kontrolü kaldırır. 4. kural (SkipIfRequesterRoleAtLeast) adımda açıkça tanımlandığı için tetiklenmiş adıma da uygulanır; kilitli adımlar bundan da etkilenmez. 4. ve 5. kurallar kişiye bağlıdır ve RequesterCanSelfApproveExecute kapalıyken hiç çalışmaz; aksi halde kendi talebini onaylayamayan kişinin talebi onay adımı kalmadan geçebilirdi.

Örnek politika

Bir üretim ortamı politikası şöyle kurulabilir:

Sıra	Adım Adı	Onaylayan Rol	Koşul	Kilitli
1	Takım Lideri Onayı	RequestManager	Band en fazla Info ise atla	Hayır
2	Veritabanı Yöneticisi Onayı	DbAdmin	Band en az Medium	Hayır
3	Değişiklik Yöneticisi Onayı	ChangeManager	Band en az High	Hayır
4	Güvenlik Onayı	SystemManager	XpCmdShellUsage;LinkedServerUsage tetiklenirse	Evet

Bu politikada:

- Info bandındaki bir talep hiç onay istemez, otomatik onaylanır.
- Medium bandındaki bir talep 1. ve 2. adımı ister.
- High bandındaki bir talep 1, 2 ve 3. adımı ister.
- İçinde xp_cmdshell geçen bir talep ayrıca 4. adımı ister ve bu adım hiçbir şekilde atlanamaz.

10.6 Görevler ayrılığı (SoD) kuralları

Üç ayar üç farklı soruyu cevaplar:

Ayar	Soru
RequesterCanSelfApproveExecute	Talebi açan kendi talebini onaylayabilir ve çalıştırabilir mi?
ApproverCanExecute	Onaylayan kişi aynı talebi çalıştırabilir mi?

Ayar	Soru
RequireDistinctApproverPerStep	Aynı kişi birden çok adımı kapatabilir mi?

Bunlar önce kurum parametresi olarak tanımlanır (Bölüm 7.4), sonra politika bazında değiştirilebilir. Politikada boş bırakılan alan kurum varsayılanını kullanır.

Dondurma kuralı: Onay akışı kurulurken etkin değerler talebe yazılır. Politika veya parametre sonradan değişse bile o talep girdiği kural setiyle değerlendirilir. Denetim dosyası o günün kuralını gösterir.

Rol atlama izi

Bir adım rol kuralı nedeniyle atlandığında adım kaydı silinmez; "atlandı" durumuyla ve gerekçesiyle saklanır. Karar veren olarak "System" yazılır. Böylece denetimde "bu adım neden hiç sorulmadı" sorusu cevaplanabilir.

10.7 Kilitlenme senaryoları

Senaryo	Sonuç	Çözüm
Adım DbAdmin istiyor, sistemde DbAdmin yok	Talep sonsuza kadar bekler.	Rolü olan kullanıcı ekleyin veya adımın rolünü düşürün.
RequireDistinctApproverPerStep açık, iki adım var, yalnızca bir yetkili kişi var	İkinci adım kapatılamaz.	İkinci yetkili ekleyin.
RequesterCanSelfApproveExecute kapalı, tek yetkili kişi hem talebi açıyor hem onaylıyor	Kendi talebini onaylayamaz.	Başka bir onaylayıcı ekleyin.
Acil durum politikası tanımlı değil	Acil durum seçeneği kullanılamaz.	Bkz. 10.8.

10.8 Acil durum uygunluğu

Bir talepte acil durum seçeneğinin görünmesi için:

- Seçili sunucuların hepsi için eşleşen bir acil durum politikası bulunmalı.
- Bu politikalarda en az bir kilitli adım olmalı.

İkinci şart bilinçlidir. Acil durum, onayı tamamen kaldırmak değil, kısaltmaktır. Hiç kilitli adım yoksa acil durum ilan etmek onay mekanizmasını tümüyle devre dışı bırakırdı ve bu bir yönetim boşluğu olurdu.

Ayrıca acil durum talebi açabilmek için kullanıcının rolü EmergencyMinimumRole eşliğini geçmelidir.

Bölüm 11. Değişiklik Talebi Uçtan Uca

11.1 Durum makinesi

Değer	Durum	Anlamı	Ölü mü
1	Pending	Onay bekliyor.	Hayır
2	Approved	Onaylandı, çalıştırılmayı bekliyor.	Hayır
3	Executed	Çalıştırıldı.	Evet
4	Rejected	Reddedildi.	Evet
5	Manual	Elle uygulandığı beyan edildi.	Evet
6	NoLongerNeeded	Artık gerekli değil.	Evet
7	Executing	Çalıştırma kuyruğunda bekliyor ya da Worker'da çalışıyor.	Hayır
8	ReconciliationRequired	Uzlaştırma bekliyor: çalıştırma hedefe ulaştı ama sonucu kesin bilinmiyor. Yeniden çalıştırılmaz; yetkili kişi hedefi kontrol edip sonucu işaretler.	Hayır

Ölü durum ne demektir: Talep aktif akıştan çıkmıştır. Worker onu almaz; talep düzenlenemez, onaylanamaz, çalıştırılmaz ve zamanlanamaz. Yapılabilecek az sayıdaki işlem (kopyalama gibi) Bölüm 11.5'teki tabloda yazar. Pending ya da Approved durumundaki talebi yalnız sahibi düzenleyebilir; onaylanmış talep yeniden kaydedilince onaylar sıfırlanır.

Geçiş matrisi

Mevcut durum	Yapılabilecek işlem	Yeni durum
Pending	Onayla (son adım kapanınca)	Approved
Pending	Reddet	Rejected
Pending	Manuel işaretle	Manual
Pending	Artık gerekli değil	NoLongerNeeded
Pending	Düzenle (yalnızca sahibi)	Pending
Approved	Çalıştır	Executing; sonra Executed. Hata halinde RejectOnError'a göre Rejected

Mevcut durum	Yapılabilecek işlem	Yeni durum
		(kurulum değeri) ya da Approved, sonuç belirsizse ReconciliationRequired
Approved	Zamanla	Approved (zamanlama bilgisi eklenir)
Approved	Zamanlamayı iptal et	Approved
Approved	Reddet	Rejected
Approved	Manuel işaretle	Manual
Approved	Artık gerekli değil	NoLongerNeeded
Executing	Çalıştırmayı iptal et	Approved
Executed	Tamamlandı işaretle	Executed (bilgi güncellenir)
Rejected, Manual, NoLongerNeeded	Hiçbiri	-
Executing	(kurtarma) Sonucu belirsiz deneme	ReconciliationRequired
ReconciliationRequired	Sonucu işaretle: değişiklik hedefte var	Executed
ReconciliationRequired	Sonucu işaretle: değişiklik hedefte yok	Approved

Çalıştırma hata verdiğinde ve hedefte her şey geri alındığında davranış RejectOnError parametresine bağlıdır: true ise Rejected, false ise Approved durumuna döner. Hedefte commit olmuş olabilecek her durumda (çalışan Worker kesildi, sonuç kaydedilemedi, betik ürünün transaction'ını kendisi bitirdi) talep reddedilmez ve Approved'a dönmez; Uzlaştırma Bekliyor (ReconciliationRequired) durumuna geçer. Bu durumdaki talep düzenlenemez, çalıştırılmaz, zamanlanamaz ve pakete giremez. Çalıştırma yetkisi olan kişi hedefi kontrol eder ve talep detayındaki Sonucu işaretle düğmesiyle "değişiklik hedefte var" (talep Çalıştırıldı olur, betik tekrar koşmaz) ya da "değişiklik hedefte yok" (talep Onaylandı olur) der; neyi kontrol ettiğini nota yazar. Karar, not ve karar anının oturum bilgisi denetim kaydına ChangeRequest.ReconciliationResolved olayıyla yazılır. Panodaki "Sonucu belirsiz çalıştırma" satırı bu talepleri sayar.

Kısmi sonuç: değişikliğin yalnız bir kısmı hedefteyse (örneğin ilk blok kalıcı oldu, sonraki bloklar çalışmadı) "değişiklik hedefte var, tamamı ya da bir kısmı" seçilir; çünkü talep tekrar çalışırsa hedefe ulaşmış kısım ikinci kez yazılır. Notta neyin uygulandığı ve neyin uygulanmadığı yazılır. Kalan iş, talep detayındaki "Kalan iş için yeni talep (kopyala)" düğmesiyle açılan yeni talepte gönderilir. Yeni talep onay, risk ve denetimden yeniden geçer ve ilk talebe bağlı kaydedilir: yeni talebin detayında "Kopyalandığı talep", ilk talebin detayında "Bu talepten kopyalanan talepler" görünür.

Karar verildikten sonra talep detayındaki Uzlaştırma Kaydı kutusu talebin neden uzlaştırmaya alındığını, verilen kararı, kararı veren kişiyi, zamanı ve hedefte neyin kontrol edildiğini gösterir. Bu bilgi kanıt defterinden okunur; denetim dosyasının Uzlaştırma bölümünde de aynı bilgi yer alır.

Oracle hedeflerde ek kontrol: Oracle'da her DDL ifadesi (CREATE, ALTER, DROP, TRUNCATE, GRANT gibi), betikteki bir COMMIT ve bir yordamın içindeki COMMIT o ana kadar yapılan veri değişikliklerini (INSERT, UPDATE, DELETE, MERGE) kalıcı yapar. Hata alınırsa SQL Change Guard'ın geri alması bu değişiklikleri geri getiremez. Bu yüzden ürün Oracle'da her bloktan önce ve sonra transaction kimliğini okur ve bir veri değişikliğinin kalıcı olup olmadığını izler.

Kalıcı olmuş bir veri değişikliğinden sonra hata gelirse ya da bir blok bekleyen veri değişiklikleriyle transaction'ı kendisi bitirirse (örneğin içinde COMMIT olan bir yordam) çalıştırma durur ve talep Uzlaştırma Bekliyor durumuna geçer. Talep tekrar çalıştırılmaz; tekrar çalışsaydı aynı veri ikinci kez yazılırdı. Betik bekleyen veri değişikliklerini ROLLBACK ile geri alırsa çalıştırma durur ve talep normal hatalı çalıştırma olarak kalır. Yalnızca DDL içeren bir betik hata verirse önceki DDL ifadeleri Oracle'ın kendi davranışı gereği kalıcıdır; çalıştırma günlüğü bunu yazar ve gerekiyorsa geri alma talebi kullanılır.

Sürüm paketinde aynı kural paketin ortak transaction'ı için geçerlidir: önceki bir talebin veri değişikliği kalıcı olduysa ve sonraki talep hata verirse, paketin o ana kadar çalışan talepleri ve hata veren talep uzlaştırmaya alınır. Kayıt sırasında OracleDmlBeforeImplicitCommit kuralı aynı betikte veri değişikliğinden sonra gelen DDL'i engeller; çalışma anındaki izleme betik metninden görülemeyen durumları (yordam içindeki COMMIT, dinamik SQL, paketteki talepler arası etki) yakalar. Bilinen sınır: PRAGMA AUTONOMOUS_TRANSACTION ile işaretli bir yordamın kendi COMMIT'i ürünün transaction'ına dokunmadığı için izlenemez.

11.2 Talep oluşturma ekranı

Ekran: Talepler > Yeni Talep

Yetki: cr.add

Alan	Ne işe yarar	Zorunlu	Notlar
Açıklama	Talebin ne yaptığının insan diliyle özeti.	Evet	Listelerde ve raporlarda görünür.
Talep Tipi	Change (değişiklik) veya QueryResult (sorgu sonucu).	Evet	Rollback tipi elle seçilmez, üretilir.
Sunucular	Hedef sunucu. Değişiklik ve geri alma talebinde tek sunucu seçilir; birden çok sunucu yalnız sorgu sonucu talebinde seçilebilir, çünkü	Evet	Bkz. Bölüm 6.6.

Alan	Ne işe yarar	Zorunlu	Notlar
	sunucular arasında dağıtık transaction yoktur.		
Bilet Numarası	ITSM bilet numarası.	ChangeTicketRequired parametresine bağlı	Biçim kontrolü ChangeTicketRegex ile yapılır; veri çıkarma talebinde RequestTicketRegex tanımlıysa o uygulanır. ITSM açıksa numara ITSM'de doğrulanır (Bölüm 22).
Sorgu Zaman Aşımı	Betiğin en fazla ne kadar çalışabileceği.	-	Alt sınır DefaultQueryTimeout, üst sınır MaxQueryTimeout.
Betikler	Bir veya daha çok SQL metni.	Evet	Her betiğin adı ve sırası vardır.
Acil Durum	Acil durum talebi mi.	-	Görünmesi için Bölüm 10.8 şartları gerekir.
Acil Durum Gerekçesi	Acil durum seçildiyse zorunlu yazılı gerekçe.	Koşullu	
Acil Durum Bileti	Acil durum kaydının bilet numarası.	Koşullu	
İstenen Çalıştırma Tarihi	Talebin ne zaman çalışmasını istediğiniz.	-	Otomatik zamanlamada kullanılır.
Gecikme (dakika)	Onaydan sonra kaç dakika beklensin.	-	Tarih verilmediyse kullanılır.

Sorgu sonucu talepleri için ek alanlar Bölüm 13'te anlatılır.

Ön koşul: sunucunun onay politikası olmalı

Bir talep açılabilmesi için seçilen sunucunun, o talep tipi için bir onay politikasının kapsamında olması gerekir. Kapsam dışı bir sunucu seçilirse talep kaydedilmez ve şu hatayı alırsınız: bu sunucu için tanımlı bir onay politikası yok, önce Ayarlar > Onay Politikaları ekranından bir politika eşleştirilmelidir.

Kuralın sebebi şudur: politika eşleşmediğinde talep hiç onay adımı üretmez. Onay adımı olmayan bir talebi kimse onaylayamaz, çünkü sorun kullanıcının rolünde değil ortada onaylanacak bir

adım olmamasındadır. En yetkili kullanıcı bile onaylayamaz. Böyle bir talep açıldığı anda çıkışı olmayan bir duruma girerdi; kural bunu kaynağında keser.

Çoklu sunucu yalnız sorgu sonucu talebinde seçilebilir. Böyle bir talepte sunucuların hepsi kapsanmış olmalıdır. Kapsanan bir sunucunun varlığı diğerlerini kurtarmaz: aksi halde kapsam dışı sunucu, kendisi için hiç yazılmamış bir politikaya binerek çalışır ve o sunucu için hiçbir onay kararı verilmemiş olurdu. Hata mesajı eksik olan sunucuların adını yazar, aramanız gerekmez.

Bu bir kerelik bir kurulum işidir. Politika bir sunucuya (ya da o sunucunun bulunduğu ortama, ya da genel olarak) bağlandıktan sonra o yol kalıcı olarak çözülmüş olur. Hangi sunucuların kapsam dışında olduğunu tek bakışta görmek için Ayarlar > Tanılama ekranındaki Politikaya bağlanmamış aktif sunucular satırına bakabilirsiniz; o satır sıfır gösterdiğinde hiçbir sunucu bu kurala takılmaz.

İki durum bu kuralın dışındadır. Acil talepler ayrı bir kontrolden geçer: acil bir talep açılabilmesi için seçilen sunucuya bir acil durum politikası bağlı olmalıdır, aksi halde acil ilan edilemez. Geri alma talepleri ise hiç engellenmez. Geri alma bir kurtarma işlemidir; politikası olmadığı için engellenseydi, bir olay sırasında geri alınacak bir şey kalmazdı. Otomatik geri alma üretimi de aynı kaydetme yolundan geçtiği için bu muafiyet olmasaydı geri alma betiği sessizce üretilmezdi.

Bir talep açıldıktan sonra politika bağlaması kaldırılırsa o talep etkilenmez, ancak aynı sunucuya yeni bir talep açılmaz. Bağlamayı kaldırmadan önce o sunucuda bekleyen talep olup olmadığına bakmanız iyi olur.

11.3 Betik editörü ve ayrıştırma

Ayrıştırma ne zaman çalışır

Betik yazıldıktan sonra ayrıştırma tetiklenir ve talep kaydedilirken tekrar çalışır. Kaydetme anındaki sonuç kalıcı olarak saklanır.

Ayrıştırma neyi üretir

Üretilen bilgi	Açıklama
Nesne listesi	Betiğin dokunduğu her nesne: veritabanı, şema, ad, tip.
İşlem türü	CREATE, ALTER, DROP, INSERT, UPDATE, DELETE, GRANT gibi.
Bulgu listesi	Tetiklenen SQL standartları, önem dereceleriyle.
Kritik nesne işareti	Dokunulan nesne katalogda var mı.
Risk bandı	Tüm bulguların değerlendirilmesiyle.

Ayrıştırma hatası

Betik çözümlenemezse (sözdizimi hatası veya desteklenmeyen yapı) bulgu listesinde ayrıştırma hatası olarak görünür. Bu durumda:

- Söz dizimi hatası kaydı her zaman durdurur. Diğer hata düzeyindeki bulgularda talep, kullanıcı ikinci kayıta bunu onaylarsa kaydedilir ve ChangeRequest.ParseErrorsConfirmed olayı yazılır. Kaydı engelleyen standartlar bu onayla da geçilemez.
- Nesne listesi boş kalabilir.
- Onay adımlarında standart anahtarına bağlı tetikleyiciler çalışmaz, çünkü hangi kuralın tetiklendiği bilinemez. Bu durumda daha temkinli davranmak için band bazlı adımlar kullanmanız önerilir.

Etkilenen nesneler ve fark karşılaştırması

Ayrıştırma bittiğinde alt panelde iki sekme görünür: Ayrıştırma Sonuçları ve Etkilenen Nesneler. İkinci sekme betiğin dokunduğu her nesneyi satır satır listeler: nesne adı, ifade türü, şema, veritabanı ve nesnenin geldiği betik dosyası.

Her satırın sonundaki Fark Göster düğmesi, nesnenin hedef sunucudaki GÜNCEL hâli ile betikteki hâlini yan yana açar. Amaç tek bir soruyu cevaplamaktır: bu talep uygulanmadan önce sunucuda ne var.

Pencerede sol taraf sunucudaki tanımdır, sağ taraf betikten gelen karşılığıdır. Üst çubuktan sunucu değiştirebilirsiniz; liste yalnız talebin veritabanı türündeki aktif sunucuları gösterir, çünkü başka türdeki bir sunucuda aynı nesne aranamaz.

Nesne türüne göre sol tarafta ne görüldüğü şöyledir:

- Prosedür, fonksiyon, görünüm, tetikleyici: nesnenin sunucudaki kaynak metni.
- Tablo: sunucudaki kolonlardan, kısıtlardan ve index'lerden üretilen CREATE TABLE betiği. Tabloda saklanan hazır bir kaynak metin yoktur, bu yüzden tanım üretilir.

Sağ tarafta ne görüldüğü, betiğin ne yaptığına bağlıdır. CREATE ya da ALTER PROCEDURE gibi ifadelerde betik nesnenin yeni tam hâlidir; satır satır karşılaştırma doğrudan anlamlıdır. ALTER TABLE ADD COLUMN gibi ifadelerde ise betik yalnız yapılacak değişikliği içerir; bu durumda sağ tarafın başlığı ifade olduğunu söyler ve satır satır fark beklenmez. Sol taraf yine işe yarar: kolonun zaten var olup olmadığını, tipini ve kısıtları gösterir.

Nesne sunucuda yoksa bu bir hata değildir: yeni oluşturulan bir nesne olabilir. Bu durumda sol taraf boş kalır ve pencerede Sunucuda yok bilgisi görünür.

Betikte veritabanı adı belirtilmemişse (SQL Server tarafında USE ifadesi yoksa) ürün nesneyi sunucudaki veritabanlarında arar. Hangi veritabanının kullanıldığını görebilmeniz için sol sütun

başlığında veritabanı bilgisi yazar. Aynı adlı nesne birden fazla yerde olabileceği için, hangi veritabanında çalışacağı önemliyse betiğe USE ifadesini yazmanız önerilir.

Şema adı yazılmadığında da benzer bir belirsizlik oluşur. Ürün önce bağlanılan kullanıcının kendi şemasını dener (PostgreSQL tarafında arama yolunun ilki, Oracle tarafında oturumun şeması); yine de kesinlik için şemayı betikte yazmak en doğrusudur.

Karşılaştırma yapılamayan tek durum, ayrıştırıcının o satır için betik bloğunu çıkaramamasıdır. O satırda düğme kapalı gelir ve üzerine gelindiğinde sebebi yazar.

Nasıl kontrol edilir: Sunucuda var olan bir prosedürü değiştiren bir betik yazın (ALTER PROCEDURE), ayrıştırmayı çalıştırın, Etkilenen Nesneler sekmesinden Fark Göster deyin. Solda sunucudaki mevcut gövde, sağda sizin yazdığınız gövde görünür ve değişen satırlar işaretlenir. Aynı denemeyi var olan bir tabloya kolon ekleyen bir betikle tekrarlayın: solda tablonun bugünkü CREATE TABLE karşılığı görünür.

11.4 Talep detay ekranı

Ekran: Talepler > (bir talep seçilir)

Üst bilgi alanları

Alan	Ne gösterir
Talep numarası	Kaydın kimliği.
Açıklama	Talep açıklaması.
Durum	Bölüm 11.1'deki durumlardan biri.
Talep tipi	Change, QueryResult veya Rollback.
Risk bandı	Bölüm 12.
Sunucular	Noktalı virgülle ayrılmış hedef listesi.
Bilet numarası	ITSM bileti.
Acil durum	Acil durum talebi ise işaret ve gerekçe.
Uygulanan politika	Onay akışı kurulurken eşleşen politika adı. Boş ise politika eşleşmemiştir.
Oluşturan / Oluşturma zamanı	
Çalıştırmayı başlatan / Zamanı	Düğmeye basan kişi. Otomatik zamanlamada SYSTEM.
Çalıştıran / Çalıştırma zamanı	İşi yürüten servis veya kullanıcı.
Etkilenen satır sayısı	Çalıştırma sonucunda değişen satır sayısı.

Betikler ve nesneler tablosu

Bu tablo kılavuzun en çok sorulan kolonlarını içerir.

Kolon	Ne gösterir	Nasıl hesaplanır	Örnek
Betik	Hangi betiğe ait.	Betiğin adı.	01_tablo_ekle.sql
Şema	Nesnenin şeması.	Ayrıştırımdan.	dbo
Nesne Adı	Dokunulan nesne.	Ayrıştırımdan.	Musteri
Nesne Tipi (Object Type)	Nesnenin türü.	Ayrıştırımdan.	Table, Procedure, View
İşlem (Operation)	Nesneye yapılan işlem.	Ayrıştırımdan.	ALTER, DROP, INSERT
İfade (Statement)	Betikteki ilgili SQL parçası veya satır bilgisi.	Ayrıştırımdan, satır ve sütun numarasıyla.	satır 12
Kritik Nesne (Critical Object)	Bu nesne kritik nesne kataloğunda mı.	Talep ayrıştırıldığı anda katalogla karşılaştırılır ve karar kaydedilir. Katalog sonradan değişse bile bu işaret değişmez.	İşaretli / Boş
Riskli İşlem (Risky Operation)	Nesneye yapılan işlem yıkıcı mı.	İşlem DROP ya da TRUNCATE ise riskli sayılır. Standart bulgularından ve önem derecesinden bağımsızdır.	İşaretli / Boş
Mesaj	Tetiklenen standardın açıklaması.	Standart tanımındaki hata mesajı.	"Dinamik SQL kullanımı tespit edildi."
Önem	Bulgunun risk seviyesi.	Standart tanımındaki Tier.	High

Critical Object ve Risky Operation farkı:

- Critical Object, *neye* dokunulduğu ile ilgilidir. Kurum o nesneyi önemli ilan etmiştir.
- Risky Operation, *ne yapıldığı* ile ilgilidir. İşlem doğası gereği yıkıcıdır (DROP, TRUNCATE).

Bir talep sıradan bir tabloya tehlikeli bir işlem yapıyorsa Risky Operation işaretli, Critical Object boş olur. Kritik bir tabloya zararsız bir SELECT yapıyorsa tersi olur. İkisi birden işaretliyse talep en yüksek dikkati hak eder.

Onay adımları tablosu

Kolon	Ne gösterir
Sıra	Adımın sırası.
Adım Adı	Politikadan gelen ad.

Kolon	Ne gösterir
Gereken Rol	Adımı kapatabilecek en düşük rol.
Durum	Bekliyor, Onaylandı, Reddedildi, Atlandı.
Karar Veren	Adımı kapatan kullanıcı. Atlanan adımlarda "System".
Karar Zamanı	
Açıklama / Gerekçe	Onay yorumu veya atlama gerekçesi.
Geçersiz Kılma	Adım acil durum yetkisiyle geçildiyse işaretlidir.
Atanan Kişi	Talep sahibinin doğrudan yöneticisi adım rolünü karşılıyorsa adım ona atanır.

Çalıştırma sonucu

Alan	Ne gösterir
Çalıştırma günlüğü	Hangi betiğin hangi bloğu çalıştı, kaç satır etkilendi, hata varsa hangi blokta oluştu.
Etkilenen satır	Toplam.
Hata mesajı	Varsa.
Kısmi çalıştırma uyarısı	Oracle hedeflerde, hata öncesi çalışan blokların geri alınmamış olabileceği uyarısı.

Denetim / olay listesi

Talebe ait denetim kayıtları burada listelenir: oluşturma, düzenleme, onay, red, zamanlama, çalıştırma, iptal.

11.5 Düğmeler ve aktiflik koşulları

Her düğme için iki farklı davranış vardır:

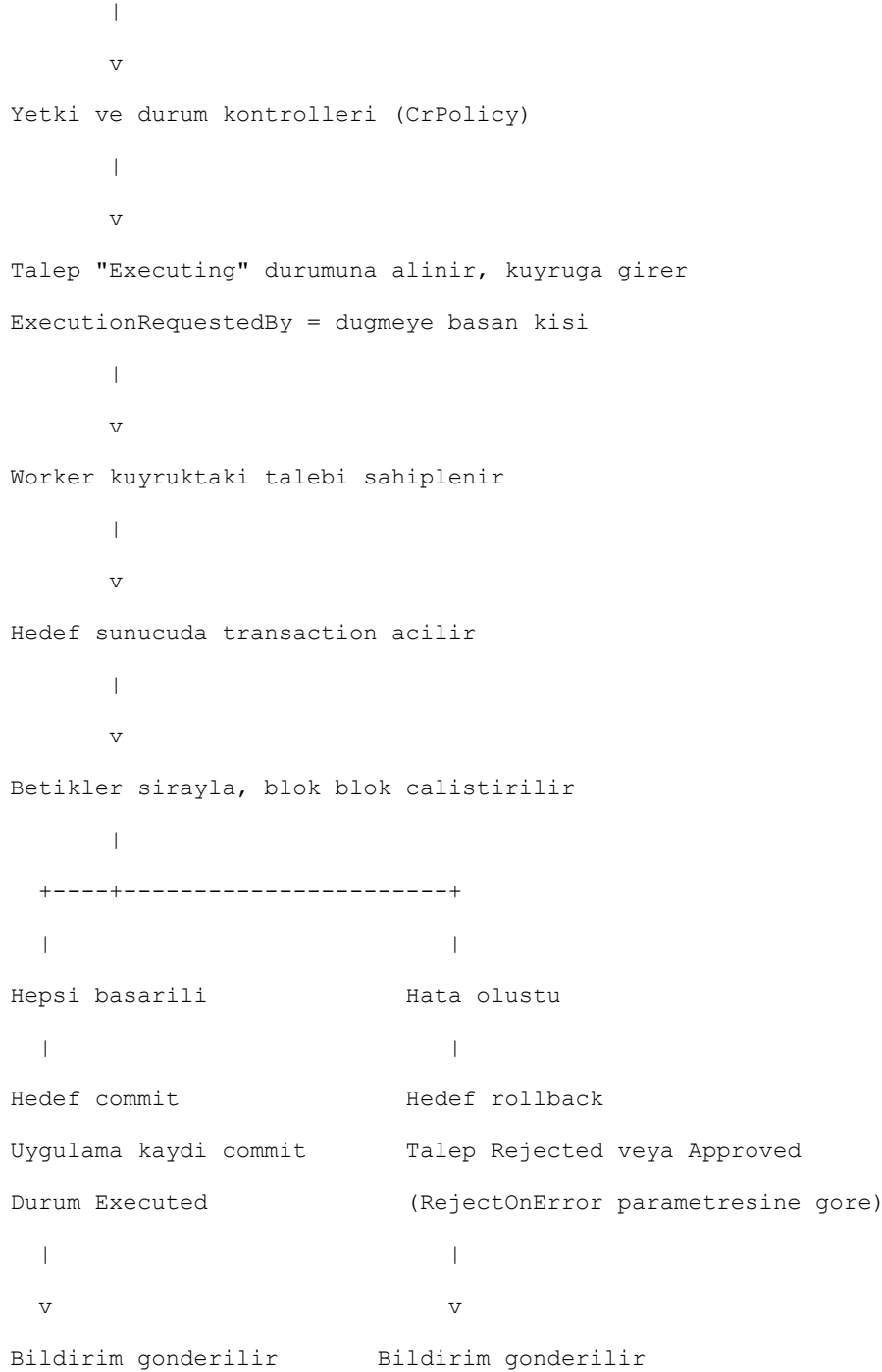
- Gizli: Kullanıcı bu işlemi hiçbir zaman yapamaz (rol yetkisi yok, talep tipi uygun değil, sahibi değil, modül lisanslı değil).
- Pasif (gri): Kullanıcı yapabilir ama şu anda yapılamaz (yanlış durum, aktif paket, kendi talebi, kaynak henüz uygulanmadı). Fare üzerine gelince sebep görünür.

Düğme	Görünme koşulu	Aktif olma koşulu
Düzenle	Talebin sahibi olmak	Talep ölü durumda değil, aktif pakette değil
Onayla	Onay yetkisi	Durum Pending, aktif pakette değil, kendi talebi değilse veya izin varsa, uygun bekleyen adım var
Reddet	Onay yetkisi	Durum Pending veya Approved
Çalıştır	Çalıştırma yetkisi, QueryGovernance kapalıysa QR için gizli	Durum Approved, aktif pakette değil, sunucu geri alma istiyorsa eksiksiz geri alma var, sunucu izole deneme istiyorsa güncel ve başarılı sandbox var, görevler ayrılığı kuralları engellemiyor
Zamanla	Onay yetkisi ve zamanlama modülü	Durum Approved; Çalıştır ile aynı geri alma, sandbox ve görevler ayrılığı koşulları
Zamanlamayı iptal et	Onay yetkisi	Durum Approved ve zamanlama var
Tamamlandı işaretle	Onay yetkisi	Durum Executed
Manuel işaretle	Onay yetkisi	Durum Pending veya Approved
Artık gerekli değil	Sahibi veya onay yetkisi	Durum Pending veya Approved
Geri alma üret	Talep tipi Change, sahibi, ekleme yetkisi, geri alma modülü	Ölü durumda değil (çalıştırma sırasında düşmüş talepler istisnadır), aktif geri alma yok
Kopyala	Ekleme yetkisi, talep tipi Rollback değil	Her zaman
Sandbox	Talep tipi Change, sandbox yetkisi ve modülü	Ölü durumda değil
Çalıştırmayı iptal et	Çalıştırma yetkisi	Durum Executing
Sonucu indir	QueryGovernance modülü, indirme kuralları	Sonuç dosyası var

Düğme ve arka uç tutarlılığı: Düğmenin aktif olup olmadığına karar veren kural ile arka ucun isteği kabul edip etmediğine karar veren kural aynı koddur. Bu, "düğme aktifti ama işlem hata verdi" durumunu büyük ölçüde önler. Onay zinciri, ITSM ve kanıt yazma sınırı gibi işlem anında yapılan kontroller ise düğme aktifken de işlemi durdurabilir; sebep mesajda yazar.

11.6 Çalıştırma akışı

Kullanıcı "Calistir" der



Zamanlanmış çalıştırma

Elle zamanlamada kullanıcı bir tarih seçer. Bu tarih en az ExecutionDelaySeconds kadar ileride olmalıdır (kurulum değeri 300 saniye; parametre daha küçük girilse de en az 30 saniye uygulanır). Zamanı gelince worker talebi alır.

Otomatik zamanlamada tarih sistem tarafından hesaplanır. Bkz. Bölüm 6.4.

Çalıştırmayı iptal etme

Talep çalışırken iptal istenebilir. Sistem iki saniyede bir iptal isteğini kontrol eder. İptal geldiğinde çalışan işlem durdurulur, hedefteki transaction geri alınır ve talep Approved durumuna döner. İptali kim isteyebilir: çalıştırma yetkisi olan her kullanıcıdır, çalıştırmayı başlatan kişi olma şartı yoktur. Bunun sebebi iptalin bir sahiplik işlemi değil, fren olmasıdır. Üretimde yanlış giden bir çalıştırmayı durdurmak, düğmeye basan kişinin o an başında olmasına bağlanamaz: o kişi toplantıda olabilir, oturumu düşmüş olabilir ya da yetkisi bu arada çekilmiş olabilir. Kendi talebini çalıştırma kısıtı da iptal için geçerli değildir; talep sahibi kendi talebini çalıştırmıyor olsa bile, çalıştırma yetkisi varsa çalışan bir işlemi durdurabilir. Hesap verebilirlik korunur, çünkü çalıştırmayı başlatan kişi ile iptali isteyen kişi ayrı ayrı tutulur ve ikisi de denetim kaydında görünür.

Çökme kurtarma

Worker servisi çalışma ortasında durursa talep Executing durumunda kalır. Bu talepler bir zaman eşiğine göre tespit edilir. Hedefte commit olmadığı kesin olan talep Approved durumuna döner; hedefte commit olmuş olabilecek talep ise Uzlaştırma Bekliyor (ReconciliationRequired) durumuna alınır ve yeniden çalıştırılmaz (Bölüm 11.1). Eşik Workers:StaleExecutionRecoveryMinutes ayarındadır ve varsayılanı 120 dakikadır. Ayrıntı ve eşiğin nasıl seçileceği: Bölüm 25.7.

Onay zinciri: kaydedilen, onaylanan ve çalışan aynıdır

Talep her kaydedildiğinde, içeriğini belirleyen her şey tek bir parmak izinde toplanır: betiklerin sırası ve metni, hedef sunucuların adresi, veritabanı ve bağlantı hesabı, talep türü ve sorgu sonucu talebinde alıcılar, teslim biçimi ve maskesiz kolonlar. Açıklama, bilet ve zamanlama parmak izine girmez. Betik metinleri ayrıca dbo.ScriptContents tablosuna yazılır; bu tablo append-only ledger tablosudur ve veritabanı motoru bu tabloda UPDATE ve DELETE işlemlerini reddeder.

Kayıt, onay planı, her onay adımı, son onay ve çalıştırma olayları bu parmak izini taşır. Her olay dayandığı önceki olaya numarasıyla bağlanır; kanıt imzası açıksa (Evidence:Signing:Enabled, kod varsayılanı kapalı) ürünün kanıt anahtarıyla imzalanır. Onay planı, onay anındaki adımları ve kurum kurallarının özetini taşır. Zincir uygulamanın olayı kabul edip kaydettiğini gösterir; onaylayanın niyetini ya da hedefte gerçekte ne olduğunu tek başına kanıtlamaz.

Worker hedefe bağlanmadan önce zinciri kontrol eder. Onaydan sonra betik, hedef sunucu, alıcı ya da onay adımları uygulamanın dışından (doğrudan tablodan) değiştirildiyse parmak izi tutmaz. Onay planı ya da imzalı bir onay adımı eksikse veya bir imza geçersizse zincir kopar. Bu durumlarda hedefe hiç bağlanılmaz, deneme gerekçesiyle ChangeRequest.ExecutionBlocked olayı olarak kayda geçer ve talep reddedilmeden Approved durumuna döner. Talep uygulamadan yeniden kaydedilirse onaylar sıfırlanır ve yeni içerik yeniden onaylanır.

Onay öncesinde de aynı kontrol yapılır: onaylayanın gördüğü içerik son kayıtlı tutmuyorsa onay verilmez ve ChangeRequest.ApprovalBlocked olayı yazılır.

Onay politikaları, onayı etkileyen parametreler, atlanamaz standartlar ve kullanıcı rolleri her yetkili değişiklikten sonra mühürlenir. Bu tablolar uygulamanın dışından değiştirilirse yeni onay planı kurulmaz ve rolü farklı görünen kullanıcı onay veremez; deneme gerekçesiyle ChangeRequest.ApprovalBlocked olayı olarak kayda geçer ve SIEM açıksa SOC'a gider. Bu sırada ayar ekranlarından yapılan bir değişiklik tablodaki hali kabul etmez, Governance.StateMismatch alarmı yazar. SystemManager farkı inceledikten sonra Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranından gerekçe yazarak yeniden temellendirir. Bu işlem Governance.Rebaselined olayıyla kayda geçer ve SIEM açıksa SOC'a alarm olarak gider. Plan kurulamayan talep yeniden kaydedilince yeni plan kurulur.

Sürüm paketinin içeriği (talepler, sıra, bağımlılıklar, çalıştırma biçimi, sunucu) da kayıt ve kuyruğa alma anında mühürlenir. Paket uygulamanın dışından değiştirilmişse çalıştırılmaz ve ReleasePackage.ExecutionBlocked olayı yazılır.

Üretim sunucusunda imzasız zincirle çalıştırma varsayılan olarak kapalıdır (Evidence:Signing:AllowUnsignedProductionExecution = false). Zincirin durumu talep detayındaki Script Bütünlüğünü Doğrula düğmesinde ve denetim dosyasının 5b bölümünde görünür. İmza kapalıyken Production hedefte çalıştırma reddedilir (SIGNING_DISABLED_PRODUCTION); bu yüzden üretim kullanımında kanıt imzası açılmalıdır. Production dışı hedeflerde imzasız zincir kabul edilir.

11.7 Kısmi başarı ve geri alma

Bir talep birden çok blok içerir. Hata oluşursa:

Veritabanı	Davranış
SQL Server, PostgreSQL	Ürünün transaction'ı geri alınır; betik transaction'ı kendisi bitirmediyse değişiklik kalmaz.
Oracle	DDL ifadeleri örtük olarak kaydedilir (implicit commit). Hatadan önce çalışan DDL blokları geri alınamaz. Çalıştırma günlüğüne bu durum açıkça yazılır.

Bu yüzden Oracle hedeflerde DDL, DCL ya da TRUNCATE içeren taleplerde etkin ve eksiksiz bir geri alma talebi zorunludur; sunucuda geri alma zorunluluğu kapalı olsa da böyle bir talep geri alma olmadan çalıştırılmaz.

Hata mesajında kaçınıcı bloğa kadar çalışıldığı ve hangi blokta durulduğu yazılır.

11.8 Geri alma (rollback) talepleri

- Geri alma talebi, bir değişiklik talebine bağlı olarak açılır.

- Yalnızca talebin sahibi üretebilir.
- Bir talebin aynı anda birden çok aktif geri alma talebi olamaz.
- Geri alma talebi normal onay akışına girer. Politikadan adım çıkmazsa kaynak talebin onay gereksinimi yansıtılır: değişikliği onaylamaya yetkili rol, geri almayı da onaylar.
- Geri alma yalnızca kaynak talep uygulandıktan sonra üretilebilir ve çalıştırılabilir. İstisna Oracle hedeflere özeldir: Oracle tarafında DDL ifadeleri örtük olarak kaydedildiği için hatadan önce çalışan bloklar üretimde kalmış olabilir; bu yüzden çalıştırması düşmüş kapanmış bir talepte bile geri alma üretilebilir ve çalıştırılabilir. SQL Server ve PostgreSQL hedeflerde bu istisna yoktur: çalıştırma tek transaction içinde yapılır, hata alındığında çalışan blokların tamamı geri alınır ve geri alınacak bir değişiklik kalmaz. Bu hedeflerde düğme kapalı gelir ve ipucunda sebebi yazar. Kural böyle daraltılmıştır çünkü aksi halde üretilen geri alma betiği, aynı nesneyi oluşturmuş başka bir talebin değişikliğini düşürebilirdi.
- Geri alma talepleri otomatik zamanlanmaz. Her zaman bir insanın çalıştırması gerekir.

Geri alma betiği nasıl üretilir

Ürün geri alma betiğini, değişikliğin ne yaptığına bakarak üretir. Kolon ekleyen bir değişikliğin geri alması kolonu düşürür, kolon düşüren bir değişikliğin geri alması kolonu geri ekler. Bu işlemlerin çoğu betiğin kendisinden çıkarılabilir. Veri değiştiren ifadeler (INSERT, UPDATE, DELETE, TRUNCATE, MERGE) ve EXEC için ise betik üretilmez: ürün o noktaya TODO işaretli bir elle müdahale notu yazar ve geri alma eksik sayılır. Veri geri alması gerekiyorsa betiği talep sahibi yazar. Bu davranış üç hedef motorda aynıdır.

Tablo düşüren (DROP TABLE) bir değişiklikte durum farklıdır. Veritabanında düşürülen bir tabloyu geri getiren bir komut yoktur. Bu yüzden ürün, tabloyu düşürmeden önce hedef sunucuya bağlanır, tablonun tanımını okur ve ondan bir CREATE TABLE betiği üretir. Yani geri alma burada bir geri sarma değil, yeniden kurmadır.

Bu ayırım önemlidir, çünkü yeniden kurma yalnızca sunucudan okunabilen şeyleri kapsar.

Yeniden kurmanın kapsamı

Geri gelenler: kolonlar ve veri tipleri, otomatik artan (IDENTITY) ayarı, boş geçilebilirlik, varsayılan değer kısıtları, birincil anahtar, benzersizlik kısıtları, kontrol (CHECK) kısıtları, yabancı anahtarlar (silme ve güncelleme davranışlarıyla birlikte) ve index'ler.

Geri gelmeyenler: hesaplanan kolonun formülü (SQL Server ve PostgreSQL hedeflerde; Oracle'da formül korunur). SQL Server hedeflerde ayrıca tablonun üzerindeki tetikleyiciler, uzantı özellikleri (açıklama alanları), bölümlleme şeması ve dosya grubu yerleşimi geri gelmez.

Hesaplanan kolon özel bir durumdur ve sonucu bilinmeden onaylanmamalıdır. SQL Server ve PostgreSQL hedeflerde kolon geri gelir, ama düz bir kolon olarak gelir: formülü yoktur, kendini

hesaplamayı bırakır ve boş kalır. Ayrıca o kolona veri yazılmasını engelleyen koruma da kalkar, yani daha önce hata veren bir kayıt işlemi artık hata vermez ve kolona istenen değer yazılabilir.

Bu liste bir eksiklik değil, yöntemin sınırındır. Betik çalışır ve tablo geri gelir. Ürün bu sınırı gizlemez: üretilen betiğin sonuna bir not satırı koyar ve aynı bilgiyi talep ekranında da gösterir.

Ekranda gördüğünüz iki farklı uyarı

Geri alma betikleri ile ilgili iki ayrı uyarı vardır. İkisi farklı şeyler söyler ve karıştırılmamalıdır.

Birincisi mavi renkli bilgi şerididir ve kapsam sınırını anlatır. Talep detay ekranının üst kısmında çıkar. Anlamı şudur: geri alma betiği hazır ve çalışır durumda, ancak yukarıdaki listedeki nesneleri geri getirmez. Bu şerit çalıştırmayı engellemez; onaylayan kişinin neyi onayladığını bilmesi için vardır. Şerit, betiğin içinde kapsam notu bulunduğunda çıkar ve pratikte tablo yeniden kurulduğunda, yani tablo düşüren bir değişikliğin geri almasında görülür. Kolon ekleyen bir değişikliğin geri almasında çıkmaz, çünkü orada tablo yeniden kurulmaz.

İkincisi sarı renkli Yapılması gereken ama yapılmayan adımlar panelidir ve gerçek bir eksiği anlatır. Geri alma planı var ama betiği eksik satırı, betikte TODO işaretli bir elle müdahale notu kaldığı anlamına gelir. İki sebebi vardır: değişiklik veri değiştiren bir ifade içeriyordur (INSERT, UPDATE, DELETE, TRUNCATE, MERGE ya da EXEC; bunlar için betik üretilmez) ya da ürün hedef sunucuya bağlanıp nesnenin tanımını okuyamamıştır. Sunucuya erişilemiyor olabilir, nesne o sunucuda bulunmuyor olabilir ya da kullanıcının okuma yetkisi yetmiyor olabilir. Bu durumlarda ürün betiğe çalışacak bir komut yazamaz, yerine bir açıklama satırı bırakır ve elde yalnız o açıklama kalır.

Aradaki fark şudur: mavi şeritte betik çalışır ve işin bir bölümünü yapar, sarı panelde betik hiçbir şey yapmaz.

Eksik geri alma betiğinin sonuçları

Sunucu ayarlarında geri alma zorunlu kılınmışsa, betiği eksik olan bir talep çalıştırılmaz. Çalıştır düğmesi kapalı gelir ve sebebi ekranda yazar. Geri alma zorunlu değilse çalıştırma engellenmez, ama uyarı yine görünür. Zorunlu olmaması, sorun olmadığı anlamına gelmez.

Uyarıyı kaldırmanın yolu betiği tamamlamaktır. Geri alma talebini düzenleyip eksik kalan yere gerçek komutu yazın ve kaydedin. Uyarı kayıtlı bir durum değildir, her açılışta betiğin o anki içeriğine bakılarak hesaplanır; betik tamamlandığı anda uyarı kendiliğinden kalkar.

Bir noktaya dikkat edin: ürün betikte eksik işareti olup olmadığına bakar, betiğin doğru iş yapıp yapmadığına bakamaz. Açıklama satırını silip yerine hiçbir şey yazmamak da uyarıyı kaldırır. Betiğin gerçekten geri alma yaptığından emin olmak inceleyen kişinin sorumluluğundadır.

Geri alma betiği değiştirildiğinde talebin onayı sıfırlanır ve kaydetme sırasında bunun teyidi istenir. Değişmiş bir geri alma, eski onayı taşıyamaz.

11.9 Çalıştırmayı başlatan kişi (attribution)

Worker çalıştırdığında "çalıştıran" alanına servis adı yazılır. Bu, denetim için yeterli değildir: asıl soru düğmeye kimin bastığıdır.

Bu yüzden ayrı bir alan tutulur:

Durum	ExecutionRequestedBy
Kullanıcı elle çalıştırdı	Kullanıcı adı
Kullanıcı elle zamanladı	Kullanıcı adı
Sistem otomatik zamanladı	SYSTEM
Sürüm paketi içinde çalıştı	Paketi çalıştıran kişi

Zamanlama iptal edilirse bu alan temizlenir. Aksi halde iptal edilmiş bir işlem için "şu kişi başlattı" yazılı kalırdı.

11.10 Acil durum geçersiz kılma (Emergency Override)

Acil durum talebinde, kilitli olmayan onay adımları yetkili kişi tarafından geçilebilir. Bu işlem:

- Yazılı gerekçe ister.
- Adım kaydına "geçersiz kılındı" işareti ve gerekçe yazar.
- Denetim kaydına ayrı bir olay olarak geçer.
- Kontrol istisnaları raporunda listelenir.
- Kontrol panelindeki istisna sayacına yansır.

Kilitli adımlar acil durumda bile geçilemez. Acil durum onayı kaldırmaz, kısaltır.

Acil durum ilan edebilmek için kullanıcının rolü en az EmergencyMinimumRole seviyesinde olmalıdır (kurulum değeri Requester).

11.11 Talep listesi ekranı

Kolon	Ne gösterir
Numara	Talep kimliği.
Açıklama	Talep açıklaması.
Tip	Change, QueryResult, Rollback.

Kolon	Ne gösterir
Durum	Bölüm 11.1.
Risk	Band.
Sunucular	Noktalı virgülle ayrılmış.
Bilet	ITSM bileti.
Oluşturan	
Oluşturma zamanı	Tarayıcınızın yerel saatiyle.
Onay durumu	Bekleyen adım varsa hangi rolün beklendiği.
Zamanlama	Varsa çalıştırma zamanı.

Filtreler: durum, tip, sunucu, tarih aralığı, oluşturan, bilet numarası, metin arama, favoriler, yalnız benim taleplerim ve gözden geçirilmemiş acil değişiklikler. Son üçü iki durumlu düğmelerdir: basılıysa filtre açıktır, tekrar basınca kapanır. Alev simgeli düğme, uygulanmış ama olay sonrası gözden geçirilmemiş acil talepleri gösterir; kontrol panelindeki sayaç da tıklandığında bu düğmeyi açar. Panodan gelindiğinde diğer filtreler devreye alınmaz, böylece panodaki sayı ile listedeki satır sayısı aynı olur.

cr.seeall yetkisi olmayan kullanıcı yalnızca kendi taleplerini görür.

Satırlarda kolonlara ek olarak küçük rozetler görünür. RB rozeti, talebin bir geri alma planı olduğunu gösterir. Gri renkli RB, planın hazır olduğu anlamına gelir. Turuncu renkli RB, planın var ama betiğinin eksik olduğu anlamına gelir; rozetin üzerine gelindiğinde sebebi okunur. Geri alma planı hiç yoksa rozet çıkmaz.

RB rozeti yalnız değişiklik taleplerinde bulunur. Sorgu sonucu taleplerinde geri alma kavramı yoktur.

Bölüm 12. Risk Bandı

12.1 Amaç ve ilke

Risk modeli tek bir soruya cevap verir: "Bu talep ne kadar dikkat gerektiriyor?"

Modelin üç temel ilkesi vardır:

1. En kötü durum belirleyicidir. Ortalama, toplam veya çarpan yoktur. Bulguların en yükseği bandı belirler.
2. Karar bandla verilir, sayıyla değil. Onay adımlarının açılması, otomatik çalıştırmanın kapanması gibi kararlar banda bakar. Sayısal skor hesaplanır ve kayıta saklanır, ancak hiçbir ekranda, raporda veya kanıt dosyasında gösterilmez: aynı kavramı anlatan iki sayı okuyan kişide soru işareti bırakır.
3. Sonuç deterministiktir. Aynı bulgular her zaman aynı bandı ve aynı skoru üretir.

12.2 Band nedir

Band, talebin risk seviyesidir. Beş kademe vardır:

Band	Sayısal değer	Anlamı
Info	0	Bilgilendirme. Risk sayılmaz.
Low	1	Düşük risk.
Medium	2	Orta risk.
High	3	Yüksek risk.
Critical	4	Kritik risk.

Her SQL standardının bir önem derecesi (Tier) vardır ve bu derece yukarıdaki beş kademeden biridir.

12.3 Band nasıl belirlenir

Betikler ayrıştırılır

|

v

Tetiklenen standart bulguları toplanır

|

v

Aynı standart anahtarına ait bulgular TEK GRUP olur

(grubun derecesi = gruptaki en yüksek derece)

|

v

BAND = tum grupların EN YÜKSEK derecesi

Hiç bulgu yoksa band Info olur.

Kritik ayrıntı: Gruplama standart anahtarına göre yapılır. Aynı standardın betik içinde on kez tetiklenmesi tek bir grup sayılır.

12.4 Skor nasıl hesaplanır (kayıt için)

Skor 0-100 arasında bir sayıdır ve yüksek sayı daha güvenli demektir. Bu bölüm skorun nasıl hesaplandığını kayıt bütünlüğü için açıklar; skor kullanıcıya gösterilmez, yalnız veritabanında saklanır. Her bandın kendi aralığı vardır:

Band	Skor aralığı
Info	90 - 100
Low	70 - 89
Medium	50 - 69
High	25 - 49
Critical	0 - 24

Hesap şu şekildedir:

```
aralik_ust = bandın ust siniri
```

```
aralik_alt = bandın alt siniri
```

```
ust_kademe_sayisi = bandı belirleyen derecedeki FARKLI standart sayisi
```

```
eger ust_kademe_sayisi <= 0 ise
```

```
    skor = aralik_ust
```

```
degilse
```

```
    dusus = min(ust_kademe_sayisi - 1, aralik_ust - aralik_alt)
```

```
    skor = aralik_ust - dusus
```

Yani üst kademede ne kadar çok farklı bulgu varsa skor aralık içinde o kadar aşağı iner, ancak asla bandın dışına çıkmaz.

12.5 Somut örnek: band High ve üç High bulgu

Bir talepte şu bulgular tetiklendi:

Standart	Derece	Kaç kez
DynamicSqlUsage	High	2
DropColumn	High	1
NoTruncateTable	High	5
TempTableUsage	Medium	3
PrintStatementInObject	Low	1

Adım adım:

1. Gruplama: Beş farklı standart anahtarı var, yani beş grup. NoTruncateTable beş kez tetiklendi ama tek grup sayılır.

2. Band: Gruplardaki en yüksek derece High'dır. Band = High.

3. Üst kademe sayısı: High derecesindeki grup sayısı = 3 (DynamicSqlUsage, DropColumn, NoTruncateTable).

4. Aralık: High için 25 - 49.

5. Düşüş: $\min(3 - 1, 49 - 25) = \min(2, 24) = 2$.

6. Skor: $49 - 2 = 47$.

Sonuç: Band High, skor 47.

Aynı örneğin varyasyonları

Durum	Üst kademe grup sayısı	Skor
Tek High bulgu	1	$49 - 0 = 49$
İki farklı High bulgu	2	$49 - 1 = 48$
Üç farklı High bulgu	3	$49 - 2 = 47$
Aynı High standardı 10 kez tetiklendi	1	$49 - 0 = 49$
30 farklı High bulgu	30	$49 - \min(29, 24) = 49 - 24 = 25$
Hiç bulgu yok	0	Band Info, skor 100
Tek Critical bulgu	1	Band Critical, $24 - 0 = 24$

Son satır önemlidir: tek bir Critical bulgu, otuz High bulgudan daha düşük (daha riskli) bir skor üretir. Bu bilinçlidir; en kötü durum belirleyicidir.

12.6 Skor açıklaması (ScoreExplain)

Band tek başına yeterli değildir: kullanıcı bandın NEDEN o seviyede olduğunu görmelidir. Sistem her talep için bir açıklama üretir:

Alan	Ne gösterir
Band	Hesaplanan risk bandı.
Skor	0-100 arası sayı. Kayıta saklanır, ekranda gösterilmez (Bölüm 12.1).
Belirleyici bulgu	Bandı belirleyen bulgu. Listede ilk sırada gösterilir.
Bulgu listesi	Her bulgu için: standart anahtarı, derecesi, mesajı, kaç kez tetiklendiği, asla atlanamaz işareti.
Etki	Her bulgunun bandı belirleyip belirlemediği. Determining bandı belirledi, Neutral belirlemedi.
Asla atlanamaz var mı	Bulgular arasında NeverSkip işaretli olan var mı.

Bulgular önce derecesine göre azalan, sonra anahtarına göre alfabetik sıralanır. Böylece en önemli bulgu her zaman üstte durur.

12.7 Asla atlanamaz (NeverSkip) kuralları

Bir SQL standardı "asla atlanamaz" olarak işaretlenebilir. Böyle bir standart tetiklendiğinde:

1. Otomatik çalıştırma yapılmaz. Talep onaylansa bile sistem onu kendiliğinden çalıştırmaz. Daha önce sistem tarafından konmuş bir zamanlama varsa temizlenir.
2. Buna bağlı onay adımı kilitlenir. Adımın atlama koşulları ne olursa olsun adım çalışır.
3. Talep detayında ve denetim dosyasında bu bulgu ayrıca işaretlenir.

Kurulumda asla atlanamaz işaretli sekiz standart vardır: CriticalObjectDrop, CriticalObjectAccess, CriticalObjectSchemaChange, XpCmdShellUsage, DclChangeDetected, LinkedServerUsage, NoManualCommitTransaction ve NoManualRollbackTransaction. Son ikisi ürünün atomiklik sözünü korur: bir talebin bütün blokları tek transaction içinde çalışır ve hata alındığında hepsi geri alınır. Betiğin kendi COMMIT ifadesi bu transaction'ı erken kapatır, kendi ROLLBACK ifadesi ise iptal eder; ikisi de yarım kalmış bir değişiklik üretebilir. Bu iki standart kurulumda ayrıca kaydı engeller; tetiklendiklerinde talep kaydedilmez. İç içe transaction açmak (NoManualBeginTransaction) asla atlanamaz işaretli değildir, ancak kurulumda o da kaydı engeller. Tam liste Ayarlar > SQL Standartları ekranında görülebilir.

Atlanmaya çalışılırsa ne olur: Ürün içinde kilitli bir adımı atlamanın yolu yoktur; atlama kuralları, rol kide mi ve acil durum geçersiz kılma kilitli adımı geçemez.

12.8 Risk bandı nerede görünür

Yer	Nasıl görünür
Talep listesi	Band rozeti.
Talep detayı	Band, bulgu listesi, açıklama.
Kontrol paneli	Risk dağılımı grafiği.
Yüksek Riskli Değişiklikler raporu	Band sütunu.
Denetim dosyası	Risk özeti ve bulgu listesi.

12.9 Bandın kararlara etkisi

Karar	Neye bakar
Onay adımının devreye girmesi	Banda (TriggerIfBandAtLeast).
Onay adımının atlanması	Banda (SkipIfBandAtMost).
Otomatik çalıştırma	NeverSkip bulgusu varlığına.
Talebin kaydedilebilmesi	"Kaydı engeller" işaretli standartlara.

Sayısal skor hiçbir kararda kullanılmaz. Yalnızca insan okuması içindir.

Bölüm 13. Sorgu Sonucu (Query Result) Akışı

13.1 Ne işe yarar

Canlı ortamdan veri okuma ihtiyacı her kurumda vardır: bir müşteri şikayetinin araştırılması, bir hatanın kök nedeninin bulunması, bir raporun doğrulanması. Bu ihtiyaç genellikle kontrolsüz karşılanır; birine "şu sorguyu çalıştır, sonucu bana at" denir.

Sorgu Sonucu özelliği bu işi kayda bağlar:

- Sorgu bir talep olarak açılır ve onaydan geçer.
- Sonuç doğrudan ekranda gösterilmez; şifreli bir dosya olarak paketlenir.
- Hassas olarak tespit edilen kolonlar varsayılan politikada (AutoMask) maskelenir.
- Kimin hangi veriyi hangi gerekçeyle aldığı kayıt altına alınır.

Bu özellik QueryGovernance modülüne bağlıdır.

13.2 Sorgu tipleri

Değer	Tip	Anlamı
0	None	Tanımsız.
1	Change	Standart değişiklik talebi.
2	QueryResult	Veri okuma talebi. Geri alınamaz, sonuç dosya olarak teslim edilir.
3	Rollback	Bir değişikliğe bağlı geri alma talebi.

13.3 Sorgu sonucu talebi oluşturma

Bölüm 11.2'deki alanlara ek olarak:

Alan	Ne işe yarar	Zorunlu
Alıcı (To)	Sonucun gönderileceği e-posta adresleri. Noktalı virgülle ayrılır.	Hayır
Bilgi (CC)	Kopya alıcılar.	Hayır
Maskesiz istenen kolonlar	Maskelenmeden gelmesi istenen kolonlar. UnmaskedColumnRequestPolicy Disabled ise gizlenir.	Hayır
Maskesiz isteme gerekçesi	Yukarıdaki liste doluysa gerekçe.	Koşullu

Betik sayısı kuralı: Sorgu sonucu talebine yalnızca tek bir betik eklenebilir. Birden çok sorgu çalıştırmanız gerekiyorsa hepsini tek betikte birleştirin; her sonuç kümesi çıktı dosyasında ayrı bir Excel sayfası olarak yer alır. Sayfa adı sunucu adı ve sıra numarasından oluşur, örnek: PROD-SQL01_01.

Kolon önizlemesi

Talep kaydedilirken, QrColumnPreviewEnabled açıkta sistem hedef sunucuya bağlanır ve sorgunun hangi kolonları döndüreceğini sorar.

Bu işlem sorguyu çalıştırmaz. Yalnızca şema bilgisi istenir, tek satır veri okunmaz, hedefte hiçbir yan etki oluşmaz.

Neden önemlidir: Önizleme, takma ad kullanılan kolonların gerçek kaynağını öğrenir.

```
SELECT TCKN AS MusteriKodu FROM Musteri
```

Bu sorguda dönen kolonun adı MusteriKodu'dur. Kolon adına bakan bir katalog bu kolonu yakalayamaz. Önizleme kaynak kolonun TCKN olduğunu öğrenir ve bu bilgi çalıştırma anında geri bağlanır. Böylece takma adla katalogu atlatmak engellenir. Kaynak kolonu çıkarılamayan sorgularda (dinamik SQL, bazı yordamlar) koruma çalıştırma anındaki içerik taramasına kalır.

Önizleme sonucu kalıcı olarak saklanır. Böylece onaylayan kişi, talep sahibinin gördüğü listenin aynısını görür ve denetim dosyasında "beklenen kolonlar" ile "gerçekleşen maskeleme" karşılaştırılabilir.

Listede her kolonun yanında beklenen karar yazar. Beş durum vardır. Maskelenecek: kolon sınıflandırma kataloguyla eşleştirdi, teslimde maskelenir. İçeriğe göre kontrol edilecek: katalogta yok, çalıştırma anında içeriği tarandı ve hassas desen bulunursa maskelenir. Belirlenemedi: sorgunun döndüreceği kolonlar çıkarılamadı (dinamik SQL ve bazı yordamlar). Maskesiz istendi, onay bekliyor: talepte bu kolon maskesiz istenmiş ama maskesiz onayı henüz verilmemiş. Maskelenmeyecek: kolon maskesiz istenmiş ve onayı verilmiş, teslimde açık gider.

Son iki durum arasındaki fark önemlidir: bir kolonu maskesiz istemek tek başına onu açmaz. Talep, maskesiz onayı verilmeden çalıştırılırsa kolon yine maskelenir. Bu yüzden ekran onay verilene kadar söz vermez, yalnızca isteğin var olduğunu söyler. Talepte kolon adı yerine yıldız yazıldıysa bütün kolonlar aynı kurala girer; kolonları belirlenemeyen satırlar ise yıldız yazılsa bile bu kapsamın dışındadır, çünkü hangi kolonların döneceği bilinmemektedir.

Bu iki durum kayıta saklanmaz, ekrana verilirken hesaplanır. Sebebi şudur: maskesiz onayı talep kaydedildikten sonra verilir; kayıt anında dondurulmuş bir değer, onay geldikten sonra yanlış bilgi göstermeye devam ederdi.

Sunucu cevap veremezse talep yine kaydedilir; önizleme zorunlu değildir.

E-posta onay adımı

QrEmailApprovalPolicy RequireApproval ise, alıcı listesindeki adresler kontrol edilir. Daha önce onaylanmamış bir adres varsa talebe ek bir onay adımı eklenir ve bu adımı QrEmailApproverRole rolündeki bir kullanıcı kapatır.

QrEmailAutoApproveUsers True ise sistemde kayıtlı kullanıcılara ait adresler onaylı sayılır.

Masksiz kolon onay adımı

UnmaskedColumnRequestPolicy değerine göre:

Politika	Davranış
RequireApproval	Ek onay adımı eklenir. UnmaskedColumnApproverRole rolündeki kişi onaylar.
AllowWithReason	Ek adım yoktur, talep sahibi kendi adına otomatik onaylanmış sayılır.
Disabled	Özellik kapalıdır. Kaydedilmiş liste temizlenir.

QrMaskingEnabled kapalıysa politika Disabled gibi davranır.

13.4 Çalıştırma anında arka planda ne oluyor

Bu, kılavuzun en çok merak edilen akışıdır. Adım adım:

1. Talep çalıştırılır (elle veya zamanlanmış)
2. Talebin TUM hedef sunucuları sırayla dolasilir
3. Her sunucuda:
 - a. Bağlantı açılır, transaction başlatılır
 - b. Betikler blok blok çalıştırılır, sonuc kumeleri okunur
 - c. Kolon meta bilgisi eklenir
 - d. Kayıt anındaki KOLON ONIZLEMESI geri bağlanır
(takma adın kaynak kolonu buradan gelir)
 - e. Satırlar belleğe alınır
4. Tüm sunuculardan veri toplandıktan sonra:
MASKELEME KARARI verilir
5. Karar her sunucu için AYRI verilir
(prod maskelenirken test açık kalabilir)
6. Maskeleme kaydı yazılır (her sunucu için bir satır)

- Politika kapalı olsa bile kayıt YAZILIR
7. Sonuclar Excel ya da CSV dosyasina yazilir (bkz. 13.7)
 8. Dosya sifreli ZIP icine konur, parola uretilir
 9. Parola sifrelenerek talep kaydina yazilir
 10. E-posta alıcılari varsa gonderim kuyruguna eklenir
 11. Calistirma gunlugu yazilir:
kac satir dondu, hangi kolonlar maskelendi,
hangi kolonlar acik gitti, sure butcesi asildi mi
 12. Talep Executed durumuna gecer

Maskleme kararı nasıl verilir

QrMaskingEnabled kapalı mı?

evet -> Hicbir tespit ve maskleme yapılmaz.

Kayıt YİNE yazılır, uygulanan politika = MaskingOff.

Denetçi masklemesiz teslimi bu kayıttan görür.

hayır -> devam

|

v

QrSensitiveDataPolicy = WarnOnly mı?

evet -> Tespit çalışır, hiçbir şey maskelenmez.

Bulunan kolonlar "açık gitti" olarak kayda yazılır.

hayır -> AutoMask (bilinmeyen değer de AutoMask sayılır)

|

v

Her sunucu için, her kolon için:

|

v

Sunucunun rejimi "Yalnız içerik" mı?

evet -> kolon adı katalogu ATLANIR, yalnız desen kontrolü yapılır

hayır -> hem katalog hem desen kontrolü

|

v

Kolon hassas mı?

hayır -> dokunulmaz

evet -> devam

|

v

Kullanıcı bu kolonu maskesiz istedi ve ONAYLANDI mı?

evet -> açık bırakılır, gerekçe "UnmaskApproved" olarak yazılır

hayır -> MASKELENİR, gerekçe "Catalog" veya "Pattern" olarak yazılır

Süre bütçesi aşılsa taranamayan kolonlar "taranmadı" olarak işaretlenir ve maskelenir. Güvenli taraf her zaman kazanır.

Kayıt ne tutar

İki tablo yazılır. Özet kayıt QrMaskingAuditLog tablosuna, ayrıntı kayıt QrMaskingAuditDetail tablosuna gider:

Özet kayıt (sunucu başına bir satır): talep numarası, sunucu adı, gönderim zamanı, gönderen, maskelenen kolonlar, maskesiz kolonlar, eşleşen desenler, uygulanan politika, teslim anındaki sunucu rejimi, muafiyet gerekçesi, tespit ayarları, istisna onayı var mı.

Ayrıntı kayıt (kolon başına bir satır): kolon adı, kaynak kolon adı, karar (maskelendi / maskelenmedi), gerekçe tipi, gerekçe ayrıntısı, uygulanan maskeleme biçimi.

Gerekçe tipleri:

Tip	Anlamı
Catalog	Kolon adı hassas kolon kataloğuyla eşleşti.
Pattern	Kolon değerleri bir hassas veri desenine uydu.
UnmaskApproved	Kullanıcı istedi ve onaylandı, açık bırakıldı.
NotScanned	Süre bütçesi nedeniyle taranamadı, güvenli tarafta maskelendi.
PolicyWarnOnly	Politika WarnOnly olduğu için maskelenmedi.
MaskingOff	Ana anahtar kapalı olduğu için hiç tespit yapılmadı.

Tespit ayarlarının kayda dondurulması önemlidir. Eşik veya örneklem sonradan değiştirilirse "bu teslimde eşik neydi" sorusu başka hiçbir yerden cevaplanamaz.

13.5 Sonuç dosyası ve teslim

Konu	Davranış
Dosya biçimi	Şifreli ZIP içinde Excel veya CSV dosyası; biçim QrOutputFormat ile yönetilir (bkz. 13.7).
Parola	Her teslim için ayrı üretilir.
Parola nerede	Talep kaydında şifreli saklanır (AES-256-GCM). Yetkili kullanıcı gerekçe yazarak görüntüler; her görüntüleme QrZipPasswordView olayıyla kayda geçer.
E-posta	Teslim biçimine bağlıdır: PortalOnly (dosya da parola da yalnız portaldan alınır), AttachmentPortalPassword (varsayılan; dosya e-postaya eklenir, parola yalnız portaldadır), AttachmentAndPassword (dosya ve parola aynı e-postada gider, gerekçe ister). Dosya MaxMailAttachmentMB sınırını aşarsa e-postaya eklenmez.
İndirme	Talep detayından.
Saklama süresi	QrFileRetentionDays gün. Süre dolunca bakım görevi dosyayı siler ve silme kayda geçer.

İndirme yetkisi

İndirmek isteyen kişi talebin sahibi mi?

evet -> QrRequesterCanDownload true mu?

evet -> indirebilir

hayir -> indiremez

hayir -> Rolu QrDownloadMinimumRole esigini geciyor mu?

evet -> indirebilir

hayir -> indiremez

Her indirmede onay kutusu ve gerekçe zorunludur. İndirme QrDownload (talep sahibi değilse QrDownloadByNonRequester) olayıyla denetim kaydına yazılır ve Veri Erişim ve Dış Aktarım raporunda görünür. Talep sahibi olmayan kişi, rolü QrDownloadMinimumRole (kurulum değeri ChangeManager) ve üstündeyse dosyayı indirebilir; alıcı listesinde olması gerekmez. Bu eşik kurumun veri erişim politikasına göre ayarlanmalıdır.

13.6 Bu akıştaki özel kurallar

Kural	Sebep
Sorgu sonucu talepleri sürüm paketi içinde çalıştırılmaz.	Paket akışında maskeleme ve kayıt üretilmez; maskelenmemiş veri kayıtsız dışarı çıkardı.
Hedefteki transaction sorgu sonucu taleplerinde commit edilmez.	Okuma işlemidir, hedefte değişiklik bırakmaz.
Bir sunucuda hata olursa tüm teslim başarısız sayılır.	Eksik sonuç teslim etmek yanıltıcı olurdu.
Aday kolon yazımı teslimi engellemez.	Öğrenme döngüsünün hatası veri teslimini durdurmamalıdır; hata günlüğe yazılır.

13.7 Sonuç dosyasının biçimi ve satır sınırı

Sonuç paketindeki veri dosyası Excel (xlsx) veya CSV olabilir. Seçim QrOutputFormat parametresiyle yapılır ve varsayılan Auto'dur: küçük sonuçlar okunaklı olduğu için Excel, büyük sonuçlar ise CSV yazılır.

Bu ayrımın sebebi Excel'in iki sınırıdır. Birincisi biçim sınırıdır: bir Excel sayfasına başlık satırı dışında en fazla 1.048.575 satır yazılabilir. Bu bir tercih değil, xlsx dosya biçiminin kuralıdır. İkincisi maliyettir: Excel yazımı satır sayısı ile birlikte hızla pahalılaşır, CSV ise akış halinde yazıldığı için çok daha ucuzdur. Ölçülmüş rakamlar bir sonraki bölümdedir.

Satır sınırı sonuç OKUNURKEN uygulanır. Sınıra ulaşıldığı anda okuma durdurulur, talep başarısız olur ve sebebi çalışma günlüğüne yazılır. Paket üretilmez, e-posta gönderilmez. Böylece bellekte sınırdan fazla satır hiçbir zaman tutulmaz ve maskeleme ile dosya yazımı hiç çalışmaz.

Geçerli sınır seçilen biçime göre hesaplanır:

- CsvOnly: yalnızca QrMaxRowCount geçerlidir, Excel tavanı devreye girmez.
- ExcelOnly: QrMaxRowCount ile 1.048.575 değerinden küçük olanı geçerlidir.
- Auto: eşik üstündeki sonuçlar CSV'ye gideceği için QrMaxRowCount geçerlidir. Eşik tanımlı değilse her sonuç Excel'e yazılacağından Excel tavanı yeniden devreye girer.

CSV dosyası noktalı virgül ayracı ve UTF-8 işaretiyle yazılır; böylece Türkçe Excel'de doğru sütunlara ayrışır ve Türkçe karakterler bozulmaz. Tarih ve ondalık değerler sunucunun yerel ayarından bağımsız, sabit bir biçimde yazılır: aynı talep iki farklı makinede aynı dosyayı üretir, denetimde karşılaştırılabilir.

Metin hücrelerinde formül etkisizleştirilmesi yapılır. Eşittir, artı, eksi veya @ işaretiyle başlayan bir metin, dosya Excel'de açıldığında formül olarak çalışırdı; bu hücreler metin olarak okunacak biçimde işaretlenir. Değerin kendisi kaybolmaz, yalnızca çalışması engellenir. Sayı, tarih ve mantıksal değerler bu işlemde etkilenmez, dolayısıyla negatif sayılar sayı olarak kalır ve dosyada toplanabilir.

13.8 Ölçülmüş maliyet ve performans

Aşağıdaki rakamlar gerçek ölçümdür, tahmin değildir. Ölçüm makinesi: Intel Core i5-8265U 1,60 GHz, 4 çekirdek ve 8 mantıksal işlemci, 8 GB bellek, Windows 11, .NET 10. Kurumsal bir sunucuda bu süreler belirgin biçimde kısılır; buradaki amaç mutlak hız değil, maliyetin nereye gittiğini göstermektir.

Senaryo: 10 kolonlu bir sonuç kümesi, kolonlardan 5 tanesi hassas olarak tespit edilip maskeleniyor (kimlik numarası, telefon, e-posta, kart numarası ve IBAN). Kural seti 14 etkin veri deseni ve 103 aktif katalog kuralı içeriyor.

2 milyon satır, 10 kolon, 5 kolon maskeli:

- Hassas veri tespiti: 0,4 saniye
- Maskeleme (5 kolon, 10 milyon hücre): 28,7 saniye
- CSV dosyasına yazma: 13,7 saniye, dosya boyutu 267 MB
- Excel dosyasına yazma: MÜMKÜN DEĞİL. Excel'in 1.048.575 satırlık biçim sınırı aşıldığı için dosya üretilemez.
- Sonuç verisinin bellekteki boyutu: 1.089 MB, sürecin zirve bellek kullanımı 1.558 MB
- Paketleme toplamı (tespit, maskeleme ve CSV yazımı): yaklaşık 43 saniye. Buna sorgunun sunucuda çalışma ve satırların ağdan okunma süresi dahil değildir; o süre sorguya ve sunucuya göre değişir.

Aynı senaryonun daha küçük boyutlardaki ölçümleri:

- 200.000 satır: tespit 0,01 sn, maskeleme 2,0 sn, CSV yazımı 0,8 sn (26 MB), Excel yazımı 28,2 sn (7,6 MB), bellek 500 MB
- 1.000.000 satır: tespit 0,04 sn, maskeleme 10,8 sn, CSV yazımı 6,4 sn (132 MB), Excel yazımı 146,8 sn (38 MB), bellek 1.558 MB
- 2.000.000 satır: tespit 0,4 sn, maskeleme 28,7 sn, CSV yazımı 13,7 sn (267 MB), Excel yazımı mümkün değil, bellek 1.558 MB

Bu tablodan çıkan üç sonuç vardır.

Birincisi, hassas veri tespiti pahalı değildir. Tespit tüm satırları değil bir örnekleme tarar (varsayılan 1000 satır), bu yüzden süresi satır sayısı ile birlikte artmaz. 2 milyon satırda bile toplam maliyetin yüzde biri kadardır. Tespit ayarlarını sıkılaştırmaktan performans kaygısıyla kaçınmak gerekmez.

İkincisi, asıl maliyet maskeleme ve dosya yazımıdır ve ikisi de satır sayısı ile doğru orantılı büyür. Maskeleme hücre başına yaklaşık 2 mikrosaniyedir; maskelenen kolon sayısı arttıkça süre orantılı artar.

Üçüncüsü, büyük sonuçlarda Excel doğru araç değildir. 1 milyon satırda Excel yazımı CSV'nin yaklaşık 23 katı sürer (146,8 saniyeye karşı 6,4 saniye) ve 1.048.575 satırın üstünde hiç çalışmaz.

Auto biçimi tam olarak bunun için vardır: sonucun boyutuna bakıp doğru dosya biçimini kendisi seçer.

Boyutlandırma önerisi: 1 milyon satırlık bir sonuç paketlenirken sürecin bellek kullanımı yaklaşık 1,5 GB'a çıkar. Worker'ın çalıştığı makinede, aynı anda çalışabilecek sorgu sonucu talebi başına bu kadar boş bellek bulunmalıdır. QrMaxRowCount değerini yükseltmeden önce bu hesabı yapmak gerekir.

Bölüm 14. Sandbox

14.1 Ne işe yarar

Sandbox, bir değişiklik talebini gerçek bir veritabanında denemek ama kalıcı hale getirmemektir. Betik bir transaction içinde çalıştırılır, sonuç kaydedilir ve transaction geri alınır.

Amaç, betiğin canlıya girmeden önce gerçekten çalışıp çalışmadığını görmektir. Sözdizimi hataları, eksik nesneler ve izin sorunları burada görülebilir. Sandbox üretim koşullarının (veri hacmi, eşzamanlı yük, kilitlenme) tam bir benzetimi değildir. Kod varsayılanında üretim sunucusunda sandbox'a izin verilmez (Sandbox:AllowOnProduction).

Bu özellik Sandbox modülüne bağlıdır.

14.2 Nasıl çalışır

Kullanıcı "Sandbox" der ve bir sunucu secer

|

v

Sandbox kaydi olusturulur (isleniyor durumunda)

|

v

Worker bekleyen sandbox kayitlarini alir

|

v

Hedefte transaction acilir

|

v

Betikler blok blok calistirilir, gunluk toplanir

|

v

Transaction HER DURUMDA geri alinir

|

v

Sonuc kaydedilir: basarili / basarisiz + gunluk

14.3 Sonucun akışa etkisi

Durum	Etki
Sandbox başarılı	Talep normal akışına devam eder. Sandbox Test Sonuçları raporunda kanıt olarak görünür.
Sandbox başarısız	Sunucuda izole deneme zorunlu değilse talep engellenmez; sonuç detayda ve raporda görünür ve onaylayanın bunu görmesi beklenir. Sunucuda izole deneme zorunluysa başarısız ya da eskimiş sandbox çalıştırmayı ve zamanlamayı engeller.
Sandbox sonrası talep düzenlendi	Sandbox sonucu "eskimiş" olarak işaretlenir. Eskimiş bir test güncel betikleri kapsamaz.

14.4 Bilinen sınırlar

Oracle hedeflerde DDL içeren talepler sandbox'lanamaz. Sebebi şudur: Oracle'da CREATE, ALTER, DROP, GRANT, REVOKE ve TRUNCATE gibi ifadeler örtük olarak kaydedilir (implicit commit). Sandbox'ın sonundaki geri alma bunları geri almaz, yani "deneme" kalıcı bir değişiklik bırakırdı.

Betikteki bir COMMIT ya da bir yordamın içindeki COMMIT de veriyi kalıcı yapar ve bu betik metninden her zaman görülemez. Ürün Oracle sandbox'ında da transaction kimliğini izler: deneme sırasında bir veri değişikliği kalıcı olursa deneme hemen durur, sonuç başarısız yazılır ve sonuç metninde "SANDBOX UYARISI" satırı çıkar. Bu durumda hedef kontrol edilmelidir; denetim dosyası da bu denemeyi istisna olarak gösterir.

DDL, DCL ya da TRUNCATE içeren bir Oracle talebinde sandbox denemesi başlatıldığında engellenir ve hangi ifade tiplerinin engele yol açtığı mesajda listelenir.

Yalnızca veri işleyen (INSERT, UPDATE, DELETE, MERGE, SELECT) Oracle betikleri sandbox'lanabilir; içlerinde COMMIT yapan bir yordam varsa yukarıdaki izleme devreye girer.

SQL Server ve PostgreSQL hedeflerde DDL ifadeleri de transaction içinde çalışır ve deneme sonunda geri alınır.

14.5 Sandbox istek ve pencere olayları

Sandbox istendiğinde isteyen kişinin adıyla ChangeRequest.SandboxRequested (paket için ReleasePackage.SandboxRequested) olayı yazılır; olay, sandbox kaydının yazıldığı aynı işlemdeydir. Worker hedefe bağlandıktan sonra, betik çalışmadan önce SandboxStarted, geri almadan sonra SandboxFinished olayını yazar (sonuç rolledBack ya da failed). Bağlantı Sandbox ya da SandboxRelease adıyla açılır. Başlangıç olayı yazılamazsa betik çalışmaz ve sandbox kaydı başarısız kapanır. Oracle'da DDL engeli bağlantı açılmadan döndüğü için bu durumda pencere de açılmaz.

Bölüm 15. Sürüm Paketi

15.1 Ne işe yarar

Birbirine bağlı birden çok talebin doğru sırayla ve birlikte çalıştırılmasını sağlar. Örnek: önce tablo eklenmeli, sonra prosedür güncellenmeli, sonra veri taşınmalı.

Bu özellik ReleasePackages modülüne bağlıdır.

15.2 Paket alanları

Alan	Ne işe yarar
Ad	Paketin adı.
Açıklama	Serbest açıklama.
Sunucu	Paketin çalışacağı sunucu.
Çalıştırma Modu	Bkz. 15.3.
Zamanlama	Paketin çalışacağı tarih.
Sorgu Zaman Aşımı	Üst sınır MaxQueryTimeout parametresidir.
Durum	Hazırlanıyor, kuyrukta, çalıştırıldı.
Başarı	Çalıştırma başarılı mı.

15.3 Çalıştırma modları

Değer	Mod	Davranış
1	AllOrNothing	Tüm talepler tek bir transaction içinde çalışır. Biri başarısız olursa hepsi geri alınır.
2	StopOnError	Her talep kendi transaction'ında çalışır. Hata olduğunda paket durur, o ana kadar başarılı olanlar kalır.

Değer	Mod	Davranış
3	ContinueOnError	Her talep kendi transaction'ında çalışır. Hata olduğunda o talep ve ona bağımlı olanlar atlanır, kalanlar devam eder.

Hangi modu seçmeli:

- Değişiklikler birbirinden ayrılamaz bir bütün oluşturuyorsa AllOrNothing.
- Sıra önemliyse ve ilk hatada durup incelemek istiyorsanız StopOnError.
- Talepler büyük ölçüde bağımsızsa ve bir hatanın tüm sürümü durdurmasını istemiyorsanız ContinueOnError.

15.4 Paket içeriği ve sıralama

Alan	Ne işe yarar
Sıra No	Taleplerin çalıştırılma sırası.
Bağımlı Olduğu Talep	Bu talep hangi talebin başarılı olmasına bağlı. ContinueOnError modunda atlama zinciri bu alandan çıkar.
Çalıştırıldı	Bu kalem çalıştı mı.
Çalıştırma Açıklaması	Kalem bazında sonuç.

15.5 Tekil talep akışından farkları

Konu	Tekil talep	Sürüm paketi
Transaction	Talep başına bir transaction.	Moda göre tek veya talep başına.
Onay	Talep bazında.	Talepler ayrı ayrı onaylanmış olmalıdır.
Talep üzerinde işlem	Serbest.	Aktif pakete alınmış talepte düzenleme, onay, çalıştırma ve zamanlama düğmeleri pasiftir. Talep artık paketin denetimindedir.
Otomatik zamanlama	Yapılabilir.	Aktif pakete alınmış talep için yapılmaz.

15.6 Kısıtlar

- Sorgu sonucu talepleri pakete alınamaz. Maskeleme ve teslim kaydı yalnızca kendi akışında üretilir.
- Bir talep aynı anda yalnızca bir aktif pakette bulunabilir.
- Paket çalıştırma zamanı da MainWorkJob tarafından denetlenir; zamanı gelen paketler önce çalıştırılır, sonra tekil talepler işlenir.

ITSM bağlantısı açıkken paketteki her talep kendi ITSM kaydıyla kontrol edilir; paketin kendi bileti yoktur. Çalıştır düğmesine basıldığında ve paket planlanan bir saatle kaydedilirken yapılan kontroller Bölüm 22.9'da anlatılır. ITSM bağlantısı kapalıyken paket ITSM'e hiç sorulmadan çalışır.

Görevler ayrılığı pakette de geçerlidir. Paketi başlatan kişi, Çalıştır düğmesine basan ya da paketi planlanan saatle kaydeden kişidir. Bu kişiye tek talepteki Çalıştır düğmesiyle aynı kural uygulanır: kurum kuralı izin vermiyorsa talep sahibi kendi talebini, onaylayan da onayladığı talebi içeren paketi başlatamaz. Kural paket planlanan saatle kaydedilirken ve Çalıştır düğmesinde uygulanır; Worker paketi başlatmadan önce aynı kuralı bir kez daha kontrol eder. Engellenen her deneme denetim kaydına ChangeRequest.ExecuteDenied olarak yazılır. Saatsiz paket bir çalıştırma kararı değildir, hazırlanması serbesttir.

Paketle çalışan talebin denetim dosyasında Sürüm paketi bölümü bulunur: paket, çalıştırma modu, talebin sırası, paketteki diğer talepler, paketi başlatan kişi, paketin sonucu ve paketin denetim kaydı. Paket planlanan saatle kaydedildiğinde bu karar, kararı verenin oturum bilgisiyle birlikte paketteki her talebe dondurulur (Bölüm 18.8).

15.7 Paket çalıştırmada pencere

AllOrNothing kipinde paket tek bir bağlantı kullanır ve tek bir pencere açar (ReleasePackage.ExecutionStarted ve ExecutionEnded; başlangıçta pakettaki talep numaraları requestIds alanında, biletleri aynı sırayla changeTicket alanında). Bu kipte hangi komutun hangi talebe ait olduğu DAM kaydından değil denetim izinden ve denetim dosyasından okunur. StopOnError ve ContinueOnError kiplerinde her talep kendi penceresini açar ve olaylarda packageId bulunur.

Bölüm 16. Nesne Geçmişi (DDL History)

16.1 Ne işe yarar

Bir veritabanı nesnesine hangi talep ile, ne zaman, kim tarafından ne yapıldığını gösterir. Liste, SQL Change Guard içindeki uygulanmış taleplerden üretilir: her satır bir talebe ve o talebin betiğine karşılık gelir. Listeyi kurarken hedef sunucuya bağlanılmaz. Bir satırda Sunucu ile karşılaştırmacı düğmesi kullanıldığında ürün o anda sunucuya bağlanır ve nesnenin oradaki güncel tanımını getirir.

Bu özellik InsightsReporting modülüne bağlıdır ve Raporlar ekranıyla aynı yetkiyi ister (report.view). Ekran betik gövdelerini gösterdiği için kapsam da kısıtlanır: tüm talepleri görme yetkisi (cr.seeall) olmayan kullanıcı yalnız kendi taleplerinden gelen kayıtları görür, bu durum ekranda ayrıca yazar.

16.2 Ekran akışı

```
Sunucu sec
|
v
Veritabanı sec
|
v
Nesne ara / listele
|
v
Nesne sec -> gecmisini gor
```

Adım	Ne gösterir
Sunucu listesi	Uygulanmış taleplerde geçen sunucular. Bir talep birden fazla sunucuya yazılmışsa her sunucu ayrı satır olur.
Veritabanı listesi	Seçilen sunucuda değiştirilmiş nesnelerin bulunduğu veritabanları.
Nesne özeti	Nesne adı, şema, tür (tablo, görünüm, prosedür, fonksiyon, tetikleyici, index ve diğerleri), kaç talepte değiştirildiği ve son

Adım	Ne gösterir
	değişiklik. Arama kutusu açtığınız veritabanının nesnelerinde çalışır.
Nesne geçmiş	Seçilen nesnenin sürümleri: sürüm numarası, talep numarası, bilet, yapılan işlem (CREATE, ALTER, DROP), ifade türü, değiştiren kişi ve uygulanma zamanı. Sürüm numarası uygulanma sırasına göre verilir ve her kullanıcıda aynıdır; yalnız kendi taleplerini görebilen bir kullanıcıda numaralar boşluklu görünür, çünkü göremediği sürümler de sayılır. Her satırda betiğin ilk satırları görünür; Betiği gör düğmesi o sürümün tam betiğini açar. İki satıra sırayla tıklandığında iki kayıt yan yana konur. Satırın sonundaki karşılaştırma düğmesi o sürümü nesnenin sunucudaki güncel tanımıyla karşılaştırır. Başlıktaki Sunucudaki güncel tanım düğmesi ise sürüm seçmeden, nesnenin sunucudaki şu anki tanımını gösterir. Tam betik, onaylanan kaydın metin defterinden gösterilir. Betiğin tablodaki bugünkü metni onaylanandan farklıysa satırda Tablodaki metin farklı işareti çıkar ve betik penceresinde uyarı görünür; bu, betiğin uygulama dışından değiştirildiğini gösterir. Aynı fark talebin denetim dosyasında SCRIPT_TABLE_DIFFERS olarak yazar.

16.3 Denetim değeri

Bu ekran bir nesnenin ürün üzerinden geçmiş değişikliklerini tek yerde toplar: denetçinin "bu prosedür en son ne zaman, hangi bilet ile, kim tarafından değiştirildi" sorusu tek ekranda cevaplanır ve betiğin kendisi de oradadır.

Listeye yalnız uygulanmış talepler girer: çalıştırılmış, elle uygulandı olarak işaretlenmiş ya da Oracle hedefte çalıştırma sırasında düşmüş olanlar. Sonuncusu Kısmi rozetiyle işaretlenir, çünkü değişikliğin tamamının uygulandığı söylenemez. Elle uygulandı olarak işaretlenen talepler de Elle rozetiyle görünür: değişikliği ürün çalıştırmamıştır, beyan edilmiştir.

Ürün dışından yapılmış bir değişiklik listede ayrı bir satır olarak görünmez; çünkü burada her satır bir talebe dayanır. Böyle bir değişikliği görmenin yolu nesnenin sunucudaki tanımına bakmaktır: başlıktaki Sunucudaki güncel tanım düğmesi bu tanıma doğrudan açar, satır sonundaki karşılaştırma düğmesi ise seçilen sürümle karşılaştırır. Son uygulanmış sürüm ile sunucudaki tanım farklıysa bu, nesnenin ürünün dışından değiştirildiğine işaret eder; tablo tanımı sunucudan yeniden üretildiği için yalnız biçim farkı da görülebilir, bu yüzden fark incelenerek okunmalıdır.

Aynı karşılaştırma talep girişinde de vardır (Bölüm 11.3). Ürün, bir değişikliği kimin ve ne zaman yaptığını yalnız kendi üzerinden geçen talepler için bilir. Ürün dışından yapılmış bir değişiklikte gösterebileceği şey, sunucudaki tanımın kayıtlarla uyuşmadığıdır; değişikliği kimin ve ne zaman yaptığı hedef veritabanının kendi

izleme düzeneğinden okunur ve bu düzeneği veritabanı yöneticiniz kurar. Bu incelemede Object Change Frequency ve Table Structure Changes raporları da kullanılır.

İki kaydın karşılaştırılması her nesne türünde aynı anlama gelmez. Prosedür, görünüm, fonksiyon ve tetikleyicide her sürüm nesnenin tam gövdesini taşır; iki sürümün farkı doğrudan okunur.

Tabloda ise kayıtlar çoğu zaman yapılan değişikliği taşır: biri CREATE TABLE, diğeri ALTER TABLE ADD COLUMN olabilir. Bu iki kayıt nesnenin iki hâli değildir ve aralarındaki fark nesnenin şeklinin değiştiği anlamına gelmez. Ürün bu durumu karşılaştırma penceresinde yazar; tablonun o anki hâli için Sunucudaki güncel tanım düğmesi kullanılır.

Bölüm 17. Denetim Kaydı ve Bütünlük

Ekran: Denetim Kaydı

Yetki: audit.view

17.1 Denetim kaydında ne tutulur

Her denetim satırı şu alanları taşır:

Alan	Ne gösterir
Olay (Action)	Ne oldu. Örnek: ChangeRequest.Approved.
Kayıt Tipi (EntityType)	Hangi tür kayıt etkilendi. Örnek: ChangeRequest, Server, SettingChange.
Kayıt Kimliği (EntityId)	Etkilenen kaydın numarası.
Eski Değer	Değişiklikten önceki durum.
Yeni Değer	Değişiklikten sonraki durum.
Yapan (PerformedBy)	Kullanıcı adı veya sistem aktörü.
IP Adresi	İsteğin geldiği adres.
Zaman (OccurredAt)	Olay zamanı, UTC olarak saklanır. Zamanı veritabanı sunucusu verir; uygulama zaman gönderemez.

17.2 Ne tutulmaz

- Sorgu sonucu verisinin kendisi hiçbir zaman denetim kaydına girmez.
- Şifreler ve parolalar maskelenmiş olarak yazılır.
- Kolon içerikleri ve satır değerleri tutulmaz.

17.3 Olay adlandırma kuralı

Olay adları KayıtTipi.Eylem biçimindedir. Aşağıdaki tablo üründe üretilen başlıca olayları listeler, tam liste değildir. Yürütme ve sandbox pencere olayları (Bölüm 17.14), onay zinciri engelleme olayları (ChangeRequest.ApprovalBlocked, ChangeRequest.ExecutionBlocked), uzlaştırma olayları (ChangeRequest.ReconciliationRequired, ChangeRequest.ReconciliationResolved) ve kanıt sınırı olayları (Evidence.BoundaryBroken, Evidence.BoundaryRestored) ilgili bölümlerde anlatılır. Denetim kaydı ekranındaki olay adı filtresi TAM eşleşme yaptığı için adlar buradaki yazımıyla aranmalıdır.

Olay	Anlamı
ChangeRequest.Create	Talep oluşturuldu.
ChangeRequest.Approve	Talep onaylandı.

Olay	Anlamı
ChangeRequest.AutoApproved	Onay adımı oluşmadığı için sistem otomatik onayladı.
ChangeRequest.Reject	Talep reddedildi.
ChangeRequest.Executed	Talep çalıştırıldı.
SettingChange.Requested	Ayar değişikliği onaya gönderildi.
SettingChange.Approved	Ayar değişikliği onaylandı ve uygulandı.
SettingChange.Rejected	Ayar değişikliği reddedildi.
SettingChange.ApplyFailed	Onaylandı ama uygulanamadı.
User.SessionsRevoked	Kullanıcının oturum yenileme kayıtları iptal edildi.
Role.SessionsRevoked	Rolü taşıyan kullanıcıların oturum yenileme kayıtları iptal edildi.
EvidencePackageExported	Denetim dosyası dışa aktarıldı.
ChangeRequest.Update	Talep güncellendi.
ChangeRequest.ApprovalStepApproved	Bir onay adımı onaylandı.
ChangeRequest.ApproveDenied	Onaylama girişimi görevler ayrılığı kuralıyla engellendi.
ChangeRequest.ExecuteDenied	Çalıştırma girişimi görevler ayrılığı kuralıyla engellendi.
ChangeRequest.QueuedForExecution	Talep çalıştırma kuyruğuna alındı; düğmeye basan kişi bu kayıta görünür.
ChangeRequest.AutoExecute	Talep otomatik çalıştırma ile başlatıldı.
ChangeRequest.ExecutionFailed	Çalıştırma hata aldı; talep RejectOnError parametresine göre reddedilir (kurulum değeri) ya da onaylı durumda kalır.
ChangeRequest.CancelExecutionRequested	Çalışmakta olan talep için iptal istendi.
ChangeRequest.ExecutionCancelledBeforeStart	Kuyrukta bekleyen talep, worker başlatmadan iptal edildi.
ChangeRequest.Schedule	Talep ileri bir zamana planlandı.
ChangeRequest.CancelSchedule	Planlanmış çalıştırma iptal edildi.
ChangeRequest.ScheduleClearedOnError	Hata nedeniyle planlama temizlendi.
ChangeRequest.MarkManual	Talep, ürün dışında elle uygulandı olarak işaretlendi.
ChangeRequest.NoLongerNeeded	Talep artık gerekli değil olarak kapatıldı.
ChangeRequest.AutoRejected	Talep otomatik olarak reddedildi.
ChangeRequest.RollbackGenerationFailed	Otomatik geri alma betiği üretilemedi; sebebi kayıta yazar.
ChangeRequest.RollbackInvalidatedByEdit	Betik düzenlendiği için mevcut geri alma planı geçersiz sayıldı.

Olay	Anlamı
ChangeRequest.ParseErrorsConfirmed	Ayrıştırma hataları kullanıcı tarafından onaylanarak kaydedildi.
ChangeRequest.EmergencyReviewed	Acil değişiklik olay sonrası gözden geçirildi.
ChangeRequest.RuleSnapshot	Talebi etkileyen kural seti kayıt anında donduruldu.
ChangeRequest.QrFileExpired	Sorgu sonucu dosyası saklama süresi dolduğu için silindi.
Server.Create	Sunucu tanımı eklendi.
Server.Update	Sunucu tanımı güncellendi.
Server.Delete	Sunucu tanımı silindi.
Server.Activated	Sunucu aktive alındı.
Server.Deactivated	Sunucu pasife alındı.
Server.RollbackRequirementDisabled	Kontrol zayıflatma: sunucuda geri alma zorunluluğu kapatıldı.
Server.RollbackRequirementEnabled	Sunucuda geri alma zorunluluğu açıldı.
Server.SandboxRequirementDisabled	Kontrol zayıflatma: sunucuda izole deneme zorunluluğu kapatıldı.
Server.SandboxRequirementEnabled	Sunucuda izole deneme zorunluluğu açıldı.
Server.MaskingRelaxed	Kontrol zayıflatma: sunucuda maskeleme rejimi gevşetildi.
Server.MaskingTightened	Sunucuda maskeleme rejimi sıkılaştırıldı.
Server.AutoExecutionEnabled	Sunucuda değişiklik taleplerinde otomatik çalıştırma açıldı.
Server.AutoExecutionDisabled	Sunucuda değişiklik taleplerinde otomatik çalıştırma kapatıldı.
Server.QrAutoExecutionEnabled	Sunucuda sorgu taleplerinde otomatik çalıştırma açıldı.
Server.QrAutoExecutionDisabled	Sunucuda sorgu taleplerinde otomatik çalıştırma kapatıldı.
Parameter.Upsert	Parametre eklendi veya güncellendi.
Parameter.Delete	Parametre silindi.
Parameter.ControlChanged	Kontrol zayıflatma: bir kontrol parametresi değiştirildi.
Parameter.DualControlDisabledNoApprover	Dört göz kuralı, ikinci onaylayan bulunmadığı için kapatıldı.
Parameter.DualControlChangedNoApprover	Dört göz kapsamı, ikinci onaylayan bulunmadığı için değiştirildi.
CriticalObject.Create	Kritik nesne tanımı eklendi.
CriticalObject.Update	Kritik nesne tanımı güncellendi.
CriticalObject.Delete	Kontrol zayıflatma: kritik nesne tanımı silindi.

Olay	Anlamı
SqlStandard.Create	SQL standardı eklendi.
SqlStandard.Update	SQL standardı güncellendi.
SqlStandard.Delete	Kontrol zayıflatma: SQL standardı silindi.
QrSensitiveColumn.Create	Hassas kolon kuralı eklendi.
QrSensitiveColumn.Update	Hassas kolon kuralı güncellendi.
QrSensitiveColumn.Delete	Kontrol zayıflatma: hassas kolon kuralı silindi.
ServerApprovalPolicy.Upsert	Sunucu ile onay politikası eşleştirmesi eklendi veya güncellendi.
ServerApprovalPolicy.Delete	Kontrol zayıflatma: sunucu ile onay politikası eşleştirmesi silindi.
ReleasePackage.Create	Sürüm paketi oluşturuldu.
ReleasePackage.Update	Sürüm paketi güncellendi.
ReleasePackage.Delete	Sürüm paketi silindi.
ReleasePackage.QueuedForExecution	Sürüm paketi çalıştırma kuyruğuna alındı.
License.Activated	Yeni lisans yüklendi.
License.Reloaded	Lisans yeniden okundu.
WorkerConfig.Delivered	Worker yapılandırması teslim edildi.
WorkerConfig.AccessDenied	Worker yapılandırma ucuna yetkisiz erişim denemesi.
Ledger.DigestPublished	Defter özeti üretildi; dış depo tanımlıysa (Evidence:Ledger:DigestOutputPath) dosya olarak yazıldı.
TableWriteLog.CoverageRecorded	Veritabanı seviyesi yazma kaydının günlük kapsam özeti deftere yazıldı.

Kontrol zayıflatma olayları ayrı adla kaydedilir. Sıradan bir ayar güncellemesi ile bir kontrolün gevşetilmesi aynı olay adıyla yazılmaz. Denetçi, kontrolün ne zaman zayıflatıldığını tek bir olay adıyla arayabilir.

17.4 Eski ve yeni değer sözleşmesi

İki kural vardır:

1. Eski değer ve yeni değer aynı biçimde yazılır. Farklı biçimlerde yazılsalardı yan yana karşılaştırılmazlardı.

2. Yazma işleminden sonra değer veritabanından geri okunur. Böylece kayda giren değer, uygulamanın niyeti değil, veritabanının gerçeği olur.

Reddedilen ayar değişikliklerinde hiçbir işlem uygulanmaz. Bu durumda istenen değerler denetim satırında saklanır; başka hiçbir yerde iz kalmaz.

17.5 Kural seti anlık görüntüsü ("o gün neydi")

Bir talep oluştuğunda, o anda geçerli olan kural seti talebe dondurulur:

- Uygulanan onay politikasının kimliği ve adı.
- Etkin görevler ayrılığı ayarları.
- Kritik nesne kararları.
- Tetiklenen standartlar ve dereceleri.

Politika sonradan silinse veya değiştirilse bile talebin denetim izi bozulmaz. Denetçi "bu talep hangi kurallarla değerlendirildi" sorusunu tek bir kayıttan cevaplayabilir.

17.6 Defter Durumu

Denetim Kaydı ekranındaki Defter Durumu düğmesi kanıt defterinin bugünkü halini gösterir. Yetki: audit.view.

Alan	Anlamı
Kanıt tablosu append-only defter	Tablo SQL Server ledger tablosu olarak mı kurulu.
Son defter özeti	En son yayımlanan özeti zamanı ve blok numarası.
Zamanında	Son özet, özet aralığının Evidence:Ledger:DigestStaleAfterIntervals katı içinde mi.
Dış depoya yazıldı	Son özet dış depoya dosya olarak yazıldı mı.
Dış depo tanımlı	Evidence:Ledger:DigestOutputPath tanımlı mı.
Son geri yükleme	Ledger.RestoreDetected olayının ya da veritabanı geri yükleme geçmişinin son tarihi.

Alan	Anlamı
Son çatal	Ledger.ForkDetected olayının son tarihi: veritabanı dışarı yazılmış özetin gerisine dönmüş.
Kritik bulgular ve sınırlamalar	Kanıt yazma sınırı kontrolünün bulguları (Bölüm 17.16).

Sonuç üç durumdan biridir. Sağlam: tablo defter, sınır sağlam, son özet zamanında alındı ve dış depoya yazıldı. Dikkat: sınır sağlam ama özet gecikti, dış depo tanımlı değil ya da son 30 gün içinde geri yükleme veya çatal kaydı var. Bozuk: tablo defter değil ya da sınır kontrolü kritik bulgu buldu; bu durumda durum değiştiren işlemler zaten durur.

Ekran "doğrulandı" demez. Kayıtların değişmediğini, kurumun dış deposundaki özet dosyalarıyla, yedeğin geri yüklendiği kopyada çalıştırılan sys.sp_verify_database_ledger gösterir. Bu doğrulama üretim sunucusunda yapılmaz; adımlar Denetçi Kiti belgesindedir.

Betik Bütünlüğü Doğrula

Belirli bir talebin onay zincirini kontrol eder: kayıt, onay ve çalıştırma olaylarının aynı parmak izini taşıdığını, imzaların geçerli olduğunu ve onaylanan metinlerin metin defterinde durduğunu gösterir. Tablodaki bugünkü metin onaylanandan farklıysa bunu ipucu olarak yazar. Talep detayından çalıştırılır. Ayrıntı: Bölüm 11.6, Onay zinciri.

17.7 Yazma kaydının kapsam özeti

TableWriteLogCoverageJob worker içinde günde bir çalışır (Workers:TableWriteLogCoverageSeconds) ve veritabanı seviyesi yazma kaydının kapsam özeti (satır sayısı, en küçük ve en büyük numara, ilk ve son kayıt zamanı) kanıt defterine TableWriteLog.CoverageRecorded olayı olarak yazar. Olay defterde durduğu için veritabanı motoru değiştirilmesini reddeder: bugünkü özetin satır sayısı ya da numara aralığı önceki olayla tutmuyorsa yazma kaydından satır silinmiştir (Bölüm 5.5).

Kanıt defterinin kendisi bu işe ihtiyaç duymaz: defterin korunması, defter özeti ve kanıt yazma sınırı kontrolü Bölüm 17.16 ve 17.17'de anlatılır.

17.8 Kanıtın kurum dışına teslimi

Defterin dış tanığı iki yoldan kurumun dışına çıkar: imzalı özet dosyaları kurumun dış deposuna yazılır (Bölüm 17.17) ve özet olayı SIEM açıksa SOC'a gider (Bölüm 17.12). Denetçi dönemin özet dosyalarını bu depodan, dönemin taleplerini ve kontrol sağlığını dönem paketinden alır (Bölüm 17.18).

Dönem paketi ayrı bir yetkiyle indirilir (audit.anchorexport, rol ekranında "Dönem Paketi İndirebilir"). Bu yetki varsayılan olarak Auditor ve SystemManager rollerinde açıktır. Denetim dosyası yetkisinden ayrı olmasının sebebi görevler ayrılığıdır: denetim dosyası yetkisi varsayılan olarak DbAdmin rolünde de açıktır ve DbAdmin, kanıt incelemesinin konusu olma ihtimali en yüksek roldür. Kurum isterse bu yetkiyi DbAdmin rolüne de verebilir.

17.9 Zaman damgası (isteğe bağlı)

İmza bir dosyanın hangi kurulumdan çıktığını gösterir, ne zaman çıktığını göstermez. O tarihi kurumun kendi saati söyler ve kurum saatini geri alabilir. Zaman damgası bu boşluğu kapatır: dosyanın özeti, kurum dışındaki veya kurumun kendi işlettiği bir zaman damgası otoritesine imzalatılır.

Bu özellik varsayılan olarak kapalıdır. Ürün kurum içinde çalışır ve zaman damgası isteğe bağlı bir eklentidir. Evidence:Timestamp:Mode ayarı Off olduğu sürece hiçbir ağ çağrısı yapılmaz.

Açmak için iki ayar yeterlidir: Evidence:Timestamp:Mode değerini On yapın ve Evidence:Timestamp:Url alanına zaman damgası sunucusunun adresini yazın. Kurum kendi iç sunucusunu kullanabilir; ürün açısından iç ve dış sunucu arasında fark yoktur. Gerekirse vekil sunucu adresi ve kimlik bilgileri de tanımlanabilir.

Denetim dosyası için ayrı bir kip verilebilir (DossierMode). Bu kip ana ayarı yalnızca daraltır, açamaz. Mode değeri Off ise damga alınmaz. Bunun sebebi şudur: dışarıya çıkışı kapatmak isteyen bir işletmecinin tek bir ayara güvenebilmesi gerekir.

Kurum verisi zaman damgası sunucusuna gitmez. Damgalanan şey dosyanın özetidir, dosyanın kendisi değil. Bu yüzden dış bir otorite kullanılsa bile içerik dışarı çıkmaz.

Damga alınamazsa hiçbir şey durmaz. Sunucuya erişilemezse, süre aşılsa veya yanıt bozuksa dosya damgasız üretilir ve iş akışı devam eder. Eksiklik gizlenmez: denetim dosyasına damga dosyası (Manifest.tsr) konmaz ve uygulama günlüğüne uyarı yazılır.

Damganın gerçekten alınıp alınmadığı Yönetişim Kurulum Kontrolü ekranından izlenir. Zaman damgası açıkken orada bir satır belirir ve API açıldığından beri yapılan son damga denemesinin sonucunu gösterir; açılıştan beri hiç deneme yoksa satır bilgi olarak görünür. Kırmızıysa en olası sebepler şunlardır: ağa çıkış engelli, vekil sunucu kimlik istiyor, adres yanlış ya da vekil sunucunun trafiği açıp yeniden imzalaması yüzünden sertifika doğrulanamıyor.

Ağa çıkış bir vekil sunucudan geçiyorsa adresi, kullanıcı adını ve parolayı Evidence:Timestamp altındaki vekil alanlarına yazın. Vekil parolası da bir sırdır; diğer sırlar gibi ortam değişkeninde tutulması beklenir ve yapılandırma dosyasında durursa hazırlık ekranı uyarı gösterir. Vekil

sunucu adresi boş bırakılırsa işletim sisteminin tanımlı vekili kullanılır; bu, vekil kullanılmıyor anlamına gelmez.

Damga, imzanın kapsadığı alanın dışındadır. Yani bir damganın paketten çıkarılması tespit edilemez. Bu bilinçli bir sınırdır ve kabul edilebilir: damganın çıkarılması kanıtı zayıflatır, sahte kanıt üretmez.

Kurumsal vekiller çoğu zaman kullanıcı adı ve parola yerine servisin kendi Windows kimliğini bekler. Bu durumda Evidence:Timestamp:ProxyUseDefaultCredentials ayarını açın; böylece ayrıca bir parola tanımlamanız da gerekmez. Bu seçenek yalnız uygulama bir etki alanı hesabıyla çalışıyorsa işe yarar. Açıkça bir kullanıcı adı yazarsanız o kullanılır.

Vekil bir etki alanı kimliği bekliyorsa ve uygulama etki alanı hesabıyla çalışmıyorsa, kullanıcı adının yanında Evidence:Timestamp:ProxyDomain alanını da doldurun. Etki alanını kullanıcı adının önüne yazmak çoğu vekilde çalışır, ancak bu her vekilde geçerli değildir; ayrı bir alan bu belirsizliği ortadan kaldırır. Vekil etki alanı istemiyorsa alanı boş bırakın. Ekranda ve günlükte vekil özeti ETKIALANI\kullanici biçiminde görünür; parola hiçbir yerde görünmez.

Kurumun zaman damgası sunucusu iç ağdaysa, vekilden geçmemesi için Evidence:Timestamp:ProxyBypass alanına adresini yazın. Birden fazla adres noktalı virgülle ayrılır ve joker kullanılabilir, örnek: tsa.kurum.local;*.kurum.local. Vekil tanımlıysa yerel adresler zaten atlanır, onlar için ayrıca liste yazmanız gerekmez.

Bağlantıyı denemek için Ayarlar > Tanılama > Zaman Damgası Testi ekranını kullanın. Ekranın üst bölümü uygulamanın kullandığı ayarları salt okunur gösterir; hangi vekilin fiilen kullanıldığı burada yazar. Alt bölümde geçici değerler girip deneyebilirsiniz; buraya yazdıklarınız hiçbir yere kaydedilmez ve ayarlarınız değişmez. Vekil parolası ekrana hiçbir zaman geri gelmez, yalnız tanımlı olup olmadığı gösterilir.

Test, zaman damgası kipine bakmaz; kapalıyken de deneyebilirsiniz. Bunun sebebi şudur: bir ayarı denemek için önce açmak zorunda kalmak, ancak üretimde denemek anlamına gelirdi.

Deneme başarısız olursa sebep adıyla gösterilir. Bu ayrım önemlidir, çünkü her sebebin çözümü farklı bir ekiptedir. Vekil kimlik istedi ve vekil sunucuya ulaşamadı sonuçları sistem ve ağ ekiplerine, sertifika doğrulanamadı sonucu güvenlik ekibine, damga sunucusuna ulaşamadı sonucu ise ağa çıkış izinlerine işaret eder. Yanıt doğrulanamadı sonucu genellikle araya bir vekil giriş sayfasının girdiğini gösterir.

Sertifika doğrulanamadı sonucunun en sık sebebi vekil sunucunun şifreli trafiği açıp kendi sertifikasıyla yeniden imzalamasıdır. Böyle bir ağda damga sunucusuna erişilebiliyor olsa bile bağlantı doğrulanamaz. Çözüm ürünün içinde değildir: kurumun kök sertifikası, uygulamanın çalıştığı makinenin güven deposunda bulunmalıdır. Windows tarafında bu depo Yerel Bilgisayar

altındaki Güvenilen Kök Sertifika Yetkilileri deposudur. Uygulama ve worker ayrı makinelerdeyse sertifikanın her ikisine de kurulması gerekir. Ürün sertifika doğrulamasını kapatan bir ayar sunmaz; doğrulaması kapalı bir bağlantıdan alınan zaman damgası, damganın verdiği güvenceyi ortadan kaldırır.

17.10 Denetim Kaydı ekranı

Kolon	Ne gösterir
Zaman	Olay zamanı, tarayıcınızın yerel saatiyle.
Olay	Olay adı.
Kayıt Tipi	Etkilenen kayıt türü.
Kayıt No	Etkilenen kaydın numarası.
Yapan	Kullanıcı veya sistem aktörü.
IP	İstek adresi.
Eski Değer / Yeni Değer	Satır açıldığında yan yana gösterilir.

Filtreler: tarih aralığı, olay adı, kayıt tipi, kayıt numarası, kullanıcı.

17.11 Kanıt paketi: denetim kayıtlarını ham haliyle teslim etme

Denetim dosyası bir talebin hikâyesini anlatır, dönem paketi dönemin bütün taleplerini ve kontrol sağlığını verir. Üçüncü bir teslim daha vardır: kayıtların ham hali. Denetçi bir aralığın olaylarını kendi aracında incelemek isterse bunu kullanır.

Ekran: Denetim Kaydı. Yetki: audit.view. Nasıl kullanılır: Kanıt Paketi düğmesine basılır, başlangıç ve bitiş kayıt numarası girilir. Denetçi bu aralığı tahmin etmez; denetim dosyası aralığı kendisi yazar (Bölüm 18.3).

Paket bir ZIP dosyasıdır ve denetim dosyası ile dönem paketiyle aynı ambalajı kullanır.

Package.json imzalanan içeriktir: aralıktaki kayıtlar (olay, kayıt tipi, kayıt numarası, eski ve yeni değer, yapan, adres ve zaman). Manifest.json paketin künyesini ve her dosyanın özetini taşır. Manifest.sig manifestin imzasıdır. PublicKey.pem açık anahtardır. Verify.ps1 doğrulama betiğidir. Üç teslim de aynı yordamla ve aynı betikle doğrulanır.

Paket teslim anındaki içeriği imzayla sabitler. Kayıtların sonradan değişmediğini paket değil defter gösterir: aynı kayıtlar defterdedir ve defter, dış depodaki özetlerle doğrulanır (Bölüm 5.4).

Dışa aktarmanın kendisi denetlenir: işlem EvidencePackageExported olarak denetim kaydına yazılır. Aynı olay adı denetim dosyası için de kullanıldığından kayıt ayrıca hangi teslimin alındığını da yazar.

17.12 SOC entegrasyonu (SIEM)

Denetim kaydı ürünün içinde durur. Bir kurumda güvenlik olaylarının izlendiği yer ise SOC'tur ve oradaki ekip ürünün ekranlarına bakmaz. Bu entegrasyon, yönetim olaylarını kurumun kendi toplayıcısına akıtır; böylece veritabanı tarafındaki hareketler kurumun geri kalanıyla aynı yerde izlenir.

Ne zaman gönderilir

Gönderim, varsayılan olarak on saniyede bir çalışan bir yoklama ile yapılır. Yoklama her turunda denetim kaydı tablosunda teslim işaretinden sonra yazılmış kayıtları okur ve varsa gönderir; yeni kayıt yoksa hiçbir şey göndermez. Bir olay bu nedenle varsayılan ayarda genellikle on saniye içinde gönderilir; toplayıcıya ulaşma süresi ağa ve toplayıcıya bağlıdır. Aralık
Workers:SiemPumpSeconds anahtarı ile değiştirilir.

Gönderim worker tarafından yapılır, API tarafından değil. Sebebi tek bir göndericinin olması gerektiğidir: API birden fazla kopya olarak çalışabilir ve her kopya kendi başına gönderirse sıra bozulur ve mükerrerlik artar.

Teslim kaldığı yerden devam eder

Ürün her uç ve her akış için bir teslim işareti tutar: buraya kadar gönderildi. Sıra sabittir; önce gönderilir, sonra işaret ilerletilir. Gönderim başarısız olursa işaret ilerlemez ve bir sonraki tur aynı yerden devam eder.

Toplayıcı üç gün kapalı kalsa bile ürün tarafında olay kaybolmaz. Toplayıcı açıldığında birikmiş olaylar sırayla akar. Buna karşılık bir çökme anında son gönderilen parti tekrar gidebilir; kanıt taşıyan bir akışta tekrar, kayıptan her zaman iyidir. Bu güvence ürünün gönderim tarafı içindir: UDP üzerinden gönderimde toplayıcının mesajı aldığı doğrulanamaz, bu yüzden kayıpsız teslim beklenen kurulumda TCP ya da TLS kullanılmalıdır. Olayın gönderilmesi, SIEM'in onu aldığını ya da işlediğini tek başına göstermez.

Diskte ayrı bir kuyruk tutulmaz. Piyasadaki log ileticileri toplayıcı erişilemez olduğunda olayları diske yazar, çünkü ellerindeki verinin başka kopyası yoktur. Burada durum farklıdır: olay zaten append-only defter tablosunda durur ve veritabanı motoru silinmesini reddeder. İkinci bir kuyruk kurmak aynı veriyi iki yerde tutmak ve iki yerin ayrışma ihtimalini yaratmak olurdu.

Tek istisna ürünün kendi günlüğü akışıdır. O akış bellekte tutulur ve kuyruk dolarsa en eski kayıt düşürülür; bir arıza anında en değerli kayıtlar en yenileridir. Düşürülen sayı nabız mesajında ve Yönetişim Kurulum Kontrolü ekranında görünür. Denetim izi ve defter özeti akışlarında kayıp yoktur.

Nabız

Beş dakikada bir nabız mesajı gönderilir. İçinde son gönderilen kayıt numarası, teslim gecikmesi, düşürülen günlük sayısı ve çalışma süresi bulunur. Nabzın amacı, SOC tarafında sessizliğin iki sebebini ayırmaktır: gerçekten olay olmaması ile ürünün durmuş olması. Nabız kesildiğinde SOC uyarı üretebilir.

Nabız ciddiye eşikinden etkilenmez. Eşik en yükseğe çekilse bile gönderilir; aksi halde eşik yükselten bir kurum, farkında olmadan, ürünün durduğunu anlamamanın tek yolunu kapatırdı. Kapatmanın meşru yolu Heartbeat akışını SiemStreams parametresinden çıkarmaktır.

Ne gönderilir, ne gönderilmez

Olayın kimliği, adı, zamanı, kimin yaptığı, kaynak adresi, ilgili talep numarası, sunucu ve sonucu gönderilir. Olay yükünden yalnızca adı bilinen alanlar dışarı çıkar; geri kalan her şey varsayılan olarak düşer. Yasak listesi yerine izin listesi kullanılmasının sebebi budur: yasak listesi olsaydı, yarın eklenen yeni bir alan kimse fark etmeden SOC'a akardı.

Parola, anahtar ve benzeri sır görünümlü değerler ayrıca maskelenir. Betik metni varsayılan olarak gönderilmez; yerine betiğin özeti gider.

Sorgu sonucu verisi hiçbir koşulda gönderilmez. SOC'a giden şey sorgunun çalıştığı bilgisidir, sonucun kendisi değildir.

17.13 SOC'a giden mesaj nasıl okunur

SOC ekibi ürünün ekranlarına bakmaz; toplayıcıya düşen satıra bakar. Bu bölüm o satırın nasıl okunduğunu anlatır. Kurulum sırasında SOC mühendisiyle aynı masada oturan kişinin ihtiyaç duyduğu bilgi buradadır.

Örnek bir mesaj

Varsayılan biçim RFC 5424 syslog başlığı ve JSON gövdedir. Gerçek bir mesaj şöyle görünür:

```
<133>1 2026-09-20T07:08:22.128Z SUNUCU01 SQL_Change_Guard 13544 146 -  
{ "eventId":146,"stream":"Audit","action":"ChangeRequest.Create","entityType":"ChangeReques  
t","entityId":"812","user":"ayse.yilmaz","severity":"Notice","outcome":"success","occurredAt":"  
2026-09-20T07:08:22.128000Z" }
```

Başlıktaki alanlar boşlukla ayrılır ve sıraları sabittir:

Alan	Ne anlama gelir
<133>	Öncelik sayısı. Tesis ile ciddiyetin birlikte kodlandığı tek sayıdır; bir sonraki başlıkta açıklanıyor.
1	Syslog sürümü. Her zaman 1 gönderilir.
2026-09-20T07:08:22.128Z	Olayın zamanı. Sonundaki Z, değerin UTC olduğunu söyler. SOC ilişkilendirmesinde en sık görülen sorun saat dilimi farkı olduğu için zaman her zaman UTC gönderilir.
SUNUCU01	Mesajı gönderen makinenin adı.
SQL_Change_Guard	Uygulama adı. Toplayıcıda kaynağı ayırt etmek için kullanılır.
13544	Süreç numarası. Aynı üründen birden fazla kopya çalışıyorsa bu alan onları ayırır.
146	Mesaj kimliği. Denetim kaydının satır numarasıdır ve toplayıcı mükerrer kaydı bu alanla eler.
-	Yapılandırılmış veri alanı. Bu biçimde kullanılmaz, boş işareti gönderilir.
{ ... }	Gövde. Olayın alanlarını taşıyan JSON. Değeri olmayan alanlar hiç yazılmaz.

Mesaj kimliği alanı akışa göre farklı bir sayı taşır. Denetim izi ve defter özeti akışlarında denetim kaydının numarasıdır ve değişmez; bu iki akışta toplayıcı mükerrer kaydı güvenle eleyebilir. Ürünün kendi günlüğü akışında süreç içinde artan bir sayaçtır ve süreç yeniden başladığında sıfırdan başlar. Nabız ile kapsam duyurusunda ise üretim anının zaman damgasıdır.

Öncelik sayısı ve local0

Syslog'da her mesajın başında tek bir sayı bulunur ve bu sayı iki bilgiyi birlikte taşır: mesajın hangi kaynak sınıfından geldiği ve ne kadar ciddi olduğu. Kaynak sınıfına tesis (facility), ciddiyet derecesine severity denir.

Tesis, syslog'un kaynakları kabaca ayırmak için kullandığı numaralı sınıftır. Sıfırdan yirmi üçe kadar tanımlıdır; ilk numaralar işletim sisteminin kendi bileşenlerine ayrılmıştır, local0 ile local7 arası ise kurumun kendi uygulamalarına bırakılmıştır. Ürün varsayılan olarak local0 kullanır ve bu

değer Siem:Endpoints[].Facility anahtarından değiştirilir. Toplayıcıda başka bir uygulama da local0 kullanıyorsa, iki kaynağı ayırmak için ürüne boş olan bir tesis verilebilir; örneğin local3. Tanınmayan bir tesis adı yazılırsa mesaj gönderilmeden kalmaz, local0 kabul edilir.

Öncelik sayısı şu formülle çıkar: öncelik = tesis numarası x 8 + ciddiye numarası. local0'ın numarası 16'dır.

Örnek: olağan bir denetim kaydının ciddiye Notice'tır, Notice'ın syslog numarası ise 5'tir. $16 \times 8 + 5 = 133$. Yukarıdaki mesajın başındaki <133> budur.

Ürünün kullandığı beş ciddiye ve local0 ile oluşan öncelik değerleri:

Ciddiyet	Syslog numarası	local0 ile öncelik	Ürün bunu ne zaman kullanır
Alert	1	129	Acil müdahale, yetki reddi ve kontrol zayıflatma olayları
Error	3	131	Başarısız işlem
Warning	4	132	Maskesiz veri çıkışı, kanıt paketi dışı aktarımı ve uygulama uyarısı
Notice	5	133	Olağan denetim kaydı ve defter özeti yayımı
Info	6	134	Nabız

Ürün syslog'un daha üst iki derecesini (Emergency ve Critical) kullanmaz. O dereceler sistemin kendisinin kullanılamaz hale gelmesi gibi durumlar içindir; bir yönetim olayının o sınıfa girmesi SOC panolarında yanlış önceliklendirmeye yol açardı.

SOC tarafında alarm kuralı yazarken bu sayı doğrudan kullanılabilir. Yaygın kurulum şudur: <129> gören olayı hemen vakaya çevir, <131> ve <132> gören olayı gün içinde incele, <133> olan olayı yalnızca sakla ve ara, <134> olan nabzın kesilmesine alarm bağla.

Ciddiyet nasıl belirlenir

Ciddiyet olayın adından çıkar; denetim kaydında ayrıca girilen bir önem alanı yoktur. Kural, sabit bir liste yerine ad kalıbı ile çalışır: adı Denied ile biten her olay yetki reddi, Failed veya Rejected ile biten her olay başarısızlık sayılır. Böylece ürüne yeni bir olay eklendiğinde ayrıca liste

güncellemesi gerekmez ve tanınmayan hiçbir olay sessizce kaybolmaz; tanınmayan olay güvenli varsayılana, yani Notice derecesine düşer.

Gerçek olay adlarıyla örnekler:

Olay	Hangi kurala girer	Ciddiyet
ChangeRequest.Create	Kural yok, varsayılan	Notice
ChangeRequest.Approve	Kural yok, varsayılan	Notice
ChangeRequest.Executed	Kural yok, varsayılan	Notice
Ledger.DigestPublished	Defter özeti	Notice
ChangeRequest.ExecutionFailed	Adı Failed ile bitiyor	Error
ChangeRequest.Reject	Başarısızlık	Error
QrZipPasswordView	Veri ifşası	Warning
EvidencePackageExported	Veri ifşası	Warning
Evidence.PeriodPackageExported	Veri ifşası	Warning
LoginFailed	Yetki reddi	Alert
ChangeRequest.ExecuteDenied	Adı Denied ile bitiyor	Alert
ChangeRequest.EmergencyReviewed	Acil müdahale	Alert
User.Delete	Kimlik kontrolü değişikliği	Alert
Parameter.ControlChanged	Kontrol zayıflatma	Alert
Siem.FilterChanged	Kontrol zayıflatma	Alert
SsoLoginFailed	Yetki reddi	Alert
LoginBreakGlass	Acil müdahale	Alert
SsoRoleMapping.Update	Kontrol zayıflatma	Alert
User.SyncedFromIdp	Kimlik kontrolü değişikliği	Alert

Olay	Hangi kurala girer	Ciddiyet
LdapLoginDenied	Adı Denied ile bitiyor	Alert
User.CreatedFromDirectory	Kimlik kontrolü değişikliği	Alert
User.SyncedFromDirectory	Kimlik kontrolü değişikliği	Alert
User.DisabledInDirectory	Kimlik kontrolü değişikliği	Alert
Ldap.ConfigurationChanged	Kimlik kontrolü değişikliği	Alert
Ldap.SyncAborted	Kimlik kontrolü değişikliği	Alert
Ledger.ForkDetected	Defter sürekliliği bozuldu	Alert

Bir olay birden fazla kurala uyabilir; bu durumda en yüksek derece kazanır. Örneğin SettingChange.Rejected hem bir ayar değişikliği kaydı hem bir ret kayıdır. Kontrol zayıflatma kuralı önce uygulandığı için olay Alert olarak gider, Error olarak değil.

Kullanıcının kendi parolasını değiştirmesi (User.PasswordChanged) olağan bir iştir ve Notice derecesindedir. Parolayı bir yöneticinin sıfırlaması (User.AdminPasswordReset) kontrol değişikliği sayılır ve Alert derecesinde gider.

Ürünün kendi günlüğü akışında kural farklıdır: orada ad yoktur, günlük satırının seviyesi doğrudan eşlenir. Fatal seviyesi Alert, Error seviyesi Error, Warning seviyesi Warning olur; geri kalan satırlar Notice derecesinde gider.

Kapsam daraltıldığında SOC'a düşen mesaj

Bölüm 7.11'de anlatılan dört parametreden biri değiştiğinde ürün ayrı bir olay gönderir. Olay, değişiklik yürürlüğe girmeden önceki yapılandırma ile gönderilir ve eski değer ile yeni değeri birlikte taşır. Gerçek bir örnek:

```
<129>1 2026-09-20T18:28:43.089Z SUNUCU01 SQL_Change_Guard 19696 1789928923089 -
{"eventId":1789928923089,"stream":"Audit","action":"Siem.FilterChanged","entityType":"Parameter","entityId":"SiemStreams","user":"admin","severity":"Alert","outcome":"success","oldValue":"Audit;Anchor;AppLog;Heartbeat","newValue":"Anchor;AppLog;Heartbeat"}
```

Gövdesi okunur biçimde yazıldığında:

```
{
  "eventId": 1789928923089,
  "stream": "Audit",
```

```
"action": "Siem.FilterChanged",
"entityType": "Parameter",
"entityId": "SiemStreams",
"user": "admin",
"severity": "Alert",
"outcome": "success",
"oldValue": "Audit;Anchor;AppLog;Heartbeat",
"newValue": "Anchor;AppLog;Heartbeat"
}
```

Bu örnekte Audit akışı kapsam dışına çıkarılmıştır. oldValue alanında Audit yazılıdır, newValue alanında yoktur; aradaki fark hangi akışın kapatıldığını doğrudan gösterir.

SOC tarafında aranacak alan action alanıdır ve değeri Siem.FilterChanged'dir. Bu olayın kendisi ciddiyet eşliğinden de, akış seçiminden de etkilenmez; kapatılan akışın kapatıldığı bilgisi her koşulda gider. Aksi halde bir kurum önce Audit akışını kapatır, sonraki daraltmaları da sessizce yapabilirdi.

Önerilen alarm kuralı: action alanı Siem.FilterChanged olan her olay SOC tarafında bir vakaya dönüşsün. Bu olay yılda birkaç kez görülür, gürültü üretmez.

17.14 Yürütme ve sandbox pencere olayları

Ürünün hedefte iş yaptığı her aralığa pencere denir. Her pencere denetim izine bir "başladı" ve bir "bitti" olayı olarak yazılır. DAM kaydındaki oturum, bu aralığın içinde, ürünün hesabıyla ve beklenen adresten geliyorsa ürünün işidir.

Olay	Kim yazar	Anlamı
ChangeRequest.ExecutionStarted ve ExecutionEnded	Worker (WorkerService)	Talebin hedefte çalıştığı aralık. Sorgu sonucu talebinde her sonucu için ayrı pencere
ReleasePackage.ExecutionStarted ve ExecutionEnded	Worker	Yalnız AllOrNothing paketi (tek bağlantı)

Olay	Kim yazar	Anlamı
ChangeRequest.SandboxRequested	API, isteyen kişi adına	Sandbox istendi. Henüz hedefe bağlanılmadı
ChangeRequest.SandboxStarted ve SandboxFinished	Worker	Sandbox denemesinin aralığı
ReleasePackage.SandboxRequested, SandboxStarted, SandboxFinished	API ve Worker	Paket sandbox'ı için aynısı

Başlangıç olayının yükünde şu alanlar bulunur: windowKind (iş türü), serverName, executionLogin (ürünün hedefte kullandığı hesap, parola asla yok), executorHost (Worker makinesinin adı), clientAddress (hedefin gördüğü adres), targetSessionId (oturum numarası), targetAuditSessionId (yalnız Oracle), sessionApplicationName (bağlantıya verilen ad), executionStartedAt (UTC), gerekirse packageId, requestIds (pakettaki talepler, noktalı virgülle), sandboxId, changeTicket (talebin ITSM kaydı, örnek CHG0030001) ve emergencyTicket (acil talepte olay kaydı, örnek INC0012345).

Bitiş olayının yükünde windowId, windowKind, windowOutcome, serverName, executionFinishedAt (UTC) ve gerekirse packageId ile sandboxId bulunur. windowId, başlangıç olayının denetim kaydı numarasıdır. Bitiş olayı hesabı, adresi ve oturumu tekrar etmez; başlangıca windowId ile bağlanır.

Bilet alanları SOC'un, açılan pencerenin hangi ITSM kaydına ait olduğunu talep numarasına gitmeden görmesini sağlar. Kurallar: biletler yalnız başlangıç olayında bulunur (bitiş olayı başlangıca windowId ile bağlıdır); değer, talep kaydedilirken dondurulan bilettir, ITSM'den o anda yeniden okunmaz; bileti olmayan talepte alan hiç yazılmaz; acil talepte değişiklik kaydı yoksa yalnız emergencyTicket bulunur; geri alma talebi kaynak talebin biletini taşır; sorgu sonucu talebinde her sonucu penceresi aynı bileti taşır; AllOrNothing paketinde changeTicket ve emergencyTicket, requestIds ile aynı sırada noktalı virgülle ayrık listedir ve bileti olmayan talep boş eleman olarak kalır (örnek: requestIds 5;6;7 ve changeTicket CHG0030005;;CHG0030007); sandbox pencereleri bilet taşımaz. Sonuç (windowOutcome)	Ne zaman
executed	Hedef değişikliği commit etti. Sorgu sonucunda sonucu okuması başarılı
failed	Betik hata verdi ve hedefte geri alındı. Sorgu sonucunda okuma hatası ya da satır sınırı aşımı
cancelled	Kullanıcı iptal etti ya da servis kapanırken iş yarıda kaldı
rolledBack	Sandbox betiği başarıyla çalıştı ve geri alındı
abandoned	Süreç çöktü, bitiş yazılamadı. Pencere sonradan kapatıldı; gerçek sonuç talep, paket ya da sandbox kaydındadır

Kurallar:

- Başlangıç olayı yazılamazsa betik hiç çalışmaz. Talep reddedilmez, Onaylı durumuna döner; denetim veritabanı kesintisi talebin hatası değildir. Paketlerde sıradaki taleplere geçilmez.
- Başlangıç olayı, hedefte ve uygulama veritabanında işlem başlamadan önce kendi kısa işleminde yazılır; yürütme başarısız olsa bile "başladı" kanıtı kaybolmaz.
- Bitiş olayı yazılamazsa iş sonucu değişmez, hata Worker günlüğüne yazılır. Eksik bitiş sonraki yetim kapatma tamamlar.

- Kullanıcı bir talebi bekleme süresi içinde, Worker henüz hedefe bağlanmadan iptal ederse pencere hiç açılmaz; talep doğrudan Onaylı'ya döner (ChangeRequest.ExecutionCancelledBeforeStart). Betik çalışırken iptal edilirse pencere cancelled ile kapanır.

- Bu olaylar Notice ciddiyetindedir ve Denetim akışından gider. ChangeRequest.Executed ve ChangeRequest.ExecutionFailed olayları pencere olaylarından ayrı olarak da yazılır.

Sorgu sonucu talebi, her hedef sunucu için ayrı bir Query penceresi açar. Bağlantı SQL Change Guard/Query/<talep no> adıyla açılır, başlangıç olayı hedefte işlem açılmadan önce yazılır, okuma bir işlem içinde yapılır ve işlem commit edilmeden geri alınır (hedefte değişiklik kalmaz). Bitiş olayı o sunucunun okuması bitince yazılır: okuma başarılıysa executed, okuma hatası ya da satır sınırı aşımıysa failed, iptalse cancelled. Böylece DAM'deki bir okuma (SELECT) kaydı, ürünün hesabıyla, aynı oturum numarasıyla ve pencerenin zaman aralığında ise hangi sorgu sonucu talebine ait olduğu bulunabilir. Ürünün Health, Preview, Definition ve Test bağlantıları da okuma yapar ama pencere açmaz.

17.15 Pencere olaylarının SIEM'e taşınması

Pencere olaylarının alanları (windowId, windowKind, windowOutcome, executionLogin, executorHost, clientAddress, targetSessionId, targetAuditSessionId, sessionApplicationName, executionStartedAt, executionFinishedAt, packageId, requestIds, sandboxId, changeTicket, emergencyTicket) SOC'a bilinçli olarak çıkar: hesap adı, makine adı ve istemci adresi, SIEM'in "bu oturum ürünün penceresine denk geliyor mu" sorusunu cevaplaması için gereklidir. Parola ve bağlantı dizesi hiçbir zaman yükte yoktur. Tüm biçimlerde (JSON, RFC 5424, LEEF, CEF) alanlar taşınır. CEF'te sınırlı alan olduğu için pencere olayları sabit alanlara yazılır:

Öznitelik	CEF alanı
executionStartedAt, executionFinishedAt	start, end (epoch milisaniye)
executionLogin	duser
executorHost	shost
clientAddress	src (olayın kendi adresi boşsa; Worker olaylarında boştur)
sessionApplicationName	requestClientApplication
windowId	cn1 (etiket windowId)
targetSessionId	cn2 (etiket targetSessionId)
sandboxId, yoksa packageId	cn3 (etiketi hangisiyse o)
serverName, windowKind, windowOutcome	cs4, cs5, cs6
targetAuditSessionId	CEF'te taşınmaz. JSON, RFC 5424 ve LEEF'te vardır
changeTicket	cs3 (etiket changeTicket)
emergencyTicket	flexString1 (etiket emergencyTicket)
requestIds	flexString2 (etiket requestIds)

Oracle kullanan kurum için CEF dışında bir biçim önerilir. Alanlar SIEM'e giderken 256 karakterde kırılır; çok büyük pakette requestIds ve bilet listesi kırılabilir, tam liste denetim izinde ve denetim dosyasındadır. Hesap adı token, secret ya da password gibi bir kelime içeriyorsa SIEM'e giderken maskelenir; ürün hesabına böyle ad verilmemelidir. SIEM mesajındaki host alanı olayı gönderen Worker makinesidir, hedef sunucu değildir.

17.16 Kanıt defteri ve kanıt yazma sınırı

Denetim kayıtları uygulama veritabanında evidence şemasındaki AuditLogs tablosunda tutulur. Tablo SQL Server'ın append-only ledger (defter) tablosudur: veritabanı motoru kayıt değiştirmeyi ve silmeyi sysadmin dahil herkes için reddeder. Ürün tabloya yalnız evidence.usp_Audit_Append yordamıyla yazar; olay zamanını yordam veritabanı sunucusunun saatinden kendisi verir (UTC), yani uygulama geriye ya da ileriye tarihli kayıt yazamaz. Raporlar ve ekranlar dbo.AuditLogs görünümünü okur. Bu koruma tablonun içeriğine yöneliktir; veritabanının eski bir yedeğe döndürülmesine ya da veritabanı dosyalarının doğrudan değiştirilmesine karşı tek başına yeterli değildir. Bu durumlar dış depoya yazılan defter özetiyle fark edilir (Bölüm 17.17).

Defter, yordamın yazdığını korur; yordamın doğru yazdığını korumaz. Bu yüzden ürün API açılışında, 15 dakikada bir ve Worker'ın kendi işiyle şu sınırı denetler: kanıt tablosu defter mi, tabloda tetikleyici var mı, yazma yordamı ürünün yayımladığı sürümle aynı mı, evidence şemasında beklenmeyen bir nesne var mı, tabloya başka bir nesne başvuruyor mu, tablo düşürülüp yeniden kurulmuş mu, veritabanında TRUSTWORTHY ya da DB_CHAINING açık mı.

Sınır bozulursa ürün Evidence.BoundaryBroken olayını yazar, bildirim e-postası gönderir ve talep kaydetme, onay, ret, çalıştırma gibi durum değiştiren işlemleri sınır düzelene kadar durdurur; ekranlar okunabilir kalır. Düzeline Evidence.BoundaryRestored yazılır. Kanıt tablosu yoksa, defter değilse ya da veritabanı SQL Server 2022'den eskiyse API hiç açılmaz.

Bir işin durumunu değiştiren olay (talep kaydı, onay, ret, çalıştırma sonucu) her zaman o değişiklikte aynı transaction içinde yazılır. Olay yazılamazsa değişiklik de yapılmaz. Başarısız girişte kullanıcının yazdığı ad, hesap sistemde yoksa kayda girmez; "unknown" yazılır, çünkü kullanıcılar bu alana bazen parolalarını yazar ve defterden silinemez. Olay içeriği kayda girmeden önce taranır: parola, sır ve anahtar alanları maskelenir; açıklama ve gerekçe gibi serbest metinlerde geçerli bir TC kimlik numarası, kart numarası ya da IBAN varsa maskelenir ve maskelenen alanların adı olayın _redacted listesine yazılır.

17.17 Defter özeti

Worker saatte bir (Evidence:Ledger:DigestIntervalMinutes) özet turunu başlatır; API veritabanından defter özeti alır. Özet, o ana kadarki bütün defter kayıtlarını kapsayan tek bir

değerdir. API özeti imzalar (imza açıksa), Evidence:Ledger:DigestOutputPath ile tanımlı dış depoya dosya olarak yazar (imza açıksa yanında .sig dosyası bulunur) ve denetim kaydına Ledger.DigestPublished olayını ekler; olay SIEM açıksa SOC'a da gider. Dış depo tanımlı değilse dosya yazılmaz. Deponun değiştirilemez olması (örneğin WORM ya da saklama kilidi) ve veritabanı yöneticisinin bu depoya yazamaması kurumun sağlamasıdır. Bu koşullar sağlandığında, veritabanını yöneten biri sonradan kayıtları değiştirse bile dışarı yazılmış özet değişmediği için değişiklik denetçinin doğrulamasında görünür.

Özet üretilemezse ya da depoya yazılamazsa Ledger.DigestFailed yazılır. Veritabanı geri yüklenirse API bunu özet turunda msdb geri yükleme geçmişinden fark eder ve Ledger.RestoreDetected yazar. Yönetişim Kurulum Kontrolü ekranındaki "Son defter özeti" satırı özet iki aralık boyunca gelmezse uyarır; SOC'ta da aynı kural kurulur.

Süreklilik kontrolü: her özet turunda depodaki son özet dosyası okunur ve veritabanının defter zinciriyle karşılaştırılır (bir sonraki bloğun "önceki blok özeti" dışarı yazılmış özete eşit olmalıdır). Veritabanı o özeti gerisindeyse (eski yedeğe dönüş) ya da zincir uyuşmuyorsa (başka sunucuda geri yükleme, veritabanı dosyasında değişiklik) Ledger.ForkDetected olayı yazılır ve kritik bildirim gider. Bu kontrol satırları yeniden özetlemez, bu yüzden üretimde her turda çalışır; geri yükleme geçmişi silinse bile, dış depoda özet dosyası bulunduğu sürece çatalı yakalar.

Denetim dosyasının "10b. Kanıt Durumu" bölümü talebin son kaydını kapsayan dış özeti gösterir ve üç durumdan birini yazar: "Dış özetle kapsandı", "Henüz kapsanmadı" ya da "Doğrulama başarısız". "12. Alan Doğrulaması" bölümü ise dosya üretilirken defteri sys.sp_verify_database_ledger ile doğrular ve sonucu yazar: VERIFIED (değiştirilemez depodaki dış özet dosyası okundu ve defter ona kadar doğrulandı), VERIFIED_INTERNAL (dış dosya okunamadı, yalnız defterin içindeki özet kullanıldı; bu bağımsız bir doğrulama değildir ve dosya "doğrulandı" demez), NOT_COVERED (son kaydı kapsayan özet henüz yok), UNAVAILABLE ya da FAILED. Ürünün kendi doğrulaması bağımsız değildir; bağımsız hükmü denetçi, değiştirilemez depodaki özetlerle veritabanının bir kopyasında aynı yordamı çalıştırarak verir. Adımlar Denetçi Kiti belgesindedir.

17.18 Dönem paketi

Ekran: Denetim Kaydı. Yetki: audit.anchorexport (rol ekranında "Dönem Paketi İndirebilir"; görevler ayrılığı gerekçesi Bölüm 17.8'de).

Nasıl kullanılır: Denetim Kaydı ekranında başlangıç ve bitiş tarihini seçin ve Dönem Paketi düğmesine basın. Dönem en fazla 92 gündür; önerilen kullanım ayda bir pakettir. Paket iç denetime teslim edilir ve teslim kurumun belge sisteminde kaydedilir.

Paketin içinde Population.json (dönemin bütün talepleri, talep tablosu ile denetim kaydı arasında satır satır uzlaştırılmış olarak; Period Population raporuyla aynı içerik), ControlHealth.json (dönemde yayımlanan defter özetleri, özetler arasındaki boşluklar, başarısız özetler, sınır bozulma ve düzelme olayları, geri yüklemeler, worker kesintileri ve bugünkü sınır kontrolünün sonucu), Exports.json (dönemde alınan kanıt dosyaları ve paketlerin günlüğü), Chain.json (her talebin onay zinciri durumu ve dönemde zincir kapısında engellenen denemeler), Manifest.json, Manifest.sig, PublicKey.pem ve Verify.ps1 bulunur. Dışa aktarmanın kendisi Evidence.PeriodPackageExported olarak denetim kaydına yazılır. Bir olay türünde 20.000'den fazla kayıt varsa paket kırılmaz, hiç üretilmez; bu durumda dönem kısaltılır.

Bölüm 18. Denetim Dosyası (Evidence Dossier)

18.1 Ne işe yarar

Tek bir talebin tüm yaşam döngüsü kanıtını, denetçiye verilebilecek biçimde tek bir ZIP dosyasında toplar.

Kullanım senaryosu: Denetçi "şu değişikliğin kanıtını göster" der. Talep detayından dosya dışa aktarılır ve denetçiye verilir. Denetçi dosyayı sisteme girmeden inceleyebilir ve doğrulayabilir.

18.2 Kim üretir

Dışa aktarma için iki katman yetki gerekir:

1. audit.evidenceexport yetkisi. Bu yetki rol tanımından gelir. Varsayılan olarak Auditor, DbAdmin, ChangeManager ve SystemManager rollerinde açıktır.
2. Talebi görme yetkisi. cr.seeall yetkisi yoksa kullanıcı yalnızca kendi taleplerinin dosyasını üretebilir.

İki katmanın sebebi: dışa aktarma yetkisi, görmediğiniz bir talebin verisine erişim sağlamamalıdır.

18.3 Dosya içeriği

Dosya	İçerik
Dossier.json	Kanonik veri. Talebin künyesi, onay adımları, betikler, risk özeti, sandbox sonuçları, ITSM doğrulamaları, kararları verenlerin oturumu, denetim izi ve talebin denetim kaydı aralığı. Paket özeti bu dosya üzerinden hesaplanır.
Manifest.json	Paketin künyesi: biçim adı ve sürümü, kurulum kimliği, ürün sürümü, talep numarası, üretim zamanı, dosyayı üreten kullanıcı, imzalayan anahtarın kimliği, paket özeti (packageHash), denetim kaydı numarası ve pakete giren her dosyanın SHA-256 özeti.
Dossier.pdf	Aynı bilginin okunabilir, yazdırılabilir hali.
Manifest.sig	Manifest.json dosyasının imzası. Kurumun özel anahtarıyla üretilir. Denetçi bunu açık anahtarla doğrular ve dosyanın bu

Dosya	İçerik
	kurulumdan çıktığını görür. Yalnız imzalama açıkken pakete konur.
PublicKey.pem	İmzayı doğrulamak için kullanılan açık anahtar. Gizli değildir, paylaşılabilir. Bu anahtarla imza doğrulanabilir ama yeni bir imza üretilemez. Yalnız imzalama açıkken pakete konur.

Talebin denetim izi dosyaya eksiksiz alınır; üst sınır 100.000 kayıttır. Sınır aşırsa iz kırılır ve bu durum dosyada istisna olarak yazılır.

Dosya, talebin denetim kaydı aralığını da yazar: ilk ve son kayıt numarası. Denetçi bu aralığın olaylarını ham haliyle incelemek isterse aynı aralığın kanıt paketini ister (Bölüm 17.11). Aralık yazılmasaydı denetçinin hangi paketi isteyeceğini kuruma sorması gerekirdi; denetlenen tarafın kendi kanıtının kapsamını belirlemesi denetim açısından zayıf bir kurgudur.

Aralık içindeki numaraların bir kısmı bu talebe ait değildir ve bu normaldir. Denetim kaydı kurumun tamamının günlüğüdür; bir talep işlenirken başka kullanıcılar da işlem yapar. Bu yüzden bir talebin satırları bitişik olmaz.

Manifest.json içindeki dosya listesi sayesinde denetçi, paketteki her dosyayı tek tek karşılaştırabilir. Bir dosyanın tek karakteri değişse özeti tutmaz.

Pakette ayrıca Verify.ps1 doğrulama betiği bulunur (Bölüm 18.6). Zaman damgası açıksa manifestin RFC 3161 zaman damgası Manifest.tsr dosyası olarak eklenir.

Kurulum kimliği (installationId) imzalanan içeriğin içindedir. Bir kurumun imzalı kanıt dosyası başka bir kurumun paketine konursa kurulum kimliği tutmaz ve bu doğrulamada fark edilir.

İmzalama kurumun ayarıdır (Evidence:Signing:Enabled). İmzalama kapalıysa dosya üretilir ve içine Manifest.sig ile PublicKey.pem konmaz; paketin üretildikten sonra değişmediği yine gösterilebilir, ancak hangi kurulumdan çıktığı gösterilemez ve bu dosyanın içeriğinden görülür. İmzalama açıkken anahtar kullanılamıyorsa (anahtar tanımsız, sertifika bulunamadı, özel anahtar okunamıyor) dosya ÜRETİLMEZ ve kullanıcıya "imzalanamadı" mesajı gösterilir: imzalı olması beklenen bir dosya hiçbir zaman sessizce imzasız çıkmaz.

18.4 Sorgu sonucu verisi neden girmez

Denetim dosyasına sorgu sonucu verisi hiçbir zaman konmaz.

Sebebi şudur: denetim dosyası, kontrol mekanizmasının çalıştığını kanıtlamak içindir, verinin kendisini taşımak için değil. Sonuç verisini dosyaya koymak, maskeleye ve indirme yetkisi kontrollerini tümüyle

atlatan bir yan kapı açardı. Denetim dosyası indirme yetkisi olan biri, sonuç dosyası indirme yetkisi olmadan canlı veriye ulaşırdı.

Dosyada bulunan: sorgunun metni, kaç satır döndüğü, hangi kolonların maskelendiği, hangi kolonların açık gittiği ve neden.

Dosyada bulunmayan: satır içeriklerinin kendisi.

Maskeme kaydının bütünlüğü: Teslim anında her sunucunun maskeme kaydının özeti kanıt defterine yazılır (QueryResult.MaskingRecorded olayı). Denetim dosyası üretilirken tablodaki kayıt aynı kuralla yeniden özetlenir ve defterdeki değerle karşılaştırılır. Sonuç dosyada her teslimin altında yazar: kayıt teslim anındaki özetle aynıysa doğrulandı, değilse değiştirilmiş (dosyanın hükmü kırmızıya döner), defterde izi yoksa iz yok. Böylece dosyadaki maskeme bilgisine duyulan güven yalnız dosyanın imzasına değil, teslim anında deftere yazılan olaya da dayanır.

Dosya ayrıca her teslimde kaç kolon ve kaç satır teslim edildiğini gösterir. Maskelenen ve açık giden kolon listeleri yalnız hassas bulunan kolonları içerir. Maskesiz istenen bir kolon sonuçta yoksa ya da zaten hassas değilse o satır muafiyet etkisiz olarak yazılır; maskesiz teslim edildi diye yazılmaz.

18.5 Dışa aktarmanın kendisi denetlenir

Dosya üretildiğinde denetim kaydına EvidencePackageExported olayı yazılır. Bu kayıt:

- Kimin, ne zaman, hangi talep için dosya ürettiğini tutar.
- Paket özetini (packageHash) taşır.
- Veri Erişim ve Dışa Aktarım raporunda görünür.

Yani "kanıt üretme" işleminin kendisi de kanıtlanır.

Bu olay denetim kaydında durur, dosyanın kendi zaman çizelgesine girmez. Sebebi şudur: dosyayı almanın kendisi dosyanın içine girseydi, durumu hiç değişmemiş bir talep her indirmede farklı bir paket özetini verirdi. Bugünkü davranışta değişmemiş bir talep kaç kez indirilirse indirilsin aynı paket özetini verir; denetçi iki dosyayı birebir karşılaştırabilir. Kaybolan bir bilgi yoktur: bir talep için kaç kez kanıt dosyası alındığı Denetim İzi ekranından ve Veri Erişim ve Dışa Aktarım raporundan görülür.

Manifest.json dosyasının özeti her indirmede farklıdır ve bu beklenen davranıştır: manifest üretim zamanını, dosyayı üreten kullanıcıyı ve denetim kaydı numarasını taşır. Karşılaştırma her zaman paket özetini (packageHash) üzerinden yapılır.

18.6 Dosya nasıl doğrulanır

1. Denetçi elindeki ZIP dosyasını acar

2. Manifest.json icinden iki degeri okur:
 - packageHash
 - auditEntryId
3. Denetim Kaydi ekranindaki "Kanıt Doğrula" islemini acar
4. İki degeri girer
5. Sistem, o numaradaki denetim kaydini bulur
6. Kaydin icindeki packageHash ile girilen degeri karsilastirir

Döner sonu:

Alan	Anlamı
Geerli mi	İki özet aynı mı.
Denetim kaydı numarası	Karşılaştırılan kayıt.
Dışa aktarma zamanı	Dosyanın üretildiğı an.
Dışa aktaran	Dosyayı üreten kullanıcı.
Beklenen özet	Denetim kaydındaki değeri.
Verilen özet	Denetinin girdiğı değeri.

Doğrulama başarısız olursa ne anlama gelir

Durum	Anlamı
Kayıt bulunamadı	Verilen numarada bir dışa aktarma kaydı yok. Dosya bu sistemden çıkmamış olabilir veya numara yanlış girilmiştir.
Özetler farklı	Dosya üretildikten sonra değıştirilmiş. İeriğeri güvenilemez.
Özetler aynı	Dosya üretildiğı andaki halindedir.

Doğrulama, dosyanın içeriğinin doğru olduğunu değil, değışmediğini kanıtlar. İeriğeri dayandığı kayıtların değışmediğini kanıt defteri gösterir (Bölüm 5.4 ve 17.16).

Sisteme hiç girmeden doğrulama

Yukarıdaki yol, denetinin ürüne erişmesini gerektirir. İkinci bir yol daha vardır ve hiçbir erişim istemez: paketin içindeki imza, yine paketin içindeki açık anahtarla doğrulanır. Deneti bunu kendi bilgisayarında, yaygın bir araçla yapar. Kuruma ait hiçbir gizli değeri paylaşılmaz.

1. ZIP dosyası açılır.

2. Manifest.json içindeki listede yazan her dosyanın SHA-256 özeti hesaplanır ve listedeki değerle karşılaştırılır. Böylece paketteki hiçbir dosyanın değişmediği görülür.

3. Manifest.sig imzası, PublicKey.pem açık anahtarıyla Manifest.json üzerinde doğrulanır. Örnek komut: `openssl dgst -sha256 -verify PublicKey.pem -signature Manifest.sig Manifest.json`

Beklenen çıktı: Verified OK. Bu iki adım da geçerse şu iki şey birlikte gösterilmiş olur: paket üretildiği andaki halindedir ve o anda bu kurulumun anahtarıyla imzalanmıştır.

Bir noktaya dikkat: denetçinin elindeki açık anahtarın gerçekten kuruma ait olduğunu ayrıca teyit etmesi gerekir. Aksi halde kurum, başka bir anahtarla imzalanmış bir paketi kendi anahtarıymış gibi verebilirdi. Teyidin yolu, anahtarın parmak izini kurumdan ayrı bir kanaldan almaktır. Parmak izi, açık anahtarın ikili hâlinin SHA-256 özetidir; PEM dosyasının kendisinin özeti değildir.

Kurum bu parmak izini Ayarlar altındaki Yönetişim Kurulum Kontrolü ekranından okur. İmzalama anahtarının parmak izi satırı, denetçinin karşılaştıracığı değeri olduğu gibi gösterir. Değer denetçiye paketten ayrı bir kanaldan verilir: yazı, sözleşme eki ya da kurumsal portal. Ürün bu yayımın yapıp yapılmadığını göremez, o yüzden satır bir hatırlatma olarak durur.

Paketin içindeki doğrulama betiği

Her pakette Verify.ps1 adlı bir doğrulama betiği bulunur. Denetçi paketi açıp tek komutla kontrol edebilir: `powershell -ExecutionPolicy Bypass -File Verify.ps1`

Betik Windows Gezgini üzerinden de çalıştırılabilir: dosyaya sağ tıklanır ve Run with PowerShell seçilir. Bu yolla açılan pencere sonucu yazdıktan sonra Enter bekler, böylece çıktı ekranda kalır. Betik başka bir betiğin içinden çağrılıyorsa -NoPause parametresi eklenir ve bekleme yapılmaz. Beklenmedik bir hata olursa betik sessizce kapanmaz: hatayı yazar ve bu hatanın paketin kendisi hakkında bir şey söylemediğini belirtir.

Betik, manifestte listelenen her dosyanın özetini kontrol eder, manifest imzasını doğrular ve açık anahtarın parmak izini yazdırır. Ne doğrulayacağını manifestten okuduğu için aynı betik denetim dosyasında, dönem paketinde ve kanıt paketinde çalışır.

Betiğin özeti manifestte yazılır ve manifest imzalanır. Böylece betiğin sonradan değiştirilmesi, manifest imzası ve betiğin özeti standart araçlarla (openssl, Get-FileHash) kontrol edildiğinde görünür; değiştirilmiş bir betiğin kendi "geçti" çıktısı buna kanıt değildir.

Betik kanıtın parçası değildir ve bunu kendi başlığında söyler. Yaptığı her şey elle de yapılabilir. Denetçi bağımsız olmak istiyorsa aynı kontrolleri en az bir kez kendi araçlarıyla yapmalıdır; paketin içinden çıkan bir aracın geçti demesi tek başına kanıt sayılmaz.

Betik imzayı doğrulayamadığı durumda geçti demez. İmza doğrulaması Windows ile birlikte gelen PowerShell sürümünde de çalışır; denetçinin ayrıca bir yazılım kurması gerekmez. Anahtar herhangi bir sebeple yüklenemezse betik sonucu eksik olarak bildirir, bunun yerine hangi komutların çalıştırılabileceğini yazar ve farklı bir çıkış kodu döndürür. Dosya özetlerinin tutması, imzanın doğrulandığı anlamına gelmez.

18.7 Çok uzun betikler ve PDF

Bir talepte çok sayıda ve çok uzun betik varsa PDF binlerce sayfaya çıkar ve kimsenin okumadığı bir belgeye dönüşür. Bunu önlemek için PDF içindeki betik metni gerektiğinde kısaltılır. Kısaltılan yere, kaç satırın gizlendiğini ve tam metnin nerede olduğunu söyleyen bir not düşülür.

Kısaltma yalnızca gerektiğinde devreye girer. Tek betikli sıradan bir talepte birkaç yüz satırlık metin olduğu gibi yazılır. Betik sayısı arttıkça her betiğe düşen yer azalır.

Kısaltma kanıt değerini etkilemez. Betiklerin tam metni her zaman Dossier.json dosyasının içindedir ve paket özeti o dosya üzerinden hesaplanır. PDF okumak içindir; doğrulama Dossier.json üzerinden yapılır.

18.8 Kararları verenlerin oturumu

Talep üzerindeki her insan kararında, kararı veren kişinin o anki oturumunun kimlik bilgisi kararlar birlikte dondurulur. Denetim dosyası bu bilgiyi "Kararları Verenlerin Oturumu" bölümünde gösterir.

Alan	Anlamı
Karar	Talep kaydedildi, onay adımı (adım numarasıyla), reddedildi, çalıştırma istendi, çalıştırma zamanlandı, sürüm paketiyle çalıştırma istendi, sürüm paketi planlanan saatle kaydedildi, acil değişiklik gözden geçirildi, elle uygulandı, artık gerekli değil.
Giriş	Yerel parola, kurum dizini (LDAP) ya da kurum hesabı (SSO, sağlayıcının adıyla).
MFA	Evet (ürünün kendi kodu), Evet (kimlik sağlayıcısı bildirdi), Hayır ya da Kimlik sağlayıcısı bildirmedi.

Alan

Anlamı

Acil durum girişi

Kurum hesabıyla giriş açıkken yerel parolayla açılmış oturum. Bu oturumla verilen karar ayrıca İstisnalar listesine yazılır.

Oturum numarası

Denetim Günlükleri'ndeki giriş kaydıyla (LoginSuccess, MfaSuccess, SsoLoginSuccess, LoginBreakGlass) aynı numaradır. Denetçi kararı bu numarayla girişe bağlar.

Bilgi kararın verildiği anda yazılır ve sonradan hesaplanmaz. Kişinin hesabı sonradan kurum hesabına çevrilse ya da başka bir yolla girse de dosyada yazan, o günkü oturumdur. Kanıt olmayan bir oturumda (bu bilgi tutulmadan önce açılmış oturum) giriş "Bilinmiyor" olarak yazılır; bilgi uydurulmaz.

Sistemin kendi işlemleri (zamanlanmış çalıştırma, otomatik onay) bir kişi oturumu olmadığı için bu bölümde yer almaz; onlar zaman çizelgesinde SYSTEM ya da WorkerService olarak görünür.

18.9 Denetçi bu dosyayla neyi ispatlayabilir

Soru	Dosyadaki cevap
Bu değişikliği kim istedi?	Talep künyesi.
Ne değiştirdi?	Betikler ve ayrıştırılmış nesne listesi.
Riski neydi?	Risk bandı, bandı belirleyen bulgu ve bulgu listesi.
Hangi kurala göre değerlendirildi?	Uygulanan politika adı ve dondurulmuş görevler ayrılığı ayarları.
Kim onayladı?	Onay adımları, karar verenler, zamanlar.
Atlanan adım var mı, neden?	Atlanan adımlar gerekçeleriyle.
Test edildi mi?	Sandbox sonuçları.
Ne zaman ve kim tarafından çalıştırıldı?	Çalıştırmayı başlatan kişi, çalıştıran servis, zamanlar, sonuç.
Bu belge sonradan değiştirildi mi?	Paket özeti doğrulaması.
Bu dosya gerçekten bu kurumdan mı çıktı?	Manifest imzası ve açık anahtar.
Kararı veren kişi o an nasıl giriş yapmıştı?	Kararları verenlerin oturumu: giriş yolu (yerel parola, kurum dizini, kurum hesabı), MFA, acil durum girişi ve oturum numarası (Bölüm 18.8).

Soru	Dosyadaki cevap
ITSM'de izin var mıydı?	ITSM doğrulamaları: kayıta ve çalıştırmada ITSM'de o an görülen durum ve verilen karar (Bölüm 22).
Sürüm paketiyle mi çalıştı, paketi kim başlattı?	Sürüm paketi: paket, çalıştırma modu, sıra, paketteki diğer talepler, paketi başlatan kişi (Çalıştır düğmesine basan ya da paketi planlanan saatle kaydeden), paketin sonucu ve paketin denetim kaydı.

18.10 Yürütme pencereleri ve istisnalar

Denetim dosyasında Yürütme pencereleri bölümü bulunur. Talebin kendi denetim izindeki ve talebin yer aldığı AllOrNothing paketlerinin denetim izindeki başlangıç ve bitiş olayları windowId ile birleştirilir. Her pencere için pencere numarası, tür, sunucu, başlangıç, bitiş, sonuç; altında hesap, makine, hedefin gördüğü adres, oturum numarası ve uygulama adı yazılır. Dossier.json içinde executionWindows alanı olarak da bulunur. Sorgu sonucu verisi dosyaya girmez; pencere yalnız bilgi taşır.

Aynı pencere için birden fazla bitiş varsa (örneğin kurtarma eşiği aşılmıca önce abandoned, sonra işin gerçek bitiş yazıldıysa) son bitiş geçerlidir. İstisnalar son bitişe göre üretilir.

İstisna kodu	Anlamı
EXECUTION_CANCELLED	Yürütme iptal edildi
EXECUTION_ABANDONED	Yürütme penceresi yarım kaldı (süreç durdu); gerçek sonuç talep kaydından okunur
SANDBOX_ABANDONED	Sandbox penceresi yarım kaldı
EXECUTION_WINDOW_OPEN	Başlangıcı var, bitiş yok ve talep şu an Yürütülüyor durumunda değil

Denetçi bu bölümle "Bu talep hedefte hangi hesapla, hangi adresten, hangi oturumla ve hangi aralıkta çalıştı" sorusunu dosyanın içinden cevaplar ve DAM kaydını bu aralıkla eşleştirir.

Tablodakilere ek olarak iki istisna kodu daha üretilir. EXECUTION_LOGIN_MISMATCH: hedefin pencerede gördüğü hesap, sunucu tanımındaki hesaptan farklıdır; DAM mutabakatı gözlenen hesapla yapılır. SANDBOX_TARGET_COMMITTED: sandbox penceresi executed sonucuyla kapanmıştır, yani denemede hedefte veri kalıcı olmuştur (Oracle'da betikteki ya da yordamdaki COMMIT gibi).

Bölüm 19. Kontrol Paneli (Dashboard)

Ekran: Kontrol Paneli

Yetki: dashboard.view

19.1 Zaman ayrımı

Paneldeki sayılar iki gruba ayrılır ve ekranda da ayrı gösterilir:

Grup	Anlamı
Aralık (Range)	Seçilen tarih aralığında olan işlerin sayısı. Geçmişe bakar.
Şimdi (Now)	Şu an bekleyen işlerin sayısı. Tarih aralığından bağımsızdır.

Bu ayırım önemlidir. İki tek bir kart dizisinde karıştırılırsa "toplam 500, bekleyen 12" gibi birbiriyle ilgisiz sayılar yan yana gelir ve panel yanlış okunur.

19.2 Aralık kartları

Kart	Ne gösterir	Nasıl hesaplanır
Oluşturulan	Aralıkta açılan talep sayısı.	Oluşturma tarihine göre.
Çalıştırılan	Aralıkta başarıyla çalıştırılan talep sayısı.	Çalıştırma tarihine göre.
Başarısız	Aralıkta çalışma denemesi başarısız olan talep sayısı.	
Reddedilen	Aralıkta reddedilen talep sayısı.	

19.3 Şimdi kartları

Kart	Ne gösterir
Onay bekleyen	Şu an Pending durumundaki talepler.
Çalıştırma bekleyen	Onaylanmış ama henüz çalıştırılmamış talepler.
Çalışan	Şu an Executing durumundaki talepler.
Önümüzdeki 24 saatte zamanlanmış	Zamanlaması şu andan itibaren 24 saat içinde olan onaylı talepler.
Bekleyen ayar onayı	Karar bekleyen ayar değişiklikleri.

19.4 Çalıştırma başarı oranı

Formül: başarılı / (başarılı + başarısız).

Reddedilen talepler bu hesaba dahil değildir, çünkü reddedilen talep hiç çalıştırılmamıştır ve başarısızlık sayılmaz.

Aralıkta hiç çalıştırma denenmediyse kart boş görünür. Sıfır yazmak "hepsi başarısız oldu" gibi okunurdu.

19.5 Grafikler ve listeler

Bölüm	Ne gösterir	Nasıl okunur
Eğilim (Trend)	Zaman içinde oluşturulan ve çalıştırılan talep sayısı.	İki çizgi arasındaki fark birikmiş iş yükünü gösterir. Oluşturma sürekli çalıştırmanın üstündeyse kuyruk büyüyor demektir.
En aktif kullanıcılar	Aralıkta en çok talep açan kullanıcılar.	Tek bir kişide aşırı yoğunlaşma, bilgi ve yetki yoğunlaşmasına işaret edebilir.
Sunucu yükü	Sunucu başına talep sayısı.	Hangi ortamın en çok değişiklik aldığını gösterir.
En uzun bekleyenler	En eski bekleyen talepler.	Talep numarası, açıklama, bilet, açan kişi, açılış zamanı, durum, hangi adımda ve hangi rolde beklediği.
Risk dağılımı	Bandlara göre talep sayısı ve yüzdesi.	Band boş (hesaplanmamış) kayıtlar ayrı görünür. Critical dilimin büyümesi dikkat gerektirir.
Onay kuyruğu	Rol bazında bekleyen adım sayısı ve ortalama bekleme süresi.	Hangi rolün darboğaz olduğunu gösterir. Ortalama bekleme saatinin yükselmesi o rolde yeterli kişi olmadığına işaret eder.

19.6 İstisnalar kartı

Normal akışın dışına çıkan taleplerin sayısıdır. Denetçi ve yönetim için "kontrol çalışıyor mu" sorusunun panel karşılığıdır.

Sayaç	Ne sayar
Acil durum	Aralıkta açılan acil durum talepleri.
Geçersiz kılınan adımlar	Acil durum yetkisiyle geçilen onay adımları.
Kendi kendine onaylanan	Talep sahibinin kendi talebini onayladığı durumlar.
Onaysız maskesiz veri	Maskesiz kolon istenmiş ama onay alınmamış talepler.
ITSM kuralına uymayan bilet	Kapanmış, bulunamayan ya da yanlış türdeki ITSM kaydıyla yapılan talep denemeleri (reddedilenler ve uyarıyla geçenler).
ITSM doğrulaması yapılamayan	ITSM'e ulaşamadığı için kurala göre geçilen doğrulamalar.
ITSM kapısında duran çalıştırma	ITSM kaydı hazır olmadığı için durdurulan çalıştırmalar.

Sayaç	Ne sayar
CAB onayı aranmadan geçen (geri alma, acil)	Çalıştırma kapısında CAB onayı beklemeden geçen geri alma ve acil talepler.

Kartta ayrıca şu satırlar bulunur: hiçbir kişinin onayından geçmeden kuralla onaylanan High ya da Critical bantlı talepler, görevler ayrılığı kuralının engellediği onaylama ya da çalıştırma girişimi olan talepler (Bölüm 27.4), gözden geçirilmemiş acil değişiklikler (Bölüm 27.5) ve uzlaştırma bekleyen (ReconciliationRequired) talepler. Son iki sayaç tarih aralığından etkilenmez. Bu sayılardan herhangi biri beklenenden yüksekse ayrıntısı Kontrol İstisnaları raporundadır. ITSM satırlarının ayrıntısı ITSM Control Exceptions raporundadır.

19.7 Rol bazında farklar

Panel, kullanıcının yetkisine göre daralır. cr.seeall yetkisi olmayan kullanıcı yalnızca kendi taleplerine ait sayıları görür. Ayar onayı sayacı, ilgili yetkisi olmayan kullanıcıda görünmez.

19.8 Boş veri durumu

Seçilen aralıkta hiç kayıt yoksa kartlar sıfır, grafikler boş durum mesajıyla görünür. Bu bir hata değildir.

19.9 Panodaki açıklama işaretleri

Panodaki her sayının yanında küçük bir bilgi işareti vardır. Üzerine geldiğinizde o sayının ne saydığı, hangi zaman aralığına baktığı ve ayrıntısını nereden görebileceğiniz yazar. Böylece "bu sayı nereden geliyor" sorusunun cevabı için belgeye bakmanız gerekmez.

Örnek: En aktif kullanıcılar bölümündeki işaret, sıralamanın açılan talep sayısına göre yapıldığını, çalıştıran ya da onaylayan kişilerin sayılmadığını söyler. Kontrol istisnalarındaki her satırın kendi işareti vardır ve ayrıntının hangi ekranda ya da raporda olduğunu yazar.

Kontrol istisnaları listesinde değeri sıfır olan satırlar da gösterilir. Sıfır, kontrolün kaldırıldığı değil o dönemde hiç yaşanmadığı anlamına gelir; satırın kaybolması yanlış izlenim verirdi. Her satır tıklanabilir ve ayrıntının bulunduğu ekranı açar: talep bazındaki ayrıntılar Kontrol İstisnaları raporunda (panodaki tarih aralığı hazır gelir), engellenen görevler ayrılığı girişimleri Denetim Kaydı ekranında, gözden geçirme bekleyen acil değişiklikler talep listesinde açılır. Böylece sayının altındaki kayıtların hangileri olduğu sorusu tek tıkla cevaplanır.

Sayıların üzerine tıklandığında talep listesi açılır ve o sayıya karşılık gelen kayıtlar görünür. Liste açılırken daha önce kaydettiğiniz filtreler (tarih aralığı, yalnız kendi talepleriniz, favoriler) devreye alınmaz. Aksi halde panoda dört yazarken listede bir satır görünür ve iki ekran birbirini yalanlardı.

19.10 Worker göstergesi ve kesinti kaydı

Worker servisi her 30 saniyede bir API'ye kendi durumunu bildirir. Bu bildirim kalp atışı denir. Son bildirimin üzerinden 90 saniye geçtiyse worker durmuş kabul edilir.

Durum, uygulamanın üst çubuğunda her ekranda aynı yerde görünür:

- Worker çalışıyorsa yeşil bir nokta ve Worker yazısı görünür. Üzerine geldiğinizde son bildirim zamanı ve mekanizmanın nasıl çalıştığı yazar.

- Worker durmuşsa kırmızı çerçeveli bir uyarı ve "Worker durdu" yazısı görünür. Üzerine geldiğinizde son bağlantı zamanı, bunun sonucu ve ne yapmanız gerektiği yazar.

Uyarının anlamı şudur: zamanlanmış işler ve çalıştırma bekleyen talepler worker geri gelene kadar ilerlemez. Talepler kaybolmaz, sırada bekler; worker döndüğünde kaldığı yerden devam eder. Gösterge 30 saniyede bir tazelenir, worker döndüğünde uyarı kendiliğinden kaybolur.

Gösterge üst çubukta durur, tek bir ekranda değil. Sorunu fark ettiğinizde hangi ekranda olacağınız belli olmadığı için bilgi her yerde aynı yerdedir.

Kesinti denetim kaydına yazılır

Üst çubuktaki gösterge o anki durumu söyler, geçmişini değil. Denetçinin sorusu ise geçmişe aittir: dün gece işler neden çalışmadı, worker kaç saat kapalıydı.

Bu yüzden durum değiştiğinde denetim kaydına birer olay yazılır:

- Worker.Offline: worker haber vermeyi kesti. Kayıta son bildirim zamanı ve üzerinden geçen süre bulunur.

- Worker.Online: worker geri geldi. Kayıta kesintinin kaç dakika sürdüğü bulunur.

Kayıtları yazan taraf bir kullanıcı değildir; işlemi yapan alanında SYSTEM yazar. Yalnız durum değişiminde kayıt üretilir. Her kontrolde kayıt üretilseydi denetim izi 30 saniyede bir satırla dolar ve okunmaz hale gelirdi.

Uygulama yeni açıldığında worker henüz haber vermemiş olabilir. Bu bir kesinti değildir ve kayıt üretmez; izleme ilk gerçek bildirimden sonra başlar.

Nasıl kontrol edilir: Worker servisini durdurun, en fazla iki dakika bekleyin ve üst çubuktaki göstergenin kırmızıya döndüğünü görün. Denetim Kaydı ekranında Worker.Offline olayını bulun. Servisi yeniden başlattığınızda gösterge kendiliğinden düzelir ve Worker.Online olayı yazılır; kaydın içinde kesintinin kaç dakika sürdüğü yazar.

Bölüm 20. Raporlar

Ekran: Raporlar

Yetki: report.view

Modül: InsightsReporting

20.1 Genel kurallar

- Raporlar beş grupta toplanmıştır ve toplam 34 rapor vardır.
- Rapor çıktıları İngilizce üretilir. Sebebi, raporların denetim ve uyum çalışmalarında kurum dışına verilebilmesi ve uluslararası denetçilerin de okuyabilmesidir.
- Her raporun kendi parametreleri vardır. Tarih aralığı parametreleri varsayılan olarak son 30 günü kapsar.
- Bazı raporlar rol kısıtlıdır. Kısıt hem listede hem çalıştırmada arka uçta uygulanır.
- Rapor sorguları zaman aşımına tabidir (Reports:QueryTimeoutSeconds, varsayılan 500 saniye).

20.2 Ortak parametreler

Parametre	Tip	Anlamı
Start Date	Tarih	Aralığın başlangıcı. Varsayılan: 30 gün önce.
End Date	Tarih	Aralığın bitişi. Varsayılan: bugün.
Server	Liste	Sunucu filtresi. Çoklu sunucu taleplerinde liste içinde arama yapılır.
Status	Liste	Talep durumu.
Object Name	Metin	Nesne adı filtresi.
ITSM Ticket No	Metin	Bilet numarası.
Request No	Sayı	Talep numarası.
Minimum Risk Band	Liste	Risk bandı eşiği. Varsayılan: 3 (High).
Statement Category	Liste	DDL, DML, DCL gibi.
Statement Type	Liste	CREATE, ALTER, DROP gibi.
Environment	Liste	Ortam.
Database Type	Liste	Veritabanı türü.
Principal / Account	Metin	Veritabanı hesabı.
User	Metin	Uygulama kullanıcısı.
Record Type	Metin	Denetim kaydı tipi.
Include deleted accounts	Onay kutusu	Silinmiş hesaplar dahil edilsin mi.

Tarih filtreleri yerel gün sınırıyla çalışır. Ayrıntı: Bölüm 23.5.

20.3 Change Governance grubu

Rapor	Neyi gösterir	Hangi soruyu cevaplar	Kısıt
Change Request Summary	Talep başına tek satır: durum, risk bandı, uygulanan politika, acil durum işareti, çalıştırmayı başlatan kişi, etkilenen satır sayısı.	"Bu dönemde hangi değişiklikler yapıldı?"	-
Change Request by Object	Hangi talep hangi nesneye dokundu.	"Şu tabloyu son altı ayda kim değiştirdi?"	-

Rapor	Neyi gösterir	Hangi soruyu cevaplar	Kısıt
Work in Progress	Henüz çalıştırılmamış talepler ve kaç gündür bekledikleri.	"Kuyrukta ne var, ne kadar bekliyor?"	-
Rejected and Cancelled Requests	Reddedilen veya iptal edilen talepler, kararı veren kişi ve gerekçe. Karar veren bilgisi onay adımından okunur, sonraki otomatik güncellemeler bunu ezemez.	"Neden reddedildi, kim reddetti?"	-
High Risk Changes	Seçilen band ve üstündeki talepler, acil durum işareti ve uygulanan politika.	"En riskli değişiklikler hangileriydi?"	-
Rollback Changes	Geri alma talepleri ve kaynak talepleri.	"Hangi değişiklikler geri alındı?"	-
Approval and Execution Duration	Talep, son onay ve çalıştırma arasındaki saat farkları.	"Süreç nerede tıkanıyor?"	-
Execution Activity	Hedef sunucularda gerçekte ne çalıştı: başlatan kişi, çalıştıran servis, süre, etkilenen satır, sonuç, hata metni. Otomatik zamanlamada başlatan SYSTEM görünür. Sürüm paketi içinde çalıştıysa paket de gösterilir.	"Canlıda ne çalıştı?"	-
Approval Step Detail	Her onay adımı: gereken rol, karar veren, karar zamanı, geçersiz kılma işareti ve gerekçe.	"Çift kontrol gerçekten uygulandı mı?"	-
Sandbox Test Results	Test sunucusu, sonuç, çalıştıran, testten sonra talep düzenlendi mi. Talep sandbox'ları ile sürüm paketi sandbox'ları aynı listededir; Scope kolonu ikisini ayırır. Paket satırında paketteki talepler ';' ile ayırık listelenir ve risk bandı paketteki taleplerin en yüksek bandıdır. Eskimiş test güncel betikleri kapsamaz.	"Canlıya çıkmadan önce denendi mi?"	-

Rapor	Neyi gösterir	Hangi soruyu cevaplar	Kısıt
Control Exceptions	Normal akıştan çıkan talepler: acil durum kayıtları, geçersiz kılınan adımlar, kendi kendine onaylananlar, onaysız maskesiz veri istekleri, engellenen görevler ayrılığı girişimleri (kaç deneme yapıldığı ve kimin denediği, ';' ile ayrık), onay zinciri kapısında duran onay ve çalıştırmalar (içerik, plan ya da yönetim durumu tutmadı), bileşimi tutmayan sürüm paketindeki çalıştırmalar ve hiçbir kişinin onayından geçmeden kuralla onaylanan yüksek riskli talepler. Onay politikası olmayan sunucuya talep kaydedilemediği için politikasız talep bu listede yer almaz.	"Kontroller nerede devre dışı kaldı?"	Auditor, DbAdmin, ChangeManager, SystemManager
ITSM Control Exceptions	ITSM kontrolünün normal akıştan çıktığı her an: kurala uymayan bilet, yapılamayan doğrulama, durdurulan çalışma, CAB onayı aranmadan geçen talep. Her satırda ITSM'de o an görülen durum ve karar yazar.	"ITSM kontrolü nerede durdurdu, nerede atlandı?"	Auditor, DbAdmin, ChangeManager, SystemManager
Period Population	Dönemin bütün talepleri, talep tablosundan ve denetim kaydından ayrı ayrı toplanıp satır satır karşılaştırılmış olarak. Her satırda tablodaki durum ile denetim kaydından türetilen durum yan yana durur; PopulationCheck kolonu Match, NotInAuditTrail, NotInTable, StatusMismatch ya da InProgress yazar. Uyuşmayan satırlar üstte gelir.	"Bu dönemin bütün taleplerini aldığımı nasıl bilirim?"	Auditor, DbAdmin, ChangeManager, SystemManager

Denetçiler genellikle Control Exceptions raporundan başlar. Bu rapor boşsa seçilen dönemde ürünün kaydettiği bir kontrol istisnası yoktur; ürün dışında yapılan işlemler bu rapora girmez. Gruptaki on dördüncü rapor Emergency Change Review'dur: acil değişiklikleri gerekçesi, olay bileti ve olay sonrası gözden geçirme durumuyla listeler, gözden geçirme bekleyenler önce gelir (Bölüm 27.5). Kısıtı: Auditor, DbAdmin, ChangeManager, SystemManager.

20.4 Object & Structure grubu

Rapor	Neyi gösterir	Nasıl yorumlanır
Critical Object Access	Kritik işaretli nesneye dokunan talepler. Kritiklik, talep ayrıştırıldığında kaydedilen karardır; sonraki katalog düzenlemeleri geçmişten yeniden yazmaz.	Bu listedeki her satır ayrıca incelenmelidir.
Object Change Frequency	Prosedür, fonksiyon, tetikleyici, görünüm ve tabloların ne sıklıkta değiştiği. En sık değişenler üstte.	Üstteki nesneler mimari borç veya istikrarsızlık işaretidir.
Table Structure Changes	ALTER TABLE ADD ve DROP COLUMN işlemleri, etkilenen kolon adları ve sayıları.	Veri kaybı riski en yüksek işlemler buradadır.
Data Modification Frequency	Tablo bazında INSERT, UPDATE, DELETE, MERGE ve prosedür çağrılarının sıklığı, son çalışma tarihi.	Sık elle veri düzeltmesi alan tablolar süreç sorununa işaret eder.
Multi Release Objects	Birden çok bilet altında değişen nesneler.	Birkaç takımın aynı nesneyi düzenlediği sıcak noktaları gösterir.
Active Conflicts	Aynı ortamda, farklı biletlerle, aynı nesneyi değiştirmek üzere olan açık talepler.	Çakışmayı canlıya ulaşmadan yakalamak için kullanılır.

20.5 Access & Authorization grubu

Rapor	Neyi gösterir	Kısıt
Privileged Account Operations	Talepler içindeki tüm yetkilendirme ifadeleri: GRANT, REVOKE, DENY, hesap ve rol yönetimi, hedef hesap ve verilen yetkiler.	Auditor, DbAdmin, ChangeManager, SystemManager
User DDL Activity	Kullanıcı başına CREATE, ALTER, DROP ve yetkilendirme işlem sayıları, o kullanıcının kaç talebinin yüksek riskli veya acil durum olduğu.	-
User Permission Matrix	Her hesap: rolü, hiyerarşi seviyesi, hesap durumu, kimlik doğrulama tipi,	Auditor, DbAdmin, ChangeManager, SystemManager

Rapor	Neyi gösterir	Kısıt
	bağlı kurum kimlik sağlayıcıları, son kurum hesabı girişi ve rolün tüm yetki seti. Erişim kontrolü kanıtı tek tabloda.	
User Access Changes	Hesap ve rol yaşam döngüsü: kim hesap açtı, kim yetki değiştirdi, kim sildi, canlandırdı veya kilidi açtı ve hangi adresten. Kurum hesabıyla giriş olayları da listelenir: kimlik sağlayıcısının açtığı hesaplar, gruptan eşitlenen roller, kimlik bağları, grup ile rol eşlemesi değişiklikleri, acil durum hesabıyla yapılan her giriş (kurum hesabıyla giriş açıkken yerel şifreyle giriş) ve kurum hesabıyla giriş ayarlarındaki her değişiklik.	Auditor, DbAdmin, ChangeManager, SystemManager

Expected Access Principals raporu

Expected Access Principals: ürünün her hedef sunucuda hangi hesapla, hangi makineden ve hangi adresten bağlandığını gösterir. DAM ve SIEM tarafında "beklenen kaynak" listesi bu rapordan kurulur. Rapor yetkisi: Auditor, DbAdmin, ChangeManager, SystemManager.

Filtreler: tarih aralığı (varsayılan son 30 gün) ve sunucu adı. Kayıtlı her sunucu için bir satır gelir; hiç iş yapılmamış sunucu da listelenir.

Kolon	Anlamı
ServerName, Environment, DatabaseType	Sunucu adı, ortamı ve türü (SqlServer, PostgreSQL, Oracle)
ProductLogin	Ürünün o sunucuda kullandığı SQL hesabı. Parola raporda yoktur
SeenRoles	Aralıkta görülen iş türleri (Execute, Query, Release, Sandbox, SandboxRelease), noktalı virgülle
SeenHosts	Ürünün bağlandığı makine adları, noktalı virgülle
SeenClientAddresses	Hedefin gördüğü istemci adresleri, noktalı virgülle
LastUsedAt, WindowCount	Son kullanım zamanı ve aralıktaki pencere sayısı

Sınır: Liste yalnız pencere açan işlerden (Worker) türer. API makinesinin bağlantıları (önizleme, nesne tanımlama, bağlantı deneme) pencere açmaz; API makinesinin adresi bu raporda görünmez ve ayrıca öğrenilmelidir. Rapor, kanıt niteliğinde olduğu için kirli okuma yapmaz ve hesabın parolasını içermez.

20.6 Data & Privacy grubu

Rapor	Neyi gösterir	Kısıt
Query Result Activity	Canlı veri okuyan her talep: dönen satır sayısı, alıcı adresi, istenen maskesiz kolonlar ve teslimde uygulanan maskeleme kararı.	Auditor, DbAdmin, ChangeManager, SystemManager
Sensitive Column Touches	Hassas veri kataloğundaki bir kolonu ekleyen veya silen yapısal değişiklikler, kolonun sınıflandırması ve maskeleme biçimi. Tam ve içeren kuralları maskeleme motoruyla aynı biçimde uygulanır; şema veya tabloyla sınırlı bir kural yalnızca o kapsamda eşleşir. Düzenli ifade kuralları burada tam kolon adıyla eşleştirilir.	-
Masking Activity	Her teslimde maskelemenin ne yaptığı: uygulanan politika ve rejim, kaç kolon ve kaç satır teslim edildi (DeliveredColumnCount, DeliveredRowCount), kaç hassas kolon maskelendi, kaç hassas kolon açık gitti ve bu onaylı mıydı. Maskelenen ve açık giden sayıları yalnız hassas bulunan kolonları sayar; hassas kolonu olmayan bir teslimde ikisi de sıfırdır. Onaylı maskesiz kolon isteği hiçbir kolonu açmadıysa (ad sonuçta yok ya da kolon zaten hassas değil) UnmaskRequestNoEffectCount kolonunda görünür. Maskeleme kapalıyken yapılan teslimler MaskingOff politikasıyla görünür.	Auditor, DbAdmin, ChangeManager, SystemManager
Sensitive Column Catalog	Sınıflandırma kataloğunun ve öğrenme döngüsünün durumu: aktif kurallar, kapsamları, maskeleme biçimleri ve karar bekleyen aday kolonlar. Hiçbir veri değeri içermez.	-
Masking Exempt Servers	Maskeleme rejimi gevşetilmiş sunucular: hangi mod, yazılı gerekçe, kim ne zaman ayarladı ve o sunucudan kaç teslim yapıldı.	Auditor, DbAdmin, ChangeManager, SystemManager
Manual Data Modifications	Veriyi doğrudan değiştiren talepler (DML veya prosedür çağırısı).	-
Data Access and Export Log	Kim sonuç dosyası indirdi, hangi gerekçeyle ve hangi adresten, kim	Auditor, DbAdmin, ChangeManager, SystemManager

Rapor	Neyi gösterir	Kısıt
	denetim dosyası dışı aktardı, hangi sonuç dosyası saklama süresi dolduğu için silindi, kim kısıtlı bir raporu açtı. Kişisel veri erişim izidir.	

20.7 Configuration & Compliance grubu

Rapor	Neyi gösterir	Kısıt
Configuration Changes	Kontrollerin kendisine yapılan her değişiklik, eski ve yeni değerleriyle. Ekrandan yapılanlar: sunucular, parametreler, onay politikaları, roller, SQL standartları, kritik nesneler, hassas kolonlar, desenler, mail kaynakları, ITSM biletleri, lisans, kurum kimliği rol eşlemeleri ve bakım görevleri. Ayar dosyasından yapılanlar (kayıt tipi Configuration): uygulama ayarları, kurum hesabıyla giriş, izin ve ITSM bağlantı ayarları. App.ControlRelaxed, bir kontrolü gevşeten ayar değişikliğini işaretler. AuditLogId kolonu her satırı denetim kaydındaki olaya bağlar.	Auditor, DbAdmin, ChangeManager, SystemManager
Settings Approval Trail	Ayarlarda çift kontrol kanıtı: kim değişiklik istedi, kim onayladı veya reddetti, karar ne kadar sürdü ve aynı kişi ikisini birden yaptı mı.	Auditor, DbAdmin, ChangeManager, SystemManager

20.8 Rapor okuma önerileri

Amaç	Bakılacak raporlar
Denetime hazırlık	Control Exceptions, Approval Step Detail, Settings Approval Trail, User Permission Matrix
Kişisel veri uyumu	Query Result Activity, Masking Activity, Data Access and Export Log, Masking Exempt Servers
Süreç verimliliği	Approval and Execution Duration, Work in Progress, Execution Activity

Amaç	Bakılacak raporlar
Teknik borç	Object Change Frequency, Multi Release Objects, Active Conflicts
Yetki gözden geçirme	User Permission Matrix, User Access Changes, Privileged Account Operations

20.9 Dışa aktarma

Rapor sonuçları ekranda tablo olarak gösterilir ve dosya olarak dışa aktarılabilir. Kısıtlı raporların açılması denetim kaydına yazılır ve Data Access and Export Log raporunda görünür.

Bölüm 21. Bildirimler ve E-posta

21.1 Hangi olayda kime bildirim gider

Olay	Alıcı
Talep oluşturuldu	İlgili onay adımının rolündeki kullanıcılar.
Onay adımı sıraya geldi	O adımı kapatabilecek roldeki kullanıcılar. Adım bir kişiye atanmışsa o kişi.
Talep onaylandı	Talep sahibi.
Talep zamanlandı	Talep sahibi.
Talep çalıştırıldı	Talep sahibi. Sorgu sonucu taleplerinde ayrıca alıcı listesi.
Talep reddedildi	Talep sahibi, gerekçe ile.
Onay adımı reddedildi	Talep sahibi, gerekçe ile.
Talep artık gerekli değil işaretlendi	Talep sahibi.
Otomatik çalıştırma başarısız	Bildirim kuyruğuna hata bildirimi.
Sürüm paketi başarısız	Bildirim kuyruğuna hata bildirimi.
Worker beklenmedik hata	Workers:WorkerErrorMailTo adresine kritik bildirim.

Adım bir kullanıcıya atanmışsa (talep sahibinin doğrudan yöneticisi adım rolünü karşılıyorsa) bildirim öncelikle ona gider.

21.2 Transaction içinde e-posta gönderilmez

E-posta gönderimi hiçbir zaman veritabanı işleminin içinde yapılmaz. Bunun yerine bildirim kuyruğa yazılır, işlem tamamlandıktan sonra worker kuyruğu boşaltır.

Sebebi: SMTP sunucusu yavaşsa veya erişilemezse veritabanı işlemi kilitli kalırdı. Ayrıca işlem geri alınsa bile e-posta gönderilmiş olurdu ve "gerçekleşmemiş bir olayın bildirimi" ortaya çıkardı.

Kullanıcıya yansıması: ekranda işlem tamamlandı mesajını gördükten sonra e-posta birkaç saniye içinde gelir, anında gelmeyebilir. Gönderim aralığı Workers:NotificationFlushSeconds ayarındadır.

21.3 E-posta Kaynakları ekranı

Ekran: Ayarlar > E-posta Kaynakları

Yetki: settings.email

Sorgu sonucu teslimlerinde kullanılabilecek adreslerin havuzudur.

Alan	Ne gösterir
E-posta	Adres.
Aktif	Kullanımda mı.
Onaylı	Adres onaylanmış mı. Onaysız adrese teslim ek onay adımı gerektirir.
Onaylayan / Onay zamanı	
Kaynak	Elle mi eklendi, sistem mi ekledi.

21.4 Bildirim Kayıtları ekranı

Ekran: Ayarlar > Bildirim Kayıtları

Yetki: settings.notificationlogs

Kolon	Ne gösterir
Kanal	Gönderim kanalı (e-posta).
Alıcı	Hedef adres.
Konu	E-posta konusu.
Durum	Gönderildi, başarısız, kuyrukta.
Hata	Başarısızsa sebebi.
Deneme sayısı	Kaç kez denendi.
Zaman	

Bir bildirim gitmediyse ilk bakılacak yer burasıdır. Kayıtlar 90 gün sonra bakım göreviyle silinir.

Bölüm 22. ITSM Entegrasyonu ve Bilet Numarası

22.1 Ne işe yarar

Kurumun ITSM sistemindeki kaydın (değişiklik kaydı, hizmet talebi, olay kaydı) numarasını talebe bağlar. Böylece SQL Change Guard kaydı ile kurumsal süreç kaydı eşleşir. ITSM entegrasyonu açıksa numara ITSM'de doğrulanır ve yapılan iş ITSM kaydına not olarak yazılır (Bölüm 22.5).

Ekran: Ayarlar > ITSM

Yetki: settings.itsm

22.2 Alanlar

Alan	Ne işe yarar
Kayıt no	Kayıt numarası. Numara ve tür birlikte benzersizdir.
Başlık	Biletin konusu.
Bağlantı	Bilete doğrudan gitmek için adres.
Kaynak	Satırı kimin yazdığı: Elle, Talepten ya da ITSM ürününün adı (ServiceNow, Jira, GenericRest).
Tür	Değişiklik kaydı, olay kaydı ya da hizmet talebi.
ITSM durumu	ITSM'de son görülen durum ve ürünün sınıfı (Hazır, Onay bekliyor, Kapanmış, Sınıflanamadı, Açık). Yalnız ITSM açıkken dolar.
Planlanan zaman	ITSM'deki planlanan başlangıç ve bitiş. Yalnız ITSM açıkken dolar.
Son doğrulama	Kaydın ITSM'de en son ne zaman sorgulandığı.

22.3 Zorunluluk ve biçim kontrolü

Değişiklik bileti iki parametre ile yönetilir. Acil taleplerde istenen olay (incident) numarasının kendi parametreleri vardır: EmergencyTicketRequired ve EmergencyTicketRegex. Dördü de Bölüm 7.6'da alan alan anlatılır.

Parametre	Etkisi
ChangeTicketRequired	Bilet numarasının hangi taleplerde zorunlu olduğunu belirler: Always (hepsinde), ExceptEmergency (acil olmayanlarda), Never (hiçbirinde).
ChangeTicketRegex	Girilen numaranın biçimini kontrol eder. Boş ise kontrol yapılmaz.

Parametre	Etkisi
RequestTicketRegex	Veri çıkarma talebi hizmet talebine dayanıyorsa numaranın biçimini kontrol eder. Boş ise ChangeTicketRegex uygulanır.

Örnek: ChangeTicketRequired Always ve ChangeTicketRegex ^CHG\d{7}\$ iken:

Girilen	Sonuç
CHG0012345	Kabul edilir.
CHG12345	Reddedilir, yedi hane gerekir.
0012345	Reddedilir, örnek eksik.
(boş)	Reddedilir, zorunlu.

Bilet numarası talep listesinde, raporlarda ve denetim dosyasında görünür. Çakışma raporları da bilet numarasını kullanarak aynı nesneyi farklı biletlerle değiştirmeye çalışan talepleri bulur.

22.4 Bilet listesine kayıt ne zaman eklenir

Talep kaydedilirken girilen numara ITSM kayıtları listesinde yoksa listeye eklenir. Böylece aynı numara sonraki taleplerde listeden seçilebilir. ITSM kapalıyken satırın kaynağı Talepten olur. ITSM açıkken satır ITSM'de görülen bilgilerle yazılır ve kaynağı ITSM ürününün adıdır (Bölüm 22.12). Satırın listeye hangi talepten ve kim tarafından eklendiği denetim kaydında (IsmTicket.AutoCreated) yazar.

Sıra şöyledir: önce talebin bütün kontrolleri çalışır, sonra bilet satırı eklenir, sonra talep kaydedilir. Bunun üç pratik sonucu vardır.

1. Kontrolden geçemeyen talep listeye bilet bırakmaz. Örneğin pasife alınmış bir sunucu seçildiği için kaydetme reddedilirse ITSM kayıtları listesinde yeni satır oluşmaz. Aksi halde hiç kaydedilmemiş taleplerin numaraları listede birikirdi.

2. Biçim kontrolünden geçmeyen numara listeye girmez. ChangeTicketRegex ile uyuşmayan numara hem kaydetmede reddedilir hem de listede oluşmaz.

3. Aynı bileti taşıyan talepler birbirini beklemez. Bir sürüm paketinin bütün talepleri aynı bilet numarasını taşıyabilir; bilet satırı kaydetme işleminin dışında ve kısa süreli eklendiği için talepler sıraya girmez. İki kişi aynı anda aynı numarayı ekleyecek olursa liste yine tek satır tutar ve kimseye hata dönmez.

Nasıl kontrol edilir: ITSM kapalıyken Ayarlar > ITSM ekranını açın. Listedeki olmayan bir numarayla talep kaydedin, numaranın listeye eklendiğini görün. Aynı numarayla ikinci bir talep kaydedin, listenin yine tek satır gösterdiğini görün. Biçime uymayan bir numara ile kaydetmeyi denediğinizde hem talep kaydedilmez hem de listede satır oluşmaz.

Bilet satırı ile talep arasındaki bağ tek yönlüdür: talep hangi numarayı taşıyorsa onu kullanır. Listedeki bir satırı silmek, o numarayı taşıyan talepleri etkilemez.

22.5 ITSM entegrasyonu

SQL Change Guard kurumun ITSM sistemine bağlanabilir. Desteklenen sistemler: ServiceNow, Jira (Cloud ve Data Center) ve kaydı REST API ile sunan diğer ITSM ürünleri (ServiceCore gibi). Bağlantı açıkken ürün üç iş yapar:

1. Talep kaydedilirken numarayı ITSM'de sorgular: kayıt var mı, türü doğru mu, kapanmış mı.
2. Çalıştırmadan hemen önce kaydı yeniden sorgular: değişiklik kaydı CAB tarafından onaylanmış ve uygulanabilir durumda mı.
3. Talepteki önemli adımları (açıldı, onaylandı, zamanlandı, çalıştırıldı, başarısız oldu, ITSM kontrolünde durdu) ITSM kaydına not olarak yazar.

Ürün ITSM'de kayıt açmaz, kaydın durumunu değıştirme ve ITSM'e betik metni, sonuç verisi ya da parola göndermez. Karar verilirken ITSM'de görülen durum denetim kaydına yazılır; ITSM'deki kayıt sonradan değışse bile o anki görüntü kaybolmaz.

ITSM kapalıyken (IsmEnabled = false) ürün ITSM'e hiç gitmez; numara yalnız biçim ve zorunluluk kurallarıyla kontrol edilir (Bölüm 22.3).

ITSM'deki onay ile üründeki onay farklı sorulara cevap verir. ITSM'deki CAB onayı "bu iş yapılsın mı" sorusunu cevaplar. Üründeki onay "bu betik, bu sunucuda, bu haliyle çalışsın mı" sorusunu cevaplar. İkisi de gerekir.

22.6 Kayıt türleri

Tür	Örnek	Nerede kullanılır
Değişiklik kaydı	CHG0030001	Değişiklik talebindeki "Değişiklik kaydı no" alanı
Hizmet talebi	RITM0010001	Veri çıkarma talebindeki "Hizmet talebi no" alanı
Olay kaydı	INC0012345	Acil talepteki "Olay no" alanı

ITSM açıkken talep ekranındaki alanın adı talebin türüne göre değışir; ITSM kapalıyken alan her talepte "Bilet no" olarak görünür. Veri çıkarma talebinin hangi kayda dayandığını ItsmQueryResultTicketKind belirler: Request (hizmet talebi), Change (değişiklik kaydı) ya da None (ITSM'de doğrulanmaz, alan "Bilet no" olarak görünür). Tür talep kaydedilirken talebe yazılır; parametre sonradan değışse de eski talepler kendi türüyle sorgulanır.

22.7 ITSM'deki durum nasıl okunur

Durum adları kurumdan kuruma değıştiği için ürün değışiklik kaydının durumunu dört sınıftan birine çevirir:

Sınıf	Anlamı	Nasıl belirlenir
Hazır	Çalıştırılabilir	Durum ItsmReadyStates listesinde ve, ITSM onayı ayrı bir alanda tutuyorsa, onay ItsmApprovedValues listesinde
Onay bekliyor	Açık ama henüz hazır değil	Durum hazır listesinde değil ya da onay henüz verilmemiş

Sınıf	Anlamı	Nasıl belirlenir
Kapanmış	Kapanmış ya da iptal edilmiş	Durum ItsmClosedStates listesinde. Jira'da "Done" kategorisindeki her durum
Sınıflanamadı	Hazır sayılmaz	Durum ya da beklenen onay alanı gelmedi

ServiceNow'da CAB onayı durumdan ayrı bir alandır. Ürün ikisine birden bakar: durum Implement olsa bile onay Approved değilse kayıt hazır sayılmaz. Jira'da onay iş akışındaki durumla ifade edilir; orada yalnız durum okunur.

Olay kaydı ve hizmet talebinde CAB onayı yoktur. Bunlar Açık ya da Kapanmış olarak görünür.

22.8 Talep kaydedilirken

Numara alanından çıkınca alanın yanında kaydın ITSM'deki durumu renkli bir etiketle ve altında kaydın başlığı görünür. Yanındaki düğme kaydı ITSM'de açar. Etiket yalnız bilgidir; karar kaydederken sunucuda verilir.

ITSM'in cevabı	ItsmVerifyOnSave = Block	ItsmVerifyOnSave = Warn
Kayıt var, türü doğru, kapanmamış (CAB onayı henüz olmasa da)	Kaydedilir	Kaydedilir
Kapanmış, bulunamadı ya da yanlış tür	Kaydedilmez	Kaydedilir, istisna olarak kayda geçer
ITSM'e ulaşamadı	ItsmUnavailablePolicy kuralına göre	ItsmUnavailablePolicy kuralına göre

CAB onayı kayıta aranmaz: talep CAB'dan önce hazırlanabilir. Onay çalıştırmadan önce aranır. Kaynağa bağlı geri alma talebi hiçbir sonuçta reddedilmez. Acil talepte olay numarası ItsmVerifyIncident kuralına göre aynı şekilde sorgulanır.

22.9 Çalıştırmadan hemen önce

ItsmExecuteGate = Block iken her çalışma yolunda (Çalıştır düğmesi, zamanlanmış çalışma, onaydan sonra otomatik çalışma, sürüm paketi) kayıt ITSM'de yeniden sorgulanır. Bu sorgu önbellek kullanmaz. Çalıştır düğmesinde iki kez bakılır: düğmeye basıldığında ve Worker betiği başlatmadan hemen önce, çünkü onay bu arada geri çekilmiş olabilir. Sürüm paketinin Çalıştır düğmesi de aynı şekilde çalışır: düğmeye basıldığında paketteki her talep kendi ITSM kaydıyla

kontrol edilir. Duran bir talep varsa paket kuyruğa alınmaz ve duran talepler tek mesajda listelenir.

Durum	Sonuç
Değişiklik kaydı Hazır	Çalışır
Onay bekliyor ya da Sınıflanamadı	Durur
Kapanmış, bulunamadı ya da yanlış tür	Durur
ItsmEnforceWindow = true iken planlanan aralığın dışında ya da kayıta aralık yok	Durur
Veri çıkarma talebi hizmet talebine dayanıyor, kayıt kapanmamış	Çalışır

Duran talep ölü duruma düşmez, Onaylandı olarak kalır ve ITSM kaydı uygun olduğunda yeniden çalıştırılabilir. Zamanlanmış çalıştırma durursa zamanlama temizlenir ve talep sahibi ile talebi onaylayanlara e-posta gider. Sürüm paketindeki bir talep durursa paket hiç başlamaz; böylece paketin yarısı çalışıp yarısı kalmaz.

Talep Zamanla düğmesiyle zamanlanırken ya da sürüm paketi planlanan bir saatle kaydedilirken de kayıt ITSM'de sorgulanır. Talep o saatte kesin olarak duracaksa zamanlama kabul edilmez: kayıt kapanmışsa, bulunamıyorsa, yanlış türdeyse ya da ItsmEnforceWindow = true iken zamanlanan saat planlanan aralığın dışındaysa. CAB onayı henüz yoksa, kayıta planlanan aralık yoksa ya da ITSM'e ulaşılamıyorsa zamanlama kabul edilir, çünkü bunlar o saate kadar değişebilir; karar çalıştırma anında verilir. Reddedilen zamanlama denetim kaydına ve Kontrol İstisnaları'na yazılır, ITSM kaydına not olarak gitmez. Acil talep ve kaynağa bağlı geri alma bu kontrolden de muaftır.

Bu üç durumda zamanlama kaydedilir ama kullanıcı o an uyarılır: ekranda, kapatılana kadar açık kalan bir uyarı penceresi çıkar. Örnek: değişiklik kaydı Authorize durumundayken (CAB onayı yok) talep gece 02:00'ye zamanlanırsa pencere, kayıt o saate kadar onaylanmazsa çalıştırmanın duracağını söyler. CAB 02:00'den önce onaylarsa talep o saatte çalışır. Onaylamazsa çalıştırma durur, talep Onaylandı olarak bekler, zamanlama temizlenir ve talep sahibiyle onaylayanlara e-posta gider. Sürüm paketinde uyarılar talep numarasıyla ayrı ayrı gösterilir. Uyarı bir karar değildir, denetim kaydına yazılmaz; kanıt çalıştırma anındaki ITSM kararıdır.

İki muafiyet vardır. Kaynağa bağlı geri alma talebi bu kontrolden muaftır: kaynak değişiklik uygulandıktan sonra ITSM kaydı çoğu zaman kapanır ve bozulan bir şeyin geri alınması engellenmemelidir. Acil talepte CAB onayı aranmaz, çünkü acil değişikliğin onayı çoğu kurumda

sonradan verilir; kapanmış, bulunamayan ya da yanlış türdeki değişiklik kaydı acil talepte de durdurur. Her muafiyet denetim kaydına ve Kontrol İstisnaları'na yazılır.

22.10 ITSM'e ulaşılamazsa

ITSM çökebilir, ağ kopabilir ya da entegrasyon hesabının parolası değişebilir. Ne olacağını ItsmUnavailablePolicy belirler: AllowAndRecord (varsayılan) işlemi sürdürür ve doğrulamanın yapılamadığını kayda geçirir; Block kaydı ve çalıştırmayı durdurur. Acil talep iki durumda da geçer.

"Kayıt bulunamadı" ile "ITSM'e ulaşılamadı" ayrıdır: birincisi bir kural ihlalidir, ikincisi bağlantı sorunudur. Kimlik hatası (entegrasyon hesabı ya da parolası yanlış) ulaşılamadı sayılır ve Yönetişim Kurulum Kontrolü ekranında kırmızı görünür.

Worker ITSM'e bağlanmaz; çalıştırmadan önceki kararı API'den ister. API'ye ulaşılamazsa (ağ kesintisi, API yeniden başlıyor) ItsmUnavailablePolicy uygulanır. API cevap verip karar vermezse (örneğin Worker'daki API anahtarı yanlış ya da API'de bir hata var) çalıştırma başlatılmaz: bu bir kurulum hatasıdır, ITSM'in erişilemezliği değildir ve kapıyı açmaz. Acil talep ve kaynağa bağlı geri alma iki durumda da geçer. Her iki durum da talebin ITSM doğrulamalarında gerekçesiyle görünür.

22.11 ITSM'e yazılan notlar

Talebin olayları ITSM kaydına not olarak yazılır: ServiceNow'da iş notu (work note), Jira'da yorum. Notun açık olup olmadığını ItsmWriteBackEnabled, hangi olayların yazılacağını ItsmWriteBackEvents belirler. Not talep numarasını, yapılan işi, sunucuyu, işlemi yapan kişiyi, zamanı, risk bandını ve talebe giden bağlantıyı taşır. Örnek:

SQL Change Guard #1042: executed successfully. Server: SQLPROD01. By: WorkerService (started by ayse.dba), 01.10.2026 22:06 Europe/Istanbul (UTC+03:00). Risk band: Medium. Details: <https://change-guard.kurum.local/change-requests/1042>

Notlar sırayla gönderilir. ITSM'e ulaşılamazsa notlar kaybolmaz, ITSM düzelince kaldığı yerden gider. 15 dakika boyunca hiç not gönderilemezse Itsm.WriteBackStalled alarmı bir kez yazılır. ITSM'de silinmiş bir kayda not yazılamazsa not atlanır ve bu da kayda geçer (Itsm.WriteBackSkipped).

22.12 ITSM ekranı

Ayarlar > ITSM ekranının üst kısmında bağlantı kartı bulunur: hangi ITSM'e bağlı olduğu, son sorgunun sonucu ve notların durumu. Bağlantıyı test et düğmesi örnek bir kayıt numarasını ITSM'de sorgular; görülen durumu, sınıfı, onayı ve planlanan zamanı gösterir. Bu test ITSM kapalıyken de çalışır; entegrasyonu açmadan önce ayarları doğrulamak için kullanılır.

Altındaki ITSM kayıtları listesi iki halde çalışır. ITSM kapalıyken liste talep ekranındaki öneriler içindir ve elle yönetilir; talepte yazılan numaralar da buraya eklenir. ITSM açıkken liste ITSM'in kopyasıdır ve salt okunurdur: talepte ya da çalıştırmada doğrulanan her kayıt başlığı, durumu ve planlanan zamanıyla buraya girer. Elle eklenen bir satır ITSM'de olmayan bir izin varmış gibi gösterirdi.

Talep detay ekranındaki ITSM doğrulamaları paneli o talep için yapılan her ITSM kontrolünü gösterir: zaman, aşama, karar, ITSM'deki durum, onay ve gerekçe. Aynı bilgi Denetim Dosyası'nda yer alır.

22.13 Kurulum

Bağlantı bilgileri appsettings.json dosyasındaki Itsm bölümünde durur: Provider (ServiceNow, Jira ya da GenericRest), BaseUrl, AuthType, Username ve Password ya da Token. Parola ve anahtar sırdır; üretimde ortam değişkeninde tutulur (Itsm__Password, Itsm__Token). Bu bölümdeki her değişiklik API açılışında Itsm.ConfigurationChanged olayıyla denetim kaydına yazılır.

Entegrasyon hesabına en az yetki verilir: kayıtları okuma ve not ekleme. Durum değiştirme ve silme yetkisi verilmez. API sunucusundan ITSM adresine HTTPS çıkışı gerekir; ITSM'den ürüne bağlantı gerekmez. Worker ITSM'e bağlanmaz.

Önerilen sıra:

1. appsettings.json dosyasında bağlantıyı tanımlayın ve API'yi yeniden başlatın.
2. Ayarlar > ITSM ekranında gerçek bir kayıt numarasıyla Bağlantıyı test edin.
3. ItsmReadyStates, ItsmClosedStates ve ItsmApprovedValues listelerini ITSM yöneticinizle birlikte kurumunuzun durum adlarına göre ayarlayın.
4. Bilet biçimi parametrelerini (ChangeTicketRegex, RequestTicketRegex, EmergencyTicketRegex) kurumunuzun numaralarına göre ayarlayın.
5. ItsmEnabled değerini true yapın.
6. Yönetişim Kurulum Kontrolü ekranında ITSM entegrasyonu grubunu kontrol edin.

22.14 Dikkat edilmesi gerekenler

- ITSM parametrelerinin hepsi kontrol ayarıdır: değişiklik denetim kaydına yazılır ve ayar onayı açıkta ikinci bir yöneticinin onayına düşer.
- ItsmReadyStates listesine CAB onayından önceki bir durum yazılırsa onaysız değişiklik çalıştırılabilir. Listeyi ITSM yöneticinizle birlikte belirleyin.

- Pano üzerindeki dört ITSM satırı ve ITSM Control Exceptions raporu kurala uymayan biletleri, yapılamayan doğrulamaları, durdurulan çalıştırmaları ve CAB onayı aranmadan geçen talepleri gösterir. Acil değişikliklerin sonradan gözden geçirilmesi bu listeye yapılır.

Bölüm 23. Tarih ve Saat Modeli

23.1 Saklama: her zaman UTC

Sistemdeki tüm tarih alanları DATETIMEOFFSET tipindedir ve UTC olarak saklanır. İstisna yoktur.

Etkilenen tablolar: talepler, denetim kayıtları, onay adımları, sunucular, kullanıcılar, parametreler, bakım kayıtları, bildirim kayıtları, maskeleme kayıtları ve diğerleri. Her tablodaki CreatedAt, ModifiedAt, OccurredAt, ExecutedAt, ScheduledAt gibi alanların hepsi UTC'dir.

23.2 Neden UTC saklanır

Üç sebep vardır:

1. Yaz saati uygulaması. Yerel saatte saklanan bir kayıt, saat geri alındığında aynı saatin iki kez yaşanmasına sebep olur. "02:30'da ne oldu" sorusunun iki farklı cevabı olur. UTC'de bu belirsizlik yoktur.
2. Farklı şehirlerdeki kullanıcılar. İstanbul'daki kullanıcı ile Londra'daki kullanıcı aynı olayı farklı saatlerde görür, ama kayıt tek ve tutarlıdır.
3. Sıralama. Denetim kayıtlarının doğru sıralanabilmesi için tek bir zaman eksenine gerekir.

23.3 Gösterim

Yer	Hangi saat gösterilir
Web arayüzü	Tarayıcının yerel saati. Kullanıcı ayar yapmaz, otomatik dönüşür.
Sunucu tarafında üretilen belgeler (denetim dosyası PDF, e-posta metinleri)	Display:TimeZone ayarındaki saat dilimi. Varsayılan Europe/Istanbul.
Raporlar	Rapor çıktısındaki tarihler UTC'den gösterim saat dilimine çevrilir.
Denetim kaydı	Ekranda yerel saat, veritabanında UTC.

Sunucu tarafında üretilen belgelerde tarayıcı saati bilinemez; bu yüzden merkezi bir saat dilimi ayarı kullanılır.

Yanlış saat dilimi girilirse: Uygulama belge üretimini durdurmaz, UTC'ye düşer ve günlüğe bir uyarı yazar. Ayrıca belgelerde kullanılan saat dilimi etiketi görünür, böylece okuyan kişi hangi dilimin uygulandığını görebilir. Kurulumdan sonra bir belge üretip bu etiketi kontrol etmeniz önerilir.

23.4 Somut örnek

Bir talep 2 Ağustos 2026 saat 12:00 UTC'de çalıştırıldı.

Kim bakıyor	Ne görür
İstanbul'daki kullanıcı (UTC+3)	2 Ağustos 2026, 15:00
Londra'daki kullanıcı (yaz saati, UTC+1)	2 Ağustos 2026, 13:00
Denetim dosyası PDF (Display:TimeZone = Europe/Istanbul)	2 Ağustos 2026, 15:00
Veritabanı kaydı	2026-08-02 12:00:00 +00:00

Üç görüntü de aynı anı gösterir. Kayıt tektir.

23.5 Filtrelerde yerel gün sınırı

Bir kullanıcı "2 Ağustos" için filtre uyguladığında, kastettiği kendi yerel gününün başlangıcı ve sonudur.

İstanbul'daki bir kullanıcı için 2 Ağustos:

- Başlangıç: 1 Ağustos 21:00 UTC
- Bitiş: 2 Ağustos 21:00 UTC

Sistem bu dönüşümü otomatik yapar. Kullanıcı UTC hesabı yapmak zorunda kalmaz.

Bu ayrıntı raporlarda önemlidir: aynı raporu farklı saat dilimlerinden çalıştıran iki kişi, aynı tarihi seçse bile biraz farklı kayıt kümesi görebilir. Bu bir hata değildir, her ikisi de kendi gününü doğru görmektedir.

Bölüm 24. Dil ve Yerelleştirme

24.1 Arayüz dili

Web arayüzü Türkçe ve İngilizce çalışır. Dil seçimi arayüz tarafındadır ve kullanıcı istediği zaman değiştirebilir. Tüm etiketler, mesajlar ve yardım metinleri kaynak dosyalarında tutulur.

24.2 API mesajlarının dili

API mesajları her zaman İngilizce döner. API'nin kanonik dili sabittir; istemcinin dil tercihi API cevabını değiştirmez.

Sebeup: API cevapları günlüklere, denetim kayıtlarına ve entegrasyonlara girer. Bunların dilinin isteği yapan kişiye göre değişmesi, aynı olayın iki farklı dilde kaydedilmesine yol açardı ve arama ile karşılaştırmayı zorlaştırdı.

Arayüz, aldığı cevabı kendi dil kaynaklarıyla eşleştirerek kullanıcının seçtiği dilde gösterir. Yani kullanıcı Türkçe mesaj görür, ancak arka planda kayda giren metin İngilizcedir.

24.3 Rapor çıktıları

Rapor adları, açıklamaları ve kolon başlıkları İngilizcedir. Sebeup Bölüm 20.1'de anlatıldı.

24.4 Genel kabul görmüş terimler

Rol adları gibi genel kabul görmüş teknik terimler çevrilmez. DbAdmin, ChangeManager, SystemManager her iki dilde de aynı yazılır. Bu terimlerin çevrilmesi ekipler arası iletişimi zorlaştırdı.

Bölüm 25. Bakım ve İşletme

25.1 Bakım Görevleri ekranı

Ekran: Ayarlar > Bakım

Yetki: settings.maintenance

Alan	Ne işe yarar	Varsayılan
Ad	Görevin adı.	
Açıklama	Ne yaptığı.	
Yordam Adı	Çalıştırılacak saklı yordam. INTERNAL: ile başlıyorsa uygulama içi görevdir.	
Sıklık (dakika)	Kaç dakikada bir çalışacağı.	
Zaman Aşımı (saniye)	En fazla ne kadar sürebileceği.	
Deneme Sayısı	Hata durumunda kaç kez yeniden denenecek.	
Deneme Aralığı (saniye)	Denemeler arası bekleme.	
Etkin	Görev çalışsın mı.	Açık
İç Görev	Ürünle gelen, silinemeyen görev mi.	

25.2 Varsayılan bakım görevleri

Görev	Ne yapar	Sıklık	Zaman aşımı
Expired Token Cleanup	Süresi dolmuş oturum yenileme kayıtlarını, kullanılmış ya da süresi dolmuş parola sıfırlama jetonlarını, giriş biletlerini ve kurum hesabıyla giriş isteklerini siler.	60 dakika	60 saniye
Old Notification Log Cleanup	90 günden eski bildirim kayıtlarını siler.	1440 dakika (günde bir)	120 saniye
QR File Cleanup	Saklama süresi dolan sorgu sonucu dosyalarını diskten siler ve veritabanındaki yolu temizler. QrFileRetentionDays parametresine bağlıdır.	Uygulama içi	-

25.3 Bakım kayıtları

Her çalıştırma kaydedilir: başlangıç, bitiş, süre, durum, hata mesajı, deneme numarası. Bir görev sürekli hata veriyorsa bu listeden görülür.

25.4 Tanılama ekranı

Ekran: Ayarlar > Tanılama

Yetki: settings.diagnostics

Kontrol	Ne doğrular	Sorun çıkarsa
Mail yapılandırması	Uygulamanın fiilen kullandığı SMTP ayarları. Şifre gösterilmez.	Ayarların beklediğinizle aynı olduğunu doğrulayın.
Mail testi	Verilen ayarlarla veya mevcut ayarlarla deneme e-postası gönderir.	Hata mesajı SMTP sunucusundan gelir; sunucu adı, port, kimlik bilgileri ve SSL ayarını kontrol edin.
Yönetişim Kurulum Kontrolü	Kurulum sonrası yönetim ayarlarını üretim için beklenen değerlerle karşılaştırır. Dokuz grup içerir; satır sayısı kurulumda kullanılan özelliklere (kurum hesabıyla giriş, izin, ITSM, SIEM gibi) göre değişir ve her satır canlı okunur. Satırların tamamı ve ne anlama geldikleri için bkz. Bölüm 27.8.	Dikkat gösteren satırda, o satırın Nerede yönetilir sütunundaki ekrana gidip ayarı düzeltin. Karar verin gösteren satırda düzeltilecek bir hata yoktur; kurumun bilinçli bir seçim yapması beklenir.

25.5 Worker izleme

Worker servisi her 30 saniyede bir API'ye kendi durumunu bildirir; son bildirimin üzerinden 90 saniye geçtiyse worker durmuş kabul edilir. Durum, uygulamanın üst çubuğunda her ekranda görünür ve kesintinin başlangıcı ile bitiş denetim kaydına yazılır; ayrıntısı Bölüm 19.10'dadır.

Worker çevrimdışı görünüyorsa:

1. Windows servisinin çalıştığını kontrol edin.
2. WorkerApi:BaseUrl doğru mu bakın.
3. WorkerApi:Key ile API tarafındaki Workers:ApiKey aynı mı bakın.
4. Worker günlük dosyalarına bakın.

25.6 Yedekleme önerileri

Yedeklenecek	Neden	Sıklık
Uygulama veritabanı	Tüm talepler, kurallar ve denetim kayıtları.	Kurumsal politikanıza göre.
Dış özet deposu	Defter özeti dosyaları (Evidence:Ledger:DigestOutputPath). Bağımsız doğrulamanın dayanağıdır; kurumun saklama süresi boyunca silinmeden tutulur. Silmeye ve değiştirmeye kapalı olması kurumun seçtiği depoya (WORM paylaşımı, nesne kilitli depo gibi) bağlıdır; ürün bunu sağlamaz.	Ana veritabanı ile aynı.
Şifreleme anahtarları	Security:ServerPasswordKey, Security:QrZipPasswordKey, Jwt:SigningKey ve kanıt imzalama anahtarları (Evidence:Signing:Keys; eski açık anahtarlar silinmez).	Değiştikçe.
Lisans dosyası	Yeniden kurulumda gerekir.	Değiştikçe.
appsettings dosyaları	Yapılandırmanın tamamı.	Değiştikçe.

En kritik uyarı: Şifreleme anahtarları veritabanı yedeğinin içinde değildir. Yalnızca veritabanını yedekleyip anahtarları kaybederseniz kayıtlı sunucu parolalarını ve sorgu sonucu paketlerinin parolalarını çözemezsiniz; imzalama özel anahtarı kaybolursa yeni kanıt imzalanamaz. Eski imzalı paketler açık anahtarla doğrulanmaya devam eder, bu yüzden eski açık anahtarlar ve parmak izleri saklanmalıdır. Anahtarları veritabanı yedeğinden ayrı ve güvenli bir yerde saklayın.

25.7 Çökme kurtarma eşiği

Worker bir talebi çalıştırmaya başladığında o talebi sahiplenir ve başlangıç anını kaydeder. Servis çalışma ortasında durursa (çökme, yeniden başlatma, sunucu kapanması) talep Executing durumunda kalır ve kimse onu bitirmez.

Worker her turun başında bu takılı kalmış talepleri arar. Hedefte işlem yapılmadığı kesin olan talep Approved durumuna döner; hedefte commit olmuş olabilecek talep ReconciliationRequired durumuna alınır ve yeniden çalıştırılmaz, uzlaştırma kararını bir kişi verir. Aramanın ölçütü tek bir sorudur: bu talep ne kadar süredir sahiplenilmiş durumda?

Ayar	Anlamı
Workers:StaleExecutionRecoveryMinutes	Bu süreden daha uzun süredir devam eden çalıştırmalar ölü kabul edilir.

Ayar	Anlamı
Varsayılan	120 dakika
Alt sınır	5 dakika. Daha küçük bir değer yazılırsa yok sayılır ve 120 dakika kullanılır.
Üst sınır	365 gün. Daha büyük bir değer yazılırsa 365 güne çekilir.

Sınır dışı bir değer yazıldığında worker açılışında günlüğe bir uyarı yazılır.

Eşik neden var

Eşik olmasaydı, her turun başında sahiplenilmiş her talep ölü sayılırdı. Tek worker kopyasında bu sorun çıkarmaz, çünkü turlar üst üste binmez. Ancak ikinci bir worker kopyası çalıştırıldığında, o kopyanın turu birinci kopyanın o an yürütmekte olduğu talebi ölü sayıp Approved durumuna çevirebilirdi. Talep yeniden alınabilir ve aynı betik iki kez çalışabilirdi.

Değeri nasıl seçmelisiniz

Eşik, kurumunuzdaki en uzun meşru çalıştırmadan büyük olmalıdır.

Durum	Sonuç
Eşik çok küçük	Hâlâ çalışmakta olan bir talep ölü sayılabilir.
Eşik çok büyük	Gerçekten çökmüş bir talebin kurtarılması gecikir; talep o süre boyunca Executing görünür.

Örnek: en uzun betiğiniz yaklaşık 20 dakika sürüyorsa 45 dakika makul bir değerdir. Kurtarma 45 dakika içinde gerçekleşir ve 45 dakikadan kısa süren çalıştırmalar kurtarmadan etkilenmez.

Kurtarmayı beklemek istemiyorsanız takılı kalmış talepte çalıştırmayı iptal edebilirsiniz (cr.execute yetkisi gerekir). Elle uygulandı işareti Executing durumundaki talepte kullanılamaz; yalnız Pending ve Approved durumlarında açıktır.

Kurtarmada yürütme penceresi

Kurtarılan her talebin açık kalmış yürütme penceresi, aynı turda abandoned sonucuyla kapatılır. Eşik en az 5 dakikadır; 5'ten küçük değer yok sayılır ve 120 dakika kullanılır (Worker açılışında uyarı yazılır). Eşiği aşan bir iş meşru olarak sürüyorsa kurtarma onu terk edilmiş sayar ve penceresini abandoned ile kapatır; iş bitince gerçek bitiş de yazılır ve son bitiş geçerlidir. Bu yüzden eşik en uzun meşru yürütmeden büyük olmalıdır. Değeri değiştirdikten sonra Worker yeniden başlatılmalıdır.

25.8 SIEM teslimini izleme

Ayarlar > Tanılama ekranında SIEM Durumu paneli vardır. Panel her uç için şunları gösterir: açık mı, son başarılı gönderim ne zaman oldu, teslim gecikmesi kaç kayıt, arka arkaya kaç hata alındı ve son hata neydi.

Aynı panelde Test Mesajı Gönder düğmesi bulunur. Test mesajı gerçek olaylarla aynı yoldan geçer: aynı biçimleyici, aynı taşıyıcı, aynı bağlantı. Ayrı bir yol kullanılsaydı test geçtiği halde gerçek olayların gitmediği bir durum mümkün olurdu. Test, ana anahtar kapalıyken de çalışır; kurum entegrasyonu açmadan önce bağlantının kurulduğunu görmek ister.

Yönetişim Kurulum Kontrolü ekranında dokuz SIEM kontrolü yer alır: entegrasyon açık mı, uç tanımlı mı, taşıma şifreli mi, teslim gecikmesi makul mü, son başarılı gönderim yakın zamanda mı, akış kapsamı daraltılmış mı, ciddiyet eşiği yükseltilmiş mi, betik metni gönderimi açık mı ve ürün günlüğü kuyruğundan kayıt düşürülüyor mu.

Sık karşılaşılan durumlar

Belirti	Muhtemel sebep ve çözüm
Test mesajı gidiyor ama gerçek olay gelmiyor	Worker çalışmıyordur. Windows servisinin durumunu kontrol edin. Test mesajını API gönderir, gerçek olayları worker taşır.
Teslim gecikmesi sürekli büyüyor	Toplayıcı gönderimi kabul ediyor ama yavaş işliyor olabilir ya da parti büyüklüğü olay hızının altında kalmıştır. BatchSize değerini yükseltin.
Bağlantı reddediliyor, hata sertifika diyor	TlsServerCertThumbprint değeri toplayıcının sertifikasıyla uyuşmuyordur. Ürün bu durumda şifresiz gönderime düşmez; bağlantıyı reddeder.
Bazı olaylar gelmiyor	SiemMinSeverity eşiği yükseltilmiş veya SiemStreams daraltılmış olabilir. Her iki

Belirti

Muhtemel sebep ve çözüm

değişiklik de SOC'a ayrı bir olay olarak duyurulur; toplayıcıda bu duyuruyu arayın.

Ürün günlüğü kayıtları eksik

Bu akışta kayıp mümkündür ve bilinçlidir. AppLogQueueSize değerini yükseltin veya AppLogMinLevel seviyesini yükselterek hacmi düşürün.

25.9 SOC bağlantısını toplayıcı olmadan doğrulama

Kurulum sırasında kurumun SOC toplayıcısı her zaman hazır olmaz; çoğu zaman güvenlik ekibinin ayrı bir takvimi vardır. Ürünün doğru gönderdiğini beklemeden görmek için küçük bir dinleyici yeterlidir: bir portu dinleyip gelen satırı ekrana yazan bir program.

Aşağıdaki betik PowerShell 7 penceresinde çalıştırılır ve başka bir kurulum gerektirmez:

& {

 \$listener = \$null

 try {

 \$listener = [System.Net.Sockets.TcpListener]::new([System.Net.IPAddress]::Loopback, 6514)

 \$listener.Start()

 Write-Host "Dinleniyor: 127.0.0.1:6514 (Durdurmak için Ctrl+C)" -ForegroundColor Green

 while (\$true) {

 \$client = \$listener.AcceptTcpClient()

 \$stream = \$client.GetStream()

 \$buffer = New-Object byte[] 65536

 while ((\$read = \$stream.Read(\$buffer, 0, \$buffer.Length)) -gt 0) {

 \$msg = [System.Text.Encoding]::UTF8.GetString(\$buffer, 0, \$read)

 Write-Host "Gelen Mesaj: \$msg"

 }

 \$client.Close()

```

    }
}
finally {
    if ($null -ne $listener) {
        $listener.Stop()
        Write-Host "Dinleyici kapatildi." -ForegroundColor Yellow
    }
}
}

```

Sonra appsettings.json dosyasında syslog ucunun Host değerini 127.0.0.1, Port değerini 6514 ve Protocol değerini Tcp yapın, API'yi yeniden başlatın. Ayarlar > Tanılama > SOC / SIEM ekranından Test Mesajı Gönder düğmesine basın. Dinleyici penceresinde ham syslog satırı görünür.

Bu deneme üç şeyi birden gösterir. Birincisi ürün gerçekten bağlantı açıyor. İkincisi mesajı beklenen biçimde yazıyor; SOC mühendisi satırı görüp kendi ayrıştırma kuralını daha kurulum bitmeden yazabilir. Üçüncüsü toplayıcı kapalıyken kayıt kaybetmiyor.

Üçüncüsünü görmek için şu sırayı izleyin: dinleyiciyi Ctrl+C ile kapatın, üründe birkaç talep oluşturun, SOC / SIEM ekranında Son hata sütununun dolduğunu ve teslim gecikmesinin büyüdüğünü görün, sonra dinleyiciyi yeniden başlatın. Biriken kayıtlar sırayla akar, gecikme sıfıra iner ve Son hata sütunu temizlenir.

Dinleyici şifreli bağlantı kabul etmez; Protocol değeri Tls iken el sıkışma başarısız olur ve ekranda sertifika hatası görünür. Bu düzen yalnız kurulum denemesi içindir. Kurum toplayıcısına geçerken Host, Port ve Protocol değerleri gerçek toplayıcıya göre doldurulur ve Protocol değeri Tls yapılır.

Bölüm 26. Sorun Giderme

26.1 Uyarı ve hata mesajları sözlüğü

Aşağıdaki tablo, kullanıcının karşılaşılabileceği mesajları, nerede çıktığını, sebebini ve çözümünü verir.

Yetki mesajları

Mesaj (TR)	Mesaj (EN)	Nerede	Sebep	Çözüm
Bu işlem için yetkiniz yok.	You don't have permission for this action.	Her yerde	Rolünüzde gerekli yetki yok.	Yöneticinizden yetki isteyin.

Mesaj (TR)	Mesaj (EN)	Nerede	Sebep	Çözüm
Yeni talep oluşturma yetkiniz yok.	You don't have permission to create requests.	Talep ekranı	cr.add yetkisi yok.	Rolünüzü kontrol ettirin.
Bu isteği düzenleme yetkiniz yok.	You don't have permission to edit this request.	Talep detayı	Talebin sahibi değilsiniz.	Talep sahibiyle iletişime geçin.
Script çalıştırma yetkiniz yok.	You don't have execute permission.	Talep detayı	cr.execute yetkisi yok.	Yetkili bir kullanıcıdan çalıştırmasını isteyin.
Bu işlem için onay yetkisi gereklidir.	Approval permission is required.	Talep detayı	cr.approve yetkisi yok.	Yetkili onaylayıcıya yönlendirin.
QR dosyasını indirme yetkiniz yok.	You don't have permission to download this QR file.	Talep detayı	QrRequesterCanDownload kapalı veya rolünüz QrDownloadMinimumRole eşliğinin altında.	Bölüm 7.7.
Denetçi rolüne onaylama veya çalıştırma yetkisi verilemez.	The auditor role cannot be granted approve or execute permissions.	Roller ekranı	Denetçi görevler ayrılığı gereği akışa giremez.	Farklı bir rol kullanın.
Bu hesap kapatılmıştır.	This account has been closed.	Giriş ekranı	Kullanıcı silinmiş.	Yöneticinize başvurun.

Durum mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Sadece Pending durumundaki istekler onaylanabilir.	Only Pending requests can be approved.	Talep zaten onaylanmış veya kapanmış.	Sayfayı yenileyin.
Sadece Approved durumundaki istekler çalıştırılabilir.	Only Approved requests can be executed.	Talep henüz onaylanmamış.	Onay sürecinin tamamlanmasını bekleyin.
Sadece Approved durumundaki istekler zamanlanabilir.	Only Approved requests can be scheduled.	Aynı sebep.	
Tamamlanmış veya iptal edilmiş istekler düzenlenemez.	Completed or cancelled requests cannot be edited.	Talep ölü durumda.	Yeni talep açın veya mevcut talebi kopyalayın.

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Bu durumda {{0}} {1} yapılamaz.	Cannot perform '{1}' in status: {0}.	İşlem mevcut durumla uyumsuz.	Bölüm 11.1'deki geçiş matrisine bakın.
Sadece zamanlanmış Approved isteklerin zamanlaması iptal edilebilir.	Only scheduled Approved requests can have their schedule cancelled.	Talepte zamanlama yok.	

Görevler ayrılığı mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
İstek sahibi kendi isteğini onaylayamaz.	The requester cannot approve their own request.	RequesterCanSelfApproveExecute kapalı.	Başka bir onaylayıcıya yönlendirin.
İstek sahibi kendi scriptini çalıştıramaz.	The requester cannot execute their own script.	Aynı ayar.	Yetkili başka kişi çalıştırmalı.
Bu talebi onaylayan kişi aynı talebi çalıştıramaz.	The person who approved this request cannot execute it.	ApproverCanExecute kapalı.	Farklı bir yetkili çalıştırmalı.

Geri alma mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Bu sunucu için çalıştırmadan önce rollback kaydı zorunludur.	A rollback record is required before execution on this server.	Sunucuda "Rollback Zorunlu" açık ve geri alma yok.	Geri alma talebi oluşturun.
Bu talep için zaten aktif bir rollback kaydı var.	An active rollback already exists for this request.	İkinci geri alma denemesi.	Mevcut geri almayı kullanın.
Rollback yalnızca talebin sahibi tarafından oluşturulabilir.	Rollback can only be created by the owner of the request.	Sahibi değilsiniz.	Talep sahibinden isteyin.
Kaynak talep henüz çalıştırılmadı.	The source request has not been executed yet.	Geri alma, kaynak uygulanmadan çalıştırılmaz.	Önce kaynak talebi çalıştırın.
Rollback sadece Change tipindeki talepler için oluşturulabilir.	Rollback can only be generated for Change type requests.	Sorgu sonucu talebinde geri alma yoktur.	-
Rollback tipi talepler kopyalanamaz.	Rollback type requests cannot be copied.		Kaynak talebi kopyalayın.

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Rollback talebi kaynak talebin sunucusuyla eşleşmelidir.	The rollback request server must match the source request server.	Sunucu değiştirilmiş.	Aynı sunucuyu seçin.
Kaynak talebin scriptleri düzenlendiği için mevcut rollback geçersiz kılındı.	The existing rollback was superseded because the source request scripts were edited.	Kaynak değişti, eski geri alma artık uymuyor.	Talep yeniden onaylandığında güncel geri alma oluşur; otomatik kapalıysa elle oluşturun.

Sürüm paketi ve sandbox mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Bu talep '{0}' yayın paketi altında. Önce paketten çıkarın.	This request is under release package '{0}'. Remove it from the package first.	Talep aktif pakette.	Paketten çıkarın veya paket üzerinden ilerleyin.
Sürüm paketine yalnızca değişiklik talepleri eklenebilir.	Only change requests can be added to a release package.	Sorgu sonucu talebi eklenmeye çalışıldı.	Bölüm 15.6.
Sorgu sonucu talepleri release paketi içinde çalıştırılmaz.	Query result requests cannot be executed inside a release package.	Maskeleme ve kayıt yalnızca kendi akışında üretilir.	Talebi tek başına çalıştırın.
Oracle sunucuları şu an release paketlerinde desteklenmemektedir.	Oracle servers are not currently supported in release packages.	Bilinen sınır.	Oracle taleplerini tek tek çalıştırın.
Sandbox yalnızca 'Change' tipindeki talepler için geçerlidir.	Sandbox is only available for 'Change' type requests.		-
Paket başlatılmadı: #{0} numaralı talep ITSM kontrolünden geçemedi. {1}	The package was not started: request #{0} did not pass the ITSM check. {1}	Paketteki bir talebin ITSM kaydı çalıştırmaya hazır değil.	Mesajdaki gerekçeye göre ITSM kaydını düzeltin ya da talebi paketten çıkarın. Bölüm 22.9.
Paket zamanlanamadı: #{0} numaralı talep planlanan saatte ITSM kontrolünden geçemez. {1}	The package could not be scheduled: request #{0} would not pass the ITSM check at the scheduled time. {1}	Kayıt kapanmış ya da planlanan saat ITSM'deki aralığın dışında.	Saati ITSM'deki planlanan aralığın içinde seçin ya da talebi paketten çıkarın. Bölüm 22.9.
ITSM kontrolü zamanlamayı durdurdu: {0}	The ITSM check stopped the scheduling: {0}	Tek talep zamanlanırken aynı kontrol.	Saati planlanan aralığın içinde seçin ya da ITSM kaydını düzeltin.

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Paketteki {0} numaralı talep için görevler ayrılığı kuralı çalıştırmanıza izin vermiyor.	Segregation of duties does not allow you to execute request {0} contained in the package.	Paketi başlatan ya da planlanan saatle kaydeden kişi, paketteki bir talebin sahibi ya da onaylayanıdır.	Paketi başka bir yetkili başlatsın ya da planlanan saatle kaydetsin.
Paket başlatılmadı: görevler ayrılığı kuralı, paketi başlatan {1} kullanıcısının #{0} numaralı talebi çalıştırmasına izin vermiyor.	The package was not started: segregation of duties does not allow {1}, who started the package, to execute request #{0}.	Worker paketi başlatmadan önceki kontrolde aynı kuralı uyguladı.	Paketi başka bir yetkiliyle yeniden kurun.

Ayar onayı mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Değişiklik onaya gönderildi. Onaylanana kadar mevcut değer geçerlidir.	The change was sent for approval.	Dört göz kuralı devrede.	Yetkili bir meslektaşınızdan onay isteyin.
Bu kayıt için onay bekleyen bir değişiklik zaten var.	There is already a pending change for this record.	İkinci istek.	Önce mevcut isteği sonuçlandırın.
Bu değişiklik için karar zaten verilmiş.	A decision has already been made for this change.	Başkası sizden önce karar verdi.	Listeyi yenileyin.
Kendi talep ettiğiniz ayar değişikliğini onaylayamaz veya reddedemezsiniz.	You cannot approve or reject a settings change you requested yourself.	Dört göz kuralı.	Aynı yetkiye sahip başka bir kullanıcı karar vermeli.
Reddetme gerekçesi zorunludur.	A rejection reason is required.	Gerekçe boş.	Gerekçe yazın.
Değişiklik onaylandı ancak uygulanamadı: {0}	The change was approved but could not be applied: {0}	Onay anında komut hata verdi.	Gerekçeyi okuyun, sorunu giderip yeniden isteyin.
Dört göz kuralı için parametre yetkisine sahip en az iki kullanıcı gerekir.	The four eyes rule needs at least two users holding the parameters permission.	Tek yetkili kullanıcı var.	İkinci yetkili kullanıcı tanımlayın.

Sunucu ve lisans mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Sunucu aktif değil: {0}	Server is not active: {0}	Sunucu pasife alınmış.	Sunucuyu aktif edin veya başka sunucu seçin.

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Bu sunucunun veritabanı tipi {{0}} lisansınız tarafından desteklenmiyor.	This server's database type {{0}} is not covered by your license.	Lisans kapsamı dışı.	Lisansınızı güncelleyin.
Seçilen sunucunun veritabanı tipi {{0}} talep sunucusu tipi {{1}} ile uyuşmuyor.	The selected server type {{0}} does not match the request server type {{1}}.	Farklı türde sunucular karıştırılmış.	Aynı türde sunucular seçin.

Talep içeriği mesajları

Mesaj (TR)	Mesaj (EN)	Sebep	Çözüm
Talep en az 1 script içermelidir.	A request must have at least 1 script.	Boş talep.	Betik ekleyin.
QueryResult tipi talepler için yalnızca 1 script eklenebilir.	QueryResult requests can only have 1 script.	Çoklu betik denemesi.	Sorguyu tek betikte birleştirin.
En erken zamanlama tarihi: {0} (minimum {1} saniyelik gecikme).	Earliest schedule date: {0} (minimum delay: {1} seconds).	Seçilen tarih çok yakın.	Daha ileri bir tarih seçin. Bölüm 6.4.
Tam maskeleyme dışında bir rejim seçtiğinizde gerekçe zorunludur.	A reason is required when a mode other than full masking is selected.	Muafiyet gerekçesi boş.	Yazılı gerekçe girin.

Çalıştırma günlüğü notları

Not	Anlamı
-- {0} blok başarıyla çalıştı; {1}. blokta HATA alındı ve yürütme durdu.	Kaçta kadar çalıştığını ve nerede durduğunu gösterir.
-- ORACLE ATOMİKLİK NOTU: ...	Oracle hedefte, hata öncesi çalışan DDL ifadeleri kalıcı olabilir. Kalıntı durumu inceleyin ve gerekirse geri alma talebini elle çalıştırın.
-- Detection time budget exceeded; unscanned columns were masked.	Hassas veri tespiti süre bütçesini aştı, taranamayan kolonlar güvenli tarafta maskelendi.

26.2 Sık karşılaşılan senaryolar

Giriş yapılamıyor

Kontrol	Ne yapmalı
Hesap kilitli mi	Ardışık hatalı denemeler hesabı kilitler. Auth:AccountLockoutMinutes kadar bekleyin veya yöneticiye kilidi açtırın.
Hesap silinmiş mi	"Bu hesap kapatılmıştır" mesajı geliyorsa yönetici hesabı canlandırmalıdır.
LDAP mı yerel mi	LDAP hesabında şifre kurum dizininden değişir.
İki adımlı doğrulama	Hesabınızda iki adımlı doğrulama kuruluysa doğrulayıcı uygulamadan kod girmeniz gerekir. Kurulu değilse kod istenmez. Kurumunuz kaydolmayı zorunlu tuttuysa, kurulu olmayan hesapta giriş sonrası doğrudan kurulum adımı açılır ve tamamlanmadan başka bir ekrana geçilemez. Bkz. Bölüm 2.4.9.
Kurum hesabı mı	Kurum hesabı tipindeki hesap şifre ekranından giremez; "... ile giriş yap" düğmesini kullanın. Dönüşte "yöneticinize başvurun" diyen bir mesaj görürseniz grubunuz bir role eşlenmemiş ya da hesabınız başka bir kimliğe bağlıdır; yöneticiniz Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranından kontrol eder.

Sunucuya bağlanılamıyor

Kontrol	Ne yapmalı
Bağlantı testi	Ayarlar > Sunucular ekranından test edin, mesajı okuyun.
Ağ ve port	Güvenlik duvarını ve port numarasını kontrol edin.
Kimlik bilgileri	Şifre değişmiş olabilir.
Şifreleme anahtarı	Security:ServerPasswordKey değiştiyse eski şifreler çözülemez. Şifreyi yeniden girin.
Lisans	Veritabanı türü lisans kapsamında mı.

Talep çalışmıyor

Kontrol	Ne yapmalı
Durum	Talep Approved mı.
Bekleyen onay adımı	Talep detayında hangi adımda beklediğine bakın.
Zamanlama	Zamanlanmışsa zamanı gelmemiş olabilir.
Geri alma zorunluluğu	Sunucuda "Rollback Zorunlu" açıksa geri alma oluşturun.
Asla atlanamaz bulgu	Böyle bir bulgu varsa otomatik çalıştırma yapılmaz, elle çalıştırın.
Worker	Worker çalışıyor mu.
Aktif paket	Talep bir sürüm paketinde olabilir.

Worker çalışmıyor

Kontrol	Ne yapmalı
Servis durumu	Windows servisini kontrol edin.
MainWorkEnabled	Bayrak false olabilir.
API anahtarı	WorkerApi:Key ile Workers:ApiKey aynı mı.
Günlükler	Worker günlük dosyalarına bakın.

Rapor boş geliyor

Kontrol	Ne yapmalı
Tarih aralığı	Varsayılan son 30 gündür. Aralığı genişletin.
Sunucu filtresi	Yanlış sunucu seçilmiş olabilir.
RoI kısıtı	Kısıtlı raporlarda yetkiniz olmayabilir.
Modül	InsightsReporting modülü lisanslı mı.
Veri	Gerçekten o dönemde kayıt olmayabilir. Bu iyi bir sonuç da olabilir.

E-posta gitmiyor

Kontrol	Ne yapmalı
Mail:Enabled	Kapalı olabilir.
Mail:DevMode	Açıksa tüm e-postalar test adresine gider.
Bildirim kayıtları	Ayarlar > Bildirim Kayıtları ekranından hata mesajını okuyun.
Mail testi	Ayarlar > Tanılama ekranından deneme e-postası gönderin.
Worker	Bildirimleri worker gönderir; çalışıyor mu.

Bölüm 27. Yönetişim Kontrolleri ve Şeffaflık

Bu bölüm, bir kontrolün var olmasıyla işlemesi arasındaki farkı kapatan mekanizmaları anlatır. Kural kitapta yazılı olabilir; asıl soru, kurala uyulmadığında bunun kimseye sormadan görülüp görülmediğidir.

27.1 Eksik yönetim adımı göstergesi

Talep listesinde ve talep detayında, yapılması gereken ama yapılmamış adımlar kırmızı bir rozetle görünür. Rozetin üzerine gelindiğinde eksikler madde madde okunur. Detay ekranında aynı bilgi sayfanın en üstünde bir panel olarak durur.

Rozetin gösterdiği durumlar altı tanedir. Sunucu geri alma planı zorunlu kılıyor ama plan yok. Geri alma planı var ama betiği eksik. Otomatik geri alma planı üretilmedi. İzole deneme zorunlu ama hiç yapılmadı. Son deneme başarısız. Deneme başarılıydı ama betik sonradan değişti.

Rozet yalnız canlı taleplerde çıkar: onay bekleyen, onaylanmış (çalıştırma bekleyen), çalışan ve uzlaştırma bekleyen. Ölü talepler (çalıştırılmış, reddedilmiş, elle uygulanmış, artık gerekli değil) işaretlenmez. Bir talebin kapandığı gün yürürlükte olan kural bugünkünden farklı olabilir; kapanmış talebi bugünün kuralıyla işaretlemek geriye dönük ve yanlış bir suçlama üretir.

Rozet yalnız değişiklik taleplerinde çıkar. Sorgu talebinde geri alma ve izole deneme kavramı yoktur; oraya rozet koymak listeyi anlamsız uyarıyla doldurur ve zamanla bütün rozetlerin göz ardı edilmesine yol açar.

Ekran ile komut aynı cevabı verir. Eksiği olan bir talepte çalıştırma ve zamanlama düğmeleri kapalıdır ve düğmenin üzerine gelindiğinde aynı gerekçe yazar. Bu eksikler için ekranın izin verip sunucunun reddettiği bir durum oluşmaz; değerlendirme tek bir yerde yapılır ve hem ekrana hem komuta aynı kaynaktan verilir. Onay zinciri, ITSM ve kanıt yazma sınırı gibi işlem anı kontrolleri düğme açıkken de işlemi durdurabilir (Bölüm 11.5).

27.2 İzole deneme zorunluluğu

Ayarlar > Sunucular ekranında her sunucu için İzole deneme zorunlu seçeneği vardır. Açık olduğunda bir değişiklik ancak güncel ve başarılı bir izole deneme varsa çalıştırılabilir. Sunucu listesinde bu ayar ayrı bir rozet olarak görünür; hangi sunucuların koruma altında olduğu tek bakışta okunur.

Güncellik şöyle belirlenir: deneme sonucunun oluşma zamanı, talebin son değişiklik zamanından sonra olmalıdır. Betik denemeden sonra düzenlenirse deneme bayat sayılır ve çalıştırma yeniden engellenir. Bu, en yanıltıcı durumu kapatır: eski betiğin başarılı sonucuna dayanarak yeni betiğin üretime gitmesi.

Kural üç alıřtırma yolunda da aynıdır: elle alıřtırma, zamanlanmış alıřtırma ve sürüm paketi. Kural tek bir serviste toplanmıştır; kopyalanmadığı için üç yol zamanla farklı davranmaz. Paket, tek tek alıřtırmanın yerine geçmez; paketteki her talep için deneme durumu ayrıca doğrulanır. Bayrak modüle baėlıdır: ilgili modül lisanslı deėilse bayrak açık olsa bile kapı alıřmaz, bu yüzden yönetim kurulum kontrolü bayrağın deėeri yerine modülün lisanssız olduğunu yazar.

Varsayılan kapalıdır. Ayar açılmadan önce o sunucu için sandbox ortamının tanımlı olduğundan emin olunmalıdır; aksi halde o sunucuda hiçbir deėişiklik alıřtırılmaz hale gelir. Ayarın kapatılması denetim izine ayrı bir olay adıyla yazılır, böylece kontrolün ne zaman ve kim tarafından gevşetildiėi tek sorguyla görülür.

Oracle örtülü commit üreten deėişikliklerde izole deneme yalnızca güvenli senaryolarda alıřır. Bu tür deėişikliklerde koruma izole denemeden deėil, zorunlu geri alma planından gelir.

27.3 Geri alma planının bütünlüėü

Geri alma betiėi üretilirken hedef sunucudan nesne tanımı alınamayabilir: aė kesintisi, bakım penceresi ya da nesnenin bulunamaması. Böyle durumlarda betiėe bir eksiklik iřareti konur ve o betik artık geerli bir geri alma sayılmaz.

Sunucuda geri alma zorunluysa yarım betikle alıřtırma engellenir, ekranda sebebi yazar ve talep listesindeki rozet eksikėi gösterir. Yarım bir planla üretime çıkmak, plan olmadan çıkmaktan daha tehlikelidir; çünkü ekte plan var sanılır ve olay anında bunun yanlış olduğu anlaşılr.

Otomatik geri alma üretimi onay anında sistem bağlamında alıřır. Üretim, onayı veren kullanıcının talep ekleme yetkisine baėlı deėildir. Görevler ayrılığının doğru kurulduğu bir kurumda onaylayan kullanıcı zaten talep ekleyemez; üretimi bu yetkiye bağlamak, kontrolü doğru kuran kurumu cezalandırırdı.

Üretim başarısız olursa talep sessizce onaylı kalmaz. Talepte üretilemedi bilgisi, zamanı ve hata sebebi saklanır; olay denetim izine sistem adına yazılır ve ekranda görünür. Sonradan bir geri alma planı oluşturulduğunda bu iřaret kendiliėinden temizlenir.

Üretilecek bir řey olmaması bir hata deėildir. Yalnız okuma yapan ya da geri alınacak bir etkisi olmayan bir betik için plan üretilmemesi normaldir ve bu durum başarısızlık olarak iřaretlenmez.

Tablo tanımından üretilen geri alma betiėi birincil anahtar, benzersizlik kısıtları, kontrol kısıtları, yabancı anahtarlar ve indeksleri içerir. Kapsam dışında kalan öğeler betiėin başında tek bir açıklama satırıyla belirtilir. Bu açıklama SQL Server, PostgreSQL ve Oracle için tek bir metin kaynağından gelir; üç veritabanı türünde farklı uyarı metinleri oluşmaz.

27.4 Engellenen görevler ayrılığı girişimleri

Görevler ayrılığı parametreleri (RequesterCanSelfApproveExecute, ApproverCanExecute) kapalıyken bir kullanıcı kendi talebini onaylamaya veya çalıştırmaya kalktığında sistem işlemi engeller. Kurulum varsayılanında bu parametreler açıktır ve engelleme olmaz. Engelleme denetim izine kendi olay adıyla yazılır: onay denemesi ChangeRequest.ApproveDenied, çalıştırma denemesi ChangeRequest.ExecuteDenied adıyla kaydedilir. Kayıt talep numarasını, engelleme sebebini ve girişimde bulunan kullanıcıyı içerir.

Kaydın değeri şudur: engellenen girişim, kontrolün çalıştığının kanıtıdır. Kaydı olmayan bir kural için denetçi gerçekten engelliyor mu yoksa hiç denenmedi mi sorusuna cevap veremez.

Tekrarlayan girişimler ayrıca bir davranış sinyalidir ve kurumun kendi iç değerlendirmesine girdi olur.

Denetim kaydının yazılamaması işlemin sonucunu değiştirmez. Engelleme her koşulda geçerlidir; kayıt hatası yalnızca uygulama günlüğüne düşer. Kanıt üretimi korumanın önüne geçemez.

Kayıtlar Kontrol İstisnaları raporunda talep bazında görünür: kaç girişim olduğu ve kimlerin denediği ayrı kolonlarda listelenir. Bu bir kanıt rapordur ve kirli okuma ipucu kullanmadan çalışır. Tek tek kayıtlar Denetim Kaydı ekranındadır. Olay adı filtresi TAM eşleşme yapar; adın bir parçasını yazmak sonuç döndürmez ve kayıt hiç yokmuş gibi görünür. İki olay adı birlikte aranacaksa aralarına noktalı virgül konur:

ChangeRequest.ApproveDenied;ChangeRequest.ExecuteDenied. Kontrol panelindeki Engellenen görevler ayrılığı girişimi satırına tıklandığında bu ekran zaten doğru adlarla açılır.

27.5 Acil değişiklik gözden geçirme

Acil yol onayı atlamaz, kısaltır: onay olaydan önce alınır ve acil politikanın en az bir adımı atlanamaz olmak zorundadır. Buna ek olarak, uygulanmış her acil değişiklik için olay sonrası bir gözden geçirme kaydı tutulur.

Panel talep detayının üst kısmında görünür. Panelde talebi açan, çalıştıran, acil gerekçesi ve olay bileti yazar. Onay yetkisi olan bir kullanıcı iki soruyu cevaplar (değişiklik gerçekten acil miydi, kalıcı çözüm için talep açıldı mı) ve zorunlu bir not yazar. Not boş bırakılamaz; notsuz bir gözden geçirme kaydı kanıt değeri taşımaz.

Gözden geçirme bir onay değildir ve yaptırım üretmez. Hayır, planlanabilirdi cevabı verilse bile talep geri alınmaz, kimse uyarılmaz; cevap yalnızca kayda geçer. Yaptırım eklenseydi insanlar dürüst cevap vermeyi bırakır ve kaydın değeri biterdi. Amaç ceza değil, örüntüyü görünür kılmaktır: aynı ekipten her ay çıkan acil değişiklik, sürecin değil planlamanın sorununu gösterir.

Kısıtlar şunlardır. Talebi açan kişi kendi talebini gözden geçiremez. Gözden geçirme yalnız uygulanmış talepler için yapılır. Uygulanmış sayılan durumlar şunlardır: değişiklik çalıştırıldı, elle uygulandı, ya da Oracle hedefte çalıştırma sırasında düştü. Sonuncusu hedef veritabanına bağlıdır. SQL Server ve PostgreSQL hedeflerde bir talebin bütün blokları tek transaction içinde çalışır; hata alındığında hepsi geri alınır ve üretimde bu talepten hiçbir şey kalmaz, dolayısıyla gözden geçirilecek bir olay da yoktur. Oracle tarafında DDL ifadeleri örtük olarak kaydedildiği için hatadan önce çalışan bloklar üretimde kalabilir; gözden geçirmeye en çok ihtiyaç duyulan olay budur. Bir kez yapılır ve sonradan değiştirilmez. Yetki hem oturum jetonundan hem canlı veritabanından doğrulanır; yetkisi çekilmiş bir kullanıcı elindeki jetonla gözden geçirme yapamaz.

Kontrol panelinde gözden geçirilmemiş acil değişiklik sayacı vardır; tıklandığında doğrudan bekleyen talepler listelenir. Sayaç seçilen tarih aralığından etkilenmez, çünkü bekleyen bir borç geçmiş bir olay değildir ve tarih aralığı daraltıldığında görünmez olmamalıdır. Sayaç, talep listesindeki filtre, listedeki Gözden Geçirilmedi rozeti ve talep detayındaki düğme aynı tanımı kullanır: uygulanmış ve henüz gözden geçirilmemiş acil talepler. Dördünün aynı tanımı kullanması, panelde görünmeyen bir işin talep detayında yapılabilir görünmesini ya da listede rozet taşımayan bir talebin panoda sayılmasını engeller. Bu yüzden çalıştırma sırasında düşmüş bir acil talep de listede rozet taşır.

Acil Değişiklik Gözden Geçirme raporu acil değişiklikleri gerekçeleri, olay biletleri ve gözden geçirme durumlarıyla listeler. Bekleyenler önce gelir ve kaç gündür beklediği yazar. Kayıt ayrıca talebin denetim dosyasına ayrı bir bölüm olarak girer; denetçi kanıt paketini açtığında gözden geçirmenin yapıp yapılmadığını orada görür.

27.6 Maskesiz kolon onayının risk bandına etkisi

Sorgu sonucunda maskesiz hassas kolon gösterilmesine onay verildiğinde talebin risk bandı yeniden hesaplanır. Betik değişmemiştir ama talep gerçekten daha riskli hale gelmiştir; bandın bunu yansıtmaması, bandı okuyan kişiyi yanıltır.

Yeniden hesaplama kaydedilmiş bulgu ayrıntılarından yeniden kurgulanır ve her bulgunun tekrar sayısı korunur. Böylece yeni bir bulgu eklenmesi, eski bulguların ağırlığını değiştirmez. İşlem tekrar edilebilirdir: aynı onay iki kez işlense bile bulgu bir kez eklenir.

Bulgu risk açıklamasında ayrı bir satır olarak görünür, böylece bandın neden yükseldiği okunabilir. Kritiklik derecesi SQL Standartları ekranından yönetilir: kurum kendi eşliğini seçer ya da standardı pasife alarak kuralı tamamen kapatır.

27.7 İlk girişte parola değiştirme

Kurulumla gelen yönetici hesabı ilk girişte parolasını değiştirmek zorundadır. Aynı kural, yöneticinin parolasını sıfırladığı hesaplar için de geçerlidir.

Parola değiştirmesi gereken kullanıcının oturum jetonu ayrı bir işaret taşır. Bu işaret varken istek hattındaki bir katman, parola değiştirme ve jeton yenileme dışındaki bütün istekleri reddeder. Yani o oturum parola değiştirmekten başka hiçbir işe yaramaz.

Kontrol sunucuda yapılır. Arayüzün kullanıcıyı parola ekranına yönlendirmesi kullanım kolaylığıdır, güvenlik sınırı değildir; arayüz atlansa bile sunucu isteği reddeder. Parola değiştirildiği anda yeni jeton işareti taşımaz ve oturum normale döner; yeniden giriş yapmak gerekmez.

Parolası hâlâ değişmemiş hesaplar Ayarlar > Kullanıcılar listesinde ayrı bir rozetle görünür. Böylece kimsenin bakmadığı bir hesap kurulum parolasıyla yaşamaya devam etmez ve yönetici listeye bakarak eksik hesabı görür.

27.8 Yönetişim kurulum kontrolü ekranı

Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranı, kurulum sonrası yönetim ayarlarını üretim için beklenen değerlerle karşılaştırır. Her satır o anki değerinden canlı okunur; ekran kaydedilmiş bir rapor değildir, açıldığı anın durumunu gösterir. Amacı bir not vermek değil, hiçbir ayarın farkında olunmadan varsayılan değerinde kalmamasını sağlamaktır.

Kontroller dokuz grupta toplanır: görevler ayrılığı, geri alma ve izole deneme, talep disiplini, kimlik ve parola, veri koruma, ITSM entegrasyonu, denetim ve kanıt, sır yerleşimi, ürün dışında doğrulanacaklar. Görevler ayrılığı grubunda ayarların yanında kadro da sayılır: ayarlar sıkı ama onaylayacak ikinci kişi yoksa kurum kendini kilitler.

Her satır ayarın nerede yönetildiğini de söyler: ilgili ekranın adı ve ayarın tam anahtarı yazar. Anahtar dile çevrilmez, çünkü aranacak olan metnin kendisidir. Doğru cevabı kuruma göre değişen satırlar Karar verin olarak işaretlenir; bu satırlarda tek bir doğru cevap yoktur, bilinçli bir seçim yapılması yeterlidir. Ekran bir dayatma üretmez, bir kararın verilip verilmediğini gösterir.

Ekranın çıktısı denetçiye gösterilebilir ve kurulum kabul kaydının parçası olarak saklanabilir. Aynı liste kurulum belgesinde de bulunur; belgeye yazılan liste zamanla güncelliğini yitirir, ekrandaki liste yitirmez.

Satırın sütunları

Her satırda beş sütun vardır. Kontrol adı neyin sorulduğunu söyler; adın üzerine geldiğinizde o kontrolün neden var olduğunu anlatan bir açıklama çıkar. Nerede yönetilir sütunu ayarın hangi ekrandan değiştirileceğini ve ayarın tam anahtarını verir; anahtar dile çevrilmez, çünkü ekranda

arayacağınız metnin kendisidir. Şu anki değer sütunu kurulumunuzdaki değeri gösterir. Beklenen sütunu ürünün beklediği değeri gösterir. Durum sütunu satırın üç halinden birini gösterir: Uygun, Karar verin veya Dikkat.

Beklenen sütununda tire ne demek

Tire, o satırın evrensel bir doğrusu olmadığı anlamına gelir. Ürün bazı ayarlarda net bir beklenti koyar: talep sahibi kendi talebini onaylayabilsin mi sorusunun beklenen cevabı hayırdır, onaylayabilecek kişi sayısının beklentisi iki ve üzeridir. Bazı ayarlarda ise doğru cevap kuruma göre değişir; bilet numarası biçimi böyledir. Bir kurumda numaralar CR-12345, diğerinde INC0001234 görünümündedir, üçüncüsünde biçim kontrolü hiç istenmez. Böyle satırlarda ürün değer dayatmaz, yalnızca konu hakkında bilinçli bir karar verilip verilmediğini sorar.

Üç durum ve ne yapmanız gerektiği

Uygun. Ayar üretim için uygun durumdadır, yapılacak bir şey yoktur.

Karar verin. Ortada hata yoktur; eksik olan sizin kararınızdır. Bu satırlarda Beklenen sütunu tire gösterir. Ayarı kendi kurumunuza göre değiştirdiğinizde ya da mevcut değer doğru olduğuna karar verip bilinçli olarak dokunduğunuzda satır düzene geçer.

Dikkat. Ayar ürünün beklediği değerde değildir ya da çalışmayan bir kontrol vardır. Bu bir tercih değil, düzeltilmesi gereken bir durumdur. Örneğin çalıştırılmayan bir düzenli ifade yazılmışsa biçim kontrolü sessizce devre dışı kalır; satır bunu Karar verin değil Dikkat olarak gösterir, çünkü kurum kontrolün çalıştığını sanıyordur.

Ekranın üstündeki sayaçlar

Listenin üstünde üç sayaç vardır ve üçü birbirinden ayrıdır; bir satır yalnızca birinde sayılır. Uygun sayacı beklenen değerde olan satırları verir. Dikkat sayacı kurumun kapatması gereken satırları verir. Karar bekliyor sayacı ise kurumun kendi kararını vermesi ya da ürün dışında doğrulaması gereken satırları verir.

İki sayacın ayrı tutulmasının sebebi şudur: karar bekleyen satırların bir kısmı ürünün hiçbir zaman kendiliğinden kapatamayacağı satırlardır. Hepsi tek sayaçta toplansaydı Dikkat sayısı hiçbir zaman sıfıra inmez ve bir süre sonra kimse o sayıya bakmazdı.

Örnek: bilet numarası biçimi satırı

Bu satır Karar verin gösteriyorsa sebebi şudur: değer hâlâ kurulumla gelen desendir (ServiceNow biçimi, ^CHG\d{7}\$) ve parametre hiç kaydedilmemiştir, yani kurumunuzun kendi bilet biçimine göre gözden geçirilmemiştir.

Nereye bakacaksınız: Ayarlar > Parametreler ekranı, ChangeTicketRegex anahtarı.

Ne yazacaksınız: kurumunuzun bilet numarası kalıbını düzenli ifade olarak. Numaralarınız CHG0012345 görünümündeyse (ServiceNow) kurulum değeri zaten doğrudur; değeri bir kez kaydetmeniz yeterlidir. OPS-123 görünümündeyse (Jira) ^OPS-\d+\$ yazarsınız. Yanındaki örnek biçim alanına da gerçek bir numara örneği yazmanız iyi olur; kullanıcı hatalı numara girdiğinde ekranda bu örnek gösterilir.

Boş bırakırsanız ne olur: biçim kontrolü yapılmaz, bilet alanına yazılan her metin kabul edilir. Bu da geçerli bir karardır ve satırı düzene geçirir.

Değiştirmez ve kaydetmezseniz ne olur: kontrol çalışmaya devam eder, kurulum deseni geçerli olur. Kurumunuzun numaraları bu kalıba uymuyorsa kullanıcılar geçerli numaralarını giremez ve talep kaydedemez. Satır bu yüzden kaydedilene kadar karar bekler.

Yanlış bir desen yazarsanız ne olur: çalıştırılmayan bir desen kaydedilmez, kaydetme sırasında hatanın nerede olduğu söylenir. Böyle bir değer doğrudan veritabanına yazılırsa satır Dikkat gösterir ve o istekte biçim kontrolü uygulanmaz.

Olay numarası biçimi satırı (EmergencyTicketRegex) aynı mantıkla çalışır. Kurulum değeri ServiceNow olay kaydı biçimidir (^INC\d{7}\$); kaydedilene ya da değiştirilene kadar karar bekler. Boş bırakmak da geçerli bir karardır.

Ekrandaki bütün satırlar ve ne anlama geldikleri

Aşağıda ekranda görebileceğiniz satırlar grup sırasına göre listelenmiştir. Her madde şunu söyler: satırın ekrandaki adı, parantez içinde ayarın tam anahtarı, kontrolün neyi sorduğu, beklenen değer ve ayarın nereden yönetildiği. Kullanılmayan bir özelliğe ait satırlar hiç görünmeyebilir; örneğin kurum hesabıyla giriş kapalıysa ve sağlayıcı tanımlı değilse o özelliğin ayrıntı satırları çıkmaz.

Görevler ayrılığı

Onaylayan çalıştırabilir mi (ApproverCanExecute). Bir talebi onaylayan kişinin aynı talebi kendisinin çalıştırmasına izin verilip verilmediğini gösterir. Beklenen değer false: onaylayan ile çalıştıran farklı kişiler olmalıdır. Ayarlar > Parametreler ekranından yönetilir.

Talep sahibi kendi talebini onaylayabilir mi (RequesterCanSelfApproveExecute). Talebi açan kişinin aynı talebi onaylayıp çalıştırabilmesine izin verilip verilmediğini gösterir. Beklenen değer false. Ayarlar > Parametreler ekranından yönetilir.

Her onay adımında farklı onaylayan (RequireDistinctApproverPerStep). Çok adımlı bir onay akışında aynı kişinin birden fazla adımı kapatıp kapatamayacağını gösterir. Beklenen değer true: kapalıyken çok adımlı akış tek kişiyle tamamlanabilir ve adım sayısının verdiği güvence kaybolur. Ayarlar > Parametreler ekranından yönetilir.

Onay verebilecek kullanıcı sayısı (cr.approve). Onay yetkisi taşıyan kullanıcı sayısını verir. Beklenen değer iki ve üzeridir. Görevler ayrılığı ayarları sıkı ama onaylayacak ikinci kişi yoksa kurum kendini kilitler: talep sahibi onaylayamaz, başka onaylayan da yoktur. Ayarlar > Kullanıcılar ekranından yönetilir.

Denetçi rolünde kullanıcı (Auditor). Denetçi rolündeki kullanıcı sayısını verir. Beklenen sütununda tire vardır: denetçi rolü zorunlu değildir, kurum denetimi başka bir rolle de yürütebilir. En az bir denetçi tanımlandığında satır düzene geçer. Ayarlar > Kullanıcılar ekranından yönetilir.

Geri alma ve izole deneme

Bu üç satırın değeri kaç sunucuda açık olduğu / toplam sunucu biçimindedir. Üretim ortamı tanımlı sunucu varsa yalnız üretim sunucuları sayılır; yoksa bütün aktif sunucular sayılır. İlgili modül lisansınızda yoksa değer yerine modülün lisanslı olmadığı yazar, çünkü lisanssız modülde sunucudaki bayrak hiçbir şey yapmaz ve açık göstermek yanıltıcı olurdu. Üçü de Ayarlar > Sunucular ekranından, sunucu tanımı üzerinden yönetilir.

Geri alma zorunlu (RollbackRequired). Bu sunucuya giden bir değişiklik talebinin eksiksiz bir geri alma betiği olmadan çalıştırılıp çalıştırılamayacağını gösterir. Beklenen: bütün sunucularda açık.

Otomatik geri alma üretimi (AutoRollbackEnabled). Nesne tanımı değişikliklerinde geri alma betiğinin ürün tarafından üretilip üretilmeyeceğini gösterir. Beklenen: bütün sunucularda açık.

İzole deneme zorunlu (SandboxRequired). Betiğin üretimde çalışmadan önce izole bir kopyada denenmesinin zorunlu olup olmadığını gösterir. Beklenen: bütün sunucularda açık.

Talep disiplini

Değişiklik bileti zorunlu mu (ChangeTicketRequired). Talep açılırken değişiklik bilet numarasının istenip istenmeyeceğini gösterir; üç değeri vardır: her zaman, acil talepler hariç, hiç. Beklenen sütununda tire vardır: doğru cevap kuruma göre değişir, yalnızca bilinçli bir seçim yapılmış olması aranır. Ayarlar > Parametreler ekranından yönetilir.

Bilet numarası biçimi (ChangeTicketRegex). Bilet numarasının hangi kalıba uyacağını belirleyen düzenli ifadedir. Kurulumla gelen örnek desen (^CHG\d{7}\$) hâlâ duruyor ve parametre hiç kaydedilmemişse satır karar bekler. Desen çalıştırlamıyorsa satır Dikkat gösterir, çünkü o durumda biçim kontrolü sessizce devre dışı kalır. Ayarlar > Parametreler ekranından yönetilir.

Acil talepte olay numarası zorunlu mu (EmergencyTicketRequired). Acil bir değişiklikte olay numarasının istenip istenmeyeceğini gösterir. Olay kaydı, normal yolun neden kısaltıldığının kanıtıdır. Beklenen sütununda tire vardır. Ayarlar > Parametreler ekranından yönetilir.

Olay numarası biçimi (EmergencyTicketRegex). Olay numarasının kalıbıdır. Kurulum değeri (^INC\d{7}\$) hâlâ duruyor ve parametre hiç kaydedilmemişse satır karar bekler; boş bırakmak da geçerli bir karardır. Desen çalıştırılmazsa satır Dikkat gösterir. Ayarlar > Parametreler ekranından yönetilir.

ITSM entegrasyonu grubu. ITSM'in kullanılıp kullanılmadığını, bağlantının tanımlı ve erişilebilir olduğunu, kayıta ve çalıştırmada doğrulamanın açık olduğunu, CAB onayının ayrıca okunup okunmadığını, sertifika doğrulamasını, notların gidip gitmediğini ve parola ile anahtarın ortam değişkeninde durduğunu gösterir. ITSM kapalıyken ana satır Karar verin gösterir; ITSM kullanmamak da bilinçli bir karar olabilir. Ayrıntı Bölüm 22.

Acil durum ilan yetkisi (EmergencyMinimumRole). Bir talebi acil ilan edebilmek için gereken en düşük rolü gösterir. Beklenen değer, talep sahibi rolünden daha yüksek bir roldür: acil ilan etmek onay adımlarını kısaltan bir yetkidir ve herkeste olmamalıdır. Ayarlar > Parametreler ekranından yönetilir.

Acil onay politikası (IsEmergencyPolicy). Acil olarak işaretlenmiş onay politikası sayısını gösterir. Beklenen değer bir ve üzeridir, ancak satırın düzene geçmesi için sayı yetmez: acil politikalardan en az birinde atlanamaz bir onay adımı bulunmalıdır. Tamamı atlanabilir adımlardan oluşan bir acil politika, onaysız değişikliğe yol açar. Ayarlar > Onay Politikaları ekranından yönetilir.

Politikaya bağlanmamış aktif sunucular (ServerApprovalPolicy). Hiçbir onay politikasının kapsamadığı aktif sunucuları sayar ve ilk beşinin adını yazar. Beklenen değer sıfırdır. Kapsanmayan bir sunucuya talep kaydedilemez (geri alma talebi hariç); o sunucuda yeni iş açılmaz. Ayarlar > Onay Politikaları ekranından yönetilir.

Kritik nesne listesi (CriticalObjects). Kritik olarak işaretlenmiş nesne sayısını gösterir. Beklenen değer bir ve üzeridir. Liste boşken kritik nesneye dokunma kuralları hiç tetiklenmez: kural motoru çalışır görünür ama kurumun en değerli tabloları korumasız kalır. Ayarlar > Kritik Nesneler ekranından yönetilir.

Kimlik ve parola

Parola en az uzunluk (Auth:Password:MinLength). Beklenen değer on iki ve üzeridir. Yapılandırma dosyasından yönetilir.

Parola geçmişi (Auth:Password:HistoryCount). Kaç eski parolanın yeniden kullanılamayacağını gösterir. Beklenen değer beş ve üzeridir; sıfır, kullanıcının doğrudan eski parolasına dönebilmesi demektir. Yapılandırma dosyasından yönetilir.

Büyük harf zorunluluğu (Auth:Password:RequireUppercase). Beklenen değer true. Kapalıyken parola karmaşıklığı yalnız uzunluğa kalır. Yapılandırma dosyasından yönetilir.

MFA kayıt oranı (Mfa:Enabled). Erişimi olan yerel ve LDAP kullanıcılardan kaçının çok faktörlü doğrulamaya kaydolduğunu kaydolun / toplam biçiminde gösterir. Beklenen değer herkesin kaydolmasıdır. Bu satırın ayrı bir kontrol olmasının sebebi şudur: çok faktörlü doğrulamanın açık olması yetmez, ikinci faktör yalnız kaydolmuş kullanıcıdan istenir ve kaydolmayan kullanıcı parolayla girer. Çok faktörlü doğrulama kurum genelinde kapalıysa satır bir eksiklik değil, bir tercih olarak gösterilir. Kurum hesapları bu orana girmez: ürünün iki adımlı doğrulamasını kuramazlar, çok faktörlü doğrulamalarını kimlik sağlayıcısı yapar ve Kurum MFA doğrulaması denetleniyor satırında ölçülür. Ayarlar > Kullanıcılar ekranından takip edilir.

MFA kaydı zorunlu (Mfa:EnforceEnrollment). Kaydolmanın zorunlu tutulup tutulmadığını gösterir. Beklenen değer true. Açıkken kaydolmamış kullanıcı giriş yapar ancak oturumu yalnız kurulum adımına yarar, başka hiçbir işlem çalışmaz; kural sunucu tarafında uygulanır. Kapalıyken kaydolmak kullanıcının tercihi kalır. Yapılandırma dosyasından yönetilir.

Kurulum yöneticisi parolası değiştirildi mi (MustChangePassword). Kurulumla gelen yönetici hesabının parolasını değiştirip değiştirmediğini gösterir. Beklenen değer true. Değiştirilmediği sürece üretim veritabanına değişiklik onaylayan sistem, kurulum belgesinde yazan bir parolayla korunuyor demektir. Ayarlar > Kullanıcılar ekranından yönetilir.

Kurum hesabıyla giriş (Sso:Enabled). Kurum hesabıyla girişin açık olup olmadığını gösterir. Beklenen değer true, ancak satır bilgi niteliğindedir: kurum hesabıyla giriş zorunlu değildir. Açıkken işten ayrılan kişinin erişimi kurumun tek bir yerinden kapanır. Yapılandırma dosyasından yönetilir. Kapalıyken ve hiçbir kimlik sağlayıcısı tanımlı değilken aşağıdaki altı satır görünmez.

Kurum hesabı ayar hataları (Sso:Providers). Hatalı tanımlanan kimlik sağlayıcılarını ve hatanın hangi alanda olduğunu gösterir. Beklenen değer sıfırdır; hatalı sağlayıcı kullanılmaz. Yapılandırma dosyasından yönetilir.

Grup ile rol eşlemesi (SsoRoleMappings). Tanımlı kimlik sağlayıcılarına ait etkin eşleme sayısını gösterir; ayardan kaldırılmış bir sağlayıcının eşlemesi sayılmaz, çünkü kimseye rol vermez. Beklenen değer bir ve üzeridir; eşleme yoksa kurum hesabıyla gelen hiç kimse rol alamaz. Ayarlar > Kurum Kimliği (SSO ve LDAP) ekranından yönetilir.

Kurum MFA doğrulaması denetleniyor (Sso:Providers:N:RequireMfaClaim). Kaç kimlik sağlayıcısında çok faktörlü doğrulama bilgisinin denetlendiğini gösterir. Beklenen değer bütün sağlayıcılardır. Yapılandırma dosyasından yönetilir.

Kimlik sağlayıcısı üstverisi HTTPS ile okunuyor (Sso:Providers:N:RequireHttpsMetadata). Kaç kimlik sağlayıcısında üstverinin yalnız HTTPS ile okunmasının zorunlu tutulduğunu gösterir. Ürün kimlik sağlayıcısının imza anahtarlarını bu adresten okur; adres HTTPS değilse araya giren biri sahte anahtar verip sahte kimlikle giriş yapabilir. Beklenen değer bütün sağlayıcılardır. Değerin false olması yalnız yerel test içindir. Yapılandırma dosyasından yönetilir.

Acil durum hesabı (Auth:LocalLoginAllowedUsers). Kimlik sağlayıcısı çöktüğünde girebilecek yerel, şifreli ve SystemManager rolündeki hesap sayısını gösterir. Liste doluysa yalnız listedeki hesaplar sayılır. Beklenen değer bir ve üzeridir. Ayarlar > Kullanıcılar ekranından ve yapılandırma dosyasından yönetilir.

Şifre ile giriş yalnızca acil durum hesaplarında (Auth:LocalLoginAllowedUsers). Şifre ekranından girebilecek yerel hesap listesini gösterir. Beklenen değer tanımlı bir listedir; boş liste bütün yerel hesapların kurumun kimlik politikasını atlayarak şifreyle girebildiği anlamına gelir. LDAP hesapları da şifre ekranından girer ve bu listeden etkilenmez; canlı LDAP hesabı varsa sayısı değerinin yanında yazar (örnek: admin | Ldap: 12) ve satır uyarı verir. Geçiş döneminde bu beklenen bir durumdur; geçiş bitince LDAP hesapları kurum hesabına çevrilir. Yapılandırma dosyasından yönetilir.

Aşağıdaki dizin (LDAP) satırları yalnız dizin kullanılıyorsa görünür (Ldap:Host dolu, Auth:Mode Ldap ya da en az bir LDAP hesabı var). Dizin tanımlı ama kimse kullanmıyorsa satırlar bilgi niteliğindedir.

Dizin (LDAP) ayar hataları (Ldap). Kurulum dosyasındaki dizin ayarı hatalarını gösterir. Beklenen değer sıfırdır. Yapılandırma dosyasından yönetilir.

Dizin bağlantısı şifreli (Ldap:Security). Beklenen değer Ldaps ya da StartTls. None iken kişilerin şifresi ağda açık gider.

Dizin sertifikası doğrulanıyor (Ldap:AllowUntrustedCertificate). Beklenen değer false. true yalnız kendinden imzalı sertifikalı test ortamı içindir.

Dizin hesaplarının rol kaynağı (Ldap:RoleSource). Bilgi niteliğindedir: Manual ya da Directory.

Dizin grubu ile rol eşlemesi (SsoRoleMappings). "Dizin (LDAP)" sağlayıcısının etkin eşleme sayısı. Beklenen değer bir ve üzeridir; yalnız rol dizinden geliyorsa uyarı verir.

Grup tam adla eşleniyor (Ldap:GroupMatch). Beklenen değer Dn. Kısa adla eşlemede başka klasördeki aynı adlı grup da rol verir.

Dizin servis hesabı (Ldap:BindDn). Beklenen değer tanımlı. Eşitleme ve SearchDn biçimi için gereklidir.

Dizin eşitlemesi açık (Ldap:Sync:Enabled). Beklenen değer true. Kapalıyken dizinde kapatılan kişinin üründeki hesabı ve açık oturumu açık kalır.

Son dizin eşitlemesi (Ldap:Sync:IntervalMinutes). Beklenen değer, eşitleme aralığının iki katı içinde tamamlanmış bir eşitlemedir. Durduysa hiçbir değişiklik yapılmamıştır; neden Ldap.SyncAborted kaydında yazar.

Ürünün kilit eşiği dizininkinden küçük (Auth:AccountLockoutMaxAttempts). Değer "ürün / izin" biçimindedir; dizinin eşiği son eşitlemede okunur. Ürün dizinden önce kilitlemezse şifre tahmini ürün ekranı üzerinden kişinin dizindeki hesabını kilitler.

Veri koruma

Maskeleme açık mı (QrMaskingEnabled). Sorgu sonucu taleplerinde hassas kolonların maskelenip maskelenmeyeceğini gösterir. Beklenen değer true. Kapalıyken tespit de maskeleme de yapılmaz, yalnız kayıt tutulur. Ayarlar > Parametreler ekranından yönetilir.

Sonuç teslim biçimi (QrDeliveryMode). Sonuç dosyasının ve şifresinin hangi kanaldan teslim edileceğini gösteren kurum tavanıdır. Beklenen sütununda tire vardır, çünkü doğru cevap kuruma bağlıdır. Ancak en gevşek biçim seçilmişse, yani paket ve parolası aynı e-postada gidiyorsa, satır uyarır: o e-postayı eline geçiren herkes dosyayı açabilir. Ayarlar > Parametreler ekranından yönetilir.

Maskeleme dışı bırakılan sunucular (MaskingMode). Kolon adına göre maskelemenin devre dışı olduğu aktif sunucuları sayar. Beklenen değer sıfırdır. Bu rejim sentetik veri barındıran ortamlar içindir; üretim sunucusunda seçilmişse hassas kolonlar kolon adına bakılarak maskelenmiyor demektir. Ayarlar > Sunucular ekranından yönetilir.

Tanımlı hassas veri deseni (SensitiveDataPatterns). Etkin hassas veri deseni sayısını gösterir. Beklenen değer bir ve üzeridir. Desen yoksa içerik tabanlı tespit çalışacak bir kural bulamaz. Ayarlar > Hassas Veri Desenleri ekranından yönetilir.

Denetim ve kanıt

Ayar değişikliğinde dört göz kuralı (SettingsApprovalPolicy). Ayar ekranlarındaki değişikliklerin ikinci bir kişinin onayına düşüp düşmeyeceğini gösterir. Beklenen değer, yalnız kontrol ayarları ya da bütün ayarlar seçeneklerinden biridir; kapalı olması beklenen değer değildir. Ayarlar > Parametreler ekranından yönetilir.

Kurulum kimliği (Evidence:Signing:InstallationId). Kanıt dosyası, dönem paketi, kanıt paketi ve defter özetinin aynı kurulumdan geldiği bu değerle doğrulanır. Boş bırakılırsa hepsi kimliksiz üretilir ve denetçinin karşılaştırması boş ile boşu karşılaştırıp geçer. Dolu olması da yetmez: ürünle gelen geliştirme değeri değiştirilmeden bırakılırsa satır dikkat ister, çünkü iki ayrı kurumun dosyaları aynı etiketi taşıdığına birbirinin yerine geçen dosyalar ayırt edilemez. Kurulum başına benzersiz olmalı, her ortam ayrı kimlik almalı (örnek: KURUM-PROD-01, KURUM-TEST-01) ve sonradan değiştirilmemelidir; değişirse eski kanıt dosyaları yenileriyle birlikte doğrulanamaz.

Ürün sürümü (Directory.Build.props). Kanıt paketlerinin künyesine yazılan sürümü gösterir. Bu satırın geçme koşulu yoktur, değeri görünür kılmak için vardır: destek çağrısında ve denetçi

sorusunda aynı değerden konuşulur. Değerin sonundaki karşılık, sürümün hangi koddan üretildiğini gösterir; aynı numarayla düzeltme almış bir kurulum ile almamış bir kurulumu ayıran tek şey odur. Değer ürünün derlemesinden gelir, ekrandan ya da yapılandırma dosyasından değiştirilemez.

Kanıt tablosu defter mi (Database:EvidenceLedger). Denetim kayıtlarının append-only ledger tablosunda tutulduğunu gösterir. Beklenen değer: Append-only ledger tablosu.

Kanıt yazma sınırı. Kanıt tablosunda tetikleyici, yazma yordamında değişiklik ya da kanıt şemasında beklenmeyen nesne olmadığını gösterir. Bulgu varsa bulgu kodları yazılır ve değişiklik işlemleri durur.

Son defter özeti (Evidence:Ledger:DigestIntervalMinutes). En son defter özetinin ne zaman yayımlandığını gösterir. Özet aralığının Evidence:Ledger:DigestStaleAfterIntervals katından uzun süre özet yoksa dikkat ister.

Özetler için değiştirilemez depo (Evidence:Ledger:DigestOutputPath). Tanımlı değilse hiçbir kayıt "dış özetle kapsandı" olarak görünmez.

İmza anahtarı nerede tutuluyor (Evidence:Signing:Keys:{id}:CertificateThumbprint). Beklenen değer Windows sertifika deposudur. Yapılandırma dosyasındaki ya da ortam değişkenindeki anahtarı sunucuyu yöneten herkes kopyalayabilir.

Bu grupta ayrıca şu satırlar bulunur: imzalama açık mı (Evidence:Signing:Enabled; Production hedefte imza kapalıyken çalıştırma reddedilir), imzalama anahtarının parmak izi (Bölüm 18.6), imzasız Production çalıştırmasına izin (Evidence:Signing:AllowUnsignedProductionExecution; beklenen false), hedef sunucu sertifika doğrulaması, yönetim durumu mührü, zaman damgası açıksa zaman damgası sağlığı ve dokuz SIEM satırı (Bölüm 25.8). Geri alma ve izole deneme grubunda üretim sunucusunda izole deneme izni (Sandbox:AllowOnProduction) satırı, ürün dışında doğrulanacaklar grubunda koşula bağlı olarak worker ucunun taşıma güvenliği satırı da vardır.

Bildirim gönderimi (Mail:Enabled / Mail:DevMode). Bildirim e-postalarının gerçekten gönderilip gönderilmediğini gösterir. Beklenen değer true. Geliştirme kipi açıksa bütün e-postalar tek bir adrese yönlendirilir ve satır bunu ayrıca belirtir. Bildirim gitmiyorsa onay bekleyen talep kimsenin önüne düşmez: akış durur ve sebebi görünmez. Yapılandırma dosyasından yönetilir.

Bakım ve arşivleme görevi (MaintenanceTasks). Tanımlı ve etkin en az bir bakım görevi olup olmadığını gösterir. Beklenen değer true. Satır görevlerin içeriğine bakmaz; kanıt defteri için arşivleme ya da silme görevi yoktur, ledger tablosu silmeye kapalıdır. Ayarlar > Bakım Görevleri ekranından yönetilir.

Sır yerleşimi (üretim öncesi)

Bu grubun satır adları çeviri değil, ayarın kendi yoludur; ekranda arayacağınız metnin kendisi olduğu için olduğu gibi yazılır. Değer üç halden birini alır: yapılandırma dosyası, ortam değişkeni veya tanımsız. Beklenen değer ortam değişkenidir. Gerekçe şudur: yapılandırma dosyası kaynak kontrolünde durur, bir sır orada düz metin duruyorsa depoya erişebilen herkes o sırra sahiptir. Zorunlu olmayan bir sır hiç tanımlı değilse bu bir eksiklik sayılmaz, çünkü o özellik kullanılmıyordur. Grup bir dayatma değil, üretime çıkmadan önce kapatılması gereken bir listedir.

Listede şu sırlar bulunur: uygulama veritabanı bağlantı dizesi, jeton imzalama anahtarı, sunucu parolası şifreleme anahtarı, sorgu sonucu paketi şifreleme anahtarı, worker erişim anahtarı, e-posta parolası, izin bağlantı parolası ve sonuç paketi parola anahtarı. Kurum hesabıyla giriş için tanımlı her kimlik sağlayıcısının istemci sırrı ve (sertifika tanımlıysa) SAML sertifika parolası da ayrı satır olarak listelenir. İlk beşi zorunludur; kalanlar yalnız ilgili özellik kullanılıyorsa tanımlı olur.

Ürün dışında doğrulanacaklar

Bu gruptaki satırları ürün doğrulayamaz; bunlar ağ, işletim sistemi ve altyapı tarafında kurulur. Grubun tamamı bilgi niteliğindedir ve Dikkat sayacını etkilemez. Listede yer almalarının sebebi, görünmeyen bir riskin kurulum sırasında hiç düşünülmemesini engellemektir.

Worker ucu ağ seviyesinde kısıtlı (WorkerEndpointNetworkRestricted). Bu satır bir beyandır ve arkasında çalışan bir kontrol yoktur. Worker yapılandırma ucu, worker çalışabilsin diye sır taşımak zorundadır; ucun yalnız worker sunucusundan erişilebilir olması bir güvenlik duvarı veya ters vekil kuralıdır ve ürün bunu göremez. Değer üç hallidir: boş, evet, hayır. Boş bırakmak kararın hiç verilmediğini, hayır ise riskin bilerek kabul edildiğini söyler; denetimde bu iki cevap farklı sorular doğurur. Evet demek uçta hiçbir şeyi değiştirmez; yaptığı şey kararın kimin tarafından ne zaman verildiğini denetim izine yazmaktır. Beyan bir kontrol ayarı sayıldığı için, dört göz kuralı kapsamındayken değiştirilmesi ikinci bir kişinin onayına düşer. Ayarlar > Parametreler ekranından yönetilir.

Worker ucu erişim izi, son otuz gün (Workers:ApiKey). Bu satır beyan değil, ölçümdür. Worker yapılandırma ucuna gelen her istek, başarılı da başarısız da, adresiyle birlikte denetim izine yazılır. Satır iki sayı gösterir: ucu kaç farklı adres çağırdı ve kaç kez yanlış anahtarla denendi. Beklenen değer tek adres ve sıfır reddedilen denemedir. İkinci bir adres ya worker sunucusunun taşındığını ya da ucu başka birinin de çağırdığını söyler. Reddedilen deneme ise ucun ait olmadığı bir yerden görülebildiğini söyler; ağ kısıtı yerinde olsaydı o istek uca hiç ulaşamazdı. Sınırı da bilinmelidir: adres bağlantının kendisinden okunur, taklit edilebilir bir başlıktan değil. Bu yüzden worker ile uygulama arasında ters vekil varsa bütün çağrılar vekilin adresinden görünür ve farklı adres sayısı hep bir kalır; reddedilen deneme sayısı bu durumda da çalışmaya devam eder.

DAM ve SIEM eşleşmesi beyanları

Ürün dışında doğrulanacaklar grubunda iki öneri satırı vardır. İkisi de kurumun kararını kaydeder; ürün DAM yapılandırmasını ya da hesabın başka yerde kullanılıp kullanılmadığını denetleyemez.

Satır (parametre)	Seçenekler	Ne zaman geçer
Ürünün SQL hesabı yalnız ürüne ait (TargetAccountDedicated)	Yes, No	Yes seçildiğinde
API ve Worker adresleri DAM izin listesinde (DamAllowlistMaintained)	Yes, No, NotUsed	Yes ya da NotUsed seçildiğinde (NotUsed: kurum DAM kullanmıyor)

Boş bırakılan satır "Karar verin" gösterir. İkisi de öneri niteliğindedir: geçmediğinde üstteki "Dikkat" sayacını artırmaz. Beyanı değiştirmek bir kontrol değişikliğidir: dört göz kuralı açıksa onaya düşer, kimin ne zaman değiştirdiği denetim izine yazılır ve SIEM'e gider.

Gönderim eşiği ve Gönderilen akışlar satırlarının açıklamasında şu uyarı yer alır: eşik Notice'in üstündeyse ya da Denetim akışı kapalıysa yürütme penceresi olayları SOC'a gitmez. Bu cümle açıklamanın sabit parçasıdır; eşiğin değerine göre değişmez.

27.9 Kural motorunun kapsamı ve sınırı

Kural motoru betiği her hedef motor için o motorun dilbilgisiyle ayrıştırır ve cümle yapısı üzerinden çalışır. Bu yüzden filtresiz bir UPDATE, kritik nesne üzerinde DROP veya adlandırma kuralı gibi betiğin kendisinden okunabilen durumları yakalamak için tasarlanmıştır. Yorum satırındaki bir kelime kural tetiklemez, parantezle sarılmış bir koşul gözden kaçmaz. Sınır: PostgreSQL ayrıştırıcısı bazı kontrollerde yardımcı düzenli ifadeler kullanır; Oracle'da dilbilgisi ayrıştırması başarısız olursa analiz düzenli ifade tabanlı yöntemle düşer ve bu yöntemin isabeti daha düşüktür.

Bir sorgunun indeksli kolon kullanıp kullanmadığı ise betikten okunamaz; hedef veritabanının kataloğuna bakmayı ve o anki indeks tanımlarını bilmeyi gerektirir. Bu kontrol bugün kural motorunun kapsamında değildir ve veritabanı izleme araçlarının alanına girer.

Bu sınır bilinçlidir. Kesin cevap verilemeyen bir alanda uyarı üretmek, güvenilir uyarılarla ekranı doldurur ve zamanla bütün uyarıların göz ardı edilmesine yol açar. Kural motoru bu yüzden betikten okunamayan konularda uyarı üretmez.

27.10 Kapalı düğmeler ve sebepleri

Bir işlem yapılamıyorsa sebebi o düğmenin yanında yazar. Kural şudur: kapalı bir düğmenin üzerine gelin, ipucu sebebi tam bir cümleyle söyler. Kullanıcının neden yapamadığını anlamak için belgeye, günlüğe veya bir yöneticiye sormaya ihtiyacı olmaz.

Düğmeler üç şekilde davranır. Yetkiniz yoksa düğme hiç görünmez: yapamayacağınız bir işlemi ekranda tutmanın anlamı yoktur. Yetkiniz var ama talebin durumu uygun değilse düğme kapalı görünür ve sebep ipucunda yazar. Şartlar tutuyorsa düğme açıktır.

İpucundaki sebep, düğmeye bassaydınız sunucunun vereceği cevabın aynısıdır. Ekran ile komut aynı kuralı kullanır; kapalı bir düğmenin sebebi gerçek sebeptir. Açık bir düğme de işlem anı kontrolleri (onay zinciri, ITSM, kanıt yazma sınırı) nedeniyle reddedilebilir; sebep mesajda yazar.

Sebeplerin talebin durumuna göre değişir ve bu fark önemlidir. Talep hâlâ canlıysa cümle beklemeniz gerektiğini söyler: gözden geçirme için değişiklik henüz uygulanmamıştır, geri alma için kaynak talep henüz çalıştırılmamıştır. Talep kapanmışsa cümle yapacak bir şey olmadığını söyler: bu talep uygulanmadan kapandı, geri alınacak bir değişiklik yok, bu talep kapandı üzerinde başka işlem yapılamaz. Aynı cümlenin her duruma yazılması kullanıcıyı boş yere beklettiği için sebeplerin durumuna göre ayrılmıştır. Kapanmış bir talepte ayrıca sayfanın üst kısmında tek satırlık bir bilgi kutusu görünür; talebin kapandığını, hangi durumda kapandığını ve üzerinde işlem yapılamayacağını fare gezdirmeden söyler. Aynı işi yeniden yapmak isteyen kullanıcı talebi kopyalayabilir.

Ayar ekranlarında dört göz kuralı da aynı biçimde görünür. Üzerinde onay bekleyen bir kayıta düzenleme ve silme kapalıdır; satırdaki Onay bekliyor rozetinin ipucunda hem bunun sebebi hem bekleyen değişikliğin özeti yazar.

27.11 Talep kopyalama

Bir talep kopyalandığında yeni bir talep açılır. Kopya, elle açılmış bir talepten daha ayrıcalıklı değildir: aynı kaydetme kapılarından geçer. Sunucu hâlâ tanımlı ve aktif mi, lisans kapsamında mı, kurumun bilet kuralı sağlanıyor mu, betik içeriği kurallara uyuyor mu, hepsi yeniden kontrol edilir.

Kopya kaynağın betiklerini ve alanlarını taşır. Onay akışı kopya için yeniden kurulur: o an geçerli onay politikası uygulanır ve talebin başlangıç durumu bu politikaya göre belirlenir. Kaynağın onay geçmiş, çalıştırma bilgisi ve risk fotoğrafı taşınmaz; kopya yeni bir olaydır.

Acil durum işareti kopyalanmaz. Acil ilan etmek bir yetkidir ve uygun bir acil politika gerektirir; kopya bu iki kontrolü atlatmamalıdır. Acil gerekçesi ve olay numarası da taşınmaz: bunlar belirli bir olaya aittir, aylar önceki bir arızanın gerekçesi yeni talebe yapılmamalıdır. Acil bir talebin kopyası normal talep olarak açılır ve ekranda kaynağın acil işaretli olduğu, bu bilginin kopyaya taşınmadığı yazar. Gerekiyorsa kullanıcı işareti kendisi koyar, güncel gerekçeyi yazar ve o yol her iki kontrolden de geçer.

Geri alma talepleri kopyalanmaz. Bir geri alma her zaman belirli bir talebe aittir; kopyası hangi değişikliği geri aldığı belirsiz bir betik yığınının dönüşüdür.

Bölüm 28. Ekler

28.1 Enum sözlüğü

Roller (enmRole)

Değer	Ad	Hiyerarşi seviyesi
0	NoAccess	0
5	Viewer	5
10	Auditor	10
15	Requester	15
20	RequestManager	20
25	DbAdmin	25
30	ChangeManager	30
35	SystemManager	35

Talep durumu (ChangeRequestStatus)

Tablodaki değerlere ek olarak 8 = ReconciliationRequired (uzlaştırma gerekli) vardır. Ölü durum değildir ama dondurulmuştur: hedefte commit olup olmadığı belirsiz bir çalıştırmadan sonra girilir, düzenlenemez, yeniden çalıştırılmaz ve yalnız uzlaştırma kararıyla çıkarılır. Değer	Ad	Ölü durum
1	Pending	Hayır
2	Approved	Hayır
3	Executed	Evet
4	Rejected	Evet
5	Manual	Evet

Tablodaki değerlere ek olarak 8 = ReconciliationRequired (uzlaştırma gerekli) vardır. Ölü durum değildir ama dondurulmuştur: hedefte commit olup olmadığı belirsiz bir çalıştırmadan sonra girilir, düzenlenemez, yeniden çalıştırılmaz ve yalnız uzlaştırma kararıyla çıkarılır. Değer	Ad	Ölü durum
6	NoLongerNeeded	Evet
7	Executing	Hayır

Talep tipi (QueryType)

Değer	Ad
0	None
1	Change
2	QueryResult
3	Rollback

Veritabanı tipi (DatabaseType)

Değer	Ad
1	SqlServer
2	Oracle
3	PostgreSQL

Risk bandı (RiskTier)

Değer	Ad	Skor aralığı
0	Info	90 - 100
1	Low	70 - 89
2	Medium	50 - 69
3	High	25 - 49
4	Critical	0 - 24

Sürüm paketi çalıştırma modu (ReleaseExecutionMode)

Değer	Ad
1	AllOrNothing
2	StopOnError
3	ContinueOnError

Onay adımı durumu

Değer	Anlamı
0	Bekliyor
1	Onaylandı
2	Reddedildi
3	Atlandı

Sunucu ortamı

Değer
Production
Staging
Development
Test

Onay politikası çözümlemesinde önem sırası: Production > Staging > Test > Development > tanımsız.

Maskeleme rejimi

Değer	Anlamı
Strict	Katalog ve desen birlikte.
ContentOnly	Yalnızca desen.

Maskeleme politikası kaydı

Değer	Anlamı
AutoMask	Tespit edilen kolonlar maskelendi.
WarnOnly	Tespit yapıldı, maskelenmedi.
MaskingOff	Ana anahtar kapalıydı, hiç tespit yapılmadı.

Maskeleme gerekçe tipleri

Değer	Anlamı
Catalog	Kolon adı kataloğa uydu.
Pattern	Değer desene uydu.
UnmaskApproved	Onaylı istisna.
NotScanned	Süre bütçesi nedeniyle taranamadı, güvenli tarafta maskelendi.
PolicyWarnOnly	Politika WarnOnly.
MaskingOff	Ana anahtar kapalı.

Aday kolon durumu

Değer	Anlamı
New	Karar bekliyor.

Değer	Anlamı
Accepted	Kataloğa alındı.
Ignored	Yok sayıldı.

Ayar değişikliği durumu

Değer	Anlamı
Pending	Karar bekliyor.
Approved	Onaylandı ve uygulandı.
Rejected	Reddedildi.
Failed	Onaylandı ama uygulanamadı.

Lisans durumu

Değer	Anlamı	Kısıtlı mod
Valid	Geçerli.	Hayır
Trial	Deneme.	Hayır
Expiring	Bitişe az kaldı.	Hayır
GracePeriod	Ek süre içinde.	Hayır
Expired	Süresi dolmuş.	Evet
Invalid	Geçersiz.	Evet
Missing / NoLicense	Yok.	Evet

28.2 Parametre hızlı referansı

Anahtar	Grup	Varsayılan	Kontrol ayarı
DefaultQueryTimeout	Genel	30	Hayır
MaxQueryTimeout	Genel	3600	Hayır
ExecutionDelaySeconds	Genel	300	Hayır

Anahtar	Grup	Varsayılan	Kontrol ayarı
RejectOnError	Genel	true	Evet
RequesterCanSelfApproveExecute	Görevler Ayrılığı	true	Evet
ApproverCanExecute	Görevler Ayrılığı	true	Evet
RequireDistinctApproverPerStep	Görevler Ayrılığı	false	Evet
EmergencyMinimumRole	Görevler Ayrılığı	Requester	Evet
SettingsApprovalPolicy	Ayar Onayı	Disabled	Evet
ChangeTicketRequired	ITSM Bilet	Always	Evet
ChangeTicketRegex	ITSM Bilet	^CHG\d{7}\$	Evet
EmergencyTicketRequired	ITSM Bilet	Never	Evet
EmergencyTicketRegex	ITSM Bilet	^INC\d{7}\$	Evet
QrFileRetentionDays	Sorgu Sonucu	1	Evet
QrRequesterCanDownload	Sorgu Sonucu	true	Evet
QrDownloadMinimumRole	Sorgu Sonucu	ChangeManager	Evet
QrDeliveryMode	Sorgu Sonucu	AttachmentPortalPassword	Evet
QrMaxRowCount	Sorgu Sonucu	1000000	Evet
QrOutputFormat	Sorgu Sonucu	Auto	Hayır
QrCsvThresholdRowCount	Sorgu Sonucu	500000	Hayır
QrExcelAutoFitMaxRows	Sorgu Sonucu	50000	Hayır
QrMaskingEnabled	Hassas Veri	true	Evet
QrSensitiveDataPolicy	Hassas Veri	AutoMask	Evet
QrSensitiveDetectionSampleSize	Hassas Veri	1000	Evet

Anahtar	Grup	Varsayılan	Kontrol ayarı
QrSensitiveDetectionThresholdPct	Hassas Veri	20	Evet
QrSensitiveDetectionSampleMode	Hassas Veri	Random	Evet
QrSensitiveDetectionTimeBudgetSeconds	Hassas Veri	10	Evet
QrColumnPreviewEnabled	Hassas Veri	true	Hayır
UnmaskedColumnRequestPolicy	Hassas Veri	RequireApproval	Evet
UnmaskedColumnApproverRole	Hassas Veri	SystemManager	Evet
QrEmailApprovalPolicy	E-posta Onayı	RequireApproval	Evet
QrEmailApproverRole	E-posta Onayı	ChangeManager	Evet
QrEmailAutoApproveUsers	E-posta Onayı	True	Evet
SiemEnabled	SIEM	true	Evet
SiemStreams	SIEM	Audit;Anchor;AppLog;Heartbeat	Evet
SiemMinSeverity	SIEM	Notice	Evet
SiemIncludeScriptText	SIEM	false	Evet
RequestTicketRegex	ITSM Bilet	(boş)	Evet
ItsmEnabled	ITSM Bilet	false	Evet
ItsmVerifyOnSave	ITSM Bilet	Block	Evet
ItsmExecuteGate	ITSM Bilet	Block	Evet
ItsmEnforceWindow	ITSM Bilet	false	Evet
ItsmVerifyIncident	ITSM Bilet	Warn	Evet
ItsmQueryResultTicketKind	ITSM Bilet	Request	Evet
ItsmUnavailablePolicy	ITSM Bilet	AllowAndRecord	Evet
ItsmReadyStates	ITSM Bilet	Scheduled;Implement	Evet
ItsmClosedStates	ITSM Bilet	Review;Closed;Canceled;Cancelled;Resolved;Closed Complete;Closed Incomplete;Closed Skipped	Evet
ItsmApprovedValues	ITSM Bilet	Approved	Evet
ItsmWriteBackEnabled	ITSM Bilet	true	Evet
ItsmWriteBackEvents	ITSM Bilet	Talep olayları	Evet

28.3 Yetki anahtarları hızlı referansı

Tabloda yer almayan bir anahtar daha vardır: audit.anchorexport, dönem paketinin dışı aktarılmasını açar (Bölüm 17). Kurulumda Auditor ve SystemManager rollerinde bulunur. Anahtar	Açtığı ekran veya işlem
cr.add	Talep oluşturma
qr.add	Sorgu sonucu talebi oluşturma
cr.execute	Çalıştırma
cr.sandbox	Sandbox
cr.approve	Onaylama, reddetme, zamanlama, manuel işaretleme
cr.seeall	Tüm talepleri görme
report.view	Raporlar
dashboard.view	Kontrol paneli
audit.view	Denetim kaydı ve doğrulama işlemleri
audit.evidenceexport	Denetim dosyası dışı aktarma
rp.manage	Sürüm paketleri
settings.servers	Sunucular
settings.users	Kullanıcılar
settings.roles	Roller
settings.params	Parametreler
settings.approvals	Onay politikaları
settings.standards	SQL standartları
settings.critical	Kritik nesneler
settings.itsm	ITSM biletleri
settings.qrsensitive	Hassas kolonlar ve aday kolonlar
settings.patterns	Hassas veri desenleri
settings.email	E-posta kaynakları

Tabloda yer almayan bir anahtar daha vardır: audit.anchorexport, dönem paketinin dışa aktarılmasını açar (Bölüm 17). Kurulumda Auditor ve SystemManager rollerinde bulunur.	Açtığı ekran veya işlem
Anahtar	
settings.maintenance	Bakım görevleri
settings.notificationlogs	Bildirim kayıtları
settings.license	Lisans
settings.diagnostics	Tanımlama

28.4 UTC saklama notu

Aşağıdaki tabloların tarih alanlarının tamamı DATETIMEOFFSET tipindedir ve UTC saklanır:

Users, ChangeRequests, ChangeRequestApprovalSteps, ChangeRequestResultColumns, AuditLogs, RefreshTokens, Servers, SqlStandards, CriticalObjects, EmailSources, ReleasePackages, Parameters, Scripts, ScriptObjects, ItsmTickets, QrSensitiveColumns, ReportDefinitions, ReportParameters, MaintenanceTasks, MaintenanceTaskLogs, NotificationLogs, ApprovalPolicies, ApprovalPolicySteps, ServerApprovalPolicies, SensitiveDataPatterns, QrMaskingAuditLog, QrMaskingAuditDetail, SensitiveColumnCandidates, SettingChangeRequests, SandboxResults, RiskCalc_Result.

Gösterim kuralları Bölüm 23'tedir.

28.5 Kurulum kontrol listesi

- [] Boş veritabanı oluşturuldu.
- [] ConnectionStrings:Default dolduruldu.
- [] Jwt:SigningKey üretildi ve yazıldı.
- [] Security:ServerPasswordKey üretildi ve yazıldı.
- [] Security:QrZipPasswordKey üretildi ve yazıldı.
- [] Mail ayarları yapıldı, DevMode false.
- [] Display:TimeZone kuruma göre ayarlandı.
- [] AllowedOrigins içine web arayüzü adresi eklendi.
- [] QueryResult:OutputPath klasörü oluşturuldu ve yetki verildi.

- [] Workers:ApiKey ile worker tarafındaki WorkerApi:Key eşleştirildi.
- [] API başlatıldı, şema ve varsayılan veri oluştu.
- [] Lisans yüklendi.
- [] admin şifresi değiştirildi.
- [] Worker servisi kuruldu ve başlatıldı.
- [] Kanıt imzalama ayarlandı (Evidence:Signing: anahtar, InstallationId) ve açık anahtarın parmak izi denetçiye ayrı kanaldan verildi. İmzalama kapalıyken Production hedefte çalıştırma reddedilir.

28.6 İlk yapılandırma kontrol listesi

- [] Sunucular tanımlandı ve bağlantı testleri başarılı.
- [] Kritik nesneler listesi girildi.
- [] SQL standartları gözden geçirildi, gerekmeyenler kapatıldı.
- [] Hassas kolon kataloğu ve desenler gözden geçirildi.
- [] En az bir genel onay politikası tanımlandı.
- [] Ortam bazlı politikalar tanımlandı.
- [] Acil durum politikası tanımlandı (kullanılacaksa).
- [] Kullanıcılar eklendi ve rolleri atandı.
- [] Her ayar yetkisine en az iki kullanıcı atandı.
- [] SettingsApprovalPolicy kuruma uygun değere getirildi.
- [] ChangeTicketRegex kurumun bilet biçimine göre ayarlandı.
- [] ITSM kullanılıyorsa bağlantı test edildi, durum listeleri ITSM yöneticisiyle birlikte ayarlandı ve ItsmEnabled açıldı.
- [] Görevler ayrılığı parametreleri kararlaştırıldı.
- [] Test talebi açılıp uçtan uca yürütüldü.

28.7 Denetim hazırlığı kontrol listesi

- [] Kontrol İstisnaları raporu çalıştırıldı, her satır açıklanabiliyor.
- [] ITSM kullanılıyorsa ITSM Control Exceptions raporu çalıştırıldı, her satır açıklanabiliyor.
- [] Onay Adımı Detayı raporu ile çift kontrol kanıtı alındı.
- [] Ayar Onay İzi raporu ile kontrol değişiklikleri gözden geçirildi.

- [] Kullanıcı Yetki Matrisi raporu alındı.
- [] Veri Erişim ve Dışa Aktarım Kaydı raporu incelendi.
- [] Maskeleye Etkinliği raporunda MaskingOff kaydı olup olmadığı kontrol edildi.
- [] Maskeleye Muafiyetli Sunucular raporundaki gerekçeler güncel.
- [] Defter Durumu Sağlam; dönemin özet dosyaları silmeye ve değiştirmeye kapalı (WORM gibi) depoda ve bir kopyada sys.sp_verify_database_ledger başarılı (Denetçi Kiti).
- [] Örnek talepler için denetim dosyası üretildi ve doğrulandı.