

SQL Change Guard

Teknik Şartname

Mimari, Güvenlik, Entegrasyon ve Gereksinimler

SQL Server | PostgreSQL | Oracle

1. Mimari Genel Bakış

SQL Change Guard katmanlı bir mimariye sahiptir ve kurum içinde (on-premise) çalışır; dış bağlantılar (ITSM, SIEM, kimlik sağlayıcısı, zaman damgası) isteğe bağlıdır.

- Sunum katmanı: React tabanlı web arayüzü
- Uygulama katmanı: REST API (.NET 10)
- Arka plan servisi: Zamanlanmış işler için Windows Service (Quartz zamanlayıcı)
- SQL analiz katmanı: Her veritabanı için ayrı parser (Oracle için ANTLR4 tabanlı PL/SQL parser)
- Policy Engine ve Audit Engine
- Uygulama veritabanı: SQL Server 2022 ve sonrası (yönetim verisi ve append-only defter tablosundaki denetim kaydı)
- Hedef veritabanları: SQL Server, PostgreSQL, Oracle

2. Veritabanı Bağımsızlığı

Vendor bağımlılıkları izole edilmiştir. Her hedef veritabanı için ayrı parser, splitter, executor ve rollback üretici bulunur; aynı yönetim modeli üç veritabanında da çalışır.

- SQL Server: T-SQL parser (ScriptDom tabanlı), GO batch ayracı
- PostgreSQL: dollar-quote farkındalıklı ; ayracı
- Oracle: PL/SQL blok koruması, standalone / ve ; ayracı; DDL/DCL/TRUNCATE örtülü commit tespiti (öncesinde DML varsa uyarı)

3. Güvenlik

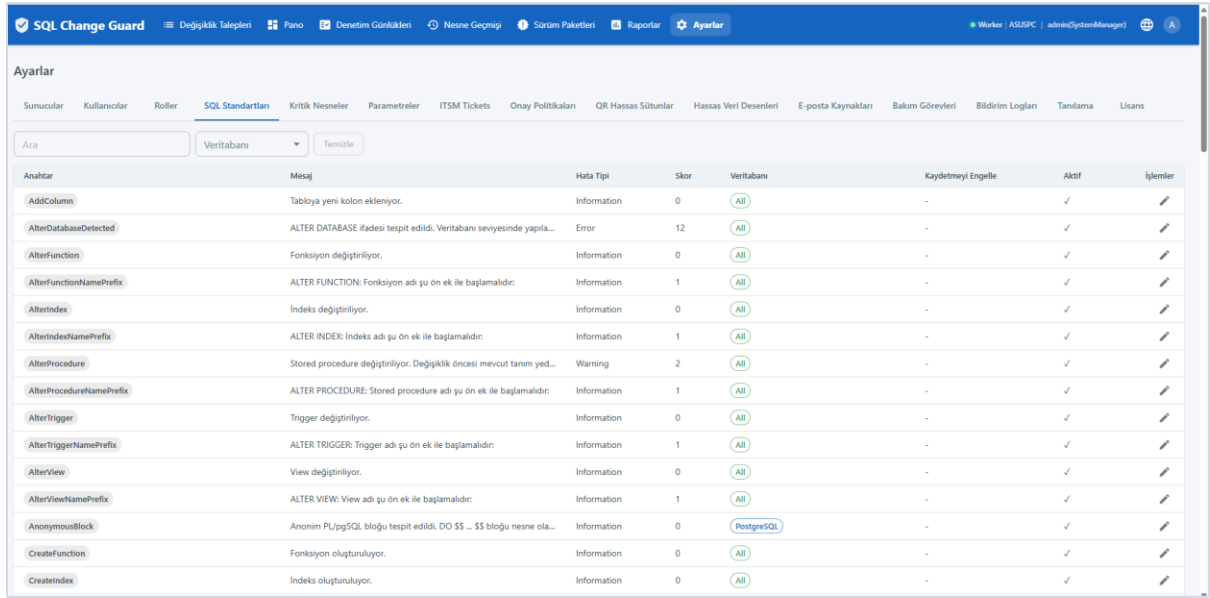
- Kimlik doğrulama: JWT tabanlı; LDAP / Active Directory entegrasyonu (LDAPS ya da StartTLS, izin grubundan rol eşlemesi, iç içe gruplar, değişmeyen kimlikle hesap bağlama, zamanlanmış izin eşitlemesi ve toplu kapatma güvenlik sınırı); kurum hesabıyla giriş (SSO): OIDC ve SAML 2.0
- Çok faktörlü kimlik doğrulama (MFA) desteği
- Rol bazlı ve backend zorunlu yetkilendirme (endpoint, servis, ekran, aksiyon, worker)
- Sunucu şifreleri at-rest AES-GCM ile şifreli saklanır
- Sorgu sonuçları şifreli ZIP olarak teslim edilir
- Zip parolası varsayılan olarak mailde gitmez; portalde gerekçeyle görüntülenir ve görüntüleme denetlenir
 - Append-only audit: SQL Server ledger tablosu (veritabanı motoru UPDATE ve DELETE işlemlerini reddeder) ve yapılandırılan klasöre yazılan defter özeti (imza açıksa imzalı)
 - Görevler ayrılığı (separation of duties)

4. Entegrasyon

- LDAP / Active Directory (kullanıcı ve kimlik); Microsoft Entra ID, AD FS, Keycloak, Okta gibi OIDC ya da SAML 2.0 kimlik sağlayıcıları (kurum hesabıyla giriş)
- SMTP (bildirim ve onay e-postaları)
- SIEM: Syslog (UDP, TCP, TLS) ya da dosya; RFC 5424 (JSON ya da yapılandırılmış veri), CEF, LEEF ve JSON biçimleri
- ITSM: ServiceNow, Jira ve genel REST bağlayıcısı; bilet numarası biçimi regex ile doğrulanır, bilet kayıta ve çalıştırmada doğrulanabilir, bilete not yazılır (entegrasyon varsayılan olarak kapalıdır)

5. Konfigürasyon ve Kurallar

- Konfigürasyon appsettings ve Parameters tablosu üzerinden yönetilir; ortama özgü değerler ve sırlar koda gömülmez
- 88 SQL standart kuralı ekrandan aktif/pasif edilebilir ve veritabanı tipine göre filtrelenir
- Onay politikaları sunucu, ortam ve sorgu tipine göre tanımlanır
- Hassas veri desenleri (regex) ve kritik obje listesi yönetilebilir
- Kritik nesne tanımlarında veritabanı ve şema boş bırakılabilir: boş veritabanı tüm veritabanları, boş şema tüm şemalar demektir. Nesne tipi her zaman zorunludur ve eşleşmede birebir aranır. Aynı kural üç veritabanı tipinde de geçerlidir.
- Tüm tarihler UTC saklanır; kullanıcıya yerel saat gösterilir



The screenshot shows the 'Ayarlar' (Settings) page of the SQL Change Guard application. The 'SQL Standartları' (SQL Standards) tab is selected. A table lists various SQL standard rules with columns for 'Anahtar' (Key), 'Mesaj' (Message), 'Hata Tipi' (Error Type), 'Skor' (Score), 'Veritabanı' (Database), 'Kaydetmeyi Engelle' (Prevent Saving), 'Aktif' (Active), and 'İşlemler' (Actions). The 'Veritabanı' column is filtered to show 'All' for most rules, except for 'AnonymousBlock' which is set to 'PostgreSQL'.

Anahtar	Mesaj	Hata Tipi	Skor	Veritabanı	Kaydetmeyi Engelle	Aktif	İşlemler
AddColumn	Tabloya yeni kolon ekleniyor.	Information	0	All	-	✓	✎
AlterDatabaseDetected	ALTER DATABASE ifadesi tespit edildi. Veritabanı seviyesinde yapıla...	Error	12	All	-	✓	✎
AlterFunction	Fonksiyon değiştiriliyor.	Information	0	All	-	✓	✎
AlterFunctionNamePrefix	ALTER FUNCTION: Fonksiyon adı şu ön ek ile başlamalıdır:	Information	1	All	-	✓	✎
AlterIndex	İndeks değiştiriliyor.	Information	0	All	-	✓	✎
AlterIndexNamePrefix	ALTER INDEX: İndeks adı şu ön ek ile başlamalıdır:	Information	1	All	-	✓	✎
AlterProcedure	Stored procedure değiştiriliyor. Değişiklik öncesi mevcut tanım yed...	Warning	2	All	-	✓	✎
AlterProcedureNamePrefix	ALTER PROCEDURE: Stored procedure adı şu ön ek ile başlamalıdır:	Information	1	All	-	✓	✎
AlterTrigger	Trigger değiştiriliyor.	Information	0	All	-	✓	✎
AlterTriggerNamePrefix	ALTER TRIGGER: Trigger adı şu ön ek ile başlamalıdır:	Information	1	All	-	✓	✎
AlterView	View değiştiriliyor.	Information	0	All	-	✓	✎
AlterViewNamePrefix	ALTER VIEW: View adı şu ön ek ile başlamalıdır:	Information	1	All	-	✓	✎
AnonymousBlock	Anonim PL/pgSQL bloğu tespit edildi. DO \$\$... \$\$ bloğu nesne ola...	Information	0	PostgreSQL	-	✓	✎
CreateFunction	Fonksiyon oluşturuluyor.	Information	0	All	-	✓	✎
CreateIndex	İndeks oluşturuluyor.	Information	0	All	-	✓	✎

SQL Standart Kuralları - aktif/pasif ve veritabanı tipine göre filtre

6. Denetim ve Raporlama

34 hazır rapor Excel ve PDF olarak alınabilir; dinamik rapor tanımları desteklenir. Rapor yetkisi iki katmanlıdır: ekran yetkisi ve rapor bazlı rol kısıtı. Kısıt hem listede hem çalıştırmada sunucu tarafında

uygulanır.

Raporlar

- Değişiklik Genel Bakış
- Değişiklik Talep Özeti
- Nesneye Göre Değişiklik Talebi
- Devam Eden İşler (WIP)
- Reddedilen / İptal Talepler
- Yüksek Riskli Değişiklikler
- Rollback Edilen Değişiklikler
- Onay Süresi Analizi
- NESNE & YAPİ ANALİZİ
- Kritik Nesne Erişimleri
- Nesne Değişiklik Sıklığı
- Tablo Yapı Değişiklikleri
- Veri Değişiklik Sıklığı
- Çok Kız Değiştirilen Nesneler
- Aktif Çakışmalar

Değişiklik Talep Özeti
Belirli tarih aralığında oluşturulan değişiklik taleplerini; durum, sunucu, talep no ve güvenlik skoru bilgileriyle listelen.

Filtreler

Başlangıç Tarihi: 2026-06-08
Bitiş Tarihi: 2026-07-08
Durum:
Sunucu Adı:
Değişiklik Talep No:

Raporu Çıktır Excel PDF 21 kayıt bulundu

RequestId	Description	Status	QueryType	CreatedBy	ServerName	ChangeTicket	SafetyScore	CreatedAt	ExecutedAt	ExecutedBy
21	Operasyon ekibine müşteri verisi gönderme	Pending	QueryResult	admin	ASUSPC	CR-00002	20	08.07.2026 15:57:15	-	-
20	Operasyon ekibine müşteri verisi gönderme	Executed	QueryResult	developer	ASUSPC	CR-00002	20	08.07.2026 12:57:06	08.07.2026 12:58:34	WorkerServ
19	Operasyon ekibine müşteri verisi gönderme	Executed	QueryResult	developer	ASUSPC	CR-00002	20	08.07.2026 12:50:21	08.07.2026 12:53:13	WorkerServ
18	Müşteri verisi çekme	Pending	QueryResult	developer	ASUSPC	CR-00001	0	08.07.2026 12:47:13	-	-
17	Müşteri verisi çekme	Pending	QueryResult	dbadmin	ASUSPC	CR-00001	0	08.07.2026 12:46:30	-	-
16	Müşteri verisi çekme	Executed	QueryResult	developer	ASUSPC	CR-00001	0	08.07.2026 11:57:42	08.07.2026 12:08:49	WorkerServ
15	Müşteri verisi çekme	Executed	QueryResult	admin	ASUSPC	CR-00001	0	08.07.2026 00:34:24	08.07.2026 00:37:54	WorkerServ
14	customer table add	Executed	Change	admin	ASUSPC	CR-00001	0	08.07.2026 00:28:24	08.07.2026 00:28:45	WorkerServ
13	aaaa	Executed	QueryResult	admin	oracletest	CR-00001	0	07.07.2026 23:06:50	07.07.2026 23:07:11	WorkerServ
12	ssss	Executed	Change	admin	oracletest	CR-00001	87	07.07.2026 23:04:54	07.07.2026 23:05:09	WorkerServ
11	ssss	Executed	Change	admin	oracletest	CR-00001	87	07.07.2026 23:03:59	07.07.2026 23:04:09	WorkerServ
10	ssss	Executed	Change	admin	oracletest	CR-00001	91	07.07.2026 23:01:26	07.07.2026 23:01:40	WorkerServ
9	ssss	Rejected	Change	admin	oracletest	CR-00001	91	07.07.2026 23:00:46	-	WorkerServ
8	aaaa	Executed	QueryResult	admin	oracletest	CR-00001	37	07.07.2026 22:57:32	07.07.2026 22:57:42	WorkerServ

Rol kısıtlı bir raporun okunması da denetim izine yazılır: kim, hangi raporu, hangi filtrelerle ve kaç satır görmüş. Kayıta satır verisi tutulmaz. Kısıtsız raporlarda kayıt tutulmaz, böylece denetim izi gürültüye boğulmaz.

ITSM bilet ekleme, güncelleme ve silme işlemleri de denetim izine yazılır. Bilet bilgisi bir kontrol ayarı olmadığı için dört göz onayına düşmez; tek kanıt denetim kayıdır.

Kanıt dosyasında hedef bilgisi sunucu adı, veritabanı motoru ve veritabanı adı olarak birlikte yazılır. Veritabanı adı sunucu tanımındaki varsayılan veritabanından gelir; script içinde USE varsa çalışma anında onu ezdiği için o da ayrı satırda gösterilir.

Bir sorgu sonucu talebi birden çok sunucuya gidebilir; sunucu adları noktalı virgülle ayrılır. Sunucu çözümlemesi bu ayrımı dikkate alır: veritabanı tipi ve adı her sunucu için ayrı çözülür, otomatik çalıştırma ancak hedef sunucuların hepsi izin veriyorsa açılır, sunuculardan biri silinmişse makine çalıştırmaz.

Sorgu sonucu paketindeki veri dosyası Excel veya CSV olarak yazılır ve seçim ayarla yönetilir. Varsayılan Auto biçiminde küçük sonuçlar Excel, belirlenen eşğin üstündeki sonuçlar CSV olarak üretilir. Bunun iki sebebi vardır: bir Excel sayfasına en fazla 1.048.575 veri satırı yazılabilir ve Excel yazımı satır sayısı ile birlikte hızla pahalılaşır. CSV dosyası noktalı virgül ayracı ve UTF-8 işaretiyle yazılır; metin hücrelerinde formül olarak çalışabilecek değerler etkisizleştirilir, sayısal değerler ise sayı olarak kalır.

Teslim edilebilecek satır sayısının bir üst sınırı vardır ve bu sınır sonuç okunurken uygulanır: sınıra ulaşıldığı anda okuma durdurulur, talep başarısız olur ve denetim izine yazılır. Böylece bellekte sınırdan fazla satır tutulmaz, maskeleme ve dosya yazımı hiç çalışmaz. Üst sınır bir kontrol ayarıdır ve dört göz kuralının kapsamına girer, çünkü değeri yükseltmek tek bir onaylı talebin daha fazla canlı veriyi kurum dışına taşıyabilmesi demektir.

Ölçülmüş maliyet (10 kolonlu sonuç, 5 kolon maskeli, 4 çekirdekli dizüstü sınıfı makine): 1 milyon satırda hassas veri tespiti 0,04 saniye, maskeleme 10,8 saniye, CSV yazımı 6,4 saniye, süreç belleği

yaklaşık 1,5 GB. Tespit örneklem tabanlı olduğu için süresi satır sayısı ile artmaz; maliyetin tamamına yakını maskeleme ve dosya yazımındadır.

Raporlar - 34 hazır rapor, beş grup

- Change Governance: talep özeti, nesne bazlı talep izi, devam eden işler, reddedilen ve iptal edilenler, yüksek riskli değişiklikler, rollback değişiklikleri, onay ve çalıştırma süreleri, çalıştırma etkinliği, onay adımı detayı, sandbox test sonuçları, kontrol istisnaları, acil değişiklik gözden geçirme, ITSM kontrol istisnaları, dönem popülasyonu
- Object & Structure: kritik nesne erişimi, nesne değişim sıklığı, tablo yapısı değişiklikleri, veri değişim sıklığı, birden fazla sürümde değişen nesneler, aktif çakışmalar
- Access & Authorization: ayrıcalıklı hesap işlemleri, kullanıcı DDL etkinliği, kullanıcı yetki matrisi, kullanıcı erişim değişiklikleri, beklenen erişim hesapları (Expected Access Principals)
- Data & Privacy: sorgu sonucu etkinliği, hassas kolon dokunuşları, maskeleme etkinliği, sınıflandırma kataloğu, maskeleme muafiyeti olan sunucular, elle veri müdahaleleri, veri erişimi ve dışa aktarım kaydı
- Configuration & Compliance: yapılandırma değişiklikleri, ayar değişikliği onay izi

7. Sistem Gereksinimleri

Bileşen	Gereksinim
Uygulama veritabanı	SQL Server 2022 veya üzeri (denetim kayıtları append-only defter tablosunda)
Sunucu ortamı	Windows Server (IIS/Kestrel + Windows Service)
Çalışma zamanı	.NET 10
Hedef veritabanları	SQL Server, PostgreSQL, Oracle
İstemci	Modern web tarayıcısı (Chrome, Edge, Firefox)
Ağ	Kurum içi; internet bağlantısı gerekmez

8. Kurulum

Şema, numaralı ve checksum korumalı dört kurulum betiğiyle uygulanır; Database:AutoMigrate açıkken bunu API açılışta kendisi yapar, kapalıyken betikleri veritabanı yöneticisi uygular. Kurulum adımları 06 Kurulum Ön Hazırlık ve 07 Kurulum ve İşletim belgelerindedir.

9. İletişim

- Web: www.sqlchangeGuard.com
- E-posta: onur.egilmez@sqlchangeGuard.com | info@sqlchangeGuard.com
- Telefon: 0505 621 29 02
- LinkedIn: [linkedin.com/company/sqlchangeGuard](https://www.linkedin.com/company/sqlchangeGuard)

Şifreleme ve Anahtar Yönetimi

SQL Change Guard hassas verileri üç ayrı kategoride, amacına uygun kriptografik yöntemlerle korur. Geri döndürülmesi gerekmeyen sırlar tek yönlü özetlenir (hash); uygulamanın çalışması için geri açılması gereken sırlar ise kimlik doğrulamalı şifreleme ile saklanır. Böylece her veri, ihtiyacına en uygun ve endüstri standardı yöntemle korunur.

1. Kullanıcı parolaları: BCrypt (tek yönlü hash)

Kullanıcı parolaları BCrypt algoritmasıyla (iş faktörü 12 ve kayıt başına rastgele salt) özetlenerek saklanır. Bu tek yönlü bir işlemdir: parolanın açık hali hiçbir yerde tutulmaz ve geri elde edilemez. Kimlik doğrulama, girilen parolanın yeniden özetlenip saklanan özetle karşılaştırılmasıyla yapılır. Veritabanı ele geçirilse bile özetten parola doğrudan elde edilemez; zayıf parolalar deneme yoluyla bulunabileceği için parola kuralları ayrıca önemlidir.

2. Sunucu veritabanı parolaları: AES-256-GCM (şifreleme)

Hedef veritabanlarına bağlanmak için kullanılan parolalar (Servers.SqlPassword) at-rest olarak AES-256-GCM kimlik doğrulamalı şifreleme ile saklanır. GCM modu hem gizlilik hem de bütünlük sağlar: her kayıt rastgele bir nonce ve doğrulama etiketi (tag) içerir, kurcalanan veri çözülemez. Uygulama, hedef veritabanına bağlanırken parolayı yalnızca bellekte, kısa süreliğine çözer.

3. QR paket zip parolaları: AES-256-GCM (şifreleme)

Sorgu sonucu (QueryResult) paketlerinin parola korumalı zip dosyaları için üretilen parolalar da sunucu parolalarıyla tamamen aynı ilkeyle, AES-256-GCM ile şifrlenerek saklanır. Böylece geri döndürülebilir tüm sırlar tek, doğrulanabilir bir kriptografik yöntem kullanır; bu da hem güvenliği hem de sistemin anlaşılabilirliğini artırır.

Denetim izi bütünlüğü: append-only defter

Denetim kayıtları (audit trail) SQL Server 2022 ile gelen append-only ledger (defter) tablosunda (evidence.AuditLogs) tutulur. Veritabanı motoru kayıt değiştirmeyi ve silmeyi sysadmin dahil herkes için reddeder. Ürün tabloya yalnız evidence.usp_Audit_Append yordamıyla yazar; şemanın sahibi girişi olmayan ayrı bir kullanıcıdır, bu yüzden dbo şemasındaki bir tetikleyici ya da yordam tabloya yazamaz. Ürün tablonun defter olduğunu, tetikleyici taşımadığını, yazma yordamının yayımlanan sürümle aynı olduğunu ve şemada beklenmeyen nesne bulunmadığını düzenli olarak denetler; sınır bozulursa durum değiştiren işlemler durur. Kayıtların bütünlüğü gizli bir anahtara dayanmaz.

Anahtar yönetimi

Sunucu ve QR zip parolalarını şifreleyen anahtarlar 256-bit uzunluğundadır (32 bayt, base64) ve uygulama yapılandırmasının Security bölümünde toplanır: Security:ServerPasswordKey (sunucu parolaları) ve Security:QrZipPasswordKey (QR zip parolaları). Anahtarlar üretim ortamında ortam değişkeni (environment variable) olarak sağlanır; kaynak koda veya veritabanına gömülmez.

Özet: Kullanıcı parolası tek yönlü hash (BCrypt) ile; sunucu ve QR zip parolaları çift yönlü şifreleme (AES-256-GCM) ile; denetim izi ise append-only defter ve dış özetle (imza açıkça imzalı) korunur.

Defter özeti: Worker varsayılan olarak saatte bir özet turunu başlatır; API veritabanının defter özetini alır, imzalar (imza açıkça; RSA, 3072 bit önerilir) ve yapılandırılan klasöre (Evidence:Ledger:DigestOutputPath) yazar. Bu klasörün değiştirilemez bir depoda (WORM gibi) olması kurumun sağlamasıdır; klasör tanımlı değilse dış dosya yazılmaz. Denetçi bu özetlerle veritabanının bir kopyasında sys.sp_verify_database_ledger yordamını çalıştırarak defterin değişmediğini doğrular. Eski bir yedeğe dönülmesi ancak bu dış özetle karşılaştırmada fark edilir.

Kanıt imza anahtarı Windows sertifika deposunda dışa aktarılamaz olarak tutulabilir (yapılandırmada yalnız parmak izi). İmzalama açıkken anahtar kullanılamazsa kanıt çıktısı üretilmez; imzasız dosya sessizce çıkmaz.

Oturum yenileme jetonları, parola sıfırlama bağlantıları ve iki adımlı doğrulama biletleri veritabanında açık metin olarak tutulmaz; SHA-256 özetleri saklanır. Bu değerler kriptografik olarak rastgele üretildiği için özet, veritabanını okuyabilen birinin bunlarla oturum açmasını ya da parola sıfırlamasını engeller.

Yönetişim Kapıları ve Kural Motoru Kapsamı

Kural motorunun kapsamı ve sınırı

Kural motoru betiği gerçek dilbilgisiyle ayrıştırır: SQL Server için Microsoft ScriptDom, PostgreSQL için libpg_query tabanlı ayrıştırıcı, Oracle için ANTLR4 PL/SQL grameri kullanılır. Kurallar ağaç düğümleri üzerinden çalışır; bu yüzden yorum satırındaki bir kelime kural tetiklemez, parantezle sarılmış bir koşul gözden kaçmaz. Sınır: PostgreSQL'de bazı kontroller yardımcı düzenli ifadelerle yapılır; Oracle'da ağaç ayrıştırması başarısız olursa düzenli ifade analizine düşülür.

Kapsam içinde olan: betiğin kendisinden okunabilen her şey. Filtresiz DELETE ve UPDATE, kritik nesne üzerinde DROP ve TRUNCATE, betiğe elle yazılmış BEGIN, COMMIT ve ROLLBACK ifadeleri, adlandırma kuralları, izin verilmeyen ifadeler, örtülü commit üreten Oracle ifadeleri, hassas kolonlara erişen SELECT ifadeleri.

Kapsam dışında olan: hedef veritabanının kataloğuna bakmayı gerektiren kontroller. Bir sorgunun indeksli kolon kullanıp kullanmadığı bunun tipik örneğidir; cevap betikte değil, o anki indeks tanımlarındadır ve zaman içinde değişir. Bu alan veritabanı izleme araçlarının konusudur.

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 betikten okunabileni değerlendirir.

İzole deneme kapısı

Sunucu tanımındaki izole deneme zorunluluğu bayrağı açıkken, çalıştırma için güncel ve başarılı bir deneme sonucu aranır. Deneme sonucunun güncelliği, sonucun oluşma zamanı ile talebin son değişiklik zamanı karşılaştırılarak belirlenir; betik denemeden sonra düzenlenmişse sonuç bayat sayılır.

Kapı tek bir serviste toplanmıştır ve üç çalıştırma yolunda da aynı servis çağrılır: elle çalıştırma, zamanlanmış çalıştırma ve sürüm paketi. Kuralın kopyalanmaması, üç yolun zamanla farklı davranmasını engeller.

Aynı değerlendirme arayüzdeki düğme durumunu da belirler. Ekran ile komut aynı kaynaktan beslendiği için bu kapı açısından ekranın izin verip sunucunun reddettiği bir durum oluşmaz; onay zinciri, ITSM ve kanıt yazma sınırı gibi işlem anında yapılan kontroller ise düğme açıkken de işlemi durdurabilir ve sebebi mesajda yazar.

Geri alma planının bütünlüğü

Geri alma üretimi sırasında nesne tanımı okunamazsa betiğe bir eksiklik işareti konur ve betik geçerli bir geri alma sayılmaz. Bu kontrol tek bir yerde tanımlıdır; hem çalıştırma kapısı hem de ekrandaki gösterge aynı tanımı kullanır.

Otomatik geri alma üretimi onay anında sistem bağlamında çalışır ve onaylayan kullanıcının talep ekleme yetkisine bağlı değildir. Görevler ayrılığının doğru kurulduğu bir kurumda onaylayan kullanıcı talep ekleyemez; üretimin bu yetkiye bağlanması kontrolün kendisini cezalandırırdı.

Üretim başarısız olursa talepte üretilemedi bayrağı, zamanı ve hata sebebi saklanır; olay denetim izine sistem adına yazılır. Sonradan bir geri alma planı oluşturulduğunda bayrak temizlenir.

Tablo tanımından üretilen geri alma betiği birincil anahtar, benzersizlik kısıtları, kontrol kısıtları, yabancı anahtarlar ve indeksleri içerir. Kapsam dışında kalan öğeler betiğin başında tek bir açıklama satırıyla belirtilir ve bu açıklama üç veritabanı türünde de aynı kaynaktan gelir. Veri değişiklikleri (INSERT, UPDATE, DELETE, MERGE, TRUNCATE, EXEC) için geri alma betiği üretilmez; yerine elle müdahale notu yazılır ve plan eksik sayılır. Hesaplanan kolon ifadesi SQL Server ve PostgreSQL'de korunmaz, düz kolon olarak yazılır ve bu not satırında belirtilir.

Engellenen görevler ayrılığı girişimleri

Görevler ayrılığı kuralı bir onaylama veya çalıştırma girişimini engellediğinde, engelleme denetim izine kendi olay adıyla yazılır. Kayıt talep numarasını, engelleme sebebini ve girişimde bulunan kullanıcıyı içerir.

Denetim kaydının yazılamaması işlemin sonucunu değiştirmez: engelleme her koşulda geçerlidir, kayıt hatası yalnızca uygulama günlüğüne düşer. Kanıt üretimi, korumanın önüne geçemez.

İlk girişte parola değiştirme

Parola değiştirmesi gereken kullanıcının oturum jetonu ayrı bir işaret taşır. Bu işaret varken istek hattındaki bir davranış katmanı, parola değiştirme ve jeton yenileme dışındaki bütün istekleri reddeder.

Kontrol arayüzde değil sunucuda yapılır. Arayüzün kullanıcıyı yönlendirmesi kullanım kolaylığıdır, güvenlik sınırı değildir. Parola değiştirildiği anda yeni jeton işareti taşımaz ve oturum normale döner.

İki adımlı doğrulama kodu yalnız parola adımından dönen tek kullanımlık, kısa ömürlü biletle birlikte kabul edilir; kullanıcı adı ve kod bilinerek giriş yapılamaz. Bir biletle sınırlı sayıda hatalı kod denenebilir, hatalı kodlar hesap kilidine sayılır ve kabul edilmiş bir kod ikinci kez kullanılamaz. LDAP hesapları da iki adımlı doğrulama kullanabilir.

Oturumun toplam süresi yapılandırmayla sınırlıdır (Auth:MaxSessionHours); jeton yenileme bu süreyi uzatmaz. Parola değişince kullanıcının diğer oturumları, parola sıfırlanınca, rol ya da kimlik tipi değişince ve hesap kapatılınca bütün oturumları kapanır. Kapatma hemen etkilidir: erişim jetonu bir oturum sürümü taşır ve her istekte veritabanıyla karşılaştırılır, eski sürümlü jeton reddedilir. Denetim kayıtlarındaki IP adresi bağlantıdan okunur; X-Forwarded-For başlığı yalnız yapılandırmada tanımlı ters vekillerden geldiğinde işlenir.

Kurum hesabıyla giriş (SSO)

Ürün OIDC (yetkilendirme kodu akışı, PKCE) ve SAML 2.0 ile kurumun kimlik sağlayıcısına bağlanır; birden fazla sağlayıcı aynı anda tanımlanabilir. Şifre ve çok faktörlü doğrulama kurumun giriş sayfasında yapılır, şifre ürüne gelmez. Kimlik sağlayıcısının cevabı imza, süre, hedef kitle ve tek kullanımlık istek bilgisiyle doğrulanır; cevaptaki çok faktörlü doğrulama bilgisi denetlenebilir. Kişi değişmeyen kimliğiyle bulunur; e-posta ya da kullanıcı adıyla eşleştirme yapılmaz ve yerel bir hesaba kendiliğinden bağlanılmaz.

Rol, kimlik sağlayıcısındaki gruptan eşleme tablosuna göre verilir; birden fazla grup eşleşirse en yüksek rol kazanır. SystemManager rolü eşlemeyle verilemez. Eşleme değişiklikleri ayar değişikliği onayından (dört göz) geçebilir. Rol her girişte yeniden hesaplanabilir; rolü düşen kişinin açık oturumları hemen kapanır. Kurum hesabı oturumunun süresi ayrıca sınırlanır. Kimlik sağlayıcısı erişilemezse yalnız tanımlı acil durum hesapları şifreyle girer ve her girişleri denetim izine yazılır ve SIEM bağlıysa SOC'a alarm olarak gider. Giriş, ret, hesap açma, rol eşitleme ve kimlik bağı olayları denetim izine yazılır.

Yönetişim kurulum kontrolü

Tanılama altındaki yönetim kurulum kontrolü, kontrolleri şu gruplarda değerlendirir: görevler ayrılığı, geri alma ve izole deneme, talep disiplini, kimlik ve parola (kurum hesabıyla giriş kontrolleri dahil), veri koruma, denetim ve kanıt, ITSM, sır yerleşimi, ürün dışında doğrulananlar. Her kontrol o anki değerinden canlı okunur; sonuç saklanmaz.

Her kontrol satırı ayarın kaynağını da taşır: hangi ekrandan yönetildiği ve tam anahtar adı. Kaynak dile çevrilir, anahtar çevrilmez; çünkü aranacak olan metnin kendisidir. Doğru cevabı kuruma göre değişen kontroller tavsiye niteliğinde işaretlenir. Ekran bir dayatma üretmez; bir kararın verilip verilmediğini gösterir. Bir bayrağın bağlı olduğu modül lisanslı değilse bayrağın değeri yerine bu bilgi yazılır: çalışmayan bir kapıyı açık göstermek yanıltır.

Acil değişiklik gözden geçirme

Uygulanmış acil değişiklikler için olay sonrası gözden geçirme kaydı tutulur. Kayıt gözden geçiren kişiyi, zamanı, zorunlu notu, değişikliğin gerçekten acil olup olmadığı cevabını ve kalıcı çözüm için talep açılıp açılmadığı cevabını içerir.

Yetki kontrolü hem jetondan hem canlı veritabanından yapılır; yetkisi çekilmiş bir kullanıcı elindeki jetonla gözden geçirme yapamaz. Talebi açan kişi kendi talebini gözden geçiremez ve gözden geçirme yalnız bir kez yapılır.

Bekleyen gözden geçirmeler kontrol panelinde tarih aralığından bağımsız bir sayaçla, ayrıca kendi raporunda bekleme süresiyle birlikte izlenir. Kayıt talebin denetim dosyasına ayrı bir bölüm olarak girer.

Maskesiz kolon onayının risk bandına etkisi

Maskesiz hassas kolon gösterimine onay verildiğinde talebin risk hesabı yeniden yapılır. Yeniden hesaplama, kaydedilmiş bulgu ayrıntılarından yeniden kurgulanır; her bulgunun tekrar sayısı korunur, böylece yeni bulgu eklenmesi eski bulguların ağırlığını değiştirmez.

İşlem tekrar edilebilirdir: aynı onay iki kez işlense bile bulgu bir kez eklenir. Bulgunun kritiklik derecesi SQL standartları kataloğundan yönetilir; standart pasife alınırsa kural tümüyle devre dışı kalır.

Bağlantı kontrolü işinin ölçeklenmesi

Sunucu bağlantı kontrolü işi, sunucuları eş zamanlı denetler. Eş zamanlılık derecesi yapılandırmadan verilir; geçersiz bir değer verilirse güvenli varsayılanı düşülür ve üst sınır aşılmaz. Bildirim üretimi eş zamanlı bölümün dışında, tek sıra halinde ve sunucu adına göre sıralı yapılır; böylece aynı kesinti için üretilen bildirimlerin sırası çalıştırmadan çalıştırmaya değişmez.

DAM ve SIEM Eşleşmesi

Oturum adı ve oturum yoklaması

Hedef veritabanına açılan her bağlantı SQL Change Guard/<Rol>/<Numara> adını taşır (en fazla 63 karakter, yalnız ASCII). Roller: Execute, Query, Release, Sandbox, SandboxRelease (havuz kapalı, pencere açar), Health, Preview, Definition, Test (havuz açık, pencere açmaz). SQL Server ve PostgreSQL'de ad bağlantı dizesindeki uygulama adıdır; Oracle'da bağlantı açıldıktan sonra MODULE, ACTION ve CLIENT_IDENTIFIER alanlarına yazılır. Bağlantı açılınca tek bir okuma sorgusu oturum numarasını ve hedefin gördüğü istemci adresini alır; sorgu başarısız olursa alanlar boş kalır ve iş devam eder. Oturum adı istemci beyanıdır ve taklit edilebilir; DAM kuralları hesap, istemci adresi ve oturum numarasına dayanmalıdır. Ürün DAM değildir: canlı trafiği dinlemez, ürün dışında açılan oturumları DAM aracı görür.

Yürütme ve sandbox pencere olayları

Olay	Yazan
ChangeRequest.ExecutionStarted, ExecutionEnded	Worker
ReleasePackage.ExecutionStarted, ExecutionEnded (AllOrNothing)	Worker
ChangeRequest.SandboxRequested, ReleasePackage.SandboxRequested	API, isteyen kişi adına
ChangeRequest.SandboxStarted, SandboxFinished;	Worker

ReleasePackage.SandboxStarted, SandboxFinished	
---	--

Başlangıç yükü: windowKind, serverName, executionLogin, executorHost, clientAddress, targetSessionId, targetAuditSessionId (yalnız Oracle), sessionApplicationName, executionStartedAt, packageId, requestIds, sandboxId, changeTicket (talebin ITSM kaydı), emergencyTicket (acil talepte olay kaydı). Biletler yalnız yürütme başlangıcında bulunur, talep kaydında dondurulmuş değerdir ve AllOrNothing paketinde requestIds ile aynı sırada noktalı virgülle ayrık listedir (biletsiz talep boş eleman); sandbox pencereleri bilet taşımaz. Bitiş yükü: windowId (başlangıç olayının denetim kaydı numarası), windowKind, windowOutcome (executed, failed, cancelled, rolledBack, abandoned), serverName, executionFinishedAt, packageId, sandboxId. Başlangıç olayı yazılamazsa betik çalışmaz ve talep reddedilmez; bitiş olayı yazılamazsa iş sonucu değişmez. Olaylar Notice ciddiyetindedir.

Rapor, denetim dosyası ve Kurulum Kontrolü

Expected Access Principals raporu her sunucu için ürünün hesabını, görülen rolleri, makine adlarını ve istemci adreslerini verir (parola yok, kirli okuma yok). Denetim dosyası Yürütme pencereleri bölümü ve EXECUTION_CANCELLED, EXECUTION_ABANDONED, SANDBOX_ABANDONED, EXECUTION_WINDOW_OPEN istisna kodlarını içerir. Yönetişim kurulum kontrolünde TargetAccountDedicated ve DamAllowlistMaintained beyanları öneri satırlarıdır.

SIEM taşıması

Pencere alanları SIEM izin listesindedir ve JSON, RFC 5424, LEEF, CEF biçimlerinde taşınır. CEF'te start, end, duser, shost, src, requestClientApplication, cn1 ila cn3 ve cs4 ila cs6 alanlarına yazılır; changeTicket cs3, emergencyTicket flexString1, requestIds flexString2 alanındadır (etiketleriyle). targetAuditSessionId CEF'te taşınmaz.