SQL Change Guard

Sıkça Sorulan Sorular

Kurumsal SSS

SQL Server | PostgreSQL | Oracle

Genel

SQL Change Guard tam olarak ne yapar?

Veritabanı değişikliklerini (Database Change Governance), production veri erişimini (Production Query Governance) ve uyumluluğu (Compliance and Audit) tek platformda yönetir. Değişiklikleri deployment öncesi 84+ kuralla analiz eder, risk skorlar, onay akışına alır, çalıştırır ve tam audit tutar.

Migration araçlarından (Flyway, Liquibase gibi) farkı nedir?

Migration tabanlı yaklaşımın ötesinde; production veri erişimi yönetişimi, hassas veri maskeleme, policy engine, risk analizi, otomatik rollback ve denetime hazır audit trail sunar. Yani sadece schema deployment değil, uçtan uca veritabanı operasyon yönetişimidir.

Veritabanı ve Kurulum

Hangi veritabanlarını destekliyor?

SQL Server, PostgreSQL ve Oracle. Her biri için ayrı parser ve kural motoru vardır; aynı yönetişim modeli üçünde de çalışır. Uygulamanın kendi yönetim veritabanı SQL Server'dır.

İnternet bağlantısı gerekiyor mu?

Hayır. Tamamen kurum içi (on-premise) çalışır. Kurulum en fazla 30 dakikada tamamlanacak şekilde tasarlanmıştır.

Güvenlik ve Uyumluluk

WHERE koşulsuz DELETE/UPDATE gibi hataları nasıl engelliyor?

Script yüklendiğinde parser devreye girer. WHERE koşulu eksik DELETE/UPDATE tespit edilince risk skoru kritik seviyeye düşer ve kural bloklayıcıysa kayıt/deployment engellenir.

KVKK ve bankacılık denetimine uygun mu?

Evet. KVKK, ISO 27001, COBIT ve ITIL gözetilerek tasarlanmıştır. Hassas veri maskeleme, değiştirilemeyen (hash zinciri) audit kayıtları, onay kanıtları ve 30 hazır rapor ile denetime hazırdır.

Hassas veriyi nasıl koruyor?

TC, kart, IBAN, telefon gibi desenler regex ve doğrulama algoritmalarıyla tespit edilir; hassas kolonlar otomatik maskelenir (tam maske / kısmi maske). Maskesiz veri ek onay gerektirir; sonuçlar şifreli ZIP olarak teslim edilir ve indirme kaydı tutulur.

Bir denetçi tek bir talebin tüm kanıtını isterse ne veririm?

Talep detay ekranından tek tıkla Denetim Dosyası indirilir: talebin künyesi, görevler ayrılığı, onay kanıtı, script parmak izi (onaylanan ile çalıştırılanın aynı olduğunun ispatı), risk skoru, çalıştırma kaydı ve tüm denetim izi tek dosyada (PDF ve JSON) toplanır. Dosya bir paket mührü (SHA-256) taşır ve

sistem üzerinden değişmediği doğrulanabilir. İndirme ayrı bir yetki gerektirir ve işlemin kendisi de audit altına alınır.

Değişiklik ve Rollback

Rollback nasıl çalışır?

Her değişiklik için rollback script'i üretilebilir. Oracle'da DDL/DCL/TRUNCATE örtülü COMMIT yaptığından, bu tür Oracle değişikliklerinde rollback zorunludur ve onay anında otomatik hazırlanabilir. Kaynak talep düzenlenirse rollback güncellenir.

Sandbox ne işe yarar?

Değişikliği canlıya geçmeden gerçek ortamda çalıştırıp geri alarak (BEGIN-ROLLBACK) doğrular. Böylece hatalar production'a ulaşmadan görülür.

Ticari

Fiyatlandırma nasıl?

Sunucu sayısı, kullanıcı adedi ve modüllere göre kişiselleştirilir. Bankacılık, finans ve kamu için özel paketler mevcuttur. Ücretsiz demo talep ederek teklif alabilirsiniz.

Nasıl başlarım?

info@sqlchangeguard.com adresine yazın veya 0505 621 29 02 numarasından ulaşın; 20-30 dakikalık kısa bir online demo planlayalım.

İletişim

- Web: www.sqlchangeguard.com
- E-posta: onur.egilmez@sqlchangeguard.com | info@sqlchangeguard.com
- Telefon: 0505 621 29 02
- LinkedIn: linkedin.com/company/sqlchangeguard

Hassas Veri Maskeleme: Doğrulamalı Tespit ve Sunucu Bazlı Rejim

Maskeleme iki bağımsız mekanizma ile çalışır ve ikisi birbirinin kör noktasını kapatır.

Birincisi sınıflandırma kataloğudur. Kolonun adına bakar, verinin içine hiç bakmaz. Örnek: adında TCKN geçen her kolon maskelenir. Bu mekanizma sayısal kolonları da kapsar; kimlik numarasını sayı olarak tutan sistemlerde tek koruma budur. Her kurala denetçiye gösterilen bir etiket atanır: KVKK-Kimlik, KVKK-İletişim, KVKK-Sağlık, KVKK-Eğitim, PCI-Kart gibi. Kurulumla birlikte finans, perakende, sağlık ve eğitim alanlarını kapsayan hazır bir başlangıç seti gelir.

İkincisi veri desenleridir. Kolonun adına bakmaz, hücrelerin içeriğine bakar. Önemli olan tarafı şudur: bir desene doğrulama algoritması bağlanabilir. Kimlik numarası için checksum, kart numarası için

Luhn, IBAN için mod-97. Böylece 11 haneli bir sipariş numarası boşa maskelenmez, gerçek kimlik numarası ise maskelenir. Bu, gereksiz maskesiz veri taleplerini ortadan kaldırır.

Kolon önizlemesi. Talep kaydedilirken sistem hedef sunucuya bağlanır ve sorgunun hangi kolonları döndüreceğini sorar. Sorgu çalıştırılmaz, tek satır veri okunmaz. Böylece talep sahibi ve onaylayan, teslimden önce hangi kolonun maskeleneceğini görür. Sorguda takma ad kullanılmış olsa bile kaynak kolon tespit edilir ve maskeleme atlanamaz.

Sunucu bazlı rejim. Maskeleme verinin özelliği olduğu için ayar sunucu tanımındadır. İki rejim vardır: tam maskeleme ve yalnız içerik. Yalnız içerik rejimi sentetik veri barındıran ortamlar içindir; kolon adına göre maskeleme yapmaz, ama o sunucuya gerçek veri yüklenirse doğrulamalı desenler devreye girer ve maskeleme kendiliğinden geri gelir. Bu rejim yazılı gerekçe olmadan seçilemez ve değişikliği denetim izine ayrı bir olay olarak yazılır. Aynı talep birden fazla sunucuya gidiyorsa kararlar sunucu bazında verilir: üretim sunucusundan gelen sonuç maskelenirken sentetik veri barındıran sunucudan gelen sonuç açık kalabilir.

Kanıt. Her teslimde hangi kolonun neden maskelendiği kolon bazında kaydedilir: sınıflandırma kataloğu, veri deseni, onaylı maskesiz istek ya da süre bütçesi aşımı. Kayıt sunucu bazındadır ve teslim anındaki rejim ile muafiyet gerekçesi kayda dondurulur; sunucu tanımı sonradan değiştirilse bile kanıt bozulmaz. Maskeleme kurumsal bir anahtarla tamamen kapatılabilir, ancak kapatıldığında da her teslim kayda geçer ve denetim dosyasında kırmızı hükümle işaretlenir.

Öğrenme döngüsü. Desenle yakalanan ama katalogda olmayan kolonlar aday olarak birikir; veritabanı yöneticisi bunları kalıcı kural haline getirir ya da yok sayar. Aday listesinde hiçbir veri değeri tutulmaz, yalnızca kolon, tablo ve desen adları vardır. Böylece sınıflandırma, kimse üretim verisine bakmadan zamanla keskinleşir.

Kanıt: O Gün Hangi Kurallar Geçerliydi

Kurallar zamanla değişir. Bir ayar bugün sıkı, altı ay önce gevşek olabilir. Denetimde sorulan soru şudur: bu talep işlendiği gün hangi kurallara tabiydi? Sistem bu soruyu bugünkü ayarlara bakarak değil, o gün dondurulmuş kayda bakarak cevaplar.

Kural seti anlık görüntüsü. Her talep kaydedildiğinde o anda geçerli olan kural seti tek bir denetim kaydına yazılır: hedef sunucuların künyesi ve kontrol bayrakları (rollback zorunluluğu, otomatik çalıştırma, maskeleme rejimi), onay ve görevler ayrılığı kuralları, hassas veri maskeleme ayarları, sonuç dosyası erişim kuralları, o gün bloklayıcı olan SQL standartlarının listesi ve açık olan lisans modülleri. Kural sonradan değişse bile bu kayıt değişmez.

Teslim anındaki ayarlar. Bir talep bir tarihte kaydedilip başka bir tarihte çalıştırılabilir. Maskeleme çalıştırma anında yapıldığı için, o andaki eşik, örneklem boyutu, örnekleme biçimi ve süre bütçesi de teslim kaydına ayrıca dondurulur. Böylece bir teslimde neden hiçbir kolonun maskelenmediği sorusu kesin olarak cevaplanır.

Kontrol değişiklikleri ayrı olay olarak kaydedilir. Bir ayarın değişmesi ile bir kontrolün gevşetilmesi aynı şey değildir. Maskeleme rejiminin gevşetilmesi, rollback zorunluluğunun kaldırılması, otomatik çalıştırmanın açılması, bir tespit deseninin kapatılması, bir sınıflandırma kuralının silinmesi, alıcı havuzuna adres eklenmesi, bakım görevinin durdurulması ve lisans modüllerinin değişmesi kendi olay adlarıyla yazılır. Gevşetme ve sıkılaştırma farklı adlar alır. Denetim ekranında olay adına göre

arama yapılabilir; böylece hangi kontrolün ne zaman ve kim tarafından gevşetildiği tek listede görülür.

İki bağımsız kayıt katmanı. Uygulama denetim izi iş anlamı taşıyan olayları tutar ve ekranda görünür. Veritabanı seviyesindeki ikinci katman ise uygulamadan bağımsız çalışır: yönetim aracıyla doğrudan veritabanına yapılan bir değişiklik de yakalanır. İki katman birbirinin yerine geçmez, biri diğerini tamamlar.

Denetim dosyasında görünür. Talep bazlı denetim dosyası, o talebin işlendiği gün geçerli olan kural setini ayrı bir bölümde okunur biçimde listeler. Denetçi tek bir belgeyle hem ne olduğunu hem hangi kurallara göre olduğunu görür.

Sürüm paketi kapsamı. Sürüm paketleri yalnızca değişiklik taleplerini taşır. Sorgu sonucu talepleri paket içinde yer alamaz; sonuç dosyası ancak hassas veri maskelemesi uygulayan ve denetim kaydı üreten kendi akışında teslim edilir. Bu kural yalnızca ekranda değil, arayüzden bağımsız olarak sunucu tarafında da doğrulanır.

Ayar Değişikliklerinde Dört Göz İlkesi

Bir kontrolü zayıflatan ayar değişikliği tek kişinin kararıyla yapılmamalıdır. Sistem, ayar ekranlarındaki değişiklikleri onaya bağlayabilir: değişiklik hemen uygulanmaz, önce onay bekler ve onaylanana kadar eski değer geçerli kalır.

Nasıl çalışır. Onay bekleyen değişiklik ayrı bir kayıtta durur; gerçek ayar tablosuna onay verilene kadar dokunulmaz. Bu sayede sistemin geri kalanı eski değeri okumaya devam eder ve yarım uygulanmış bir ayar durumu hiç oluşmaz. Onay verildiğinde değişiklik, kullanıcı kaydetmiş gibi aynı yoldan uygulanır; lisans limiti, doğrulama ve eşzamanlılık kontrolleri o anda yeniden çalışır.

Onay yetkisi. Bir ayar değişikliğini, o ekranın yetkisine sahip başka bir kullanıcı onaylar. Ayrı bir onaylayan rolü tanımlanmaz; yetkiler zaten rol tanımında vardır. Kimse kendi talep ettiği değişikliği onaylayamaz veya reddedemez; bu kural isteğe bağlı değildir. Onay listesi kullanıcının yetkisine göre filtrelenir: kişi yalnızca yetkili olduğu ekranların onaylarını görür.

Kapsam. Özellik kurumsal bir parametre ile yönetilir ve üç seçeneği vardır: kapalı, yalnızca kontrol ayarları, tüm ayarlar. Varsayılan kapalıdır. Yalnızca kontrol ayarları seçeneğinde sunucu tanımları, kullanıcı kayıtları, rol yetki matrisi, onay politikaları, SQL standartları, kritik obje listesi, hassas kolon kataloğu, hassas veri desenleri, onaylı e-posta adresleri, bakım işleri ve maskeleme, onay, görevler ayrılığı gibi kontrol parametreleri onaya düşer; işletme verisi niteliğindeki ayarlar akışı yavaşlatmaz. Özelliğin kendisi de bir kontroldür: açmak anında uygulanır, kapatmak onay ister. Parola sıfırlama ve kullanıcı kilidi açma bilinçli olarak kapsam dışıdır; bunlar yardım masası işlemleridir ve denetim kaydına yazılır.

Ekranda görünüm. Onay bekleyen değişikliği olan kayıt, ilgili ayar ekranında işaretlenir ve yeniden düzenlenemez; ekranın üstünde kaç değişikliğin beklediğini gösteren bir uyarı bulunur. Kaydetme sonrası kullanıcıya değişikliğin uygulanmadığı, onaya gönderildiği açıkça bildirilir. Ayrı bir onay ekranında eski ve yeni değer yan yana gösterilir, değişen alanlar vurgulanır.

Kayıt. Talebin açılması, onaylanması, reddedilmesi ve onaylandığı halde uygulanamaması ayrı denetim olayları olarak yazılır. Onay anında değişikliğin kendi denetim kaydı da oluşur, böylece kimin onayladığı ile değerin ne olduğu ayrı ayrı izlenebilir. Reddetme gerekçe ister.

Kurulum notu. Kimse kendi talebini onaylayamadığı için, kapsamdaki her ekran yetkisine sahip en az iki kullanıcı bulunmalıdır. Uygulamada bu tek şarta iner: en az iki sistem yöneticisi kullanıcı tanımlı olmalıdır.

Denetçi Rolü

Denetim ekiplerinin ihtiyacı çoğu zaman tek bir şeydir: görmek. Kim ne yaptı, hangi onaydan geçti, hangi veri kime gitti. Bunun için sisteme yönetici yetkisi vermek gerekmez. SQL Change Guard bu ihtiyacı ayrı bir rolle karşılar.

Denetçi ne yapar. Tüm talepleri görür, denetim kayıtlarını inceler, raporları ve kontrol panelini kullanır, bir talebin kanıt dosyasını üretip indirir, denetim izinin bütünlüğünü doğrular ve bildirim günlüklerini görür.

Denetçi ne yapamaz. Talep açamaz, onaylayamaz, çalıştıramaz, sandbox kullanamaz, hiçbir ayar ekranını yönetemez ve sorgu sonucu dosyasını indiremez.

Son madde bilinçli bir tasarımdır. Kanıt paketine sorgu sonucu verisi girmez; denetçi kanıta ulaşır, üretim verisine ulaşmaz. Denetim yapabilmek için kişisel veri görmek gerekmediği için bu sınır denetimi zayıflatmaz, aksine kurumun veri yüzeyini daraltır.

Kanıt ekleme ve silme yoktur. Kanıt dosyası talebin kendisinden üretilir; düzenlenebilen bir kanıt deposu bulunmaz. Denetçinin kanıt ekleyip silebilmesi, kanıtın kanıt olma değerini ortadan kaldırırdı.

Görevler ayrılığı. Denetçi onay adımlarında onaylayan olarak seçilemez ve denetçi rolüne onaylama ya da çalıştırma yetkisi verilemez. Denetleyen kişinin onaylayan konumuna geçmesi kontrolün kendisini ortadan kaldırır, bu yüzden kural isteğe bağlı değildir.

Kurulum notu. Ürün tek yönetici hesabıyla gelir; hazır bir denetçi hesabı gönderilmez. Kurum kendi denetçisini kendi tanımlar, böylece parolası bilinen bir denetim hesabı hiçbir kurulumda bulunmaz.