

SQL Change Guard

Sıkça Sorulan Sorular

Kurumsal SSS

SQL Server | PostgreSQL | Oracle

Genel

SQL Change Guard tam olarak ne yapar?

Veritabanı deęişikliklerini (Database Change Governance), production veri erişimini (Production Query Governance) ve uyumluluk kanıtını (Compliance and Audit) tek platformda yönetir. Deęişiklikleri deployment öncesi 88 SQL standardıyla analiz eder, risk bandına yerleştirir, onay akışına alır, çalıştırır ve denetim izi tutar. Ürün kendi üzerinden yapılan işlemleri yönetir; canlı veritabanı trafiğini dinlemez ve ürün dışında yapılan işlemleri engellemez.

Migration araçlarından (Flyway, Liquibase gibi) farkı nedir?

Migration tabanlı yaklaşımın ötesinde; production veri erişimi yönetiřimi, hassas veri maskeleme, policy engine, risk analizi, geri alma betięi üretimi ve imzalı denetim kanıtı sunar. Yani sadece schema deployment deęil, uçtan uca veritabanı operasyon yönetiřimidir.

Veritabanı ve Kurulum

Hangi veritabanlarını destekliyor?

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

İnternet bağlantısı gerekiyor mu?

Hayır. Ürün kurum içinde (on-premise) çalışır ve temel işleyiři için internet gerektirmez. İsteęe baęlı zaman damgası açılırsa dışarıya yalnız SHA-256 özeti gider; bu özellik varsayılan olarak kapalıdır. Kurulum adımları 06 Kurulum Ön Hazırlık ve 07 Kurulum ve İşletim belgelerindedir.

Güvenlik ve Uyumluluk

WHERE koşulsuz DELETE/UPDATE gibi hataları nasıl engelliyor?

Script kaydedilirken parser devreye girer. WHERE koşulu eksik DELETE ya da UPDATE, High risk bandında bir bulgudur ve kurulumda kaydı engelleyen kural olarak gelir: talep bu haliyle kaydedilemez, dolayısıyla çalıştırılamaz.

KVKK ve bankacılık denetimine uygun mu?

Ürün tek başına mevzuata uyum ya da sertifika sağlamaz. KVKK, ISO 27001, COBIT ve ITIL kontrol beklentilerine katkı sağlayan kayıtlar üretir: hassas veri maskeleme, append-only defter tablosundaki denetim kayıtları, onay kanıtları ve 34 hazır rapor. Hangi kaydın hangi beklentiye katkı sağladığı 11 Uyumluluk ve KVKK belgesindedir.

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.

Kurum hesabımızla (Entra ID, AD FS) giriş yapılabilir mi?

Evet. Ürün OIDC ve SAML 2.0 ile kurumun kimlik sağlayıcısına bağlanır (örneğin Microsoft Entra ID, AD FS, Keycloak, Okta). Kullanıcı şifresini ve çok faktörlü doğrulamasını kurumun kendi giriş sayfasında girer; şifre ürüne gelmez. Rol, kurumdaki gruptan tanımladığınız eşlemeye göre verilir ve gruptan çıkarılan kişinin yetkisi bir sonraki girişinde düşer. SystemManager rolü eşlemeyle verilmez. Kimlik sistemine ulaşamazsa yalnız belirlediğiniz acil durum hesapları şifreyle girer ve her girişleri denetim izine yazılır. LDAP ile yerel hesaplar aynı anda kullanılmaya devam edebilir.

Active Directory'miz var ama SSO kurmak istemiyoruz. Kullanıcılar kurum şifresiyle girebilir mi?

Evet. Ürün kurum dizinine (Active Directory ya da OpenLDAP gibi bir LDAP dizini) şifreli bağlantıyla bağlanır. Kişi giriş ekranına kurum kullanıcı adını ve şifresini yazar; ürün şifreyi saklamaz, dizine sorar. Rol yönetici tarafından verilebilir ya da dizindeki gruptan tanımladığınız eşlemeye göre gelebilir. Düzenli izin eşitlemesi, dizinde kapatılan ya da silinen kişinin ürünündeki erişimini kendiliğinden kapatır ve açık oturumunu bitirir; toplu bir hata herkesi dışarıda bırakmasın diye güvenlik sınırı vardır. İki adımlı doğrulama izin hesaplarında da kullanılabilir.

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 içerikle çalıştırılacak içeriğin ürün tarafından karşılaştırıldığının kaydı; hedefte gerçekleşen işlemi tek başına kanıtlamaz), risk bandı, çalıştırma kaydı ve tüm denetim izi tek bir ZIP paketinde (PDF ve JSON) toplanır. Paketteki dosyaların SHA-256 özetleri bir manifestoda listelenir ve manifesto imzalanır; paketin değişmediği iki yoldan doğrulanabilir: sistem üzerinden ya da sisteme hiç girmeden. İkinci yolda imza, paketteki açık anahtarla doğrulanır; denetçi bunu kendi bilgisayarında yapar ve kuruma ait hiçbir gizli değer paylaşılmaz. Açık anahtarın parmak izi kurumdan ayrıca teyit edilmelidir, çünkü paketin içindeki doğrulama betiği tek başına kanıt değildir. Kanıt imzalaması açılmamışsa paket imzasız olur ve doğrulama bunu UNSIGNED olarak bildirir. İndirme ayrı bir yetki gerektirir ve işlemin kendisi de audit altına alınır.

Değişiklik ve Rollback

Rollback nasıl çalışır?

Değişiklikler için geri alma betiği üretilebilir: nesne değişikliklerinde (DDL) betik nesnenin önceki tanımından üretilir; veri değişikliklerinde (INSERT, UPDATE, DELETE, MERGE) betik üretilmez, elle müdahale notu yazılır ve plan eksik sayılır. Oracle'da DDL, DCL ve TRUNCATE örtülü COMMIT yaptığından bu tür Oracle değişikliklerinde geri alma planı zorunludur ve onay anında otomatik hazırlanabilir. Kaynak talebin betikleri düzenlenirse eski geri alma planı kullanıcı onayıyla geçersiz kılınır ve yeniden hazırlanması gerekir.

Sandbox ne işe yarar?

Değişikliği hedef veritabanında transaction içinde çalıştırıp geri alarak (BEGIN-ROLLBACK) ön doğrulama yapar; böylece söz dizimi ve nesne hataları canlı çalıştırmadan önce görülür. Üretim koşullarının tam benzetimi değildir. Oracle'da DDL, DCL ve TRUNCATE örtük COMMIT yaptığı için bu ifadeleri içeren talepler sandbox'ta çalıştırılmaz; varsayılan ayarda üretim sunucusunda sandbox kapalıdır.

Ticari

Fiyatlandırma nasıl?

Fiyat iki kalemden oluşur: sabit platform bedeli ve üretim veritabanı sunucusu bedeli. Sunucu bedeli kademelidir, her yeni sunucu bir öncekinden daha ucuzdur. Kullanıcı sayısı sınırsızdır; bütün modüller ve üç veritabanı motoru platform bedeline dahildir, modüller ayrı satılmaz; test, geliştirme ve hazırlık ortamları ücretsizdir. Ayrıntı 13 Lisans Modeli belgesindedir. Ücretsiz demo talep ederek teklif alabilirsiniz.

Nasıl başlarım?

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

İletişim

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

Hassas Veri Maskeleye: Doğrulamalı Tespit ve Sunucu Bazlı Rejim

Maskeleye 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-Identity, KVKK-Contact, KVKK-Health, KVKK-Education, PCI-Card 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 numarasının boşa maskelenmesi büyük ölçüde önlenir, gerçek kimlik numarası ise maskelenir. Bu, gereksiz maskesiz veri taleplerini azaltır.

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; takma ad vermek kolon adına bağlı maskeleye atlatmaz.

Sunucu bazlı rejim. Maskeleye verinin özelliği olduğu için ayar sunucu tanımındadır. İki rejim vardır: tam maskeleye ve yalnız içerik. Yalnız içerik rejimi sentetik veri barındıran ortamlar içindir; kolon adına göre maskeleye yapmaz, ama o sunucuya gerçek veri yüklenirse doğrulamalı desenler devreye girer ve desenle tanınan alanlarda maskeleye kendiliğinden geri gelir; deseni olmayan alanlar (ad, adres gibi) bu rejimde açık gider. 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. Maskeleye 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, maskeleye rejimi), onay ve görevler ayrılığı kuralları, hassas veri maskeleye 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. Maskeleye 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 o günkü ayarlarla cevaplanabilir.

Kontrol değişiklikleri ayrı olay olarak kaydedilir. Bir ayarın değişmesi ile bir kontrolün gevşetilmesi aynı şey değildir. Maskeleye 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 çalışan tetikleyicilerle, yönetim aracıyla doğrudan veritabanına yapılan bir değişikliğin de izini kaydeder. Bu katman yardımcı kayıttır: tetikleyici kapatılabilir ve kayıtlar silinebilir; asıl güvence defter tablosu ve dış defter özetiyle karşılaştırmadır. 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 maskeleye 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 kayıta 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. Aynı 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 değer 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 varsayılan ayarda sorgu sonucu dosyasını indiremez (indirme için gereken asgari rol kurum parametresidir, varsayılanı ChangeManager).

Son madde bilinçli bir tasarımıdır. 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.

Kural Motoru Neyi Yakalar, Neyi Yakalamaz

Kural motoru betiği gerçek dilbilgisiyle ayrıştırır ve cümle yapısı üzerinden çalışır. Bu yüzden filtresiz bir UPDATE, kritik nesne üzerinde DROP veya adlandırma kuralı gibi betiğin kendisinden okunabilen durumları yakalar. Oracle'da ağaç ayrıştırması başarısız olursa daha sınırlı düzenli ifade analizine düşülür.

Bir sorgunun indeksli kolon kullanıp kullanmadığı ise betikten okunamaz; hedef veritabanının kataloğuna bakmayı gerektirir. Bu kontrol bugün kural motorunun kapsamında değildir ve veritabanı izleme araçlarının alanına girer.

Bu ayrım bilinçlidir. Kural motoru betiğe bakarak kesin cevap verebildiği şeyleri kontrol eder; kesin cevap veremeyeceği bir alanda uyarı üretmek, güvenilirmez uyarılarla ekranı doldurur ve zamanla bütün uyarıların göz ardı edilmesine yol açar.

Bir Adım Atlanırsa Nasıl Görürüm

Talep listesinde ve talep detayında, yapılması gereken ama yapılmamış adımlar kırmızı bir rozetle görünür. Rozetin üzerine gelindiğinde eksikler madde madde listelenir. Aranarak bulunması gereken bir bilgi değil, listeye bakıldığı anda görünen bir bilgidir.

Rozet şu durumları gösterir: sunucu geri alma planı zorunlu kılıyor ama plan yok; geri alma planı var ama betiği eksik; otomatik geri alma planı üretilmedi; izole deneme zorunlu ama hiç yapılmadı; son deneme başarısız; deneme başarılıydı ama betik sonradan değişti.

Rozet yalnız canlı talepler için çıkar. Kapanmış talepler (çalıştırılmış, reddedilmiş, elle uygulanmış, iptal edilmiş) işaretlenmez: o talebin kapandığı gün yürürlükte olan kural bugünkünden farklı olabilirdi ve geriye dönük suçlama yanıltıcı olur.

Acil Değişiklikler Sonradan Gözden Geçiriliyor mu

Evet. Acil yol onayı atlamaz, kısaltır. Buna ek olarak uygulanmış her acil değişiklik için olay sonrası bir gözden geçirme kaydı tutulur. Onay yetkisi olan bir kullanıcı iki soruyu cevaplar (değişiklik gerçekten acil miydi, kalıcı çözüm için talep açıldı mı) ve zorunlu bir not yazar.

Gözden geçirme bir onay değildir ve yaptırım üretmez. Amaç ceza değil, örüntüyü görünür kılmaktır: aynı ekipten her ay çıkan acil değişiklik, sürecin değil planlamanın sorununu gösterir.

Kişi kendi açtığı acil talebi gözden geçiremez. Kontrol panelinde gözden geçirilmemiş acil değişiklik sayacı bulunur ve Acil Değişiklik Gözden Geçirme raporunda bekleyenler kaç gündür beklediğiyle listelenir.

Denetim Kayıtlarını Veritabanı Yöneticisi Değiştirebilir mi

Yerinde değiştiremez ve silemez. Denetim kayıtları SQL Server 2022 ile gelen append-only defter (ledger) tablosunda tutulur. Veritabanı motoru kayıt değiştirmeyi ve silmeyi sysadmin dahil herkes için reddeder. Tablonun düşürülüp yeniden kurulması engellenmez ama motorun kendi geçmişinde iz bırakır ve ürün bunu yakalar.

Veritabanı dosyasını doğrudan değiştirmek ya da eski bir yedeğe dönmek ise dış tanıkla fark edilir: varsayılan olarak saatte bir API veritabanının defter özetini (imza açıksa imzalı) bir dosya olarak yapılandırılan klasöre yazar. Bu klasörün değiştirilemez bir depoda (WORM gibi) olması kurumun sağlamasıdır. Denetçi bu özetlerle veritabanının bir kopyasında doğrulama yapar; kayıtlar özetle uyuşmazsa doğrulama başarısız olur.

Ürün ayrıca yazma yolunu da denetler: kanıt tablosuna tetikleyici eklenmesi, yazma yordamının değiştirilmesi ya da kanıt şemasına nesne eklenmesi fark edilir ve değişiklik işlemleri sınır düzelene kadar durur. Ürün bunun için SQL Server 2022 ya da sonrasını ister.

Denetçi Bir Dönemin Bütün Taleplerini Gördüğünü Nasıl Bilir

Dönem paketiyle. Denetim Kaydı ekranındaki Dönem Paketi düğmesi seçilen dönem için imzalı bir paket üretir. Paket dönemin bütün taleplerini iki ayrı kaynaktan, talep tablosundan ve denetim kaydından toplar ve satır satır uzlaştırır; uyuşmayan her satır açıkça işaretlenir. Pakette ayrıca dönemdeki defter özetleri, aralarındaki boşluklar, kanıt yazma sınırı olayları, veritabanı geri yüklemeleri ve dışa aktarma günlüğü bulunur. Paketin ve özetlerin nasıl doğrulanacağı Denetçi Kiti belgesindedir.