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 tamamen kurum içi (on-premise) çalışır.

- 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 (yönetim verisi); değiştirilemeyen audit için ayrı Immutable veritabanı
- 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 yönetişim 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 atomiklik güvencesi

3. Güvenlik

- Kimlik doğrulama: JWT tabanlı; LDAP / Active Directory entegrasyonu
- 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
- Değiştirilemeyen (immutable) audit: hash zinciri ile korunan kayıtlar
- Görevler ayrılığı (separation of duties)

4. Entegrasyon

- LDAP / Active Directory (kullanıcı ve kimlik)
- SMTP (bildirim ve onay e-postaları)

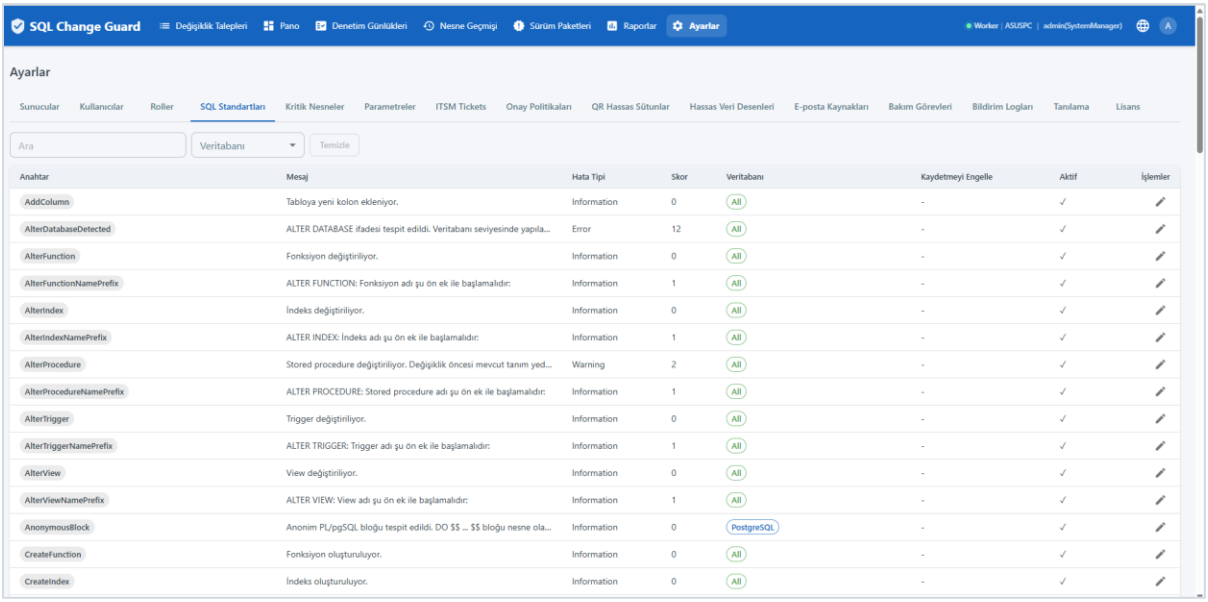
- REST API (dış sistemlerden tüketim)
- ITSM ticket alanı (değişiklik talebine ticket bağlama; format regex ile doğrulanır)

5. Konfigürasyon ve Kurallar

- Konfigürasyon appsettings ve Parameters tablosu üzerinden yönetilir; hardcoded bilgi yoktur
- 84+ 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

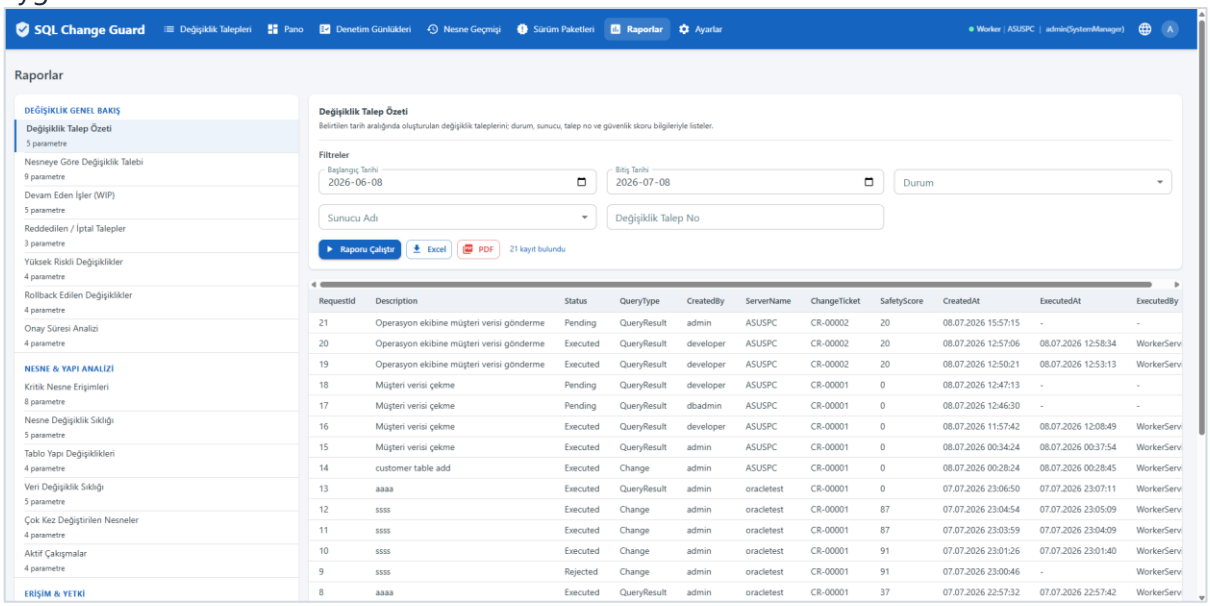


SQL Standart Kuralları - aktif/pasif ve veritabanı tipine göre filtre

6. Denetim ve Raporlama

30 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.



Rol kısıtlı bir raporun okunması da denetim izine yazılır: kim, hangi raporu, hangi filtrelerle ve kaç satır görmüş. Kayıtta 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 kaydıdır.

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.

Raporlar - 30 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
- 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
- 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 2016 veya üzeri**
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

Sistem sıfırdan bir kurum ortamında en fazla 30 dakikada ayağa kaldırılabilecek şekilde tasarlanmıştır. Şema, numaralı ve checksum korumalı migration script'leri ile otomatik uygulanır. Ortam bağımlılıkları minimumdur.

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

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 dahi parolalar geri döndürülemez.

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 şifrelenerek saklanır. Böylece geri döndürülebilir tüm sırlar tek, doğrulanabilir bir kriptografik yöntem kullanır; bu da hem güvenliği hem de sistemin anlaşılırlığını artırır.

Denetim izi bütünlüğü: HMAC-SHA256

Denetim kayıtları (audit trail) bir hash zinciriyle korunur ve güncel sürüm HMAC-SHA256 kullanır. Anahtar veritabanında tutulmaz, yalnızca uygulama yapılandırmasından gelir; böylece yalnızca veritabanına erişimi olan bir kişi bile denetim zincirini yeniden üretip geçmişi sessizce değiştiremez.

Anahtar yönetimi

Tüm şifreleme anahtarları 256-bit uzunluğundadır (32 bayt, base64) ve uygulama yapılandırmasının Security bölümünde toplanır: Security:ServerPasswordKey (sunucu parolaları), Security:QrZipPasswordKey (QR zip parolaları) ve Audit:HmacKey (denetim izi). Anahtarlar üretim ortamında user-secrets veya ortam değişkeni (environment variable) üzerinden 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 HMAC-SHA256 ile korunur.