

SQL Change Guard Kurulum ve İlk Kullanım Kılavuzu

Bu kılavuz SQL Change Guard'ın boş bir ortamda kurulmasından ilk deęişiklik talebinin alıřtırılıp denetim dosyasının doęrulanmasına kadar btn adımları sırayla anlatır. Her adımın ayrıntısı ve entegrasyonlar (kurum dizini, kurum hesabıyla giriş, ITSM, SIEM) Kurulum ve İşletim Kılavuzu'ndadır; hazırlık listesi Kurulum Ön Hazırlık Listesi'ndedir.

1. Ön kořullar ve desteklenen ortamlar

Bileřen	Gereksinim
Uygulama sunucusu	Windows Server (4 çekirdek, 8 GB bellek önerilir), IIS, ASP.NET Core Hosting Bundle (.NET 10), IIS URL Rewrite modl. API, Worker ve web arayz aynı sunucuda alıřabilir
Uygulama veritabanı	SQL Server 2022 ya da sonrası (Express dahil). Denetim kayıtları SQL Server'ın yalnız eklenebilir defter (ledger) tablosunda tutulduęu iin daha eski srm desteklenmez
Ynetilecek veritabanları	SQL Server, PostgreSQL, Oracle (lisansla aık olan trler). Desteklenen en dřk hedef srmleri kurulum ncesinde rn ekibiyle teyit edilir
Tarayıcı	Gncel Edge, Chrome ya da Firefox
Aę	Tarayıcıdan web arayzne ve API'ye 443; API ve Worker'dan uygulama veritabanına 1433; API ve Worker'dan ynetilecek veritabanlarına kendi portları
Defter zeti deposu	API uygulama havuzu hesabının yeni dosya yazabildięi ve okuyabildięi ama deęiřtiremedięi/silemedięi bir klasr (WORM paylařım, nesne kilitli depo). zeti Worker'ın bařlattıęı turda API yazar. Veritabanı yneticisi buraya yazamamalıdır

Kurulumdan nce hazır olması gerekenler: sunucular, DNS adları ve HTTPS sertifikaları, veritabanı hesapları, lisans dosyası, kanıt imzalama anahtarı (RSA, Kurulum ve İşletim Kılavuzu Blm 2.3).

2. SQL Server gereksinimleri ve izinler

2.1 Uygulama veritabanı

İki kurulum yolu vardır. Seçim API'deki Database:AutoMigrate ayarıyla yapılır.

Yol	Kim kurar	Hesabın izni
A (varsayılan, AutoMigrate = true)	Ürün, ilk açılışta	Kurulum sırasında veritabanında db_owner. Veritabanı yoksa ürün oluşturur; bunun için dbcreator da gerekir. Kurulumdan sonra izin Yol B'deki izinlere indirilebilir
B (AutoMigrate = false)	DBA, betiklerle	Aşağıdaki en az yetki

Yol B'de uygulama hesabına verilecek izinler (sysadmin ve db_owner verilmez):

```
USE [SQLChangeGuard];  
  
CREATE USER [uygulama_hesabi] FOR LOGIN [uygulama_hesabi];  
  
ALTER ROLE db_datareader ADD MEMBER [uygulama_hesabi];  
  
ALTER ROLE db_datawriter ADD MEMBER [uygulama_hesabi];  
  
GRANT EXECUTE ON SCHEMA::dbo TO [uygulama_hesabi];  
  
ALTER ROLE evidence_api_writer ADD MEMBER [uygulama_hesabi];  
  
ALTER ROLE evidence_worker_writer ADD MEMBER [uygulama_hesabi];  
  
GRANT VIEW LEDGER CONTENT TO [uygulama_hesabi];  
  
GRANT VIEW DEFINITION ON SCHEMA::evidence TO [uygulama_hesabi];  
  
DENY UPDATE, DELETE ON dbo.TableWriteLogs TO [uygulama_hesabi];
```

API ve Worker aynı hesabı kullanabilir; bu varsayılandır. İstenirse Worker'a ayrı bir hesap verilir: API hesabı yalnız evidence_api_writer, Worker hesabı yalnız evidence_worker_writer rolüne eklenir, diğer izinler ikisine de verilir. Bu durumda veritabanı, Worker hesabının onay, ret, uzlaştırma kararı gibi kullanıcı kararlarını ve giriş olaylarını yazmasını reddeder.

2.2 Yönetilecek veritabanları

Her hedef sunucu için ürünün kullanacağı bir hesap açılır. Bu hesap onaylanan betiklerdeki işlemleri yapabilecek yetkide olmalıdır; ürün ayrıca geri alma betiği üretmek ve nesne karşılaştırmak için nesne tanımlarını okur (SQL Server'da VIEW DEFINITION). Hesap bilgisi ürünün Sunucular ekranında girilir ve parola şifrelenerek saklanır.

3. Veritabanının oluşturulması ve şema kurulumu

3.1 Yol A: ürün kurar

1. Boş veritabanını oluşturun (ya da hesaba dbcreator verin, ürün oluşturun).
2. API'yi ilk kez başlattığınızda (Bölüm 4) günde her betik için [Schema] Applying ve [Schema] Completed satırları görünür. Ürün defter doğrulaması için gereken anlık görüntü yalıtımını da açar: ALLOW_SNAPSHOT_ISOLATION was turned on.

3.2 Yol B: DBA kurar

1. Betikler API klasöründe DbScripts\sqlserver altındadır: 001_Tables.sql, 002_SeedData.sql, 003_StoredProcedures.sql, 004_TableWriteLogs.sql. Sırayla uygulanır:

```
sqlcmd -S SQLSUNUCU -d SQLChangeGuard -I -f 65001 -b -i 001_Tables.sql
```

```
sqlcmd -S SQLSUNUCU -d SQLChangeGuard -I -f 65001 -b -i 002_SeedData.sql
```

```
sqlcmd -S SQLSUNUCU -d SQLChangeGuard -I -f 65001 -b -i 003_StoredProcedures.sql
```

```
sqlcmd -S SQLSUNUCU -d SQLChangeGuard -I -f 65001 -b -i 004_TableWriteLogs.sql
```

2. API klasöründeki DbScripts\DbSchemaVersions.ps1 çalıştırılır; ürettiği SchemaVersions_Register.sql incelenip uygulanır.

3. Veritabanına başka bağlantı yokken bir kez:

```
ALTER DATABASE [SQLChangeGuard] SET READ_COMMITTED_SNAPSHOT ON WITH ROLLBACK IMMEDIATE;
```

```
ALTER DATABASE [SQLChangeGuard] SET ALLOW_SNAPSHOT_ISOLATION ON;
```

4. Bölüm 2.1'deki izinler verilir.

Kontrol: kanıt tablosunun defter olduğunu görün.

```
SELECT SCHEMA_NAME(schema_id) AS sema, name, ledger_type_desc FROM sys.tables WHERE  
ledger_type <> 0;
```

Beklenen: evidence, AuditLogs, APPEND_ONLY_LEDGER_TABLE.

4. API kurulumu

1. API klasörünü sunucuya kopyalayın (ör. D:\SQLChangeGuard\api).
2. IIS'te bir uygulama havuzu açın (.NET CLR sürümü: No Managed Code) ve kök dizini API klasörü olan bir site tanımlayın. HTTPS bağlamasını ve sertifikayı ekleyin.
3. Uygulama havuzu hesabına logs klasörüne yazma, sorgu sonucu dosya klasörünü okuma (indirme için), defter özeti deposunda yeni dosya yazma ve okuma ve kanıt imza sertifikasının özel anahtarını okuma yetkisi verin.
4. appsettings.json içinde en az şunları yazın: AllowedOrigins (web arayüzünün adresi), Database:AutoMigrate, Display:TimeZone, QueryResult:OutputPath, Evidence:Signing:Enabled = true, Evidence:Signing:InstallationId, imza anahtarının açık anahtarı ya da sertifika parmak izi, Evidence:Ledger:DigestOutputPath. İmzanın kod varsayılanı kapalıdır; imza kapalıyken kanıt dosyası imzasız üretilir ve Production olarak tanımlı sunucularda talep çalıştırılmaz.
5. Sırları ortam değişkeni olarak tanımlayın (yönetici komut isteminde setx /M). Zorunlu olanlar:

Ortam değişkeni	Ne işe yarar
ConnectionStrings__Default	Uygulama veritabanı bağlantı dizesi
Jwt__SigningKey	Oturum jetonlarının imzası (en az 32 karakter)
Security__ServerPasswordKey	Sunucu parolalarının şifrlenmesi (base64, 32 bayt)
Security__QrZipPasswordKey	Sorgu sonucu paketi parolalarının şifrlenmesi (base64, 32 bayt)
Workers__ApiKey	Worker'ın API'ye kendini tanıtmaması (Worker'daki WorkerApi__Key ile aynı değer)

6. Uygulama havuzunu başlatın. Günlük dosyası: logs\scg-YYYYMMDD.log. Hata satırı olmamalıdır.

5. Worker kurulumu (Windows servisi)

1. Worker klasörünü sunucuya kopyalayın (ör. D:\SQLChangeGuard\worker).

2. Worker'daki appsettings.json içinde WorkerApi:BaseUrl ayarına API adresini yazın. WorkerApi__Key ortam değişkenini API'deki Workers__ApiKey ile aynı değerle tanımlayın.

3. Worker ayrı bir veritabanı hesabıyla bağlanacaksa Worker sunucusunda ConnectionStrings__Worker ortam değişkenini tanımlayın. Tanımlanmazsa Worker, API ile aynı hesabı kullanır ve bağlantı bilgisini açılışta API'den alır.

4. Servisi kaydedin ve başlatın (yönetici komut istemi):

```
sc.exe create "ChangeGuardWorker" binPath= "D:\SQLChangeGuard\worker\SCG.Workers.exe" start=
auto DisplayName= "SQL Change Guard Worker"
```

```
sc.exe start "ChangeGuardWorker"
```

5. Servis hesabına logs klasörüne ve sorgu sonucu klasörüne yazma yetkisi verin. Defter özeti deposunda Worker hesabına izin gerekmez; özeti API yazar.

6. Worker günlüğünde şu satırları görün: Worker configuration loaded from API ve Worker database connection source. Bir özet aralığı sonra (varsayılan 60 dakika) API günlüğünde [Ledger] Digest published satırı görünür ve depoda ledger-digest-*.json dosyası (imza açıksa yanında .sig) oluşur.

6. Web arayüzü (istemci)

1. Web arayüzü klasörünü sunucuya kopyalayın.
2. IIS'te ayrı bir site açın, kök dizini bu klasördür; HTTPS bağlamasını ekleyin.
3. IIS URL Rewrite modülü kurulu olmalıdır (klasördeki web.config sayfa yenilemelerini index.html'e yönlendirir).
4. API'nin AllowedOrigins ayarında bu adresin yazılı olduğunu kontrol edin.

7. Lisans ve ilk giriş

1. Web arayüzünü açın ve kurulumla gelen yönetici hesabıyla girin: kullanıcı adı admin, parola admin123. Ürün ilk girişte parolayı değiştirmeye zorlar; yeni parolayı belirleyin.
2. Ayarlar > Lisans ekranında lisans dosyasının içeriğini yükleyin. Ürün imzayı doğrular.
3. Ayarlar > Kullanıcılar ekranında kullanıcıları ekleyin (ya da kurum dizini veya kurum hesabıyla girişi kurun). İlk deneme için en az üç kişi önerilir: talep açan (Requester ya da RequestManager), onaylayan (ChangeManager) ve çalıştıran (DbAdmin). En az bir yerel SystemManager hesabını acil durum hesabı olarak tutun.
4. Ayarlar > Sunucular ekranında ilk hedef sunucuyu tanımlayın: ad, adres, veritabanı türü, varsayılan veritabanı, hesap ve parola, ortam (Production ya da Test). Bağlantıyı test edin.
5. Ayarlar > Onay Politikaları ekranında bu sunucu ve talep türü için politikayı tanımlayın (kaç adım, hangi rol). Hedef sunucu hiçbir onay politikasının kapsamında değilse talep kaydedilmez (geri alma talebi bu kuraldan muaftır).
6. Ayarlar > Tanılama > Yönetişim Kurulum Kontrolü ekranını açın. "Kanıt tablosu defter mi" ve "Kanıt yazma sınırı" satırları yeşil olmalıdır. Dikkat işaretli satırlar için karar verin.

8. İlk başarılı talep

1. Talep açan kişiyle girin ve Yeni Talep'e tıklayın. Tür: Değişiklik. Sunucu: Bölüm 7'de tanımladığınız sunucu. Bilet numarası kurumunuz istiyorsa yazılır. Betik örneği:

```
USE [TestVeritabani]
```

```
GO
```

```
CREATE TABLE dbo.SqlChangeGuardIlkDeneme (Id INT NOT NULL PRIMARY KEY, Aciklama NVARCHAR(100) NULL)
```

```
GO
```

2. Kaydedin. Ürün betiği ayrıştırır, nesneleri ve risk bandını gösterir. Engelleyici bir standart ihlali varsa kayıt yapılmaz ve nedeni yazılır.

3. Onaylayan kişiyle girin, Değişiklik Talepleri listesinde talebi açın ve Onayla'ya basın. Politika birden fazla adım istiyorsa her adımı yetkili kişi onaylar.

4. Çalıştıran kişiyle girin ve Çalıştır'a basın. Talep kuyruğa alınır, Worker birkaç saniye içinde çalıştırır. Durum Çalıştırıldı (Executed) olur; çalıştırma günlüğü talep detayında görünür.

5. Hedef veritabanında tablonun oluştuğunu kontrol edin.

Talep "Uzlaştırma Bekliyor" (Reconciliation Required) durumuna geçerse: çalıştırma hedefe ulaşmış ama sonucu kesin bilinmiyordur (örneğin Worker çalışırken kesildi, betik ürünün transaction'ını kendisi bitirdi ya da Oracle hedefte bir veri değişikliği kalıcı olduktan sonra hata alındı). Talep yeniden çalıştırılmaz.

Çalıştırma yetkisi olan kişi hedefi kontrol eder ve talep detayındaki Sonucu işaretli düğmesiyle "değişiklik hedefte var" ya da "değişiklik hedefte yok" der; ne kontrol ettiğini nota yazar. Değişikliğin yalnız bir kısmı hedefteyse "hedefte var" seçilir, notta neyin uygulandığı ve neyin uygulanmadığı yazılır ve kalan iş "Kalan iş için yeni talep (kopyala)" düğmesiyle açılan yeni talepte gönderilir. Karar ve not, talep detayındaki Uzlaştırma Kaydı kutusunda ve denetim dosyasında görünür.

9. Denetim dosyasını üretip doğrulamak

1. Denetim Dosyası İndirebilir yetkisi olan bir kullanıcıyla (ör. Auditor) talep detayını açın ve Denetim Dosyası'na tıklayın. EvidenceFile_CR-....zip iner.
2. ZIP içinde Dossier.pdf, Dossier.json, Manifest.json, Manifest.sig, PublicKey.pem ve Verify.ps1 bulunur. Klasörde şunu çalıştırın:

```
powershell -NoProfile -ExecutionPolicy Bypass -File Verify.ps1
```

İmza ve dosya özetleri tutmalıdır.

3. Dossier.pdf'in ilk sayfasındaki hüküm kırmızı olmamalıdır. "12. Alan Doğrulaması" bölümünde bütün alanlar PASS olmalıdır; defter sonucu, son kaydı kapsayan özet yazıldıktan sonra VERIFIED olur (özet yazılmadan önce NOT_COVERED görünür, bir sonraki özet aralığını bekleyin). "13. Olay Zamanı ve Defter Commit Zamanı" bölümünde bütün olaylar TIME_OK olmalıdır.

Bu adımlar tamamsa kurulum çalışıyordur: talep kayıt altına alındı, onay ve çalıştırma kanıtı deftere yazıldı, defter dış özetle doğrulandı ve denetim dosyası imzalı olarak üretildi.

10. Sık karşılaşılan sorunlar

Belirti	Neden	Çözüm
API açılmıyor, günlükte bağlantı hatası	ConnectionStrings__Default yanlış ya da hesap yetkisiz	Bağlantı dizesini ve Bölüm 2.1'deki izinleri kontrol edin
API açılmıyor, "checksum" ya da betik hatası	Uygulanmış bir kurulum betiği değiştirilmiş	Teslim edilen betikleri değiştirmeyin; destekle görüşün
Worker başlamıyor, "Failed to load worker configuration"	API adresi yanlış ya da WorkerApi__Key, Workers__ApiKey ile aynı değil	İki değeri ve adresi kontrol edin
Talep kaydı "SAVE_BLOCKED_BY_STANDARD" ile reddediliyor	Betik, engelleyici bir SQL standardını ihlal ediyor	Mesajdaki kurala göre betiği düzeltin
Denetim dosyasında defter sonucu UNAVAILABLE	ALLOW_SNAPSHOT_ISOLATION kapalı ya da hesapta VIEW LEDGER CONTENT yok	Bölüm 3.2 ve 2.1
Denetim dosyasında NOT_COVERED	Son kaydı kapsayan defter özeti henüz yazılmadı	Bir özet aralığı bekleyin; API günlüğünde [Ledger] Digest published satırını görün
Denetim dosyasında VERIFIED_INTERNAL	API, defter özeti deposunu (Evidence:Ledger:DigestOutputPath) okuyamıyor; doğrulama yalnız defterin içindeki özetle yapıldı	Yolu API sunucusundan da görülen mutlak bir yol (UNC) yapın ve API uygulama havuzu hesabına bu klasörde okuma yetkisi verin
Durum değiştiren işlemler yapılamıyor, "evidence write boundary" uyarısı	evidence şemasında değişiklik yapılmış (tetikleyici, yordam)	Değişikliği geri alın; Yönetişim Kurulum Kontrolü ekranı bulguyu gösterir