SQL SERVER SAĞLIK RAPORU

SRV-ERP01 · Üretim

Cardinal

Rapor tarihi 20.08.2026 16:39

ÖRNEK	SÜRÜM	QUERY STORE	TARAMA ZAMANI
inst-erp01	SQL 2019 · Standard	Açık	22.07.2026 12:00

HEALTH SCORE

19 / 100

RİSKLİ

BULGU ÖZETİ

0	18	22	5	2
KRİTİK	YÜKSEK	ORTA	DÜŞÜK	BİLGİ

47 bulgu · 47 açık · 0 pas geçildi

Eğilim: geçmiş veri birikmeye devam ediyor.

Yönetici özeti

Örnek riskli bantta. Kritik/yüksek bulgular üretim performansını ve kararlılığını doğrudan tehdit ediyor; ilk üç madde öncelikli ele alınmalıdır.

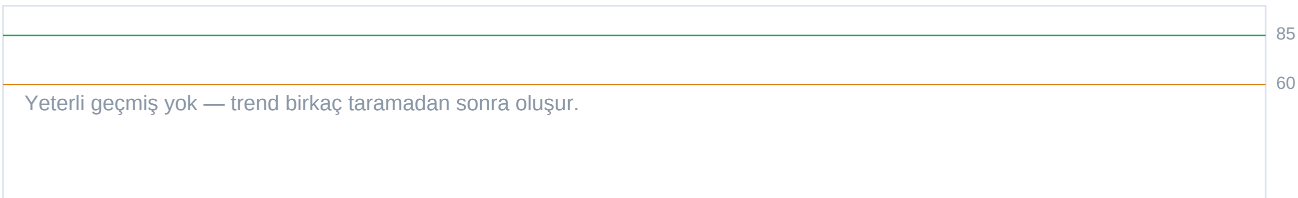
Önce ele alınması gerekenler:

1. Auto-shrink açık veritabanı var — Auto-shrink sürekli küçültme/büyütme döngüsü yaratır: ağır indeks fragmentasyonu, IO ve CPU israfı. Neredeyse hiçbir senaryoda önerilmez.
2. Denetim tanımlı ama çalışmıyor — Denetim tanımı var ama hiçbir audit çalışmıyor — yani kayıt tutulduğu sanılıyor, tutulmuyor. Bu, hiç denetim olmamasından daha tehlikelidir: uyum raporu kapsama olduğunu iddia ederken iz kaydı boştur. Genellikle durdurulmuş audit ya da yazılamayan hedef dosya/klasör anlamına gelir.
3. Disk okuma gecikmesi yüksek (IO stall) — Ortalama okuma başına >30ms gecikme yavaş depolama demektir; sorgular IO'da bekler, PLE düşer. Genelde yavaş disk, yanlış RAID/katman ya da bellek baskısının belirtisi.

Kategori kırılımı

Bekleme profili	33	4 bulgu
Sorgu verimliliği	0	6 bulgu
İndeks sağlığı	72	2 bulgu
IO / bellek	22	4 bulgu
Konfigürasyon	0	11 bulgu
Bakım	0	6 bulgu
Güvenlik / uyum	0	14 bulgu

Skor geçmişi ve sapmalar



Bu taramada baseline'a göre anormal sapma tespit edilmedi.

Bulgular (47)

Önem sırasına göre listelenmiştir. Her bulgu için etki, öneri ve düzeltme betiği verilir; betikler yalnız incelemeniz içindir ve platform tarafından hiçbir zaman çalıştırılmaz.

YÜKSEK ### 1. Auto-shrink açık veritabanı var

Konfigürasyon · cfg-auto-shrink

Etki: Auto-shrink sürekli küçültme/büyütme döngüsü yaratır: ağır indeks fragmentasyonu, IO ve CPU israfı. Neredeyse hiçbir senaryoda önerilmez.

Öneri: İlgili veritabanlarında auto-shrink'i kapat; disk yönetimini planlı bakımla yap.

Düzeltme T-SQL — bu örneğe göre otomatik üretildi yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [ERP_DB] SET AUTO_SHRINK OFF;
ALTER DATABASE [ARSIV_DB] SET AUTO_SHRINK OFF;
```

YÜKSEK ### 2. Denetim tanımlı ama çalışmıyor

Güvenlik / uyum · sec-audit-not-running

Etki: Denetim tanımı var ama hiçbir audit çalışmıyor — yani kayıt tutulduğu sanılıyor, tutulmuyor. Bu, hiç denetim olmamasından daha tehlikelidir: uyum raporu kapsama olduğunu iddia ederken iz kaydı boştur. Genellikle durdurulmuş audit ya da yazılamayan hedef dosya/klasör anlamına gelir.

Öneri: Audit'i tekrar başlatın ve neden durduğunu bulun: hedef klasör dolmuş/erişilemiyor olabilir, ON_FAILURE ayarı servisi durdurmuş olabilir. Audit durumunu izlemeye alın — sessizce durabilen bir denetim, denetim değildir.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Hangi audit'in durduğunu görün:
SELECT a.name, s.status_desc, s.audit_file_path
FROM sys.server_audits a
LEFT JOIN sys.dm_server_audit_status s ON s.audit_id = a.audit_id;

-- Sonra ilgili audit'i başlatın:
ALTER SERVER AUDIT [Audit_Guvenlik] WITH (STATE = ON);
```

YÜKSEK ### 3. Disk okuma gecikmesi yüksek (IO stall)

IO / bellek · io-high-read-stall

Etki: Ortalama okuma başına >30ms gecikme yavaş depolama demektir; sorgular IO'da bekler, PLE düşer. Genelde yavaş disk, yanlış RAID/katman ya da bellek baskısının belirtisi.

Öneri: En yüksek gecikmeli dosyaları belirle; depolama katmanını/latency'i incele, bellek baskısını (PLE) ve eksik indeksleri kontrol et.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Araştırma: yüksek gecikmeli dosyaları listele (yukarıdaki kanıt sorgusu).
-- Çözüm depolama/altyapı tarafında; T-SQL ile düzelmez.
```

YÜKSEK ### 4. FULL recovery veritabanında log yedeği gecikmiş

Bakım · maint-no-log-backup

Etki: FULL recovery modelinde log yedeği alınmazsa transaction log dosyası şişer VE point-in-time kurtarma penceresi kaybolur; log dolarsa veritabanı yazılamaz hale gelir.

Öneri: FULL recovery DB'lerde sık (ör. 15-60 dk) log yedeği zamanla. Log yedeği gerekmiyorsa veritabanını SIMPLE recovery'ye al.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
BACKUP LOG [VeritabaniAdi] TO DISK = N'Y:\Backup\VeritabaniAdi_LOG.trn' WITH CHECKSUM, COMPRESSION;
```

YÜKSEK ### 5. Hiç Cumulative Update uygulanmamış (RTM/GDR dalı)

Bakım · maint-no-cu-applied

Etki: Ana sürüm destekli olsa bile hiç CU uygulanmamış: yıllardır çıkan performans/kararlılık düzeltmeleri ve güvenlik yamaları eksik. 'Destekli sürüm' raporu bunu göstermez — bakımsızlığın gizli ama kritik bir göstergesi.

Öneri: Uygun en güncel Cumulative Update'i (CU) test ortamında dene, sonra bakım penceresinde uygula. GDR (security-only) yerine CU dalına geçmeyi değerlendir.

Tespit edilenler (1)

- SRV-ERP01 · SQL 2019 · 15.0.2130.3 (RTM) — RTM/GDR dalı — hiç Cumulative Update uygulanmamış · CU dalı 4000+ (güncel ~4410, ~CU30 (2025)).

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- CU kurulumu bir işletim/servis işidir; T-SQL ile yapılmaz.
-- Güncel build'i doğrula: SELECT SERVERPROPERTY('ProductVersion'), SERVERPROPERTY('ProductUpdateLevel');
-- Microsoft build listesinden sürümüne uygun en güncel CU'yu indir.
```

YÜKSEK

6. Max Server Memory sınırsız (varsayılan)

Konfigürasyon · cfg-max-memory-unlimited

Etki: SQL Server tüm belleği talep edebilir; işletim sistemine ve diğer servislere bellek kalmaz, sayfalama (paging) ve kararsızlık riski doğar.

Öneri: Toplam RAM'den OS + diğer bileşenlere pay bırakacak şekilde bir üst sınır belirle (kaba kural: RAM - max(4GB, %10)).

Düzeltme T-SQL — bu örneğe göre otomatik üretildi — yalnız gösterim — çalıştırılmaz

```
-- Toplam RAM 65.536 MB · OS/diğer servisler için 6.554 MB ayrıldı ? Max Server Memory 58.982 MB
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'max server memory (MB)', 58982; RECONFIGURE;
```

YÜKSEK

7. MAXDOP is left at 0 (unbounded parallelism)

Konfigürasyon · cfg-maxdop-default

Etki: On multi-core / multi-NUMA servers, MAXDOP 0 lets a single query fan out across every scheduler, driving CXPACKET/CXCONSUMER waits and CPU pressure under concurrency.

Öneri: Set MAXDOP from the core and NUMA layout (commonly 4-8; not more than the cores in a single NUMA node). Pair with Cost Threshold for Parallelism.

Düzeltme T-SQL — bu örneğe göre otomatik üretildi — yalnız gösterim — çalıştırılmaz

```
-- 16 mantıksal işlemci · 2 NUMA düğümü ? önerilen MAXDOP 8
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'max degree of parallelism', 8; RECONFIGURE;
```

YÜKSEK

8. Page Life Expectancy chronically low (memory pressure)

IO / bellek · mem-low-ple

Etki: Sustained low PLE means the buffer pool is churning — pages evicted and re-read from disk, adding IO latency to otherwise memory-resident workloads.

Öneri: Investigate memory-hungry plans (big scans / missing indexes), verify Max Server Memory is set, and confirm the box is not starved of RAM. Do not chase a single dip — evaluate over a window.

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Investigative, not a blind fix:
SELECT TOP 20 qs.total_logical_reads, qs.execution_count, SUBSTRING(st.text, 1, 200) AS query_text
FROM sys.dm_exec_query_stats AS qs
CROSS APPLY sys.dm_exec_sql_text(qs.sql_handle) AS st
ORDER BY qs.total_logical_reads DESC;
```

YÜKSEK

9. Plan regresyonu: sorgular eski planından çok yavaşladı

Sorgu verimliliği · qs-plan-regression

Etki: Query Store'a göre bazı sorgular geçmişteki en iyi planlarına kıyasla 3 kattan fazla yavaşladı. Klasik neden: istatistik güncellemesi veya parametre sniffing sonrası derlenen kötü plan. Bu 'yaşayan organizma' sinyalinin en değerlisi — dün hızlı olan bugün yavaş.

Öneri: Regresyona giren sorgunun Query Store'daki plan geçmişini incele; bilinen iyi planı zorla (force plan). Kök neden istatistik/parametre sniffing ise onu da gider (OPTIMIZE FOR, RECOMPILE, stat güncelleme).

Tespit edilenler (2)

- ERP_DB · query_id 4821 · ~180 ms ? 2.400 ms (13.3x) — 36.500 çalıştırma · Query Store'da iyi planı force etmeyi değerlendir

  ```
  SELECT o.Id, o.Total FROM dbo.Orders o WHERE o.CustomerId = @p1 AND o.OrderDate >= @p2
  ```
- ERP_DB · query_id 5190 · ~90 ms ? 620 ms (6.9x) — 12.100 çalıştırma · Query Store'da iyi planı force etmeyi değerlendir

  ```
  SELECT SUM(l.Qty*l.Price) FROM dbo.OrderLines l WHERE l.ProductId = @p1
  ```

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Query Store'da iyi planı bul, sonra:
-- EXEC sys.sp_query_store_force_plan @query_id = <id>, @plan_id = <iyi_plan_id>;
-- (Kanıt sorgusundaki query_id'yi kullan; planları SSMS > Query Store > 'Regressed Queries' ile karşılaştır.)
```

YÜKSEK

10. public rolüne fazladan sunucu izni verilmiş

Güvenlik / uyum · sec-public-server-perms

Etki: public rolüne verilen her izin, sunucuya bağlanabilen HER login'e verilmiş demektir — en düşük yetki ilkesinin tam tersi. Kurulumda gelen varsayılanların dışındaki izinler bilinçli verilmiştir ve çoğu zaman unutulmuştur.

Öneri: Fazladan izinleri public'ten geri alın ve gerçekten ihtiyacı olan hesap ya da role verin. Geri almadan önce hangi uygulamanın kullandığını doğrulayın — public üzerinden çalışan eski bir uygulama kırılabilir.

Tespit edilenler (1)

- VIEW SERVER STATE — kapsam: server — her login'e geçerli

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Önce ne verilmiş, görün:
SELECT permission_name, class_desc, state_desc
FROM sys.server_permissions
WHERE grantee_principal_id = 2 AND class <> 105;

-- Sonra gereksiz olanı geri alın (örnek):
-- REVOKE VIEW SERVER STATE FROM [public];
```

YÜKSEK 11. Query Store sessizce READ_ONLY'ye düştü (veri toplamıyor)

Konfigürasyon · qs-readonly-unexpected

Etki: Query Store READ_WRITE isteniyor ama fiilen READ_ONLY — yeni veri toplanmıyor. Genelde depolama sınırına (max_storage_size_mb) ulaşılmıştır. Regresyon/plan analizi sessizce kör kalır; en tehlikeli durum, çünkü açık sanılır ama çalışmaz.

Öneri: readonly_reason'ı incele. Depolama sınırını artır veya temizleme politikasını (stale query cleanup, capture mode AUTO) sıkılaştır; sonra READ_WRITE'a geri al.

Tespit edilenler (1)

- ARSIV_DB · READ_ONLY (READ_WRITE isteniyordu) — depolama 1.024/1.024 MB · readonly_reason: 65540 (depolama sınırı doldu)

Düzeltme T-SQL — bu örneğe göre otomatik üretildi yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [ARSIV_DB] SET QUERY_STORE (MAX_STORAGE_SIZE_MB = 2048, QUERY_CAPTURE_MODE = AUTO, CLEANUP_POLICY
= (STALE_QUERY_THRESHOLD_DAYS = 30));
ALTER DATABASE [ARSIV_DB] SET QUERY_STORE = ON (OPERATION_MODE = READ_WRITE);
```

YÜKSEK 12. Signal wait oranı yüksek (CPU baskısı)

Bekleme profili · waits-high-signal

Etki: Signal wait, kaynak hazır olduktan sonra sorgunun CPU'da sıra beklediği süredir. Yüksek oran (>%25) CPU'nun darboğaz olduğunu gösterir.

Öneri: En çok CPU tüketen sorguları (sys.dm_exec_query_stats) incele; MAXDOP/CTFP ayarlarını gözden geçir; gerekiyorsa çekirdek ekle.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Araştırma: en yüksek total_worker_time'a sahip sorgular.
SELECT TOP 20 qs.total_worker_time, qs.execution_count, SUBSTRING(st.text, 1, 200) AS q FROM
sys.dm_exec_query_stats qs CROSS APPLY sys.dm_exec_sql_text(qs.sql_handle) st ORDER BY qs.total_worker_time
DESC;
```

YÜKSEK 13. Son 24 saatte başarısız olan SQL Agent job'ları var

Bakım · agent-failed-jobs

Etki: Başarısız job'lar sessizce yedek, indeks bakımı, istatistik güncelleme veya DBCC gibi kritik işlerin çalışmadığı anlamına gelebilir — bakımsızlık riskinin doğrudan göstergesi.

Öneri: Başarısız job'ların adım geçmişini (sysjobstepslogs / job history) incele, kök nedeni gider; job'lara başarısızlık bildirimi (operator/e-posta) ekle.

Tespit edilenler (2)

- ERP - Gecelik Yedek — son hata: 2026-07-22 02:00
- Index Maintenance (Ola) — son hata: 2026-07-22 03:15

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Job geçmişini incele:
-- EXEC msdb.dbo.sp_help_jobhistory @job_name = N'JobAdi';
```

YÜKSEK 14. Son 24 saatte tam yedek (FULL backup) alınmamış

Bakım · maint-no-full-backup

Etki: Güncel tam yedek yoksa donanım/bozulma/fidye durumunda veri kaybı doğrudan yedek yaşına eşittir. Hiç yedeği olmayan veritabanı en yüksek risktir.

Öneri: Düzenli yedek işi kur (Ola Hallengren bakım çözümü önerilir); en az günlük tam + kısa aralıklı log yedeği. Yedeklerin geri yüklenebilirliğini test et.

Tespit edilenler (2)

- ERP_DB — son tam yedek: 2026-07-19 03:00 (~72 saat önce)
- ARSIV_DB — hiç tam yedek yok

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
BACKUP DATABASE [VeritabaniAdi] TO DISK = N'Y:\Backup\VeritabaniAdi_FULL.bak' WITH CHECKSUM, COMPRESSION, INIT;
```

YÜKSEK 15. Şu an uzun süren sorgu(lar) çalışıyor

Sorgu verimliliği · queries-active-slow

Etki: Tarama anında 5 saniyeden uzun süren canlı sorgular var. Detayda bunları TETİKLEYEN uygulama ve kullanıcı ile yavaşlık nedeni (bekleme türü) gösterilir. Süreklilik gösteriyorsa gerçek bir darboğazdır.

Öneri: Detaydaki uygulama/kullanıcıyı ve bekleme nedenini kullanarak kaynağı belirle: bloklama (kilit), disk IO (eksik indeks), bellek grant veya CPU baskısı. Query Store / plan analizi ile kalıcı çözüm.

Tespit edilenler (2)

- ERP-App (.Net SqlClient) · DOMAIN\erp_svc · APPSRV01 — 12.400 ms · disk IO bekliyor — yavaş depolama ya da eksik indeks (tarama)

  ```
  SELECT SUM(Total) FROM dbo.OrderLines WHERE ProductId = @p1
  ```

- Excel (Microsoft Office) · DOMAIN\muhasebe · FIN-PC07 — 9.100 ms · istemciye veri gönderiyor — uygulama sonuçları yavaş çekiyor

  ```
  SELECT * FROM dbo.Orders
  ```

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Canlı incele: SELECT r.session_id, r.wait_type, r.blocking_session_id, DB_NAME(r.database_id) db,
s.login_name, s.program_name, r.total_elapsed_time/1000 AS ms FROM sys.dm_exec_requests r JOIN
sys.dm_exec_sessions s ON s.session_id=r.session_id WHERE s.is_user_process=1 AND r.total_elapsed_time>5000
ORDER BY r.total_elapsed_time DESC;
```

YÜKSEK 16. TRUSTWORTHY açık veritabanı

Güvenlik / uyum · sec-trustworthy-db

Etki: TRUSTWORTHY açık ve veritabanı sysadmin yetkili bir hesaba aitse, o veritabanında db_owner olan herkes sunucunun tamamında sysadmin'e yükselebilir. Belgelenmiş ve saldırganların rutin olarak kullandığı bir yetki yükseltme yoludur.

Öneri: TRUSTWORTHY'yi kapatın. Gerçekten gerekiyorsa (CLR ya da veritabanları arası erişim), bunun yerine sertifika ile imzalanmış modül kullanın ve veritabanının sahibini sysadmin olmayan bir hesaba alın.

Tespit edilenler (2)

- ERP_DB — sahip: sa
- ARSIV_DB — sahip: BILGITEKyonetici

Düzeltme T-SQL — bu örneğe göre otomatik üretildi — yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [ERP_DB] SET TRUSTWORTHY OFF;
ALTER DATABASE [ARSIV_DB] SET TRUSTWORTHY OFF;
```

YÜKSEK 17. xp_cmdshell etkin

Güvenlik / uyum · sec-xp-cmdshell

Etki: xp_cmdshell, SQL üzerinden işletim sistemi komutu çalıştırmayı sağlar; ele geçirilen bir SQL hesabı sunucunun tamamını tehdit eder. Ciddi saldırı yüzeyi.

Öneri: İhtiyaç yoksa kapat. Gerekliyse, çağıran hesapları en aza indir ve proxy hesap/Agent job ile izole et.

Tespit edilenler (2)

- ERP_DB · dbo.usp_ExportToFile — kod referansı (SQL_STORED_PROCEDURE)
- Agent job: Nightly File Sync — adım: copy-exports

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'xp_cmdshell', 0; RECONFIGURE;
```

YÜKSEK

18. Zorlanan plan (forced plan) uygulanamıyor

Sorgu verimliliği · qs-forced-plan-failing

Etki: Bir plan zorlanmış (force plan) ama SQL Server onu uygulayamıyor (force_failure_count > 0) — sessizce eski/kötü plana düşüyor. Force işlemi yapıldığı sanılırken koruma çalışmıyor; regresyon geri gelmiş olabilir.

Öneri: Başarısızlık nedenini (last_force_failure_reason_desc) incele — indeks/şema değişikliği çoğu zaman planı geçersiz kılar. Planı yeniden değerlendir; artık geçerli değilse force'u kaldırıp güncel iyi planı yeniden zorla.

Tespit edilenler (1)

- ERP_DB · query_id 4821 · plan 77 — 18 başarısızlık · neden: NO_INDEX (plan zorlandı ama indeks değişmiş)

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Nedeni gör, sonra gerekiyorsa temizle ve yeniden zorla:
-- EXEC sys.sp_query_store_unforce_plan @query_id = <id>, @plan_id = <id>;
-- EXEC sys.sp_query_store_force_plan @query_id = <id>, @plan_id = <gecerli_iyi_plan_id>;
```

ORTA

19. Anlık bloklama (blocked session) var

Bekleme profili · blocking-active

Etki: Tarama anında engellenen oturumlar var. Süreklilik gösteriyorsa, uzun süren transaction'lar veya uygunsuz izolasyon seviyesi kullanıcı gecikmelerine ve zaman aşımlarına yol açar.

Öneri: Bloklama zincirini (sp_WhoIsActive paterni) incele; kök transaction'ı ve sorunlu sorguyu tespit et. Süreklilik varsa baseline'la (bu ürünün trend özelliği) doğrula.

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Bloklama zinciri:
SELECT r.session_id, r.blocking_session_id, r.wait_type, r.wait_time, SUBSTRING(t.text,1,200) AS q FROM
sys.dm_exec_requests r CROSS APPLY sys.dm_exec_sql_text(r.sql_handle) t WHERE r.blocking_session_id <> 0;
```

ORTA

20. Cost Threshold for Parallelism still at default (5)

Konfigürasyon · cfg-ctfp-default

Etki: The 1995-era default of 5 makes trivial queries go parallel, wasting workers and inflating parallelism waits.

Öneri: Raise Cost Threshold for Parallelism (commonly 25-50) so only genuinely expensive plans parallelize.

Düzeltme T-SQL — bu örneğe göre otomatik üretildi — yalnız gösterim — çalıştırılmaz

```
-- Cost Threshold for Parallelism şu an 5 ? önerilen 50
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'cost threshold for parallelism', 50; RECONFIGURE;
```

ORTA

21. Deadlock oluşmuş (restart'tan beri)

Bekleme profili · deadlocks-present

Etki: Son yeniden başlatmadan bu yana deadlock yaşanmış. Deadlock'lar iptal edilen işlemler ve kullanıcı hataları demektir; genelde erişim sırası veya indeks/eskalasyon kaynaklıdır.

Öneri: system_health Extended Event oturumundaki deadlock graph'ları incele; kaynak erişim sırasını standardize et, doğru indekslerle lock kapsamını daralt.

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- system_health'ten son deadlock graph'ları (2016+):
-- SELECT XEvent.query('.') FROM (SELECT CAST(target_data AS xml) td FROM sys.dm_xe_session_targets t JOIN
sys.dm_xe_sessions s ON s.address=t.event_session_address WHERE s.name='system_health' AND
t.target_name='ring_buffer') a CROSS APPLY td.nodes('//RingBufferTarget/event[@name="xml_deadlock_report"]') AS
X(XEvent);
```

ORTA

22. Fazla sayıda sysadmin hesabı

Güvenlik / uyum · sec-sysadmin-sprawl

Etki: sysadmin yetkisi sunucuda sınırsızdır: her veriyi okur, her denetimi kapatır, iz bırakmadan geri alır. Yetki dağıldıkça ele geçirilen tek bir hesap bütün örneği verir ve olay sonrası 'kim yaptı' sorusu cevapsız kalır. Zamanla biriken ayrılmış personel ve uygulama hesapları en yaygın nedendir.

Öneri: Listeyi gözden geçirin: ayrılan personeli ve artık kullanılmayan uygulama hesaplarını çıkarın. Uygulamalar sysadmin ile bağlanmamalı — ihtiyacı olan yetkiyi (çoğu zaman db_owner ya da daha azı) hedefli verin.

Tespit edilenler (7)

- ERP_SERVIS — sql login
- BILGITEKahmet — windows login
- BILGITEKayrilan_personel — windows login

- RAPOR_KULLANICI — sql login
- BILGITEKSQLAdmins — windows group
- ENTEGRASYON — sql login

  … ve 1 kayıt daha (panelde tamamı görünür).

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Mevcut sysadmin üyeleri:
SELECT m.name, m.type_desc, m.create_date, m.is_disabled
FROM sys.server_role_members rm
JOIN sys.server_principals r ON r.principal_id = rm.role_principal_id AND r.name = 'sysadmin'
JOIN sys.server_principals m ON m.principal_id = rm.member_principal_id;

-- Gereksiz üyeyi çıkarın (uygulamayı doğruladıktan sonra):
-- ALTER SERVER ROLE [sysadmin] DROP MEMBER [hesap_adi];
```

ORTA 23. guest kullanıcısı etkin veritabanı

Güvenlik / uyum · sec-guest-enabled

Etki: guest etkinken, o veritabanında kullanıcısı olmayan HERHANGİ bir login veritabanına bağlanabilir. Yalnızca örneğe bağlanabilen bir hesap, hiç yetkilendirilmediği veritabanlarını görebilir hale gelir — yatay erişim yayılmasının klasik yolu.

Öneri: Kullanıcı veritabanlarında guest'in CONNECT iznini geri alın. (master, msdb ve tempdb'de guest gereklidir, onlara dokunmayın.)

Tespit edilenler (1)

- RAPOR_DB — guest kullanıcısında CONNECT izni var

Düzeltme T-SQL — bu örneğe göre otomatik üretildi — yalnız gösterim — çalıştırılmaz

```
USE [RAPOR_DB];
REVOKE CONNECT FROM guest;
```

ORTA 24. High-impact missing index (above impact threshold)

İndeks sağlığı · idx-high-impact-missing

Etki: The missing-index DMVs are naive and noisy; only surface suggestions above an impact threshold AFTER dedup/consolidation, otherwise you recommend 40 near-duplicate indexes.

Öneri: Consolidate overlapping suggestions, weigh against write cost and existing indexes, then propose a single covering index. Never apply raw DMV output verbatim.

Tespit edilenler (2)

- ERP_DB · dbo.Orders — tahmini etki ~4.200.000

```
USE [ERP_DB];
CREATE INDEX [IX_Orders_CustomerId] ON dbo.Orders ([CustomerId], [OrderDate]) INCLUDE ([Total]);
```

- ERP_DB · dbo.OrderLines — tahmini etki ~1.850.000

```
USE [ERP_DB];
CREATE INDEX [IX_OrderLines_ProductId] ON dbo.OrderLines ([ProductId]) INCLUDE ([Qty], [Price]);
```

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Template only; engine fills columns after consolidation. Review before creating.
-- CREATE INDEX IX_<table>_<cols> ON <schema>.<table> (<equality_columns>, <inequality_columns>) INCLUDE
(<included_columns>);
```

ORTA 25. Instant File Initialization kapalı

Konfigürasyon · cfg-ifi-disabled

Etki: Veri dosyası büyümesi ve restore işlemleri sıfırlama nedeniyle çok daha yavaş; auto-growth anında bloklamaya yol açar.

Öneri: SQL Server servis hesabına 'Perform volume maintenance tasks' (SeManageVolumePrivilege) hakkını ver; sonra servisi yeniden başlat.

Düzeltme T-SQL — yalnız gösterim — çalıştırılmaz

```
-- Windows: secpol.msc ? Perform volume maintenance tasks ? SQL servis hesabını ekle ? servisi restart.
-- (2022'de kurulum sırasında da açılabilir.)
```

ORTA 26. İstatistik güncelliği eskimiş tablolar var

Bakım · maint-stats-stale

Etki: Eskimiş istatistikler kardinalite tahminini bozar; optimizer kötü planlar seçer, sorgular zamanla yavaşlar. Bakımsız sistemlerde sinsi bir dejenerasyon kaynağı.

Öneri: İlgili tablolarda istatistikleri güncelle; düzenli bir bakım işi (Ola Hallengren IndexOptimize) planla.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Örnek (tablo bazlı): UPDATE STATISTICS dbo.FactSales WITH FULLSCAN;
-- Tercihen bakım penceresinde otomatik iş olarak.
```

ORTA 27. Kullanılmayan (yalnızca yazılan) indeksler var

İndeks sağlığı · idx-unused

Etki: Hiç okunmayan ama her yazımda güncellenen indeksler INSERT/UPDATE/DELETE'i yavaşlatır, disk ve bakım maliyeti ekler. Not: sayaçlar son restart'tan beri; kaldırmadan önce yeterli gözlem süresi gerekir.

Öneri: Yeterli gözlem penceresinden sonra (haftalar) gerçekten kullanılmayan indeksleri devre dışı bırak/kaldır. Unique/constraint destekleyenlere dokunma.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Önce DISABLE ile test et, sonra DROP:
-- ALTER INDEX [IX_Adi] ON [dbo].[Tablo] DISABLE;
-- DROP INDEX [IX_Adi] ON [dbo].[Tablo];
```

ORTA 28. msdb geçmişi temizlenmiyor (şişme)

Bakım · sysdb-msdb-history-bloat

Etki: Yedek ve job geçmişi hiç budanmıyorsa msdb büyür; SSMS raporları ve bazı sorgular yavaşlar, gereksiz yer tutulur.

Öneri: sp_delete_backuphistory ve sp_purge_jobhistory ile düzenli budama işi kur (ör. 90-180 günden eski kayıtları sil).

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
DECLARE @d datetime = DATEADD(day, -90, GETDATE());
EXEC msdb.dbo.sp_delete_backuphistory @oldest_date = @d;
```

ORTA 29. PAGE_VERIFY CHECKSUM değil

Konfigürasyon · cfg-page-verify

Etki: CHECKSUM olmadan disk kaynaklı sayfa bozulmaları (I/O corruption) sessizce fark edilmeden kalabilir.

Öneri: Tüm veritabanlarında PAGE_VERIFY CHECKSUM'a geç.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [VeritabaniAdi] SET PAGE_VERIFY CHECKSUM;
```

ORTA 30. Paralellik beklemeleri yüksek (CXPACKET/CXCONSUMER)

Bekleme profili · waits-cxpacket-high

Etki: Bekleme profilinin büyük kısmı paralellik senkronizasyonu; genelde düşük MAXDOP/CTFP ayarları veya eksik indeks yüzünden tarama-ağırlıklı paralel planlar.

Öneri: Önce MAXDOP ve Cost Threshold for Parallelism ayarlarını düzelt; ardından en pahalı paralel planları ve eksik indeksleri incele.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Önce cfg-maxdop-default ve cfg-ctfp-default bulgularını uygula; sonra sp_BlitzCache ile paralel planları
gözden geçir.
```

ORTA 31. Parola politikası uygulanmayan SQL login'leri

Güvenlik / uyum · sec-weak-password-policy

Etki: CHECK_POLICY kapalı olan login'de Windows parola politikası uygulanmaz: karmaşıklık zorunlu değildir ve — daha önemlisi — hesap kilitleme çalışmaz. Bu, parolanın sınırsız denenebilmesi demektir; SQL portu erişilebilir durumdaysa kaba kuvvet saldırısı önünde hiçbir engel kalmaz.

Öneri: Bu login'lerde CHECK_POLICY'yi açın. Açmadan önce mevcut parolanın politikayı karşıladığından emin olun, aksi halde ilk bağlantıda hata alınır. Uygulama hesaplarında parola süre sonunu (CHECK_EXPIRATION) kapalı bırakabilirsiniz.

Tespit edilenler (2)

- ERP_SERVIS — CHECK_POLICY kapalı — karmaşıklık/kilitleme kuralı uygulanmıyor
- ENTEGRASYON — CHECK_POLICY kapalı — karmaşıklık/kilitleme kuralı uygulanmıyor

Düzeltme T-SQL — bu örneğe göre otomatik üretildi yalnız gösterim — çalıştırılmaz

```
ALTER LOGIN [ERP_SERVIS] WITH CHECK_POLICY = ON, CHECK_EXPIRATION = OFF;
ALTER LOGIN [ENTEGRASYON] WITH CHECK_POLICY = ON, CHECK_EXPIRATION = OFF;
```

ORTA **32. Plan cache tek-kullanımlık planlarla şişmiş** Sorgu verimliliği · queries-plan-cache-single-use

Etki: Ad-hoc sorguların çoğu tek kullanımlık plan üretiyor; plan cache belleği israf oluyor ve yeniden derleme (compile) CPU'su artıyor.

Öneri: 'Optimize for ad hoc workloads' ayarını aç; mümkünse parametreli sorgu/stored procedure kullanımını yaygınlaştır.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'optimize for ad hoc workloads', 1; RECONFIGURE;
```

ORTA **33. Riskli sunucu özellikleri açık** Güvenlik / uyum · sec-risky-features

Etki: Bu anahtarlar kurulumda KAPALI gelir; açıksa biri bilerek açmıştır ve çoğu zaman tek seferlik bir ihtiyaç için açılıp unutulmuştur. Her biri saldırı yüzeyi ekler: CLR yönetilmeyen kod çalıştırır, sp_OA* işletim sistemi nesnelerine erişir, OPENROWSET sunucudan dışarı veri taşır, sahiplik zinciri ise veritabanları arasında yetki sızdırır.

Öneri: Açık olan her özellik için 'hangi uygulama kullanıyor' sorusunu cevaplayın. Cevap yoksa kapatın. Gerçekten gerekliyse kullanımını tek bir hesaba ve veritabanına daraltıp denetim kapsamına alın.

Tespit edilenler (2)

- Ole Automation Procedures — sp_OA* — SQL üzerinden COM nesnesi çalıştırma
- Ad Hoc Distributed Queries — OPENROWSET/OPENDATASOURCE — dışarı veri çekme/gönderme

Düzeltme T-SQL — bu örneğe göre otomatik üretildi yalnız gösterim — çalıştırılmaz

```
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'Ole Automation Procedures', 0; RECONFIGURE;
EXEC sys.sp_configure 'Ad Hoc Distributed Queries', 0; RECONFIGURE;
```

ORTA **34. Şifrelenmemiş istemci bağlantıları** Güvenlik / uyum · sec-unencrypted-connections

Etki: Bağlantılar TLS olmadan kuruluyor: sorgular ve dönen veri ağ üzerinde açık geçiyor. Aynı ağ segmentinde trafiği dinleyebilen biri hem iş verisini hem de SQL kimlik doğrulama trafiğini görebilir. Şube ya da VPN üzerinden bağlanan ERP kurulumlarında risk belirgin biçimde yükselir.

Öneri: Sunucuya geçerli bir sertifika tanımlayıp Force Encryption'ı açın ya da istemci bağlantı dizelerinde Encrypt=True kullanın. Önce hangi istemcilerin şifresiz bağlandığını tespit edin — eski sürücüler TLS'i desteklemeyebilir.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Şifresiz bağlanan oturumları ve istemcilerini görün:
SELECT c.session_id, s.login_name, s.host_name, s.program_name, c.encrypt_option, c.client_net_address
FROM sys.dm_exec_connections c
JOIN sys.dm_exec_sessions s ON s.session_id = c.session_id
WHERE c.encrypt_option = 'FALSE';

-- Düzeltme sunucu tarafındadır: SQL Server Configuration Manager -> Protocols -> Force Encryption = Yes
-- (geçerli bir sertifika tanımlandıktan sonra; servis yeniden başlatma gerektirir)
```

ORTA **35. tempdb dosyalarında yüzde-tabanlı büyüme** Konfigürasyon · tempdb-percent-growth

Etki: tempdb'de yüzde büyüme, yoğun yük altında öngörülemez ve giderek büyüyen büyüme olaylarına yol açar; büyüme sırasında IFI yoksa uzun bloklamalar oluşur.

Öneri: tempdb dosyalarını sabit MB büyümeye ayarla ve başlangıç boyutunu tipik kullanıma göre yeterli ver (mümkünse hiç büyümesin).

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE tempdb MODIFY FILE (NAME = tempdev, FILEGROWTH = 512MB);
```

ORTA **36. tempdb tek veri dosyası kullanıyor** IO / bellek · tempdb-single-file

Etki: Tek tempdb veri dosyası, yoğun geçici nesne kullanımında allocation (PFS/GAM/SGAM) çekişmesine yol açar; PAGELATCH beklemeleri artar.

Öneri: tempdb'yi çekirdek sayısına göre eşit boyutlu birden çok veri dosyasına böl (genelde 4-8, çekirdek sayısını aşma).

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Örnek: 4 eşit dosyaya çıkar (boyutları eşitle).
```

```
-- ALTER DATABASE tempdb ADD FILE (NAME = tempdev2, FILENAME = 'T:\tempdb2.ndf', SIZE = 1024MB, FILEGROWTH =
512MB);
```

ORTA 37. tempdb veri dosyaları eşit boyutlu değil

IO / bellek · tempdb-uneven-files

Etki: Eşit olmayan tempdb dosyaları, orantılı doldurma (proportional fill) algoritması yüzünden büyük dosyaya yönelen IO'ya ve allocation çekişmesine yol açar; çoklu dosyanın faydasını azaltır.

Öneri: Tüm tempdb veri dosyalarını aynı başlangıç boyutu ve aynı (sabit MB) auto-growth ile yapılandır.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Tüm tempdb dosyalarını eşitle:
-- ALTER DATABASE tempdb MODIFY FILE (NAME = tempdev, SIZE = 1024MB, FILEGROWTH = 512MB);
```

ORTA 38. Yüksek ortalama süreli sorgular var

Sorgu verimliliği · queries-slow-top

Etki: Ortalama çalışma süresi yüksek sorgular (plan cache'teki toplam istatistiğe göre) kullanıcı gecikmesinin ve kaynak tüketiminin ana kaynağıdır. Not: sayaçlar plan cache ömrüyle sınırlıdır.

Öneri: En pahalı sorguların planını incele: eksik indeks, tarama (scan), kötü kardinalite tahmini, parametre sniffing. Query Store açıksa regresyonları oradan izle.

Tespit edilenler (1)

- ~8.200 ms ort · 1.240 çalıştırma · ~1.900 ms CPU — ~4.200.000 logical read/çalıştırma

```
SELECT * FROM dbo.Orders o JOIN dbo.OrderLines l ON l.OrderId = o.Id WHERE o.CustomerId = @p1 ORDER BY o.OrderDate
```

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- En pahalı sorgular (süre/CPU/okuma) — kanıt sorgusuna bak; planı SSMS'te 'Include Actual Execution Plan' ile
incele.
```

ORTA 39. Yüksek süre değişkenliği: parametre sniffing adayları

Sorgu verimliliği · qs-high-variance

Etki: Aynı sorgunun çalışma süresi çok oynuyor (standart sapma > ortalama). Genelde parametre sniffing: aynı plan bazı parametre değerlerinde hızlı, bazılarında felaket. Kullanıcı 'bazen anında, bazen donuyor' der.

Öneri: Parametreye duyarlı sorguyu tespit et; OPTIMIZE FOR UNKNOWN, RECOMPILE, veya sorguyu yeniden yaz. 2022+ ise Parameter Sensitive Plan (PSP) optimizasyonu devreye girebilir. Query Store'dan iyi/kötü planları karşılaştır.

Tespit edilenler (1)

- ERP_DB · query_id 6033 — ort ~140 ms · std sapma ~410 ms · parametre sniffing adayı

```
SELECT * FROM dbo.Invoices WHERE Status = @p1
```

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Değişkenliği yüksek sorguyu kanıt sorgusundan bul. Seçenekler:
-- 1) OPTION (OPTIMIZE FOR UNKNOWN) 2) OPTION (RECOMPILE) 3) tutarlı bir planı force et.
```

ORTA 40. Yüzde-tabanlı auto-growth kullanan dosyalar var

Konfigürasyon · cfg-autogrowth-percent

Etki: Yüzde büyüme, dosya büyüdükçe giderek daha büyük ve öngörülemez büyüme olaylarına yol açar; uzun bloklamalar ve disk sıçramaları.

Öneri: Auto-growth'u sabit MB değerine çevir (ör. 256MB-1GB, dosya boyutuna göre).

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [VeritabaniAdi] MODIFY FILE (NAME = N'MantiksalDosyaAdi', FILEGROWTH = 512MB);
```

DÜŞÜK 41. 'sa' hesabı etkin

Güvenlik / uyum · sec-sa-enabled

Etki: Etkin ve bilinen adıyla 'sa', brute-force saldırılarının birincil hedefidir. Uygulama bağlantılarında sa kullanımı ayrıca en düşük yetki ilkesini ihlal eder.

Öneri: 'sa' hesabını devre dışı bırak veya yeniden adlandır; uygulamalar için ayrı, sınırlı yetkili hesaplar kullan.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
ALTER LOGIN [sa] DISABLE;
-- veya yeniden adlandır: ALTER LOGIN [sa] WITH NAME = [yonetim_hesabi];
```

DÜŞÜK **42. Default trace kapalı** Güvenlik / uyum · sec-default-trace-off

Etki: Default trace, SQL Server'ın maliyeti neredeyse sıfır olan yerleşik iz kaydıdır: nesne oluşturma ve silme, izin değişikliği, dosya büyümesi, yapılandırma değişikliği gibi olayları tutar. Kapalıyken bu olaylar için geriye dönük bakılacak hiçbir kayıt kalmaz — 'bu tablo ne zaman silindi' sorusu cevapsız kalır.

Öneri: Yerine tam kapsamlı bir Extended Events oturumu ya da SQL Server Audit kurulmadıysa default trace'i açın; maliyeti ihmal edilebilir, sağladığı geriye dönük görünürlük yüksektir.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
EXEC sys.sp_configure 'show advanced options', 1; RECONFIGURE;
EXEC sys.sp_configure 'default trace enabled', 1; RECONFIGURE;
```

DÜŞÜK **43. Karşılıksız (orphan) veritabanı kullanıcıları** Güvenlik / uyum · sec-orphaned-users

Etki: Sunucudaki hiçbir login'e karşılık gelmeyen veritabanı kullanıcıları duruyor; genellikle başka bir sunucudan restore edilmiş veritabanından kalır. Tek başına bir açık değildir ama yetki tablosunu kirletir: aynı adla yeni bir login açıldığında beklenmedik biçimde eski izinleri devralabilir.

Öneri: Her birini inceleyin: hâlâ gerekliyse doğru login'e eşleyin, gereksizse silin. Silmeden önce kullanıcının şema ya da nesne sahipliği olup olmadığını kontrol edin.

Tespit edilenler (3)

- ERP_DB · eski_uygulama — karşılığı olan login yok (orphan)
- ARSIV_DB · devir_kullanici — karşılığı olan login yok (orphan)
- RAPOR_DB · test_hesap — karşılığı olan login yok (orphan)

Düzeltme T-SQL — bu örneğe göre otomatik üretildi yalnız gösterim — çalıştırılmaz

```
USE [ERP_DB];
-- Aynı adda bir login varsa eşleyin:
ALTER USER [eski_uygulama] WITH LOGIN = [eski_uygulama];
-- Kullanılmıyorsa (şema/nesne sahipliği yoksa) kaldırın:
-- DROP USER [eski_uygulama];
USE [ARSIV_DB];
-- Aynı adda bir login varsa eşleyin:
ALTER USER [devir_kullanici] WITH LOGIN = [devir_kullanici];
-- Kullanılmıyorsa (şema/nesne sahipliği yoksa) kaldırın:
-- DROP USER [devir_kullanici];
USE [RAPOR_DB];
-- Aynı adda bir login varsa eşleyin:
ALTER USER [test_hesap] WITH LOGIN = [test_hesap];
-- Kullanılmıyorsa (şema/nesne sahipliği yoksa) kaldırın:
-- DROP USER [test_hesap];
```

DÜŞÜK **44. model veritabanı FULL recovery modelinde** Konfigürasyon · sysdb-model-full-recovery

Etki: model FULL olduğunda oluşturulan her yeni veritabanı FULL recovery ile başlar; log yedeği alınmazsa transaction log'lar sessizce şişer.

Öneri: Yeni DB'lerin varsayılan olarak SIMPLE başlamasını istiyorsan model'i SIMPLE'a al; FULL kasıtlıysa log yedek politikasının tüm yeni DB'leri kapsadığından emin ol.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [model] SET RECOVERY SIMPLE;
```

DÜŞÜK **45. Query Store kapalı veritabanları var** Konfigürasyon · cfg-query-store-off

Etki: Query Store kapalıyken sorgu regresyonlarını, plan değişimlerini ve tarihsel performansı analiz etme imkânı kaybedilir — bu ürünün en güçlü sinyallerinden biri.

Öneri: Kritik veritabanlarında Query Store'u aç (READ_WRITE); 2017+ ise wait istatistikleri de toplanır.

Düzeltme T-SQL — bu örneğe göre otomatik üretildi yalnız gösterim — çalıştırılmaz

```
ALTER DATABASE [CRM_DB] SET QUERY_STORE = ON (OPERATION_MODE = READ_WRITE);
ALTER DATABASE [STOK_DB] SET QUERY_STORE = ON (OPERATION_MODE = READ_WRITE);
ALTER DATABASE [LOG_DB] SET QUERY_STORE = ON (OPERATION_MODE = READ_WRITE);
```

BİLGİ **46. Karma kimlik doğrulama modu (bilgi)** Güvenlik / uyum · sec-auth-mode-mixed

Etki: Sunucu SQL login'lerini kabul ediyor. Çoğu ERP ve muhasebe uygulaması bunu gerektirdiği için tek başına bir açık değildir; denetim raporunda kayıt altına alınır. Riski, SQL login'lerinin Active Directory'nin parola politikası, hesap kilitleme ve merkezî devre dışı bırakma yeteneklerinden yararlanamamasıdır — personel ayrıldığında hesabı kapatmak ayrı bir iş olur.

Öneri: Karma mod gerekiyorsa SQL login sayısını en aza indirin, hepsinde CHECK_POLICY açık olsun ve personel erişimini Windows kimlik doğrulaması üzerinden verin. Gerekmiyorsa Windows-only moda geçin.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Bilgi amaçlı bulgudur; otomatik düzeltme önerilmez.
-- Windows-only moda geçiş SSMS sunucu özellikleri ya da Configuration Manager üzerinden yapılır
-- ve servis yeniden başlatma gerektirir. Önce tüm uygulamaların Windows kimlik doğrulamasına
-- geçebildiği doğrulanmalıdır; aksi halde uygulamalar bağlanamaz.
```

BİLGİ **47. Veritabanları diskte şifrelenmemiş — TDE kapalı (bilgi)** Güvenlik / uyum · sec-tde-missing

Etki: Veri dosyaları ve yedekler diskte şifresiz duruyor. Sunucuya sızmadan da veri kaybı mümkündür: kopyalanan bir MDF ya da yedek dosyası başka bir SQL Server'a attach/restore edilerek okunabilir. Yedeklerin şirket dışına çıktığı senaryolarda (bulut, harici disk, kurye) belirleyici olur; kişisel veri barındıran veritabanlarında KVKK açısından da değerlendirilmelidir.

Öneri: Kişisel veri barındıran veritabanları için TDE'yi (SQL 2019+ tüm sürümlerde mevcut) ya da en azından yedek şifrelemesini değerlendirin. Anahtar yönetimi plan gerektirir — sertifika kaybedilirse veri geri dönülemez biçimde kaybolur.

Düzeltme T-SQL yalnız gösterim — çalıştırılmaz

```
-- Bilgi amaçlı bulgudur. TDE, anahtar yönetimi planı olmadan uygulanmamalıdır.
-- Sertifikayı MUTLAKA ayrı ve güvenli bir yerde yedekleyin; sertifika kaybı = veri kaybı.
-- USE master;
-- CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<guclu-parola>';
-- CREATE CERTIFICATE TDE_Sertifika WITH SUBJECT = 'TDE';
-- BACKUP CERTIFICATE TDE_Sertifika TO FILE = 'D:\Keys\TDE_Sertifika.cer'
-- WITH PRIVATE KEY (FILE = 'D:\Keys\TDE_Sertifika.pvk', ENCRYPTION BY PASSWORD = '<guclu-parola>');
-- USE [VeritabaniAdi];
-- CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256 ENCRYPTION BY SERVER CERTIFICATE TDE_Sertifika;
-- ALTER DATABASE [VeritabaniAdi] SET ENCRYPTION ON;
```

Yöntem ve kapsam

Bu rapor 22.07.2026 12:00 tarihli taramadan üretildi. Veriler yalnızca SQL Server'ın kendi yönetim görünümlerinden (DMV), Query Store'dan ve sistem sayaçlarından okundu; hiçbir kullanıcı tablosuna, satırına veya iş verisine erişilmedi. Toplama salt-okunurdur — hiçbir yapılandırma değiştirilmez.

Health Score, yedi kategorinin ağırlıklı bileşimidir: her kategori 100'den başlar, tetiklenen her bulgu önem derecesine göre kendi kategorisinden puan düşer, en ağır bulgu ayrıca toplam skora tavan uygular. Ağırlıklar ve cezalar yapılandırma verisidir; kalibrasyon değiştiğinde skorlar yeniden hesaplanabilir.

Öneri betikleri değişiklik yönetimi süreciniz içinde, test ortamında doğrulandıktan sonra uygulanmalıdır. Bakım penceresi ve yedek gereksinimleri müşteriye özeldir ve bu rapor kapsamında değerlendirilmemiştir.