

RELIABILITY FRIDAY

BLACK FRIDAY EDITION

En büyük kampanyanız,  
en büyük kesintiniz olmasın.

# Black Friday Öncesi Sistem Hazırlığı: Teknik Rehber

TEKNİK REHBER • 24 SAYFA • KASIM 2026

## GİRİŞ

## Kampanya trafiği neden farklıdır?

1961'de Philadelphia polisi, Şükran Günü'nün ertesindeki cumaya "Black Friday" dedi, çünkü şehir kilitleniyordu. Bugün aynı kalabalık ödeme sayfalarını kilitliyor. O yıllarda kalabalık bir cumaya sığıyordu; bugün e-ticarete indirimler kasım boyunca sürüyor ve 11.11, Black Friday ile Cyber Monday bu dönemin en yoğun günleri. Teknik açıdan bu, tek bir peak değil; dört hafta boyunca yüksek seyreden bir baseline ve üstüne binen birkaç peak demektir.

Yüksek trafikli bir dönem, normal günün büyüğü değildir. Trafik aynı anda yükselir, kullanıcı davranışı değişir, third-party limitleri görünür hâle gelir ve küçük gecikmeler retry dalgalarına dönüşür. Her peak'te yükün şekli aynıdır: istekler aynı birkaç akışa (ürün sayfası, sepet, checkout) yığılır, bot trafiği bu yığılmaya eklenir. Application katmanı yatay ölçeklenir; database, session store, stok kilidi ve ödeme entegrasyonu aynı hızda ölçeklenmez. Darboğaz önce bu katmanlarda aranır.

Bu yüzden hazırlık daha fazla CPU veya sunucu ayırmakla bitmez. Ekip, kritik customer journey'lerin beklenen yükte ve öngörülen arızalar altında nasıl davrandığını kanıtlamak zorundadır.

Ayın tamamına yayılan bir kampanya, hazırlığı üç yerden değiştirir:

- **CHANGE FREEZE** Ay boyunca kısıtlı değişiklik, peak günlerinde tam freeze gerekir.  
**TEK HAFTAYA**  
**SIĞMAZ.**
- **KAPASITE** Geçici quota artışları ve autoscaling alt sınırları ay boyu maliyet üretir.  
**HAFTALARCA**  
**YÜKSEK KALIR.**
- **EKIP DÖRT** Tek gecelik bir plan ikinci peak'e yetmez.  
**HAFTA ON-CALL**  
**KALIR.**

2026'da bu günler 11 Kasım Çarşamba (11.11), 27 Kasım Cuma (Black Friday) ve 30 Kasım Pazartesi'ye (Cyber Monday) denk geliyor; Şükran Günü kasımın dördüncü perşembesi, yani 26 Kasım. Takvim bölümü bu tarihlere göre hazırlandı; kendi kampanya takviminize göre kaydırın.

## ÇERÇEVE

## Hazır olmanın tanımı

Bir sistem, normal koşullarda tahmini peak trafiği taşıdığı için hazır sayılmaz. Hazır bir sistem kritik journey'leri hedef SLO içinde sürdürür, en önemli arıza senaryolarında kontrollü biçimde bozulur, overload sırasında kendini korur ve ekibin bildiği süre içinde toparlanır. Bu iddiaların her biri test sonucu, dashboard, runbook veya tatbikat kaydıyla doğrulanır.

Peak güvenilirliği = doğrulanmış kapasite × arıza toleransı × operasyon kabiliyeti

Çarpanlardan biri sıfıra yaklaştığında toplam güvenilirlik de düşer; en küçük doğrulanmış sınır kampanyanın gerçek sınırıdır. Bu yüzden rehber kapasite planlama, performans testi, resilience, graceful degradation, change management ve incident command pratiklerini tek bir çalışma sisteminde birleştirir. Shopify'nin BFCM hazırlık programındaki scale test ve Resiliency Matrix yaklaşımından, Google SRE'nin overload, load shedding, retry ve incident response ilkelerinden, AWS Operational Readiness Review ve Azure mission-critical test pratiklerinden yararlanır; kaynaklar eclit.com'daki web sürümünde.

## Temel ilkeler

| İLKE                                   | OPERASYONEL ANLAMI                                                                                                           |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Kritik journey sistem sınırıdır        | Checkout, ödeme, sipariş oluşturma veya müşteri erişimi gibi iş sonuçları, servis bazında metriklerden önce gelir.           |
| Kanıt hazırlığın para birimidir        | "Hazırız" ifadesi tek başına kabul edilmez; her iddia güncel ve erişilebilir bir kanıta bağlanır.                            |
| Failover kapasitesi peak kapasitesidir | Bir zone, node veya dependency kaybında kalan kapasite talebi taşımıyorsa yedeklilik kâğıt üzerindedir.                      |
| Overload tasarlanır                    | Timeout, retry, concurrency limit, load shedding ve degraded mode önceden belirlenir; incident sırasında keşfedilmez.        |
| Bilinmeyen risk test girdisidir        | Yeni servisler, büyük migration'lar ve geçmiş verisi olmayan akışlar daha yüksek güvenlik payıyla ele alınır.                |
| Değişiklik hızı risk bütçesidir        | Kampanya yaklaştıkça sistemin değişim hızı azaltılır; acil değişiklikler daha dar kapsam ve daha güçlü rollback ile yapılır. |

## Rehber nasıl kullanılır

1. Teknik lider, event owner'ı ve kapsam içindeki kritik customer journey'leri belirler.
2. Her servis sahibi kendi kapasite sınırını, dependency'lerini, failure mode'larını ve kanıtlarını doldurur.
3. Merkezi readiness review, riskleri yedi kanıt kapısı üzerinden değerlendirir.
4. Kırmızı kapılar kapanmadan go kararı verilmez. Amber kapılar için yazılı risk kabulü, tetikleyici eşikler ve geri dönüş planı gerekir.
5. Kampanya sonrasında tahmin ile gerçek karşılaştırılır; kontrol listesi incident bulgularıyla güncellenir.

Kontrol listesi maddeleri dört parçadan oluşur. **Yapılacak:** ne yapılmalı ve hangi araçla. **Nasıl fark edilir:** kontrol atlandığında sorunun ilk görüldüğü yer. **Neden önemli:** kontrolün arkasındaki teknik gerekçe ve kaynağı. **Komut:** örnek değerlerle verilen komutlar; eşikleri kendi SLO'nuza göre değiştirin.

## TAKVİM

## Hazırlık takvimi · Kasım 2026

Önce zemin, sonra iki freeze, arada bir prova.

| NE ZAMAN         | YAPILACAK                                                                                                                | İLGİLİ MADDE   |
|------------------|--------------------------------------------------------------------------------------------------------------------------|----------------|
| Kasım başlamadan | Yük testi, darboğaz listesi, quota ve limit artışları, restore testi, rollback provası                                   | 01, 02, 04, 10 |
| 1–30 Kasım       | Kısıtlı değişiklik dönemi: yalnızca test edilmiş, geri alınabilir ve düşük riskli değişiklikler, yoğun saatlerin dışında | 03             |
| 9–12 Kasım       | 11.11 çevresinde tam change freeze, war room ve canlı SLO takibi                                                         | 03, 05, 06     |

|                     |                                                                  |                      |
|---------------------|------------------------------------------------------------------|----------------------|
| 13–17 Kasım         | 11.11 sonrası ara değerlendirme, düzeltmeler ve ikinci yük testi | 01, 06               |
| 20 Kasım – 1 Aralık | Black Friday ve Cyber Monday için tam change freeze, war room    | 03, 05, 06, 10       |
| 1–4 Aralık          | Geçici kaynakların küçültülmesi ve postmortem                    | 02, kampanya sonrası |

## Peak'e geri sayım

Aşağıdaki geri sayım ilk peak'e (11.11) göredir. Black Friday için aynı döngü, 13–17 Kasım ara değerlendirmesiyle kısaltılmış olarak yeniden koşulur; ilk peak'in bulguları ikincisinin test senaryosudur.

| DÖNEM            | ANA İŞLER                                                                                    | ÇIKIŞ KRITERİ               |
|------------------|----------------------------------------------------------------------------------------------|-----------------------------|
| T-12 – T-8 hafta | Kapsam, event owner, kritik journey'ler, trafik tahmini, dependency map, vendor bildirimleri | Baseline ve risk listesi    |
| T-8 – T-4 hafta  | Servis ve platform testleri, darboğaz düzeltmeleri, quota artışları, observability eksikleri | İlk capacity envelope       |
| T-4 – T-2 hafta  | Full-scale test, failover under load, chaos senaryoları, incident tatbikatı                  | Yük altında recovery kanıtı |
| T-2 – T-1 hafta  | Son düzeltmeler, tekrar testleri, emergency access kontrolü, freeze başlangıcı               | Yedi kapının ilk kararı     |
| T-7 – T-2 gün    | Dress rehearsal, war room provası, dashboard ve iletişim şablonları                          | Go / no-go kararı           |
| T-1 – T-0 gün    | Capacity pre-scale, cache warming, son değişiklik kontrolü, on-call handover                 | Event state                 |
| T+0 – T+3 gün    | Canlı komuta, trend takibi, kontrollü optimizasyon, veri toplama                             | Event log ve karar kaydı    |
| T+3 – T+10 gün   | Tahmin–gerçek karşılaştırması, incident review, kalıcı aksiyonlar                            | Yeni readiness baseline     |

## KARAR

### Yedi kanıt kapısı ve go / no-go

Go veya no-go kararı genel bir kanaate değil, yedi bağımsız kanıt alanına dayanır. Her kapının tek bir sorumlusu, son kanıt tarihi ve açık riskleri vardır. Bir kapının yeşil olması belgesinin var olduğunu değil, içeriğinin güncel ve test edilmiş olduğunu gösterir.

| KAPI         | KARAR SORUSU                                                                  | ASGARI KANIT                        |
|--------------|-------------------------------------------------------------------------------|-------------------------------------|
| 1 · Talep    | Peak, burst, coğrafya, kullanıcı karması ve iş yükü vektörü tahmin edildi mi? | Forecast dosyası ve varsayımlar     |
| 2 · Kapasite | Normal ve arızalı durumda güvenli kapasite ölçüldü mü?                        | Scale test sonuçları ve limitler    |
| 3 · Journey  | Kritik customer journey'ler SLO içinde uçtan uca doğrulandı mı?               | Synthetic test ve journey dashboard |

|                  |                                                                            |                                      |
|------------------|----------------------------------------------------------------------------|--------------------------------------|
| 4 · Dayanıklılık | Önemli failure mode'lar yük altında denendi mi?                            | Game Day kaydı ve Resiliency Matrix  |
| 5 · Koruma       | Timeout, retry, load shedding ve degraded mode mekanizmaları çalışıyor mu? | Konfigürasyon ve overload testi      |
| 6 · Operasyon    | Alarm, runbook, on-call, yetki ve iletişim akışı prova edildi mi?          | Tatbikat ve erişim doğrulaması       |
| 7 · Değişiklik   | Freeze, emergency change ve rollback kuralları uygulanabilir mi?           | Değişiklik takvimi ve rollback testi |

## Durum kuralları

| DURUM   | TANIM                                                                           | KARAR ETKİSİ       |
|---------|---------------------------------------------------------------------------------|--------------------|
| Yeşil   | Kanıt güncel, sahibi belli, hedef karşılanmış, açık yüksek risk yok             | Go                 |
| Amber   | Hedef kısmen karşılanmış veya workaround var; tetikleyici, owner ve süre yazılı | Risk kabulü ile go |
| Kırmızı | Kanıt yok, test başarısız, kritik limit bilinmiyor veya recovery doğrulanmamış  | No-go              |

Ortalama bir readiness skoru kritik bir kırmızıyı gizler. 100 kontrolün 95'inin tamamlanması etkileyici görünür; eksik beş kontrol payment database kapasitesi, WAF fail-open davranışı veya rollback yetkisiyle ilgiliyse sistem hazır değildir. Kapılar birbirini telafi etmez: yönetim özeti renklerle sunulabilir, teknik karar kapı bazında verilir.

## Go / no-go review

Review toplantısının amacı sunum dinlemek değil, eksik kanıt ve kabul edilmemiş riski ortaya çıkarmaktır. Her kapı sahibi üç dakikada hedefi, sonucu, açık riski ve istediği kararı sunar; tartışma kanıt üzerinde yürür. Toplantıya girmeden şunlar hazır olmalı:

- Talep modeli ve marketing campaign takvimi güncel (kanıt: forecast version · sorumlu: event owner)
- Full-scale ve failover under load sonuçları erişilebilir (test run ID · platform)
- Kritik journey SLO dashboard'ları canlı (dashboard URL · journey owner)
- Açık P0/P1 teknik riskler owner ve tarihle listeli (risk register · tech lead)
- Vendor quota ve escalation teyitleri tamam (vendor kaydı · service owner)
- On-call roster, break-glass hesapları ve war room prova edildi (drill log · ops lead)
- Freeze ve emergency change authority duyuruldu (change plan · change owner)

Karar kaydında şu alanlar bulunur: karar (go / koşullu go / no-go), karar zamanı, Event Commander, kırmızı kapılar, kabul edilen amber riskler, koşullar ve son tarih, bir sonraki review.

## No-go kriterleri

- Kritik journey'nin peak test sonucu yok veya SLO karşılanmıyor.
- Tek bir failure domain kaybında kalan doğrulanmış kapasite tahmini peak'in altında.

- Payment, order veya benzeri write akışında idempotency ve reconciliation belirsiz.
- Overload davranışı kontrolsüz retry, sınırsız queue veya process crash üretiyor.
- Kritik dependency için owner, alarm veya çalışır runbook yok.
- Incident response rollerinde veya production erişiminde doğrulanmamış boşluk var.
- Event penceresinde geri döndürülemeyen yüksek riskli migration planlanmış.

## KAPASİTE

## Talep modeli ve capacity envelope

Kapasite tahmini tek bir RPS sayısı değildir. Aynı toplam trafik; cache hit ratio, authenticated kullanıcı oranı, ürün karması, payload boyutu veya checkout dönüşüm oranı değiştiğinde bambaşka bir altyapı yükü üretir. Bu yüzden talep, her kritik journey için çok boyutlu bir iş yükü vektörü olarak modellenir. Kampanyada kullanılabilecek güvenli sınır, en yüksek laboratuvar sonucu değil; planlanan arıza senaryosu ve güvenlik payı düşüldükten sonra kalan doğrulanmış kapasitedir.

### Talep vektörü

| BOYUT             | MODELLENMESİ GEREKEN DAVRANIŞ                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------|
| Trafik şekli      | Baseline, ramp, burst, flash sale, soak ve cooldown ayrı modellenir.                            |
| Kullanıcı karması | Anonymous, authenticated, yeni kullanıcı, bot, partner ve admin trafiği ayrılır.                |
| İşlem karması     | Browse, search, login, cart, checkout, payment, order, webhook ve raporlama oranları yazılır.   |
| Coğrafya          | Bölge, ISP, cihaz ve saat dilimi dağılımı; CDN ve region routing etkisiyle birlikte ele alınır. |
| Veri şekli        | Hot key, popüler ürün, yüksek fan-out sorgu, büyük payload ve cold cache senaryoları eklenir.   |
| Dış sistemler     | Payment, fraud, SMS, e-posta, ERP ve partner API rate limitleri iş yüküne bağlanır.             |

### Temel hesaplar

$$P = \text{baseline} \times \text{büyüme} \times \text{kampanya etkisi} \times \text{belirsizlik katsayısı}$$

Peak tahmini P'de katsayılar aynı veriden türetilmemelidir; aksi hâlde aynı büyüme iki kez sayılır. En iyi, beklenen ve stres senaryoları ayrı tutulur.

$$H = \text{doğrulanmış kapasite} / \text{tahmini peak}$$

Headroom H yalnızca normal durumda değil, kaybedilmesi planlanan en büyük failure domain çıkarıldıktan sonra da hesaplanır.

$$L = \lambda \times W$$

Little's law'a göre sistemdeki ortalama eş zamanlı iş sayısı  $L$ , geliş hızı  $\lambda$  ile sistemde kalma süresi  $W$ 'nin çarpımıdır. Latency iki katına çıkarsa aynı RPS için concurrency de yaklaşık iki katına çıkar; connection pool ve thread pool bu yüzden latency'ye bağlı dolar.

$$\Delta Q = \text{geliş hızı} - \text{işleme hızı}$$

Queue büyümesi  $\Delta Q$ 'daki pozitif fark kısa süreli görünse bile kuyruk yaşını hızla büyütür. Dashboard yalnızca queue depth değil, oldest message age göstermelidir.

## Capacity envelope çalışma tablosu

Her bileşen için iki profil çıkarılır: normal limit ve arıza altı limit. Headroom ikisine göre ayrı hesaplanır.

| BİLEŞEN       | NORMAL LIMIT | ARIZA ALTI LIMIT | PEAK İHTİYAÇ | HEADROOM | DARBOĞAZ SINYALI                   |
|---------------|--------------|------------------|--------------|----------|------------------------------------|
| Edge ve CDN   | ___ RPS      | ___ RPS          | ___ RPS      | ___      | Origin fetch ve WAF latency        |
| Load balancer | ___ conn/s   | ___ conn/s       | ___ conn/s   | ___      | Active connection ve SYN backlog   |
| Application   | ___ RPS      | ___ RPS          | ___ RPS      | ___      | Concurrency ve p99                 |
| Database      | ___ TPS      | ___ TPS          | ___ TPS      | ___      | Lock wait ve replica lag           |
| Cache         | ___ ops/s    | ___ ops/s        | ___ ops/s    | ___      | Eviction ve hit ratio              |
| Queue         | ___ msg/s    | ___ msg/s        | ___ msg/s    | ___      | Oldest message age ve consumer lag |
| Third party   | ___ req/s    | ___ req/s        | ___ req/s    | ___      | 429 ve timeout                     |

## Capacity plan için kırmızı bayraklar

- Autoscaling'in ihtiyaç duyduğu quota ayrılmamış veya scale-out süresi peak ramp süresinden uzun.
- Application instance sayısı artırıldığında database connection pool ve streaming connection toplamı doğrulanmamış.
- Failover region boş görünse de image pull, warm-up, cache fill veya data replication nedeniyle zamanında trafik alamıyor.
- Test anonymous browse ağırlıklı; authenticated checkout, webhook veya admin akışları gerçek oranında temsil edilmiyor.
- Cloud veya CDN sağlayıcısına büyük quota ve kapasite artışı önceden bildirilmemiş.
- Tek sonuç ortalama latency; p99, error rate, saturation ve recovery time raporlanmıyor.

## Kritik customer journey'ler ve SLO

Servisler altyapı organizasyonuna göre bölünür; müşteri deneyimi bu sınırları izlemez. Hazırlığın ana birimi bu yüzden servis değil kritik journey'dir: ürün görüntüle → sepete ekle → ödeme → sipariş onayı. Her journey edge'den veri katmanına ve dış servislere kadar uçtan uca izlenir.

### Journey reliability sheet

Her kritik journey için bir satır doldurulur; boş kalan alan açık risktir.

| ALAN              | DOLDURULACAK BİLGİ                                                                   |
|-------------------|--------------------------------------------------------------------------------------|
| Journey           | Örnek: ürün görüntüle → sepete ekle → ödeme → sipariş onayı                          |
| İş sonucu         | Başarılı sipariş, başarılı giriş, bilet tahsisi veya dosya erişimi                   |
| SLI               | Success rate, p95/p99 latency, correctness, freshness ve queue completion            |
| Event SLO         | Örnek: checkout success $\geq$ %99,5 ve p99 < 2,5 s                                  |
| Peak iş yükü      | RPS, concurrency, payload, kullanıcı karması ve burst süresi                         |
| Dependency'ler    | DNS, CDN, WAF, auth, database, cache, payment, fraud, messaging                      |
| Failure davranışı | Fail closed, fail open, cached response, asynchronous completion veya feature off    |
| Koruma            | Timeout budget, retry budget, circuit breaker, concurrency limit, load shed priority |
| Recovery          | Runbook, rollback, failover ve beklenen toparlanma süresi                            |
| Kanıt             | Test run ID, dashboard URL, Game Day kaydı ve owner                                  |

### SLI seçimi

| SLI          | ÖLÇÜM                                         | DIKKAT                                                               |
|--------------|-----------------------------------------------|----------------------------------------------------------------------|
| Availability | Başarılı ve geçerli yanıt oranı               | HTTP 200 tek başına yeterli değildir; iş sonucu doğrulanır.          |
| Latency      | p50, p95, p99 ve deadline aşımı               | Ortalama, tail latency bozulmasını gizler.                           |
| Correctness  | Doğru fiyat, stok, sipariş veya bakiye        | Hızlı ama yanlış cevap başarısızlıktır.                              |
| Freshness    | Verinin üretim ile görünürlük arasındaki yaşı | ETL ve streaming backlog müşteri etkisine çevrilir.                  |
| Durability   | Kabul edilen işlemin kaybolmaması             | Acknowledgement öncesi persistence noktası bilinmelidir.             |
| Completion   | Asenkron işin hedef sürede tamamlanması       | Queue depth yerine oldest message age ve completion latency izlenir. |

### Synthetic transaction tasarımı

- Shallow probe yalnızca endpoint erişimini kontrol eder; deep probe gerçek iş sonucunu doğrular. İkisi farklı alarmlara bağlanır.

- Test kullanıcısı, ürün ve ödeme verisi peak sırasında tükenmeyecek ve gerçek müşteriyle çakışmayacak şekilde ayrılır.
- Synthetic transaction farklı region ve ISP noktalarından çalışır. İçeriden başarılı görünen servis dış kullanıcı için erişilemez olabilir.
- Canary sonucu genel error rate içinde kaybolmaz; bağımsız metric ve alarmı bulunur.
- Her kritik journey dashboard üzerinde tek satırda success, latency, volume ve saturation ile görünür.

## KONTROL LİSTESİ

## Kontrol listesi · 01–03 · Yük testi, limitler ve değişiklik politikası

## 01 Peak yükü kampanyadan önce siz üretin

Gerçek kullanıcı yolunu (ana sayfa, arama, ürün, sepet, checkout) izleyen bir senaryoyu, beklenen peak istek hızının üzerine çıkarak çalıştırın. k6, JMeter, Locust ya da Gatling bu iş için yeterli. Ortalama yerine p95 ve p99 latency'ye, error rate'e, database connection sayısına ve queue depth'e bakın. Testi CDN ve WAF arkasından da koşun, çünkü kampanya günü trafik oradan gelecek. Başarılı bir test yalnızca hedef RPS'ye ulaşmaz; sistem sınırını, sınırın yaklaştığını gösteren sinyalleri, sınır aşıldığında müşterinin gördüğü davranışı ve yük düştüğünde toparlanma süresini ortaya çıkarır. Her test bir hipotezle başlar ve yeniden üretilebilir bir sonuçla biter.

| TEST                   | AMAÇ                                              | RAPORLANACAK ÇIKTI                               |
|------------------------|---------------------------------------------------|--------------------------------------------------|
| Baseline               | Normal üretim karmasını doğrula                   | Mevcut p50/p95/p99 ve resource cost              |
| Ramp                   | Autoscaling ve warm-up davranışını ölç            | Scale trigger ve ready-to-serve süresi           |
| Peak                   | Tahmini peak'i hedef SLO ile taşı                 | Journey SLO ve saturation                        |
| Burst                  | Ani flash sale veya push trafiğini uygula         | Queue spike ve load shed başlangıcı              |
| Soak                   | Uzun süreli yükte leak ve birikimi bul            | Memory, GC, connection ve backlog trendi         |
| Stress                 | Breaking point ve bozulma şeklini bul             | İlk limit ve müşteri etkisi                      |
| Failover under load    | Peak yükte zone, region veya node kaybet          | Recovery time ve kalan headroom                  |
| Dependency degradation | Latency, timeout, 429 ve partial error enjekte et | Retry amplification ve circuit breaker davranışı |
| Recovery               | Yük veya arıza sonrası normale dönüşü ölç         | Backlog drain ve reentry davranışı               |

GERÇEKÇİ  
TRAFİK  
ÜRETİMİ.

Open workload model kullanın: yeni istekler önceki yanıtın bitmesini beklemez, böylece latency artarken yük kaybolmaz; gerçek internet trafiği de böyle davranır. Kullanıcı akışlarını production oranlarına göre ağırlıklandırın; nadir ama pahalı akışları ayrıca stress senaryosuna alın. Cache warm ve cold durumlarını ayrı koşun; cache busting yalnızca bilinçli bir senaryo olarak kullanılır. Test verisi hot key, kampanya ürünü, yüksek fan-out ve gerçek payload boyutlarını kapsasın. Load generator kapasitesini hedefin üstünde doğrulayın; generator saturation sistem limiti sanılmamalıdır. Third-party sistemlere gerçek zarar verecek çağrı yapılmaz; mock, sandbox veya önceden onaylı limit kullanılır.

```
// k6 · örnek değerler: hedef hızı ve eşikleri kendi peak trafiğinize ve SLO'nuza göre ayarlayın.
import http from 'k6/http';

export const options = {
  scenarios: {
    kampanya: {
      executor: 'ramping-arrival-rate', // open workload model
      startRate: 50,
      timeUnit: '1s',
      preAllocatedVUs: 200,
      maxVUs: 2000,
      stages: [
        { target: 600, duration: '10m' }, // peak hıza çık
        { target: 600, duration: '20m' }, // peak'te kal
      ],
    },
  },
  thresholds: {
    http_req_duration: ['p(95)<800'], // milisaniye
    http_req_failed: ['rate<0.01'],
  },
};

export default function () {
  // Gerçek senaryoda ana sayfa → arama → ürün → sepet → checkout adımları sırayla çağrılır.
  http.get('https://staging.example.com/urun/123');
}
```

javascript

NASIL FARK  
EDİLİR

Dashboard'lar normal görünürken müşteri hizmetlerine "ödeme sayfası dönüp duruyor" şikâyetleri gelmeye başlar.

## NEDEN ÖNEMLİ

Ortalama, kuyrukta bekleyen isteklerin yaşadığı gecikmeyi gizler; p95 ve p99 onu gösterir. Örnekteki eşikler şunu söyler: her 20 istekten en fazla biri 0,8 saniyeyi geçebilir, her 100 istekten en fazla biri hata alabilir. Closed model ile warm cache üzerinde geçen bir test, gerçek peak'i temsil etmeyebilir.

TEST KABUL  
KRITERİ.

Test ancak şu altı kanıt varsa geçmiş sayılır:

- Kritik journey SLO'ları test boyunca karşılandı (run raporu ve dashboard snapshot · journey owner)
- Normal ve failure senaryosu ayrı raporlandı (iki kapasite profili · platform)
- İlk saturation noktası ve leading indicator belirlendi (grafik ve threshold · servis owner)

- Retry ve timeout davranışı downstream yüküyle birlikte ölçüldü (attempt histogramı · app owner)
- Test sonrası backlog hedef sürede boşaldı (queue age trendi · data owner)
- Bulgular düzeltildi ve aynı senaryo yeniden koşuldu (karşılaştırmalı run ID · event owner)

Test raporunda aynı zaman ekseninde şu grafikler bulunur: offered load, accepted load ve completed business transaction; journey success rate ile p50/p95/p99 latency; CPU'nun yanında concurrency, connection, queue age, database wait, cache hit ve third-party error; autoscaler desired / ready / serving instance sayıları ve warm-up süresi; failure injection, operatör aksiyonu, recovery başlangıcı ve tam recovery zaman damgaları.

## 02 Quota ve limitleri tek tabloda toplayın

Cloud hesabınızdaki vCPU, IP adresi, load balancer ve NAT gateway quota'larını yan yana yazın. Yanına database'in max\_connections değerini, application'ın connection pool boyutunu ve firewall'un concurrent session ile saniyedeki yeni bağlantı (CPS) limitlerini ekleyin. Autoscaling'ın üst sınırının bu limitlere sığdığını doğrulayın. Capacity envelope tablosundaki "normal limit" sütunu bu listeden doldurulur.

```
# AWS: EC2 quota'ları
aws service-quotas list-service-quotas --service-code ec2 --output table

# Azure: bölgedeki vCPU kullanımı ve limitleri
az vm list-usage --location westeurope --output table
```

bash

```
-- PostgreSQL: anlık connection sayısı ve üst sınır
SELECT count(*) FROM pg_stat_activity;
SHOW max_connections;
```

sql

### NASIL FARK EDİLİR

Autoscaling yeni sunucu açmaya çalışır ama açamaz; konsolda tek satırlık bir quota hatası durur. Ya da sunucular açılır ama database "too many connections" hatası vermeye başlar.

### NEDEN ÖNEMLİ

Autoscaling yalnızca quota kadar büyür ve her yeni application instance'ı kendi connection pool'unu getirir. Bunu restorandaki masalar gibi düşünün: her sunucu kendi rezervasyonu gelir, restoranın masa sayısı (max\_connections) ise değişmez; masalar dolunca database yeni bağlantıları reddeder. Connection pool toplamı instance sayısı ile çarpılıp database'in connection bütçesine bağlanır. Quota artışı sağlayıcı onayı gerektirebilir; talebi kasımdan önce açın ve bütçe alarmlarını artırılmış quota'lara göre güncelleyin.

## 03 Değişiklikleri ay boyunca kısıtlayın, peak'lerde dondurun

Kasım boyunca production'a yalnızca test edilmiş, geri alınabilir ve düşük riskli değişiklikler çıksın, onlar da yoğun saatlerin dışında. Peak günlerinin çevresinde (takvimdeki iki freeze dönemi) tam change freeze uygulayın. Kapsamı yazılı olsun: application release'leri, Infrastructure as Code (Terraform vb.) değişiklikleri, database schema değişiklikleri, WAF ve CDN kuralları. Freeze sistemi dokunulmaz yapmak değildir; amaç değişiklik sayısını azaltmak, istisnaları görünür kılmak ve rollback kapasitesini korumaktır.

| DÖNEM               | POLİTİKA              | İZİN VERİLEN DEĞİŞİKLİK                                                    | KAMPANYA TAKVİMİNDEKİ KARŞILIĞI              |
|---------------------|-----------------------|----------------------------------------------------------------------------|----------------------------------------------|
| T-4 – T-2 hafta     | Feature freeze        | Kullanıcı davranışını değiştirmeyen, test edilmiş reliability düzeltmeleri | Ekim sonu – kasım başı                       |
| T-2 hafta – T-3 gün | Code ve config freeze | Yalnızca event riskini düşüren ve rollback'i doğrulanmış değişiklik        | 1-30 Kasım kısıtlı değişiklik                |
| T-72 – T-0 saat     | Strict freeze         | Incident Commander veya change authority onaylı acil değişiklik            | 9-12 Kasım ve 20 Kasım – 1 Aralık tam freeze |
| Peak sırasında      | Live change control   | Ölçülebilir tetikleyiciye bağlı, küçük blast radius ve anlık gözlem        | 11.11, Black Friday, Cyber Monday            |
| T+0 – T+3 gün       | Controlled thaw       | Trafik normale döndükten ve backlog boşaldıktan sonra aşamalı              | 13-17 Kasım ve 1-4 Aralık                    |

EMERGENCY  
CHANGE KAYDI.

Freeze sırasında her istisna şu alanları doldurur: trigger (hangi metric ve eşik değişikliği gerektiriyor), hipotez (müşteri etkisini hangi mekanizmayla azaltacak), blast radius (hangi region, tenant, endpoint veya trafik yüzdesi), validation (ilk 5, 10 ve 20 dakikada hangi metrikler izlenecek), rollback (tek adım, owner, süre ve geri dönüş eşiği), approver (IC ve teknik owner; güvenlik etkisi varsa security owner), kayıt (zaman damgası, commit veya config ve sonuç).

CANARY VE  
ROLLBACK  
KURALLARI.

Canary yalnızca error rate ile değil kritik journey success, tail latency ve saturation ile değerlendirilir; canary gerçek trafik karmasını temsil etmiyorsa sonuç genellenmez. Rollback yeni deploy kadar test edilir; schema veya data migration geri dönüşü imkânsızsa forward-fix planı ve koruma modu bulunur. Config değişikliği de kod gibi versiyonlanır, peer review ve audit edilir. Peak sırasında aynı anda birden fazla hipotez değiştirilmez; aksi hâlde hangi değişikliğin sonucu etkilediği bilinemez.

NASIL FARK  
EDİLİR

Kesinti, kampanyadan bir gün önce yapılan "küçük" bir konfigürasyon değişikliğinin ardından başlar ve war room'daki ilk soru "en son ne değişti?" olur.

## NEDEN ÖNEMLİ

Google'ın SRE kitabına göre kesintilerin yaklaşık %70'i canlı sistemde yapılan bir değişiklikten kaynaklanır. Ayın tamamını dondurmak ise başka bir risk yaratır: değişiklikler birikir ve aralıkta tek seferde, daha büyük bir release olarak çıkar. Kısıtlı değişiklik ile peak freeze'i bu iki riski dengeler. Reliability Friday serimizin kuralı da bu: Don't Deploy on Friday. Verify on Friday.

## KONTROL LİSTESİ

## Kontrol listesi · 04-06 · Restore, synthetic monitoring ve on-call

## 04 Yedeği değil, restore'u ölçün

Kritik database'leri en son yedekten bir test ortamına restore edin. İki süreyi ayrı ölçün: verinin geri yüklenme süresi ve application'ın yeniden sipariş alabildiği ana kadar geçen süre. Point-in-time recovery (PITR) kullanıyorsanız belirli bir saate dönmeyi de deneyin ve sonuçları RPO ve RTO hedeflerinizle

karşılaştırın. Kanıt, yedeğin varlığı değil; son test kaydındaki restore süresi ve doğrulanmış veri bütünlüğüdür.

**NASIL FARK  
EDİLİR**

Backup dashboard'u aylardır yeşildir. Restore ilk kez gerçek bir arızada denenir ve planlanandan saatler sonra biter.

**NEDEN ÖNEMLİ**

Eksik WAL ya da binlog dosyaları, erişilemeyen encryption key'ler ve sürüm uyumsuzlukları ancak restore sırasında ortaya çıkar. Kampanya gününde kaybedilen her dakika, sıradan bir gündekinden daha çok siparişe mal olur.

## 05 Müşterinin yolunu synthetic check'lerle izleyin

Ana sayfa, arama, sepete ekleme ve ödeme adımlarını dışarıdan, birden fazla bölgeden ve dakikada bir deneyen synthetic check'ler kurun. Alarmları CPU ve memory eşiklerine değil SLO'ya bağlayın: örneğin ödeme adımında beş dakikalık pencerede error rate ve p95 latency. Synthetic transaction tasarımı için bir önceki bölümdeki beş kural geçerlidir.

```
# Basit bir endpoint kontrolü: HTTP kodu ve toplam süre
curl -s -o /dev/null -w '%{http_code} %{time_total}s\n' https://www.example.com/sepet
```

**bash**

Observability tarafında kampanya öncesi şu altı kontrol kapatılır:

- Dashboard RED ve USE metriklerini kritik journey'lerle aynı zaman ekseninde gösteriyor.
- Telemetry pipeline peak yükte çalışıyor; log hacmi ve cardinality limiti incident anında körlük yaratmıyor.
- Alarm SLO tehdidine ve aksiyona bağlı; noisy alarm'lar kampanya öncesi temizlendi.
- Third-party dependency, quota, certificate, replication ve queue age için leading indicator alarmı var.
- Deploy, config, failover ve marketing push grafiklere event marker olarak düşüyor.
- War room için tek ekranlık executive view ile derin teknik dashboard'lar ayrılmış.

**NASIL FARK  
EDİLİR**

Altyapı dashboard'ları yeşilken siparişler düşer. Sorunu ilk siz değil, sosyal medyada şikâyet eden müşteri fark eder.

**NEDEN ÖNEMLİ**

Altyapı metrikleri nedeni gösterir; synthetic check ve SLO alarmı ise müşterinin yaşadığı sonucu.

## 06 On-call'u dört haftaya, runbook'u kampanya saatlerine göre planlayın

Kampanya ayı için on-call rotasyonunu, escalation matrisini ve kritik senaryolar için kısa runbook'ları hazırlayın. Ödeme sağlayıcısı yavaşlarsa, database connection'ları dolarsa ya da CDN hata dönerse ilk üç adım ne? Rollback, kampanyayı durdurma ve müşteriye duyuru kararlarının kimde olduğunu yazın. Aynı kişinin hem sistemi düzeltmeye hem koordinasyon yapmaya hem de paydaşları bilgilendirmeye çalışması response kalitesini düşürür; roller olay başlamadan atanır ve dress rehearsal sırasında prova edilir.

ROL

SORUMLULUK

ARAYÜZ

|                         |                                                           |                                     |
|-------------------------|-----------------------------------------------------------|-------------------------------------|
| Event Commander         | Genel event durumu, go / no-go, risk kabulü ve öncelikler | Business ve teknik liderlik         |
| Incident Commander (IC) | Incident ilanı, koordinasyon, rol atama ve karar kontrolü | Tüm response ekipleri               |
| Operations Lead         | Mitigation, teknik workstream ve runbook uygulaması       | Servis ve platform owner'ları       |
| Communications Lead     | İç ve dış güncelleme, müşteri ve status iletişimi         | CSM, support, marketing, leadership |
| Scribe                  | Zaman damgası, hipotez, aksiyon, owner ve sonuç kaydı     | IC                                  |
| Business Liaison        | Müşteri etkisi, gelir ve kampanya önceliği                | Business owner                      |

Bu rol dağılımı bir örnektir; kendi organizasyonunuzda roller birleşebilir veya farklı adlanabilir.

### Incident ilan tetikleyicileri

| TETİKLEYİCİ                                             | AKSIYON                                                  |
|---------------------------------------------------------|----------------------------------------------------------|
| Kritik journey SLO iki ardışık ölçüm penceresinde ihlal | Incident ilan et ve IC ata                               |
| Error rate normalin 3 katı ve yükseliyor                | İlgili owner ile teknik workstream aç                    |
| Arıza altı capacity headroom %10'un altına düştü        | Degradation veya traffic control başlat                  |
| Queue oldest age recovery SLO'yu aşacak trendde         | Ingest limit veya consumer recovery planı                |
| Third-party 429 veya timeout hızla artıyor              | Retry budget'ı düşür ve fallback'i değerlendir           |
| Telemetry kaybı kritik journey'yi görünmez yaptı        | Riski yükselt, değişikliği durdur, bağımsız probe kullan |

### WAR ROOM ÇALIŞMA DÜZENİ.

Tek karar kanalı, tek incident kaydı ve sabit conference bridge kullanılır. Her aksiyon owner ve zaman damgasıyla yazılır; sonucu gelmeden aynı hipotez unutulmaz. Teknik ekipler thread veya ayrı workstream'de çalışır, kararlar ana kanalda özetlenir. Güncelleme ritmi önceden belirlenir; yeni bilgi yoksa bile durum ve bir sonraki kontrol zamanı yazılır. IC sistemi düzeltmeye dalmaz; koordinasyon, öncelik ve iletişim kontrolünü korur. Recovery ilanı tek metriğe dayanmaz: journey SLO, backlog, saturation ve error trendi birlikte normale dönmelidir.

### Event dashboard yerleşimi

| BÖLÜM             | GÖSTERİLECEK METRIKLER                                                  |
|-------------------|-------------------------------------------------------------------------|
| Business outcome  | Sipariş, ödeme, login, active user ve başarısız iş sonucu               |
| Critical journeys | Success rate, p95/p99 latency ve volume                                 |
| Traffic           | Offered, accepted, shed, bot ve retry trafiği                           |
| Capacity          | Headroom, concurrency, ready instance, database saturation ve queue age |
| Dependencies      | Third-party success, latency, 429 ve region health                      |

Change markers Deploy, config, failover, feature flag ve marketing push

Incident Severity, owner, başlangıç zamanı, son update ve next update

#### NASIL FARK EDİLİR

Gece 02.00'de alarm çalar. Telefonu açan kişi, ödeme sağlayıcısında kime ulaşacağını ve kampanyayı durdurma yetkisinin kimde olduğunu bilmez.

#### NEDEN ÖNEMLİ

Olay anında aranan her bilgi müdahale süresine eklenir. Rotasyon ve runbook, yorgun bir ekibin de aynı adımları atabilmesini sağlar.

#### KONTROL LİSTESİ

## Kontrol listesi · 07–10 · Dış servisler, botlar, tarihler ve kill switch

### 07 Dış servislere timeout, retry budget ve circuit breaker koyun

Ödeme, 3D Secure, SMS ile doğrulama (OTP), kargo, stok ve e-posta entegrasyonlarını listeleyin. Her çağrı için açık bir timeout ve jitter'lı exponential backoff ile sınırlı retry tanımlayın. Ardından bir circuit breaker ve bir fallback davranışı ekleyin: kuyruğa alma, alternatif sağlayıcı ya da kullanıcıya net bir mesaj. Ödeme çağrılarında idempotency key kullanın. Overload sırasında amaç bütün istekleri kabul etmek değil, sistemin çökmesini önlerken en değerli müşteri işlemlerini tamamlamaktır; bu kontroller upstream'den downstream'e tutarlı çalışmalı, autoscaling, load balancing ve load shedding birbirine zıt sinyal üretmemelidir.

#### TIMEOUT BUDGET.

Bir müşteri isteğinin toplam deadline'ı, zincirdeki her çağrıya bağımsız ve daha uzun timeout vermekle korunamaz. Her hop kalan budget'ı bilmeli; artık kullanıcıya fayda üretmeyecek iş başlanmamalı veya iptal edilmelidir. Client vazgeçtikten sonra server tarafta devam eden iş, görünmeyen yükü büyütür. Aşağıdaki dağılım bir örnektir; değerler journey SLO'nuzdan türetilir.

| KATMAN          | ÖRNEK BUDGET | KURAL                                                            |
|-----------------|--------------|------------------------------------------------------------------|
| Client toplam   | 2 000 ms     | Kullanıcı beklentisi ve journey SLO'dan türetilir                |
| Edge ve network | 200 ms       | Tekrar DNS veya TLS maliyeti hesaba katılır                      |
| Application     | 1 400 ms     | Alt çağrı budget'larının toplamı değil kritik yol dikkate alınır |
| Database        | 350 ms       | Query timeout, transaction sınırından kısa olur                  |
| Recovery payı   | 50 ms        | Yanıt serileştirme ve iptal için bırakılır                       |

#### RETRY BUDGET.

Retry kapasite üretmez; yalnızca geçici ve lokal hataların başka bir denemede başarılı olma olasılığını kullanır. Birden fazla katmanda bağımsız retry yapılırsa tek kullanıcı işlemi katlanarak büyür: üç katmanın her biri ilk deneme dâhil dört attempt yaparsa database'e kadar  $4^3$ , yani 64 attempt oluşabilir. Bu yüzden retry tek bir kontrollü katmanda, exponential backoff ve jitter ile, açık bir bütçe içinde yapılır.

| DURUM     | ÖRNEK                                                       | DAVRANIŞ                  |
|-----------|-------------------------------------------------------------|---------------------------|
| Retriable | Geçici connection reset, seçili 5xx, lokal backend overload | Sınırlı attempt ve jitter |

|                 |                                                                    |                                    |
|-----------------|--------------------------------------------------------------------|------------------------------------|
| Non-retriable   | Validation error, auth failure, malformed request, business reject | Hemen döndür                       |
| Global overload | Yüksek retry ratio, tüm backend'lerde saturation                   | Retry'ı durdur ve load shed et     |
| Write operation | Payment veya order create                                          | Idempotency key olmadan retry etme |

#### NASIL FARK EDİLİR

Çağrı merkezine aynı cümle gelmeye başlar: "Kartımdan para çekildi ama siparişim görünmüyor."

#### NEDEN ÖNEMLİ

Timeout tanımlanmamış ya da çok uzun bırakılmış bir çağrı, yavaş bir dış servis yüzünden thread'leri ve connection'ları tutar; kuyruk büyür ve sağlıklı istekler de yavaşlar. Sınırsız retry, yavaşlayan servise giden yükü katlayıp kesintiye çevirir. Ödeme çağrısını idempotency key olmadan yeniden denemek çift tahsilat riski doğurur. Circuit breaker evdeki sigorta gibi çalışır: arıza tek bir odada kalır, bütün ev kararmaz.

## 08 Bot trafiğini ödeme akışından ayırın

WAF'ta bot management ve rate limiting kurallarını endpoint bazında ayarlayın: login, sepet, stok sorgusu ve ödeme için ayrı limitler. Credential stuffing ve kart testi (card testing) saldırılarını yakalamak için login ve ödeme endpoint'lerinde başarısız deneme oranını izleyin. DDoS korumanızın application katmanını (L7) da kapsadığını doğrulayın. Rate limit global, tenant ve endpoint seviyesinde iş önceliğine göre uygulanır; bot davranışını normal müşteri burst'ünden ayıran kuralların false positive riski kampanya öncesi test edilir. Her güvenlik kontrolü için fail-open veya fail-closed kararı yazılı ve onaylı olmalı; fraud kontrollerinin latency'si ve fail mode'u ödeme journey'siyle birlikte test edilmelidir. Privileged access, break-glass hesapları, MFA ve audit kayıtları ile security kural değişiklikleri için emergency rollback ve iletişim owner'ı da bu maddenin parçasıdır.

#### NASIL FARK EDİLİR

Kampanya ürünü, gerçek müşteriler sepete ulaşmadan "tükendi" görünür.

#### NEDEN ÖNEMLİ

Imperva'nın 2026 Bad Bot Report'una göre web trafiğinin yarısından fazlası (%53) botlardan geliyor. Ayıklanmayan her bot isteği, gerçek müşterilerle aynı connection pool'u, aynı stok sorgusunu ve aynı ödeme limitini kullanır.

## 09 Certificate, domain, DNS ve disk tarihlerini kontrol edin

Kasım içinde süresi dolacak TLS certificate'larını ve domain'leri kampanya başlamadan yenileyin; certificate yenilemeyi ACME ile otomatikleştirin. Secret, license ve token expiry tarihlerinin de event penceresi dışında olduğunu doğrulayın. Kampanya sırasında trafik yönlendirmesi planlıyorsanız DNS TTL değerlerini önceden düşürün. Log ve metric hacmi haftalarca yüksek kalacağı için disk doluluk alarmlarını, log rotation'ı ve retention sürelerini gözden geçirin.

```
# Certificate'ın bitiş tarihi
echo | openssl s_client -servername www.example.com -connect www.example.com:443 2>/dev/null |
openssl x509 -noout -enddate

# DNS kaydının TTL değeri (ikinci sütun)
dig +noall +answer www.example.com
```

bash

**NASIL FARK  
EDİLİR**

Bir sabah mobil uygulama ve API istemcileri aynı anda bağlantı hatası verir, tarayıcı kırmızı bir güvenlik uyarısı gösterir. Ya da loglarla dolan bir disk yüzünden servis yazamaz hâle gelir ve durur.

**NEDEN ÖNEMLİ**

CA/Browser Forum kararıyla 15 Mart 2026'dan bu yana verilen ve tarayıcıların güvendiği TLS certificate'ları en fazla 200 gün geçerli; her certificate yılda en az iki kez yenilenmeli. 15 Mart 2027'de süre 100 güne, 15 Mart 2029'da 47 güne inecek ve yenileme yılda yaklaşık sekiz kereye çıkacak.

**10 Kill switch ve virtual waiting room hazırlayın**

Yük altında kapatılabilecek bileşenleri (öneri motoru, canlı stok sayaçları, kişiselleştirme, ağır raporlar) feature flag ile tek hamlede kapatılabilir hâle getirin. Ödeme akışını en üstte tutan bir öncelik sırası belirleyin. Kapasite sınırına yaklaşıldığında devreye girecek bir virtual waiting room eşiği tanımlayın. Feature flag ve kill switch tek owner'a bağlı olmamalı; audit ve rollback adımları bulunmalı.

**Load shedding önceliği**

| ÖNCELİK | İŞ SINIFI                                        | OVERLOAD DAVRANIŞI                                |
|---------|--------------------------------------------------|---------------------------------------------------|
| P0      | Ödeme doğrulama, sipariş kaydı, kimlik doğrulama | En son shed edilir; ayrılmış concurrency kullanır |
| P1      | Sepet, stok kontrolü, fiyat                      | Degraded response veya kısa cache kullanılabilir  |
| P2      | Arama, öneri, kişiselleştirme, yorumlar          | Daha ucuz sonuç veya feature off                  |
| P3      | Raporlama, export, webhook replay, batch         | Ertelenir veya queue'ya alınır                    |
| P4      | Crawler, bot ve düşük değerli otomasyon          | Rate limit veya erken reject                      |

**Graceful degradation kataloğu**

| MEKANİZMA         | ÖRNEK                              | KORUDUĞU KAYNAK            | RISK                     |
|-------------------|------------------------------------|----------------------------|--------------------------|
| Feature disable   | Recommendation'ı kapat             | CPU ve downstream QPS      | Dönüşüm etkisi           |
| Stale cache       | Son bilinen katalog verisi         | Database read              | Freshness ve correctness |
| Reduced result    | Daha az arama sonucu               | CPU, memory, network       | Deneyim kalitesi         |
| Async completion  | Bildirim veya raporu ertele        | Senkron latency            | Backlog büyümesi         |
| Admission control | Concurrency üstünü reddet          | Thread, connection, memory | Kontrollü 429            |
| Traffic partition | Premium veya kritik müşteri havuzu | Ayrılmış kapasite          | Adalet ve sözleşme       |

**NASIL FARK  
EDİLİR**

Yük arttığında ödeme sayfası da yavaşlar, çünkü ağır bileşenlerle aynı kaynakları paylaşır ve onları kapatacak bir düğme yoktur.

**NEDEN ÖNEMLİ**

Graceful degradation, tam kesintiyle kısmi hizmet arasındaki farktır. Öneri motoru kapanırsa müşteri fark etmeyebilir, ödeme kapanırsa fark eder. Virtual waiting room bankadaki sıra numarası gibidir: kimse geri çevrilmez, ama herkes içeri aynı anda girmez.

## DAYANIKLILIK

## Dependency ve failure modeli

Dependency haritası yalnızca servislerin birbirini çağırdığını gösterirse yetersiz kalır. Her bağlantı için failure semantics yazılır: timeout olduğunda ne olur, retry kimde yapılır, stale veri kabul edilir mi, startup dependency yoksa servis açılır mı ve dependency geri geldiğinde trafik nasıl toparlanır?

### Resiliency Matrix

Shopify'ın yüksek trafikli etkinlikler için kullandığı Resiliency Matrix, her arıza senaryosunda müşterinin hangi journey'leri hangi kalitede tamamlayabildiğini tek tabloda gösterir. Tabloyu doldurmak başlı başına bir tabletop exercise'dır; satırları ve sütunları taramak sistemin en kırılgan yerini gösterir. Aşağıdaki hücreler örnektir; kendi dependency'lerinize göre doldurun.

| FAILURE SENARYOSU        | BROWSE | LOGIN  | CHECKOUT | SIPARIŞ   | BEKLENEN DAVRANIŞ                       |
|--------------------------|--------|--------|----------|-----------|-----------------------------------------|
| CDN cache miss artışı    | Yavaş  | Normal | Normal   | Normal    | Origin protection ve request coalescing |
| Auth latency yüksek      | Normal | Yavaş  | Kısmi    | Normal    | Deadline ve sınırlı retry               |
| Primary database kaybı   | Cached | Kısmi  | Kapalı   | Asenkron  | Failover ve write fence                 |
| Payment provider timeout | Normal | Normal | Kısmi    | Pending   | Idempotency ve reconciliation           |
| Kafka consumer lag       | Normal | Normal | Normal   | Gecikmeli | Backlog age SLO ve consumer scale       |
| Bir region kaybı         | Normal | Normal | Normal   | Normal    | Önceden ayrılmış failover capacity      |

### Failure mode kaydı

Matristeki her hücrenin arkasında sekiz sorusu cevaplanmış bir kayıt bulunur.

| ALAN               | SORU                                                                         |
|--------------------|------------------------------------------------------------------------------|
| Trigger            | Hangi arıza veya eşik bu durumu başlatır?                                    |
| Detection          | Hangi metric veya synthetic test bunu kaç dakikada algılar?                  |
| Blast radius       | Hangi müşteri segmenti, region veya journey etkilenir?                       |
| System response    | Otomatik koruma mekanizması ne yapar?                                        |
| Operator action    | Hangi owner hangi runbook adını uygular?                                     |
| Recovery condition | Servisin sağlıklı kabul edilmesi için hangi göstergeler gerekir?             |
| Reentry risk       | Trafik geri verildiğinde cache fill, retry veya rebalance dalgası oluşur mu? |
| Evidence           | Bu davranış en son ne zaman ve hangi yükte test edildi?                      |

## Test edilecek failure sınıfları

| SINIF           | ÖRNEKLER                                                                          |
|-----------------|-----------------------------------------------------------------------------------|
| Capacity        | CPU, memory, connection, thread, file descriptor, IOPS, quota ve queue saturation |
| Latency         | Dependency yavaş ama erişilebilir; timeout zinciri ve concurrency büyümesi        |
| Partial failure | Node, zone, shard, partition veya müşteri segmenti bazında hata                   |
| Data            | Replica lag, stale cache, poison message, duplicate ve out-of-order event         |
| Network         | Packet loss, DNS sorunu, MTU, latency, partition ve asymmetric routing            |
| Control plane   | Autoscaler, orchestrator, config store, IAM veya deployment sistemi sorunu        |
| Third party     | 429, timeout, invalid response, schema change veya hard outage                    |
| Human           | Yanlış config, eksik yetki, hatalı dashboard ve runbook sapması                   |

Her Game Day senaryosu için kart şu alanları taşır: hipotez, başlangıç yükü, enjekte edilen arıza, beklenen müşteri davranışı, beklenen alarm ve otomasyon, abort kriteri, gözlenen davranış, recovery süresi, bulgular ve owner.

### KATMANLAR

## Teknik katman kontrolleri

Aşağıdaki kontroller servis sahiplerinin kendi alanlarında doğrulaması gereken minimumlardır. Her kontrol bir evidence link, owner ve son doğrulama tarihiyle tutulur. Observability ve security kontrolleri 05 ve 08 numaralı maddelerde yer aldığı için burada tekrarlanmadı.

### DNS, CDN, WAF ve edge

- DNS TTL, secondary DNS ve registrar erişimi doğrulandı; acil değişiklik yetkisi test edildi.
- CDN cache key, TTL, stale-if-error, origin shield ve request coalescing davranışları ölçüldü.
- Cold cache ve cache purge sonrası origin kapasitesi test edildi.
- WAF rule evaluation, bot management, DDoS profili ve rate limit kapasitesi peak'e göre ayarlandı.
- TLS handshake, certificate expiry, OCSP ve connection reuse metrikleri dashboard'da.

### Network ve load balancer

- New connection rate, active connection, SYN backlog, ephemeral port ve NAT table kapasitesi ölçüldü.
- Health check, application'ın gerçekten trafik alabilir olduğunu ölçüyor; warm-up bitmeden node healthy sayılmıyor.
- Connection draining ve keepalive süreleri deploy, scale ve failover davranışıyla uyumlu.
- Zone veya region kaybında routing convergence ve session stickiness etkisi test edildi.

- Load shedding hataları load balancer tarafından başarı gibi yorumlanmıyor; feedback loop kontrol edildi.
- Bandwidth yanında packet rate (PPS), drop, retransmit ve load balancer data plane limitleri izleniyor.

## Compute, Kubernetes ve runtime

- Request ve limit değerleri gerçek profile uyumlu; CPU throttling ve memory OOM davranışı peak testinde ölçüldü.
- HPA sinyali leading indicator kullanıyor; CPU'dan önce queue age veya concurrency gerekiyorsa uygulandı.
- Cluster autoscaler quota, IP, subnet, image pull ve scheduling kısıtlarıyla birlikte test edildi.
- Startup, readiness ve liveness probe'ları overload altında restart loop üretmiyor.
- JVM GC, heap, thread pool; .NET thread starvation; runtime connection pool metrikleri görünür.
- Pod disruption budget ve topology spread, failure domain kaybında kalan kapasiteyi koruyor.

## Application ve API

- Her downstream çağrıda deadline, bounded retry, idempotency ve cancellation davranışı tanımlı.
- N+1 query, pahalı serialization, büyük payload ve senkron fan-out profilleri giderildi veya sınırlandı.
- Circuit breaker threshold ve half-open davranışı test edildi; recovery sırasında thundering herd oluşmuyor.
- Concurrency limit ve queue bound açık; sınırsız in-flight request kabul edilmiyor.
- İş hataları teknik error rate içinde kaybolmuyor; checkout rejection ile system failure ayrılıyor.

## Database ve data platform

- Peak TPS, connection, lock wait, buffer cache, IOPS, log flush ve replication lag sınırları ölçüldü.
- Hot partition, hot key ve kampanya ürünü için skew testi yapıldı.
- Read replica lag durumunda stale read ve read-your-writes kararları journey bazında yazılı.
- Failover sırasında write fencing, transaction retry ve duplicate write davranışı test edildi.

## Cache, queue ve streaming

- Cache hit ratio yanında origin amplification, eviction, memory fragmentation ve hot key izleniyor.
- Cache stampede için jittered TTL, request coalescing veya single flight uygulandı.
- Queue depth yanında oldest message age, arrival rate, completion rate ve dead letter ölçülüyor.
- Consumer scaling partition sayısı, ordering ve downstream kapasiteyle uyumlu.
- Duplicate delivery ve out-of-order message için idempotent consumer davranışı test edildi.
- Backlog drain süresi kampanya sonrası recovery SLO içinde hesaplandı.

## Third party ve vendor

- Quota, burst, concurrent connection ve günlük limitler yazılı olarak doğrulandı.
- Vendor, kampanya tarihi, beklenen hacim ve escalation contact bilgisiyle bilgilendirildi.
- Timeout, 429, partial response ve schema deviation senaryoları simüle edildi.
- Fallback provider veya manuel süreç için veri tutarlılığı ve reconciliation planı var.
- Vendor status page tek sinyal değil; bağımsız synthetic ölçüm bulunuyor.
- Support contract, severity tanımı ve escalation süresi event command planına işlendi.

### RUNBOOK

## Peak günü runbook'u

Bu bölüm genel bir iskelet sunar; her ortam için komut, dashboard, owner ve escalation bağlantıları kurumun kendi sistemlerine göre eklenir. Aynı iskelet 11.11, Black Friday ve Cyber Monday için ayrı ayrı koşudur.

| ZAMAN         | AKSIYON                                                   | OWNER            |
|---------------|-----------------------------------------------------------|------------------|
| T-120 dk      | On-call check-in, bridge ve iletişim kanalı açılışı       | Event Commander  |
| T-90 dk       | Capacity pre-scale, quota ve ready instance kontrolü      | Platform         |
| T-75 dk       | Cache warming ve kritik synthetic transaction             | App ve edge      |
| T-60 dk       | Replication lag, queue age, backup ve third-party health  | Data ve servis   |
| T-45 dk       | Freeze audit ve son değişikliklerin gözden geçirilmesi    | Change owner     |
| T-30 dk       | Journey dashboard baseline snapshot                       | Observability    |
| T-15 dk       | Go checkpoint ve açık risklerin okunması                  | Event Commander  |
| T-0           | Campaign start marker ve sıklaştırılmış gözlem            | Scribe           |
| T+0 – T+60 dk | 5 veya 10 dakikalık trend review; gereksiz değişiklik yok | IC ve Ops        |
| Peak sonrası  | Backlog drain, scale-down gate ve controlled thaw         | Platform ve Data |

## Canlı karar eşikleri

Eşikler örnektir; boş bırakılan değerler kendi SLO'nuzdan doldurulur.

| METRIC           | UYARI              | AKSIYON                               | RECOVERY               |
|------------------|--------------------|---------------------------------------|------------------------|
| Journey success  | < event SLO        | Incident ve dependency triage         | 3 pencere SLO üstü     |
| p99 latency      | > hedefin 1,5 katı | Concurrency ve database wait kontrolü | Trend baseline'a yakın |
| Retry ratio      | > %__              | Retry budget'ı düşür                  | 2 pencere eşik altı    |
| Queue oldest age | > __ dakika        | Ingest limit ve consumer scale        | Backlog drain trendi   |

|                     |       |                        |                     |
|---------------------|-------|------------------------|---------------------|
| Database connection | > %__ | Admission control      | Headroom %__        |
| Cache hit           | < %__ | Origin protection      | Hit ratio stabilize |
| Third-party 429     | > %__ | Rate limit ve fallback | Provider normal     |

## Scale-down için güvenlik koşulları

- Offered load belirlenen süre boyunca düşüş trendinde.
- Queue ve streaming backlog hedef recovery süresinde boşalıyor.
- Cache hit ratio ve database load normalleşti.
- Geç gelen webhook, batch ve reconciliation trafiği hesaplandı.
- Bir sonraki coğrafi peak veya kampanya dalgası başlamadan önce yeterli süre var.
- Scale-down, failure domain başına minimum failover capacity'yi koruyor.

### SONRASI

## Ara değerlendirme ve kampanya sonrası

İlk peak'i ikincisinin provası olarak kullanın. 11.11'den sonraki günlerde kısa bir ara değerlendirme yapın ve bulguları Black Friday'den önce kapatın. Kasım bittiğinde büyüttüğünüz kaynakları (autoscaling alt sınırları, geçici sunucular, büyütülmüş database sınıfları) geri küçültmeyi takvime bağlayın; aksi hâlde aralık faturasına yansır.

Kampanya problemsiz geçtiğinde de review yapılır. Hazırlık programının hangi varsayımları doğru çıktı, hangi kapasite kullanılmadı, hangi alarm gereksizdi ve hangi manuel müdahale gelecekte otomatikleştirilebilir soruları cevaplanır. Bu notlar bir sonraki kampanyanın yük testi senaryosu olur.

| KARŞILAŞTIRMA      | SORULAR                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------|
| Tahmin ve gerçek   | Peak zamanlaması, trafik, kullanıcı karması ve dönüşüm ne kadar saptı?                     |
| Kapasite           | Hangi bileşen sınıra en çok yaklaştı; headroom doğru muydu?                                |
| Müşteri sonucu     | Journey SLO, correctness ve destek talebi nasıl değişti?                                   |
| Otomasyon          | Hangi autoscaling veya protection mekanizması beklendiği gibi çalışmadı?                   |
| Operasyon          | Hangi karar gecikti; hangi dashboard veya yetki eksikti; hangi runbook adımı işe yaramadı? |
| Maliyet            | Pre-scale ve kampanya maliyeti, korunan iş sonucuyla uyumlu muydu?                         |
| Kalıcı iyileştirme | Hangi geçici çözüm platform kabiliyetine dönüşmeli?                                        |

## Kaldır, standartlaştır veya ürünleştir

Kampanya hazırlığında üretilen her geçici mekanizma üç gruptan birine atanır: kaldır, standartlaştır veya ürünleştir. Resiliency Matrix, synthetic journey, capacity model ve incident drill gibi kabiliyetler yalnızca Black Friday için bırakılmaz; normal operasyon standardına eklenir. Böylece bir sonraki peak hazırlığı sıfırdan başlamaz.

## Aksiyon kalite kriteri

- Aksiyon belirli bir failure mechanism'i azaltır; genel iyileştirme ifadesi değildir.
- Owner ve tarih bulunur; başarı metriği ölçülebilir.
- Mümkünse guardrail veya otomatik kontrol hâline getirilir.
- Aynı sınıf incident'i diğer servislerde de arayan yatay tarama içerir.
- Tamamlandığında aynı test veya Game Day senaryosuyla yeniden doğrulanır.

Bu rehber yaşayan bir standarttır. Her yüksek etkili incident, başarısız test veya kampanya review'u sonrasında kontrol listesine yeni bir madde eklenebilir; yeni madde belirli bir failure mechanism'e, açık bir kanıt ve uygulanabilir bir owner modeline dayanmalıdır. Yılda en az bir kez sahiplik, araç bağlantıları ve risk eşikleri gözden geçirilir.

### ANTI - PATTERN

## Anti-pattern kataloğu

Aşağıdaki cümleler readiness toplantılarında sık duyulur ve her biri bir kanıt boşluğunu örter.

| YANLIŞ GÜVEN SINYALI       | GERÇEK RISK                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| "CPU %30, hazırız"         | Darboğaz connection, lock, queue, IOPS, downstream quota veya tail latency olabilir.                |
| "Autoscaling çözer"        | Scale-out gecikir; quota, IP, warm-up ve downstream kapasite sınırları vardır.                      |
| "Load test geçti"          | Yanlış trafik karması, closed model veya warm cache gerçek peak'i temsil etmeyebilir.               |
| "İki region var"           | İkinci region peak'i tek başına taşıyamıyorsa ve failover yük altında denenmediyse koruma sağlamaz. |
| "Retry reliability sağlar" | KontROLSÜZ retry, geçici hatayı cascading failure'a çevirir.                                        |
| "Queue veri kaybını önler" | Sınırsız backlog recovery süresini bozar ve downstream'i kampanya sonrasında da baskılar.           |
| "Freeze risk yaratmaz"     | Eski kritik açıklar ve kapasite problemleri de risk taşır; istisna süreci gerekir.                  |
| "Dashboard var"            | Karar eşiği, owner ve runbook yoksa grafik operasyon kabiliyeti değildir.                           |
| "Backup var"               | Restore süresi ve doğrulanmış bütünlük bilinmiyorsa recovery kanıtı yoktur.                         |
| "Incident olmadı"          | Sistemin güvenli olduğu anlamına gelmeyebilir; tahmin düşük veya gözlem eksik olabilir.             |

ECLIT  
NOTU

Sisteminizin sınırını müşterilerinizden önce siz öğrenin. Don't Deploy on Friday. Verify on Friday.

## KONTROL TABLOSU

## Kontrol tablosu · yazdırıp doldurun

On madde, iki kampanya sonrası iş; her satırda bir sorumlu ve bir tarih. Tabloyu kasım başlamadan doldurun. Freeze dönemlerinde yalnız "Durum" sütunu güncellenir; yeni iş eklenmez.

| NO | KONTROL                                                                               | SORUMLU | HEDEF TARİH | DURUM |
|----|---------------------------------------------------------------------------------------|---------|-------------|-------|
| 01 | Peak yük testi koşuldu; p95, p99, error rate ve database connection sayısı kaydedildi |         |             | —     |
| 02 | Quota ve limit tablosu çıkarıldı; artış talepleri açıldı                              |         |             | —     |
| 03 | Değişiklik politikası ve iki freeze dönemi yazılı olarak duyuruldu                    |         |             | —     |
| 04 | Son yedekten restore denendi; iki süre ölçüldü                                        |         |             | —     |
| 05 | Synthetic check'ler ve SLO alarmları kuruldu                                          |         |             | —     |
| 06 | Dört haftalık on-call rotasyonu, escalation matrisi ve runbook'lar hazır              |         |             | —     |
| 07 | Dış servislerde timeout, retry budget, circuit breaker ve idempotency key             |         |             | —     |
| 08 | Endpoint bazında rate limit; L7 DDoS koruması doğrulandı                              |         |             | —     |
| 09 | Certificate, domain, DNS TTL, disk ve log retention süreleri kontrol edildi           |         |             | —     |
| 10 | Feature flag'ler ve virtual waiting room eşiği tanımlandı                             |         |             | —     |
| +  | 11.11 sonrası ara değerlendirme yapıldı; bulgular kapatıldı                           |         |             | —     |
| +  | Aralık başında scale-down ve postmortem takvime bağlandı                              |         |             | —     |

## Event readiness ana kaydı

Kampanya başında tek sayfada doldurulur: kampanya ve tarih, Event Commander, teknik lider, kritik journey'ler, tahmini peak ve burst, freeze başlangıcı, go / no-go tarihi, war room, vendor escalation. Yedi kapı özeti aynı sayfada yer alır: her kapı için owner, kanıt, durum (R / A / G) ve açık risk.

## Runbook doğrulama kaydı

- Runbook başka bir ekip üyesi tarafından uygulanabildi (tatbikat kaydı)
- Tüm komut ve bağlantılar güncel (kontrol tarihi)
- Gerekli production yetkileri doğrulandı (access test)
- Rollback adımı gerçek ortam benzerinde denendi (test run)
- Recovery condition açık ve ölçülebilir (dashboard)
- Escalation kişi ve süreleri güncel (roster)

## ECLIT NOTU

Sisteminizin sınırını müşterilerinizden önce siz öğrenin.