

Staging/Prod & Node Bazlı Config Drift Tarama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; staging/prod ve node/cluster seviyesinde konfigürasyon kaymalarını (*configuration drift*) düzenli ölçüp "beklenen (*laC / baseline*)" ile "gerçekleşen (*actual*)" durum arasındaki farkları şeffaf bir şekilde görünür kılmak için hazırlanmıştır. Manuel müdahaleler veya unutulmuş geçici ayarlar sonucu oluşan kritik drift türlerini risk seviyelerine göre sınıflandırır ve otomatik düzeltme (*enforcement / re-alignment*) mekanizmalarıyla ilişkilendirir. Güncelleme (*patch*) ve yeni sürüm (*release*) sonrasında drift taramasını rutin bir adıma dönüştürerek sürdürülebilir bir ortam eşliği (*environment parity*) sağlar.

Kim Kullanır?: DevOps / SRE Mühendisleri, Sistem Yöneticileri, Platform Ekipleri (Otel / B2B Altyapıları).

Nasıl Kullanılır?

- laC depolarınızı (*Terraform, Ansible vb.*) veya CIS Baseline referansınızı tanımlayarak taranacak ortam ve node/cluster listesini belirleyin.
- Port, kullanıcı yetkileri, paket sürümleri ve log/agent konfigürasyonlarını taratıp beklenen vs. gerçek durum farklarını çıkarın.
- Tespit edilen kaymaları risk sınıfına göre etiketleyin; laC rerun / Ansible apply ile otomatik düzeltme ve re-scan doğrulamasını başlatın.

TEMPLATE — Staging/Prod & Node Bazlı Config Drift Tarama Şablonu

1) Referans ve Kapsam

- Baseline Kaynağı (Expected State):** Terraform State / Ansible Playbooks / Git Repository / CIS Baseline v1.0
- Hedef Ortamlar (Environments):** Staging / Pre-Prod / Production Cluster
- Node / Cluster Listesi:** *k8s-prod-cluster-01, app-node-[01..08], db-cluster-primary, dmz-proxy-01*
- Kabul Edilen Farklar (Allowed Differences) Dokümanı:** Var (Staging'deki daha yüksek log debug seviyesi ve kısıtlı test portları izinli farklar listesinde tanımlıdır).

2) Drift Kontrol Seti (Beklenen vs. Gerçekleşen)

Drift Alanı	Kontrol Yöntemi	Beklenen (Expected / laC)	Gerçek (Actual / Live Node)	Risk	Aksiyon
Port / Firewall	Nmap / Security Group Scan	Sadece TCP 80, 443 açık	TCP 80, 443, 8080 (Geçici port) açık	Kritik	Portu anında kapat + Security Group'u laC ile sync et

User / Role	/etc/passwd / IAM Scan	Yalnızca deploy & sysadmin kullanıcıları	Yetkisiz test-user oluşturulmuş	Kritik	Kullanıcıyı sil + SSH yetkilerini iptal et
Paket Sürümü	dpkg -l / rpm -qa / Driftctl	OpenSSL 3.0.2-0ubuntu1.10	OpenSSL 3.0.2-0ubuntu1.02 (Eski)	Önemli	Otomatik yama/Ansible pipeline tetikle
Log / Agent	systemctl status / Agent Scan	Fluentd Agent: Running	Fluentd Agent: Stopped / Inactive	Kritik	Servisi otomatik restart et + SIEM alarmı üret

3) Drift Risk Sınıflandırması & Tepki Modeli

- 🔴 **Kritik (Critical Drift):**
 - Tanım:* Güvenlik duvarı ihlalleri, yetkisiz kullanıcılar, durdurulmuş log/güvenlik agent'ları.
 - Aksiyon:* **Anında Müdahale** + Otomatik IaC Enforcement + 7/24 PagerDuty Alarmı.
- ⚠️ **Önemli (Major Drift):**
 - Tanım:* Uyumsuz kütüphane/paket sürümleri, eksik performans parametreleri, environment parity sapmaları.
 - Aksiyon:* İlk **Planlı Bakım Penceresinde** (max 48 saat) Ansible/Terraform rerun ile düzeltme.
- ℹ️ **Düşük (Minor Drift):**
 - Tanım:* Kritik olmayan geçici dosya kalıntıları, izleme metrik periyot farkları.
 - Aksiyon:* Gelecek sürüm (release) sprint backlog'una ekleme.

4) Düzeltme (Reconciliation) ve Doğrulama

- Düzeltme Yöntemi:**
 - Prod:* Otomatik IaC Apply (Terraform apply -auto-approve / Ansible-playbook --force)
 - Staging:* Otomatik Pipeline Re-alignment
 - Saha Müdahalesi:* Manuel değişiklik kesinlikle yasaktır; tüm değişiklikler Git / IaC üzerinden yapılmak zorundadır.
- Re-Scan Zorunluluğu: Evet (Zorunlu)** — Düzeltme uygulandıktan en geç 15 dakika sonra doğrulama taraması otomatik çalıştırılır.
- Owner ve SLA:**
 - DevOps / SRE Team:** Kritik Drift için SLA: **\$< 1\$ Saat**
 - SysAdmin Team:** Önemli Drift için SLA: **\$< 24\$ Saat**

5) Periyot ve Tetikleyiciler

- **Rutin Taramalar:** Günlük Otomatik Drift Taramaları (Her gece 02:00'de cron/pipeline ile çalışır).
- **Patch Sonrası Tarama:** İşletim sistemi veya güvenlik yamaları uygulandıktan **hemen sonra** otomatik çalışır.
- **Release Sonrası Tarama:** Prod ortamına yapılan her uygulama dağıtımı (*deployment*) sonrasında otomatik çalışır.
- **Raporlama & Görselleştirme:** Grafana Compliance Dashboard + Jira Otomatik Ticket / Slack Instant Notification.

6) Denetim ve Kontrol Listesi (Checklist)

- [] **Allowed Differences Listesi Var:** Staging ve Prod arasındaki haklı/izinli konfigürasyon farkları dökümanite edildi ve tarama motoruna istisna tanımlandı.
- [] **Patch Sonrası Drift Taraması Zorunlu:** Yamalama veya altyapı güncellemelerinden hemen sonra drift taraması otomatik tetikleniyor.
- [] **Node Bazlı Rapor Üretiliyor:** Farklılıklar sadece cluster bazında değil, sunucu/node bazında tek tek raporlanabiliyor.
- [] **Kritik Drift İçin Alarm Var:** Güvenlik ve erişim odaklı kaymalarda nöbetçi mühendise (PagerDuty/Slack) anlık bildirim gidiyor.
- [] **Düzeltilme Sonrası Re-Scan Yapılıyor:** Düzeltme adımı uygulandıktan sonra sistemin IaC ile %100 uyumlu olduğu doğrulama taramasıyla tescil ediliyor.

Deliverables (Teslim Edilecek Çıktılar)

- **Node Bazlı Drift Tarama & Mimaride Uyumluluk Şablonu (v1.0):** Beklenen vs. Gerçekleşen durum analiz dokümanı ve matrisi.
- **Terraform & Ansible Auto-Reconciliation Scriptleri:** Konfigürasyon kaymalarını tespit edip kodu canlıya zorla uygulayan otomasyon kütüphanesi.
- **Drift Risk Sınıflandırma & Alarm Entegrasyon Rehberi:** Slack, PagerDuty ve Jira otomatik bilet oluşturma entegrasyon dosyaları.
- **Environment Parity & Allowed Differences Listesi:** Staging ve Prod arasındaki izin verilen farkların kayıt ve denetim formu.



[Deliverables / Proof Card]

DevOps/SRE mühendisleri, altyapı mimarları ve sistem yöneticileri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Config Drift Tarama Deliverables Kartı. Koyu karbon gri ve parlak turuncu/cyan tonlarındaki teknolojik zemin üzerinde; "Expected vs Actual" karşılaştırma ekranı, node bazlı drift analiz grafiği, IaC (Terraform/Ansible) senkronizasyon simgeleri ve otomatik düzeltme (auto-reconciliation) döngüsü yer alıyor. Kartın üzerinde; "Node-Level Expected vs. Actual Comparison", "Automated IaC Re-alignment & Enforcement", "Critical Drift Real-time Alerting & SLAs" ve "Post-Patch & Release Verification Re-Scans" teslimat kalemi başlıkları, yanlarında parlak cyan onay işaretleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.