Kubernetes RBAC / Namespace / NetworkPolicy Güvenlik Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset; Kubernetes ortamlarında güvenliğin en yüksek etkiye sahip üç temel katmanını (RBAC erişim kontrolleri, namespace izolasyonu ve NetworkPolicy ağ kuralları) hızlıca standardize etmek için hazırlanmıştır. "Default-deny" (varsayılan olarak engelle) yaklaşımıyla pod'lar arası yetkisiz yatay ilerleme (*lateral movement*) riskini azaltır; süreci node sertleştirme (*node hardening*) ve Pod Security standartlarıyla tamamlar. Upgrade ve bakım döngülerine entegre edilerek sürdürülebilir bir k8s güvenlik altyapısı sağlar.

Kim Kullanır?: DevOps / SRE Mühendisleri, Platform Ekipleri ve Otel / B2B Microservice Yazılım Ekipleri.

Nasıl Kullanılır?

1. Cluster erişim envanterini çıkartarak kisi ve servis bazlı RBAC rol matrisini netleştirin.
2. Ortam bazlı namespace mimarisini oluşturun ve prodeksiyon ortamında "default-deny" NetworkPolicy kurallarını uygulayın.
3. Pod Security standartlarını ve node sertleştirme adımlarını CI/CD ve cluster politikalarına ekleyip periyodik olarak doğrulayın.

CHECKLIST & SPRINT PLAN — Kubernetes Cluster Güvenliği

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Kubeconfig Erişim Envanteri:** Cluster erişimine sahip tüm kullanıcı, CI/CD servisi ve dış sistemlerin kubeconfig envanteri çıkarıldı; erişimler kişi/servis bazlı tekilleştirildi.
- [ ] **Minimum Cluster-Admin Yetkisi:** cluster-admin rolü strictly sınırlandırıldı; sadece acil durum ve altyapı yönetimi için belirli hesaplara tanımlandı.
- [ ] **RBAC Least-Privilege Rol Matrisi:** Tüm kullanıcılar ve ServiceAccount'lar için minimum yetki veren (*least-privilege*) Role ve RoleBinding matrisi kurgulandı.
- [ ] **Prod / Staging Namespace Ayrımı:** Canlı (*production*) ve test (*staging/dev*) ortamları birbirinden fiziksel/mantıksal namespace seviyesinde tamamen izole edildi.
- [ ] **Default Namespace Temizliği:** Kubernetes varsayılan default namespace'i uygulama dağıtımı için kullanımı kapatıldı veya kullanımı minimuma indirildi.
- [ ] **Prod Default-Deny NetworkPolicy:** Canlı namespace'lerde tüm ingress (gelen) ve egress (giden) trafiği varsayılan olarak engelleyen default-deny kuralları aktif edildi.
- [ ] **Allowlist Servis Trafik Akışları:** Pod'ların birbiriyle ve dış servislerle iletişim kurabilmesi için sadece gerekli port ve etiketlere (*labels*) izin veren allowlist NetworkPolicy'leri tanımlandı.
- [ ] **Minimal & Korumalı Ingress Girişleri:** Dış dünyaya açık Ingress noktaları sınırlandırıldı; TLS/SSL konfigürasyonları ve WAF/rate-limiting katmanları eklendi.

- [ ] **Pod Security Standards (PSS / PSA):** Pod'ların root kullanıcısı ile çalışması engellendi (runAsNonRoot), ayrıcalıklı (*privileged*) modlar ve tehlikeli Linux yetkileri (*capabilities*) kapatıldı.
- [ ] **Node Hardening & Upgrade Planı:** Kubernetes worker node OS seviyesinde sertleştirildi; işletim sistemi ve k8s versiyon yükseltme/bakım takvimi otomatize edildi.

2) Problem → Kök Neden → Çözüm Tablosu

Problem	**Kök Neden**	**Çözüm (K8s Security)**
Her Pod Her Yere Erişiyor	NetworkPolicy kurgulanmaması / Ağ kısıtlamasının olmaması	**Default-Deny NetworkPolicy** $\mathbf{+}$ **Allowlist Kuralları**
Herkes Cluster'a Bağlanıyor	Geniş ve denetimsiz RBAC izinlerinin tanımlanması	**Least-Privilege RBAC Matrisi** $\mathbf{+}$ **Cluster-Admin Temizliği**
Staging ve Prod Karışıyor	Ortamların mantıksal ve yetki bazlı ayrılmaması	**Env Bazlı Namespace Mimarisi** $\mathbf{+}$ **ResourceQuota**
Privileged Pod / Root Erişimi	Pod güvenlik standartlarının ve zorunluluklarının olmaması	**Pod Security Standards (Non-Root / Read-Only Root FS)**

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14)

[Gün 1–5: Erişim Envanteri & RBAC/Namespace] ⟶ [Gün 6–8: NetworkPolicy & Ingress Security] ⟶ [Gün 9–12: Pod/Node Security & Observability] ⟶ [Gün 13–14: Tatbikat & Rapor]

- **Gün 1:** Kubeconfig erişimlerinin, aktif sertifikaların ve cluster yetkililerinin tam envanterinin çıkarılması.
- **Gün 2:** Kullanıcı grupları ve ServiceAccount'lar için k8s RBAC rol matrisinin tasarlanması.
- **Gün 3:** Gereksiz cluster-admin yetkilerinin kaldırılması ve acil durum (*break-glass*) erişim akışının kurulması.
- **Gün 4:** Proje ve ortam bazlı (prod, staging, ops) namespace mimarisinin yeniden yapılandırılması.
- **Gün 5:** Varsayılan default namespace içindeki kaynakların temizlenmesi ve kullanımının kısıtlanması.

- **Gün 6:** Production namespace'lerinde tüm trafiği bloklayan default-deny-all NetworkPolicy kuralının uygulanması.
- **Gün 7:** Mikroservislerin birbiriyle güvenli haberleşmesi için etiket bazlı (*label-based*) allowlist NetworkPolicy'lerinin yazılması.
- **Gün 8:** Ingress Controller kurallarının gözden geçirilmesi, gereksiz dış erişim noktalarının kapatılması.
- **Gün 9:** Pod Security Standards (PSA/PSS) kurallarının aktif edilerek runAsNonRoot ve readOnlyRootFilesystem zorunluluğunun getirilmesi.
- **Gün 10:** Worker ve master node'lar için OS seviyesinde hardening (CIS Benchmark) checklist adımlarının uygulanması.
- **Gün 11:** Kubernetes versiyon güncellemeleri ve node patch'leri için kesintisiz bakım/upgrade takviminin netleştirilmesi.
- **Gün 12:** Audit logları, Falco/Trivy güvenlik alarmları ve network akışları için observability dashboard'larının kurulması.
- **Gün 13:** Yanlış politika kısıtlamalarını test etmek adına "Policy Breakage" ve "Unauthorized Access" simülasyon tatbikatı yapılması.
- **Gün 14:** Yönetim özet raporunun hazırlanması ve 180 günlük periyodik denetim/upgrade takviminin kilitlenmesi.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	**Önce (Mevcut Durum)**	**Sonra (Sprint Sonrası)**	**Hedef Yönü**
Cluster-Admin Sayısı	Yüksek (Kontrolsüz / Geniş)	Minimum (Yalnızca SRE / Break-glass)	**Hedef ↓ (Düşüş)**
Policy Kapsaması (NetworkPolicy %)	$\%0$ (Ağ kısıtlaması yok)	$\%100$ (Default-deny + Allowlist)	**Hedef ↑(Yükselme)**
RBAC Uyum Oranı (%)	$\%30$ (Geniş roller)	$\%100$ (Least-privilege matrisi)	**Hedef ↑ (Yükselme)**
Yetkisiz Erişim Denemesi (Kullanıcı/Pod)	Yüksek	Otomatik Engellenen / Alarm Veren	**Hedef ↓ (Düşüş)**

Deliverables (Teslim Edilecek Çıktılar)

- **Kubernetes RBAC Rol Matrisi Dokümanı:** Kullanıcı, grup ve servis hesapları için tanımlanmış Role/ClusterRole YAML şablonları.
- **Namespace & ResourceQuota Planı:** Ortam izolasyon kuralları ve kaynak limitleri rehberi.
- **Production NetworkPolicy Kütüphanesi:** Default-deny ve servisler arası geçiş izinlerini içeren deklaratif k8s manifesto seti.
- **Pod Security Standardı & Node Hardening Kılavuzu:** CIS Benchmark uyumlu güvenlik kuralları ve yükseltme (*upgrade*) takvimi.

[Checklist Card]

DevOps/SRE mühendisleri, platform ekipleri ve microservice mimarları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Kubernetes Güvenlik Checklist Kartı. Koyu karbon gri ve canlı siyan/mavi/turuncu tonlarındaki teknolojik zemin üzerinde; Kubernetes dümen

simgesi, pod network izolasyon şeması, RBAC kilit ikonları ve 14 günlük k8s hardening sprint takvimi yer alıyor. Kartın üzerinde; "Least-Privilege RBAC & Sited Cluster-Admin Roles", "Production Namespace Isolation & Default-Deny NetworkPolicies", "Enforced Pod Security Standards (Non-Root/Read-Only FS)" ve "Node Hardening & Automated Upgrade Schedules" teslimat kalemi başlıkları, yanlarında parlak siyan onay işaretleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.