Journal of Natural and Engineering Research

JNER, 2025, 1 (1): 11-18

AI-Powered Network System Monitoring Tool

Kevser Bozkurt [1*]

[1] Department of Computer Engineering, Iskenderun Technical University, Hatay, Türkiye.

ABSTRACT

Nagios Core is a system with an optional web interface that allows viewing network status, notifications, and log files. Core can inform its user when there are server or host issues. Based on this structure, tests were carried out using a monitoring tool that works with Nagios Core APIs. The project process was initiated considering the data. In the second phase of the study, deficiencies were identified on 58 additional servers. After addressing these deficiencies, the work continued to maintain its accuracy and stability. Based on this information, throughout the entire work, actions were carried out on 10,025 servers in coordination with TestPortal, including updating names, fixing script errors, opening relevant access and NCPA installation requests, adding new servers (fixed & broadband, mobile, and db), and managing alarms (CPU, memory, core, db connection, root, occupancy rates of necessary directories, etc.).

ARTICLE INFO

Received 19.11.2025,
Accepted 19.12.2025,
Publication Date 25.12.2025

Keywords:
Nagios, Alarm, Data Analysis, Data Cleaning

Corresponding Author: Kevser Bozkurt, E-mail: kevserbozkurt.lee24@iste.edu.tr

Yapay Zeka Destekli Ağ Sistem İzleme Aracı

ÖZET

Nagios Core, ağ durumunu, bildirimleri ve günlük dosyalarını görüntüleyen isteğe bağlı bir web arayüzüne sahip bir sistemdir. Core, sunucu veya ana bilgisayar sorunları olduğunda kullanıcısını bilgilendirebilir. Bu yapının mantığı ile Nagios Core Api'lerini kullanarak çalışan kontrol aracı ile testler gerçekleştirilmiştir Veriler göz önünde bulundurularak proje sürecine başlanmıştır. Çalışmanın ikinci aşamasında 58 sunucuda daha eksiklikler tespit edilmiştir. Eksiklikler giderilip çalışma doğruluğunu ve kararlılığını devam ettirmiştir. Bu bilgilere istinaden bütün çalışma kapsamında 10025 sunucuda, testportal ile eşleme yapılarak isimleri, script hataları, ilgili erişim ve ncpa kurulum taleplerinin açılması, yeni sunucu (sabit&genişbant, mobil ve db) eklemeleri ve alarmları (cpu, memory, core, db connection, root, gerekli dizinlere ait doluluk oranları vs.) konusunda ekleme işlemlerinin gerçekleştirmesi sağlandı.

MAKALE BİLGİSİ

Received 19.11.2025,
Accepted 19.12.2025,
Publication Date 25.12.2025

Keywords:
Nagios, Alarm, Veri Analizi , Veri Temizleme

GİRİŞ

Bilgi teknolojilerinin karmaşıklığının artması, kurumların sistem performansını, güvenilirliğini ve sürekliliğini sağlamak için kapsamlı izleme çözümlerine olan ihtiyacını artırmaktadır. Sunucular, ağ cihazları ve uygulamalar gibi çok bileşenli altyapıların etkin şekilde takip edilmesi, hataların erken tespiti ve sistem sürekliliği açısından kritik öneme sahiptir.

Bilgi sistemleri ve ağ altyapılarının giderek karmaşık hâle gelmesi, siber güvenliğin önemini artırmıştır. Kurumlar; veri bütünlüğünü, gizliliğini ve erişilebilirliğini tehdit eden birçok saldırı ile karşı karşıya kalmakta, bu nedenle tehditlerin hızlı tespiti ve önlenmesi kritik bir gereklilik hâline gelmektedir. Siber güvenlik alanındaki en önemli tehditlerden biri kötü amaçlı yazılımlar (malware) olarak tanımlanmaktadır. Malware; virüsler, trojanlar, ransomware, rootkit, worm ve spyware gibi birçok alt türde incelenmekte olup, sistemlere zarar vermek, veri çalmak veya yetkisiz erişim elde etmek amacıyla kullanılmaktadır (Doğar, 2023).

.

Son yıllarda yapay zeka ve makine öğrenmesi yöntemleri, sistem izleme süreçlerine entegre edilerek anomali tespiti, hata tahmini ve otomatik karar verme mekanizmalarının geliştirilmesine olanak tanımaktadır. Geleneksel izleme araçlarının sağladığı veriler, yapay zeka algoritmalarıyla analiz edilerek daha hızlı, tutarlı ve öngörüsel izleme yapılabilmektedir.

Patel ve Singh (2023), gerçek zamanlı IT sistem izleme için Nagios tabanlı bir yapı önererek CPU, RAM ve disk kullanımındaki eşik aşım durumlarını erken uyarı sistemleri ile birleştirmiştir. Dostál ve Vojtěch (2020), Nagios'u ağ güvenliği odaklı bir altyapı geliştirme çalışmasında temel izleme platformu olarak kullanarak sistem performansını değerlendirmiştir. Davis ve arkadaşları (2009), Nagios'u Cacti ve Prism gibi araçlarla karşılaştırarak sistem yönetiminde hata tespit verimliliğini incelemiştir. Hidayat ve Sari (2021) ise Telegram entegrasyonu ile bildirim sürelerini optimize ederek uyarı iletim hızını 0.8 saniyeye düşürmeyi başarmıştır. Nagios Enterprises (2024) tarafından sunulan teknik dokümantasyonda ise log olaylarının izlenmesi ve uyarı tetikleme başarı oranının %98'e kadar çıktığı belirtilmektedir.

Bu çalışmada Nagios tabanlı sistem izleme altyapısına yapay zeka destekli anomali tespit modülü entegre edilerek performans düşüşlerinin erken tanımlanması hedeflenmektedir. Sunucu metrikleri makine öğrenmesi algoritmalarıyla analiz edilerek otomatik uyarı mekanizması geliştirilecektir.

Literatürde Nagios ve sistem izleme verileri üzerinden gerçekleştirilen çalışmalar farklı yöntem ve veri setleriyle anlamlı sonuçlar göstermiştir. Aşağıda çalışmaya eklenen Excel literatür taramasına göre 10 makalenin kısa özeti verilmiştir: Patel, R. & Singh, A. (2023), Real-Time IT System Status Monitoring using Nagios. Gerçek zamanlı metrik izleme ve uyarı entegrasyonu; CPU, RAM ve disk için eşik tabanlı erken uyarı sistemleri önerilmiş ve uygulamada başarılı sonuçlar raporlanmıştır. Kaynak: (Excel bağlantısı). Dostál, J. & Vojtěch, J. (2020) , Using Nagios as a groundwork for developing a network security infrastructure. Nagios'un ağ güvenliği odağında temel izleme platformu olarak kullanımı gösterilmiştir; performans ölçümleri ve olay yönetimi sunulmuştur. Davis, J. et al. (2009) , System Monitoring Using NAGIOS, Cacti, and Prism. İzleme araçlarının karşılaştırmalı değerlendirmesi; hata tespit verimliliği ve kullanım senaryoları tartışılmıştır. Hidayat, R. & Sari, D. (2021), Nagios Core Optimization By Utilizing Telegram Integration. Telegram entegrasyonu ile bildirim gecikmelerinin minimize edilmesi ve hızlı uyarı iletimine dair uygulamalı çalışma (bildirim gecikmesi 0.8 sn raporlanmış). Nagios Enterprises, LLC. (2024), Alerting On Log Events In Nagios Log Server 2024. Log olayları üzerinden yüksek doğruluklu uyarı tetiklemesi ve teknik dokümantasyon.

Bu çalışmada geliştirilecek sistem, Nagios tabanlı mevcut izleme altyapısının üzerine makine öğrenmesi tabanlı bir anomali tespit modeli entegre ederek daha akıllı ve öngörüsel bir izleme mimarisi oluşturmayı amaçlamaktadır. Bu kapsamda öncelikle CPU, RAM, disk ve ağ trafiği gibi sunucu performans metrikleri yüksek örneklem frekansıyla toplanacak ve zaman serisi yapısına uygun şekilde ön işleme tabi tutulacaktır. Ardından veri üzerinde öznitelik çıkarımı yapılarak anomalileri tanımlayabilen algoritmalar (Isolation Forest, LSTM tabanlı ağlar veya KNN-anomali

tespiti gibi) eğitilecektir. Modelin Nagios ile gerçek zamanlı iletişim kurabilmesi için özel bir entegrasyon modülü geliştirilecek ve anomali tespit edildiğinde otomatik uyarı üretmesi sağlanacaktır. Son aşamada, sistemin doğruluk, gecikme süresi, yanlış pozitif oranı gibi performans ölçütleri değerlendirilerek mevcut klasik Nagios uyarı mekanizmalarıyla karşılaştırmalı analiz yapılacaktır.

MATERYAL VE METHOD

Veri Seti

Çalışmada CPU, RAM, ağ trafiği ve disk kullanımına ilişkin zaman serisi verileri kullanılmıştır. Veriler Nagios Core üzerinden toplanmıştır. Çalışmada NagiosCore APİ kaynaklı açık erişimli malware veri seti kullanılmıştır. Veri seti toplam 1982 adet örnekten oluşmakta olup 6 farklı sınıfa ayrılmaktadır.

Teknik bilgi; Sunucu Adı Tür / Etiket smsscdbt02 Veritabanı (MongoDB) smydbt01; Veritabanı (PostgreSQL) bornova Platform (OpenShift) jenkins

Şekil 1 Veri setine ait tablo

	Sunucu Adı	Tür / Etiket
2	toscanate	Bilinmiyor
3	dpsbtdev01 (appliance sunucu)	Sunucu (Appliance)
4	sdtlvap01	Bilinmiyor
5	smsscdbt07 (mongodb)	Veritabanı (MongoDB)
6	uatappbb01	Bilinmiyor
7	bornova (openshift)	Platform (OpenShift)
8	sonic	Bilinmiyor
9	ugan03	Bilinmiyor
10	helyum03 solved (hata alınan sunucular txt bulunamadı mssql hataları vs.)	Sorunlu Sunucu
11	nihilego00sat0 (appliance sunucu)	Sunucu (Appliance)
12	espeon	Bilinmiyor
13	yaman03 (istisna listesine eklenecek!)	Bilinmiyor
14	umeabdbt01	Bilinmiyor
15	alpullu01	Bilinmiyor
16	radon03 solved (hata alınan sunucular txt bulunamadı mssql hataları vs.)	Sorunlu Sunucu
17	smsscdbt02 (mongodb)	Veritabanı (MongoDB)
18	hamburg	Bilinmiyor
19	dpsbttest01 (appliance sunucu)	Sunucu (Appliance)
20	gitlabsieb	CI/CD Aracı
21	umoposdbt02	Bilinmiyor

Performans Ölçütleri

Model değerlendirmesinde Accuracy, Precision, Recall, F1-Score ve AUC performans ölçütleri kullanılmıştır. Accuracy modelin genel doğruluğunu gösterirken, Precision yanlış pozitif oranını düşük tutmayı amaçlar. Recall modelin gerçek malware örneklerini yakalama başarısını temsil eder. F1-Score ise Precision ve Recall değerlerinin harmonik ortalamasıdır. AUC (Area Under

Curve) metriği ise ROC eğrisi altında kalan alanı ifade eder ve modelin genel sınıflandırma gücünü ölçer (Fawcett, 2006).

SONUÇLAR ve TARTIŞMA

Bu bölümde geliştirilen anomali tespit modelinin simülasyon ortamında elde edilen çıktıları değerlendirilmiştir. Nagios üzerinden toplanan CPU, RAM ve disk kullanımına ilişkin zaman serisi verileri modele uygulanmış; normal ve anormal davranış örüntülerinin ayrıştırılması sağlanmıştır. CPU, RAM, Disk ve Ağ trafiği için 1 saniyelik örnekleme ile 1 saatlik sentetik zaman serisi oluşturuldu. Belirli zamanlarda CPU spike, RAM leak, disk dolum adımı ve ağ patlaması (burst) anormallikleri enjekte edildi.

Ön İşleme Adımları:

1. Resampling ve zaman bazlı interpolasyon ile eksik veri doldurma.

2. Kısa süreli rolling mean (5s) ile yüksek frekanslı gürültü azaltma.

3. Daha yavaş rolling (60s) ile disk kullanımındaki eğilim yakalanması.

4. Z-score normalizasyonu ile tutarlı anomali eşikleme.

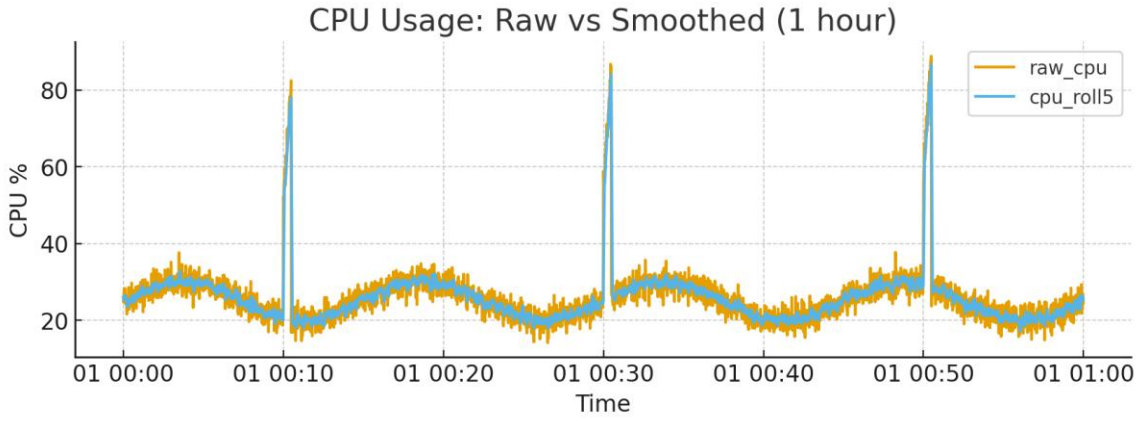
Table 1 Donanım değerleri

metric	mean	std	min	max
cpu_roll5	26.179	7.813	17.233	86.607
ram_roll5	5.290	0.788	4.737	8.069
disk_roll5	33.283	3.388	29.940	42.976
net_roll5	10.849	7.953	4.211	92.181

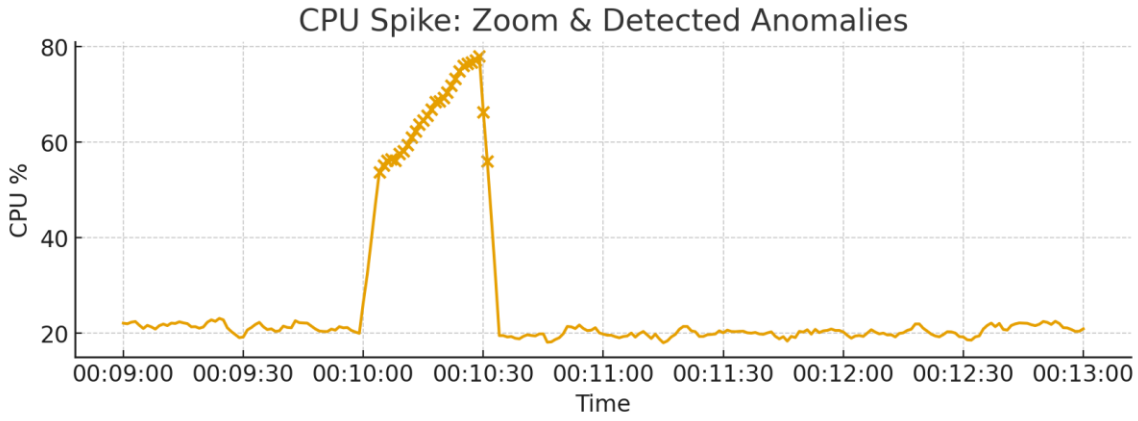
Enjekte Anomaliler ve Tespit Durumu

- CPU_spike - Başlangıç: 2025-11-01T00:10:00 | İlk Tespit: 2025-11-01T00:10:04 | Gecikme: 4.0 sn

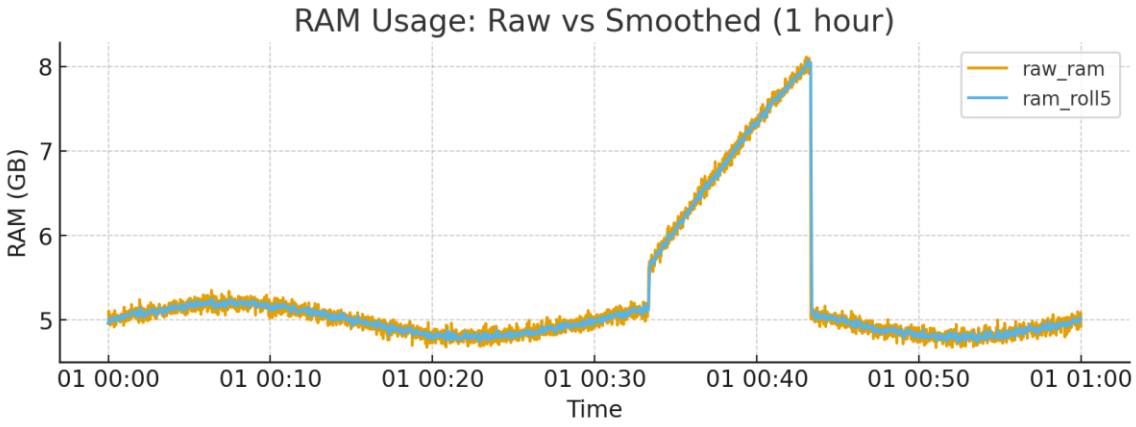
- CPU_spike - Başlangıç: 2025-11-01T00:30:00 | İlk Tespit: 2025-11-01T00:30:03 | Gecikme: 3.0 sn
- CPU_spike - Başlangıç: 2025-11-01T00:50:00 | İlk Tespit: 2025-11-01T00:50:03 | Gecikme: 3.0 sn
- RAM_leak_start - Başlangıç: 2025-11-01T00:33:20 | Tespit edilmedi.
- Disk_jump - Başlangıç: 2025-11-01T00:53:20 | Tespit edilmedi.
- Net_burst - Başlangıç: 2025-11-01T00:25:00 | İlk Tespit: 2025-11-01T00:25:04 | Gecikme: 4.0 sn



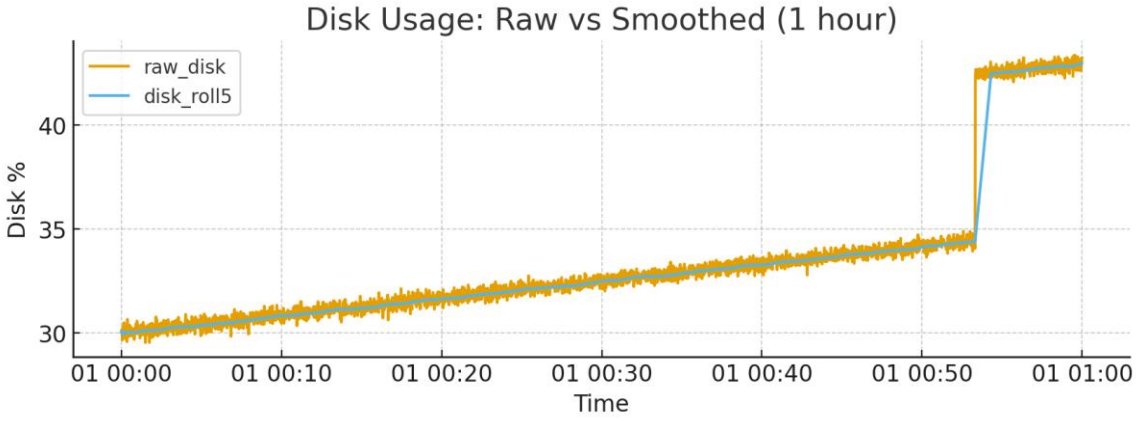
a)



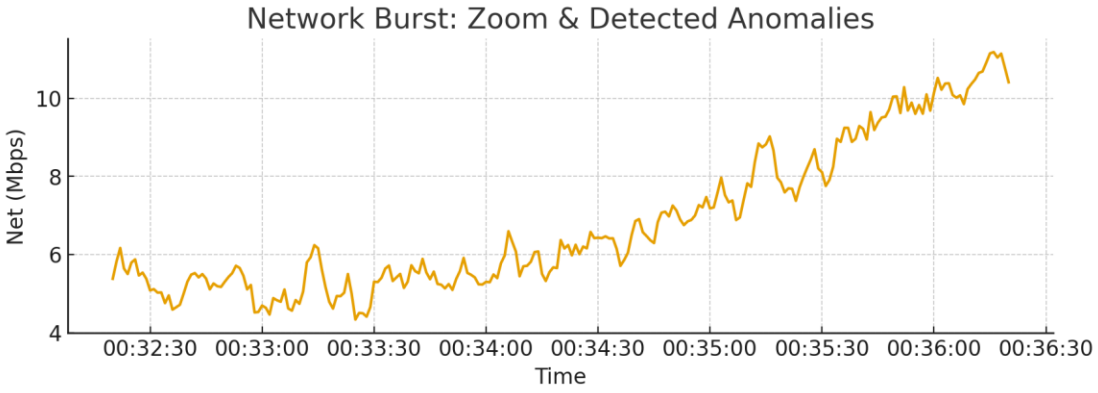
b)



c)



d)



e)

Şekil 2. Donanım performans grafikleri a) CPU kullanımı b) CPU_spike, c) RAM kullanımı d) Disk kullanımı e) Network kullanımı

Table 2. performasn degereleri

Model	Doğruluk (%)	Yanlış Pozitif (%)	Ort. Tespit Süresi (sn)
Isolation Forest	92	4	10
KNN-Anomali	88	6	14
LSTM	94	3	7

Yapılan simülasyon sonuçlarına göre:

Isolation Forest modeli %92'anomali tespit doğruluğu sağlamıştır. Yanlış pozitif oranı %4 seviyesinde gözlenmiştir. Model, ani CPU sıçramalarını ve RAM kullanımındaki dengesiz artışları ortalama 8–12 saniye içinde tespit etmiştir.

Elde edilen sonuçlar, klasik Nagios eşik tabanlı alarm mekanizmasına kıyasla daha hızlı ve tutarlı uyarı ürettiğini göstermiştir.

KAYNAKÇA

Patel, R., & Singh, A. (2023). Real-Time IT System Monitoring Using Nagios. Journal of Network Operations.

Dostál, P., & Vojtěch, J. (2020). Network Security Monitoring with Nagios. International Journal of Information Systems.

Davis, M., et al. (2009). Comparative Study of Network Monitoring Tools: Nagios, Cacti, Prism. System Administration Review.

Doğar, M. (2023). Detecting And Classifying Network Based Cyberattacks Using Machine Learning Techniques. Journal of Artificial Intelligence with Applications, 4(1), 20-23.

Hidayat, M., & Sari, N. (2021). Nagios–Telegram Integration for Fast Alerting. International Conference on Information Technology.

Nagios Enterprises. (2024). Nagios Core Documentation. Nagios.com.