T.C.

KOCAELİ SAĞLIK VE TEKNOLOJİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ PROGRAMI

YÜKSEK LİSANS BİTİRME TEZİ

ZABBIX AĞ YÖNETİM YAZILIMINA ETKİN VARLIK EKLENMESİ VE VERİLERİN GÖRSELLEŞTİRİLMESİ

Gökhan TUĞRUL

230403011

DANIŞMAN:

Dr. Öğr. Üyesi Mehmet KARA

EYLÜL-2025

T.C.
KOCAELİ SAĞLIK VE TEKNOLOJİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ PROGRAMI

YÜKSEK LİSANS

BİTİRME TEZİ

ZABBIX AĞ YÖNETİM YAZILIMINA ETKİN VARLIK EKLENMESİ VE VERİLERİN GÖRSELLEŞTİRİLMESİ

GÖKHAN TUĞRUL

230403011

DANIŞMAN:
Dr. Öğr. Üyesi Mehmet KARA

ONAY SAYFASI

Bu tez Kocaeli Sağlık ve Teknoloji Üniversitesi Lisansüstü Eğitim Enstitüsü tarafından onaylanmıştır.

_____

Enstitü Müdürü

Bu tezin Kocaeli Sağlık ve Teknoloji Üniversitesi, Bilişim Sistemleri Mühendisliği Yüksek Lisans derecesinin tüm gerekliliklerini karşıladığını onaylıyorum.

_____

Dr. Öğr. Üyesi Mehmet KARA
Bölüm Başkanı

GÖKHAN TUĞRUL tarafından teslim edilen ‘’ **Zabbix Ağ Yönetim Yazılımına Etkin Varlık Eklenmesi ve Verilerin Görselleştirilmesi ‘’** başlıklı bu tezin kapsam ve kalite bakımından Yüksek Lisans derecesi için yeterli olduğunu değerlendirmektedir.

_____

Dr. Öğr. Üyesi Mehmet KARA
Danışman

Tez Jürisi Üyeleri: (1. isim: Jüri başkanı; 2. isim: Danışman)

Doç. Dr. Serdar SOLAK
Teknoloji Fakültesi, Kocaeli Üniversitesi

Dr. Öğr. Üyesi Mehmet KARA
Mühendislik ve Doğa Bilimleri Fakültesi, Kocaeli Sağlık ve Teknoloji Üniversitesi

Dr. Öğr. Üyesi İsmet KARADUMAN
Mühendislik ve Doğa Bilimleri Fakültesi, Kocaeli Sağlık ve Teknoloji Üniversitesi

Tarih:

TEŞEKKÜR

Bu çalışmanın gerçekleşmesinde katkıda bulunan Tez Danışmanım ve Kocaeli Sağlık ve Teknoloji Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi Öğretim Üyesi Dr. Öğr. Üyesi Sayın Mehmet KARA hocama ve bu süreçte bana destek olup sabır gösteren saygıdeğer eşim Kübra ve kızım İpek'e teşekkür ederim.

ÖZ

ZABBIX AĞ YÖNETİM YAZILIMINA ETKİN VARLIK EKLENMESİ VE VERİLERİN GÖRSELLEŞTİRİLMESİ

Gökhan TUĞRUL

Kurumsal iş süreçlerinin elektronik ortama aktarıldığı günümüzde kurum bilişim sistemlerinde bulunan yazılım ve donanım varlıklarının anlık olarak durumlarının izlenmesi ve yönetilmesi, kurum iş sürekliliği için büyük önem arz etmektedir. Bilgi sistem yazılım ve donanımları ağ yönetim yazılımları kullanılarak yönetilmeye çalışılmaktadır. Çok sayıda farklı marka ağ cihazı, yazılım, IoT(İnternet of Things) cihazı, mobil bilişim cihazı, bulut bilişim cihazı olmasından dolayı ağ yönetim yazılımlarının her türlü cihazı izlemesi, yönetmesi önemli bir problem olarak karşımıza çıkmaktadır.

Bu tez çalışmasında, çok çeşitli BT(Bilgi Teknolojileri) varlıklarının bulunduğu kurumsal ağların izlenmesi ve yönetilebilmesi için yaygın olarak kullanılan açık kaynak kodlu Zabbix ve Grafana'nın entegrasyonu yapılmıştır. Zabbix, ağ performansını ve sistem bileşenlerini izleyerek kapsamlı veri toplama ve analiz imkânı sunarken; Grafana, bu verilerin anlamlı ve kolay anlaşılabilir bir şekilde görselleştirilmesini sağlar. Çalışma, bu iki aracın bir arada kullanımı ile etkin kurumsal ağ yönetiminin nasıl ele alınacağını anlatmaktadır. Zabbix'e tanımlı olmayan BT varlıklarının eklenmesi ve bu varlıklardan alınan verilerin Grafana ile görselleştirilmesi sağlanmış ve etkinliği test edilmiştir.

Anahtar Kelimeler: Zabbix, Grafana, Ağ Yönetimi, Veri Görselleştirme, Açık Kaynak Yazılımlar

ABSTRACT

ADDING EFFECTIVE ASSETS TO ZABBİX NETWORK MANAGEMENT SOFTWARE AND VISUALIZATION OF DATA

Gökhan TUĞRUL

In this age, when corporate business processes are transferred to the electronic environment, monitoring and managing the instant status of software and hardware assets in corporate information systems is of great importance for corporate business continuity. Information system software and hardware are managed using network management software. Since there are many different brands of network devices, software, IoT devices, mobile computing devices, cloud-computing devices, it is an important problem for network management software to monitor and manage all kinds of devices.

In this thesis, Zabbix and Grafana, two widely used open source software tools for monitoring and managing corporate networks with a wide variety of IT assets are integrated. While Zabbix provides comprehensive data collection and analysis by monitoring network performance and system components, Grafana provides visualization of this data in a meaningful and easily understandable way. The paper describes how to use these two tools together to address effective enterprise network management. Adding undefined IT assets to Zabbix and visualizing the data from these assets with Grafana is provided and its effectiveness is tested.

Keywords: Zabbix, Grafana, Network Management, Data Visualization, Open Source Software

İÇİNDEKİLER

TABLO LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMA LİSTESİ

SNMP	Simple Network Management Protocol
ICMP	Internet Control Message Protocol
IPMI	Intelligent Platform Management Interface
JMX	Java Management Extensions
WMI	Windows Management Instrumentation
SLA	Service Level Agreement
IoT	Internet of Things
DDoS	Distributed Denial of Service
API	Application Programming Interface
DB	Database
SQL	Structured Query Language
BT	Bilgi Teknolojileri
TCP/IP	Transmission Control Protocol / Internet Protocol
PLC	Programmable Logic Controller
CPU	Central Processing Unit
RAM	Random Access Memory
UPS	Uninterruptible Power Supply
MIB	Management Information Base
PRTG	Paessler Router Traffic Grapher
OİD	Object Identifier
SSL	Secure Socket Layer
TLS	Transport Layer Security
LDAP	Lightweight Directory Access Protocol
SAML	Security Assertion Markup Language
XML	Extensible Markup Language
YAML	Yet Another Markup Language
JSON	Java Script Object Notation
QoS	Quality of Service
CRC	Cyclic Redundancy Check

ITSM	Information Technology Service Management
REST API	Representational State Transfer Application Programming Interface
RAID	Redundant Array of Independent Disks
MS	Milisaniye
MBPS	Megabits Per Second
BİT	Binary Digit
MB	Megabayt
GB	Gigabayt

1.Giriş

Dijitalleşmenin hız kazandığı günümüzde, bilgi teknolojileri altyapılarının kesintisiz ve verimli çalışması, kurumların başarısı açısından kritik bir öneme sahiptir. Bu altyapının omurgasını oluşturan ağ yönetimi, sistem performansını gözlemlemek ve olası arızalara zamanında müdahale etmek için ağ izleme sistemlerine gereksinim duymaktadır. Ancak dijitalleşmenin sunduğu hız, verimlilik ve erişilebilirlik avantajları, aynı zamanda yeni zafiyetler ve operasyonel riskleri de beraberinde getirmiştir. Kurumların veri tabanları, e-posta sistemleri, üretim süreçleri, müşteri ilişkileri ve finansal işlemler gibi temel işlevleri artık karmaşık bilgi teknolojileri altyapıları üzerine inşa edilmekte ve bu durum BT (Bilgi Teknolojileri) altyapılarının kararlı bir şekilde çalışmasını zorunlu kılmaktadır.

Modern dijital altyapılar, yüksek erişilebilirlik, esneklik ve çeviklik gerektirmekte olup, bu gereksinimlerin karşılanabilmesi için altyapı bileşenlerinin performansının sürekli izlenmesi elzemdir. Donanımsal hatalar, yazılımsal arızalar, ağ gecikmeleri ve sistem aşırı yüklenmeleri gibi sorunlar, iş sürekliliğini doğrudan tehdit etmektedir. Özellikle bankacılık, e-ticaret ve üretim sektörlerinde yaşanan kısa süreli kesintiler bile ciddi finansal kayıplara ve itibar kaybına yol açabilmektedir. Bu noktada ağ izleme sistemleri, kurumların BT varlıklarını gerçek zamanlı olarak izleyip performans, erişilebilirlik ve güvenlik açısından değerlendirme yapmasını sağlayarak pratik yönetim imkânı sunmaktadır. Bunun yanı sıra, günümüz kurumları yalnızca fiziksel altyapılarını değil, bulut sistemlerini, hibrit yapıları ve mobil cihazları da izlemek zorundadır. Bu unsurların görünürlüğünü sağlamak ve sorunları henüz kullanıcıya yansımadan tespit edebilmek için bütünleşmiş ve akıllı ağ izleme çözümleri kritik öneme sahiptir. Özellikle siber saldırıların ve zararlı yazılımların arttığı günümüzde; anlık olay tespiti, ağ trafiği analizi ve tehdit izleme işlevleri ağ yönetiminin vazgeçilmez unsurları hâline gelmiştir. Anlık sistem izlemesi yalnızca hataları düzeltmekle kalmayıp, sistem davranışlarının analiz edilerek önleyici stratejiler geliştirilmesine de katkı sunmaktadır. Sistem yöneticileri, geçmiş performans verilerine dayanarak kaynak tahsisi yapabilir, kapasite planlaması gerçekleştirebilir ve iyileştirme alanlarını tespit edebilir. Ayrıca olay korelasyonu, uyarı yönetimi ve SLA (Service Level Agreement) takibi gibi ileri seviye özellikler, ağ izleme sistemlerinin operasyonel değerini artırmaktadır.

Dijitalleşmenin sunduğu hız ve ölçek avantajları, beraberinde izlenebilirlik, güvenilirlik ve yönetilebilirlik gibi sorumlulukları da getirmiştir. Bu bağlamda, anlık ve merkezi sistem izlemesi yalnızca BT operasyonları için değil, kurumların genel iş sürekliliği, karar alma hızı ve hizmet kalitesi açısından da stratejik bir zorunluluk hâline gelmiştir.

Zabbix açık kaynaklı, esnek, ölçeklenebilir ve geliştirilebilir mimarisiyle öne çıkan bir ağ izleme yazılımı olarak dikkat çekmektedir. Zabbix, hem küçük ölçekli kurulumlarda hem de kurumsal altyapılarda yaygın şekilde kullanılmakta; SNMP (Simple Network Management Protocol), ICMP (Internet Control Message Protocol), Modbus ve Zabbix ajanı gibi çeşitli protokollerle geniş bir izleme imkânı sunmaktadır. Ancak, toplanan verilerin anlık olarak analiz edilmesi ve görsel sunumlarla desteklenmesi için Grafana gibi güçlü bir görselleştirme aracına ihtiyaç duyulmaktadır. Zabbix ile Grafana entegrasyonu sayesinde, sistem yöneticileri sezgisel, özelleştirilebilir ve etkileşimli paneller üzerinden kapsamlı içgörüler elde edebilmektedir [1]. Roger Assunção ve arkadaşları, bu entegrasyonun kullanıcı dostu paneller ile hizmet kesintilerinin önüne geçmede kritik rol oynadığını belirtirken, Da Silva ve arkadaşları da otomatik keşif, esnek uyarı mekanizmaları ve iş odaklı metriklerin görselleştirilmesi yönüyle önemli katkılar sunduğunu vurgulamıştır [2;3].

Zaman serisi verilerinin yorumlanması yalnızca teknik ekipler için değil, aynı zamanda yönetim kademesi için de kritik bir işlevdir. Grafana üzerinde oluşturulan gösterge panelleri, farklı birimlerin kendi iş süreçlerine ilişkin metrikleri eş zamanlı izlemesine ve veri temelli kararlar almasına olanak tanımaktadır [3]. Bu yaklaşım, özellikle SLA takipleri, işlem süreleri ve hata oranları gibi metriklerin izlenmesi yoluyla operasyonel süreçlerin optimize edilmesine katkı sağlamaktadır. Öte yandan, yapay zekâ ve makine öğrenimi temelli analizlerin ağ izleme altyapılarına entegrasyonu da hızla yaygınlaşmaktadır. Bu entegrasyonlar sayesinde, geçmiş verilerden öğrenerek olası arızaların öngörülmesi, kapasite planlaması yapılması ve aykırılık tespiti gerçekleştirilmesi mümkün olmaktadır. Böylece ağ yönetimi reaktif bir yapıdan öngörülü ve pratik bir yapıya dönüşmektedir. Nitekim Moosa ve arkadaşları tarafından yapılan çalışmada, Zabbix tabanlı bir ağ izleme altyapısının zamanında müdahale ve esnek kaynak kullanımı sağladığı vurgulanmıştır. Aynı araştırmada, sistem uyarılarının Grafana gösterge panellerine entegre edilmesi sayesinde operasyonel kararların daha hızlı ve veri temelli şekilde alınabildiği belirtilmiştir [4]. Bununla birlikte, Tuan ve arkadaşları tarafından yürütülen çalışmada, Zabbix'in fiziksel ve sanal cihazlarda yüksek veri trafiği altında başarılı bir şekilde izlenebilirliği gösterilmiştir. Bu uygulama, yüksek veri hacmine sahip heterojen ağ ortamlarında Zabbix'in ölçeklenebilirlik ve güvenilirlik açısından güçlü bir çözüm sunduğunu ortaya koymuştur. Gelişmiş otomasyon özellikleri ve SNMP tabanlı derinlemesine donanım izleme, yüksek güvenilirlik gerektiren ortamlarda kesintisiz operasyonu mümkün kılmaktadır [5]. Barros ve arkadaşları Zabbix'in büyük ölçekli ağlarda uygulandığında yüksek esneklik ve genişleyebilirlik sunduğunu, Grafana ile birlikte kullanıldığında ise operasyonel verilerin daha anlaşılır ve hızlı yorumlanmasına imkân tanıdığını ifade etmektedir [6].

Guo ve arkadaşları ise enerji sektöründe Zabbix tabanlı izleme sisteminin, cihaz performans verilerini SNMP aracılığıyla toplayarak operasyonel verimliliği artırdığını ve Grafana ile bütünleşik görselleştirme sayesinde karar alma süreçlerini hızlandırdığını belirtmiştir [7]. Öte yandan, Antonio Luiz ve arkadaşları çalışmasında, endüstriyel üretim ortamlarında Zabbix'in yalnızca maliyet avantajı değil, esnek yapılandırma imkânı ve görsel raporlama kabiliyeti sayesinde iş zekâsı destekli karar alma süreçlerine de önemli katkılar sunduğu ifade edilmiştir. Grafana'nın sezgisel görselleştirme yapısı sayesinde teknik veriler sadeleştirilerek yönetim seviyesine uygun gösterge panelleri oluşturulmuş, böylece karar alma süreçlerine katkı sağlanmıştır. Bu çalışma, ağ izleme sistemleri ile karar destek sistemleri entegrasyonu konusunda literatürde önemli bir boşluğu doldurmaktadır [8].

Bilgi teknolojileri altyapılarının sürdürülebilirliği, sistem kararlılığı, performans kontrolü ve güvenlik izleme gereksinimleriyle doğrudan ilişkilidir. Bu bağlamda ağ yönetim sistemleri, merkezi izleme çözümleriyle kurumsal BT süreçlerinin bütünlüğünü garanti altına almaktadır. Özellikle SNMP; yönlendirici, ağ anahtarı, güvenlik duvarı gibi ağ donanımlarından gerçek zamanlı veri çekmeye imkân tanımakta, ağ performansının ölçülmesinde standart bir protokol olarak öne çıkmaktadır [2]. Bunun yanında ICMP protokolü ile bağlantı erişilebilirliği test edilmekte; IPMI (Intelligent Platform Management Interface), JMX (Java Management Extensions) ve WMI (Windows Management Instrumentation) gibi protokoller ise Java uygulamaları ya da Windows servislerinin gözlemlenmesini mümkün kılmaktadır [9]. Bu protokolleri destekleyen çok sayıda yazılım bulunmaktadır. Nagios, esnek modüler yapısı ve açık kaynak karakteriyle yaygın olarak kullanılmakta; PRTG ise özellikle Windows ortamlarında sezgisel grafik arayüzüyle tercih edilmektedir [10]. Grafana, zaman serisi verilerin görselleştirilmesinde benzersiz olanaklar sunarken, OpManager ve WhatsUp Gold gibi ticari araçlar, küçük ve orta ölçekli işletmelere hızlı kurulum ve düşük öğrenme eğrisi avantajı sağlamaktadır [11]. Ancak bu araçların çoğu ya lisans sınırlamaları içerir ya da özelleştirme konusunda sınırlı esneklik sağlar. Bu noktada Zabbix, tamamen açık kaynak kodlu yapısı, lisans

maliyetinden bağımsızlığı ve yüksek özelleştirile bilirliği ile öne çıkmaktadır [5]. Her ölçekte ağ altyapısına kolaylıkla entegre edilebilen bu sistem, küçük kurumlardan büyük veri merkezlerine kadar geniş bir kullanıcı yelpazesine hitap etmektedir [4].

Zabbix'in mimarisi dört temel bileşenden oluşmaktadır; merkezi sunucu, ajanlar, proxy'ler ve web tabanlı ara yüz. Merkezi sunucu tüm verilerin işlendiği ve saklandığı çekirdektir. Ajanlar, Linux, Windows ya da BSD tabanlı sistemlerde çalışarak donanım ve yazılım metriklerini raporlar; Proxy bileşeni ise coğrafi olarak dağılmış yapılardan gelen verileri birleştirerek merkezileştirir [12]. Cristina ve arkadaşları bu mimari yapının ağ gecikmesi, veri bütünlüğü ve güvenlik açısından nasıl yapılandırılabileceği konusunda örneklendirmelerde bulunmuşlardır [13].

Zabbix ajanları; CPU kullanımı, RAM tüketimi, disk kapasitesi, işlem yükü gibi kritik metrikleri raporlayabilmektedir. SNMP ile donanım durumları, ICMP ile erişim kontrolleri, JMX ve WMI ile uygulama ve servis seviyesinde izleme sağlanmaktadır. Endüstriyel otomasyon sistemlerinde ise Modbus ve SNMP protokolleriyle PLC'ler, iklimsel sensörler ve çevresel aygıtlar etkin biçimde gözlemlenmektedir [7].

Kurulum süreci Debian, Ubuntu, CentOS gibi popüler Linux dağıtımlarında desteklenmekte; veri tabanı olarak MariaDB veya PostgreSQL tercih edilmektedir. Pedro ve arkadaşları tarafından sanallaştırılmış ortamlarda yapılan kurulum çalışmalarında ise ağ gecikmesi ve kaynak tahsisi gibi başlıkların kurulum sonrası izleme kalitesine etkisi tartışılmıştır [14].

Yulvianda ve arkadaşları Zabbix'in otomatik varlık keşfi özelliği, özellikle büyük ve heterojen yapılarda SNMP ile cihazların tanınmasına yönelik çalışmalar yapmıştır [15]. Renaldi ve arkadaşları tarafından yapılan çalışmada da, bu özelliğin yapılandırma süresini kısaltarak kullanıcı hatasını azalttığı vurgulanmıştır [16].

Kurulum sonrası yapılandırma adımları arasında kullanıcı yönetimi, bileşen tanımlamaları, şablon ve tetikleyici atamaları ile bildirim sistemlerinin yapılandırılması yer almaktadır [11;17]. Bazı çalışmalarda, olay tabanlı otomatik eylemlerle sistem performansının artırıldığı ve insan müdahalesine gerek kalmadan hata yanıtı verilebildiği aktarılmıştır [18;19].

Zabbix'in kendi görselleştirme araçları temel grafik raporları oluşturabilirken, daha gelişmiş panolar için sıklıkla Grafana entegrasyonu tercih edilmektedir [20;21]. Alex Ruben ve arkadaşlarının çalışmalarında, bu entegrasyonun kesinti sürelerini ciddi oranda düşürdüğü gösterilmiştir [22]. Anderson ve arkadaşlarının yaptığı çalışmada ise Grafana entegrasyonu sayesinde orta ölçekli işletme düzeyinde karar destek mekanizmalarının güçlendirildiği ifade edilmiştir [23].

Zabbix'in sektörel uç uygulamaları oldukça geniştir. Eğitim kurumlarında, kamu altyapılarında, enerji ve güç sistemlerinde, çevresel izleme ve IoT (Internet of Things) sistemlerinde, ayrıca DDoS (Distributed Denial of Secrets) tehdit analizlerinde etkili biçimde kullanıldığı tespit edilmiştir [15;17;6;8;24]. Okul temelli bir ağ izleme örneğinde, Moosa ve arkadaşlarının yaptığı çalışmada sistemin çok düzeyli yapılandırma ile nasıl uygulandığı detaylı biçimde ele alınmıştır [4]. Kurumsal karar destek sistemlerinde de Zabbix'ten gelen veriler, performans karnesi modeli gibi yöntemlerle analiz panolarında kullanılmaktadır [25]. Mateo Munoz arkadaşlarının yaptığı çalışmada, performans metriklerinin yönetim düzeyine nasıl aktarılabileceği vurgulanmıştır [26].

Yapay zekâ destekli izleme sistemlerinde Zabbix veri kaynağı olarak kullanılmakta ve aykırılık tespiti, önleyici bakım gibi uygulamalara temel teşkil etmektedir. Chen ve arkadaşları, karar ağacı algoritmalarıyla hata tahmin modeli oluştururken, Kurmanayeva ve arkadaşları ise yaptıkları çalışmada yapay zekâ ile uyarı eşiklerinin dinamik biçimde güncellenmesini sağlamışlardır [9;27].

Ana Margarida Costa Pinto'nun karşılaştırmalı analizine göre Zabbix sisteminin maliyet etkinliği, genişletile bilirliği ve uyum kolaylığı açısından uzun vadeli izleme altyapılarında öne çıktığı anlaşılmaktadır [10].

Bu tez çalışmasında, açık kaynak kodlu ağ izleme yazılımı Zabbix ile gelişmiş veri görselleştirme aracı Grafana'nın entegrasyonu ele alınmış; özellikle SNMP tabanlı cihazlardan otomatik XML (Extensible Markup Language) şablon üretimi yapılarak, yüzlerce cihazın manuel tanımlama ihtiyacını ortadan kaldıran özgün bir yöntem geliştirilmiştir. Ayrıca, Siemens SIMATIC S7 PLC ve IM153-4PN gibi endüstriyel bileşenlerin izlenmesiyle, bu yaklaşımın Endüstri 4.0 uygulamalarında kullanılabilirliği ortaya konulmuştur. Çalışmada Zabbix'in güçlü izleme altyapısı ile Grafana'nın esnek görselleştirme kabiliyetleri birleştirilerek, yalnızca teknik personelin değil aynı zamanda karar verici yöneticilerin de faydalanabileceği çok katmanlı paneller geliştirilmiştir. Bu yönüyle çalışma, literatürdeki mevcut araştırmalardan farklı olarak hem kurumsal ağ yönetimi hem de endüstriyel üretim ortamları için bütünleşik, ölçeklenebilir ve yönetici odaklı bir izleme modeli sunmaktadır.

Tezin bundan sonraki organizasyonu aşağıdaki gibi yapılmıştır:

Bölüm 2: Zabbix'in ağ izleme mimarisi, ajanları, protokolleri, veri tabanı yapısı, web ara yüzü ve olay yönetimi modülleriyle birlikte sunduğu bütünleşik izleme yetenekleri anlatılmıştır.

Bölüm 3: Zabbix'e ağ varlıklarının manuel, otomatik keşif ve otomatik kayıt yöntemleriyle sisteme eklenmesi, etiketleme yoluyla yönetilmesi ve XML, YAML (Yet Another Markup Language), JSON (Java Script Object Notation) destekli entegrasyonlarla otomasyonun sağlanması ele alınmıştır.

Bölüm 4: Zabbix verilerinin görselleştirilmesi ve Grafana ile uyumu ele alınmıştır. Grafana uyumu ile gelişmiş paneller, zaman serisi analizleri ve etkileşimli görselleştirmeler aracılığıyla daha esnek, anlaşılır ve stratejik karar destek sağlayacak şekilde sunulmuştur.

Bölüm 5: Zabbix'in kurumsal ve endüstriyel ağlarda uygulanarak SNMP tabanlı cihaz izleme, Python betik ile otomatik şablon üretme ve farklı donanımların kapsamlı şekilde takip edilmesini sağlayan Zabbix uygulama ağı ele alınmıştır.

Bölüm 6: Zabbix'ten alınan ağ, sunucu ve PLC verilerinin Grafana panelleriyle karşılaştırmalı, çok katmanlı ve kullanıcı dostu şekilde görselleştirilmesi bu bölümde ele alınmıştır.

Bölüm 7: Sonuç ve gelecek çalışmalara yönelik öneriler sunulmuştur.

2. Ağ İzleme Yazılımları ve Zabbix'in Ağ İzleme Yetenekleri

2.1 Ağ İzleme Yazılımları

Ağ izleme, BT altyapısının sürekliliği ve performansının korunması açısından kritik öneme sahiptir. Bu amaçla birçok farklı yazılım geliştirilmiş olup, her biri belirli güçlü yönlere ve sınırlılıklara sahiptir. Literatürde öne çıkan bazı ağ izleme yazılımları aşağıda özetlenmiştir:

Nagios: Nurrohman ve arkadaşlarına göre Nagios, geniş eklenti desteği sayesinde esnek bir yapı sunsa da, büyük ölçüde manuel yapılandırmalara bağlıdır ve kullanıcı ara yüzü sınırlıdır [11].

Cacti: Serras ve arkadaşlarına göre Cacti, esas olarak SNMP verilerinden grafikler üretmeye odaklanmış olup; uyarılar, geçmiş analizleri ve farklı veri kaynaklarıyla uyum kabiliyeti sınırlıdır [12].

Prometheus: Barros ve arkadaşlarına göre Prometheus, çekme toplama modeli ve optimize edilmiş geçici depolama özelliği sayesinde mikro hizmet ortamları için uygundur. Ancak uzun vadeli veri saklama konusunda sınırlılıkları bulunmaktadır [6].

ELK Stack (Elasticsearch, Logstash, Kibana): Moosa ve arkadaşlarına göre log analizi konusunda çok güçlüdür, fakat gerçek zamanlı performans metriklerinin izlenmesi açısından Zabbix ile Grafana'nın sunduğu kapsamlı çözümün gerisinde kalmaktadır [4].

Pandora FMS: Assunção ve arkadaşlarına göre Pandora FMS, Zabbix'e benzer çok yönlü işlevler sunmaktadır. Ancak Zabbix, daha geniş topluluk desteği, hazır şablonları ve aktif kullanıcı tabanı sayesinde daha yaygın olarak kullanılmaktadır [2].

Tablo 1. Ağ izleme yazılımlarının karşılaştırılması

Yazılım	Güçlü Yönleri	Sınırlılıkları / Zayıf Yönleri	Kaynak
Nagios	Eklenti desteği, esneklik, yaygın kullanım	Manuel yapılandırma, sınırlı ara yüz	[11]
Cacti	SNMP tabanlı grafikleme, basit kurulum	Yalnızca SNMP 'ye odaklı, sınırlı entegrasyon	[12]
Prometheus	Mikro hizmet uyumu, hızlı toplama modeli	Geçici depolama, uzun vadeli analiz eksikliği	[6]
ELK Stack	Log analizi, güçlü arama ve görselleştirme	Gerçek zamanlı metrik izleme sınırlı	[4]
Pandora FMS	Çok yönlü yapı, esneklik	Daha küçük topluluk, sınırlı hazır şablon desteği	[2]
Zabbix	Çok protokollü destek, güçlü topluluk, hazır şablonlar	Öğrenme eğrisi nispeten yüksek	[2],[6]

2.2 Zabbix‘in Ağ İzleme Yetenekleri

Zabbix, açık kaynaklı ve ölçeklenebilir mimarisiyle farklı ağ izleme yazılımlarına kıyasla daha bütüncül bir çözüm sunmaktadır [2;6]. SNMP, ICMP, IPMI, JMX ve WMI gibi birçok protokolü doğal olarak destekleyen sistem, hem küçük ölçekli kurumlar hem de büyük kurumsal altyapılar için uygundur [7]. Bu kapsam Tablo 2‘de özetlenmiştir.

Tablo 2 .Zabbix‘in desteklediği protokoller ve sağladığı izleme kapsamı

Protokol	İzleme Kapsamı	Kullanım Alanı / Cihaz Türü
SNMP	Donanım metrikleri (işlemci, bellek, port trafiği, sensör verileri)	Ağ anahtarı, yönlendirici, güvenlik duvarı, PLC, IoT cihazları
ICMP	Erişilebilirlik ve gecikme testi	Tüm ağ cihazları, sunucular
JMX	Uygulama ve servis metrikleri	Java tabanlı uygulamalar
WMI	Sistem ve servis izleme	Windows sunucuları, Microsoft hizmetleri
IPMI	Donanım yönetimi (sıcaklık, fan, voltaj)	Sunucular
Modbus	Endüstriyel veri toplama	PLC’ler, sensörler, üretim hatları

Zabbix‘in tercih edilme nedenleri arasında çok protokollü destek sayesinde ağ cihazlarından sunuculara, uygulamalardan endüstriyel ekipmanlara kadar geniş yelpazede izleme imkânı sunması; ölçeklenebilir mimarisiyle farklı veri toplama yöntemlerini aynı anda kullanarak gerçek zamanlı performans takibi yapabilmesi; açık kaynak ve ücretsiz olmasıyla lisans maliyetlerini ortadan kaldırması; esnek uyarı mekanizmalarıyla tanımlanabilir eşikler, bildirim sistemleri ve otomatik aksiyonlara olanak sağlaması; geçmiş veri analiziyle performans trendlerini inceleme, kapasite planlaması ve aykırılık tespiti yapılabilmesi; güçlü küresel topluluk desteği, düzenli güncellemeler, kapsamlı dokümantasyon ve forum desteği sunması yer almaktadır [6;10;3;4;2].

Bununla birlikte Zabbix, yalnızca ağ izleme değil; aynı zamanda sunucu, uygulama, veri tabanı ve endüstriyel cihaz izleme kabiliyetleriyle hibrit altyapılar için merkezi bir yönetim çözümü sunmaktadır [8]. Bu özellikleri sayesinde rakip çözümlerden ayrılmakta ve hem BT operasyonları hem de karar destek mekanizmaları için tercih edilmektedir [6],[23]. Ayrıca Zabbix‘in güçlü otomasyon yetenekleri, insan müdahalesini en aza indirerek operasyonel verimliliğini artırmakta ve önceden tanımlanmış eylemler sayesinde kritik olaylara otomatik yanıt verilmesine olanak tanımaktadır [19]. Böylece sistemde yaşanabilecek kesintilerin süresi önemli ölçüde azaltılmaktadır. Grafana ile entegrasyonu sayesinde elde edilen veriler, yönetim kademesi için anlaşılır ve etkileşimli panellere dönüştürülmekte, bu da stratejik karar alma süreçlerine doğrudan katkı sağlamaktadır [22],[23]. Zabbix aynı zamanda rol tabanlı erişim kontrolleri ile güvenlik boyutunu desteklemekte, farklı kullanıcı gruplarının yetkilendirilmesine imkân tanımaktadır [8]. Tüm bu yönleriyle Zabbix, yalnızca bir izleme aracı değil, kurumların bütünleşik BT yönetim stratejilerinin merkezinde yer alan kapsamlı bir çözüm haline gelmiştir [10].

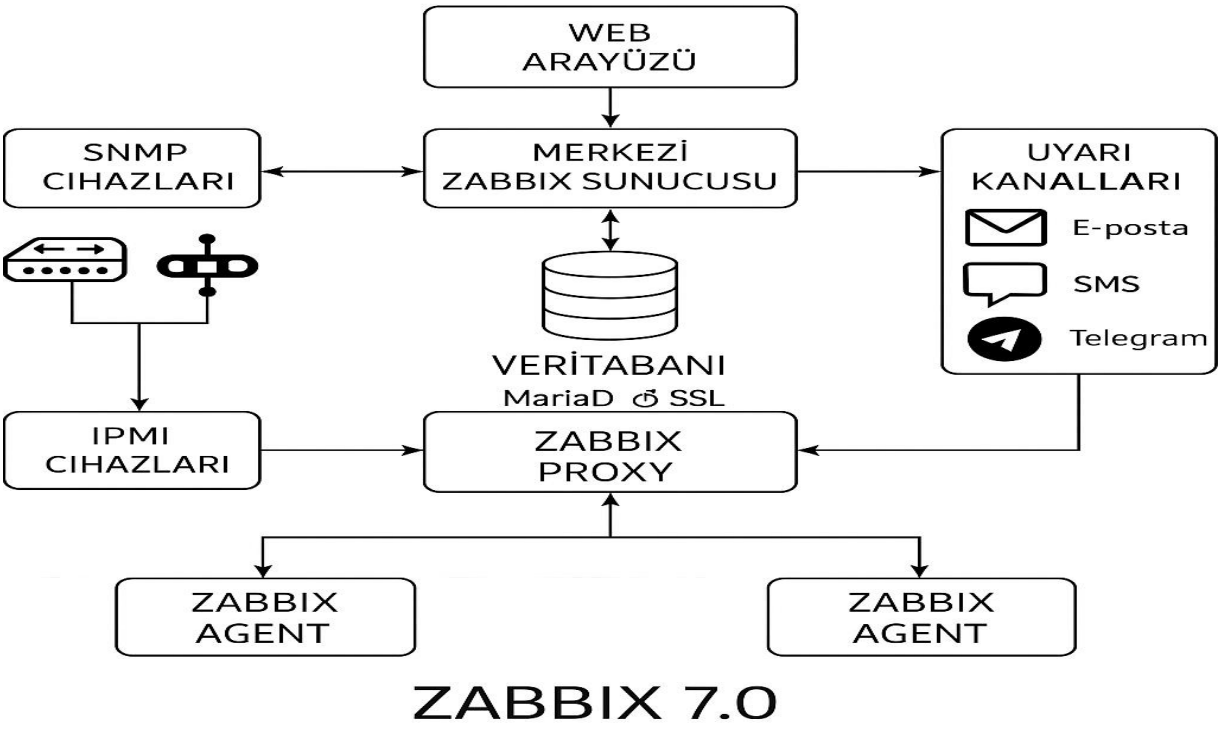
Zabbix‘in öne çıkan bir diğer yönü, kurumların farklı ölçek ve ihtiyaçlarına uyum sağlayabilecek esnek uyum kabiliyetidir. REST API (Representational State Transfer Application Programming Interface) desteği sayesinde üçüncü taraf yazılımlarla kolayca entegre edilebilmekte, ITSM (Information Technology Service Management) çözümleri,

biletleme sistemleri, otomasyon araçları ve güvenlik yazılımlarıyla birlikte kullanılabilmektedir [2]. Bu sayede olay yönetimi süreçleri uçtan uca bütünleşik bir yapıya kavuşturulmakta, hem teknik ekiplerin iş yükü azaltılmakta hem de kurumsal karar alma süreçleri hızlandırılmaktadır [23]. Endüstriyel ortamlarda ise PLC'ler, SCADA sistemleri, sensörler ve çevresel aygıtlar ile uyum sağlanarak üretim hatlarının sürekliliği garanti altına alınmaktadır [8]. Böylelikle yalnızca BT altyapısının değil, üretim ve operasyonel süreçlerin de güvenilirliği artırılmaktadır. Ayrıca, büyük veri analitiği ve yapay zekâ destekli algoritmalar ile birlikte kullanıldığında Zabbix'in sunduğu veriler öngörücü bakım, kapasite planlaması ve aykırılık tespiti gibi alanlarda kritik katkılar sunmaktadır [9],[27]. Gelecekte makine öğrenimi tabanlı dinamik eşik değerleri, otomatik karar mekanizmaları ve daha ileri düzey siber güvenlik modülleriyle birleşerek Zabbix'in yalnızca bir izleme aracı olmanın ötesinde, kurumsal dijital dönüşümün temel bileşenlerinden biri haline gelmesi beklenmektedir [6].

2.3 Zabbix Ağ Mimarisi

Mimaride yer alan başlıca bileşenler Zabbix Sunucu, Zabbix Vekil Sunucu, Veri tabanı, Zabbix Ajan, IPMI cihazları, SNMP cihazları, Web ara yüzü ve uyarı kanallarıdır. Söz konusu bileşenler bu bölüm altında açıklanmıştır.

Tez çalışmamızda kullandığımız ve hali hazırda güncel sürüm olan Zabbix 7.0 mimari yapısı Şekil 1 de görülmektedir.



Şekil 1. Zabbix 7.0 genel mimari yapısı

Merkezi Zabbix Sunucusu

Zabbix mimarisinin temelini oluşturan merkezi sunucu, tüm verilerin işlendiği ve yönetildiği ana bileşendir. İzlenen cihazlardan gelen verileri toplar, veri tabanına kaydeder, tetikleyiciler aracılığıyla olayları üretir ve ilgili uyarı mekanizmalarını devreye sokar.

Zabbix Vekil Sunucu

Vekil sunucu bileşeni, özellikle geniş ve dağınık ağ yapılarında, uzak bölgelerdeki cihazların merkezi sunucuya doğrudan erişim sağlamasına gerek kalmadan izlenmesini sağlar.

Vekil sunucu; ajanlar, SNMP veya IPMI cihazlarından veri toplar, bu verileri geçici olarak saklar ve belirli aralıklarla merkezi sunucuya iletir. Bu yaklaşım, ağ üzerindeki trafiği azaltır ve yük dengelemesi sağlar.

Zabbix Ajan

Zabbix Ajan, izlenen sistemlere doğrudan kurulan hafif istemci uygulamasıdır. Zabbix sunucusuna veya vekil sunucu bileşenine veri göndererek sistem kaynaklarının detaylı izlenmesine olanak tanır. Özellikle işlemci kullanımı, bellek durumu, disk alanı, işlemci sıcaklığı, ağ ara yüzü trafiği, çalışan servisler, oturum bilgileri, sistem aktif çalışma süresi değeri ve aktif kullanıcılar gibi birçok sistem düzeyinde bilgiyi toplar. Zabbix ajanı, çok geniş bir platform yelpazesinde çalışacak şekilde geliştirilmiştir. Resmi olarak desteklenen işletim sistemleri arasında; Windows 10, Windows 11 ve Windows Server 2012, 2016, 2019 ve 2022 sürümleri yer almaktadır. Linux tarafında ise Debian, Ubuntu, CentOS, RHEL, Fedora, SUSE ve Oracle Linux gibi yaygın dağıtımlar desteklenmektedir. Ayrıca, MacOS 10.14 ve üzeri sürümler, FreeBSD, OpenBSD, NetBSD gibi Unix türevi sistemler ile AIX, HP-UX ve Solaris gibi kurumsal işletim sistemleri için de ajan paketleri sunulmaktadır. Bu geniş destek yelpazesi, Zabbix'in çok platformlu yapılarda esnek ve bütüncül izleme sağlayabilmesini mümkün kılmaktadır.

Zabbix ajanı iki farklı sürüm halinde sunulmaktadır: Klasik Zabbix ajanı ve Zabbix Ajan 2. Klasik sürüm C programlama diliyle yazılmıştır ve uzun süredir kararlı şekilde kullanılmaktadır. Buna karşılık Zabbix Ajan 2, Google tarafından geliştirilen ve yüksek performanslı uygulamalar için tercih edilen Golang programlama dili ile yazılmıştır. Bu yeni nesil ajan, eklenti tabanlı mimarisi sayesinde daha esnek yapı sunmakta ve Prometheus Exporter uyumluluğu, Kafka, PostgreSQL gibi sistemler için yerleşik parça desteği ile daha fazla metrik toplayabilmektedir. Bu özellikler, özellikle karmaşık altyapılarda detaylı ve özelleştirilebilir izleme gereksinimlerini karşılamak açısından önemlidir.

Zabbix Ajan ile Toplanabilen Veriler

Windows işletim sistemine kurulan Zabbix ajan aracılığıyla çok sayıda sistemsel ve uygulama düzeyinde veri toplanabilmektedir. Toplanabilecek başlıca metrikler arasında; işlemci kullanımı (örneğin %idle, %user, %system gibi), bellek durumu (toplam, kullanılabilir ve kullanılan bellek miktarı), her birim için ayrı ayrı disk kullanımı ve Windows servislerinin çalışma durumu (örneğin "MSSQLSERVER" servisi aktif mi?) yer almaktadır. Ayrıca, güvenlik, sistem ve uygulama gibi günlük kayıtlarının tutulduğu Windows Olay Günlükleri de izleme kapsamına alınabilmektedir. Sistemde çalışan süreçlerin adları, ağ ara yüzlerinin durumu ile birlikte gönderilen/alınan paket ve byte trafiği gibi ağ performansı göstergeleri de ajan üzerinden izlenebilir. Buna ek olarak, oturum açan kullanıcı sayısı ve kullanıcı adları, sistemdeki kullanıcı etkinliklerinin takip edilmesini sağlarken, PowerShell betikleri aracılığıyla özel kontroller gerçekleştirilerek izleme kapsamı ihtiyaca göre genişletilebilmektedir.

Linux işletim sistemlerinde çalışan Zabbix ajan aracılığıyla, sistem performansına ve kaynak kullanımına dair birçok kritik metrik gerçek zamanlı olarak izlenebilmektedir.

Örneğin, system.cpu.util[,user] öğesi, işlemcinin kullanıcı modunda geçirdiği zamanın yüzdesini ölçerken, system.cpu.load[percpu,avg1] parametresi son bir dakikalık ortalama işlemci yükünü her bir işlemci çekirdeği için ayrı ayrı hesaplamaktadır. Disk kullanımı, vfs.fs.size[/,used] ile izlenebilirken; belirli bir dosyanın sistemde mevcut olup olmadığı, örneğin /var/log/syslog dosyası için vfs.file.exists[/var/log/syslog] öğesiyle kontrol edilmektedir. Ağ trafiği açısından, net.if.in[eth0] ile belirli bir ara yüz üzerinden gelen veri miktarı; net.if.out[eth0] ile ise dışa gönderilen veri miktarı ölçülebilmektedir. Ayrıca system.uptime öğesi cihazın yeniden başlatılmadan önceki toplam çalışma süresini saniye cinsinden verirken, proc.num[] sistemdeki aktif işlem sayısını ve system.sw.packages öğesi ise ilgili Linux sistemine yüklü toplam yazılım paketlerinin sayısını raporlamaktadır. Bu öğeler sayesinde, Linux tabanlı sunucuların sistemsel sağlık durumu, performans düzeyi ve kaynak kullanımı ayrıntılı şekilde izlenebilmektedir.

Mimari Yapı ve Protokoller

Zabbix ajanı, Zabbix sunucusu veya vekil sunucu ile genellikle TCP (Transmission Control Protocol)/10050 portu üzerinden iletişim kurmakta olup, bu iletişim hem aktif hem de pasif modda gerçekleştirilebilmektedir. Aktif modda ajan, belirli zaman aralıklarında sunucuya bağlanarak gerekli verileri pratik biçimde iletirken; pasif modda ise sunucu, ajana bağlanarak veri çekimini doğrudan kendisi başlatmaktadır. Ajan, sistemden bilgi toplamak amacıyla çeşitli yerleşik anahtarlar kullanmaktadır. Örneğin, system.run[] sunucu üzerinden komut çalıştırılmasına olanak tanırken; agent.ping ajan servisinin çalışır durumda olup olmadığını kontrol eder. Ayrıca, log[] komutu kullanılarak belirli günlük dosyaları analiz edilerek anormal durumlar tespit edilebilmektedir. Zabbix Ajan 2 sürümü ile birlikte, TLS desteği sayesinde ajan ile sunucu arasındaki iletişim şifrelenebilmekte; dâhili eklenti sistemi ile özelleştirilebilir modüller desteklenmekte ve paralel sorgulama mekanizması ile daha düşük kaynak tüketimi sağlanabilmektedir. Çok platformlu desteği, geniş metrik yelpazesi ve özelleştirilebilir yapısı sayesinde Zabbix ajanı, hem sunucu sistemlerinde hem de uç kullanıcı cihazlarında kapsamlı performans ve durum takibi yapılmasını mümkün kılmakta; özellikle Zabbix Ajan 2 ile gelen modüler yapı, gelecekteki izleme ihtiyaçlarına uyarlanabilir bir altyapı sunmaktadır.

SNMP Cihazları

SNMP, TCP/IP (Transmission Control Protocol / Internet Protocol) ağlarında yer alan cihazların yönetimi ve izlenmesi amacıyla yaygın biçimde kullanılan bir protokoldür. SNMP destekli cihazlar (örneğin yönlendiriciler, anahtarlar, erişim noktaları, UPS (Uninterruptible Power Supply) cihazları, IP kameralar ve yazıcılar) Zabbix gibi ağ izleme yazılımlarıyla kolaylıkla bütünleştirilebilir. Bu cihazlar, sistem performans metriklerini ve olay durumlarını MIB (Management Information Base) olarak adlandırılan veri kümeleri üzerinden sunar. Zabbix, bu bilgileri nesne tanımlayıcısı kullanarak sorgular ve SNMP cihazlarının performansını merkezi olarak izleyebilir. SNMP cihazları çoğunlukla doğrudan Zabbix sunucusu veya gerekiyorsa vekil sunucu üzerinden izlenir. İzleme işlemi, SNMPv1, SNMPv2c ve daha güvenli olan SNMPv3 gibi protokol sürümleri üzerinden gerçekleştirilebilir. Özellikle SNMPv3, kimlik doğrulama ve şifreleme mekanizmaları içerdiğinden kurumsal yapılarda tercih edilmektedir.

Zabbix, SNMP cihazlarını izlemek için hazır şablonlar sunmakta ve bu şablonlar sayesinde cihazın türüne özel metrikler (işlemci, bellek, trafik, bağlantı durumu gibi) otomatik olarak izlenebilir hale gelmektedir. Eğer cihaz için Zabbix'te hazır bir şablon bulunmuyorsa, SNMP nesne tanımlayıcıları manuel olarak eklenerek özelleştirilmiş şablonlar oluşturulabilir.

SNMP üzerinden verilerin etkin şekilde alınabilmesi için bazı temel yapıların doğru anlaşılması gerekmektedir. Bunların başında Yönetim Bilgi Tabanı gelmektedir. MIB, ağ cihazlarının sunduğu izlenebilir verilerin anlamlı bir sözlük biçiminde tanımlandığı veri yapısıdır.

Bu yapının içinde yer alan her bir veri öğesi, kendine özgü bir nesne tanımlayıcı ile temsil edilmektedir. Örneğin, bir ağ cihazındaki işlemci sıcaklığı .1.3.6.1.4.1.x.y.z gibi bir OİD(Object Identifier) ile erişilebilmektedir. SNMPv1 ve SNMPv2c sürümlerinde erişim kontrolü için kullanılan community string ifadesi (örneğin "public" veya "private") ise, adeta parola işlevi görmektedir. Ayrıca, SNMP cihazları belirli olaylar gerçekleştiğinde (örneğin bağlantı kesilmesi, aşırı yüklenme) Zabbix gibi izleme sistemlerine trap adı verilen anlık bildirimleri otomatik olarak gönderebilmektedir.

Zabbix ile SNMP protokolü kullanılarak izleme yapılabilmesi için belirli adımlar izlenmelidir. İlk olarak, izlenecek cihazın SNMP desteğinin aktif hale getirilmesi gerekmektedir. Ardından, Zabbix web ara yüzü üzerinden ilgili ağ cihazı tanımlanır ve SNMP ara yüzü yapılandırılır. Sonrasında cihaz türüne uygun bir SNMP şablonu ilişkilendirilerek veri öğeleri, tetikleyiciler ve grafik tanımları yapılır. Zabbix geliştirici topluluğu, bu süreçte özellikle OİD değerlerinin SNMPwalk gibi araçlarla test edilmesini, veri toplama aralıklarının cihaz performansını etkilemeyecek şekilde yapılandırılmasını ve eşik değerlerinin sahadaki ihtiyaçlara uygun biçimde tanımlanmasını önermektedir. Eğer çok sayıda benzer cihaz izlenecekse, bu durumda Low-Level Discovery (LLD) mekanizmasının kullanımıyla yapılandırmaların otomatikleştirilmesi tavsiye edilmektedir. Zabbix'in SNMP desteği sayesinde, ağ omurgası, üretim altyapısı ve uzak lokasyonlardaki donanımlar merkezi olarak izlenebilmekte; böylece arıza öncesi tespit imkânı sunularak iş sürekliliği önemli ölçüde artırılabilmektedir.

IPMI Cihazları

IPMI protokolünü destekleyen sunucular ve donanımlar, donanım düzeyindeki bilgilerin (örneğin sıcaklık, fan hızı, güç durumu) uzaktan yönetimini sağlar. Bu veriler genellikle Zabbix Vekil Sunucu aracılığıyla toplanır.

Veri Tabanı (MariaDB üzerinden SSL (Secure Sockets Layer))

Zabbix, tüm yapılandırma bilgilerini, toplanan verileri, olay günlüklerini, tarihsel izleme kayıtlarını ve kullanıcı ayarlarını bir ilişkisel veri tabanı yönetim sistemi üzerinde depolar. Desteklenen veri tabanı sistemleri arasında MySQL/MariaDB, PostgreSQL, Oracle Database ve TimescaleDB gibi alternatifler yer almaktadır. Bu çeşitlilik sayesinde Zabbix, farklı sistem gereksinimlerine ve altyapı tercihlerine kolaylıkla uyum sağlayabilir. Zabbix veri tabanı yapısı, yüksek hacimli veri saklamaya ve hızlı sorgulama performansına göre optimize edilmiştir. Zaman serisi verileri (özellikle veri öğesi, geçmiş veri kayıtları ve eğilim tabloları, sistem kaynak kullanımını minimize etmek ve sorgu performansını korumak amacıyla özel indeksler, döngüsel veri silme ve bölümleme gibi yapılarla desteklenir. Zabbix 6.0+ sürümleriyle birlikte, zaman serisi verilerde TimescaleDB desteği ile otomatik arşivleme ve sıkıştırma da mümkün hale gelmiştir. Zabbix geniş bir veri tabanı kümesini desteklemektedir. Tablo 3'te desteklediği veri tabanları, performans özellikleri ve veri tabanlarına ait açıklamalar görülmektedir.

Tablo 3. Zabbix‘in desteklediği veritabanları

Veri tabanı	Açıklama	Performans Notu
MySQL/MariaDB	En sık tercih edilen veri tabanı altyapılarından biridir ve özellikle küçük ve orta ölçekli sistem kurulumları için yeterli performans ve kararlılık sağlar.	Düşük donanımda kararlı çalışır.
PostgreSQL	Karmaşık sorgularda daha güçlüdür, TimescaleDB entegrasyonu ile yüksek veri sıkıştırması sağlar.	Büyük kurumsal yapılar için önerilir.
Oracle	Ticari sistemlerde yüksek güvenilirlik sunar; lisans gerektirir.	Yüksek maliyetli ama güçlü.
TimescaleDB	PostgreSQL üzerinde çalışır, zaman serisi verileri için özel olarak tasarlanmıştır.	Uzun dönem veri saklama ve performans için idealdir.

Zabbix Veri Tabanı Yapısı ve Veri Tabanına Güvenli Bağlantı

Zabbix sunucusu ile veri tabanı sunucusu arasında iletişim, SSL/TLS protokolü kullanılarak şifreli olarak yapılabilir. Bu, özellikle farklı sunucularda çalışan bileşenlerde veri güvenliğini sağlar. Zabbix, BT varlıklarından toplanan tüm izleme verilerini optimize edilmiş yapıdaki veri tabanı tablolarında saklamaktadır. Bu tablolar, hem yapılandırma bilgilerini hem de zaman serisi verilerini ayrı ayrı tutacak şekilde gruplandırılmıştır. Ana bilgisayarlar, veri öğeleri, tetikleyiciler, grafikler ve şablonlar gibi tablolar sistemin yapılandırma bileşenlerini içerirken; sayısal zaman serisi verileri, tam sayı zaman serisi verileri, metin tabanlı zaman serisi verileri ve zaman serisi özet veri tabloları ise zaman serisi verilerini kaydederek geçmiş performans analizlerine olanak sağlar. Olaylar, uyarılar ve onay kayıt tabloları olay ve uyarı yönetimiyle ilişkili tüm kayıtları barındırırken, kullanıcılar, kullanıcı grupları ve bildirim türleri gibi tablolar ise kullanıcı yetkilendirmeleri ve bildirim kanallarının tanımlandığı yapılardır. Bu ayrıştırılmış tasarım sayesinde Zabbix veri tabanı, yüksek performanslı ve sürdürülebilir bir veri yönetimi altyapısı sunmaktadır. Özellikle sayısal zaman serisi veri tabloları her veri öğesi tipi için ayrı tutulur. Bu yapılandırma veri tabanı sorgularını optimize eder ve depolama maliyetini düşürür. Ayrıca döngüsel veri silme ayarlarıyla eski verilerin otomatik silinmesi sağlanır. Zabbix‘in veri tabanı altyapısı; güvenli, ölçeklenebilir ve yüksek veri işleme kapasitesine sahip bir mimariyle yapılandırılmıştır. Veri tabanı tercihi yapılırken altyapının büyüklüğü, veri yoğunluğu ve uzun vadeli saklama ihtiyaçları göz önünde bulundurulmalıdır.

Web Ara Yüzü

Zabbix sürümünde web ara yüzü, daha modüler ve kullanıcı dostu bir yapı sunarak sistem yöneticilerinin ağ izleme, veri toplama ve alarm yönetimi işlemlerini daha verimli bir şekilde gerçekleştirmesine olanak tanır. Ara yüzdeki ana menü başlıkları şu işlevsel bölümlerden oluşmaktadır:

Gösterge Panelleri

Zabbix'te gösterge panelleri, kullanıcının özel ihtiyaçlarına göre yapılandırabileceği genel izleme ekranlarıdır. Bu paneller aracılığıyla sistem durumu, olaylar ve performans metrikleri gibi kritik bilgiler; grafikler, tablolar ve diğer dinamik bileşenler yardımıyla görsel olarak sunulur. Böylece kullanıcılar, izledikleri sistemlerin anlık durumunu hızlı ve etkili biçimde değerlendirme imkânına sahip olur. Fakat 4.1 Zabbix'in Görselleştirme Sınırlılıkları ve Grafana'nın Katkısı başlığı altında anlatılacağı üzere Zabbix'in birçok görsel kısıtlılığı mevcuttur.

İzleme

Zabbix'te gerçek zamanlı sistem izleme işlemleri, "İzleme" bölümü üzerinden gerçekleştirilir. Bu bölüm; Ağ Varlıkları, Problemler, Son Veriler, Grafikler, Ekranlar ve Haritalar gibi alt menüler aracılığıyla detaylı izleme olanağı sunar. Kullanıcılar, bu alandan aktif alarmları, tetikleyici durumlarını ve ağ topolojisini yansıtan haritaları anlık olarak görüntüleyebilir, böylece sistemin mevcut durumunu hızlı şekilde analiz edebilir.

Hizmetler

Zabbix'te servis düzeyinde izleme ve SLA yönetimi "Hizmetler" bölümü üzerinden gerçekleştirilir. Bu bölümde, kurum içi hizmetlerin performansı ve kullanılabilirliği tanımlanarak izlenebilir; böylece belirlenen SLA hedeflerinin takibi yapılabilir ve hizmet kalitesi sürekliliği güvence altına alınabilir.

Envanter

Zabbix'te izlenen varlıklara ait envanter bilgileri "Envanter" bölümünde tutulur. Bu alanda cihaz, sunucu, modem gibi bileşenlerin seri numarası, üretici, model gibi bilgileri manuel olarak girilebildiği gibi, yapılandırmaya bağlı olarak otomatik olarak da oluşturulabilir. Bu sayede ağ bileşenlerinin kimlik bilgileri merkezi bir şekilde yönetilebilir.

Raporlar

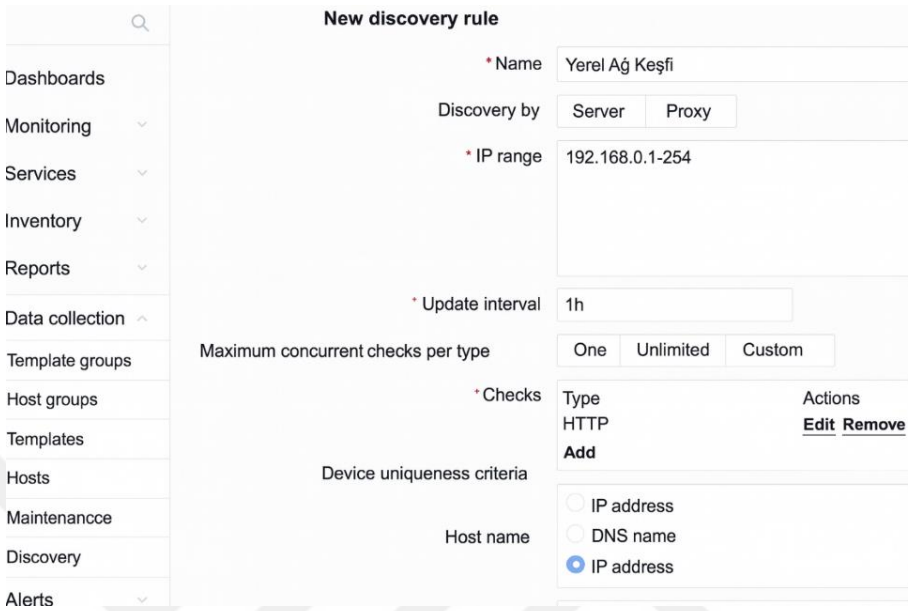
Zabbix'in "Raporlar" bölümü, sistem tarafından toplanan veriler üzerinden belirli aralıklarla oluşturulan grafiksel ve metrik tabanlı raporları içerir. Bu bölümde SLA, problem geçmişi ve diğer performans göstergelerine dayalı analizler sunularak sistem yöneticilerinin geçmiş olayları değerlendirmesi ve performans eğilimlerini izlemesi sağlanır.

Veri Toplama

Zabbix'in "Yapılandırma" bölümü, izlenecek verilerin kaynaklarının tanımlandığı temel bileşendir. Bu bölümde; Ağ Varlıkları, Şablonlar, Veri Öğeleri, Tetikleyiciler, Keşif Kuralları ve Web Senaryoları gibi alt başlıklar yer alır. Kullanıcılar bu alandan izlenecek cihazları ekleyebilir, veri öğelerini tanımlayabilir ve sistemde oluşabilecek olayları tespit etmek için tetikleyici kuralları oluşturabilirler. Bu ekran aracılığıyla, keşif sürecinde kullanılacak IP aralıkları, protokol türleri ve tetikleyici koşullar ayrıntılı olarak tanımlanabilmektedir. Belirlenen kurallar doğrultusunda ağ üzerindeki cihazların otomatik olarak algılanması ve uygun gruplara dâhil edilmesi sağlanmaktadır. Ayrıca, keşif işlemleri belirli periyotlarla yinelenerek sisteme sonradan eklenen cihazların da izleme kapsamına alınması mümkün hâle

gelmektedir. Bu yaklaşım, manuel tanımlama gereksinimini en aza indirerek özellikle geniş ölçekli ağlarda operasyonel verimliliği artırmaktadır. Böylelikle izleme sistemi, dinamik ağ ortamlarında sürdürülebilir ve ölçeklenebilir bir yapıya kavuşmaktadır.

Veri toplama bölümü ve keşif kuralları tanımlama ekranı Şekil 2 de yer almaktadır.



Şekil 2. Zabbix'te veri toplama bölümü ve keşif kuralları tanımlama ekranı

Alarmlar

"Alarmlar" bölümü, Zabbix'te olay yönetimi ve bildirim yapılandırmalarının gerçekleştirildiği kritik bir alandır. Bu bölümde; Aksiyonlar, Olay Korelasyonu, Olay Günlüğü ve Kademeli Uyarı Sistemi gibi alt sekmeler yer alır. Oluşan olaylara bağlı olarak sistemin nasıl tepki vereceği, hangi koşullarda hangi aksiyonların çalışacağı bu alanda tanımlanır. Ayrıca e-posta, Telegram, Webhook gibi çeşitli bildirim kanalları yine bu bölümden yapılandırılarak olaylara ilişkin uyarıların ilgili kişilere otomatik olarak iletilmesi sağlanır.

Kullanıcılar

"Kullanıcılar" bölümü, Zabbix sistemine erişecek kullanıcı hesaplarının ve kullanıcı gruplarının tanımlandığı alandır. Bu bölümde rol tabanlı erişim kontrolü sağlanarak farklı yetki seviyelerine (örneğin Admin, Viewer) sahip kullanıcılar oluşturulabilir. Ayrıca sistemde kullanılacak giriş yöntemleri, örneğin dâhili doğrulama, LDAP(Lightweight Directory Access Protocol) veya SAML(Security Assertion Markup Language) tabanlı kimlik doğrulama, yine bu sekme üzerinden yapılandırılmaktadır.

Yönetim

"Yönetim" sekmesi, Zabbix sisteminin genel yapılandırma ayarlarının yapıldığı bölümdür. Bu alanda vekil sunucuların tanımlanması, medya tiplerinin (örneğin e-posta, Telegram) yapılandırılması, kimlik doğrulama yöntemlerinin belirlenmesi ve döngüsel veri silme politikalarının ayarlanması gibi işlemler gerçekleştirilir. Ayrıca veri tabanı yönetimi, sistem

performansı ve genel yapılandırma parametreleri bu sekme üzerinden kontrol edilerek Zabbix altyapısının sağlıklı ve verimli çalışması sağlanır.

Destek, Entegrasyon ve Yardım

“Destek” sekmesi altında Zabbix kullanıcıları için çeşitli yardımcı kaynaklar sunulmaktadır. Bu bölümde yer alan “Destek” alt başlığı, resmi yardım dokümanlarına ve destek bağlantılarına erişim sağlar. “Entegrasyonlar” kısmı, Zabbix‘in Grafana, VMware, AWS gibi üçüncü parti sistemlerle olan hazır uyum senaryolarını içerir. “Yardım” alt menüsü ise kullanıcı kılavuzları, API(Application Programming Interface) dokümantasyonu ve sürüm notlarına yönlendirme yaparak kullanıcıların Zabbix’e etkin ve verimli şekilde kullanmasına destek olur.

Kullanıcı Ayarları

Kişisel kullanıcı ayarları, tema değişiklikleri, dil tercihi ve bildirim tercihleri burada yapılır. Bu menü yapısına uygun olarak Zabbix'te bir yönetici hem sistem genelini hem de bireysel cihazları yapılandırabilir, izlemesini özelleştirebilir ve anlık olaylara karşı hızlı aksiyonlar tanımlayabilir.

Uyarı Kanalları

Zabbix, olaylara ve tetikleyicilere bağlı olarak çeşitli uyarı mekanizmalarını devreye sokabilir. Desteklenen uyarı kanalları arasında e-posta, kısa mesaj (SMS), Telegram gibi mesajlaşma uygulamaları yer almaktadır. Bu sayede sistem yöneticileri, olası arızalara anlık olarak müdahale edebilir.

2.4 Zabbix Özellikleri ve Modül Yapısı

Zabbix gelişmiş performans, daha yüksek esneklik ve kullanıcı dostu özelliklerle öne çıkmaktadır. Özellikle güvenlik, uyum kabiliyeti, olay yönetimi ve ölçeklenebilirlik açısından önemli iyileştirmeler sunmaktadır.

Olay Korelasyon Motoru

Olay Korelasyonu, büyük ve karmaşık bilgi teknolojileri altyapılarında meydana gelen olayların (örneğin arıza, servis kesintisi, performans düşüşü) birbirleriyle olan ilişkilerini analiz ederek daha anlamlı hale getirme sürecidir. Temel amacı, aynı probleme bağlı birçok uyarıdan tekil, anlamlı bir olay çıkarmaktır. Bu sayede sistem yöneticileri, gürültüye neden olan yüzlerce bildirimin arasından gerçekten önemli olana odaklanabilir.

Olay Korelasyonunun Temel Prensipleri

Olay korelasyonu, Zabbix gibi izleme sistemlerinde olayların daha anlamlı ve yönetilebilir hâle getirilmesini sağlayan önemli bir mekanizmadır. Bu yapı, dört temel prensibe dayanır: Olay birleştirme, benzer türdeki olayları tek başlık altında toplayarak daha sade bir görünüm sağlar; örneğin, CPU kullanımı aşımı ve disk giriş/çıkış sorunları aynı altyapı bileşeniyle ilişkiliyse tek bir uyarı olarak sunulabilir. Nedensellik analizi, olaylar arasındaki sebep-sonuç ilişkisini kurarak yöneticinin olaya müdahale sürecini kolaylaştırır; örneğin bir anahtarlama cihazının çökmesi, bağlı cihazların bağlantı kaybını tetikleyebilir. Önceliklendirme sayesinde sistem, kritik olayları daha üst seviyede değerlendirerek yöneticilerin hızlı karar almasını mümkün kılar. Son olarak, gürültü azaltma prensibi, sistemin aynı soruna dair tekrar tekrar alarm

üretmesini engelleyerek bilgi kirliliğini önler ve sadece anlamlı verileri öne çıkarır. Bu prensipler sayesinde olay yönetimi hem daha etkin hem de daha sade bir şekilde gerçekleştirilir.

Zabbix'te Olay Korelasyonu

Zabbix'te olay korelasyonunun gelişmiş yönetimi, olayların daha doğru analiz edilmesini sağlayan çeşitli özelliklerle desteklenmektedir. İlişkilendirme kuralı tanımı, belirli tetikleyici etiketleri veya olay kaynaklarını esas alarak olaylar arasında mantıksal ilişki kurmak için kullanılır. Olay bastırma mekanizması, bir olay başka bir olayın doğal sonucuysa ikincil olayın görünmesini engelleyerek yalnızca birincil olayın izlenmesini sağlar. Zaman tabanlı ilişkilendirme ile belirli bir zaman aralığında (örneğin 60 saniye içinde) gerçekleşen olaylar birlikte gruplanabilir, böylece ardışık alarm zincirleri sadeleştirilebilir. Ayrıca otomatik temizleme özelliği sayesinde bir olay düzeldiğinde, ona bağlı diğer olaylar da otomatik olarak kapatılabilir. Bu yapı, hem sistem yöneticilerinin yükünü hafifletir hem de olay yönetimini daha sistematik ve anlamlı hâle getirir.

Örnek Senaryo

Bir omurga anahtarlama cihazının arızalanması durumunda geleneksel izleme sistemleri her bağlantı kaybını ayrı bir alarm olarak değerlendirir ve yöneticiye 10 farklı kullanıcı bilgisayarı için 10 ayrı alarm gönderir. Bu durum bilgi kirliliğine yol açar ve müdahale sürecini zorlaştırır. Oysa Zabbix'in korelasyon yapısı sayesinde, bu alarm zinciri tek bir ana olay altında toplanır ve sistem yöneticisi yalnızca omurga anahtarı arızasını görerek doğrudan kök nedene odaklanabilir. Böylece hem zaman hem kaynak açısından daha verimli bir olay yönetimi sağlanmış olur.

Görselleştirme ve Yönetim

Zabbix web ara yüzünde yer alan *İzleme* > *Problemler* menüsü, sistemde meydana gelen olayların grup halinde izlenmesini sağlar; kullanıcı, ilgili olaya tıkladığında bu olayın beslendiği alt tetikleyicileri grafiksel olarak görüntüleyebilir ve olaylar arasındaki ilişkilendirme kuralları ise *Yönetim* > *Olay Korelasyonu* sekmesi üzerinden tanımlanabilir.

Yüksek Ölçeklenebilirlik

Zabbix'in vekil sunucu mimarisi geliştirilmiş; her bir vekil sunucunun toplayabileceği veri miktarı artırılmış, milyonlarca metriğin daha az kaynak tüketimiyle izlenmesi sağlanmış ve bu sayede büyük ölçekli yapılarda merkezi sunucunun üzerindeki yük daha verimli şekilde dağıtılmıştır.

Geliştirilmiş UI/UX(User Interface/User Experience) ve Görsel Bileşen Yapısı

Zabbix'in yeni grafik motoru sayesinde gelişmiş veri görselleştirme yetenekleri sunulmaktadır. Kullanıcılar, şablon ekranı üzerinde sürükle-bırak yöntemiyle özel grafikler oluşturabilir ve ihtiyaçlarına uygun veri temsilleri hazırlayabilir. Ayrıca sistem, kullanıcı tanımlı görsel bileşenleri destekleyerek; haritalar, çubuk grafikleri, JSON veri gösterimleri gibi birçok farklı formatta veri sunumuna olanak tanır. Bu sayede hem operasyonel takip hem de üst yönetim raporlaması daha anlaşılır ve sezgisel hale gelir.

Yeni Bildirim ve Otomasyon Kanalları

Zabbix, Telegram, Slack ve Microsoft Teams gibi modern iletişim platformlarıyla tam bütünleşmiş çalışabilen bildirim modülleri sunmaktadır. Webhook altyapısı sayesinde dış sistemlerle çift yönlü veri alışverişi mümkün hale gelirken, kullanıcılara özel tanımlanabilen tetikleyici eylemler ile olay gerçekleştiğinde otomatik betik çalıştırma gibi gelişmiş tepkisel işlemler de gerçekleştirilebilmektedir. Bu özellikler, özellikle kurumsal otomasyon süreçlerinde Zabbix'in esnekliğini ve uyum yeteneğini artırmaktadır.

Dâhili Keşif ve Otomatik Konfigürasyon

Zabbix, dinamik ve geniş ağ yapılarında manuel tanımlamayı ortadan kaldırmak için dâhili keşif ve otomatik yapılandırma mekanizmalarını sunar. Bu özellikler sayesinde yeni eklenen ağ cihazları, sunucular veya servisler otomatik olarak keşfedilir, yapılandırılır ve izleme kapsamına alınır.

Ağ Keşfi

Zabbix'in otomatik keşif özelliği, geniş protokol desteği sayesinde SNMP, ICMP, Zabbix Ajan ve IPMI üzerinden ağ cihazlarını tarayarak veri toplayabilir. Bu taramalar, zamanlayıcı aracılığıyla belirli aralıklarla otomatik olarak gerçekleştirilerek ağın güncel yapısının sürekli izlenmesini sağlar. Ayrıca, tanımlanan koşullu işlemler sayesinde keşfedilen cihazlara otomatik olarak şablon atama, belirli gruplara ekleme veya özel etiketleme gibi işlemler yapılabilir. Bu yapı, büyük ve dinamik ağlarda manuel müdahale ihtiyacını azaltarak yönetim süreçlerini önemli ölçüde kolaylaştırır.

Zabbix ara yüzü üzerinden otomatik keşif kuralı oluşturmak için sırasıyla "Yapılandırma > Keşif > Kural Oluştur" adımları izlenir. Ardından keşif yapılacak IP aralığı (örneğin 10.0.0.1-254) belirlenir ve SNMP topluluk adı olarak genellikle "public" kullanılır. Kontrol edilecek servisler arasında Zabbix ajanı, SNMP ve ICMP seçenekleri yer alır. Keşif sonucunda yapılacak eylemler kısmında ise, örneğin keşfedilen cihaza otomatik olarak "Template OS Linux" şablonu atanabilir ve cihaz "Linux Sunucuları" adlı gruba dâhil edilebilir. Bu süreç, özellikle Linux tabanlı sistemlerin hızlı şekilde izleme kapsamına alınmasını sağlar.

Otomatik Kayıt

Zabbix ajan kurulu sunucular, ilk bağlantıda kendi bilgilerini (makine adı, üst veri, IP vb.) Zabbix Server'e iletir. Server, üst veriye göre belirlenen kuralları çalıştırır. Zabbix'te otomatik sunucu sınıflandırması için çeşitli mekanizmalar kullanılmaktadır. Bu kapsamda ilk adımda, ajan tarafında yer alan /etc/zabbix/zabbix_agentd.conf dosyasındaki "HostMetadata" değeri aracılığıyla sınıflandırma yapılabilir. Bu üst veri bilgisi, sunucunun işletim sistemi ya da belirli bir kategoriye ait olup olmadığını belirtmekte kullanılır. Sunucuya ait üst veri bilgisine göre tanımlanan eylemler aracılığıyla, gelen sunucuya otomatik olarak şablon atanabilir, bir gruba eklenebilir ya da özel makrolar tanımlanabilir. Böylece manuel işlem yapılmasına gerek kalmadan merkezi yönetim kolaylaştırılır. Örneğin, "HostMetadata=Linux" olarak tanımlanan bir sunucuya otomatik olarak "Template OS Linux" şablonu atanabilir ve "*Linux Servers"* grubuna dâhil edilebilir. Bu sayede Zabbix ortamına dâhil edilen yeni sistemler, belirlenen kurallar doğrultusunda otomatik olarak yapılandırılır.

Örnek Ajan Ayarı:

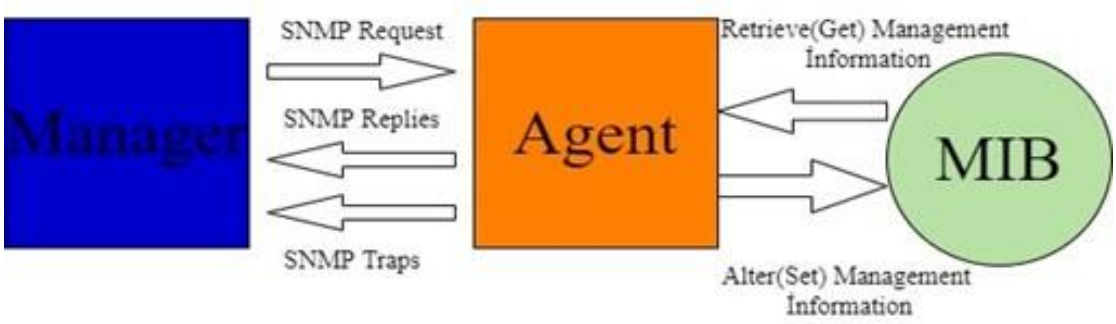
Server=10.0.0.1 Hostname=server01 HostMetadata=Linux

Güvenlik Özellikleri

Zabbix, güvenlik açısından gelişmiş özellikler sunarak kurumsal ağ izleme süreçlerini güvence altına alır. SSL/TLS protokolleri üzerinden şifreli veri iletimi zorunlu hale getirilebilir, bu da hem sunucu-ajan hem de istemci ara yüzü arasındaki iletişimin güvenliğini artırır. Ayrıca kullanıcı oturum yönetimi gelişmiş yetkilendirme seçenekleriyle desteklenmekte, iki faktörlü kimlik doğrulama ile hesap güvenliği üst seviyeye çıkarılmaktadır. Zabbix API üzerinden yapılan erişimlerde ise kimlik doğrulama anahtarları kullanılarak sadece yetkilendirilmiş kullanıcıların sisteme müdahale etmesi sağlanır. Bu özellikler, hem veri güvenliğini hem de erişim bütünlüğünü korumada kritik rol oynamaktadır.

Şekil 3 örneğinde görüleceği üzere SNMP protokolünde yönetici, ajan ve yönetim bilgi tabanı arasındaki temel iletişim akışı bulunmaktadır. Yöneticiden gelen istekler ajan tarafından işlenmekte, sonuçlar SNMP yanıtları veya tuzakları olarak geri iletilmektedir.

Haberleşme yapısının temel gösterimi Şekil 3 te yer almaktadır.



Şekil 3. Ağ haberleşme yapısında bulunan varlıklar

3.Zabbix'e Etkin Varlık Eklenmesi ve Yönetimi

Zabbix'in güçlü ve ölçeklenebilir yapısının temelini, izlenen varlıkların doğru biçimde tanımlanması, yapılandırılması ve sürekli güncel tutulması oluşturmaktadır. Etkin bir izleme altyapısı kurabilmek için sadece cihazların verilerini toplamak yeterli değildir; aynı zamanda bu verilerin hangi cihazlara ait olduğunu, bu cihazların hangi grup ve bölümde yer aldığını ve ne tür metrikler ile izleneceğini açıkça tanımlamak gerekir. Bu kapsamda Zabbix; manuel, yarı otomatik ve tamamen otomatik olmak üzere üç temel varlık tanımlama ve izlemeye alma yöntemi sunar.

3.1 Manuel Ağ Varlığı Tanıma ve İzlemeye Alma Süreci

Zabbix web ara yüzü üzerinden klasik yöntemle gerçekleştirilen manuel varlık tanımlama süreci, özellikle küçük ölçekli ağlar veya özel yapılandırma gerektiren durumlar için uygun bir yöntemdir. Bu süreçte, kullanıcı *Yapılandırma >Ana Bilgisayarlar >Oluştur* adımlarını izleyerek yeni bir cihaz ekleyebilir. Ana bilgisayar adı, görünen ad, grup bilgisi ile birlikte izleme yöntemi olarak kullanılacak olan ara yüz türü (örneğin SNMP veya ajan tabanlı bağlantı)

tanımlanır. Ardından, ilgili cihazla uyumlu şablonlar (örneğin *Generic by SNMP*) seçilerek atanır. Dileyen kullanıcılar için "*Envanter Modu"* aktif hale getirilerek, cihazın tipi, üreticisi, seri numarası gibi envanter bilgileri manuel olarak girilebilir. Ancak bu yöntem, cihaz sayısının artması durumunda zaman açısından verimsiz hâle gelmekte ve sürdürülebilirliği azalmaktadır. Bu nedenle, orta ve büyük ölçekli ağlarda manuel tanımlama yöntemi önerilmemektedir.

3.2 Otomatik Ağ Keşfi

Zabbix, belirli aralıklarla tanımlanan IP aralıklarını tarayarak; SNMP, ICMP veya Zabbix Agent protokolü ile ulaşılabilen cihazları otomatik olarak keşfedebilir.

Zabbix sisteminde, ağ üzerindeki cihazların otomatik olarak tanımlanabilmesi için keşif kuralları oluşturulmaktadır. Bu işlem, ara yüz üzerinden *Yapılandırma > Keşif > Kural Oluştur* adımları izlenerek gerçekleştirilir. Örneğin, 10.0.0.1–254 IP aralığını kapsayan bir yerel ağ segmenti için keşif işlemi yapılandırılabilir. Keşif sırasında Zabbix ajan, SNMPv2c ve ICMP ping kontrol türleri kullanılmakta ve bu kontrollerin her 3600 saniyede bir tekrarlanması sağlanmaktadır. Keşif kuralına bağlı olarak tetiklenen eylemler ise *Yapılandırma > Eylemler > Keşif* menüsü üzerinden tanımlanır. Örneğin, "Keşif kuralı 'LAN subnet' olan ve SNMP servisi aktif durumda bulunan" koşulu sağlandığında; keşfedilen cihaz, otomatik olarak "Network Devices" grubuna eklenmekte, "Şablon SNMP Generic" adlı hazır şablon atanmakta ve ağ varlığı adı olarak cihazın IP adresi kullanılmaktadır. Bu yapı sayesinde, manuel müdahale gerektirmeksizin SNMP destekli ağ bileşenlerinin dinamik olarak sisteme dâhil edilmesi mümkün olmaktadır.

3.3 Otomatik Kayıt Mekanizması

Zabbix ajan yüklü bir cihaz, sunucuya ilk bağlantıyı gerçekleştirdiğinde, önceden tanımlanan üst veri bilgisi ile birlikte kendini tanıtır. Sunucu, gelen bu üst veri bilgisine göre ilgili aksiyonları tetikleyerek ağ varlığını otomatik olarak izleme kapsamına alır.

3.3.1 Ajan Üzerinde Yapılandırma

Zabbix ajan, izleme yapılacak istemci sistemlerde çalıştırılan ve bu sistemle ilgili verileri toplayarak Zabbix sunucusuna gönderen yazılımdır. Ajan'ın doğru şekilde yapılandırılması, sistemin izleme altyapısına bütünleşmesi için kritik öneme sahiptir.

Linux veya Windows işletim sistemine sahip izleme hedeflerinde, yapılandırma genellikle /etc/zabbix/zabbix_agentd.conf dosyası üzerinde gerçekleştirilir. Aşağıda örnek olarak verilen satırlar, bu yapılandırma dosyasında tanımlanmış üç temel parametreyi ifade etmektedir:

Server=10.0.0.1 Hostname=SRV-WIN01 HostMetadata=Windows

Server=10.0.0.1
Bu satır, ajanın hangi Zabbix sunucusuna veri göndereceğini belirtir. Burada girilen IP adresi, Zabbix sunucusunun IP'sidir. Bu parametre, Zabbix sunucusunun yalnızca yetkilendirilmiş ajanlardan veri kabul etmesini sağlar. Güvenlik açısından önemli bir kontrol noktasıdır.

Hostname=SRV-WIN01
Bu parametre, izlenen sistemin Zabbix'te tanımlanacak olan ana makine adıdır. Bu ad, sunucu ara yüzü üzerinden tanımlanacak ağ varlığı ile birebir aynı olmalıdır. Aksi takdirde veri eşleşmesi ve doğru raporlama sağlanamaz.

HostMetadata=Windows
Bu alan, otomatik kayıt ve keşif süreçlerinde kullanılmak üzere sistemin hangi kategoriye ait olduğunu belirtir. Örneğin, burada tanımlanan "Windows" değeri sayesinde, Zabbix sunucusu üzerinde yapılandırılmış otomatik kayıt eylemleri bu ajana uygun şablonları ve gruplamaları otomatik olarak atayabilir.

Bu yapılandırma sayesinde, ajan yüklü sistem Zabbix'e aktif bir izleme varlığı olarak tanıtılmış olur. Aynı zamanda "HostMetadata" alanı sayesinde sistemin türüne göre otomatik işlemler (örneğin; belirli şablonların atanması, belirli ağ varlığı gruplarına eklenmesi vb.) gerçekleştirilir. Bu, özellikle büyük ölçekli ağlarda manuel yapılandırma yükünü önemli ölçüde azaltır ve sistemin yönetilebilirliğini artırır.

3.3.2 Otomatik Kayıt Aksiyonu

Zabbix'in otomatik kayıt özelliği, özellikle bulut tabanlı sistemler ve dinamik sanallaştırma altyapılarında yüksek verimlilik sağlar. Bu yöntem sayesinde, izleme sistemiyle önceden tanımlı iletişim bilgilerine sahip olan yeni bir sanal makine başlatıldığında, manuel müdahaleye gerek kalmadan otomatik olarak tanımlanıp izlenmeye alınabilir. Otomatik kayıt işlemleri *Yapılandırma* > *Eylemler* > *Otomatik Kayıt* sekmesi üzerinden yapılandırılır. Örneğin, "Ana bilgisayar üst veri bilgisi 'Windows' ifadesini içerdiğinde" koşulu tanımlanarak yalnızca Windows işletim sistemine sahip makinelerin hedeflenmesi sağlanabilir. Bu koşul sağlandığında; cihaz otomatik olarak "Windows Sunucuları" adlı gruba eklenmekte, "Template OS Windows" adlı şablon atanmakta ve "{$ENV}=Production" biçiminde özel bir makro tanımlanarak cihazın çalışma ortamı belirtilmektedir. Bu yapı, Zabbix'in dinamik ortamlarda esnek ve sürdürülebilir bir izleme altyapısı sunmasını mümkün kılmaktadır.

3.4 Varlık Yönetimi, Etiketleme, Gruplama ve Sürüm Takibi

Zabbix, ağ varlıklarını sadece grup olarak değil; aynı zamanda etiket ve özel envanter ile de sınıflandırır. Bu etiketler sayesinde olay korelasyonu sağlanabilir (örneğin, tüm üretim ortamı sunucularında yüksek işlemci kullanımı durumunda tek bir alarm üretilir), SLA bazlı raporlamalar gerçekleştirilebilir ve sürüm ya da lokasyon bazlı filtreleme ile grafiksel karşılaştırmalar yapılabilir.

Örnek Etiketleme:

Tag: env Value: Production

Tag: type Value: Firewall

Zabbix, yapılandırma ve varlık tanımı süreçlerinde XML, YAML ve JSON veri tanımlama dillerini desteklemektedir.

XML

Zabbix'te izleme yapılandırmalarının yeniden kullanılabilirliği ve paylaşıla bilirliği önemli bir avantaj sağlar. Bu kapsamda, şablonlar, öğeler, tetikleyiciler, grafikler ve diğer yapılandırmalar XML formatında dışa ve içe aktarılabilir; özellikle SNMP tabanlı hazır şablonlar genellikle XML uzantılı dosyalar olarak paylaşılır. Bir BT varlığına ait bir özelliğin XML tanımı aşağıdaki örnekte yer almaktadır.

xml

<item>

<name>CPU Load</name>

<key>system.cpu.load[percpu,avg1]</key>

<type>0</type>

</item>

YAML Yapılandırması

Zabbix Ajan 2 ile gelen en önemli yeniliklerden biri eklenti destekli modüler yapıdır. YAML dosyaları kullanılarak, HTTP/HTTPS, PostgreSQL gibi servisler için izleme yapılandırmaları yapılabilir.

Zabbix'te PostgreSQL veri tabanı eklentisini etkinleştirmek için kullanılan bir yapılandırma dosyasına ait YAML örneği aşağıdadır.

yaml

plugins:

postgres:

enabled: true

user: zabbix

password: secret

JSON (API Tabanlı Entegrasyonlar ve Webhook Bildirimleri)

Zabbix, sistemler arası otomasyon ve uyum ihtiyaçlarını karşılamak amacıyla RESTful(modern web servislerinin geliştirilmesinde yaygın olarak kullanılan bir yazılım mimarisi) mimariye sahip bir API (Uygulama Programlama Ara yüzü) sunmaktadır. Bu API aracılığıyla, kullanıcı tanımı, cihaz ekleme, şablon atama, tetikleyici güncelleme gibi işlemler doğrudan JSON formatında gerçekleştirilebilmektedir. Böylece izleme altyapısı sadece grafik ara yüz üzerinden değil, aynı zamanda otomasyon senaryoları ve üçüncü parti yazılımlar aracılığıyla da yönetilebilir hale gelmektedir. Öte yandan, Zabbix'in Webhook (geri çağırım bağlantısı) desteği sayesinde oluşan olaylar belirli koşullar altında dış servislerle paylaşılabilir. Slack, Telegram, Microsoft Teams, Jira gibi platformlara otomatik uyarılar gönderilebilir. Bu yapı, olay yönetimini merkezi hale getirerek hızlı tepki verilmesini sağlar ve iş sürekliliğini destekler. Bu uyum yetenekleri sayesinde Zabbix yalnızca izleme aracı olmaktan çıkmakta, aynı zamanda otomasyon altyapısının merkezinde yer alan bir olay yöneticisi rolünü üstlenmektedir.

Zabbix API kullanılarak yeni bir ağ varlığı eklemek için yapılan bir JSON formatı örneği aşağıdadır.

JSON

{ "jsonrpc": "2.0",

"method": "host.create",
"params": {
"host": "MyServer01",
"interfaces": [
{ "type": 1,
"main": 1,
"useip": 1,
"ip": "10.0.0.101",
"dns": "",
"port": "10050" }],
"groups": [{"groupid": "2"}],
"templates": [{"templateid": "10001"}] },
"auth": "api_token",
"id": 1}

Zabbix‘in XML, YAML ve JSON gibi çoklu veri tanım dillerini desteklemesi; platformun esneklik, taşınabilirlik ve uyum yeteneklerini artırmaktadır. XML, şablon paylaşımı ve yapılandırma dışa/içe aktarımları için ideal bir formatken; YAML, Agent 2 'nin eklenti tabanlı yeni nesil yapılandırma ihtiyaçlarını karşılamaktadır. JSON ise modern yazılım mimarilerinde sıkça kullanılan RESTful API'ler ve Webhook bildirimleri için en etkili formattır. Bu çeşitlilik, Zabbix‘in hem teknik kullanıcılar hem de uyum mühendisleri için güçlü bir izleme altyapısı sunduğunu göstermektedir.

4.Verilerin Görselleştirilmesi ve Grafana Entegrasyonu

Grafana, zaman serisi verilerini görselleştirmek, analiz etmek ve izlemek için kullanılan açık kaynak kodlu, etkileşimli bir veri paneli platformudur. Modern BT altyapılarında sistem performansını izlemek, verileri analiz etmek ve uyarı mekanizmaları kurmak için yaygın olarak kullanılmaktadır.

Grafana, Prometheus, InfluxDB, Elasticsearch, MySQL ve özellikle Zabbix gibi çok sayıda veri kaynağını destekler. Özelleştirilebilir panelleri, kullanıcı dostu ara yüzü ve kapsamlı eklenti desteği sayesinde sistem yöneticileri kadar üst düzey karar vericiler için de etkili bir analiz aracıdır.

4.1 Zabbix‘in Görselleştirme Sınırlılıkları ve Grafana'nın Katkısı

Zabbix‘in yerleşik grafik motoru, izleme verilerini temel düzeyde görselleştirebilse de, gelişmiş analiz gereksinimlerini karşılamakta yetersiz kalmaktadır. Özellikle çok katmanlı veri korelasyonu, kullanıcıya özgü panellerin tasarlanması ve etkileşimli grafik çıktılarının oluşturulması gibi ileri düzey ihtiyaçlar için Grafana, Zabbix’e kıyasla daha güçlü ve esnek bir araç olarak öne çıkmaktadır [17]. Bu eksiklikleri gidermek üzere Zabbix ile bütünleşmiş şekilde çalışan Grafana, gelişmiş zaman serisi analizleri, sezgisel paneller, kullanıcıya özel grafikler ve çoklu veri kaynağı desteği gibi özellikleri ile öne çıkar. Özellikle büyük ağ yapılarında ve sürekli değişen ortamlarda, verilerin korelasyonu ve hızlı yorumlanması açısından Grafana, Zabbix‘in zayıf kaldığı alanları tamamlayıcı bir yapı sunmaktadır.

Zabbix‘in izlediği veriler yalnızca fiziksel cihazlarla sınırlı değildir; sistem kaynakları, donanım durumları, servis erişilebilirliği, yazılım servisleri ve IoT sistemleri gibi çok geniş bir yelpazeye yayılır. Sistem kaynakları düzeyinde Zabbix; işlemci kullanımı, bellek tüketimi, disk girdi/çıktı performansı ve ağ trafiği gibi temel performans metriklerini toplayabilir. Bu tür veriler, sistemin genel sağlık durumu ve kaynak kullanımı hakkında anlık bilgiler sunar.

Donanım izleme açısından Zabbix, SNMP ve IPMI gibi protokoller sayesinde ağ anahtarı, yönlendirici ve güvenlik duvarı gibi cihazlardan port durumu, trafik hacmi ve aktif çalışma süresi gibi verileri toplayabilir. IPMI aracılığıyla sıcaklık, fan hızı, voltaj ve güç tüketimi gibi donanım düzeyindeki ölçümler alınabilir, bu da özellikle veri merkezlerinde donanımsal risklerin önceden tespit edilmesine olanak tanır. Zabbix aynı zamanda temel ağ servislerinin izlenmesini de sağlar. HTTP/HTTPS, ICMP, SMTP, DNS ve LDAP gibi servislerin erişilebilirliği, yanıt süreleri ve kesinti durumları düzenli olarak kontrol edilebilir. Yazılım katmanında ise Linux ve Windows hizmetlerinin çalışma durumları, log dosyası içerik analizi ve Java/JMX gibi platformlara özel uygulama performans metrikleri gözlemlenebilir. Bu katmanda gerçekleşen anormallikler doğrudan kullanıcı deneyimini etkileyebileceğinden, erken uyarı sistemleri açısından kritik öneme sahiptir.

Endüstriyel sistemler ve IOT cihazları da Zabbix tarafından kapsamlı biçimde izlenebilir. Modbus protokolü üzerinden PLC cihazlarından gelen sıcaklık, basınç ve durum gibi veriler analiz edilebilirken; MQTT protokolü ile düşük bant genişliğine sahip IoT cihazlarının durumu izlenebilir. Bu altyapı sayesinde üretim hattındaki sensör verileri, enerji tüketimi ve dijital sinyaller gerçek zamanlı olarak takip edilebilir. Toplanan veriler yalnızca izleme amacıyla değil, olay analizi ve karar destek süreçlerinde de etkin biçimde kullanılır. Zabbix, tetikleyici durumları, olay geçmişini, kesinti sürelerini ve uyarıları detaylı biçimde kaydeder. Özellikle Grafana ile gerçekleştirilen uyum sayesinde bu veriler daha okunabilir hâle gelir. Zaman serisi analizleri, eşik değer bazlı alarm yönetimi ve özelleştirilebilir paneller aracılığıyla pratik bir karar destek altyapısı oluşturulur. Bu yapı, üretim hattındaki bir PLC’nin enerji tüketimi ile aynı alandaki ağ trafiği arasında zaman bazlı ilişki kurmaya imkân verir.

Zabbix‘in verilerini Grafana ile birlikte InfluxDB, Prometheus, Elasticsearch gibi farklı veri kaynaklarında işleyerek tek bir gösterge paneli üzerinde sunabilmesi; özellikle IoT sistemleri, hibrit bulut altyapıları ve DevOps süreçlerinde ciddi bir avantaj sağlar. Bu bütüncül yapı, sadece BT sistemlerinin değil, aynı zamanda üretim, enerji ve operasyonel altyapıların izlenmesini de mümkün kılar.

4.2 Entegrasyon Süreci

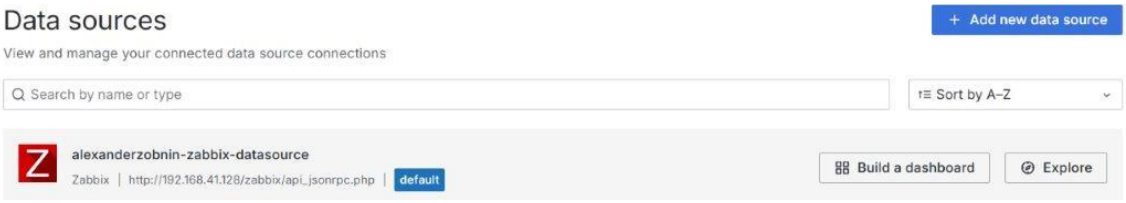
Grafana'nın Zabbix ile entegrasyonu, yalnızca teknik bir kurulum süreci değil, aynı zamanda sistem yöneticilerine gelişmiş görselleştirme yetenekleri sunan stratejik bir yapı oluşturur. Bu süreç; veri kaynaklarının yapılandırılması, yetkilendirme ve bağlantı testleri, zaman serisi ayarları ve gösterge paneli oluşturma gibi adımlardan oluşur. Ancak bu başlık altında, kurulumun adım adım anlatımından ziyade entegrasyonun sağladığı fonksiyonel yetenekler, görselleştirme imkânları ve ara yüz üzerinden yapılan yapılandırmaların işlevsel etkileri açıklanacaktır.

4.2.1 Veri Kaynağı Tanımı ve API Bağlantısı

Grafana, Zabbix'i bir veri kaynağı olarak tanıyabilmekte ve API üzerinden erişim sağlamaktadır. Şekil 4 da görüldüğü üzere, sunucu adresi ve API uç noktası girilerek tanımlama

gerçekleştirilir. Bu yapı, Zabbix'in topladığı tüm verilerin zaman serisi tabanlı olarak Grafana'ya aktarılmasına olanak sağlar.

Zabbix'te veri kaynağının eklendiği ekran Şekil 4'te görülmektedir.

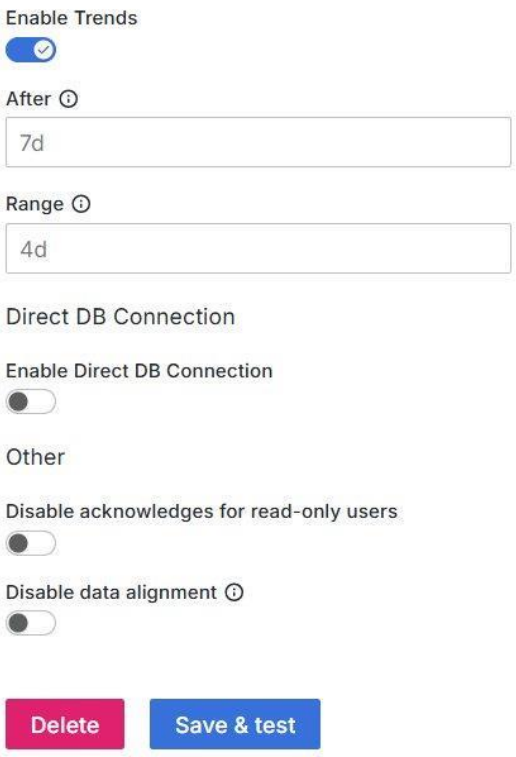


Şekil 4. Zabbix veri kaynağının eklendiği ekran

4.2.2 Eğilim Tabloları Ayarları ve Veri Aralığı

Zabbix'in zaman serisi verilerini daha anlamlı şekilde görselleştirebilmek için, geçmiş verilerin alınacağı zaman aralıkları Grafana üzerinden belirlenebilir. Sistem yöneticisi, Zabbix'te tutulan eğilim tabloları ve geçmiş veri kayıtları arasından grafiklerde gösterilecek olan zaman aralığını seçebilir.

Şekil 5'te eğilim tablosu ve bağlantı ayarlarının yapılandırıldığı panelin görüntüsü görülmektedir.



Şekil 5. Eğilim tablosu ve bağlantı ayarlarının yapılandırıldığı ekran

4.2.3 Gösterge Paneli Oluşturma

Grafana'nın en güçlü yönlerinden biri, dinamik ve özelleştirilebilir gösterge panelleridir. İşlemci kullanımı, bellek durumu, disk doluluğu, ağ trafiği ve tetikleyici uyarıları gibi birçok veri noktası bir arada sunulabilir. Sistem yöneticileri, bu panelleri hem hazır şablonlarla hem de kendi belirledikleri veri kaynaklarına göre manuel olarak oluşturabilir.

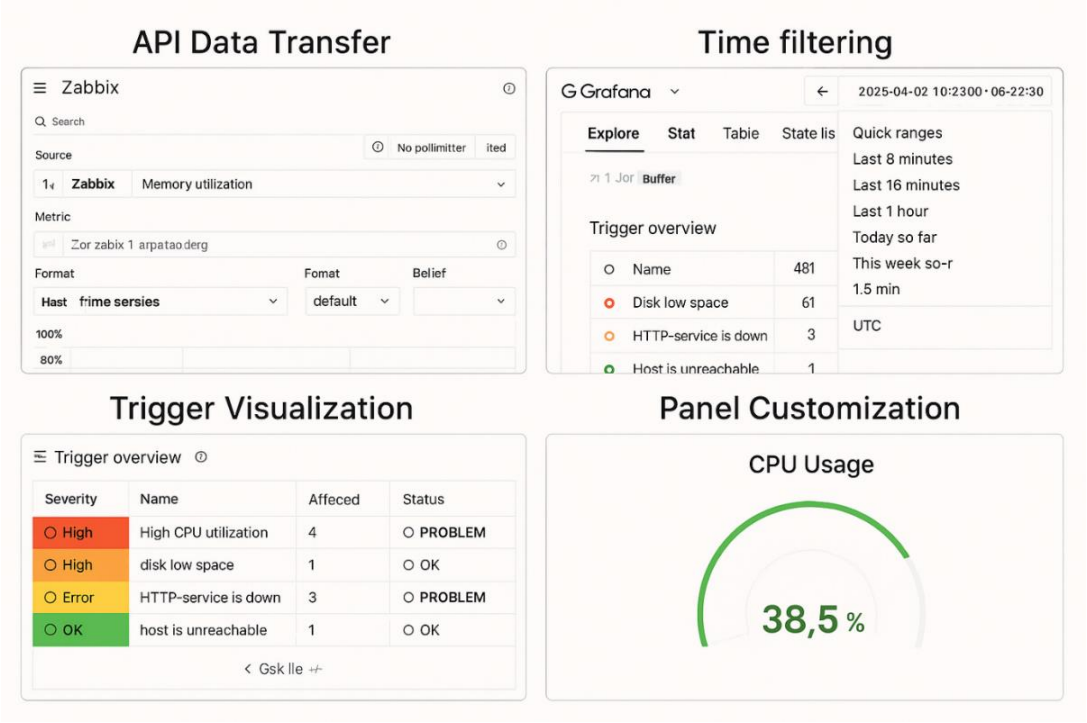
API üzerinden doğrudan veri aktarımı, Zabbix‘in veri tabanına manuel sorgular yazmadan gerçek zamanlı verilerin Grafana panellerine taşınmasını sağlar; bu özellik, Zabbix‘in standart ara yüzünde sınırlı veri dışa aktarma seçeneklerine kıyasla daha esnek ve hızlı bir uyum sunar.

Zaman filtreleme, Grafana kullanıcılarının belirli tarih aralıklarına göre verileri dinamik olarak süzmesine olanak tanır; bu işlev Zabbix ara yüzünde yalnızca ön tanımlı zaman dilimleriyle sınırlıyken, Grafana’da kullanıcıya özel esnek zaman aralıkları oluşturulabilir.

Tetikleyici görselleştirme, Zabbix’te oluşan olayların ve alarmların grafiksel olarak gösterilmesini sağlar; bu sayede sistem yöneticisi, hangi zaman aralığında hangi olayların tetiklendiğini doğrudan grafik üzerinde görerek daha hızlı analiz yapabilir, oysa Zabbix'te bu bilgiler ayrı sekmelerde ve metin tabanlı sunulmaktadır.

Panel kişiselleştirme özelliği sayesinde, kullanıcılar sadece ihtiyaç duydukları verileri içeren görsel bileşenler oluşturabilir, panelleri sürükle-bırak yöntemiyle düzenleyebilir ve farklı roller için özelleştirilmiş şablonlar tasarlayabilir; Zabbix ara yüzü bu düzeyde görsel esneklik ve özelleştirme imkânı sunmamaktadır.

API veri aktarımı, zaman filtreleme, tetikleyici görselleştirme ve panel kişiselleştirmeye dair ekran örnekleri Şekil 6 da görülmektedir.



Şekil 6. Veri aktarımı, zaman filtreleme, tetikleyici görselleştirme ve gösterge paneli özelleştirme işlevlerine ait ekran

4.3 Uygulama Alanları ve Stratejik Değer

Zabbix-Grafana uyumu, yalnızca görsel estetik sunmakla kalmayıp aynı zamanda kurumsal karar destek mekanizmalarının etkinliğini artıran stratejik bir yapı olarak öne çıkmaktadır. Literatürde yapılan araştırmalar, bu uyumun ağ yönetimi, veri görselleştirme ve sistem performans analizlerinde sağladığı bütünlük sayesinde kurumlara operasyonel verimlilik, hızlı müdahale ve ileri düzeyde izleme kabiliyetleri sunduğunu göstermektedir [18].

Öncelikle, operasyonel verimlilikte kayda değer artış sağlandığı gözlemlenmiştir. Grafana panelleri sayesinde sistem yöneticileri; işlemci kullanımı, bellek durumu, disk kapasitesi gibi çok sayıda metriği eşzamanlı olarak izleyebilmekte, bu da operasyonel süreçlerdeki etkileşimleri sadeleştirmektedir [25].

Bununla birlikte, BT ekiplerinin müdahale süresinde azalma elde edilmiştir. Özellikle önceden tanımlı tetikleyiciler ve gerçek zamanlı alarm sistemleri sayesinde sorunlara erken müdahale edilerek kesintilerin önüne geçilebilmiştir [7].

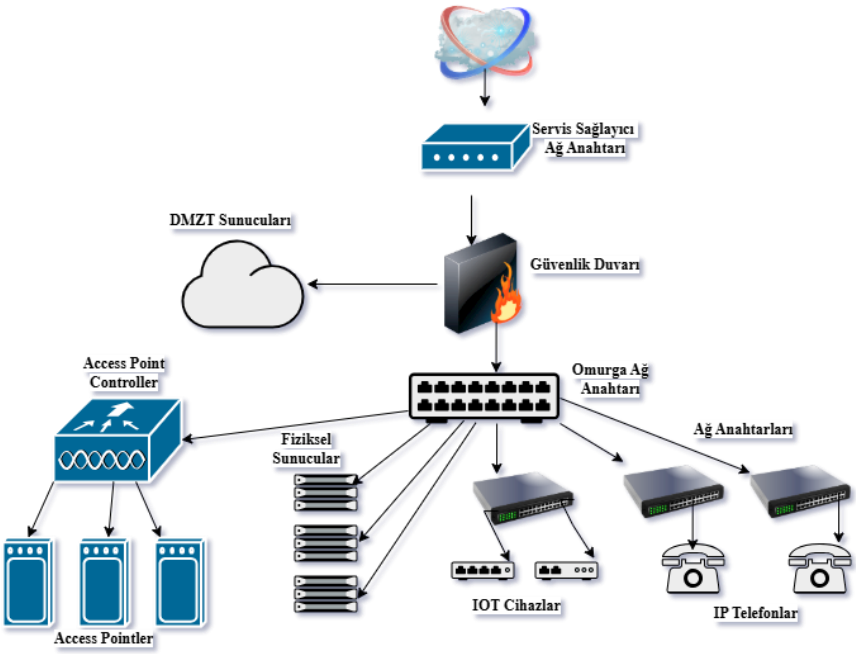
Ayrıca, üst düzey yöneticilere sunulan çıktıların anlaşıla bilirliği büyük oranda artmıştır. Grafana'nın sezgisel görselleştirme yapısı sayesinde teknik veriler sadeleştirilerek yönetim seviyesine uygun gösterge panelleri oluşturulmuş, böylece karar alma süreçlerine katkı sağlanmıştır.

Grafana'nın uyarı sistemleri de entegrasyonun güçlü yönlerinden biridir. Zabbix'ten alınan tetikleyici bilgileri temel alınarak Grafana panelleri üzerinden e-posta, Slack ve Telegram gibi platformlara bildirim gönderilmekte ve olaylara hızlı reaksiyon verilebilmektedir [19].

5.Kurumsal Ağ ve Endüstriyel Ağ Uygulaması

Bu çalışma kapsamında uygulama yapılan kurumun bünyesinde yaklaşık 500 son kullanıcıya hizmet veren bir bilgi teknolojileri altyapısı mevcuttur. Bu altyapı, iki fiziksel lokasyonun fiber bağlantı ile birbirine entegre edilmesiyle oluşturulmuş, yüksek bant genişliği ve düşük gecikme süresi ile çalışan bir omurga üzerine inşa edilmiştir. Mevcut topoloji içerisinde 1 adet omurga ağ anahtarı, 1 adet güvenlik duvarı, 50 adet ağ anahtarı, 1 adet kablosuz ağ denetleyici ve 30 adet kablosuz erişim noktası yer almaktadır. Ayrıca, 5 adet fiziksel ve 25 adet sanal olmak üzere toplam 30 adet sunucu sistemde aktif olarak kullanılmaktadır. Üretim alanlarında kullanılan 100 âdete yakın IoT cihaz ve yaklaşık 45 adet IP telefon bulunmaktadır.

Şekil 7 de kurumun genel topolojisi görülmektedir.



Şekil 7. Kurum genel topoloji ekranı

Bu çok katmanlı ve karmaşık yapının 7/24 izlenebilirliğini ve operasyonel sürekliliğini sağlamak amacıyla açık kaynak kodlu bir ağ izleme yazılımı olan Zabbix tercih edilmiştir. Zabbix, merkezi bir sunucu üzerinden çeşitli protokoller yardımıyla (SNMP, ajan, ICMP, anlık bildirim) ağ bileşenlerinden veri toplayabilmekte, kritik olayları tetikleyiciler aracılığıyla tanımlayabilmekte ve bu olayları yöneticilere alarm mekanizmalarıyla bildirebilmektedir.

Kurulan sistemde, omurga ağ anahtarı, güvenlik duvarı, ağ anahtarı, kablosuz ağ denetleyici ve kablosuz erişim noktası gibi ağ donanımları SNMP protokolü üzerinden izlenmekte; sunucu sistemlerde ise Zabbix ajan kullanılarak işlemci, bellek, disk kullanımı, işlem durumu ve servislerin sağlık durumu gibi metrikler elde edilmektedir. Toplamda her bir ana cihaz için yüzlerce metrik tanımlanmış, bu metriklerin eşik değerleri üzerinden tetikleyiciler oluşturulmuştur. Zabbix sunucusu, bu metriklere dayanarak cihazların performans durumu, erişilebilirlik ve olay geçmişi gibi bilgileri toplayarak merkezi bir veri tabanında saklamaktadır.

Ağ yapısının sadeleştirilmiş hali aşağıdaki gibidir:

- Servis Sağlayıcı Ağ Anahtarı → Güvenlik Duvarı → Omurga Ağ Anahtarı
- Omurga Ağ Anahtarı üzerinden:

  Bir kolda: Kablosuz Ağ Denetleyici → 30 Access Point

  Diğer kolda: 50 Ağ Anahtarı→ Son kullanıcı sistemleri

  Veri merkezi tarafında: 5 Fiziksel + 25 Sanal Sunucu

  Üretim alanlarında 100 IoT cihaz ve 45 IP telefon
- İki lokasyon, fiber ile doğrudan bağlanmış ve tüm Zabbix izleme sistemi merkez lokasyonda konumlandırılmıştır.

Ancak uygulamada gözlemlenen durum, Zabbix'in ham verileri etkili biçimde toplamasına rağmen, yönetimsel raporlama, karar destek ve görsel analiz gibi ihtiyaçlara yanıt vermekte sınırlı kaldığı yönündedir. Özellikle yüksek seviyeli yöneticilere yönelik özet raporların ve etkileşimli görselleştirme olanaklarının yetersizliği, bu tür platformların başka araçlarla uyumunu gerekli kılmaktadır [2]. Web ara yüzü temel grafik desteği sunsa da, sistem yöneticileri dışında kalan teknik olmayan kullanıcılar için verinin okunabilirliği ve sistem genel durumu hakkında özet sunumu noktasında eksiklikler tespit edilmiştir.

Bu nedenle Zabbix üzerindeki görselleştirme sınırlılığından dolayı görselleştirme konusunda çok sayıda kabiliyeti olan Grafana kullanılmıştır. 7. bölümde Grafana ayrıntılı bir şekilde ele alınmıştır. Zabbix, bu noktada güçlü bir veri toplayıcı ve alarm üretici sistem rolü üstlenirken; görselleştirme, analiz ve karar destek gibi yetenekler için üçüncü parti yazılımlarla tamamlayıcı bir yapı hâline gelmiştir.

Bu tez çalışması kapsamında geliştirilen Zabbix tabanlı izleme altyapısı, hem kurumsal bir üretim ağına hem de endüstriyel kontrol bileşenlerini barındıran karmaşık bir operasyonel teknoloji ortamına uygulanmıştır. Denetim altına alınan altyapı, üretim tesislerinde sıkça karşılaşılan hibrit yapılara uygun olarak tasarlanmış; BT ile OT katmanlarının birlikte izlenmesine olanak tanımıştır.

Uygulama alanı olarak seçilen yerel ağ ortamında; farklı üretim hatları ve sunucu sistemlerini birbirine bağlayan çok sayıda aktif cihaz bulunmaktadır. İzleme sistemine entegre edilen örnek donanımlar aşağıdaki şekilde sınıflandırılmıştır:

1 adet Omurga Ağ Anahtarı: Omurga bağlantısını sağlayan yüksek kapasiteli ağ anahtarı port bazlı trafik ve işlemci yükü kritik önemdedir.

2 adet Kenar Ağ Anahtarı: Alt ağlardaki cihazlara hizmet veren dağıtım ağ anahtarları; port trafiği, arıza durumu ve SNMP erişilebilirliği takip edilmiştir.

1 adet Kablosuz Ağ Denetleyici: Kablosuz ağ kontrol birimi; SNMP ile erişilebilirlik, trafik yoğunluğu ve cihaz durumları takip edilmiştir.

2 adet IoT Cihaz: Sensör verileri sağlayan ve SNMP desteği sunan gömülü sistemler; paket kaybı, bağlantı istikrarı ve sıcaklık verileri temelinde değerlendirilmiştir.

1 adet IP Telefon: Cihaz durumu ve ping yanıt süresi temelinde ICMP protokolü ile izlenmiştir.

1 adet Jeneratör: SNMP protokolü ile çalışan güç kaynağı; voltaj durumu, batarya seviyesi ve çalışma süresi gibi kritik parametrelerle takip edilmiştir.

4 adet Sunucu: Dell IDRAC, ClearPass, QRadar ve Voyager gibi işlevsel farklılıklar gösteren sistemler; işlemci yükü, bellek tüketimi, servis çalışır lığı ve disk doluluk oranı gibi temel göstergelerle izleme kapsamına alınmıştır.

Veri toplama süreci, cihazın desteklediği protokole göre uyarlanmış; SNMPv2c protokolüyle sağ anahtarı, güvenlik duvarı, jeneratör gibi cihazlardan; SNMPv1 ile Siemens PLC cihazlarından veri çekilmiştir. Her cihaza özgü şablonlar atanmış, bu şablonlar sayesinde aşağıdaki metrik grupları sürekli olarak gözlemlenmiştir:

İşlemci kullanımı, bellek durumu, disk kapasitesi, ağ trafiği, ICMP gecikme süresi, paket kaybı,

SNMP ajan durumu, servis çalışır lığı, cihaz açık kalma süresi.

Ayrıca Zabbix‘in Low-Level Discovery (LLD) özelliği kullanılarak ağ anahtarı portları, disk birimleri ve servisler otomatik olarak tespit edilip yapılandırılmıştır. Ağ üzerinde IP aralıklarına göre oluşturulan otomatik keşif kuralları sayesinde yeni eklenen cihazlar kendiliğinden izlemeye alınmış; üst veri filtreleri yardımıyla uygun gruplara ve şablonlara yönlendirilmiştir.

5.1 Python Betik ile Otomatik Zabbix Şablon Oluşturma ve Güncelleme Süreci

Zabbix‘in izleme altyapısında SNMP tabanlı cihazlardan veri toplamak için kullanılan şablonlar, xml formatında dışa ve içe aktarılabilmektedir. Bu özellik, manuel işlemlerin otomatikleştirilmesini ve geniş ölçekli izleme yapılandırmalarının daha etkin yönetilmesini mümkün kılar. Bu kapsamda geliştirilen bir Python betik aracılığıyla, kullanıcı tanımlı SNMP nesne tanımlayıcılarına karşılık gelen veri öğeleri otomatik olarak bir Zabbix şablon xml dosyasına dönüştürülmektedir.

5.1.1 Betiğin Temel Yapısı

Bu tez kapsamında geliştirilen generate_zabbix_template.py adlı Python betiği, geçmişte GitHub üzerinde yayımlanmış olan ancak günümüzde erişilemeyen “zabbix-templator” projesinden [28] esinlenilerek oluşturulmuştur. Söz konusu açık kaynak proje, SNMP OİD

tabanlı veri tanımlarını kullanarak otomatik Zabbix XML şablonları üretmeye olanak sağlamaktaydı. Ancak projenin güncel sürümlerle uyumsuz kalması ve GitHub üzerinden erişime kapatılması nedeniyle, bu çalışmada söz konusu mantık yeniden yapılandırılmıştır. Yeni geliştirilen betik, Python'un lxml. etree kütüphanesi kullanılarak SNMP nesne tanımlayıcılarını, veri öğesi adı, açıklama, veri türü ve birim gibi parametrelerle birleştirip Zabbix'in tanımlı XML formatına dönüştürmektedir.

Betik çalıştırıldığında zabbix_template. xml adlı dosya otomatik olarak oluşturulmakta ve bu dosya Zabbix ara yüzü üzerinden içe aktarılabilmektedir. Bu yöntem sayesinde kullanıcılar, özellikle çok sayıda SNMP tabanlı veri öğesi barındıran cihazlar için manuel tanımlama yapmadan, yapılandırılmış ve kullanılabilir Zabbix şablonlarını dinamik biçimde oluşturabilmektedir. Geliştirilen betiğin etkili şekilde kullanılabilmesi için belirli adımların sırasıyla uygulanması gerekmektedir. SNMP cihazlardan veri alınması, bu verilerin betik yapısına uygun şekilde tanımlanması ve nihai olarak Zabbix sistemine şablon biçiminde aktarılması süreci; hem zaman kazancı sağlamakta hem de kullanıcı müdahalesine bağlı hataların önüne geçmektedir. Aşağıda, bu otomasyon sürecinin nasıl işlediği adım adım açıklanmıştır.

Kullanım Süreci

SNMP tabanlı izleme yapılacak cihazlardan veri toplama süreci, öncelikle SNMPwalk komutu kullanılarak cihazın desteklediği nesne tanımlayıcılarının elde edilmesiyle başlar. Elde edilen bu OİD'ler, anlamlı açıklamalar ve etiketlerle birlikte Python betiği içerisine tanımlanır. Betik çalıştırıldığında, tanımlanan tüm bu bilgiler kullanılarak Zabbix'e uygun bir XML şablon dosyası otomatik olarak oluşturulur. Oluşturulan şablon, Zabbix web ara yüzü üzerinden "Yapılandırma → Şablonlar → İçeri Aktar" adımları takip edilerek sisteme entegre edilir ve kullanılabilir hâle getirilir.

Avantajları

Bu yöntem sayesinde SNMP destekli yeni cihazların izleme yapılandırmaları kısa sürede hazırlanabilir, nesne tanımlayıcılarla yapılan güncellemeler kolayca şablona entegre edilebilir, insan hatası riski azalır ve sürüm kontrolü sağlanabilir; tez kapsamında incelenen Siemens SIMATIC S7 ve IM153-4PN modüllerine ait özel SNMP nesne tanımlayıcılar ile betiğin doğruluğu test edilmiştir.

Örnek Nesne Tanımlayıcıları Tanımı (Betik içinde)

Aşağıdaki örnekte Zabbix SNMP izleme sistemleri için otomatik şablon üretimi yapan bir Python betiği içerisinde tanımlanmış bir veri öğesi tanımı verilmiştir.

python

{ "name": "System Uptime",

"oid": "1.3.6.1.2.1.1.3.0",

"key": "sysUpTime",

"units": "uptime",

"value_type": "3", # COUNTER

"description": "Device uptime in hundredths of seconds." }

Zabbix altyapısına uyumu sırasında Python ile otomatik XML şablon üretimi, hem izleme süreçlerinin hızlanmasını sağlamakta hem de büyük ölçekli ortamlarda merkezi yönetimi kolaylaştırmaktadır. Özellikle kurumsal ağ izleme sistemlerinde, yüzlerce cihazın hızlı bir şekilde entegre edilmesi için bu tarz otomasyon çözümleri kritik öneme sahiptir.

Şekil 8 örneğinde görüleceği üzere cihazın hangi parametreleri desteklediğini ve hangi metriklerin izlenebileceği ortaya koyulmaktadır. Elde edilen nesne tanımlayıcıları, Zabbix şablonuna dönüştürülerek cihazın sistematik ve sürekli izlenmesine olanak sağlamaktadır.

Şekil 8 de SNMPwalk komutu ile 10.0.60.11 ip adresine sahip cihaz üzerinde çalışan nesne tanımlayıcıları değerleri görülmektedir.

```
root@zabbix:/home/zabbix# snmpwalb -v1 -c public 10.60.0.1
iso.3.6.1.2.1.1.1.0  STRING: Siemens, SIMATIC S7, CPU 15125-1 EN, 6ES7
512-1DI00-0AB0, HV: Version 7, FV: Version
           H· C—Nt89925672J021"
iso.3.6.1.2.1.1.1.0  OCTT: (119249430)1 day:  9.08:»14.30
iso.3.6.i.2.1.1.1.0 = ""
iso.3.8.1.2.1.1.1.0 = ""
iso.3.6.1.2.1.1.1.0 ='"
iso.3.6.1.2.1.1.1.0  INTEGER  79
iso.3.6.1.2.1.1.1.1.1 Timeticks (0) 00:00.00.00
iso.3.6.1.2.1.1.1.1.2 = OID: iso.0.8802.1
iso.3.6.1.2.1.1.1.1.3 = OID: iso.0.6243.1
iso.3.6.1.2.1.1.1.1.4 = OID: iso.3.6.1.1
iso.3.6.1.2.1.1.1.1.5 = OID: iso.3.6.1.1.1
iso.3.6.1.2.1.1.1.1.6 = OID: iso.3.6.1.1.1
iso.3.6.1.2.1.1.1.1.7 = OID: iso.3.6.1.1.1
iso.3.6.1.2.1.1.1.1.8 = OID: iso.3.6.1.1.1
iso.3.6.1.2.1.1.1.1.9 = OID: iso.3.6.1.1.1
iso.3.6.1.2.1.1.1.1.1 = STRING: isso0020ctiieee802doti.ieee802dotimbs.11d
iso.3.6.1.2.1.1.1.1.1  INTEGER:.occieerdoct.ieee802dotmbs.iid
iso.3.6.1.2.1.1.9.1.5 = STRING: "iso.org.dod.internet.mib 2"
iso.3.6.1.2.1.1.9.1.4 = STRING: "iso.org.dod.internet.mib 2.1·MIB"
iso.3.6.1.2.1.1.9.1.5 = STRING: "iso.org.dod.internet.mib 2.cngMIB"
iso.3.6.1.2.1.1.9.1.6 = STRING: "iso.org.dod.internet.mib 2.udgMIB
iso.3.6.1.2.1.1.9.1.7 = STRING: "iso.org.dod.internet.mib 2.snmp"
iso.3.6.1.2.1.1.9.1.8 = STRING: "iso.org.dod.internet.mib 2.1miIB"
iso.3.6.1.2.1.1.9.1.9 = INTEGER: 1  00ITEGD.1
iso.3.6.1.2.1.1.9.1.1 = INTEGER: 1
iso.3.6.1.2.1.1.9.1.2 = INTEGER: 2
iso.3.6.1.2.1.1.9.1.3 = INTEGER: 3
iso.3.6.1.2.1.1.9.1.4 = INTEGER: 4
iso.3.6.1.2.1.1.9.1.5 = INTEGER: 5
iso.3.6.1.2.1.1.9.1.6 = INTEGER: 6
iso.3.6.1.2.1.1.9.1.7 = INTEGER: 1
iso.3.6.1.2.1.1.9.1.8 = INTEGER:
iso.3.6.1.2.1.1.9.1.9 = INTEGER: 1
iso.3.6.1.2.1.1.9.1.0 = INTEGER: 1
iso.3.6.1.2.1.1.9.1.1 = STRING: "Siemens, SIMATIC S7, Internal. X1"
iso.3.6.1.2.1.1.9.1.2 = STRING: "Siemens, SIMATTC S7, Ethernet Port. X1PIR
iso.3.6.1.2.1.1.9.1.1 = STRING: "Siemens, SIMATTC S7, Ethernet Port. X1PIR
iso.3.6.1.2.1.1.9.1.2 = INTEGER: 6
```

Şekil 8. Snmpwalk komutu ile çalışan nesne tanımlayıcıları değerlerinin görüldüğü ekran

Şekil 9 örneğinde görüldüğü üzere, Python kodu aracılığıyla SNMP tabanlı cihazlara ait öğelerin tanımlanması ve Zabbix formatında XML şablon dosyası üretilmiştir. Bu yöntem, manuel tanımlamaya kıyasla zaman tasarrufu sağlayarak otomasyonu desteklemektedir.

Şekil 9 da nano metin düzenleyicisinde generate_zabbix_template adında bir dosya oluşturulmakta ve bu dosyanın içine Zabbix şablon üretimini sağlayacak olan Python betiği yazılmıştır.

```
root8zabbix:/home/zabbix# nano generate zabblx_templa
GNU hano 6.2
from ixm imporetree
import uuid
items = [
        "name": "System Uptime",
        "oid": "1.3.6.1.2.1.3.0"",
        "key": "ifInOcters",
        "value_type": UNSINGEND"
]       "units": "B"
    },
        "name": "PortI InOctets".
        "oid": "1.3.6.1.2.1.2.2.10.1",
        "key": "ifInOctets.1",
        "value_type": "B"
]       "units": "B"

zbx = etree.Element("zabbix_export" =
exree.SubElement(zbx, version").teixt "7.0"

templates = etree.SubElemet(zbx, "templates")
templatet = etree.SubElemet(zbx, "templates")
templatet = etree.SubElemet(template).text,uuid().hex
templatet = etree.SubElemenftame_.text vuid.uudi4(.hex
templatet = etree SubElement(name) ,= uniud.udd," ato"
groups = etree.SubElement(gtoups,"groups"
group = etree.SubElement(group),"group")
items_tag = subElement(items)
for item in items:
    etree.SubElement(it=template_tag,item')
    etree.SubElement(item_tag,"item").hex
    etree.SubElement(item_tag = 2 = uuid4(L).hex
    etree.SubElement(item_tag,"snmpoid")=uuid( ,key"
    etree.SubElement(item_tag,"key")= item."key"
    items_tag = delemfttemp,'d' = "60s")
    item_tag = history(item_?d') = "7d")
    item_tag = trends(item'30d') = "30d'
    item_tag = value_type(item)raiuetype= "value_type"
    item_tag = units(item_tag")' item "nunits")
```

Şekil 9. Nano metin düzenleyicisinde dosya oluşturulan ve içerisine Python betiği yazılan ekran

Şekil 10 örneğinde görüldüğü üzere bilgisayarda komut istemi açılarak Zabbix sunucusunun IP adresi ve şablonu kaydettiğimiz isimle birlikte hangi klasöre şablonun indirilmesi gerektiği belirtilmiştir. Sorulan şifre Zabbix için belirlediğimiz şifredir.

Şekil 10 da komut istemi üzerinden şablonun indirileceği ekran görülmektedir.

```
C:\Users\gokhantest>sp zabbix@192.168.41.128:/home/zabbix/zemplate.xml
C:\Users\gokhantest\s password:
zabbix_template.xml                                   100% 1645  1.6MB/s
```

Şekil 10. Komut istemi üzerinden şablonu bilgisayarımıza indireceğimiz ekran

Tezin ana konusu kapsamında geliştirilen Python tabanlı otomatik şablon ekleme yöntemi, özellikle şablonu bulunması güç veya imkânsız olan eski nesil IoT cihazlarının Zabbix üzerinde izlenmesine önemli bir kolaylık sağlamıştır. Örneğin, çalışma kapsamında kullanılan Siemens PLC için hazır bir şablon arama süreci yaklaşık bir saat sürmüş, üretici firmaya yapılan talebe ise geri dönüş alınamamıştır. Buna karşın, cihaz için izlenebilecek parametrelerin belirlenmesi ve bu parametrelere ait genel OİD değerlerinin tespit edilmesi yalnızca 30 dakika içerisinde tamamlanmıştır. Toplamda beş izlenebilir parametre için gerekli OİD değerleri belirlendikten sonra, Python betiği aracılığıyla bu değerlerin şablona entegre edilmesi ve Zabbix üzerine otomatik olarak eklenmesi yaklaşık üç dakika sürmüştür. Böylece manuel süreçlere kıyasla zaman tasarrufu sağlanmış, aynı zamanda insan hatası olasılığı da önemli ölçüde azaltılmıştır.

Tablo 4. Eski nesil IoT cihazlarda manuel şablon arama ile Python Script tabanlı otomatik şablon ekleme sürelerinin karşılaştırılması

Süreç Adımı	Manuel Yöntem	Python Script Yöntemi	Kazanım
Hazır şablon arama	1 saat (şablon bulunamadı, üreticiye talep gönderildi, dönüş alınmadı)	Gerek yok	Zaman tasarrufu
İzlenecek parametrelerin belirlenmesi ve OID değerlerinin tespiti	30 dakika	30 dakika	Aynı süre
Şablon oluşturma ve Zabbix'e ekleme	Manuel yöntemle mümkün değil / çok uzun sürecekti	3 dakika	Süreklilik ve hız
Toplam izlenebilir değer sayısı	Belirlenemedi	5 parametre (İşlemci, bellek, çalışma süresi vb.)	İzleme kapsamı sağlandı
Genel değerlendirme	Şablon bulunamadığı için süreç tamamlanamadı	Tamamlandı, 5 parametre aktif izleniyor	%90+ zaman tasarrufu, hata riski azaldı

5.2 IoT Cihazın (Siemens Simatic S7 PLC) İzlenmesi

Siemens Simatic S7 PLC cihazı üretimde kullanılan ve verileri oldukça önemli bir bileşendir. Fakat cihaz eski olduğundan sadece SNMPv1 desteği olduğu tespit edildi. Öncelikle Snmpwalk komutu ile cihaz üzerinde çalışan nesne tanımlayıcıları değerleri keşfedildi ve o nesne tanımlayıcılarına karşılık gelen parametreler bulundu. Daha sonra yukarıda "Python Betik ile Otomatik Zabbix Şablon Oluşturma ve Güncelleme Süreci" başlığı altında anlatıldığı gibi işlemler gerçekleştirildi ve cihaza özgü şablon oluşturuldu.

5.2.1 PLC Veri Değerlerinin İncelenmesi

Şekil 11 örneğinde görüldüğü üzere, Siemens PLC cihazına ait donanım ve yazılım bilgileri, port durumu, işlemci yükü, yazılım sürümü ve sistem çalışma süresi gibi metriklerin Zabbix ara yüzünde izlenebilir. Bu yapı sayesinde cihazın performans ve ağ durumu sürekli takip edilerek olası arızalara erken müdahale imkânı sağlanmaktadır.

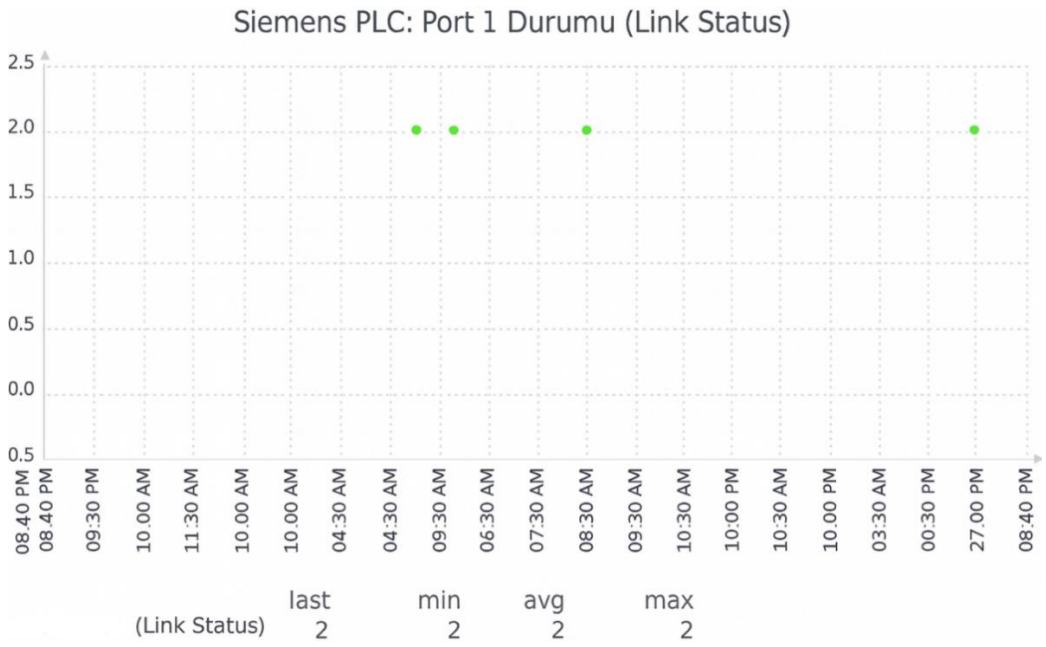
Şekil 11 de PLC için oluşan bütün veri değerleri görülmektedir.

Host	Last check	Last value	Change	Tags
Siemens PLC	50m 15s	Siemens, SIMATIC...		History
CPU Tanim				History
Hardware Version (Link Status)	50m 15s	2		History
Port 1 Durumu (Link Status)	50m 15s	0 B		Graph
Port 1 Gelen Ven (RX bytes)	50m 15s	0 B		Graph
Port 1 Hatali Alinan Paketier	50m 15s	0		Graph
Port 1 MAC Adresi	50m 15s	EC 1C 5D 02 9C 3D		Graph
Processor Load Level				Application System
SNMP Alinan Istekler	50m 15s	7942		
Sottware Version	50m 15s	4		Application
System State	50m 15s	1 day, 07:42.55		Graph
Çalişma Süresi (Uptime)	50m 16s	4M 0g 3h 49m		Graph

Şekil 11. PLC veri değerlerini gösteren ekran

Şekil 12 örneğinde görüldüğü üzere minimum, maximum ve ortalama değerlerin aynı olması, portun kesintisiz ve stabil bir bağlantı sağladığını göstermektedir. Bu durum, sistemin sürekliliği ve güvenilir veri aktarımı açısından önemli bir performans göstergesi olarak değerlendirilmektedir. Ayrıca portun kararlı yapısı, ağ üzerindeki potansiyel kesinti risklerini minimize ederek üretim süreçlerinin sürekliliğine katkı sağlamaktadır. Elde edilen bulgular, PLC tabanlı otomasyon sistemlerinde ağ güvenilirliğinin yüksek düzeyde sağlandığını ortaya koymaktadır.

Şekil 12 de PLC'nin 1. portunun durumu görülmektedir.

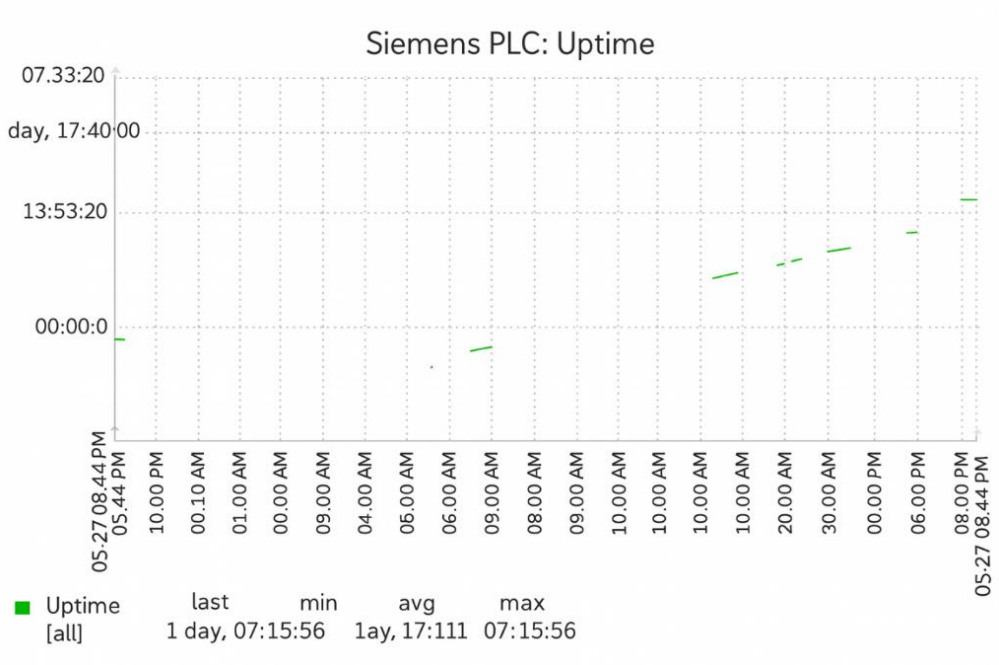


Şekil 12. PLC'nin 1.portunun durumunu gösteren ekran

Şekil 13 örneğinde görüleceği üzere, Siemens PLC'nin kesintisiz çalışma süresi Zabbix ara yüzü üzerinden zaman serisi olarak izlenmektedir. Grafik, cihazın çalışma süresinin minimum 1 gün 7 saat 15 dakika, ortalama 1 gün 7 saat ve maksimum 1 gün 17 saat olarak ölçüldüğünü göstermektedir. Bu değerler, cihazın uzun süreli istikrarlı çalıştığını ve kesinti yaşanmadığını

ortaya koymaktadır. Dolayısıyla sistem sürekliliği yüksek düzeyde korunmuş ve endüstriyel süreçlerde güvenilirlik sağlanmıştır.

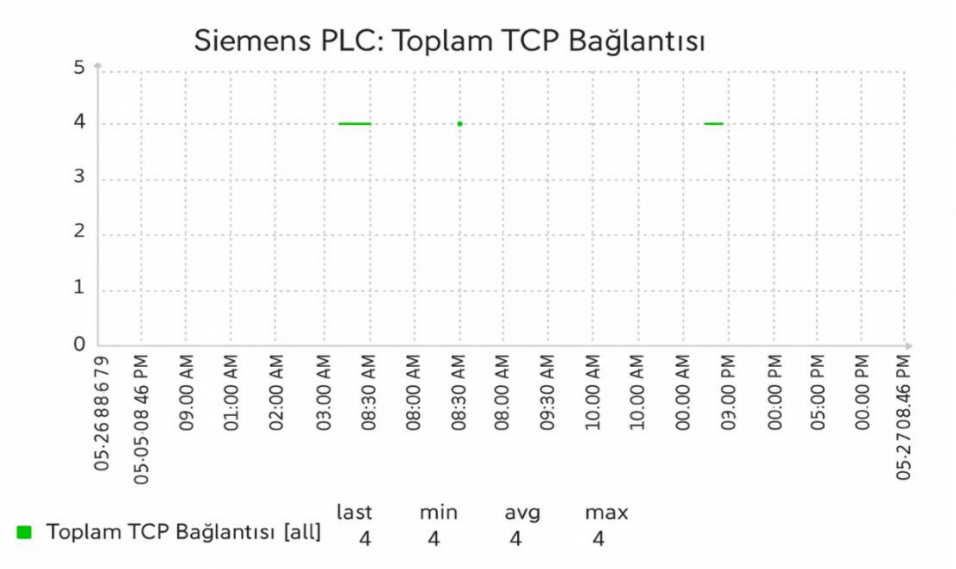
Şekil 13 te PLC'nin çalışma süreleri görülmektedir.



Şekil 13. PLC'nin çalışma sürelerini gösteren ekran

Şekil 14 örneğinde görüleceği üzere Siemens PLC'nin Zabbix üzerinden izlenen toplam TCP bağlantı sayısı verilmektedir. Grafik verilerine göre cihazın minimum, maksimum ve ortalama bağlantı sayısı 4 olup, son ölçümde de 4 aktif bağlantı görülmektedir. Bu durum, cihazın ağ üzerinden sabit sayıda TCP oturumu ile çalıştığını ve bağlantı yoğunluğunda dalgalanma yaşanmadığını ortaya koymaktadır. İstikrarlı bağlantı düzeyi, PLC'nin iletişim kararlılığını ve ağ performansında sürekliliği göstermektedir.

Şekil 14 te PLC'ye yapılan toplam TCP bağlantı sayısını göstermektedir.



Şekil 14. PLC'ye yapılan toplam TCP bağlantı sayısını gösteren ekran

5.3 IoT Cihazın (Siemens IM153-4PN Modül) İzlenmesi

5.3.1 Modül Veri Değerlerinin İncelenmesi

Şekil 15 örneğinde görüleceği üzere, Siemens PLC 'ye ait IP adresi (10.0.60.12), port açıklamaları, hata durumları, MAC adresleri, giriş-çıkış trafiği ve port hızları gösterilmektedir. Ölçümlere göre Port 1'de herhangi bir hata bulunmazken, Port 2 çıkış trafiği 2.51 GB (Gigabayt) seviyesinde kaydedilmiş ve 100 Mbps (Megabits Per Second) hızla çalıştığı görülmüştür. Bu veriler, cihazın ağ bağlantılarının aktif olduğunu, iletişimde hata yaşanmadığını ve port performansının kararlı bir şekilde sürdüğünü ortaya koymaktadır. Ayrıca Port 2'nin yüksek veri çıkışı, cihazın üretim hattında aktif olarak kullanıldığını göstermektedir. Bu durum, sistemin sürekli veri alışverişi içinde olduğunu ve operasyonel sürekliliği desteklediğini kanıtlamaktadır.

Şekil 15'te Modül veri değerleri görülmektedir.

Device IP Address	51m 57s	10.0.60.12
Port1 Description	51m 58s	Siemens, SIM TIC
Port1 In Errors	0 B	0 errors
Port1 MAC Addrass	13s	AC 64 17 F8 68 A3
Port1 Oper Status	13s	1
Port2 Oper Status	13s	0 errors
Port2 In Octets	13s	0 errors
Port2 Oup Status	13s	100 Mbps
Port2 Description	13s	1
Port2 In Errors	13s	AC 64 17 F8 63 A
Port2 In Octets	13s	2.51 GB
Port2 Oper Status	13s	AC 64 17 F8 95 A
Port2 Status	13s	1

Şekil 15. Modül veri değerlerini gösteren ekran

Şekil 16 örneğinde görüleceği üzere, Siemens PLC'nin Port 3'e ait veri trafiği, hata kayıtları, hız bilgisi ve sistemin genel çalışma süresi gösterilmektedir. Ölçümlere göre Port 3'te giriş trafiği 1.43 gb, çıkış trafiği ise 2.88 gb olarak kaydedilmiş olup hata sayısı bulunmamaktadır. Cihazın çalışma süresinin 132 gün 19 saat olduğu görülmekte, bu da uzun dönemli kesintisiz operasyon sağlandığını göstermektedir. Port 3 üzerinden gerçekleşen veri alışverişinin yoğunluğu, PLC'nin ağ iletişiminde aktif olarak kullanıldığını ortaya koymaktadır. Ayrıca hata oranlarının sıfır olması, cihazın güvenilirliğini ve ağ performansındaki istikrarı desteklemektedir.

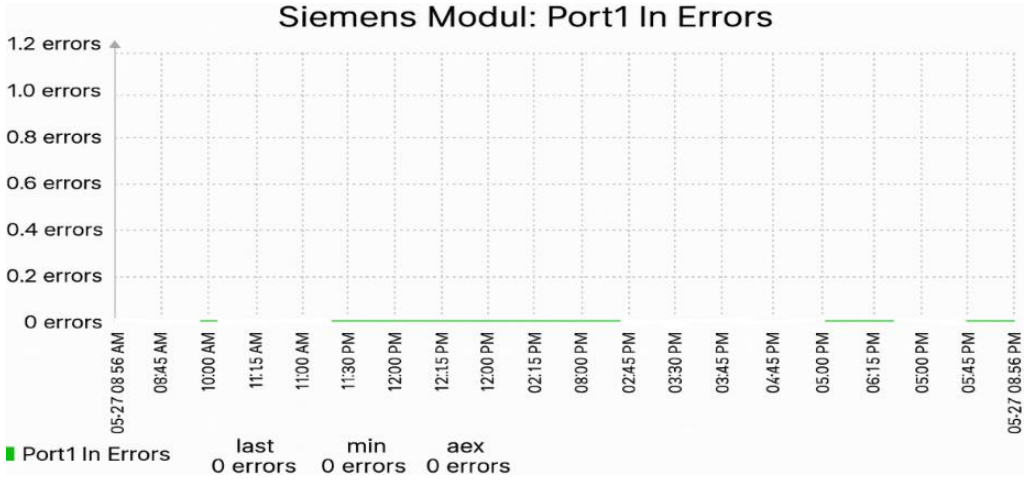
Şekil 16 da Modül veri değerleri görülmektedir.

Name	Last check	Last value	Change
Port2 Out Errors	13s	0 errors	
Port3 Oper Status	13s	1.43 GB	+2.91 MB
Port3 In Errors	13s	Siemens, SIMATIC...	
Port3 In Octets	13s	AC 64 1	
Port3 MAC Address	13s	0 errors	
Port3 Oper Status	13s	0 errors	
Port3 Oper Status	13s	0 errors	
Port3 Speed	13s	1	+0 errors
Port3 Up-Errors	13s	2.88 GB	
Port3 Up Octetes	13s	2 dbps	+1.56 MB
System Uptime	13s	132 days, 19:14:00	

Şekil 16. Modül veri değerlerini gösteren ekran

Şekil 17 örneğinde görüleceği üzere Siemens modülünün Port1 giriş hataları Zabbix ara yüzü üzerinden zaman serisi halinde gösterilmektedir. Grafik verilerine göre son, minimum, ortalama ve maksimum hata sayısı 0 olarak ölçülmüş, portta herhangi bir hata kaydedilmemiştir. Bu sonuç, ilgili portun ağ iletişiminde istikrarlı çalıştığını ve veri iletiminde kayıp ya da bozulma yaşanmadığını ortaya koymaktadır. Ayrıca, hatasız bağlantı performansı cihazın güvenilirliğini artırmakta ve endüstriyel ağlarda süreklilik sağlamaktadır.

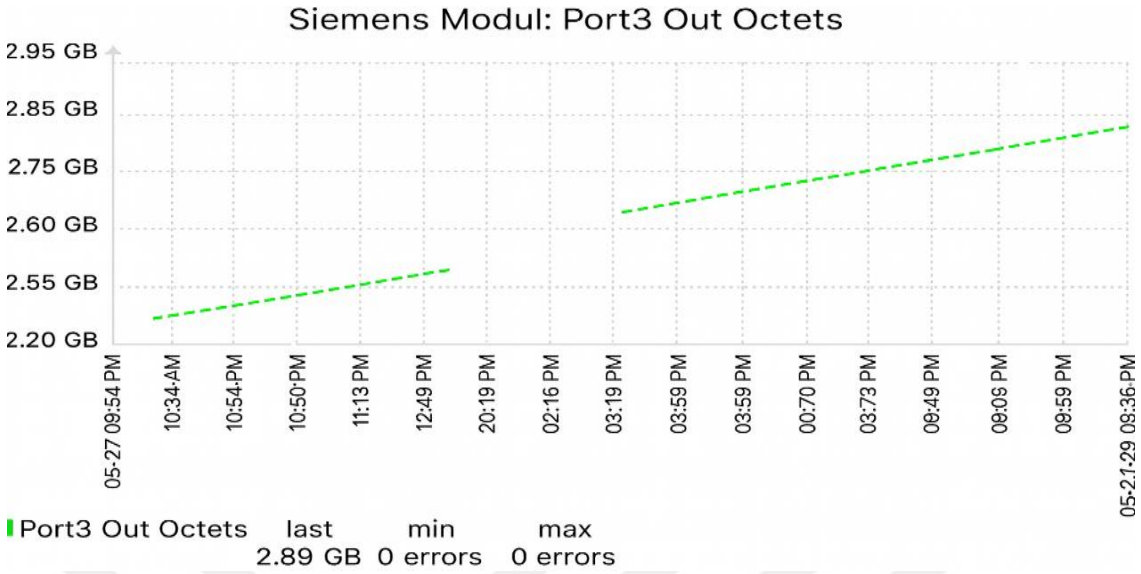
Şekil 17 de modülün 1.portuna gelen hatalı paket sayısı görülmektedir.



Şekil 17. Modülün 1.portuna gelen hatalı paket sayısını gösteren ekran

Şekil 18 örneğinde görüleceği üzere Siemens modülünün Port 3 çıkış trafiği Zabbix ara yüzünde zaman serisi grafiği olarak gösterilmektedir. Grafik verilerine göre Port 3 üzerinden gerçekleşen toplam çıkış trafiği 2.89 GB olup minimum ve maksimum değerler sabit şekilde ölçülmüştür. Trafikte herhangi bir hata kaydedilmemiş, bu da portun veri aktarımını kesintisiz ve güvenilir şekilde sağladığını ortaya koymaktadır. Ayrıca trafiğin zamana bağlı olarak kademeli biçimde artması, cihazın sürekli olarak dışa veri ilettiğini ve aktif bir üretim sürecinde kullanıldığını göstermektedir.

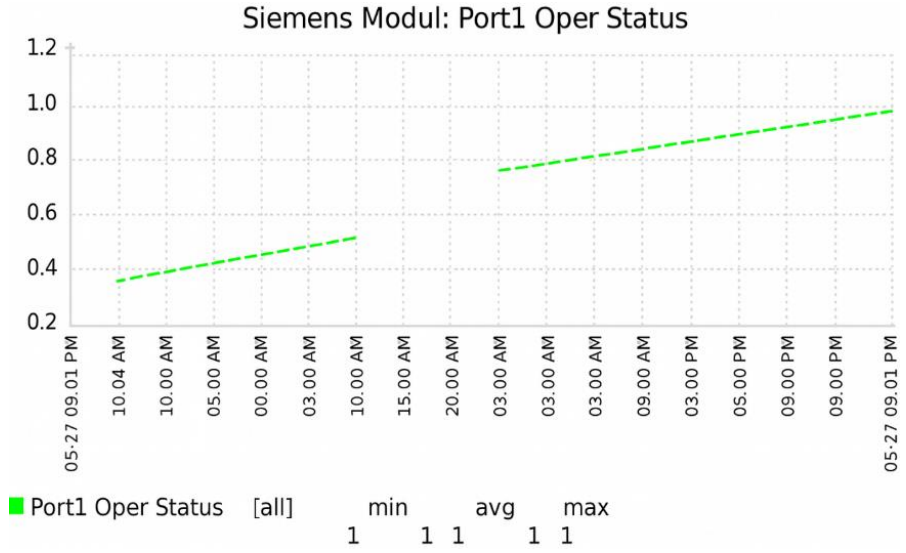
Şekil 18 de modülün 3.portu üzerinden gönderilen bayt miktarı görülmektedir.



Şekil 18. Modülün 3.portu üzerinden gönderilen bayt miktarını gösteren ekran

Şekil 19 örneğinde görüleceği üzere, Siemens modülünün Port 1 çalışma durumu Zabbix ara yüzünde zaman serisi grafiği olarak gösterilmektedir. Grafik verilerine göre Port 1 'in minimum, maksimum ve ortalama değeri 1 olup, portun sürekli aktif durumda çalıştığı görülmektedir. Bu durum, portun herhangi bir kesinti yaşamadan istikrarlı bir şekilde ağ iletişimini sürdürdüğünü ortaya koymaktadır. Ayrıca portun operasyonel durumunda dalgalanma bulunmaması, cihazın güvenilir veri aktarımı sağladığını kanıtlamaktadır.

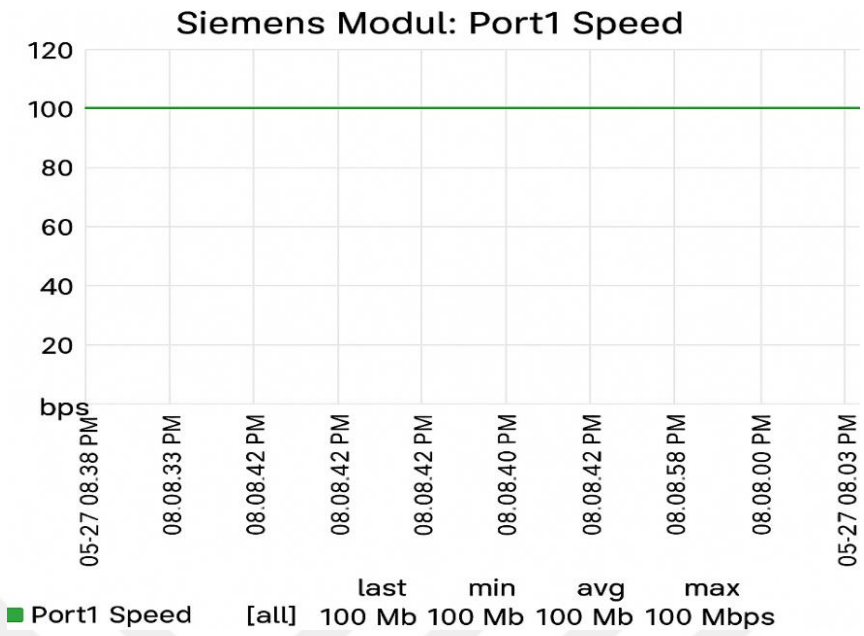
Şekil 19 da modülün 1.portunun gerçek zamanlı çalışma durumu görülmektedir.



Şekil 19. Modülün 1.portunun çalışma durumunu gösteren ekran

Şekil 20 örneğinde görüleceği üzere, Siemens modülünün Port1 hız değeri Zabbix ara yüzünde izlenmektedir. Grafik verilerine göre Port1 'in minimum, maksimum ve ortalama değerleri 100 Mbps olarak sabit kalmış, son ölçümde de aynı hız korunmuştur. Bu durum, portun sürekli olarak 100 Mbps hızında çalıştığını ve hız dalgalanması yaşanmadığını göstermektedir. Ayrıca sabit hız değeri, ağ iletişiminin istikrarlı olduğunu ve cihazın güvenilir veri aktarımı sağladığını ortaya koymaktadır.

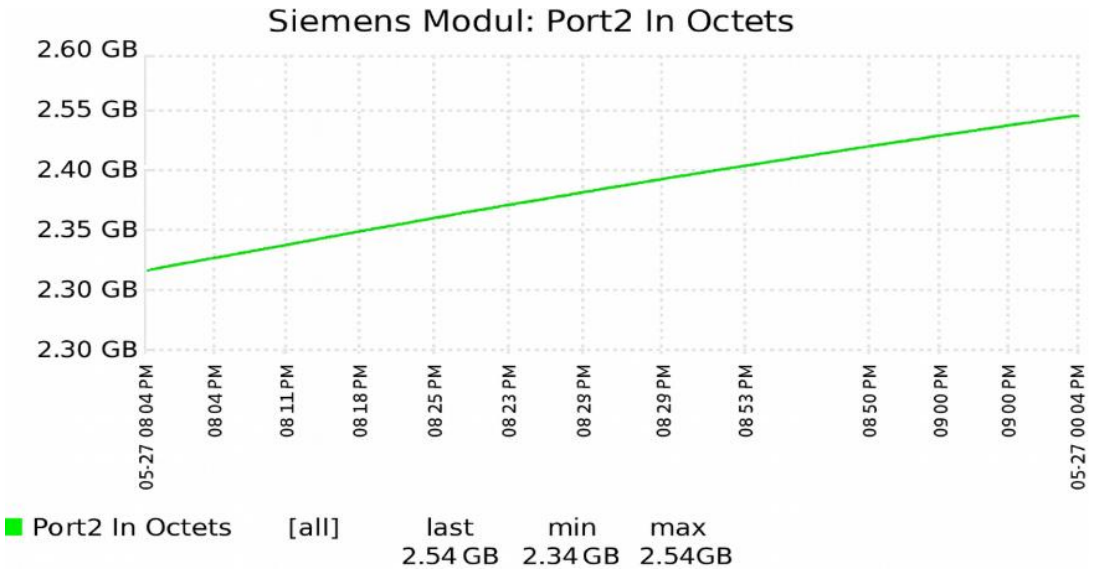
Şekil 20 de modülün 1.portunun hızını gösterir.



Şekil 20. Modülün 1.portunun hızını gösteren ekran

Şekil 21 örneğinde görüleceği üzere, Siemens modülünün Port 2 üzerinden aldığı giriş trafiği Zabbix ara yüzünde zaman serisi grafiği olarak izlenmektedir. Grafik verilerine göre Port 2 'nin minimum değeri 2.34 GB, maksimum değeri 2.54 GB olup, son ölçümde 2.54 GB seviyesine ulaşmıştır. Trafiğin zamana bağlı olarak düzenli artış göstermesi, portun sürekli veri aldığını ve aktif olarak kullanıldığını ortaya koymaktadır. Ayrıca hata kaydının bulunmaması, giriş trafiğinin güvenilir şekilde işlendiğini ve cihazın ağ performansının kararlı olduğunu kanıtlamaktadır.

Şekil 21 de modülün 2.portu üzerinden alınan bayt miktarı görülmektedir.

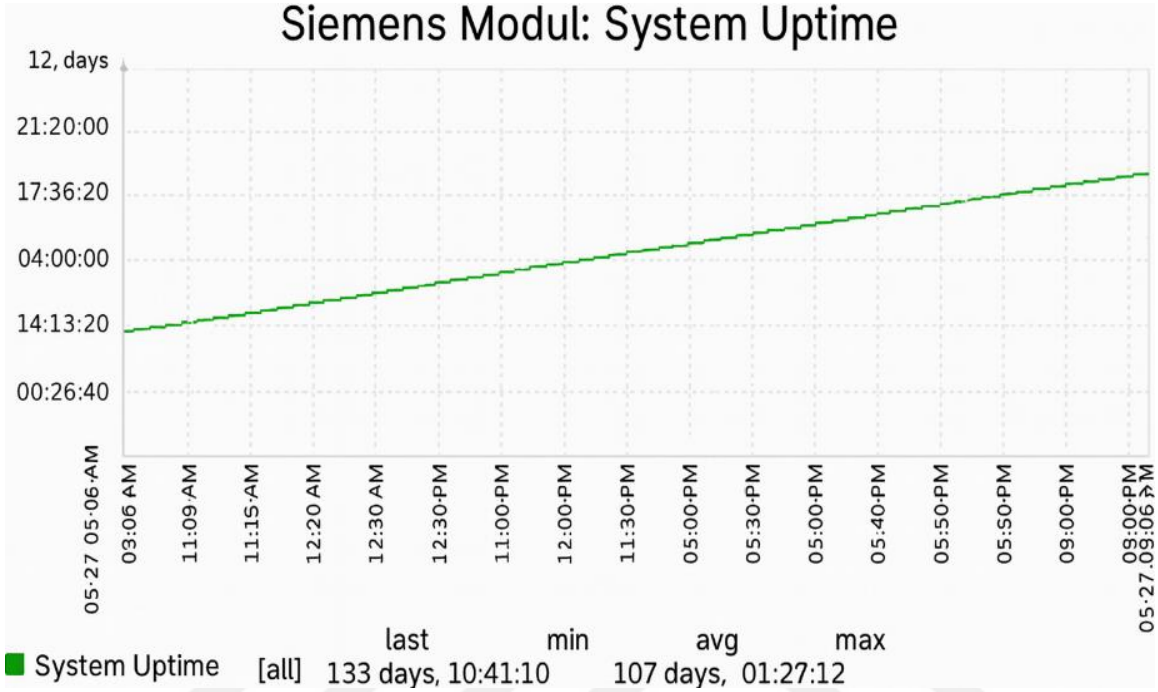


Şekil 21. Modülün 2.portu üzerinden alınan bayt miktarını gösteren ekran

Şekil 22 örneğinde görüleceği üzere, Siemens modülünün çalışma süresi Zabbix ara yüzü üzerinden zaman serisi grafiği olarak gösterilmektedir. Grafik verilerine göre cihazın minimum çalışma süresi 107 gün, ortalama değeri 127 gün ve son ölçümde ulaştığı süre 133 gün 10 saat

olarak kaydedilmiştir. Bu değerler, cihazın uzun dönem boyunca kesinti yaşamadan çalıştığını ve sistem sürekliliğini yüksek seviyede koruduğunu ortaya koymaktadır. Ayrıca uptime eğrisinin düzenli artışı, modülün istikrarlı bir şekilde çalıştığını ve endüstriyel süreçlerde güvenilirlik sağladığını göstermektedir.

Şekil 22 de modülün son açılma anından itibaren geçen süre görülmektedir.



Şekil 22. Modülün son açılma anından itibaren geçen süreyi gösteren ekran

5.2.1 ve 5.3.1 bölümlerinde yer alan Şekil 11 den Şekil 22 ye kadar olan görseller, Zabbix üzerinden izlenen PLC (Siemens CPU 1512SP-1 PN) ve IoT modülü (Siemens IM153-4PN) ile ilgili temel ağ ve sistem verilerini göstermektedir. Her bir ekran görüntüsü, ilgili cihazın port durumu, MAC adresleri, SNMP istekleri, veri alışverişi ve çalışma süresi gibi teknik ölçütleri yansıtmaktadır. Bu veriler aracılığıyla cihazların durumlarının anlık olarak takip edilebildiği ve Zabbix'in SNMP protokolü üzerinden çeşitli metrikleri başarıyla çekebildiği görülmektedir. Ancak elde edilen ekran görüntülerinin oldukça metin tabanlı ve teknik olması, görsel derinlikten yoksun bir izleme deneyimi sunduğunu ortaya koymaktadır. Grafiksel temsilin sınırlı olması, özellikle yöneticiler ve teknik olmayan kullanıcılar için verilerin yorumlana bilirliğini zorlaştırmaktadır. Aradaki görsellik farkını görebilmek adına 6.3 bölümünde aynı PLC ve modülün Zabbix'ten elde edilen verilerinin Grafana üzerinde görselleştirilmesi sağlanmıştır.

5.4 Omurga Ağ Anahtarının İzlenmesi

Ağ altyapılarının güvenilirliği, sürekliliği ve yüksek veri akış performansı, doğrudan omurga yapısının sağlıklı ve kararlı çalışmasına bağlıdır. Bu bağlamda, kurumun ağ omurgasında kullanılan HP 5406Rzl2 (model: J9850A) cihazı, sanal yerel alan ağı yönetimi, yönlendirme, erişim kontrol listeleri, port bazlı QoS (Quality of Service) ve gerçek zamanlı trafik izleme gibi ileri seviye ağ yönetim kabiliyetlerine sahiptir. Şasi tipi modüler yapısı sayesinde genişlemeye olanak tanıyan bu cihaz, binlerce eşzamanlı bağlantıyı yönetebilecek kapasitede olup ağ trafiğinin tamamını yöneten merkezî rol üstlenmektedir.

Zabbix izleme altyapısına SNMPv2c protokolü aracılığıyla entegre edilen bu omurga anahtar, sistemde yer alan hazır “HP Enterprise Switch by SNMP” şablonu üzerinden yapılandırılmıştır. Bu sayede cihaz üzerindeki tüm portlar otomatik olarak tanımlanmış ve veri toplama işlemi başlamıştır. İzleme kapsamında öne çıkan başlıca metrikler; aktif portlar üzerinden geçen trafik miktarları, port bazlı paket kayıpları, CRC(Cyclic Redundancy Check) hataları, işlemci kullanımı, cihazın SNMP erişilebilirlik durumu ve dâhili sensörlerden alınan sıcaklık verileridir. Bu sayede hem performans hem de donanımsal sağlık verileri sürekli olarak analiz edilmektedir.

Cihazın tüm ağ trafiğini taşıması nedeniyle yaşanabilecek performans sorunları veya donanımsal hatalar, ağın geneline olumsuz yansıyabilmektedir. Bu riski önleyebilmek amacıyla; aktif portlarda %80 üzeri bant genişliği kullanımı, sıcaklık değerinin 75°C’yi aşması ve işlemcinin %90 üzeri yüklenmesi gibi durumlar için kritik eşik değerler tanımlanmıştır. Bu eşiklerin aşılması hâlinde Zabbix aracılığıyla e-posta ve sesli alarm bildirimleri otomatik olarak tetiklenmektedir. Zabbix sistemi üzerinde bu cihaz için 1504 adet veri öğesi, 710 adet tetikleyici, 160 adet grafik ve 8 adet otomatik keşif kuralı yapılandırılmıştır. Bu kapsamlı izleme yapısı, ağ yönetiminin pratik şekilde sürdürülmesine olanak tanımaktadır. Bununla birlikte, port bazlı trafik dağılımlarının düzenli takibi sayesinde yoğunluk noktaları kolaylıkla belirlenebilmekte ve ağ kaynaklarının daha verimli kullanılması sağlanmaktadır. Cihazın sıcaklık ve işlemci yükü gibi donanımsal parametrelerinin eş zamanlı izlenmesi, olası arızaların önceden öngörülmesine katkı sunmaktadır. Tanımlanan otomatik keşif kuralları sayesinde yeni eklenen modüller ve portlar herhangi bir manuel işlem gerektirmeksizin izleme kapsamına alınmaktadır. Böylece, yönetimsel iş yükü azaltılırken sistemin sürdürülebilirliği artırılmış olmaktadır. Zabbix tabanlı izleme yaklaşımı, omurga ağ anahtarının kritik rolünü destekleyerek hem performans hem de güvenilirlik açısından kurumsal ağın sürekliliğine önemli katkılar sağlamaktadır.

5.4.1 Omurga Ağ Anahtarı Veri Öğelerinin İncelenmesi

Şekil 23 örneğinde görüleceği üzere, HP J9850A omurga ağ anahtarı cihazına ait bellek kullanımı, işlemci yükü, donanım bilgileri, sıcaklık sensör değerleri, ICMP kayıpları, yanıt süreleri ve ağ ara yüzü istatistikleri gösterilmektedir. Ölçümlere göre cihazın toplam belleği 635.78 MB (Megabayt) olup kullanılan bellek 470.47 MB seviyesindedir. CPU kullanım oranı %28.3, sıcaklık sensörü değeri ise 17 °C olarak kaydedilmiştir. Ayrıca ICMP paket kaybı bulunmamış, yanıt süresi ortalama 11.89 Mbps değerinde ölçülmüştür. Ağ ara yüzü (Interface A1) üzerinden alınan ve gönderilen paketlerde hata tespit edilmemiş, çıkış hızı 10 Gbps seviyesinde sabitlenmiştir. Bu veriler, cihazın kararlı bir şekilde çalıştığını, hatasız ağ iletişimi sağladığını ve performansının güvenilir olduğunu ortaya koymaktadır.

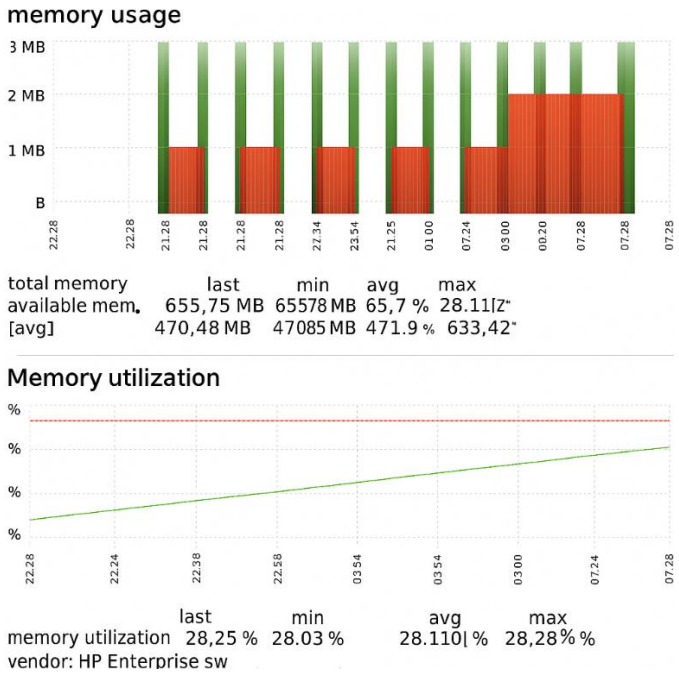
Şekil 23’te omurga ağ anahtarı üzerinde oluşan veri öğelerinin ilk ekranı gösterilmiştir.

#1. Avaliable memory	41s	470.47 MB	40.47 MB	component: memory
#1: Memory utilization	69s	28.2887 %	+0.0004855 %	component: memory
#1: Total memory	61s	635.78 MB		component: memory
#1. Used memory	4h 16m 41s	HP.J3850A Switc...	-152 B	component: system
Chassts: Hardware nodel name.	1m 49m	Rev 0		component: system
Chassts: Hardware version(revision	4h 48m	0 %	- %	component: system
CPU ultization	48n	KB 16. 63.0010		component: system
Firmware version	1m 40m	SG99HK031		component: system
HP J3850A Swrich terperature sensor : Temp	1m 40s	17 °C	+7 °C	component: temperal
ICMP loss	1m 41s	' %		component: nealth c
ICMP ping	1m 40s	0 errors		component: nealth c
ICMP response time	1m 40s	11.89 Mbps	+604.61 Kbps	component: network
Interface A1(): Blts rec eiived	1m 41s	1.68 Mbps	5624 Kbps	component: network
Interface A1(): Duplex status	1m 41s	41.48 GKbps		component: network
Interface A1(): Inbound packets dis carded	1m 41s	0		component: network
Interface A1(): Outbound packets with errors	1m 41s	10 Gt pps		component: network
Interface A1(): Outbound partus	1h 16m 41s	ethernelCsmacd (3)		component: network
Interface A1(): Operational status	1m 41s	10 Gbps		component: network
Interface A1(): Outbound packets discardel	1m 41s	0		component: network
Interface A1(): Outbound packets with errors	1m 41s	10 Gbps		component: network

Şekil 23. Omurga ağ anahtarı üzerinde oluşan veri öğelerinin ilk sayfasını gösteren ekran

Otomatik olarak bellek ile ilgili iki adet şablon Zabbix tarafından oluşturulmuştur. Şekil 24 örneğinde görüldüğü üzere, ağ anahtarı cihazının toplam bellek miktarı, kullanılan bellek ve bellek kullanım oranı Zabbix ara yüzünde izlenmektedir. Grafik verilerine göre cihazın toplam belleği 655.75 MB, mevcut kullanılabilir bellek 470.48 MB olarak ölçülmüştür. Bellek kullanım oranı son ölçümde %28.25 seviyesinde olup, minimum %28.03, maksimum ise %28.28 arasında değişim göstermiştir. Bu veriler, cihazın bellek yönetiminde istikrarlı çalıştığını ve kapasite sınırlarının oldukça altında olduğunu göstermektedir. Ayrıca bellek tüketimindeki düşük seviyeler, cihazın performansını olumsuz etkileyecek bir aşırı yüklenme bulunmadığını ortaya koymaktadır.

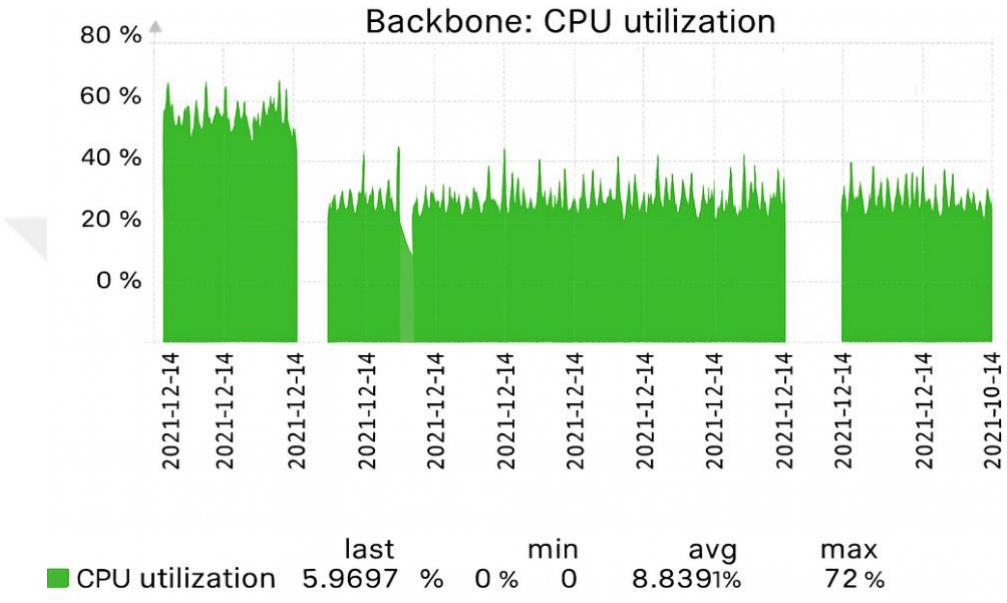
Şekil 24 te omurga ağ anahtarı için oluşturulan bellek şablonları görünmektedir.



Şekil 24. Zabbix'te omurga ağ anahtarının belleği için otomatik olarak oluşturulan şablon ekranları

Şekil 25 örneğinde görüleceği üzere, omurga ağ anahtarı cihazının işlemci kullanım oranı Zabbix ara yüzü üzerinden zaman serisi grafiği olarak gösterilmektedir. Grafik verilerine göre cihazın işlemci kullanım oranı minimum %0, maksimum %72 ve ortalama %8.83 seviyesinde ölçülmüştür. Son ölçüm değerinin %5.96 olması, cihazın mevcut yük altında düşük oranda işlemci kullandığını göstermektedir. İşlemci kullanımındaki dalgalanmalar, ağ trafiği yoğunluğu ve işlenen süreçlerin değişkenliğini yansıtmaktadır. Genel olarak ortalamanın düşük seyretmesi, omurga ağ anahtarı cihazının performans açısından yeterli kaynak kapasitesine sahip olduğunu ve aşırı yüklenme yaşanmadığını ortaya koymaktadır.

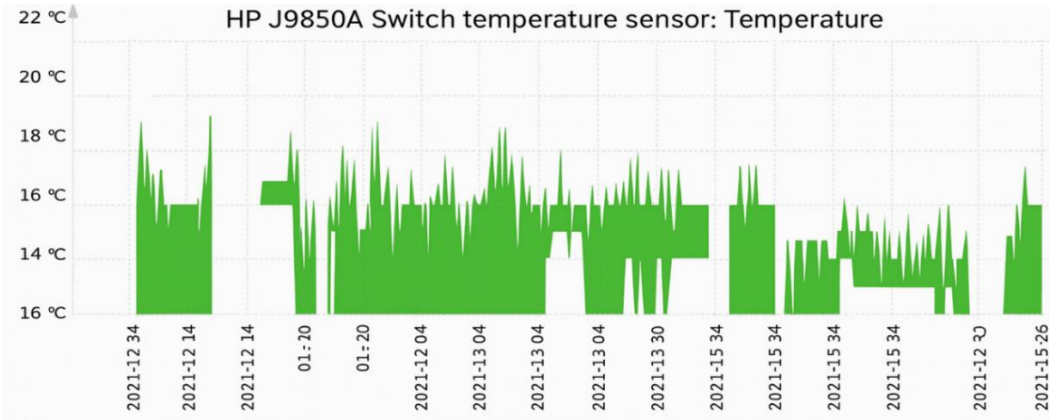
Şekil 25 te işlemci kullanım oranının 6 aylık grafiği görülmektedir.



Şekil 25. Omurga ağ anahtarının işlemci kullanım oranının 6 aylık veri grafik ekranı

Şekil 26 örneğinde görüldüğü üzere, Omurga ağ anahtarı cihazının sıcaklık sensöründen alınan değerler Zabbix üzerinden izlenmektedir. Ölçümlerde sıcaklık değerlerinin 16 °C ile 20 °C arasında değiştiği, ortalama sıcaklık değerinin ise yaklaşık 18 °C seviyesinde olduğu görülmektedir. Cihazın sıcaklık eğrisinde kısa süreli dalgalanmalar bulunsa da genel seyir istikrarlıdır.

Şekil 26 da Omurga ağ anahtarının sıcaklık değerleri görülmektedir.



Şekil 26. Omurga ağ anahtarının sıcaklık değerleri ekranı

5.4.2 Omurga Ağ Anahtarı Verilerinde Bulunan Problemlerin İncelenmesi

Şekil 27 örneğinde görüldüğü üzere, Zabbix tarafından otomatik olarak kaydedilen omurga ağ anahtarı problem kayıtları görülmektedir. İlk satırda 29 Mart 2025 saat 11:03:11 tarihinde C14 portu için Ethernet hızında bir düşüş yaşandığı ve bu olayın 41 saniye sürdüğü rapor edilmiştir. Ayrıca omurga ağ anahtarı bileşeninde de benzer hız değişim uyarılarının yaklaşık 4 ay 26 gün boyunca tekrarlandığı görülmektedir.Bu tür uyarılar, ağın kararlılığını ve performansını doğrudan etkileyen kritik parametrelerdir. Zabbix'in sunduğu bu otomatik problem tespiti sayesinde, hız düşüşlerinin tespit edilmesi ve loglanması mümkün olmuştur. Ayrıca tablodaki önem derecesi, düzeltme süresi ve sorunun süresi gibi alanlar yöneticilere detaylı durum analizi yapma fırsatı sunmaktadır. Bu yapı, ağın proaktif şekilde izlenmesini ve olası darboğazların önlenmesini kolaylaştırmaktadır.

Şekil 27 de omurga ağ anahtarından alınan veriler sonucunda görülen problemleri gösteren ekran bulunmaktadır.

Time	Severity	Recovery time	Status	Info	Duration	Update	Actions
2025-03-29 11:03:11 AM		PROBLEM	41s	Interface C14 ; Ethernet has changed to lower speed than it was before*	26d 19h	Update	class: network descript
Information		PROBLEM	Backbone	has change te lower sp eed than it was before*	4M 26d 2	Update	class: network descript
Information		PROBLEM	Backbone		4M 26d 2	Update	
Information		PROBLEM	Backbone		4M 26d 2	Update	
Information		PROBLEM	Backbone		4M 26d 2	Update	

Şekil 27. Omurga ağ anahtarı üzerinde görülen problemleri gösteren ekran

5.5 İki Adet Kenar Ağ Anahtarının İzlenmesi

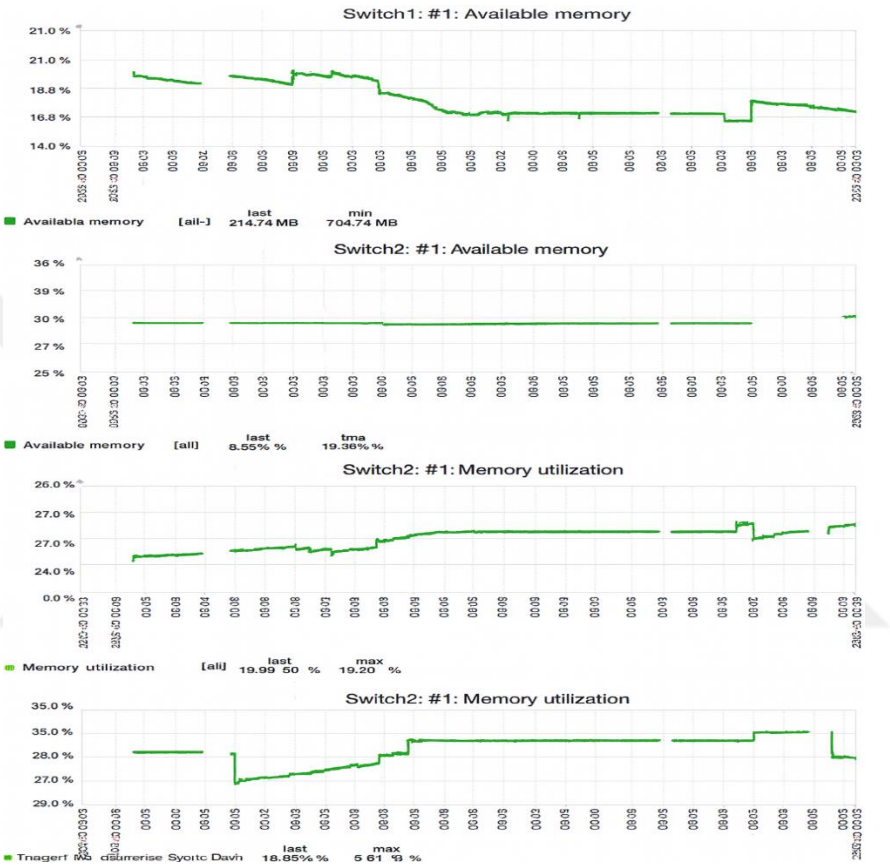
Ağ Anahtarı HPE olduğu için Zabbix'te hazır olarak bulunan şablon olan HP Enterprise Switch by SNMP seçilmiştir.

5.5.1 Ağ Anahtarı Veri Öğelerinin İncelenmesi

Şekil 28 örneğinde görüleceği üzere iki farklı ağ anahtarı cihazına ait bellek kullanım değerleri izlenmektedir. Ağ anahtarı 1 için kullanılabilir bellek, zaman içerisinde belirgin bir azalış göstermekte olup, minimum değer 704,74 MB, son değer ise 214,74 MB olarak ölçülmüştür. Bu durum cihazın yük altında kaldığını ve bellek tüketiminin sürekli arttığını göstermektedir. Ağ anahtarı 2 için kullanılabilir bellek değerleri incelendiğinde, daha dengeli bir seyir izlendiği görülmektedir. Minimum kullanılabilir bellek oranı %8,55, ortalama değeri ise %19,36

seviyesinde kalmıştır. Bu da ağ anahtarı 2'nin bellek kaynaklarının daha stabil şekilde çalıştığını ortaya koymaktadır. Ağ anahtarı 2'nin bellek kullanım oranı incelendiğinde ortalama %19,99, maksimum %19,20 olarak ölçülmüş ve bellek kapasitesinde ani dalgalanmalar olmadığı gözlenmiştir. Ancak son ölçümde bellek kullanım oranının %35 seviyelerine yaklaştığı görülmekte, bu da olası ileriye dönük yüklenmeler için dikkat edilmesi gereken bir duruma işaret etmektedir.

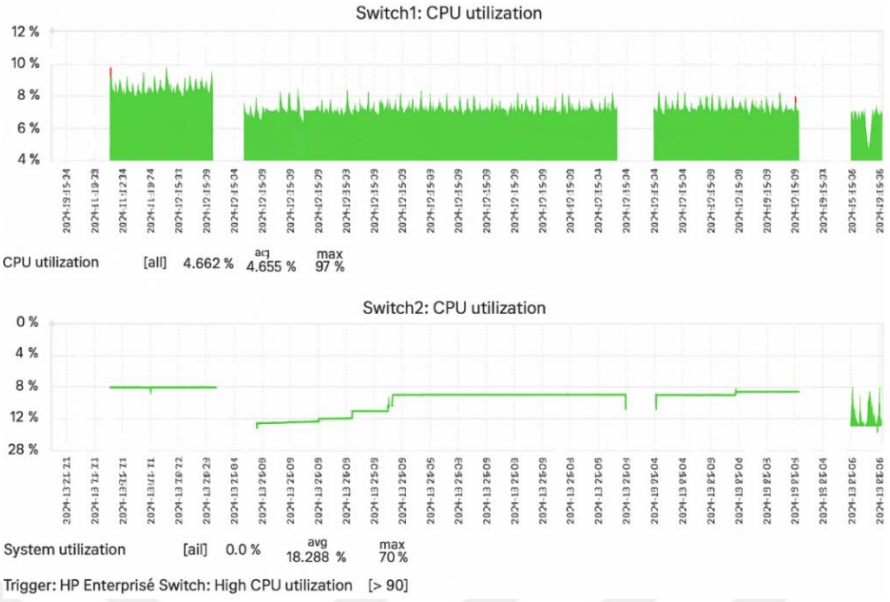
Şekil 28 de iki adet ağ anahtarının kullanılabilir bellek ve bellek kullanım oranı grafikleri görülmektedir.



Şekil 28. İki adet ağ anahtarının kullanılabilir bellek ve bellek kullanım oranı grafiklerini gösteren ekran

Şekil 29 örneğinde görüldüğü üzere ağ anahtarı 1'in işlemci kullanım oranı, genellikle %4 ile %10 arasında seyretmiş, ortalama değer %4,655, maksimum değer ise %97 olarak ölçülmüştür. Bu sonuç, bazı dönemlerde işlemci yükünün olağanüstü şekilde arttığını ve kritik seviyelere ulaştığını göstermektedir. Ağ anahtarı 2'nin işlemci kullanım değerleri incelendiğinde, genel olarak düşük seviyelerde seyretmesine rağmen ortalama %18,28 ve maksimum %70 seviyelerine ulaşmıştır. Bu durum, ağ anahtarı 2'nin zaman zaman yüksek yük altında kaldığını, fakat sürekli olarak kritik eşik değerlerini zorlamadığını ortaya koymaktadır. Elde edilen bu sonuçlar, iki cihaz arasında işlemci yük dağılımı açısından önemli farklılıklar olduğunu göstermektedir. Özellikle ağ anahtarı 1 de gözlemlenen %97'lik ani yükselme, ağ performansını olumsuz etkileyebilecek potansiyel darboğazlara işaret etmektedir. Bu nedenle, işlemci kullanım trendlerinin düzenli izlenmesi ve kritik eşik değerlerini aşan durumlarda önleyici tedbirlerin alınması gereklidir.

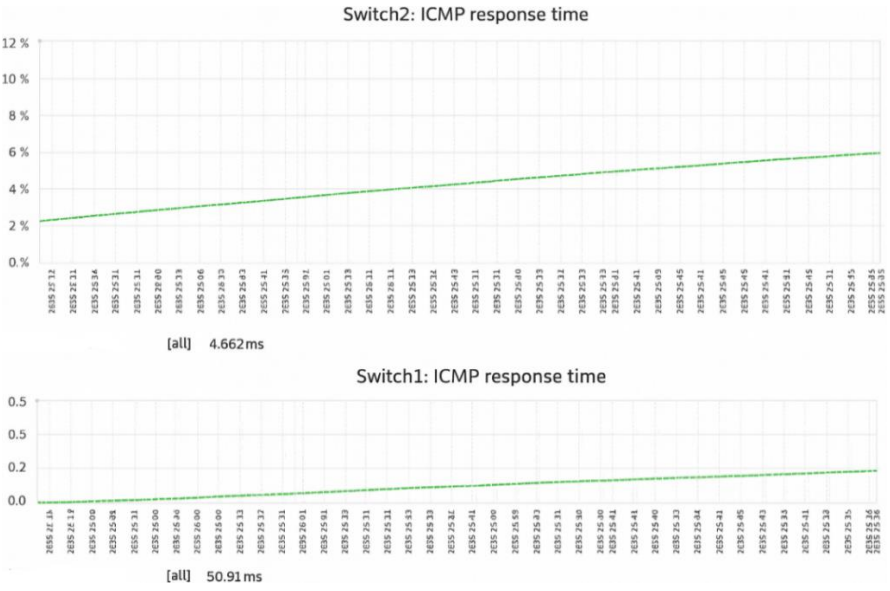
Şekil 29 da iki adet ağ anahtarının işlemci kullanım oranı grafikleri görülmektedir.



Şekil 29. İki adet ağ anahtarının işlemci kullanım oranı grafiklerini gösteren ekran

Şekil 30 örneğinde görüldüğü üzere iki ağ anahtarı cihazının ICMP yanıt süreleri karşılaştırılmaktadır. Ağ anahtarı 2'nin ICMP yanıt süresi ortalama 4,662 ms (Milisaniye) olarak ölçülmüş ve zaman içerisinde küçük dalgalanmalar göstermiştir. Bu değer, cihazın ağ üzerinde paketlere tutarlı bir şekilde yanıt verdiğini, gecikmelerin kritik seviyelere ulaşmadığını ortaya koymaktadır. Ağ anahtarı 1'in ICMP yanıt süresi ise yaklaşık 50,91 ms seviyesinde kalmış olup, ağ anahtarı 2'ye kıyasla daha yüksek bir gecikme değeri sergilemiştir. Bu durum, ağ anahtarı 1'in ağ üzerinde zaman zaman daha yavaş yanıt verdiğini göstermektedir. Genel olarak değerlendirildiğinde, ağ anahtarı 2'nin daha istikrarlı ve düşük yanıt süreleriyle ağ performansına daha olumlu katkı sağladığı, ağ anahtarı 1'in ise daha yüksek gecikme değerleri sebebiyle yoğun trafik altında performans düşüşlerine sebep olabileceği söylenebilir.

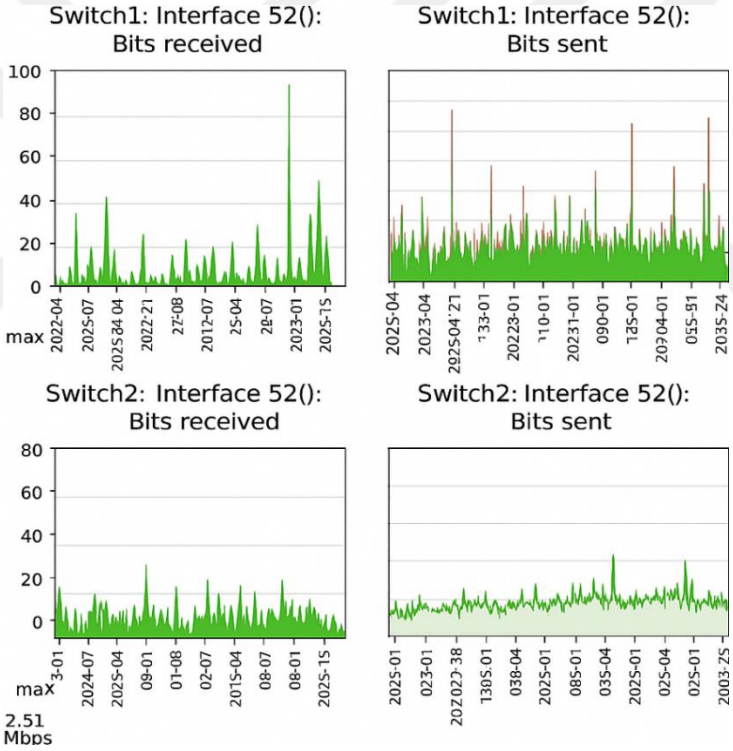
Şekil 30 da iki adet ağ anahtarının ICMP yanıt süresi grafikleri görülmektedir.



Şekil 30. İki adet ağ anahtarının ICMP yanıt süresi grafiklerini gösteren ekran

Şekil 31 örneğinden görüldüğü üzere Ağ anahtarı 1 ve Ağ anahtarı 2 cihazlarının 52. ara yüzleri üzerinden alınan ve gönderilen bit (Binary Digit) miktarları karşılaştırmalı olarak sunulmaktadır. Ağ anahtarı 1 de alınan trafik zaman zaman 100 Mbps 'ye yaklaşan ani artışlar göstermiştir. Bu durum, yoğun veri akışlarının veya ani yüklenmelerin gerçekleştiğine işaret etmektedir. Ağ anahtarı 1'den gönderilen trafik incelendiğinde, sürekli dalgalı bir yapının olduğu ve belirli dönemlerde çıkış trafiğinin yüksek zirvelere ulaştığı görülmektedir. Bu, Ağ anahtarı 1'in ağda aktif veri iletiminde daha yoğun bir rol üstlendiğini göstermektedir. Ağ anahtarı 2'de alınan trafik daha düşük seviyelerde seyretmiş olup maksimum 3 Mbps civarında kalmıştır. Bu durum, Ağ anahtarı 2'nin veri alımında daha sınırlı yük taşıdığını ortaya koymaktadır. Ağ anahtarı 2'den gönderilen trafik de benzer şekilde düşük seviyelerde kalmış, belirli noktalarda küçük artışlar gözlenmiş olsa da Ağ anahtarı 1'e kıyasla oldukça düşük değerler göstermiştir. Genel olarak değerlendirildiğinde, Ağ anahtarı 1'in ağ üzerinde çok daha yoğun bir veri trafiğini yönettiği, Ağ anahtarı 2'nin ise daha düşük kapasiteli veya yedek rol üstlenen bir cihaz olduğu söylenebilir.

Şekil 31 de iki adet ağ anahtarının fiber portları olan 52. portun gönderilen bit miktarı ve alınan bit miktarı grafikleri görülmektedir.



Şekil 31. İki adet ağ anahtarının fiber portları olan 52. portun gönderilen bit miktarı ve alınan bit miktarı grafiklerini gösteren ekran

5.5.2 İki Adet Ağ Anahtarında Bulunan Problemlerin İncelenmesi

Zabbix'in problemler sekmesi sayesinde, ağdaki portların link durumları ve bağlantı hızları gerçek zamanlı olarak izlenebilmekte, oluşan arızalar veya performans kayıpları anında kayıt altına alınabilmektedir. Bu sayede, örneğin bir portun bağlantı hızının düşmesi ya da tamamen erişilemez hâle gelmesi gibi durumlar kolayca tespit edilerek müdahale süresi kısaltılmaktadır.

Şekil 32 örneğinde görüldüğü üzere Ağ anahtarı 1 ve Ağ anahtarı 2 cihazlarında tespit edilen kritik olaylar ve hata durumları listelenmiştir. Ağ anahtarı 1 üzerinde, Ethernet ara yüzlerinin zaman zaman daha düşük hızlarda çalışmaya geçtiği ve bazı portların bağlantısının kesildiği görülmektedir. Bu olayların süreleri 19 saatten başlayarak 2 ayı aşan periyotlara kadar uzanmıştır. Ağ anahtarı 2 de**,** ara yüz 6 ve ara yüz 31 bağlantılarında kopma hataları kaydedilmiş, ayrıca ara yüz 8 ve diğer bazı portlarda hız düşüşleri yaşanmıştır. Bu durum, cihazın istikrarlı çalışma sorunları yaşadığını ve performansın doğrudan etkilendiğini göstermektedir. Bu, sorunların bazı durumlarda kritik etki yaratmasa da uzun süreli devam ettiğini ve izleme açısından dikkate alınması gerektiğini ortaya koymaktadır**.** Süre sütununda görüldüğü üzere, Ağ anahtarı 2 de yaşanan bazı bağlantı sorunlarının 28 gün boyunca devam ettiği**,** Ağ anahtarı 1 de ise belirli ara yüzlerde düşük hız problemlerinin iki aydan uzun süre gözlemlendiği anlaşılmaktadır. Bu tür olayların düzenli olarak analiz edilmesi, hem önleyici bakım planlarının hem de altyapı optimizasyonunun yapılabilmesi için kritik öneme sahiptir.

Şekil 32 de ağ anahtarlarının problemleri görülmektedir.

Recovery time	Status	Info	Host	Problem	Duration
Infornation	PROBLEM		Switch 1	HP Enterprise Switch. Interface 7), Ethernet has changed to low speed than It " was before	19 hm
Average	PROBLEM	Switch 1 1			3d 13m
Information	PROBLEM	Switch 1 2		HP Enterprise Switch Link down	28d 13m
Average	PROBLEM	Switch 2 2		Σ Interface 8 has changed to lower speed than it was	28d 13m
Information	PROBLEM	Switch 1 1		Σ Interface 4 (): Link down	28d13m
Information	PROBLEM	Switch 2 2		Interface 6 (): L.ink down	24d 12m
Information	PROBLEM	Switch 2 2		Interface changded to lower speed than	24d 12 h
Information	PROBLEM	Switch 2 1		Interface 31 Link down	24d 12m
Information	PROBLEM	Switch 1 1		Interface 38 lover speed than	2M 2d d

Şekil 32. Ağ anahtarlarının problemlerini gösteren ekran

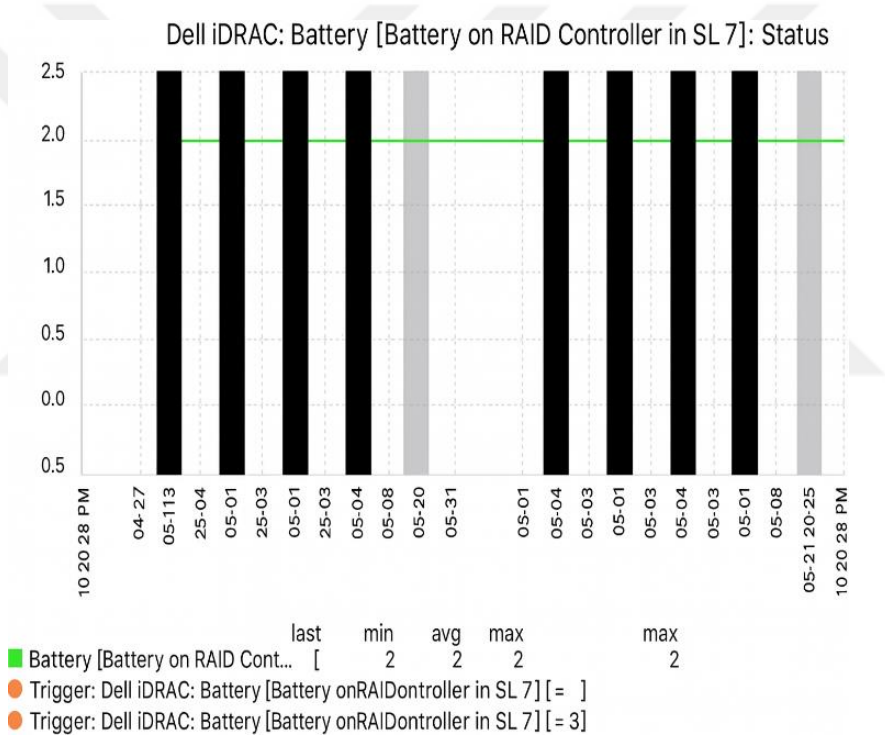
5.6 Dell IDRAC Sunucunun İzlenmesi

Burada şablon olarak Zabbix'in içerisinde Dell IDRAC sunucu şablonu olmadığından üreticinin yayınlaması ile şablon üreticinin sitesinden xml formatında alınarak aşağıda görülen kısımda Zabbix içine aktarılmıştır. (şablonlar kısmından) Daha sonrasında şablon Dell IDRAC sunucuya atanmıştır.

5.6.1 Dell IDRAC Sunucunun Veri Öğelerinin İncelenmesi

Şekil 33 örneğinde görüldüğü üzere batarya değeri sürekli olarak 2 seviyesinde sabit kalmış, minimum, maksimum ve ortalama değerlerin tamamı aynı değeri göstermiştir. Bu durum, sistemde herhangi bir dalgalanma ve ya kritik batarya arızası olmadığını ortaya koymaktadır. Siyah sütunlarla gösterilen periyotlar, sistemin bataryayı tanıdığını ve sürekli aynı durumda çalıştığını ifade etmektedir. Ayrıca grafikte tanımlı tetikleyiciler yardımıyla, batarya durumunun 2 değerinden farklı bir aralıkta olması halinde kritik uyarı üretileceği anlaşılmaktadır. Sonuç olarak, RAID (Redundant Array of Independent Disks) denetleyici bataryasının sağlıklı olduğu, herhangi bir anormallik gözlenmediği ve Zabbix tarafından sürekli kontrol altında tutulduğu görülmektedir. Bu tür kritik bileşenlerin izlenmesi, veri bütünlüğünün korunması ve olası disk hatalarında güvenli çalışmanın sürdürülebilmesi için önem arz etmektedir.

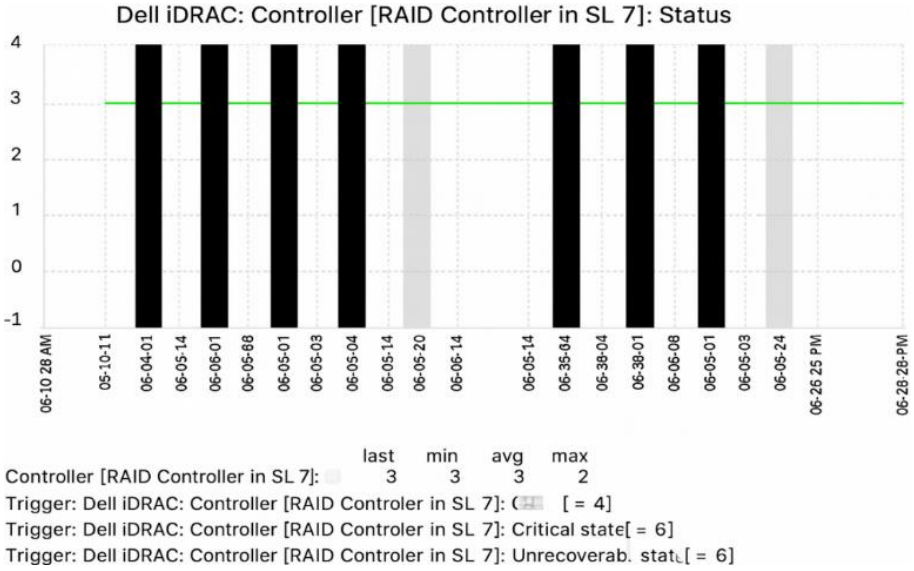
Şekil 33'te sunucunun RAID kontrol kartının üzerinde yer alan bataryanın durumu görülmektedir.



Şekil 33. Sunucunun RAID kontrol kartının üzerinde yer alan bataryanın durumunu gösteren ekran

Şekil 34 örneğinde görüldüğü üzere, değerler incelendiğinde kontrolör durumunun 3 seviyesinde sabit kaldığı, minimum, maksimum ve ortalama değerlerin de aynı sonucu verdiği görülmektedir. Bu sabit değer, kontrolörün normal çalışma modunda olduğunu göstermektedir. Zabbix üzerinde tanımlı tetikleyicilere göre, değer 4 olduğunda "uyarı", 6 olduğunda ise "kritik" durumu oluşacaktır. Bu sayede RAID kontrol kartında meydana gelebilecek anlık ve ya kalıcı hataların erken tespiti mümkün olmaktadır. Sonuç olarak, RAID kontrol kartının kararlı şekilde çalıştığı ve herhangi bir kritik durum rapor edilmediği anlaşılmaktadır.

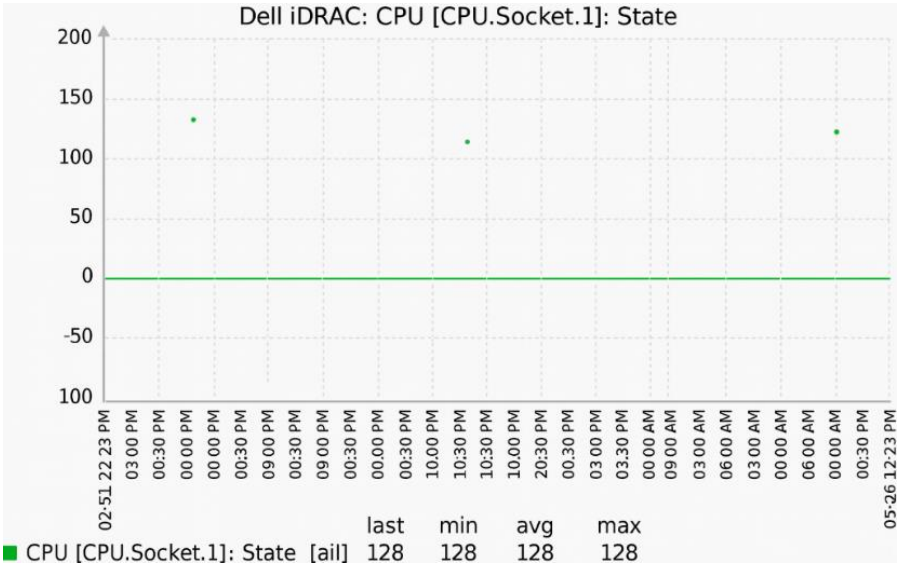
Şekil 34'te sunucunun RAID kontrol kartının çalışma durumu görülmektedir



Şekil 34. Sunucunun RAID kontrol kartının çalışma durumunu gösteren ekran

Şekil 35 örneğinde görüldüğü üzere işlemci değerleri sürekli olarak 128 seviyesinde sabit kalmış, minimum, maksimum ve ortalama değerler de aynı sonucu vermiştir. Bu durum, işlemcinin kararlı bir şekilde çalıştığını ve izleme süresi boyunca herhangi bir hata, aşırı yük ve ya anomali oluşmadığını göstermektedir. Değerin sabit kalması, işlemcinin donanım izleme açısından normal durumunu ifade etmektedir. Zabbix üzerindeki tetikleyiciler sayesinde farklı bir değer tespit edilmesi halinde sistem yöneticilerine uyarı üretilecek ve olası arızalara hızlı müdahale edilebilecektir. Sonuç olarak, grafik işlemci bileşeninin istikrarlı bir performans sergilediğini ortaya koymakta, izleme sisteminin sunucu donanım güvenilirliğini sağlama noktasında önemli katkılar sunduğunu göstermektedir.

Şekil 35'te sunucunun birinci soketi üzerindeki işlemcinin durumu görülmektedir.

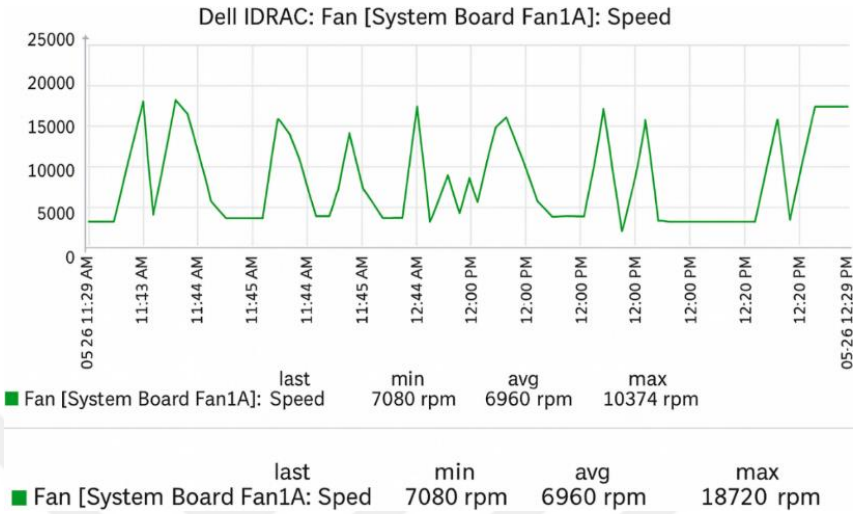


Şekil 35. Sunucunun birinci soketi üzerindeki işlemcinin durumunu gösteren ekran

Şekil 36 örneğinde görüldüğü üzere ölçüm süresince fan hızında dalgalanmalar gözlenmiş olup, en düşük değer 7080 rpm, en yüksek değer 18720-rpm olarak kaydedilmiştir. Grafikte görülen ani yükselişler, sistem sıcaklığındaki artışlara bağlı olarak fanın hızını artırmasıyla

açıklanabilir. Bu durum, sunucunun soğutma mekanizmasının doğru şekilde çalıştığını ve kritik sıcaklık eşiklerini korumak için dinamik tepkiler verdiğini göstermektedir. Sonuç olarak, fanın düzenli ve adaptif bir çalışma sergilediği; Zabbix üzerinden yapılan bu izleme sayesinde donanımın ısınmaya karşı korunduğu ve sistem güvenilirliğnin artırıldığı söylenebilir.

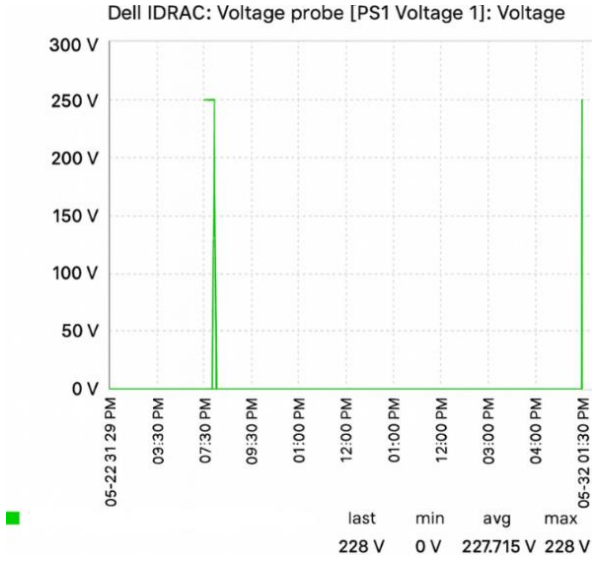
Şekil 36 da sunucunun ana kartı üzerinde yer alan birinci fanın dönüş hızı görülmektedir.



Şekil 36. Sunucunun ana kartı üzerinde yer alan birinci fanın dönüş hızını gösteren ekran

Şekil 37 örneğinde görüldüğü üzere ölçüm süresinde minimum değer 0 V, maksimum değer 228 V olarak kaydedilmiş, ortalama değer ise 227.715 V olarak gerçekleşmiştir. Son ölçümde voltaj seviyesi 228 V'tur. Grafikte görülen sıfır voltaj anları, ölçüm boşlukları ya da güç kaynağının geçici olarak devre dışı kalmasıyla açıklanabilir. Ancak ortalama değerin sürekli olarak 220–230 V aralığında seyretmesi, güç kaynağının genel olarak stabil çalıştığını göstermektedir. Bu tür bir izleme sayesinde, güç kaynaklarında oluşabilecek ani voltaj düşüşleri ve ya dalgalanmaları önceden tespit etmek mümkün olmaktadır. Böylelikle hem donanımın güvenliği korunmakta hem de kritik sistem kesintilerinin önüne geçilmektedir.

Şekil 37 de sunucunun güç kaynağı modülüne ait voltaj sensörü görülmektedir.



Şekil 37. Sunucunun güç kaynağı modülüne ait voltaj sensörünü gösteren ekran

5.6.2 Dell IDRAC Sunucunun Tetikleyicilerinin İncelenmesi

Şekil 38 örneğinde görüldüğü üzere Dell sunucuya ait batarya, RAID ve fan bileşenlerin durumu Zabbix üzerinden raporlanmaktadır. Görüldüğü üzere tüm bileşenler "OK" durumunda olsa da, sistem farklı uyarı seviyeleri ile kritik bileşenlerin anlık kontrollerini vurgulamaktadır. Özellikle Battery FAN 1 bileşeni RAID bağımlılığı altında izlenmiş ve kritik senaryolarda bile "OK" olarak değerlendirilmiştir. Sistemde "Current state" sütununa göre bataryaların ve diğer bileşenlerin stabil olduğu, kritik hata ve ya çalışmayı engelleyici bir durum bulunmadığı tespit edilmektedir. Bununla birlikte, uyarı mekanizmasının aktif çalıştığını ve olası bir arıza ve ya kapasite düşüşünde anında müdahale edilebilecek şekilde yapılandırıldığını göstermektedir. Şekil 38 de sunucunun tetikleyicileri görülmektedir.

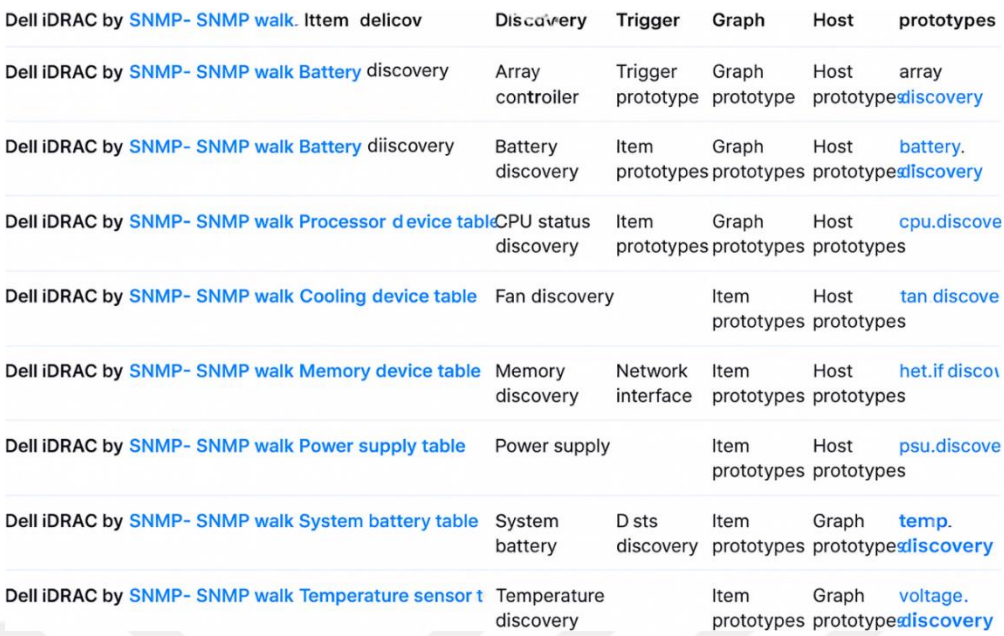
A	OK Average	OK Batterie Dependeni Battery FAN1,1 Critical state 01) C] Crittal state	Current state 0	last get ERDAOK server ina batterystatue]bylowa]>= \o
ⓘ	OK Information	OK Battrrie Dependent Battery FAN1, Critical state 0 Deponds on RAID Critical state BatteryidS in in RAID Critical state 14 RAID 0 Baid volumet in RAID Diak in RAID 0	Current state 0	last get ERDAOK server loa batterystatusbylowa]>=1) \o
ⓘ	Waming OK	OK Balance Dep, one Battery FAN1, Critical state 01) 01 OJNL)	Current state 0	last get ERDAOK server loa batterystatus] o
ⓘ	Average OK	OK Batterie Dependent Battery FAN1, Critical state 01)	Current state 0	last get ERDAOK server loa batterystatus] o
ⓘ	Average OK	OK Batterie Dependent Battery FAN1, Critical state 01) O,1	Current state 0	last get ERDAOK all server, setlFansystemBoard[Fansl 01. OsUM(10)
ⓘ	Average OK	OK Batterie Del OKAC by get (Current state BLANK D11TEM LASTVALUE J	Current state 1	last get ERDAOK all server, set]FanSystemBoard[Fansl [01]] Critical state qi N(?>, = 1) SUM,
ⓘ	Waming OK	OK DRAC by get (Recovery state(md01) RAID 0 RAID VolumeO, Critical states0 OSUM LTAVTO-Coqd	Current state 1	last get ERDAOK all server, set]FanSystemBoard[Fans [01]] NonCritical state<2,0] -0
	Warning OK	OK DRAC ok ḫet Recovery state(mdrcod1)	Current state 1	last get ERDAOK carm all

Şekil 38. Sunucunun tetikleyicilerini gösteren ekran

5.6.3 Dell IDRAC Sunucunun Keşif Kurallarının İncelenmesi

Şekil 39 örneğinde görüldüğü üzere Zabbix'in Dell IDRAC SNMP şablonunda tanımlı otomatik keşif kuralları, sunucu donanımının otomatik olarak tespit edilmesini ve izleme sistemine entegre edilmesini sağlar. RAID denetleyicileri, disk sürücüleri, işlemci, bellek, fanlar, batarya ve güç kaynakları gibi kritik bileşenler belirli aralıklarla keşfedilmekte; bu bileşenlere ilişkin veri toplama, grafik oluşturma ve alarm üretimi ise tanımlı veri öğesi, grafik ve tetikleyici prototipleri aracılığıyla gerçekleştirilmektedir.

Şekil 39 da sunucunun keşif kuralları görülmektedir.



Şekil 39. Sunucunun keşif kurallarını gösteren ekran

Tablo 5. Deney ortamında izlenen cihazların özellikleri

Cihaz Türü	Üretici / Model	Kullanılan Protokol	İzlenen Metrikler
PLC	Siemens SIMATIC S7-1500, IM153-4PN	SNMP	CPU yükü, bağlantı sayısı, giriş-çıkış modül durumu
Ağ Anahtarı	Aruba 2930F, HP 5406Rzl2	SNMP	Port trafiği, VLAN istatistikleri, hata paketleri
Omurga Ağ Anahtarı	HP J9850A	SNMP	Hata paketleri, CPU, bellek, WAN trafiği
Sunucu	Dell IDRAC	SNMP	CPU, RAM, disk durumu, fan hızı, sıcaklık

Bu çalışmada izleme yapılan cihazlar, kurumun hem bilgi teknolojileri altyapısında hem de operasyonel teknoloji katmanında kritik rol oynayan bileşenler arasından seçilmiştir. Siemens Simatic S7 PLC ve IM153-4PN modül, üretim süreçlerinde kesintisiz çalışması gereken endüstriyel IoT cihazları oldukları için tercih edilmiştir. Omurga ve kenar ağ anahtarları ise tüm ağ trafiğini yönlendiren, performans ve süreklilik açısından merkezi öneme sahip cihazlardır. Dell IDRAC sunucu, donanım sağlığı ve hizmet sürekliliği bakımından kritik olduğundan izleme kapsamına alınmıştır. Bu seçimler sayesinde, hem bilgi teknolojileri hem de operasyonel teknoloji altyapısı bütünsel olarak denetim altına alınmış ve Zabbix üzerinde farklı cihaz tiplerinde sağladığı faydalar ortaya konulmuştur. Elde edilen sonuçlar, pratik bakım, erken uyarı mekanizmaları ve karar destek süreçlerinde kayda değer iyileşmeler sağlandığını göstermektedir. Ayrıca tez kapsamında 5.2 ile 5.6 başlık numaralı bölümler arasında yer alan görsellerin Zabbix ara yüzünden ve bir sonraki bölümler olan 6.1 ile 6.6 numaralı başlıklar arasında yer alan görsellerin ise Grafana ara yüzünden elde edildiğini belirtmek gerekir. Böylelikle iki sistemin görselleştirme yetenekleri arasındaki farklılıkların doğrudan karşılaştırmalı olarak ortaya konulması amaçlanmıştır.

Tüm bu uygulama süreci sonucunda elde edilen teknik kazanımlar şunlardır:

1. Ağ altyapısında bulunan tüm aktif cihazların erişilebilirlik durumu %100 düzeyinde raporlanmış; herhangi bir erişim sorunu anlık uyarılarla tespit edilmiştir.

2. Omurga ağ anahtarı ve kenar ağ anahtarlarında port trafik analizleri yapılmış; aşırı yüklenme yaşanmadan önce uyarı sistemleri devreye alınmıştır.

3. Aktif çalışma süresini izleme sayesinde sunucuların veya ağ cihazlarının planlı/plansız yeniden başlatmaları tarih ve süre bazında kaydedilmiştir.

4. İşlemci sıcaklıkları, bellek yükü ve sistem kaynak kullanımı eşiklere yaklaşmadan önce tespit edilerek önleyici müdahale imkânı sağlanmıştır.

5. Siemens PLC cihazlarında süreç verilerinin SNMPv1 ile alınması ve bu verilerin anlık grafiğe dökülmesi, üretim operasyonlarının BT altyapısıyla bütünleşmiş izlenmesini mümkün kılmıştır.

Bu uygulama, Zabbix'in hem kurumsal BT altyapılarında hem de endüstriyel sistemlerde genişletilebilir ve özelleştirilebilir izleme olanakları sunduğunu göstermiştir. Elde edilen bu bulgular, farklı üretici ve protokollere sahip cihazların tek bir merkezi platform üzerinden bütünleşik olarak izlenebileceğini ortaya koymuştur. Ayrıca otomatik keşif ve tetikleyici mekanizmaları sayesinde insan hataları minimize edilerek izleme süreçlerinin güvenilirliği artırılmıştır. Zabbix'in esnek mimarisi hem BT altyapısında hem de endüstriyel ortamlarda operasyonel verimliliğe doğrudan katkı sağlamıştır.

6. Zabbix Ağ Altyapısı Ve Sunucu Verilerinin Grafana ile Görselleştirilmesi

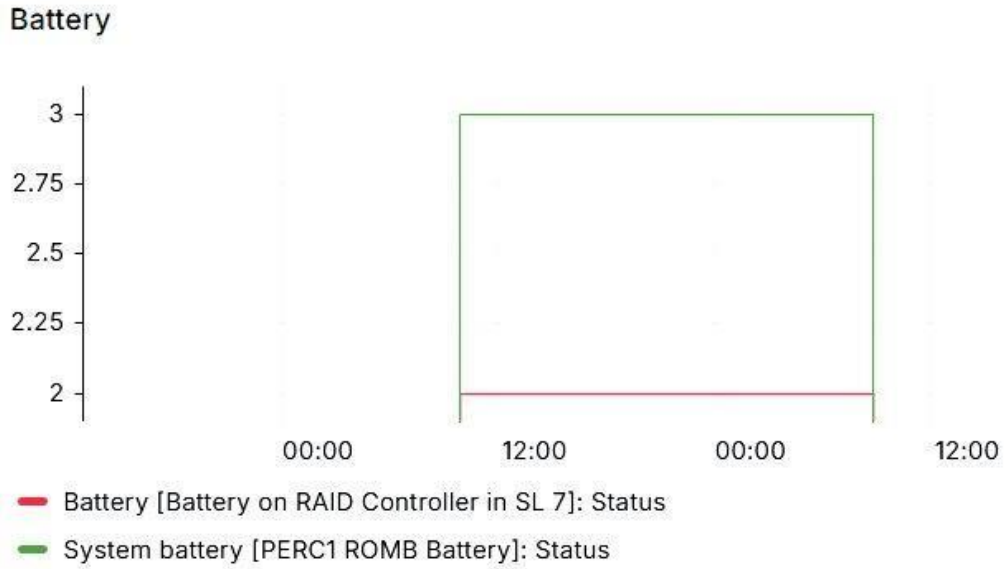
Zabbix, temel düzeyde ağ cihazlarının, sunucuların ve servislerin izlenmesine olanak tanısa da, bazı özel altyapı yapılarını görselleştirme veya mantıksal bütünlük içinde sunma konusunda sınırlılıklara sahiptir. Özellikle birden fazla cihazdan toplanan verilerin ilişkilendirilmesi, zaman bazlı karşılaştırmaların yapılması ve farklı kategorilere ait metriklerin aynı panelde birleştirilmesi, Zabbix'in yerleşik şablon bileşenleriyle sınırlı veya imkânsızdır.

Bu kapsamda, Zabbix ara yüzünde doğrudan tanımlanamayan ancak Grafana ile başarıyla görselleştirilen altyapı yapılarına aşağıdaki örnekler verilebilir:

6.1 Dell IDRAC Sunucunun Arızalı Batarya Durumu

Zabbix ve Grafana uyumu sonucu Dell IDRAC sunucunun Şekil 40 örneğinde görüldüğü üzere batarya hatasına düştüğü tespit edilmiştir. Bu grafik sunucuda RAID kartı bataryalarının artık görevini yapamadığını net biçimde gösteriyor. Kesintisiz güç kaynakları olsa bile RAID kartının önbellek güvenliği yok. Mutlaka batarya değişimi yapılmalıdır. Batarya değişimi yapılmış ve Şekil 33 örneğinden görüldüğü üzere batarya değeri sağlıklı durumuna gelmiştir.

Şekil 40 da Grafana da Dell IDRAC sunucunun arızalı batarya durumu verilmiştir.



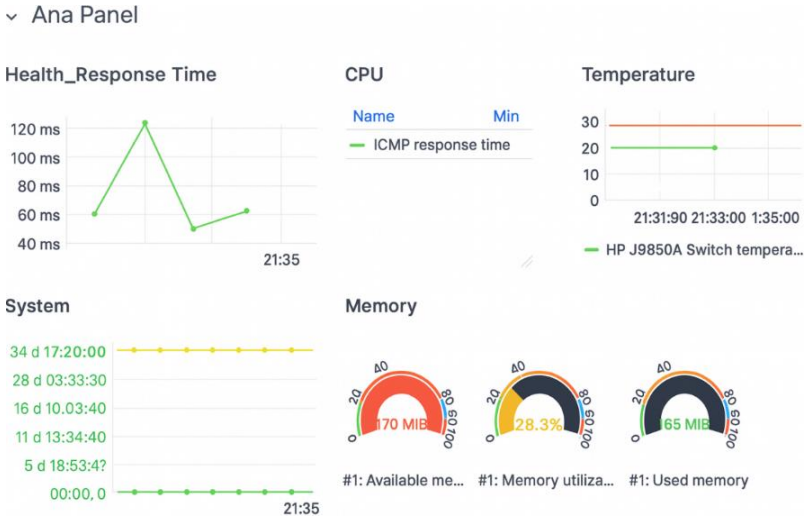
Şekil 40. Grafana da Dell IDRAC sunucunun arızalı batarya durumunu gösteren ekran

6.2 Omurga Ağ Anahtarı Trafik Yükü Dağılımı

Zabbix ara yüzünde her port için ayrı grafik alınabilirken, tüm portların trafiğini tek bir panelde kıyaslamak mümkün değildir. Grafana'da gelen ve giden bit miktarı, gelen hatalı paketler, atılan paketler gibi metrikler aynı panelde çakıştırma yöntemiyle gösterilerek portlar arası anlık trafik farkları görsel olarak analiz edilmiştir.

Şekil 40 örneğinde görüldüğü üzere Zabbix ana paneli üzerinde sistemin genel sağlık durumu, işlemci yanıt süreleri, sıcaklık değerleri ve bellek kullanım oranları görselleştirilmiştir. Sağlıklı yanıt süresi grafiğinde ICMP tabanlı yanıt sürelerinin 40–120 ms aralığında değiştiği görülmektedir. Bu değerler ağ erişilebilirliğinin stabil olduğunu, ancak zaman zaman kısa süreli gecikmeler yaşandığını göstermektedir. İşlemci bölümü altında ICMP yanıt süreleri sistem performansına işaret ederken, sıcaklık grafiğinde ağ anahtarının sıcaklık değeri yaklaşık 20 °C seviyesinde sabit kalmıştır. Bu durum donanım soğutma mekanizmalarının etkin çalıştığını ortaya koymaktadır. Sistem bölümü incelendiğinde farklı cihazların çalışma süreleri gün ve saat cinsinden gösterilmekte, en uzun sürenin 34 gün, en kısa sürenin ise 5 gün olduğu izlenmektedir. Bu bilgi, sistem sürekliliği açısından önemli bir gösterge sunmaktadır. Bellek bölümünde ise toplam bellekten 170 mb kullanılabilir, 65 mb kullanılmış ve bellek kullanım oranı %28,3 olarak görülmektedir. Düşük bellek kullanım oranı, sistemde kapasite planlaması açısından yeterli kaynak bulunduğunu göstermektedir.

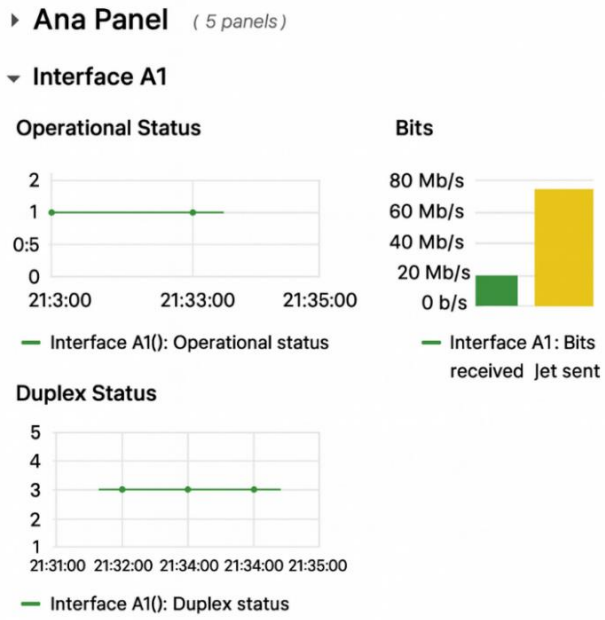
Şekil 41 de Grafana da gösterge paneli içinde oluşturulan ana panel satırı içindeki grafikler görülmektedir.



Şekil 41. Grafana da gösterge paneli içinde oluşturulan ana panel içindeki omurga ağ anahtarı grafiklerini gösteren ekran

Şekil 42 örneğinde görüldüğü üzere, çalışma durumu grafiğinde A1 ara yüzün aktif olduğu ve kesinti yaşanmadığı görülmektedir. Çift yönlü iletişim durumu grafiği ise portun tam çift yönlü iletişim modda çalıştığını göstermekte, bu durum veri gönderim ve alımında çakışma riskini ortadan kaldırarak performansı artırmaktadır. Alınan ve gönderilen veri grafiği incelendiğinde, port üzerinden alınan veri miktarı yaklaşık 20 Mb/s, gönderilen veri miktarı ise 80 Mb/s olarak kaydedilmiştir. Bu dengesizlik, ara yüzün daha çok veri iletimi için kullanıldığını ve cihazın ağ trafiğinde çıkış yönlü yükün baskın olduğunu göstermektedir. Sonuç olarak, A1 ara yüzünün kesintisiz ve tam çift yönlü modda çalıştığı, yüksek oranda veri iletimi gerçekleştirdiği ve ağ performansı açısından kritik bir işlev gördüğü anlaşılmaktadır.

Şekil 42 de Grafana'da gösterge paneli içinde oluşturulan A1 ara yüzü satırı içindeki grafikler görülmektedir.

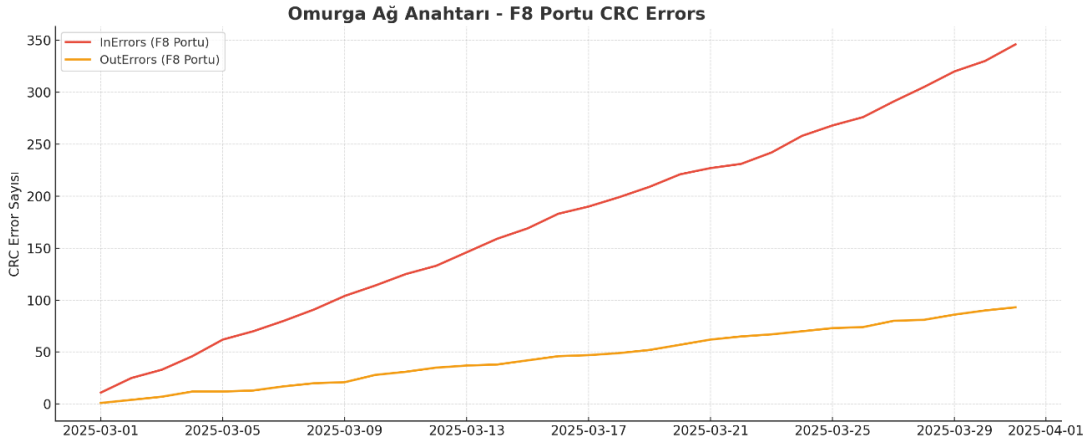


Şekil 42. Grafana' da gösterge paneli içinde oluşturulan A1 ara yüzü içindeki omurga ağ anahtarı grafiklerini gösteren ekran

6.3 Omurga Ağ Anahtarı CRC Hataları

Omurga ağ anahtarı F8 ara yüzünde, Şekil 43 örneğinde görüldüğü üzere CRC hataları tespit edilmiştir. Yapılan incelemelerde, F8 ara yüzünde sonlanan fiber bağlantının uygulama kapsamında belirlenmeyen bir ağ anahtarına yönlendiği anlaşılmıştır. Sorunun kaynağının fiber kablodan olduğu belirlenmiş ve ilgili fiber kablonun değiştirilmesiyle CRC hataları giderilerek bağlantı sağlıklı hale getirilmiştir.

Şekil 43 te Grafana da Omurga Ağ Anahtarı F8 ara yüzünün CRC hatalarının Mart 2025 ayına ait grafiksel durumu verilmiştir.



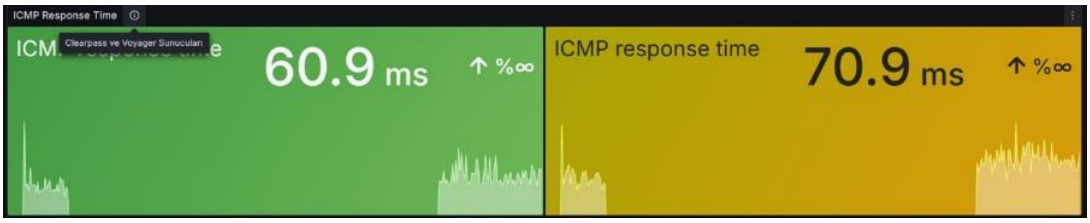
Şekil 43. Grafana da omurga ağ anahtarı F8 ara yüzünün mart ayı CRC hatalarını gösteren ekran

6.4 Sunucular Arası İşlemci/Bellek Karşılaştırma Paneli

Zabbix'te birden fazla ağ varlığının aynı grafikte karşılaştırılması karmaşık ve sınırlıdır. Grafana'da tüm sunucuların işlemci kullanım oranını gösteren ve bellek kullanım oranını gösteren değerleri tek bir multi-stat panelde gösterilmiş, en yüksek kullanımı olan sunucular anında fark edilmiştir.

Şekil 44 örneğinde görüldüğü üzere, iki farklı sunucuya yönelik ICMP yanıt süreleri izlenmektedir. Sol taraftaki ölçümde yanıt süresi 60,9 ms, sağ tarafta ise 70,9 ms olarak kaydedilmiştir. Bu değerler, ağ gecikmesinin düşük seviyelerde tutulduğunu ancak iki sunucu arasında performans farklılıklarının bulunduğunu göstermektedir. Yanıt sürelerindeki artışlar, ağ yoğunluğu, cihaz performansı ve ya yönlendirme gecikmeleri gibi faktörlerden kaynaklanabilmektedir. Grafikte görülen küçük dalgalanmalar, zaman içinde trafik yüküne bağlı olarak anlık gecikme artışlarını işaret etmektedir. Bu tür ICMP yanıt sürelerinin düzenli olarak izlenmesi, ağ performansındaki ani değişimlerin tespit edilmesine ve olası bağlantı sorunlarının önceden öngörülmesine katkı sağlamaktadır.

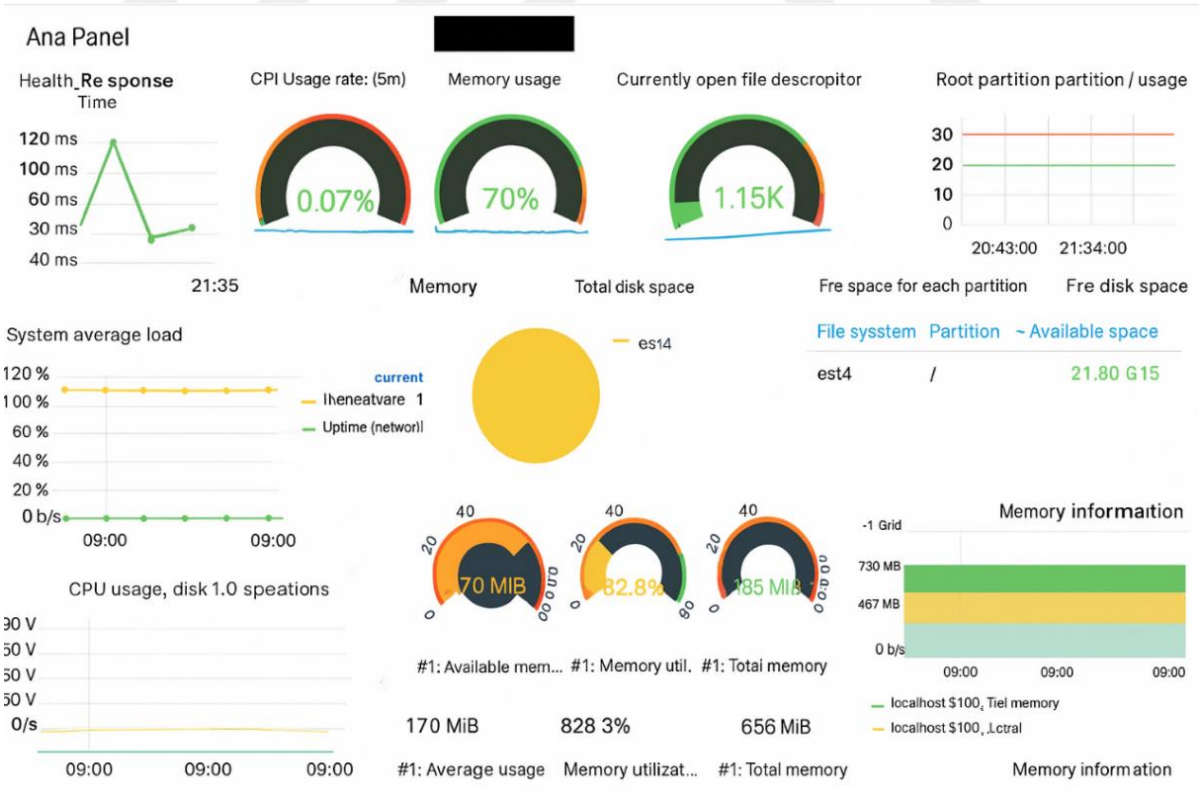
Şekil 44 te Grafana' da gösterge paneli içinde iki sunucunun yanıt verme süreleri karşılaştırılmıştır.



Şekil 44. Grafana'da gösterge paneli içinde iki sunucunun yanıt verme sürelerini karşılaştıran ekran

Şekil 45 örneğinde görüldüğü üzere, izlenen sunucuya ait kaynak kullanımı ve performans göstergeleri bütünsel olarak sunulmaktadır. Grafiklerde; işlemci kullanım oranı, bellek kullanımı, dosya tanıtıcı sayısı, disk alanı kullanımı ve sistem yanıt süreleri ayrı ayrı izlenmektedir. İşlemci kullanım oranının %0,07 gibi oldukça düşük seviyede olduğu görülmekte, bu durum sistemin işlem yükünün hafif olduğunu göstermektedir. Bellek kullanımının %70 seviyesinde olması, sistemin bellek kaynaklarını yoğun biçimde kullandığını ortaya koymaktadır. Açık dosya tanıtıcı sayısının 1150 civarında olması, aktif süreçlerin yoğunluğunu yansıtmaktadır. Disk kullanımında dosya sistemi üzerinde yaklaşık 21,8 GB boş alan bulunduğu gözlenmiştir. Ayrıca bellek istatistiklerinde toplam 656 MB belleğin %82,8'lik kısmının kullanımda olduğu tespit edilmiştir. ICMP yanıt süreleri ise 40–120 ms aralığında değişkenlik göstermiştir, bu da ağ erişiminde zaman zaman artan gecikmelere işaret etmektedir. Bu panelin düzenli olarak izlenmesi, sunucu kaynaklarının dengeli kullanımını sağlamanın yanı sıra olası bellek darboğazları, disk dolulukları ve ya ağ gecikmelerinin erken tespit edilmesine yardımcı olmaktadır.

Şekil 45 te Grafana da gösterge paneli içinde sunucular karşılaştırılmıştır.



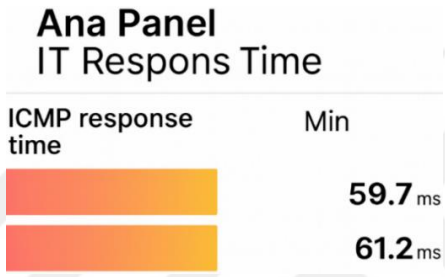
Şekil 45. Grafana' da gösterge paneli içinde sunucuları karşılaştıran ekran

6.5 PLC-Modül Grafana Görselleştirilmesi

Zabbix, PLC veri bloklarını izleyebilir ancak bu verileri anlık sinyal formunda grafikleştirmek zordur. Grafana da PLC ve modülün bağlantı sürelerinin durumu grafiksel olarak izlenmiştir.

Şekil 46 örneğinde görüldüğü üzere ICMP yanıt süresi, sunuculara gönderilen ping paketlerinin geri dönüş süresini temsil etmekte olup, ağ gecikmesi hakkında doğrudan bilgi vermektedir. Ölçümler sonucunda ortalama yanıt sürelerinin 59,7 ms ile 61,2 ms aralığında olduğu görülmektedir. Bu değerler, ağ alt yapısında belirgin bir gecikme yaşanmadığını, iletişim sürelerinin kabul edilebilir seviyede olduğunu göstermektedir. Ancak sürelerin 50 ms üzeri olması, özellikle yoğun trafik altında ağın yanıt hızının daha da optimize edilmesi gerekebileceğine işaret etmektedir.

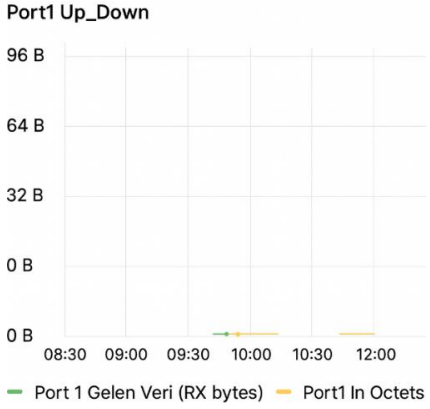
Şekil 46 da Grafana' da gösterge paneli içinde bir PLC'nin ve modülün yanıt verme süreleri karşılaştırılmıştır.



Şekil 46. Grafana da gösterge paneli içinde iki IoT cihazının yanıt verme sürelerini karşılaştıran ekran

Şekil 47 örneğinde görüldüğü üzere, 1. ara yüz üzerinden gerçekleşen veri akışı incelenmektedir. Ölçümlerde hem gelen veri miktarı hem de içeriye alınan oktetler ayrı ayrı gösterilmiştir. Sonuçlara göre port üzerinden geçen veri miktarı oldukça düşük seviyelerde kalmıştır. Grafik üzerinde yalnızca kısa süreli ve küçük ölçekli veri hareketlilikleri görülmektedir. Bu durum, 1.ara yüzün test sürecinde düşük trafikli ve ya pasif bir bağlantı için kullanıldığını göstermektedir. Veri akışının bu kadar sınırlı olması, ara yüzün kritik bir servis ve ya yoğun ağ trafiği için kullanılmadığını işaret etmektedir. Ancak uzun vadeli izlemelerde benzer şekilde düşük veri oranları gözlenirse, ara yüzün kullanılabilirliği ve ağ üzerindeki rolü yeniden değerlendirilebilir.

Şekil 47 de port 1'in hem PLC hemde modül için aktif-pasif durumu görülmektedir.

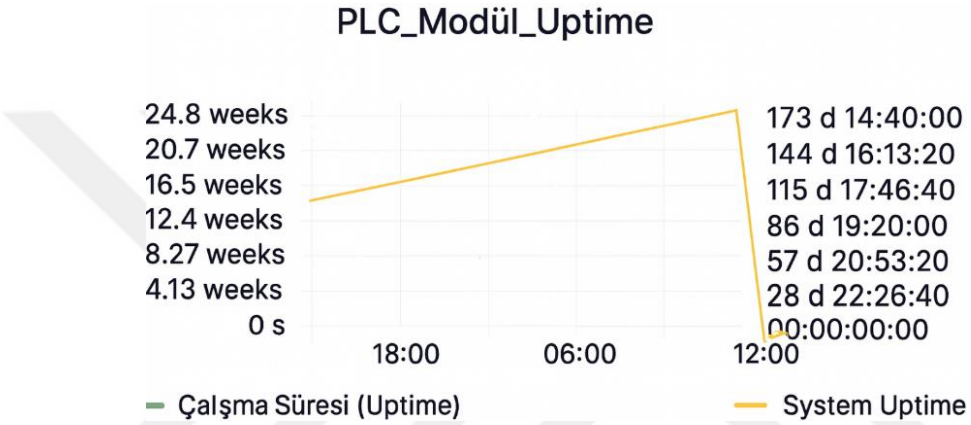


Şekil 47. Port 1'in hem PLC hemde modül için aktif-pasif durumunu gösteren ekran

Şekil 48 örneğinde görüldüğü üzere, PLC modülünün sistem çalışma süresi gün ve hafta cinsinden izlenmektedir. Veriler, modülün uzun süreli kesintisiz çalışabildiğini ve bu süreçte herhangi bir kritik hata ve ya yeniden başlatma gereksinimi olmadığını göstermektedir.

173 günün üzerinde kaydedilen çalışma süresi, sistemin kararlı, güvenilir ve sürekli hizmet verebilir yapıda olduğunu ortaya koymaktadır. Bu süre aynı zamanda, endüstriyel ortamlarda kullanılan PLC cihazlarının ne derece yüksek dayanıklılık ve kesintisiz çalışma kabiliyeti sunduğunu da göstermektedir. Ancak grafik üzerinde periyodik sıfırlamalar ve ya ani düşüşler gözlenirse, bu durum donanım güncellemeleri, yazılım yüklemeleri ve ya olası kesintilerle ilişkilendirilebilir. Bu nedenle çalışma süresi değerleri, sistemin genel güvenilirliğinin ve bakım ihtiyaçlarının değerlendirilmesi için önemli bir gösterge niteliği taşımaktadır.

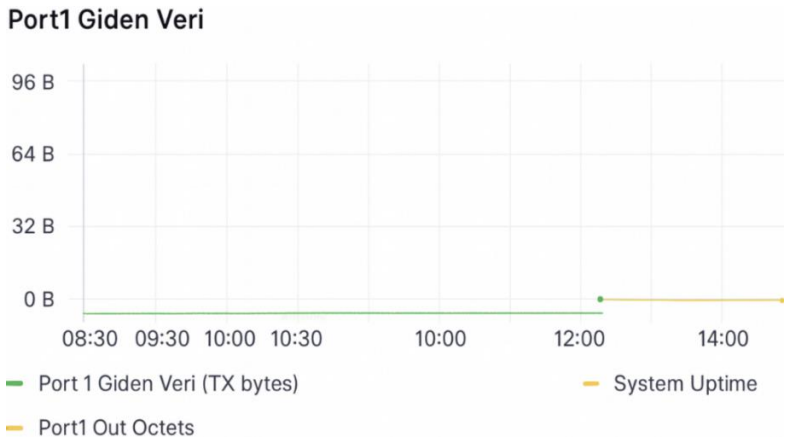
Şekil 48 de PLC ve modül için çalışma sürelerini gösteren grafik verilmiştir.



Şekil 48. PLC ve modül için çalışma sürelerini gösteren grafik ekranı

Şekil 49 örneğinde görüldüğü üzere PLC ve modül için Port1'den giden verilerin zaman içindeki değişim grafiği sunulmaktadır. Görüldüğü üzere veri çıkış miktarının oldukça düşük seviyelerde kaldığı ve belirli saat aralıklarında neredeyse sıfıra yakın değerlere ulaştığı gözlemlenmektedir. Bu durum, sistemin genel ağ trafiği üzerinde düşük bir yük oluşturduğunu ve kaynak kullanımının verimli olduğunu göstermektedir. Ayrıca bu tür ölçümler, ağ cihazlarının performansını izleyerek olası darboğazların önceden tespit edilmesine katkı sağlamaktadır.

Şekil 49 da PLC ve modül için port1'den giden veri gösterilmiştir.



Şekil 49. PLC ve modül için port1'den giden veriyi gösteren ekran

Tablo 6. Zabbix ve Grafana birlikteliğinin sağladığı katkılar

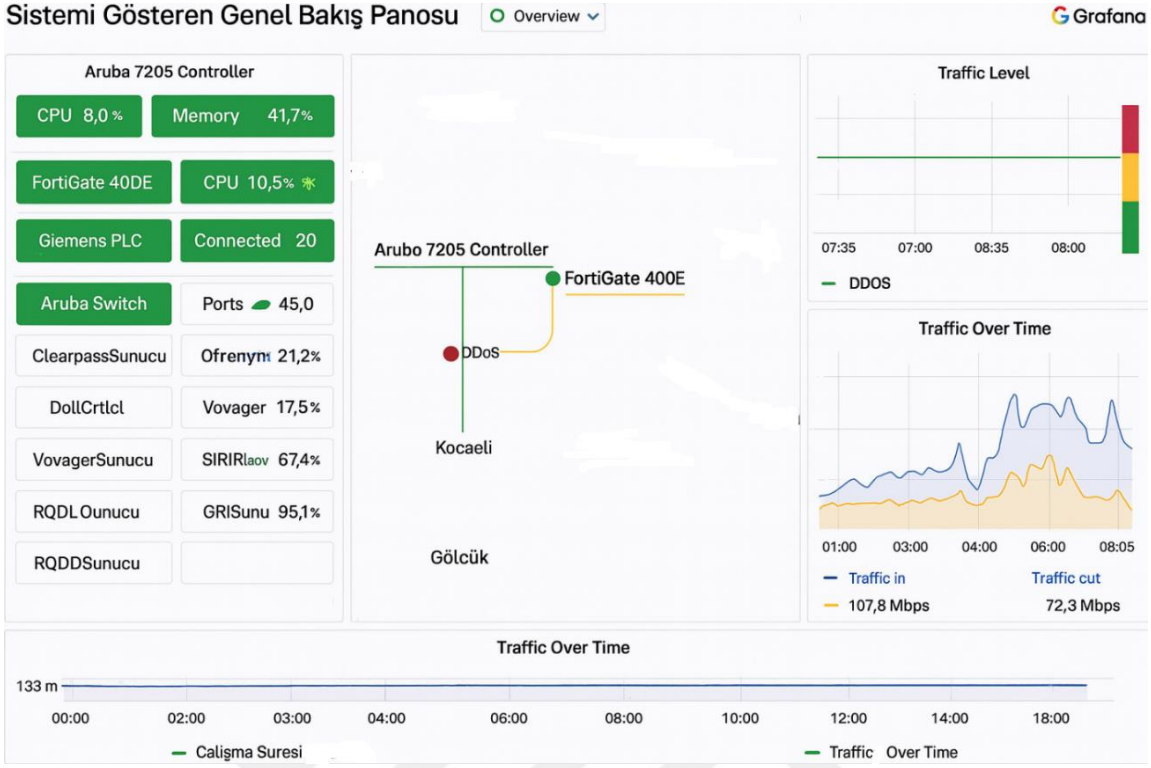
Katkı Alanı	Açıklama
Yönetim Kolaylığı	Tek ekrandan tüm ağ, sunucu ve endüstriyel cihazların izlenebilmesi
SLA Takibi	Hizmet kesintilerinin süre ve sıklığının ölçülmesi, SLA ihlallerinin tespiti
Görselleştirme Esnekliği	Farklı zaman aralıklarında, özelleştirilebilir ve etkileşimli paneller
Karar Destek Katkısı	Üst yönetime anlaşılır raporlar sunularak hızlı ve veri temelli karar alma süreçlerinin desteklenmesi

6.6 Tüm Sistemi Gösteren Genel Bakış Panosu

Zabbix ara yüzü, tüm altyapının özet durumu için kullanıcı dostu bir haritalama ya da renk kodlu durum ekranı sunamaz. Grafana' da status panel, bar gauge, worldmap gibi eklentilerle hem coğrafi hem sistemsel genel görünüm oluşturulmuştur. Şekil 61 örnek çalışmasında görüldüğü üzere ağ altyapısındaki farklı cihazların durumunu tek bir ekranda bütüncül şekilde sunarak sistemin genel sağlığını anlık olarak göstermektedir. CPU, bellek, port kullanımı ve bağlantı durumu gibi temel metrikler ayrı kutucuklar halinde görselleştirilmiş ve yorumlana bilirliği artırılmıştır. Harita tabanlı gösterim sayesinde cihazların fiziksel konumları ile mantıksal ilişkileri aynı anda izlenebilmekte, bu da özellikle çok lokasyonlu yapılarda yönetim kolaylığı sağlamaktadır. Trafik seviyesi ve zaman içindeki değişim grafikleri, olası DDoS saldırılarının veya olağandışı ağ yoğunluklarının hızlı bir şekilde tespit edilmesine imkân vermektedir. Panelde sunulan bu görsel özet, yalnızca teknik personelin değil, üst düzey yöneticilerin de ağın genel durumu hakkında hızlı karar almasına yardımcı olmaktadır. Ayrıca, farklı cihazlardan gelen verilerin aynı ara yüzde bütünleştirilmesi, Zabbix'in veri toplama gücü ile Grafana'nın gelişmiş görselleştirme kabiliyetlerinin tamamlayıcı bir şekilde kullanılabildiğini ortaya koymaktadır. Bu tür panolar kurumun operasyonel şeffaflığını artırmakta ve pratik ağ yönetimi stratejilerinin uygulanmasını kolaylaştırmaktadır. Tablo 5 'te Zabbix ve Grafana entegrasyonu ile gerçekleşen kolaylıklar görülmektedir.

Şekil 50 örneğinde görüldüğü üzere, ağ alt yapısının genel durumunu yansıtan Grafana tabanlı bir izleme paneli görülmektedir. Aruba 7205 Controller, Fortigate 400E güvenlik duvarı, Siemens PLC ve Aruba Switch gibi temel bileşenler gerçek zamanlı olarak takip edilmektedir. İşlemci ve bellek kullanım oranları, bağlı cihaz sayısı ve port yoğunluğu sistemin kaynak tüketimini değerlendirmek için önemli göstergeler sunmaktadır. Sağ tarafta yer alan grafikler, ağ trafiğinin zaman içerisindeki değişimini ayrıntılı biçimde ortaya koymaktadır. Özellikle zaman içindeki trafik grafiğinde giriş trafiğinin 107,8 Mbps, çıkış trafiğinin ise 72,3 Mbps seviyelerine ulaştığı görülmektedir. Bu veriler, ağda yaşanan ani trafik artışlarının tespit edilmesi ve olası DDoS saldırılarının önceden belirlenmesi açısından kritik rol oynamaktadır. Ortadaki topolojik harita, Kocaeli merkezli sistemden Gölcük lokasyonuna olan bağlantıları göstermektedir. Ayrıca DDOS atağına yönelik uyarı, güvenlik tehditlerinin izleme sistemine entegre biçimde tespit edilerek görselleştirildiğini kanıtlamaktadır. Bu tür panolar, hem performans yönetimini hem de güvenlik olaylarının anlık olarak gözlemlenmesini sağlayarak, sistem yöneticilerinin karar alma süreçlerini hızlandırmakta ve ağ yönetiminde bütünsel bir kontrol mekanizması oluşturmaktadır.

Şekil 50 de Grafana da sisteme genel bakış panosu verilmiştir.



Şekil 50. Grafana da sisteme genel bakışı gösteren ekran

7. Sonuç ve Öneriler

Bu tez çalışmasında, açık kaynak kodlu ağ izleme yazılımı Zabbix ile gelişmiş veri görselleştirme aracı Grafana'nın entegrasyonu ele alınmış; bu iki sistemin birlikte kullanımıyla kurumsal ağlarda izlenebilirliğin, analiz kabiliyetinin ve olaylara müdahale süresinin nasıl iyileştirilebileceği kapsamlı bir şekilde incelenmiştir. Günümüzde ağ altyapılarının büyüklüğü, karmaşıklığı ve çeşitliliği göz önünde bulundurulduğunda, yalnızca cihazların değil aynı zamanda hizmetlerin, IoT sistemlerinin ve endüstriyel kontrol ünitelerinin de sürekli olarak izlenmesi zorunlu hale gelmiştir. Bu bağlamda, Zabbix'in esnek, ölçeklenebilir ve açık kaynaklı mimarisi ile Grafana'nın güçlü görselleştirme kabiliyetleri bir araya getirilerek bütünleşik bir izleme çözümü sunulmuştur.

Tez kapsamında geliştirilen yapılandırmalarda, Python betik tabanlı şablon üretim süreci tasarlanmış ve SNMP protokolü üzerinden veri toplayan cihazlardan otomatik XML şablonlarının oluşturulması sağlanmıştır. Bu yöntem, özellikle Siemens SIMATIC S7 PLC ve IM153-4PN gibi endüstriyel bileşenlerin detaylı olarak anlık izlenmesini önemli ölçüde kolaylaştırmıştır. Burada Zabbix'in açık kaynak kodlu olmasından kaynaklı özelleştirilebilirliği ve esnekliğinden faydalanılmıştır.

Zabbix'in yerleşik görselleştirme araçlarının çok katmanlı sistemlerde sınırlı kaldığı gözlemlenmiştir. Bu sınırlılık, Grafana entegrasyonu ile aşılmıştır. Grafana panelleri sayesinde cihazlar arası karşılaştırmalı grafikler, gerçek zamanlı durum panoları, eğilim analizleri ve uyarı bazlı filtreleme mekanizmaları uygulanabilmiştir. Bu durum, yalnızca teknik ekiplerin değil aynı zamanda karar verici yöneticilerin de verilerden doğrudan yararlanmasını sağlamıştır.

Çalışma kapsamında gerçekleştirilen iyileştirmeler sayısal veriler ve grafiksel çıktılar üzerinden karşılaştırmalı olarak ortaya konulmuştur. Öncelikle Şekil 40 örneğinde görüleceği üzere Dell IDRAC sunucusunda RAID kartı bataryasının görevini yerine getirmediği tespit edilmiştir. Bu durum önbellek güvenliğini ortadan kaldırarak kritik bir risk oluşturmuştur. Yapılan batarya değişimi sonrasında batarya değeri 2 seviyesinden 3 seviyesine yükselmiş ve bu değişim yaklaşık %50 oranında bir iyileşmeye karşılık gelmiştir. Böylece sunucunun önbellek güvenilirliği yeniden sağlanmıştır. Omurga ağ anahtarı üzerinde yapılan incelemelerde, Şekil 43 örneğinde görüleceği üzere F8 portunda sürekli artan CRC hataları gözlemlenmiştir. Mart 2025 boyunca bu portta toplamda yaklaşık 350 giriş ve 90 çıkış olmak üzere 440 CRC hatası birikmiştir. Sorunun kaynağının fiber kablo olduğu belirlenmiş, kablonun değiştirilmesiyle birlikte tüm CRC hataları giderilmiştir. Bu müdahale sonucunda hata sayısı 440'dan sıfıra düşürülmüş, yani bağlantı kalitesinde %100 iyileşme sağlanmıştır.

Tezin ana konusunu oluşturan Python tabanlı otomatik şablon ekleme yöntemi ise özellikle hazır şablonları bulunmayan eski nesil IoT cihazlarının izlenmesi açısından önemli bir katkı sunmuştur. Tablo 4 örneğinde görüleceği üzere manuel yöntemle yaklaşık bir saat süren hazır şablon arama süreci çoğunlukla sonuçsuz kalırken, geliştirilen yöntem ile bu adıma gerek duyulmamıştır. Parametre ve OID değerlerinin tespiti her iki yöntemde de yaklaşık 30 dakika sürmüş; ancak Python betiği ile şablonun oluşturulup Zabbix'e eklenmesi yalnızca 3 dakika almıştır. Böylece toplam süreç manuel yöntemle tamamlanamazken, otomatik yöntemle yalnızca 3 dakika içinde başarıyla tamamlanmıştır. Bu durum, manuel sürece kıyasla %90'ın üzerinde zaman tasarrufu sağlamış ve insan hatası olasılığını en aza indirmiştir. Ayrıca, manuel yöntemle izlenebilir parametreler belirlenemezken, otomatik yöntem sayesinde işlemci, bellek ve çalışma süresi gibi toplam 5 parametre aktif olarak izlenebilir hale gelmiştir.

Bu çalışmanın başlıca katkıları şunlardır:

1) Otomatik şablon üretimi ile ağ cihazlarının izleme süreçlerinin hızlandırılması,
2) Endüstriyel PLC'lerin izlenmesine yönelik özgün uygulamalar,
3) Zabbix–Grafana uyumu sayesinde karar destek mekanizmalarına katkı,

Kurumsal ağ ve endüstriyel ağ uygulama çalışması sonucunda elde edilen bulgular şu şekilde özetlenebilir:

1. Zabbix üzerinden 1500 den fazla veri öğesi, 700'ü geçen tetikleyici ve çok sayıda grafik tanımlanarak ağ altyapısının anlık durumu başarıyla izlenmiştir.

2. Otomatik keşif ve kayıt mekanizmaları sayesinde yeni cihazların %100'ü elle işlem gerektirmeksizin izleme kapsamına alınmıştır.

3. Grafana ile oluşturulan paneller üzerinden ağ trafiği, işlemci yükü, port durumu, hata oranları gibi kritik metrikler gerçek zamanlı olarak görselleştirilmiş ve sistem yöneticilerinin müdahale süresinde %30'a varan iyileşme sağlanmıştır.

4. İzleme yapılan kablosuz bağlantı cihazının üzerinde kayıtlı bulunan 75 adet kablosuz sinyal dağıtıcı cihazların %80 inin şebekeden beslendiği ve enerji kesintisinde hizmet dışı kaldığı tespit edilmiştir.

5. Özellikle endüstriyel bileşenlerin izlenmesinde, Zabbix ve Grafana uyumunun kesinti sürelerini azalttığı, hata tespit sürecini hızlandırdığı ve sistem güvenilirliğini artırdığı gözlemlenmiştir.

Zabbix ve Grafana entegrasyonu; kurumsal BT altyapılarında merkezi izleme, hızlı karar alma ve proaktif bakım süreçlerini destekleyen güçlü bir çözüm olarak öne çıkmaktadır. Elde edilen bulgular, yalnızca altyapı sistemlerinin verimliliğini artırmakla kalmamış, aynı zamanda kurumların uzun vadeli sürdürülebilirlik ve maliyet optimizasyonu hedeflerine de katkı sağlamıştır.

Öneriler:

1. Sürdürülebilirlik açısından, Zabbix ile entegre çalışan otomasyon betiklerinin (örneğin Python ile şablon üretimi) sürekli güncellenmesi ve versiyon kontrol sistemlerine (GitHub vb.) entegre edilmesi önerilmektedir.

2. Endüstriyel IoT cihazlar gibi özel sistemler için SNMP yerine MQTT, OPC-UA gibi modern protokollerle izleme yapılması ve bu verilerin Zabbix ajanlarıyla uyumlu hale getirilmesi için çalışılmalı.

3. Yönetimsel raporlama ve SLA takibi için Grafana üzerinde yöneticilere özel, sadeleştirilmiş paneller tasarlanarak karar destek sistemleriyle entegrasyon gerçekleştirilebilir.

4. Zabbix API üzerinden otomatik envanter senkronizasyonu, servis başlatma/durdurma gibi komutların uzaktan tetiklenmesi, operasyonel verimliliği daha da artıracaktır.

5. Grafana panelleri, mobil uyumlu tasarımlarla genişletilerek bakım teknisyenleri veya saha mühendislerinin cep telefonları üzerinden sistemi anlık olarak izlemesi sağlanabilir.

6. İzlenen sistemler üzerinde zamanlanmış yük testleri ya da bağlantı simülasyonları planlanarak gerçek senaryoların etkileri izlenebilir. Bu sayede sistemin sınırları anlaşılır ve kapasite planlaması daha sağlıklı yapılır.

Zabbix ile Grafana'nın entegrasyonu, sadece teknik izleme değil; karar verme süreçlerinde de veri odaklı ve proaktif yönetim anlayışını destekleyen bir yapı sunmaktadır. Bu sistem sayesinde izleme süreçleri hızlanmış, olaylara müdahale süresi azalmış ve ağ yönetiminde şeffaflık artmıştır.

Bunun sonucu olarak da iş sürekliliği süreçlerine önemli bir katkı sağlanmıştır. Gelecekte, makine öğrenimi ve yapay zekâ destekli analizlerin bu altyapıya entegre edilmesiyle, Zabbix'in öngörüye dayalı bir ağ yönetim sistemine dönüşebileceği değerlendirilmektedir.

KAYNAKÇA

1- Katonová, E. A. Džubák, J. & Feciľak, P. (2023). Automated monitoring of network infrastructures based on the Zabbix solution. *2023 21st International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 283–288. IEEE. https://doi.org/10.1109/ICETA61311.2023.10344265

2- Assunção da Silva, R., & José da Silva, W. (2024). A implementação do Zabbix com segurança: Um estudo de caso Zabbix Safely. *Revista Foco, 17*(4), 1–10. https://doi.org/10.54751/revistafoco.v17n4-055

3- Da Silva, C. H. G. (2021). *Monitoramento de rede com a ferramenta Zabbix* (Trabalho de Conclusão de Curso). Universidade Tecnológica Federal do Paraná, Brasil.

4- Alpoim Serras, B. M. (2024). *Synoptics of Things – An open standard for managing and monitoring services of the ISoS framework in web interfaces* (Dissertação de Mestrado). Instituto Superior Técnico, Universidade de Lisboa.

5- Husna, M. A., & Rosyani, P. (2021). Implementasi sistem monitoring jaringan dan server menggunakan Zabbix yang terintegrasi dengan Grafana dan Telegram. *JURIKOM (Jurnal Riset Komputer), 8*(6), 247–255. https://doi.org/10.30865/jurikom.v8i6.3631

6- Hokkanen, L. (2024). *Järjestelmävalvojan työkalupakki* (Opinnäytetyö AMK). Jyväskylän ammattikorkeakoulu.

7- Chen, L., Wang, X., Xue, P., Zhang, Y., Gu, Y., Zhao, X., Cheng, X., Fan, M., & Xiao, S. (2023). Design of visual seismic monitoring and warning system based on Zabbix. *Journal of Physics: Conference Series, 2519*(1), 012008. IOP Publishing. https://doi.org/10.1088/1742-6596/2519/1/012008

8- Pinto, A. M. C. (2022). *Recolha e tratamento de dados para disponibilizar em dashboards* (Dissertação de Mestrado). Universidade do Minho, Escola de Engenharia.

9- Barros, L. (2023). *Sistema de monitorização de redes inteligente* (Relatório de Estágio de Licenciatura). Universidade de Lisboa.

10- Menegazzi, P. H. (2021). *Monitoramento de aplicações em tempo real utilizando o Telegram* (Trabalho de Conclusão de Curso). Universidade de Caxias do Sul, Brasil.

11- Brito, D. C. S., & Sousa, J. V. M. (2024). Implementação do monitoramento de redes com Zabbix. In *Anais do Simpósio Brasileiro de Sistemas de Informação*. Universidade Estadual do Piauí.

12- Leppänen, T. (2021). *Data visualization and monitoring with Grafana and Prometheus* (Bachelor's Thesis). Turku University of Applied Sciences.

13- Alves, K. P. S. (2021). *Monitoramento de redes com Zabbix* (Trabalho de Conclusão de Curso). Centro Estadual de Educação Tecnológica Paula Souza, Faculdade de Tecnologia de Indaiatuba.

14- Nurrohman, I. (2024). *Implementasi sistem monitoring jaringan menggunakan Zabbix dan Grafana* (Skripsi Sarjana). Universitas Teknologi Digital Indonesia. https://repository.nurulfikri.ac.id/id/eprint/532

15- Dantas, P. H. R. (2024). *Gerência de redes com Zabbix em ambiente nuvem* (Trabalho de Conclusão de Curso). Pontifícia Universidade Católica de Goiás, Escola Politécnica e Artes.

16- Gonzalez, J. S. C. (2020). *Implementación en la nube de un sistema de monitoreo de eventos de fallas para infraestructura de redes y de seguridad informática utilizando la integración de Zabbix, Grafana y Zammad* (Tesis de Grado). Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador. http://www.dspace.espol.edu.ec/handle/123456789/56359
17- Yulvianda, R., & Ismail, M. (2023). Desain dan implementasi sistem monitoring sumber daya server menggunakan Zabbix dan Grafana. *Jurnal Informatika dan Rekayasa Komputer (JAKAKOM), 3*(1), 322–329. https://doi.org/10.33998/jakakom.2023.3.1.712
18- Gonçalves, G. D. C. (2024). *Grafana como uma ferramenta de visualização de monitoramento de redes de computadores* (Trabalho de Conclusão de Curso). Pontifícia Universidade Católica de Goiás, Escola Politécnica e Artes.
19- Nguyen, A. (2023). *Optimizing VXLAN network management* (Master's Thesis). Tampere University, Faculty of Information Technology and Communication Sciences.
20- Martins Silva, P. H. (2021). *Gerenciamento de redes com Zabbix* (Trabalho de Conclusão de Curso). Universidade Tecnológica Federal do Paraná, Brasil.
21- Haro Velasco, A. R., Coral Herrera, R. del C., González Malla, E. E., & Morales Arévalo, F. D. (2023, June 20–23). Real-time monitoring and alerting system using Zabbix and Grafana software for wireless Internet access service management. In *Proceedings of the 18th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–8). IEEE. https://doi.org/10.23919/CISTI58278.2023.10211432
22- García, D. F. (2025). *Implementación de un sistema de monitoreo de red basado en Zabbix y Grafana para infraestructuras de telecomunicaciones* (Tesis de Maestría). Universidad Politécnica Salesiana, Ecuador.
23- Chavez, A., & Vieira, R. S. C. (2020). *Implantação de uma solução open source na gestão de uma rede de computadores em uma média empresa com as ferramentas Zabbix e Grafana* (Trabalho de Conclusão de Curso). Universidade Tecnológica Federal do Paraná, Brasil.
24- Guo, Y. S., Liu, C., Guo, G., & Gao, F. (2021). Research on monitoring of information equipment based on Zabbix for power supply company. *2021 3rd International Conference on Applied Machine Learning (ICAML)*, 487–491. IEEE. https://doi.org/10.1109/ICAML54311.2021.00108
25- Moosa, M. A., Vangujar, A. K., & Mahajan, D. P. (2023). Detection and analysis of DDoS attack using a collaborative network monitoring stack. *2023 16th International Conference on Security of Information and Networks (SIN)*, 120–127. IEEE. https://doi.org/10.1109/SIN60469.2023.10474700
26- Muñoz Arroyave, M. (2024). *Implementación de plataforma de monitoreo de variables de desempeño ópticas de interfaces OpenZR+ sobre plataformas desagregadas por medio de Zabbix y Grafana para aplicaciones IPoDWDM* (Trabajo de Grado). Universidad de Antioquia, Medellín.
27- Baglanuly, Z. U. & Khassymbekovna, K. D. (2025). Intelligent monitoring of network devices using artificial intelligence. In *International Scientific and Practical Conference "Endless Light in Science"* (pp. 93–102).
28- Leonardson (2021). *zabbix-templator: Automatic Zabbix template generator*. GitHub Repository.