### Giriş

Bu proje, sunucu performansının izlenmesi ve potansiyel performans sorunlarının tespit edilmesi amacıyla gerçekleştirilmiştir. Proje kapsamında, Prometheus ve Grafana kullanılarak kapsamlı bir izleme ve uyarı sistemi kurulmuştur. Bu sistem, sunucu performans metriklerinin sürekli olarak izlenmesini, görselleştirilmesini ve anormalliklerin tespit edilmesini sağlar.

### 2. Projenin Amacı

Projenin temel hedefleri:

* Sunucu performansının gerçek zamanlı izlenmesi
* Performans sorunlarının erken tespiti ve çözümü
* Sistem verimliliğinin artırılması
* Kullanıcı memnuniyetinin artırılması

### 3. Çözülen Sorunlar

Bu proje, aşağıdaki sorunların çözümüne yönelik olarak geliştirilmiştir:

* **Yavaş Sistem Performansı:** Müşterilerin sistemin yavaş çalıştığını bildirdiği durumlarda, sorunun nerede olduğunu anlamak ve çözmek için raporlar kullanılacaktır.
* **Siber Saldırılar:** Siber saldırı durumlarında, sunucuların ve veri tabanının yükünü izleyerek süreci doğru yönetmek için kullanılacaktır.
* **Sistem Optimizasyonu:** Prometheus ve Grafana kullanılarak kapsamlı bir izleme sistemi kuruldu. Sistem performans verileri anlaşılır bir şekilde görselleştirildi ve yöneticilerin hızlı karar alması sağlandı.

### 4. Teknik Detaylar

#### 4.1 Kullanılacak Teknolojiler

* **Monitoring Araçları:** Prometheus, Windows Exporter
* **Raporlama Araçları:** Grafana
* **Uyarı Yönetim Araçları:** Alertmanager

#### 4.2 Mimari Tasarım

* **Veri Toplama:** Sunuculardan gelen performans verileri Prometheus ile toplanacaktır.
* **Veri Depolama:** Toplanan veriler merkezi bir veri tabanında saklanacaktır.
* **Veri Analizi:** Performans verileri analiz edilerek anlamlı raporlar oluşturulacaktır.
* **Raporlama:** Analiz edilen veriler, Grafana ile kullanıcı dostu arayüzlerde grafiksel ve metinsel raporlar olarak sunulacaktır.

### 5. Prometheus Kuruldu

Prometheus, sistemin performansını izlemek için ana izleme aracı olarak kuruldu. Prometheus, verileri toplar, saklar ve sorguların çalıştırılmasını sağlar. Bu sayede, sistemin performans metrikleri sürekli olarak izlenebilir hale geldi.

### 6. Windows Exporter Kuruldu

Windows işletim sisteminde çalışan sunucuların metriklerini toplamak için Windows Exporter kuruldu. Bu araç, CPU, bellek, disk ve ağ kullanımı gibi performans metriklerini Prometheus'a ileterek verilerin toplanmasını sağladı.

### 7. Alertmanager Kuruldu

Alertmanager, Prometheus tarafından oluşturulan alarmların yönetimini sağlamak için kuruldu. Bu araç, belirli koşullar altında uyarılar göndererek sistem yöneticilerinin hızlı bir şekilde müdahale etmesini sağladı.

### 8. Grafana Kuruldu

Grafana, Prometheus'tan gelen verileri görselleştirmek için kullanıldı. Kurulum tamamlandıktan sonra, çeşitli panolar oluşturularak verilerin anlaşılabilir bir şekilde sunulması sağlandı.

### 9. Sorgular Yazıldı

Aşağıdaki sorgular, sistem performansının izlenmesi için yazıldı:

* **CPU Kullanımı:**

100 - (avg by (instance) (rate(windows\_cpu\_time\_total{mode="idle"}[5m])) \* 100)

Bu sorgu, CPU'nun kullanım yüzdesini hesaplar. Sistemdeki tüm CPU'ların 5 dakikalık ortalama çalışma süresi oranını hesaplayarak, CPU'nun boşta kalma süresini yüzdelik olarak gösterir ve bu değeri 100'den çıkararak kullanım yüzdesini elde eder.

* **RAM Kullanımı:**

100 \* (1 - (windows\_memory\_available\_bytes / windows\_cs\_physical\_memory\_bytes))

Bu sorgu, RAM'in kullanım yüzdesini hesaplar. Toplam fiziksel bellekten kullanılabilir belleği çıkararak mevcut RAM kullanımını yüzdelik olarak gösterir.

* **Disk Okuma:**

rate(windows\_logical\_disk\_read\_bytes\_total{instance="localhost:9182"}[1m])

Bu sorgu, diskteki okuma hızını hesaplar. Disk üzerindeki okunan byte miktarını her dakika için oranlayarak disk okuma hızını verir.

* **Disk Yazma:**

rate(windows\_logical\_disk\_write\_bytes\_total{instance="localhost:9182"}[1m])

Bu sorgu, diskteki yazma hızını hesaplar. Disk üzerindeki yazılan byte miktarını her dakika için oranlayarak disk yazma hızını verir.

* **Ağ İndirme:**

rate(windows\_net\_bytes\_received\_total{instance="localhost:9182"}[1m])

Bu sorgu, ağ üzerinden indirilen verinin hızını hesaplar. Her dakika indirilen toplam byte miktarını oranlayarak ağ indirme hızını verir.

* **Ağ Yükleme:**

rate(windows\_net\_bytes\_sent\_total{instance="localhost:9182"}[1m])

Bu sorgu, ağ üzerinden yüklenen verinin hızını hesaplar. Her dakika yüklenen toplam byte miktarını oranlayarak ağ yükleme hızını verir.

### 10. Dashboard Oluşturuldu

Grafana'da, yukarıdaki sorguları kullanarak anlaşılabilir ve kullanıcı dostu bir pano oluşturuldu. Bu pano, sistem yöneticilerinin hızlı bir şekilde durumu değerlendirmesine ve gerekli önlemleri almasına olanak tanır.

### 11. Alert Kuralları Yazıldı

Sistem performansını izlemek ve anormallikleri tespit etmek için aşağıdaki alarm kuralları yazıldı:

* **CPU Kullanımı:**

(100 - (avg by (instance) (rate(windows\_cpu\_time\_total{mode="idle"}[5m])) \* 100)) > (100 - (avg by (instance) (rate(windows\_cpu\_time\_total{mode="idle"}[5m])) \* 100))

Bu kural, CPU kullanım yüzdesinin normalinden fazla olduğunu tespit eder ve CPU'nun aşırı kullanımını belirler.

* **RAM Kullanımı:**

100 \* (1 - (windows\_memory\_available\_bytes / windows\_cs\_physical\_memory\_bytes)) > 63

Bu kural, RAM kullanım yüzdesinin %63'ten fazla olduğunu tespit eder ve aşırı RAM kullanımını belirler.

* **Disk Okuma:**

rate(windows\_logical\_disk\_read\_bytes\_total{instance="localhost:9182"}[1m]) > 2 \* rate(windows\_logical\_disk\_read\_bytes\_total{instance="localhost:9182"}[5m])

Bu kural, disk okuma hızının normalin iki katından fazla olduğunu tespit eder ve aşırı disk okuma aktivitesini belirler.

* **Disk Yazma:**

rate(windows\_logical\_disk\_write\_bytes\_total{instance="localhost:9182"}[1m]) > 2 \* rate(windows\_logical\_disk\_write\_bytes\_total{instance="localhost:9182"}[5m])

Bu kural, disk yazma hızının normalin iki katından fazla olduğunu tespit eder ve aşırı disk yazma aktivitesini belirler.

* **Ağ İndirme:**

rate(windows\_net\_bytes\_received\_total{instance="localhost:9182"}[1m]) > 1.5 \* daily\_avg\_network\_traffic

Bu kural, ağ üzerinden indirilen verinin normal günlük ortalamanın 1.5 katından fazla olduğunu tespit eder ve aşırı ağ indirme aktivitesini belirler.

* **Ağ Yükleme:**

rate(windows\_net\_bytes\_sent\_total{instance="localhost:9182"}[1m]) > 1.5 \* daily\_avg\_network\_traffic

Bu kural, ağ üzerinden yüklenen verinin normal günlük ortalamanın 1.5 katından fazla olduğunu tespit eder ve aşırı ağ yükleme aktivitesini belirler.

Bu alarm kuralları, sistemdeki potansiyel performans sorunlarını önceden tespit ederek müdahale edilmesini sağlar.

### Sonuç

Proje kapsamında kurulan izleme ve uyarı sistemi sayesinde sunucu performansı gerçek zamanlı olarak izlenebilmekte ve olası performans sorunları erken tespit edilebilmektedir. Bu sayede sistem verimliliği artırılmış ve kullanıcı memnuniyeti sağlanmıştır. Prometheus ve Grafana ile oluşturulan bu kapsamlı sistem, yöneticilerin hızlı ve etkili kararlar almasına olanak tanıyarak, sunucu altyapısının güvenilirliğini ve performansını artırmıştır.