İZLEME ve ALARM YÖNETİMİ

Proje: Güvenilirlik, ölçeklenebilirlik ve performans gerektiren uygulamalar için izleme ve alarm yönetimi ihtiyaçlarını karşılamayı hedeflemektedir.

Proje Açıklaması: AWS CloudWatch hizmetini kullanarak uygulama ve altyapı bileşenlerinin izlenmesi ve alarm yönetiminin sağlanmasıdır. AWS CloudWatch, çeşitli metrikleri toplayarak sistem performansını, kullanımı ve kaynaklarını izlemek için kullanılır.
Proje kapsamında, özel CloudWatch alarmları oluşturulacak ve önemli metrikler sürekli olarak izlenecektir. Bu alarmlar, belirli eşik değerlerinin aşılması durumunda bildirimler göndererek hızlı müdahale imkanı sağlayacaktır.

Projenin Temel Adımları:

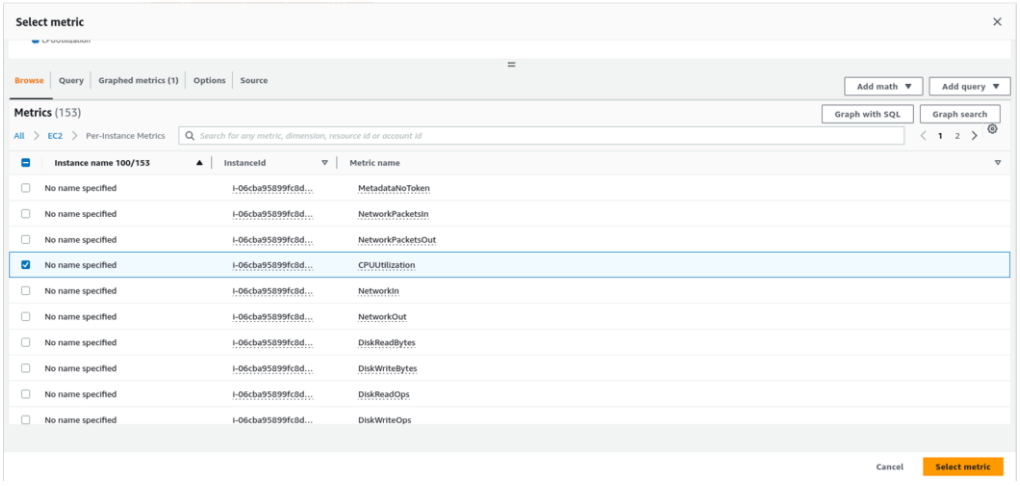
- AWS CloudWatch hizmetini kullanarak uygulama ve altyapı bileşenlerinin izlenmesi.
- Özel CloudWatch alarmları oluşturarak önemli metrikleri izleyin ve gerektiğinde bildirimler alınması.
- İzleme verilerini analiz etmek için AWS CloudWatch Logs ve AWS CloudWatch Insights gibi hizmetleri kullanılması.

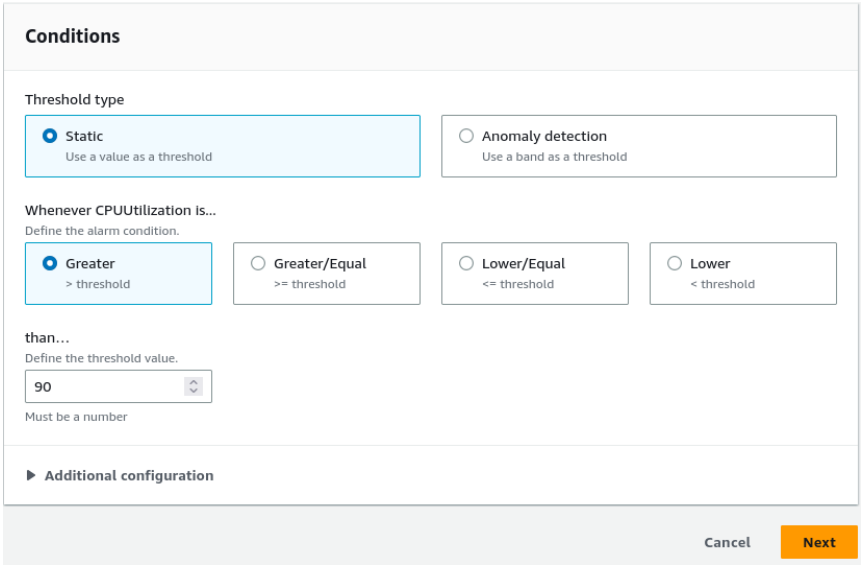
Proje İçin Kullanılacak Amazon Hizmetleri

- AWS CloudWatch
- AWS CloudWatch Logs
- AWS CloudWatch Insights

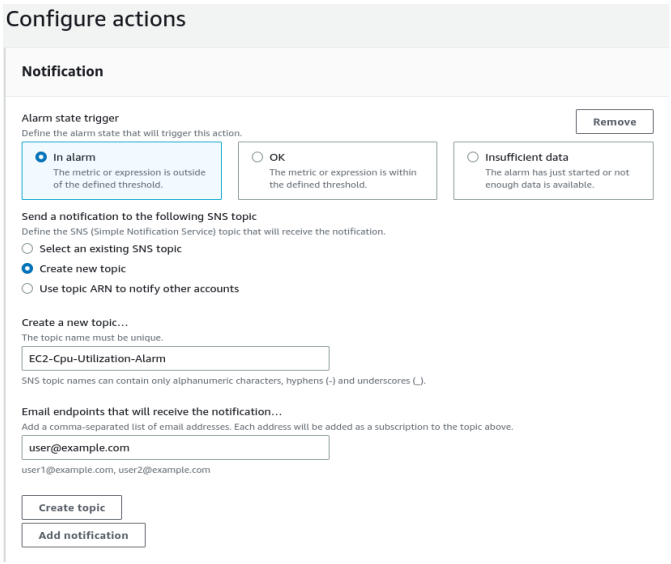
AWS CloudWatch
Uygulama, hizmet ve altyapı bileşenlerin izlenmesi, logların toplanması ve olayların yönetimi için kullanılan bir hizmettir. CloudWatch, AWS kaynaklarının performansını, durumunu ve davranışını takip etmek ve analiz etmek için metrikleri, logları ve olayları toplar ve görselleştirir.

Cloudwatch Alarm Oluşturma
CloudWatch konsoluna eriştikten sonra sol alanda bulunan "*All Alarms*" seçeneği seçilir. "*Specify metric and conditions*" sekmesinde istenilen Metric seçilir. Projede EC2 instance'ın CPU kullanımı %90'ı geçtiği takdirde alarm üretmesi için yapılandırma kullanılacaktır.

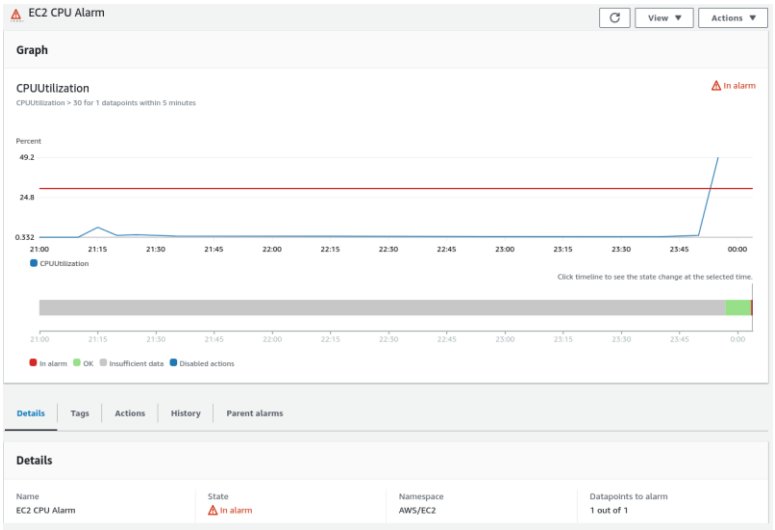




Configure Actions sekmesinde, alarm için gönderilecek bildirimin nereye gönderileceği bilgileri girilir.



Ardından gelecek gerekli bilgiler doldurulduktan sonra "*Create Alarm*" seçeneği seçilerek alarm oluşturulur. Mail'e gelen confirmation linkine tıklayarak alarm etkinleştirilir.
Proje kapsamında uygulama olarak CPU kullanımı %30 olarak ayarlanmıştır. Bash kodu ile CPU kullanımı %90 üzerine çıkartılmaya çalışılmış ve alarm test edilmiştir.



You are receiving this email because your Amazon CloudWatch Alarm "EC2 CPU Alarm" in the EU (Frankfurt) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [49.23144296148671 (24/05/23 23:53:00)] wa
greater than the threshold (30.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Thursday 25 May, 2023 00:03:30 UTC".

View this alarm in the AWS Management Console:
https://eu-central-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=eu-central-1#alarmsV2:alarm/EC2%20CPU%20Alarm

Alarm Details:
- Name: EC2 CPU Alarm
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [49.23144296148671 (24/05/23 23:53:00)] was greater than the threshold (30.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Thursday 25 May, 2023 00:03:30 UTC
xxxx
- Alarm Arn: arn:aws:cloudwatch:eu-central-1:xxx:alarm:EC2 CPU Alarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 30.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-0c753b31322a66e89]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: missing

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:eu-central-1:120703883523:Cpu-Anomaly]
- INSUFFICIENT_DATA:

CloudWatch Logs
CloudWatch Logs, uygulama günlüklerini merkezi bir konumda toplayarak günlük verilerinin izlenmesini ve analizini kolaylaştırır.

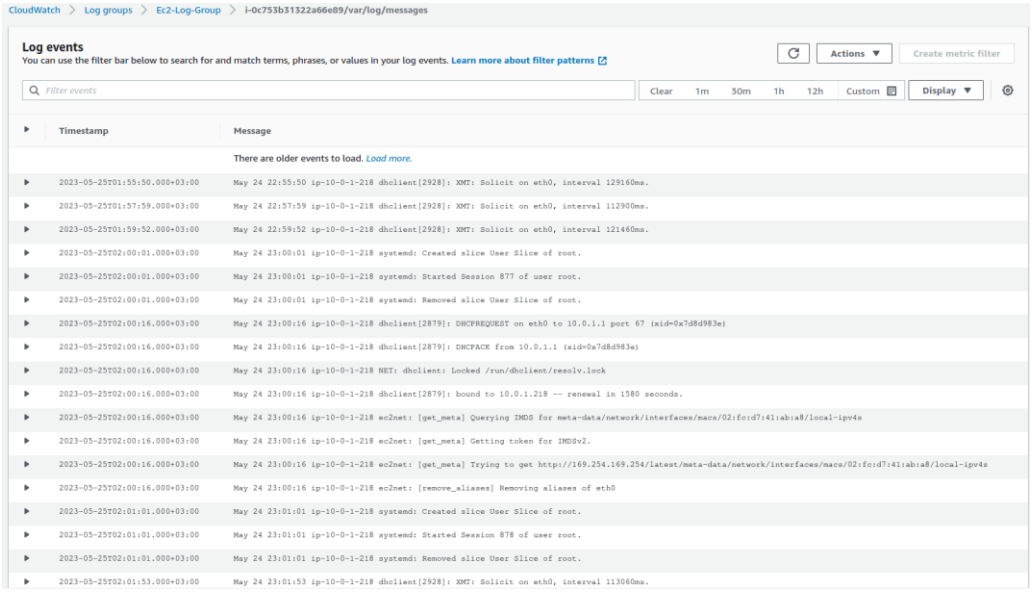
EC2 Instance İçin CloudWatch Logs Oluşturma
CloudWatch hizmetinde sol tarafta bulunan "*Log Groups*" seçeneği seçilir ve grup ismi verildikten sonra Log grubu oluşturulur. Ardından ssh ile instance'a bağlantı sağlanır ve sanal sunucuya Amazon CloudWatch Logs Agent servisi kurulur ve sistem başlatılır. Amazon CloudWatch Logs Agent, Amazon Web Services (AWS) CloudWatch hizmetine log verilerini göndermek için kullanılan bir araçtır..

"*sudo yum install -y awslogs;*
sudo systemctl enable awslogsd;
sudo systemctl start awslogsd"

Log dosyasında değişiklik yapmak için aşağıdaki komut kullanılır.
"sudo vi /etc/awslogs/awslogs.conf"

Bu dosyada, log gruplarını ve izlenecek log dosyalarını yapılandırabilirsiniz. Örneğin, /var/log/messages dosyasını izlemek için aşağıdaki gibi bir örnek ekleyebilirsiniz:
[/var/log/messages]
datetime_format = %b %d %H:%M:%S
file = /var/log/messages
log_stream_name = {instance_id}/var/log/messages
log_group_name = MyLogGroup

"*nano /etc/awslogs/awscli.conf*" komutu ile region konum ile değiştirilir. Ardından CloudWatch loglardan loglar takip edilebilir.



AWS CloudWatch Insight

AWS CloudWatch Logs Insights, Amazon CloudWatch Logs hizmetinin bir özelliğidir. Bu özellik, log verilerinizi sorgulamak, analiz etmek ve görselleştirmek için kullanılan bir hizmettir.

CloudWatch hizmetinde "*Log Group*" seçeneği seçildikten sonra sağ üstte bulunan "*View in Insight*" seçeneği seçilir. Sorgu alanına log verilerinizi sorgulayacak olan sorgu ifadesini girilir. Sorgu dili, SQL benzeri bir formattadır ve log verileri filtrelemek, gruplamak, hesaplamalar yapmak gibi birçok işlemi gerçekleştirilebilir. Örnek olarak, "*fields @timestamp, @message | filter @message like /error/*" gibi bir sorgu yazılabilir. "*Run query*" seçeneği seçilerek sorgu cevabı alınır.