CloudWatch 
What is CloudWatch? 
Amazon CloudWatch 
• CloudWatch is the monitoring service of AWS. 
• It enables you to monitor metrics of resources and 
applications that run on AWS as well as on-premise servers. 

Hangi platformda çalışırsak çalışalım bir monitoring ihtiyacımız olacak. DevOps ta open source modelleri de var. AWS nin kendi monitoring servisi de CloudWatch.

Environment ımızda gerçekleşen olayları, kurguladığımız yapıya göre AWS gözlemliyor. Biz kurgularken hangi metric lere göre neler yapmasını gerektiğini veriyoruz. Setup ı önden kuruyoruz sonra gözlemeye başlıyor. Otomatik her şeyi gözlemiyor.

Component (bileşenleri)

Basic Components 
CloudWatch Momtoring Detais 
Utilization (Percent) 
110% 120 12:10 12B 12*• 
Metrics: 
Metrics are the measurable data about your 
resources, apps or services like EC2 instance CPU utilization or 
the number of objects in an S3 bucket. 

Metrics: Biz EC2 ya gittiğimizde metric lerini zaten görüyoruz. Ancak CloudWatch da 200 tane instance bucket lar, vs. Hepsini gözlemleyebilmek mümkün. Yine sistem çöktüğünde nereye bakacağımızı bilmek için önceden ayarlanmış şekilde gözlem yapan CloudWatch a ihtiyacımız var.

Metric nedir?

Arabayı düşünelim, ön tarafta bir dashboard u var. Önümüdeki konsolda hangi birime göre ne göstermesi gerektiğine metrik denir. Örneğin hararet göstergesini C ya da F cinsinden, hız göstergesi km/h ya da m/h cinsinden verir. Hava basıncını farklı bir birimden. Bu ölçütlere metric deniyor.

Part 2 - Creating an Dashbord 
110 
220• 
R TEMP 120 

Metric ler grafik çizilerek verilen görselleştirilmesi için kullanılıyor. Odaklanmamız gerekn yeri bu sayede anlayabiliriz.

Dashboard:

Nasıl bir ön konsol istediğinizle alakalıdır. Ne görmek istiyorsak onunla ilgili widget ları koyarız.

6.94 
n*trc S 
144 
Dashboards: Dashboards enable you to create graphs and 
visualize your cloud resources and applications according to 
your needs. 

metncSOWr 
Logs table 
result; 
I n sights 
Stacked area 
C crnpwa total over 
iiå 
A stetLB 
Instantly the Status 
of a in a grid 
Number 
Instmtly Vatwt 
g metric 
with 
markdown 
Widgets: You can leverage dashboards as customizable home 
pages in the CloudWatch console to view metrics, logs and 
alarms. 

Widgetlar da göstergelerdir.

Diğer bir component Alarms tır. Örn hız 120 km/h geçerse haber ver gibi. Alarm lar action a da geçebilir. Event kadar değil ancak bir tetikleyici olarak harekete geçeriebilir.

AWS ser*zs summæy 0 
O grg 
alarrns o 
Alarms: Alarms enables you to monitor CloudWatch metrics and 
to receive notifications if the metrics fall outside of the thresholds 
(higher or lower) that you set. 
You can make Alarms trigger a Resource Actions 

Logs olmazsa olmaz. Logları human readable olarak gösterir. Filtreleme yapabiliriz.

aws 
GtouVE 
Log 
Dash boards 
Alarms 
T (Urc 
2019•0-1, 30 
E vents 
11±532 
I Logs 
I rsights 
Met'ics 
Setungs 
*euorites 
19xs:47 
Expand all Row 
2019++30 (1231105) • 
M Sage 
182.73.116.202- - Wc-al 200 o•.'indcv.s NT AppeweøK.vS3L3b 
- - "GET ; 11173 NT 36 (KHTv. 
• •ococl O 
+GacoJ 
IBC. 251.54 70 - - 200 11229 Intel Mac os X Apole,VebKit'601.7.7 
'coon] ; HTTP.f1.1' 700 11173 • NT 5 
- - -coco] as.d (Wncows w 
• • emcol "GET •uonila'sc Imo; 
- -COCO] "GET (Wit-dc-M MT to.c; 
•coca] "CET 
- - 'GET HTTP'I.I• dC4 'St •-0 WcZlIIa'S.d (Valdc•øs NT 10.0: Win64: : 
183.1786&143.. 
•r;FT 157 n NT too: : 
Logs: Logs let you monitor, store, and access your log files from 
AWS or other resources. It also allows you to centralize these 
logs for querying and analyzing. 

Events

Basic Com onents 
CloudWatch Events 
Schedule 
Expression 
I nstance 
Event 
CloudTraiI 
Targets 
Rules 
Events 
Amazon EventBridge 
Events: An event indicates changes in your AWS environment. You can 
create rules that self-trigger on an automated schedule. 
• Now it can be used in new service named "Amazon EventBridge" also. 

Alarmlara bir yönüyle benzer. Alarmda tetikleyen olay koyduğumuz bir eşiğin / limitin aşılmasıdır. Ancak Event bir takım olayları gözlemler.

SPEED 
LIMIT 
25 
CLARUSWAY 
Part 3 - Creating an Alarm 
Alarms 
- triggered by exceeding the limits 
- we watch out the limits 
can trigger 
00111[) 

Event te kaynakların hareketlerini izler. Bir schedule ( takvim ) de tetikleyici olabilir:

Part 4 - Creating an Event 
EVENTS 
can trigger Targets 
amazon 
web services 
(ICI@ 
Amazon 
API Gateway 
-triggered by changes in aws resource's status 
-we watch out the resource activity 

Events EventsBridge diye bir servise yönlendirildi.

Amazon 
aoudWatch 
AWS 
Re*l.jrces tat 
use CloudWatc:h 
Your custom 
SVR' 
Amazon 
CJoudWatch 
Available 
Statistics 
SNS email 
notification 
Auto Scaling 
AV.'S 
Managernent Console 
Statistics 
Consumer 

On-premise sistemleri de gözlemleyebilir CloudWatch. Gelen verileri analiz edebilir ya da Action alabilir. Event le oluşacak hareket ilgili şeyler olmak zorunda değil. S3 e bir obje yüklenmesi üzerine bambaşka bir action aldırabiliriz.

Metric lerde AWS nin kısıtlı tuttuğu kısımlar var. Memory gibi. Bunlar için de custom metric ler oluşturuluyor. Kendimizin bu metric lerini oluşturması gerekir. Bunlar operating systemle le ilgili metric lerdir. Çünkü AWS nin bu metricleri bizden alması gerekir.

HANDS ON a geçiyoruz.

Bir EC2 oluşturuyoruz ve advanced settingsten Detailed cloudwatch monitoring i açıyoruz. hands-on daki user datayı ekliyoruz.

Detailed CloudWatch monitoring Info 
Enable 
Additional charges apply 

user data - optional Info 
Enter user data in the field. 
#! /bin/bash 
yum update -y 
amazon-linux-extras install nginxl .12 
chkconfig nginx on 
cd /usr/share/nginx/html 
chmod 0+w /usr/share/nginx/html 
rm index. html 
wget https://raw.githubusercontent.com/awsdevopsteam/route- 
53/master/index.html 
wget https://raw.githubusercontent.com/awsdevopsteam/route- 
53/master/ken.jpg 
service nginx start\ 

User data da chkconfig, systemctl enable nginx etmenin eski hali.

service ngninx start da systemctl start nginx demek.

CloudWatch konsoluna gidiyoruz. Bir dashboard oluşturacaz. Create Dashboard diyoruz. İsim veriyoruz. Bize istediğimiz widget ları soruyor:

Add widget 
Select a widget type to add to the dashboard. 
Exp lorer 
A single widget with multiple 
tag-based graphs 
Gauge 
See the latest value of a 
metric within a lower and 
upper range 
Line 
Compare metrics over time 
Bar 
Compare categories of data 
Stacked area 
Compare the total over time 
Show percentage or 
proportional data 
x 
Number 
Instantly see the latest value 
and trend for a metric 
Custom widget - New 
Code widgets using Lambda 
and more 

Line / Metrics / EC2 / Per-Instance Metrics

Burada instance ımızın id sini yapıştırarak filtreliyoruz. Gelen seçeneklerden CPU utilization u seçiyoruz. Create Widget diyoruz:

Instance name 14/14 
geovanni_cloudwatch 
geovanni_cloudwatch 
geovanni_cloudwatch 
geovanni_cloudwatch 
Instanceld 
i-047000b8163029c8b 
i-047000b8163029c8b 
i-047000b8163029c8b 
Metric name 
DiskWriteOps 
MetadataNoToken 
CPUUtilization 
Networkln 
Cancel 
Create widget 

Başka bir widget eklemek için + ya batık.

Gauge / S3 / Storage Metrics / bir bucket için NumberofObjects seçtik.

Browse 
Query 
Graphed metrics (1) 
Options 
Source 
BucketName 4/4 
cf-templates-uzohjrtclyoa-us-east-l 
cf-templates-uzohjrtclyoa-us-east-l 
www.emreaydeniz.com 
v.ww.emreaydeniz.com 
StorageType 
AllStorageTypes 
StandardStorage 
AllStorageTypes 
StandardStorage 
Add math 
Metric name 
NumberOfObjects 
BucketSizeBytes 
NumberOfObjects 
BucketSizeBytes 
Cancel 
Add query 
Create widget 

Gösterge aralığı girip create widget diyoruz.

Browse 
Gauge range 
Min O 
Value 
Query 
Max 
Graphed metrics (1) 
2 
Options 
Source 
Add math 
O Latest value shows the value from the most recent period 
of your chosen time range. 
o 
Time range value shows the value from the entire time 
range. 
Cancel 
Add query 
Create widget 

Burada neyi izlemek istiyorsak onu widget olarak ekleyebiliyoruz. Save etmeden dashboard a kaydolmaz. Save ediyoruz.

CloudWatch Dashboards > 
em re-cloudwatch 
CPUUtilization 
Percent 
CPUUtiIization 
emre-cloudwatch 
N u mberOfObjects 
N u mbeOfObjects 
3h 
12h 
Custom 
Actions 
Save 

Dashboard u görmüş olduk.

CloudWatch > Dashboards 
(1) info 
Custom dashboards 
Custom Dashboards 
Q 
Filter dashboards 
Automatic dashboards 
Share dashboard 
Delete 
Create dashboard 
> 
Sharing 
Favorite 
o 
Name 
emre-cloudwatch 
Last update (UTC) 
2023-02-21 18:49 

Hands-on da ec2 ya stress yükleyip CPU utilization görme kısmı var ancak biz bunu atladık.

Alarms tan All Alarms a geliyoruz CW konsolda. Alarmlar Dashboard da sürekli görünmez, istediğimiz zaman görebiliriz.

Create Alarm / Select Metric / EC2 / Per-Instance Metrics

Browse 
Query 
No name specified 
No name specified 
No name specified 
No name specified 
No name specified 
Graphed metrics (1) 
Options 
Source 
i-01ebc6d6958b10375 
i-01ebc6d6958b10375 
i-01ebc6d6958b10375 
i-01ebc6d6958b10375 
i-01ebc6d6958b10375 
Add math 
CPUUtilization 
Networkln 
NetworkOut 
DiskReadBytes 
DiskWriteBytes 
Cancel 
Add query 
Select metric 

CPU Utilization seçip Select Metric diyoruz. Bizi böyle bir ekran karşılıyor:

Graph 
This alarm will trigger when the blue line goes above the red line for I datapoints within 5 minutes. 
60_5 
59.5 
17:00 
CPUUtiIization 
18:00 
Na mespace 
AWS/EC2 
Metric name 
CPUUti1ization 
Instanceld 
i-01ebc6d6958b10375 
Instance name 
19:00 
No name specified 
Statistic 
Q Average 
Period 
5 minutes 

5 dk lık periyotlarla görselleştiriyor. 5 dk boyunca ortalaması.

Greater 
> threshold 
than... 
Define the threshold value. 
60 
Must be a number 

CPU kullanımı %60 tan fazla olursa demek. Additional configuration a basıyoruz.

Additional configuration 
Datapoints to alarm 
Define the number of datapoints within the evaluation period that must be breach 
3 
out of 
4 
Missing data treatment 
How to treat missing data when evaluating the alarm. 
Treat missing data as missing 

Bu ayar her 5 dk lık periyotların ¾ ünde % 60 ı geçerse demektir. Biz 1 / 1 olarak ayarlayıp Next diyoruz.

Action alalım mı diye soruyor bu sayfada.

Alarm state trigger 
Define the alarm state that will trigger this action. 
O In alarm 
The metric or expression is 
outside of the defined 
threshold. 
o 
OK 
The metric or expression is 
within the defined threshold. 
Remove 
o 
Insufficient data 
The alarm has just started or 
not enough data is available. 

Alarm durumunda, her şey normal olduğu durumda, veri alamadığı durumlarda. Veri alamamanın içinde hiçbir veri olmadığı için alamadığı durumlar da dahildir.

Alarm ın yeni bir başlıkla gelmesini istedik ve bir başlık ismi vererek alt tarafa hangi mail adresine bildirim göndermesini istiyorsa o mail adresini giriyoruz.

Send a notification to the following SNS topic 
Define the SNS (Simple Notification Service) topic that will receive the notification. 
o 
Select an existing SNS topic 
O Create new topic 
C) Use topic ARN to notify other accounts 
Create a new topic... 
The topic name must be unique. 
cloudwatch-alarm-l 
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores 
Email endpoints that will receive the notification.. 
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above. 
user@example.com 

Create Topic diyoruz. Mesajın içeriğini düzenleyemeyiz sadece başlığı düzenleyebiliyoruz. Maile bir bildirim gelmesi gerekiyor bu adımdan sonra.

You have chosen to subscribe to the topic: 
arn:aws:sns:us-east-1:gg5714465210:doudwatch-alarm-1 
To confirm this subscription, click or visit the link below (If this was in error no action is necessary): 
Confirm subscription 
do not reptv this If wish to SNS Ænd email 

Confirm subscription a tıklamamız gerekiyor. Alarmı confirme etmiş oluyoruz.

aws 
Subscription confirmed! 
You have successfully subscribed. 
Your subscription's id is: 
Simple Notification Service 
arn : : sns : us -east-I : 995714465210 : cloudwatch- alarm-I : aadS17ac-7acI-4gca- 
b133-abaab772gaæ 
If it was not your intention to subscribe, click here to unsubscribe. 

Auto Scaling action 
Add Auto Scaling action 
EC2 action 
Add EC2 action 
Systems Manager action Info 
This action will create an Incident or Opsltem in Systems Manager when the alarm is In alarm state. 

Buradan action ekleyebiliyoruz. Biz EC2 actions a geliyoruz.

EC2 action 
Alarm state trigger 
Define the alarm state that will trigger this action. 
O In alarm 
The metric or expression is 
outside of the defined 
threshold. 
Take the following action... 
o 
OK 
The metric or expression is 
within the defined threshold. 
Remove 
o 
Insufficient data 
The alarm has just started or 
not enough data is available. 
Define what will happen to the EC2 instance with the Instance ID i-OIebc6d6gS8b10375 when this alarm is triggered. 
Recover this instance 
You can only recover certain EC2 instance types. See documentation 
O Stop this instance 
You can only stop an instance if it is backed by an EBS volume. AWS will use the existing Service Linked Role 
(AWSServiceRoIeForCIoudWatchEvents) to perform this action. Show IAM policy document 
o 
Terminate this instance 
You will not be able to terminate this instance if termination protection is enabled. AWS will use the existing Service Linked Role 
(AWSServiceRoIeForCIoudWatchEvents) to perform this action. Show IAM policy document 
o 
Reboot this instance 

Alarm geldiğinde makineyi stop et seçeneğini seçiyoruz. Reboot ya da terminate edebiliyor. Next deyip alarma isim veriyoruz:

![Add name and description 
Name and description 
Alarm name 
emre-EC2-alarm 
Alarm description - optional View formatting guidelines 
Edit 
Preview 
# This is an HI 
"double asterisks will produce strong character'* 
This is [an example](https://example.com/) inline link. ](data:image/png;base64,)

Next deyip gelen sayfada Creat alarm diyoruz.

Şimdi EC2 ya bağlanıp stres yükleyecez.

sudo amazon-linux-extras install epel -y 
sudo yum install -y stress 
--cpu 8e --timeout 2eeoø 
stress 

Stres yükleme komutları. Stresi yükledik:

[ec2-user@ip-172-31-53-98 stress 
--cpu 2øø --timeout 2øøøø 
stress: info: [3792] dispatching hogs: 2øø cpu, io, vm, hdd 

Hızlı sonuç almak için --cpu 200 olarak güncelledik.

CloudWatch taki widget ımız duruyorsa oradan ya da EC2 instance altında monitoring ten CPU Utilization a gelerek grafiği izleyebiliriz.

Alarm için mail gelecektir. Ve instance ı stop edecektir.

CPU kullanımı:



EC2 üzerinde çalışacağımız için alarm ı simemiz gerekiyor:

CloudWatch > Alarms 
Alarms (1/2) 
Q Search 
Name 
emre-EC2-alarm 
Billing Alarm 
Hide Auto Scaling alarms 
State 
Insufficient data 
Clear selection 
Any state 
Last state update 
2023-02-21 
2023-02-09 182932 
Create composite alarm 
Actions A 
Edit 
Copy 
Delete 
Create alarm 
V 
Any type 
Conditions 
Any a 
CPUUtilization > 60 for 1 datapoints 
minutes 
EstimatedCharges 7 for 1 datapo 
hours 
Add to dashboard 
Alarm actions - new 

Seçip Actions tan delete dediğimizde silinir.

Biz scheduled bir event oluşturacağız. Saat ile. Servisleri baz almayacaz.

- everyday 7:00 am 
Part 4 - Creating an Events with Lambda-2 
- everyday 18:00 pm 

Örneğin sabah 7 de bütün instance lar açılsın, akşam 6 da bütün instance lar kapansın. Bunu otomatize etmek istiyoruz. Event saati gözleyecek, Lambda yı tetikleyecek, action u Lambda yapacak.

Bunun için boto3 olmalı çünkü pyhton diliyle AWS servislerini yöneteceğiz.

Lambda ya rol vermemiz lazım çünkü AWS servisi için yetki lazım.

Event Rule 
Lambda 
Start 
Role 
Part 4 - Creating an 
Events with 
Lambda-2 
policy 
Start 
rule 
Stop 
ru e 
Stop 

Bu görev için bir custom IAM role policy miz var hands-on da. IAM konsola gidip Roles a gelelim. Create role deyip Lambda yı seçiyoruz:

(Hocamız derste önce policy oluşturdu sonra role oluştururken bu policy yi kullandı)

O 
AWS service 
Allow AWS services like 
EC2, Lambda. or others to 
perform actions in this 
account 
o 
SAML 20 federation 
Allow users federated with 
SAML 2.0 from a corporate 
directory to perform actions 
in this account 
use case 
o 
o 
AWS account 
Allow entities in other AWS 
accounts belonging to you or 
a 3rd party to perform 
actions in this account. 
Custom trust policy 
Create a custom trust policy 
to enable others to perform 
actions in this account. 
o 
Web identity 
Allows users federated by 
the specified external web 
identity provider to assume 
this role to perform actions in 
this account 
Allow an AWS service like EC2, Lambda, or others to perform actions in this account 
Common use cases 
o 
EC2 
Allows EC2 instances to call AWS services on your behalf. 
O Lambda 
Allows Lambda functions to call AWS services on your behalf 
use cases for other AVVS services: 

Create policy diyoruz, JSON u seçip policy i yapıştırıyoruz:

Create policy 
A policy defines the AWS permissions that you can assign to a user, group, or role. You can 
Visual editor 
JSON 
"Version : 
1 
2 
4 
6 
7 
8 
9 
10 
11 
Securitv O 
"2012-10-17", 
"Statement " : 
"Effect": 
"Allow" , 
"Action " : 
" logs : CreateLogGroup " 
" logs : CreateLogStream" , 
" logs : Put LogEvents " 
"Resource' 
" arn : aws : logs . 
O Errors: O Warnings: 0 Q Suggestions: O 

İsim verip create diyoruz. Daha sonra Role isim verip role oluşturuyoruz.

(Hocamız derste önce policy oluşturdu sonra role oluştururken bu policy yi kullandı)

Lambda konsoluna gidiyoruz. Create Function diyoruz.

Basic information 
Function name 
Enter a name that describes the purpose of your function. 
Stop_lnstance 
use only letters, numbers, hyphens, or underscores with no spaces. 
Runtime Info 
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby. 
Python 3.9 
Architecture Info 
Choose the instruction set architecture you want for your function code. 
O x86_64 
o 
arm64 
Permissions Info 
By default, Grnbda will an with to u*æd logs to ClmldWätch Gn this .dding triggers 

Ayarları yukarıdaki gibi yapıyoruz.

Change default execution role 
Execution role 
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console 
o 
Create a new role with basic Lambda permissions 
O use an existing role 
o 
Create a new role from AWS policy templates 
Existing role 
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs. 
Emre-Role-For-Lambda 
View the Emre-RoIe-For-Lambda role on the IAM console. 
c 

Role u existing role den seçiyoruz ve create diyoruz.

Code Source a gelip burayı temizliyoruz hands-on daki function codu nu buraya yapıştırıyoruz. Instance id yi değiştirmeyi unutmuyoruz. Deploy ediyoruz.

Tools 
4 
Window 
lambda function 
import bot03 
- 'us -east-I' 
region - 
Deploy 
= ['i-e47øeeb8163a29c8bl' FORGET TO CHANGE ME 
instances 
ec2 = bot03.cIient( , 
def context) : 
ec2 . stop_instances (Instancelds=instances) 
print(' stopped your instances: ' 
+ str(instances)) 

Test edelim:

To invoke your function without saving an event, configure the JSON event, then choose Test. 
Test event action 
O Create new event 
Event name 
Stopinstance 
Edit saved event 
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores. 
Event sharing settings 
O Private 
This event is only available in the Lambda console and to the event creator. You can configure a total of 10. Learn more 
C) Shareable 
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more 
Template - optional 
hello-world 
Event JSON 
Format JSON 

Save dedik Test e bastık:

Tools 
Window 
lambda function x 
Deploy 
Execution result 
• Execution results 
Test Event Name 
Stopins tance 
Response 
Function Logs 
START Reguestld: dffa7114-ef7a-4317-86b2-3ca64e773edf Version: SLATEST 
stopped your instances : 
ENO Requestld: dffa7114-ef7a-4317-86b2-3ca64e773edf 
REPORT Requestld: dffa7114-ef7a-4317-86b2-3ca64e773edf Duration: 504.30 ms Bi: 
Request 10 
dffa7114-ef7a-4317-86b2-3ca64e773edf' 

Instance ımızı stop ett:

(I) Info 
Instances 
Q Find instance by attribute or tag (case-sensitive) 
Name 
v Instance ID 
geovanni_cloudwa... 
i-047000b8163029c8b 
c 
Connect 
Instance state v 
@ Stopping 
Insta 
Instance 
t2. micro 

Şimdi start edecek fonksiyonu girelim. Yeni bir function create ediyoruz.

Tools 
4 
Window 
lambda function 
import bot03 
- 'us -east-I' 
region - 
Deploy 
= ['i-e47øeeb8163a29c8b" 
instances 
ec2 = bot03.cIient( 'ec2', 
def context) : 
ec2 . start_ins tan ces(lnstancelds =instances) 
print(' started your instances: ' 
+ str(instances)) 

instance id yi değiştirdikten sonra Deploy ediyoruz. Test edecez.

Test için eventi oluşturup save dedik ve test butonuna bastık. Instance start edildi:

(I) Info 
Instances 
Q Find instance by attribute or tag (case-sensitive) 
Name 
v Instance ID 
geovanni_cloudwa... 
i-047000b8163029c8b 
c 
Connect 
Instance state 
@ Running 

Şimdi Lambda functionlar da hazır. Şimdi CloudWatch ta Event-rule oluşturacaz. CloudWatch ta Events altında Rules a gidiyoruz. Bizi EventBridge servisine gönderdi.

Create rule diyoruz.

İsim veriyoruz. (event bus birkaç rules için kullanılır. advanced bir konudur.)

Biz resource larla ilgili değil zamana ayarlı rule oluşturacaz.

Name 
em restop 
Maximum of 64 characters consisting of numbers, lower/upper case letters, 
Description - optional 
Enter description 
Event bus Info 
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus. 
default 
Enable the rule on the selected event bus 
Rule type Info 
C) Rule with an event pattern 
A rule that runs when an event matches the defined 
event pattern. EventBridge sends the event to the 
specified target 
O Schedule 
A rule that runs on a schedule 

**Continue to create rule** a basıyoruz.

Burada zamanları nasıl ayarlayabileceğimizi görüyoruz.

Schedule pattern 
Occurrence Info 
You can define an one-time or recurrent schedule. 
O One-time schedule 
Date and time 
The date and time to invoke the target. 
YYYY/MM/DD 
YYW/MM/DD 
(UTC +01 :OO) Europe/Stockholm 
Timezone 
Flexible time window 
C) Recurring schedule 
hh:mm 
Use 24-hour format timestamp (hh:mm) 
If you choose a flexible time window, Scheduler invokes your schedule within the time window specify. For 
example, if you choose IS minutes, your schedule runs within IS minutes after the schedule start time. 
Select 

Dokümantasyonda detaylar ve örnekler var:

Cron expressions that lead to rates faster than 1 minute are not supported. 
Examples 
You can use the following sample cron strings when creating a rule with schedule. 
Minutes 
15 
Hours 
10 
12 
18 
Day of 
month 
Month 
Day 
of 
week 
MON- 
FRI 
Year 
Meaning 
Run at 10:00 
am ( 
+0) 
every d 
Run at 12:15 
pm (UTC+O) 
every day 
Run at 6:00 
pm (UTC+O) 
every Monday 
through Friday 

Programı bu şekilde ayarladık:

Schedule pattern 
Schedule pattern 
Choose the schedule type that best meets your needs. 
O A fine-grained schedule that runs at a 
specific time, such as 8:00 a.m. PST on 
the first Monday of every month. 
Cron expression Info 
Define the cron expression for the schedule 
C) A schedule that runs at a regular rate, 
such as every 10 minutes. 
Cro 15 
Minutes 
Next 10 trigger 
date(s) 
20 
Hours 
Day of month 
Month 
Day of week 
Year 
Local time zone 

Target types 
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target. 
o 
EventBridge event bus 
o 
EventBridge API destination 
O AWS service 
Select a target Info 
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 
targets per rule) 
Lambda function 
Function 
Stop_lnstance 
Configure version/alias 
Additional settings 
Cancel 
Skip to Review and create 
Previous 
c 
Next 

AWS service lerini seçiyoruz. Lambda function u target olarak seçtik ve stop etmesini istediğimiz için stop\_instance function unu seçtik. Next - Next Create Rule diyoruz.

Saat 15 geçe instance stop oluyor:

(I) Info 
Instances 
Q Find instance by attribute or tag (case-sensitive) 
Name 
v Instance ID 
geovanni_cloudwa... 
i-047000b8163029c8b 
C 
Connect 
Instance state 
Actions 
Status check 
Instance state 
@ Stopping 
Instance type 
t2. micro 
V 

Aynı işlemleri start etme için yapalım.

Create rule a basıp schedule ile devam ediyoruz.

Enter description 
Event bus Info 
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus. 
default 
C) Enable the rule on the selected event bus 
Rule type Info 
C) Rule with an event pattern 
A rule that runs when an event matches the defined 
event pattern. EventBridge sends the event to the 
specified target. 
O Schedule 
A rule that runs on a schedule 
EventBridge Scheduler - A new AWS scheduling capability! 
A new EventBridge scheduling functionality that provides one-time and recurring scheduling functionality independent 
of Event buses and rules. You can create a schedule to invoke targets such as a Lambda function. 
Learn More 
Continue to create rule 
Cancel 
Continue in EventBridge Scheduler 

Sol alttaki butonla devam ediyoruz.

Schedule pattern 
Schedule pattern 
Choose the schedule type that best meets your needs. 
O A fine-grained schedule that runs at a specific 
time, such as 8:00 a.m. PST on the first Monday 
of every month. 
Cron expression Info 
Define the cron expression for the schedule 
C) A schedule that runs at a regular rate, such as 
every 10 minutes. 
cron( 19 
Minutes 
Next 10 trigger date(s) 
21 
Hours 
UTC 
Day of month 
Month 
Day of week 
Year 
Tue, 21 Feb 2023 UTC 
wed, 22 Feb 2023 UTC 
Thu, 23 Feb 2023 UTC 

Target seçiyoruz:

Target types 
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target. 
o 
EventBridge event bus 
o 
EventBridge API destination 
O AWS service 
Select a target Info 
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule) 
Lambda function 
Function 
Start-instance 
Configure version/alias 
Additional settings 
Add another target 
Cancel 
Skip to Review and create 
Previous 
c 
Next 

Çalıştığını gördük.

Eventleri delete edelim.

Son örneğimiz loglarla ilgili.

AWS de Logs için bize Log grupları oluşturuyor. Sol menüden Log Groups a geliyoruz.

CloudWatch un Lambda ile instance ları start stop edebilmesi için oluşturduğumuz policy nin de loglarını burada görebiliyoruz.

Log group 
/aws/lambda/emreapigteway 
/aws/lambda/geovanni 
/aws/lambda/gevoanni2 
/aws/lambda/start-instance 
/aws/lambda/stop_lnstance 



AWS ya da on-premise teki log ları almak istiyoruz. Instance taki logları şuradan alabiliriz:

(1/1) Info 
Instances 
Q Find instance by attribute or tag (case-sensitive) 
Name 
v Instance ID 
geovanni_cloudwa... 
i-047000b8163029c8b 
c 
Connect 
Instance state 
Actions A 
Connect 
View details 
Launch instances 
Instance stat 
@ Running 
Instance: i-047000b8163029c8b (geovanni_cloudwatch) 
Get system log 
Get instance screenshot 
Manage detailed monitoring 
Manage CloudWatch alarms 
EC2 serial console 
Replace root volume 
Fleet Manager 
Manage instance state 
Instance settings 
Networking 
Security 
Image and templates 
Monitor and troubleshoot 
Details 
Security 
Networking 
Storage 
Status checks 

Sistem loglarını alabiliyoruz. Peki içinde çalışan nginx loglarını nasıl alacağız?

LOGS 
CloudWatchAgent 
Part 5 - Creating Agent 
Amazon CloudWatch 
instance logs 
NGMX 
1. 
2. 
access logs of nginx 
error logs of nginx 

AWS nin bize verdiği loglar kendi sorumlu olduğu loglar. Biz kendi yüklediğimiz şeylerle ilgili logları agent la alacaz. agent CloudWatch a ajanlık yapıyor.

Bu işlem için yani EC2 nun agent ile CloudWatch a bilgi aktarabilmesi için role ihtiyacı var.

(Lambdadaki function ları silebiliriz bu arada) Policy hazır olduğu için direk IAM de roles a gidiyoruz.

AWS Service / EC2 yu seçerek Next diyoruz. Policy seçiyoruz:

Add permissions 
Permissions policies (Selected 1/818) 
Choose one or more policies to attach to your new role. 
Q 
Filter policies by property or po/jcy name and press enter 
"cloudwatchtullaccess" X 
Policy name 
CloudWatcnFullAcc_ 
Clear tilters 
Type •7 
AWS 
Description 
Provides full access to CloudWatcn_ 

İsim verip create diyoruz:

Role details 
Role name 
Enter a meaningful name to identity this role. 
emre-cloudwatcn-tull-accessl 
Maximum 64 characters use alphanumeric and '*z, @- 
Description 
Add a short explanation for this role 
' characters. 
Allows EC2 instances to call AWS services on your behalf. 
Maximum 1000 characters. use alphanumeric and 
Step 1: Select trusted entities 
characters 

Şimdi instance a gidip role modify edecez. Bir instance a bir role tanımlayabiliriz. Fazla görev vermek istiyorsak role e policy leri ekeyecez.

(1/1) Info 
Instances 
Q Find instance by attribute or tag (case-sensitive) 
Name 
v Instance ID 
geovanni_cloudwa.. 
i-047000b8163029c8b 
Connect 
Instance state 
@ Running 
Instance state 
Actions A 
Connect 
View details 
s 
Launch instances 
Instance type 
t2. micro 
v 
Change security groups 
Get Windows password 
Modify IAM role 
Manage instance state 
Instance settings 
Networking 
Security 
Image and templates 
Monitor and troubleshoot 
Instance: i-047000b8163029c8b (geovanni_cloudwatch) 

Drop down menüden rolu seçip update ediyoruz:

EC2 > Instances > i-047000b8163029c8b > 
Modify IAM role Info 
Attach an IAM role to your instance. 
Instance ID 
Modify IAM role 
i-047000b8163029c8b (geovanni_cloudwatch) 
IAM role 
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are 
currently attached to your instance. 
em re-cloudwatch-full-access 
Create new IAM role 
Cancel 
Update IAM role 

Şimdi tekrar instance a bağlanalım.

sudo yum install -y awslogs 
sudo systemctl start awslogsd 
sudo systemctl enable awslogsd. 
rv1ce 

bu kodlarla cloudwatch agent ı instance a yüklüyoruz. Şimdi CloudWatch log groups ta instance a ait log grubu da görüyoruz:

CloudWatch Log groups 
Log groups (6) 
By default, we only load up to 10000 log groups. 
Q Filter log groups or try prefix search 
Log group 
/aws/lambda/emreapigteway 
/aws/lambda/geovanni 
/aws/lambda/gevoanni2 
/aws/lambda/start-instance 
/aws/lambda/stop_lnstance 
var/log/messages 
Data Prot... 
e Inactive 
e Inactive 
e Inactive 
e Inactive 
e Inactive 
e Inactive 

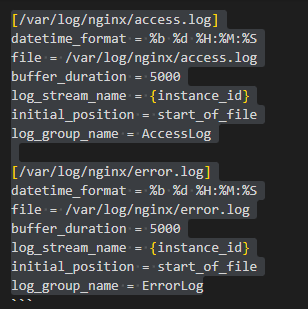
sudo su ile root a geçiyoruz

cd /etc/awslogs/

komutu ile awslogs içine giriyoruz.

vi awslogs.conf

ile editöre gidip ayarlamalar yapacağız. Biz şu anda bunu EC2 da yapıoruz ancak bunu on-premise te de yapabiliriz bu yöntemle agent kullanarak.

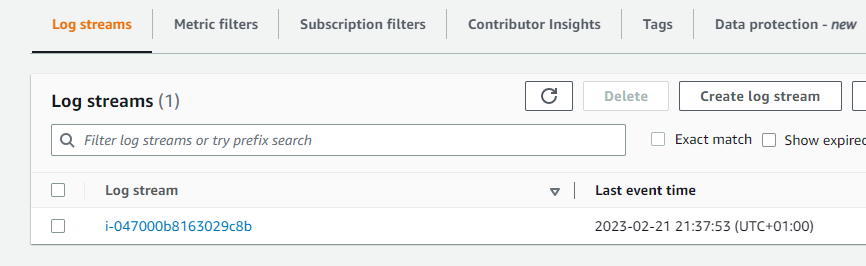


bu kodları editörün en altında yapıştırdık. bundan önce sadece sistem loglarını cloudwatch a gönderirken şimdi nginx loglarını da gönderecek. kaydedip çıkıyoruz.

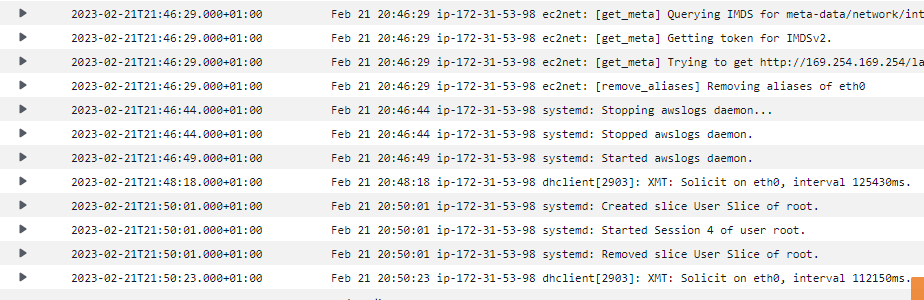
yeni ayarların geçerli olması için stop start yapıyoruz şu komutlarla:



Şimdi nginx le ilgili log kaydı oluşabilmesi için instance ın public adresini alıp browserda açalım sitemizi. log kayıtlarını görebilmek için Log stream üzerine tıklıyoruz:



Burada log kayıtlarımız:



Custom metrics lere kendimiz bakalım.

Temizli yapabiliriz. (EC2 yu silmek yeterli) Alarmları, Event rules ları silmiştik zaten.