

# Roteiro 4 - Integração com Telegram e CloudWatch

---

## Cyber Segurança em Nuvem 2024.1

Grupo: Antônio Martins, Ariel Leventhal e Enricco Gemha

### Introdução

Este roteiro tem como objetivo melhorar as medidas de segurança do ambiente nuvem da ABCPLACE, através da utilização de ferramentas como o Zabbix e Wazuh, que irão ser integrados com o Telegram, para envio de alertas, e com o CloudWatch, para monitoramento de logs.

### 1. Integração com Telegram

#### 1.0 Criação de Bot no Telegram

Para a integração do Zabbix com o Telegram, é necessário criar um bot no Telegram, utilizando o serviços do BotFather, que irá fornecer um token de acesso para o bot.

Com o bot criado, o mesmo deverá ser adicionado a um grupo de Telegram com os Administradores do Sistema, neste caso, os integrantes do grupo.



# Group Info



**Cbsec**

3 members



Notifications



**Members**

**Links**



Antonio Martins  
last seen 1 minute ago



Ariel Tamezgui Leventhal  
last seen recently

owner



cbsec  
bot

admin

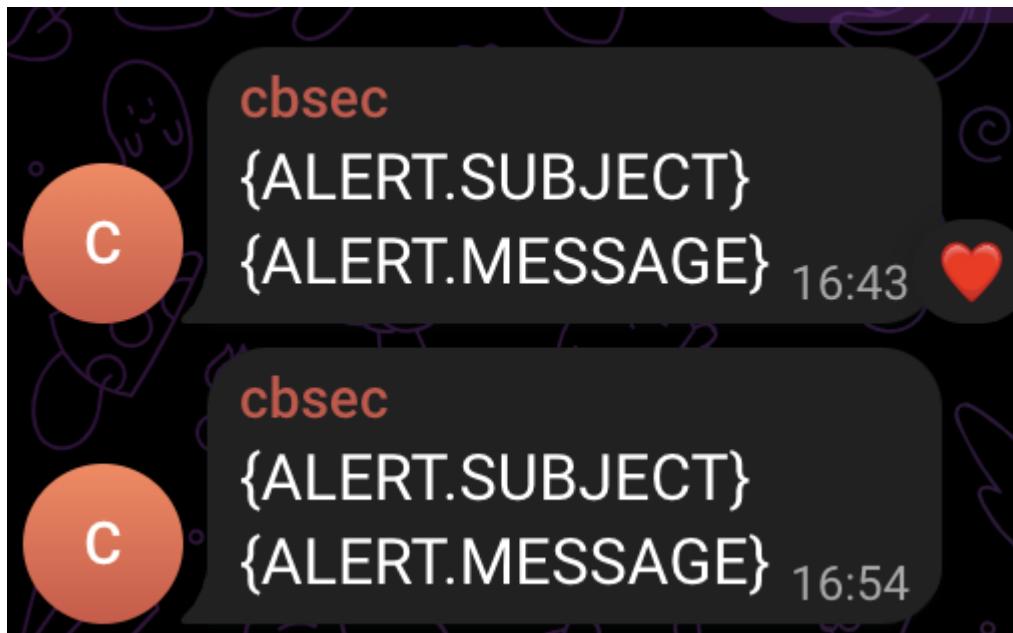
## 1.1.0 Criação de Media Types

Para a integração do Zabbix com o Telegram, é necessário criar um novo tipo de mídia, que irá permitir o envio de mensagens para o Telegram.

The screenshot shows the 'Media types' configuration screen in Zabbix. A new media type named 'Telegram' is being created. The 'Type' is set to 'Webhook'. The 'Parameters' section contains five entries: 'Message' with value '{ALERT.MESSAGE}', 'ParseMode' (empty), 'Subject' with value '{ALERT.SUBJECT}', 'To' with value '-4129271123', and 'Token' with value '7113025913:AAHaC4LcuiD8LFqC'. Below these parameters is an 'Add' button. The 'Script' field contains a placeholder script: 'var Telegram = { ... }'. The 'Timeout' is set to '10s'. Under 'Process tags', there is a checkbox which is unchecked. The 'Include event menu entry' checkbox is also unchecked. The 'Menu entry name' and 'Menu entry URL' fields are empty. The 'Description' field contains a link to the Zabbix GitHub repository and instructions: '1. Register bot: send "/newbot" to @BotFather and follow instructions  
2. Copy and paste the obtained token into the "Token" field above  
3. If you want to send personal notifications, you need to get chat id of the user you want to send messages to:'. The 'Enabled' checkbox is checked. At the bottom are 'Update', 'Clone', 'Delete', and 'Cancel' buttons.

É importante destacar que o Token utilizado é o mesmo token recebido pelo BotFather, e o **To** é referente ao identificador único do grupo de Telegram.

Para verificar se a integração foi feita corretamente, é possível enviar uma mensagem de teste.



### 1.1.1 Adição de Media em Usuário Administrador

Será configurado no usuário administrador do Zabbix a nova mídia criada.

| Username | Name   | Last name     | User role        | Groups                | Is online?                | Login | Frontend access | API access | Debug mode | Status  |
|----------|--------|---------------|------------------|-----------------------|---------------------------|-------|-----------------|------------|------------|---------|
| Admin    | Zabbix | Administrator | Super admin role | Zabbix administrators | Yes (2024-05-14 17:27:23) | OK    | System default  | Enabled    | Disabled   | Enabled |
| email    |        |               | Guest role       | Guests                | No                        | OK    | Internal        | Disabled   | Disabled   | Enabled |

User    Media 1    Permissions

| Media | Type     | Send to    | When active     | Use if severity | Status  | Action      |
|-------|----------|------------|-----------------|-----------------|---------|-------------|
|       | Telegram | 4129271123 | 1-7,00:00-24:00 | N I W A H D     | Enabled | Edit Remove |
| Add   |          |            |                 |                 |         |             |

Update    Delete    Cancel

**Media**

Type **Telegram**

\* Send to **4129271123**

\* When active **1-7,00:00-24:00**

Use if severity  Not classified  
 Information  
 Warning  
 Average  
 High  
 Disaster

Enabled

**Update** **Cancel**

### 1.1.2 Zabbix Actions

Para que o Zabbix envie mensagens para o Telegram, é necessário criar uma nova ação, que irá ser acionada quando um alerta for disparado.

| Name  | Status | Any | Enabled  | Disabled       |
|---|--------|-----|--|----------------|
|   |        |     | <b>Apply</b>   | <b>Reset</b>   |
| <b>Operations</b>   |        |     |  |                |
| <input type="checkbox"/> Name ▲                                   |        |     |  | <b>Status</b>  |
| <input type="checkbox"/> Report problems to Zabbix administrators |        |     | <b>Send message to user groups: Zabbix administrators via all media</b><br><b>Send message to users: Admin (Zabbix Administrator) via Telegram</b><br><b>Send message to user groups: Zabbix administrators via Telegram</b> | <b>Enabled</b> |
| Displaying 1 of 1 found   |        |     |  |                |

Action Operations 4

\* Default operation step duration 1h

Operations Steps Details Start in Duration Action

|   | Steps Details   | Start in    | Duration | Action                                      |
|---|---|-------------|----------|---|
| 1 | <b>Send message to user groups:</b> Zabbix administrators via all media | Immediately | Default  | <a href="#">Edit</a> <a href="#">Remove</a> |
| 1 | <b>Send message to users:</b> Admin (Zabbix Administrator) via Telegram | Immediately | Default  | <a href="#">Edit</a> <a href="#">Remove</a> |
|   | <b>Send message to user groups:</b> Zabbix administrators via Telegram  |             |          |   |

Add

Recovery operations Details Action

|  | Details   | Action                                      |
|--|---|---|
|  | <b>Notify all involved</b>  | <a href="#">Edit</a> <a href="#">Remove</a> |
|  | <b>Send message to users:</b> Admin (Zabbix Administrator) via Telegram | <a href="#">Edit</a> <a href="#">Remove</a> |
|  | <b>Send message to user groups:</b> Zabbix administrators via Telegram  | <a href="#">Edit</a> <a href="#">Remove</a> |

Add

Update operations Details Action

|  | Details | Action |
|--|---------|--------|
|  |         |        |

Pause operations for suppressed problems

Notify about canceled escalations

\* At least one operation must exist.

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

### 1.1.3 Teste de Integração com Telegram

Para testar a integração com Telegram, serão deslizadas a máquina do MySql, que irá disparar um alerta no Zabbix.

**cbsec**

Problem: Linux: MySQL-Instance has been restarted (uptime < 10m)

Problem started at 17:00:32 on 2024.05.14

Problem name: Linux: MySQL-Instance has been restarted (uptime < 10m)

Host: MySQL-Instance

Severity: Warning

Operational data: 00:00:44

Original problem ID: 226

17:00

Resolved in 5m 0s: Linux: Zabbix agent is not available (for 3m)

Problem has been resolved in 5m 0s at 17:00:58 on 2024.05.14

Problem name: Linux: Zabbix agent is not available (for 3m)

Host: MySQL-Instance

Severity: Average

Original problem ID: 225

17:01

Problem: Linux: Zabbix agent is not available (for 3m)

Problem started at 17:02:36 on 2024.05.14

Problem name: Linux: Zabbix agent is not available (for 3m)

Host: Wordpress-Instance

Severity: Average

Operational data: not available (0)

Original problem ID: 232

17:02

Com isso é possível verificar que os alertas estão funcionando, no decorrer desta atividade, foram feitos outros testes, com outras instâncias, o que gerou outros alertas:

**cbsec**

Resolved in 9m 20s: Linux: MySQL-Instance has been restarted (uptime < 10m)

Problem has been resolved in 9m 20s at 17:09:52 on 2024.05.14

Problem name: Linux: MySQL-Instance has been restarted (uptime < 10m)

Host: MySQL-Instance

Severity: Warning

Original problem ID: 226

Original problem ID: 220

17:09

**cbsec**

Problem: Linux: Wordpress-Instance has been restarted (uptime < 10m)

Problem started at 17:28:30 on 2024.05.14

Problem name: Linux: Wordpress-Instance has been restarted (uptime < 10m)

Host: Wordpress-Instance

Severity: Warning

Operational data: 00:01:41

Original problem ID: 234

17:28

Resolved in 26m 0s: Linux: Zabbix agent is not available (for 3m)

Problem has been resolved in 26m 0s at 17:28:36 on 2024.05.14

Problem name: Linux: Zabbix agent is not available (for 3m)

Host: Wordpress-Instance

Severity: Average

Original problem ID: 232

17:28

**cbsec**

Problem: Linux: Zabbix agent is not available (for 3m)

Problem started at 17:30:58 on 2024.05.14

Problem name: Linux: Zabbix agent is not available (for 3m)

Host: MySQL-Instance

Severity: Average

Operational data: not available (0)

Original problem ID: 240

17:31

**cbsec**

Problem: Linux: MySQL-Instance has been restarted (uptime < 10m)

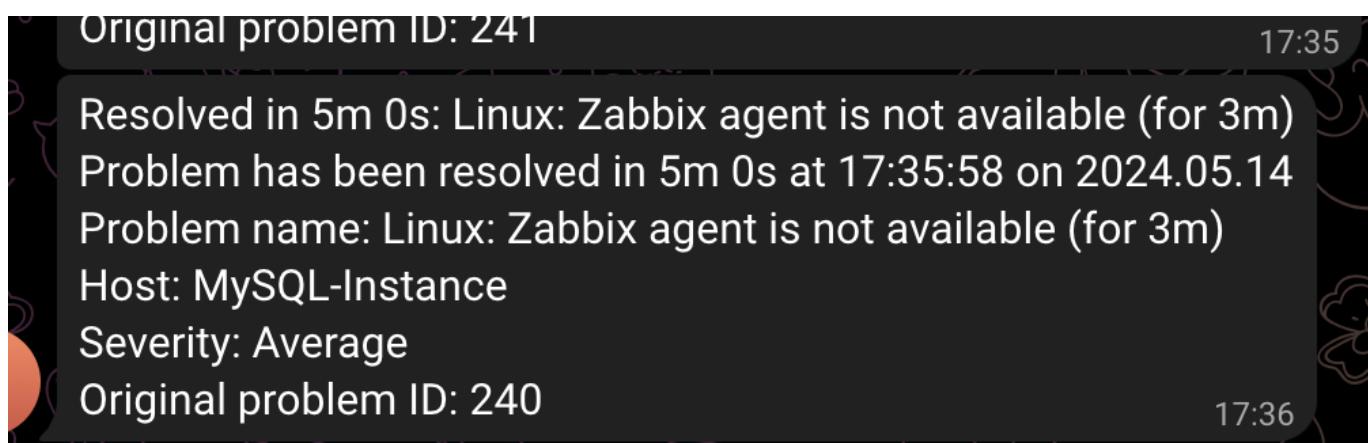
Problem started at 17:35:47 on 2024.05.14

Problem name: Linux: MySQL-Instance has been restarted (uptime < 10m)

Host: MySQL-Instance

Severity: Warning

Operational data: 00:01:06



## 2. Integração com CloudWatch

### 2.1 Configuração do CloudWatch para o Wazuh

Conforme solicitado, instalou-se e configurou-se os agentes do CloudWatch para enviar logs das instâncias ao serviço titular. Verifica-se isto nas screenshots a seguir:

```
amazon-cloudwatch-agent.deb      wazuh-agent_4.7.3-1_amd64.deb.1  'yslogd: Configuration error. Exiting'
awslogs-agent-setup.py          wazuh-install-files.tar           zabbix-release_3.0-2+bionic_all.deb
wazuh-agent_4.7.3-1_amd64.deb   wazuh-install.sh
root@ip-172-31-0-142:/home/ubuntu# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json -s
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_amazon-cloudwatch-agent.json.tmp
Start configuration validation...
2024/05/16 00:27:28 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_amazon-cloudwatch-agent.json.tmp ...
2024/05/16 00:27:28 I! Valid Json input schema.
2024/05/16 00:27:28 Configuration validation first phase succeeded
I! Detecting run_as_user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service → /etc/systemd/system/amazon-cloudwatch-agent.service.
root@ip-172-31-0-142:/home/ubuntu# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a status
{
  "status": "running",
  "starttime": "2024-05-16T00:27:30+00:00",
  "configstatus": "configured",
  "version": "1.300039.0b612"
}
root@ip-172-31-0-142:/home/ubuntu#
```

```

root@ip-172-31-0-142:/home/ubuntu# cd /opt/aws/amazon-cloudwatch-agent/etc/
root@ip-172-31-0-142:/opt/aws/amazon-cloudwatch-agent/etc# ls -la
total 28
drwxr-xr-x 3 root root 4096 May 16 01:18 .
drwxr-xr-x 7 root root 4096 May 16 00:27 ..
drwxr-xr-x 2 root root 4096 May 16 00:27 amazon-cloudwatch-agent.d
-rw-r--r-- 1 root root 1008 May 16 00:27 amazon-cloudwatch-agent.toml
-rw-r--r-- 1 root root 959 May 3 22:43 common-config.toml
-rw-r--r-- 1 root root 2 May 16 00:27 env-config.json
-rw-r--r-- 1 root root 85 May 16 00:27 log-config.json
root@ip-172-31-0-142:/opt/aws/amazon-cloudwatch-agent/etc# cd
root@ip-172-31-0-142:~# nano amazon-cloudwatch-agent.json
root@ip-172-31-0-142:~# sudo mv amazon-cloudwatch-agent.json /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
root@ip-172-31-0-142:~# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json -s
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_amazon-cloudwatch-agent.json.tmp
Start configuration validation...
2024/05/16 01:20:40 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_amazon-cloudwatch-agent.json.tmp ...
2024/05/16 01:20:40 I! Valid Json input schema.
2024/05/16 01:20:40 Configuration validation first phase succeeded
I! Detecting run_as_user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
root@ip-172-31-0-142:~#

```

## 2.2 IAM para o CloudWatch

Concedeu-se permissão ao user group **abc-place** para acessar todos os logs do CloudWatch, como visto na imagem abaixo.

| Attached entities | Policy name                          | Type            |
|-------------------|--------------------------------------|-----------------|
| 1                 | AmazonEC2ContainerRegistryFullAccess | AWS managed     |
| 1                 | AmazonEC2FullAccess                  | AWS managed     |
| 1                 | AmazonECRoleforSSM                   | AWS managed     |
| 1                 | AmazonECRolePolicyForLaunchWizard    | AWS managed     |
| 1                 | AmazonSNSFullAccess                  | AWS managed     |
| 1                 | AWSLambda_FullAccess                 | AWS managed     |
| 1                 | CloudWatchLogsFullAccess             | AWS managed     |
| 2                 | IAMFullAccess                        | AWS managed     |
| 0                 | wazuh-p2                             | Customer inline |
| 1                 | WellArchitectedConsoleFullAccess     | AWS managed     |

## 2.3 Métricas e filtros no CloudWatch para tentativas de autenticação SSH (sucesso ou falha)

Comecou criando-se o log group **auth-logs**, que recebe os logs vindos de todos os agentes do CloudWatch.

The screenshot shows the AWS CloudWatch Log Groups page. On the left, there's a navigation sidebar with sections like Dashboards, Alarms, Logs (selected), Metrics, X-Ray traces, Events, Application Signals, Network monitoring, and Insights. Under Logs, it shows Log groups, Log Anomalies, Live Tail, and Logs Insights. The main content area is titled "Log groups (2)". It displays two log groups: "auth-logs" and "cybersec-p2". Both are listed as Standard Log class, with "Configure" options for Anomaly detection, Data protection, Sensitive data, and Retention. The "auth-logs" entry has "2 filters" listed under Metric filters. At the top right, there are buttons for Actions, View in Logs Insights, Start tailing, and Create log group.

Criaram-se duas métricas associadas a **auth-logs**. Um deles reconhece padrões de logins SSH bem-sucedidos nos logs, enquanto o outro reconhece tentativas falhas.

The screenshot shows the AWS CloudWatch Metrics Filters page. The left sidebar is identical to the previous screenshot. The main content area shows two metric filters: "SSHLoginSuccess" and "SSHLoginFailure". Each filter has a "Filter pattern" section with specific regex patterns. Below that are sections for "Metric", "Metric value", "Default value", "Unit", "Dimensions", and "Alarms". The "Metric" section for both filters lists "Authentication / SuccessfulSSHLogin" and "Authentication / FailedSSHLogin". The "Metric value" for both is set to 1. The "Dimensions" and "Alarms" sections are currently empty.

## 2.4 Alarme no CloudWatch para tentativas de autenticação SSH

Definiu-se um tópico SNS (Simple Notification Service), atrelado a `cbsec10@gmail.com`, que fará a notificação via e-mail dos alarmes, como se atesta abaixo:

The screenshot shows the 'Configure actions - optional' step in the AWS CloudWatch Metrics & Alarms interface. The left sidebar lists steps 1-4. Step 1 is 'Specify metric and conditions' (selected). Step 2 is 'Configure actions' (selected). Step 3 is 'Add name and description'. Step 4 is 'Preview and create'. The main area is titled 'Notification'. Under 'Alarm state trigger', 'In alarm' is selected. Under 'Send a notification to the following SNS topic', 'Select an existing SNS topic' is selected, and 'Default\_CloudWatch\_Alarms\_Topic' is chosen. Under 'Email (endpoints)', 'cbsec10@gmail.com' is listed with a link to 'View in SNS Console'. Below these are sections for 'Lambda action' and 'Auto Scaling action', each with an 'Add [action]' button.

Em seguida, configuram-se propriamente os alarmes, um disparando após 3 tentativas falhas dentro de uma janela de 5 minutos, e outro a cada 1 tentativa bem-sucedida de autenticação.

us-east-1.console.aws.amazon.com [Option+S]

Step 2 - optional  
Configure actions

Step 3 - optional  
Add name and description

Step 4 - optional  
Preview and create

### Metric

Graph  
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

No unit  
2

Namespace  
Authentication

Metric name  
SuccessfulSSHLogins

Statistic  
Sum

Period  
5 minutes

### Conditions

Threshold type  
 Static Use a value as a threshold  
 Anomaly detection Use a band as a threshold

Whenever SuccessfulSSHLogins is...  
Define the alarm condition.

Greater > threshold  
 Greater/Equal >= threshold  
 Lower/Equal <= threshold  
 Lower < threshold

than...  
Define the threshold value.  
1  
Must be a number

▶ Additional configuration

CloudShell Feedback

us-east-1.console.aws.amazon.com [Option+S]

Step 1 - optional  
Specify metric and conditions - optional

Step 2 - optional  
Configure actions

Step 3 - optional  
Add name and description

Step 4 - optional  
Preview and create

### Metric

Graph  
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

No unit  
55

Namespace  
Authentication

Metric name  
FailedSSHLogins

Statistic  
Sum

Period  
5 minutes

### Conditions

Threshold type  
 Static Use a value as a threshold  
 Anomaly detection Use a band as a threshold

Whenever FailedSSHLogins is...  
Define the alarm condition.

Greater > threshold  
 Greater/Equal >= threshold  
 Lower/Equal <= threshold  
 Lower < threshold

than...  
Define the threshold value.  
3  
Must be a number

CloudShell Feedback

The screenshot shows the AWS CloudWatch Alarms page. The left sidebar includes sections for Dashboards, Alarms (1), Logs, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, Insights, and various links like CloudShell and Feedback. The main content area displays two alarms:

| Name                     | State   | Last state update (UTC) | Conditions   | Actions  |
|--------------------------|---|-------------------------|--|--|
| FailedSSHLoginsAlarm     | <span style="color: red;">⚠ In alarm</span>           | 2024-05-17 01:05:35     | FailedSSHLogins >= 3 for 1 datapoints within 5 minutes     | <span style="color: green;">Actions enabled</span> |
| SuccessfulSSHLoginsAlarm | <span style="color: gray;">∅ Insufficient data</span> | 2024-05-16 22:52:25     | SuccessfulSSHLogins >= 1 for 1 datapoints within 5 minutes | <span style="color: green;">Actions enabled</span> |

Com isso, pode-se observar nos gráficos o fluxo de tentativas, bem e mal-sucedidas.

The screenshot shows the AWS CloudWatch Alarms page for the FailedSSHLoginsAlarm. The left sidebar is identical to the previous screenshot. The main content area shows the alarm details and a metric graph:

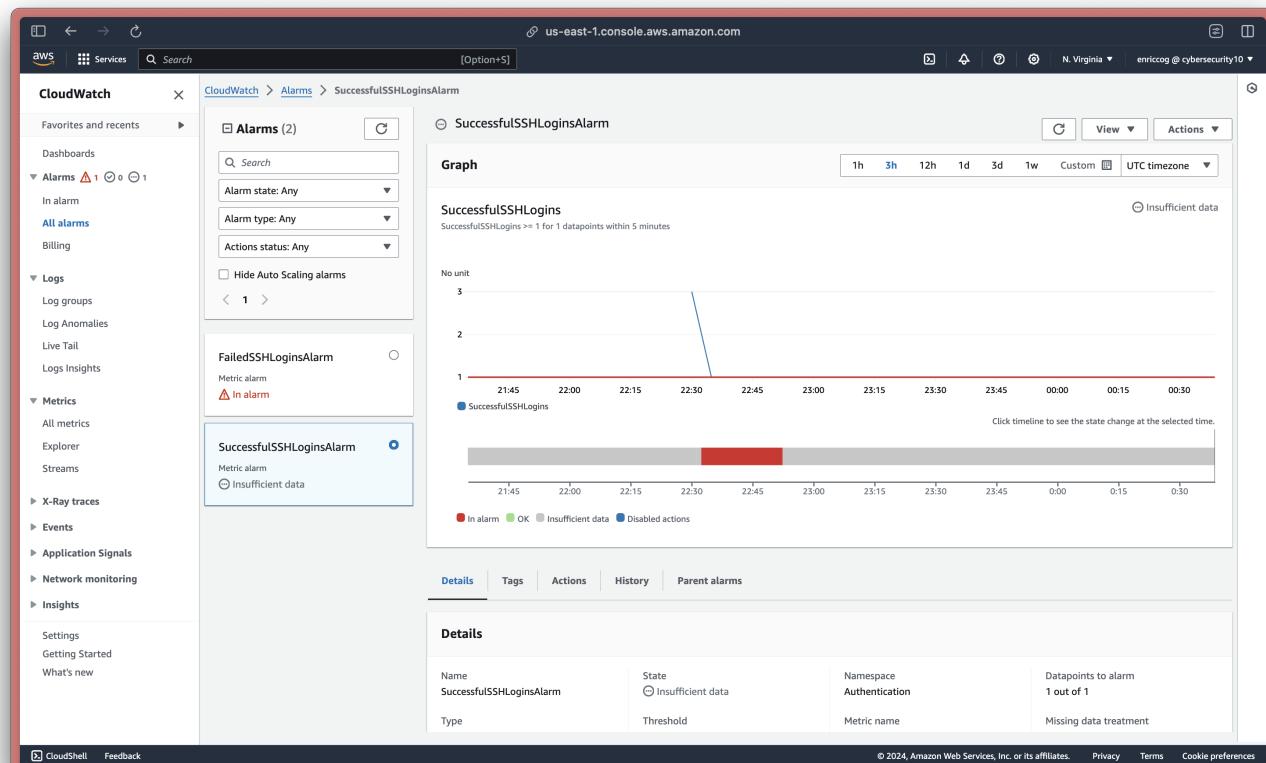
**Graph**

**FailedSSHLogins**  
FailedSSHLogins >= 3 for 1 datapoints within 5 minutes

The graph shows a blue line representing the metric value over time. A red horizontal line at value 1 indicates the threshold. The graph shows several spikes above the threshold, particularly around 22:15, 23:15, and 00:15. A legend below the graph indicates: ● In alarm, ● OK, ● Insufficient data, and ● Disabled actions.

**Details**

|                              |  |                             |                                   |
|------------------------------|--|-----------------------------|-----------------------------------|
| Name<br>FailedSSHLoginsAlarm | State<br><span style="color: red;">⚠ In alarm</span> | Namespace<br>Authentication | Datapoints to alarm<br>1 out of 1 |
| Type                         | Threshold  | Metric name                 | Missing data treatment            |



Por fim, confirmou-se o funcionamento do serviço de notificação via e-mail, para ambos os casos, como é mostrado abaixo:

**ALARM: "SuccessfulSSHLoginsAlarm" in US East (N. Virginia)**

You are receiving this email because your Amazon CloudWatch Alarm "SuccessfulSSHLoginsAlarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [3.0 (16/05/24 22:27:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Thursday 16 May, 2024 22:32:25 UTC".

View this alarm in the AWS Management Console:  
<https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/SuccessfulSSHLoginsAlarm>

**Alarm Details:**

- Name: SuccessfulSSHLoginsAlarm
- Description:
- State Change: INSUFFICIENT\_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [3.0 (16/05/24 22:27:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Thursday 16 May, 2024 22:32:25 UTC
- AWS Account: 888137825131
- Alarm Arn: arn:aws:cloudwatch:us-east-1:888137825131:alarm:SuccessfulSSHLoginsAlarm

**Threshold:**

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for at least 1 of the last 1 period(s) of 300 seconds.

**Monitored Metric:**

- MetricNamespace: Authentication
- MetricName: SuccessfulSSHLogins
- Dimensions:
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

**State Change Actions:**

- OK:
- ALARM: [arn:aws:sns:us-east-1:888137825131:Default\_CloudWatch\_Alarms\_Topic]
- INSUFFICIENT\_DATA:

Enable desktop notifications for Gmail.   notifications from this topic, please click or visit the link below to unsubscribe:  
[https://news.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:888137825131:Default\\_CloudWatch\\_Alarms\\_Topic:19a6fce3-ec4a-430f-9111-15eab042a072&Fn=mailto+hecar10@mail.com](https://news.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:888137825131:Default_CloudWatch_Alarms_Topic:19a6fce3-ec4a-430f-9111-15eab042a072&Fn=mailto+hecar10@mail.com)

The screenshot shows a Gmail inbox with the following details:

- Inbox (27 messages):** Contains two messages from "AWS Notifications".
- Message 1 (7:14 PM):** Subject: "ALARM: "FailedSSHLoginsAlarm" in US East (N. Virginia)"  
Content: You are receiving this email because your Amazon CloudWatch Alarm "FailedSSHLoginsAlarm" in the US East (N. Virginia) region has entered the ALARM state, b...  
Details:
  - Name: FailedSSHLoginsAlarm
  - Description:
  - State Change: OK -> ALARM
  - Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [3.0 (16/05/24 22:27:00)] was greater than or equal to the threshold (3.0) (minimum 1 datapoint for OK -> ALARM transition).
  - Timestamp: Thursday 16 May, 2024 22:32:35 UTC
- Message 2 (7:32 PM):** Subject: "ALARM: "FailedSSHLoginsAlarm" in US East (N. Virginia)"  
Content: You are receiving this email because your Amazon CloudWatch Alarm "FailedSSHLoginsAlarm" in the US East (N. Virginia) region has entered the ALARM state, b...  
Details:
  - Name: FailedSSHLoginsAlarm
  - Description:
  - State Change: OK -> ALARM
  - Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [3.0 (16/05/24 22:27:00)] was greater than or equal to the threshold (3.0) (minimum 1 datapoint for OK -> ALARM transition).
  - Timestamp: Thursday 16 May, 2024 22:32:35 UTC

At the bottom left, there is a notification bar: "Enable desktop notifications for Gmail." with buttons "OK" and "No thanks".

### 3. Integração do Zabbix com Email

#### 3.0 Configuração do Servidor SMTP

Para a integração com o servidor SMTP, foi utilizado o serviço da A2C Solutions, hospedado no endereço [mail.a2csolutions.com.br](mailto:mail.a2csolutions.com.br), com a porta **465** para envio de mensagens.

#### 3.1 Configuração de Media Type

Foi criada um Media Type específico para envio de mensagens por email, com as configurações do servidor SMTP, e o email de destino, com o nome **cbsecsmt**.

Media type    Message templates 8    Options

\* Name

Type

\* SMTP server

SMTP server port

\* SMTP helo

\* SMTP email

Connection security  None  STARTTLS  SSL/TLS

SSL verify peer

SSL verify host

Authentication  None  Username and password

Username

Password

Message format  HTML  Plain text

Description

Enabled

| Message type        | Template   | Actions                                     |
|---------------------|--|---|
| Problem             | <b>Problem started</b> at {EVENT.TIME} on {EVENT.DA... <a href="#">Edit</a> <a href="#">Remove</a>   |   |
| Problem recovery    | <b>Problem has been resolved</b> at {EVENT.RECOVE... <a href="#">Edit</a> <a href="#">Remove</a>     |   |
| Problem update      | <b>{USER.FULLNAME} {EVENT.UPDATE.ACTION} prob...</b>   | <a href="#">Edit</a> <a href="#">Remove</a> |
| Service             | <b>Service problem started</b> at {EVENT.TIME} on {EV... <a href="#">Edit</a> <a href="#">Remove</a> |   |
| Service recovery    | <b>Service "{SERVICE.NAME}" has been resolved</b> a... <a href="#">Edit</a> <a href="#">Remove</a>   |   |
| Service update      | <b>Changed "{SERVICE.NAME}" service status</b> to {... <a href="#">Edit</a> <a href="#">Remove</a>   |   |
| Discovery           | <b>Discovery rule:</b> {DISCOVERY RULE NAME}<br>... <a href="#">Edit</a> <a href="#">Remove</a>      |   |
| Autoregistration    | <b>Host name:</b> {HOST.HOST}<br><b>Host IP:</b> {... <a href="#">Edit</a> <a href="#">Remove</a>    |   |
| <a href="#">Add</a> |  |   |

[Update](#)[Clone](#)[Delete](#)[Cancel](#)

### 3.2 Configuração de Usuário

Como descrito nos passos da atividade, há a necessidade de se criar um usuário apenas para o envio de email.

User Media 1 Permissions

\* Username: email

Name:

Last name:

\* Groups: Zabbix administrators

Password: Change password

Language: System default

Time zone: System default: (UTC-03:00) America/Sao\_Paulo

Theme: System default

Auto-login:

Auto-logout:  15m

\* Refresh: 30s

\* Rows per page: 50

URL (after login):

Para este usuário conseguir realizar o envio de emails e ter acesso a actions, há a necessidade de dar a ele permissões de superadmin, e alterar sua Media.

| Media     | Type              | Send to         | When active | Use if severity | Status  | Action |
|-----------|-------------------|-----------------|-------------|-----------------|---|--------|
| cbsecsmtp | cbsec10@gmail.com | 1-7,00:00-24:00 | N I W A H D | Enabled         | <input type="button" value="Edit"/> <input type="button" value="Remove"/> |        |

Add

|       |                                       |
|-------|---------------------------------------|
| email | Super admin role                      |
| Admin | Zabbix Administrator Super admin role |

### 3.3 Configuração de Ação

Para que o Zabbix envie emails, é necessário criar uma nova ação, que irá ser acionada quando um alerta for disparado.

The screenshot shows the Zabbix web interface for managing trigger actions. The URL is `zabbix.abcplace.tec.br/zabbix/actionconf.php?eventsources=0`. The left sidebar is titled "ZABBIX" and includes sections for Monitoring, Services, Inventory, Reports, Configuration (with Host groups, Templates, Hosts, Maintenance, Actions selected, and Event correlation), and a search bar. The main content area is titled "Trigger actions" and displays a table of actions. The table has columns for Name, Conditions, Operations, and Status. One action is listed: "Report problems to Zabbix administrators". It has four operations: "Send message to user groups: Zabbix administrators via all media", "Send message to users: Admin (Zabbix Administrator) via Telegram", "Send message to user groups: Zabbix administrators via Telegram", and "Send message to users: email via all media". The status is "Enabled". Buttons at the bottom of the table include "Apply", "Reset", "Name" (sort), "Conditions", "Operations", "Status", "Filter", "Create", and "Delete". A footer note says "Displaying 1 of 1".