Roteiro 4 - Integração com Telegram e CloudWatch

Cyber Segurança em Nuvem 2024.1

Grupo: Antônio Martins, Ariel Leventhal e Enricco Gemha

Introdução

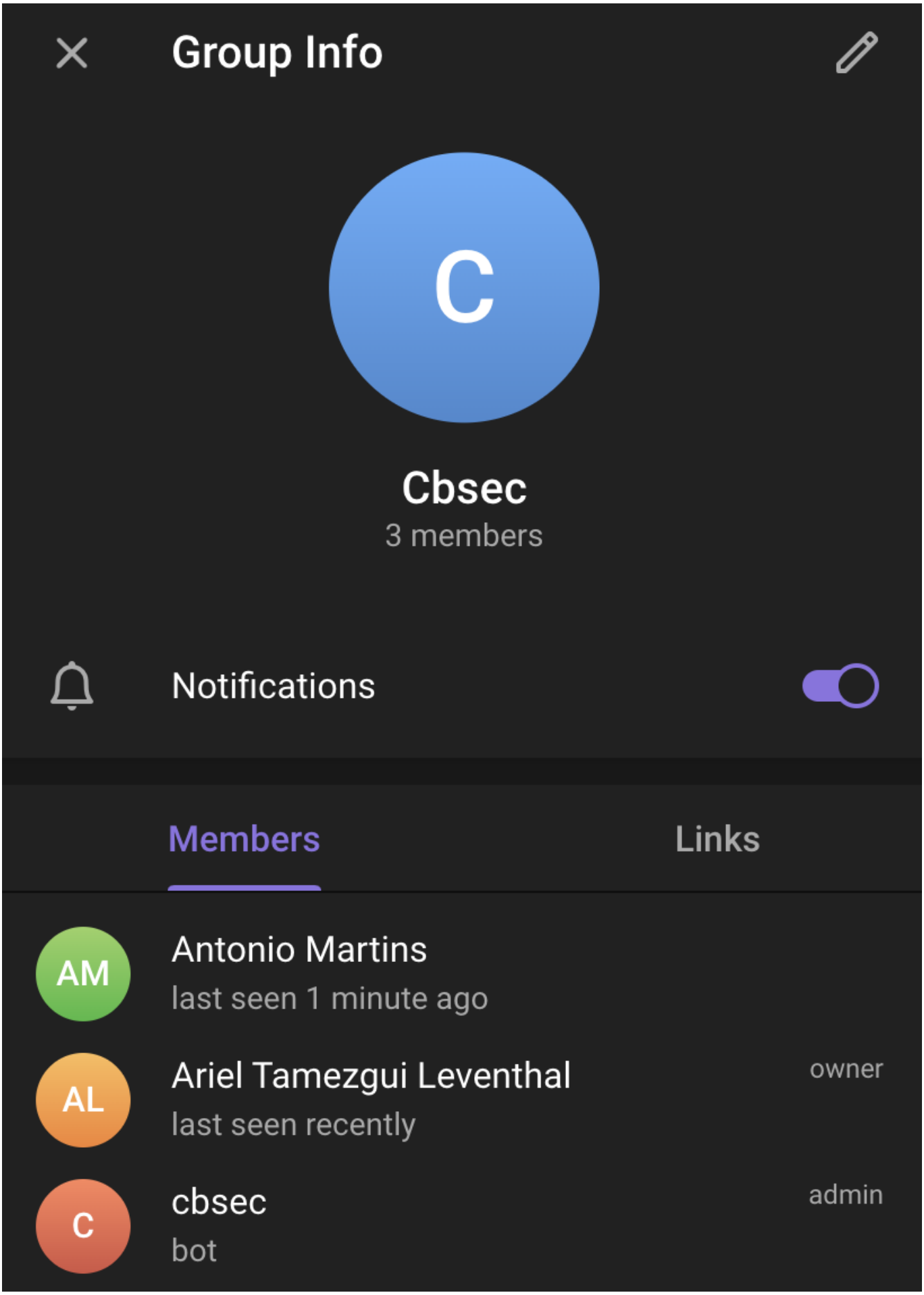
Este roteiro tem como objetivo melhorar as medidas de segurança do ambiente nuvem da ABCPLACE, através da utilização de ferramentas como o Zabbix e Wazuh, que irão ser integrados com o Telegram, para envio de alertas, e com o CloudWatch, para monitoramento de logs.

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.

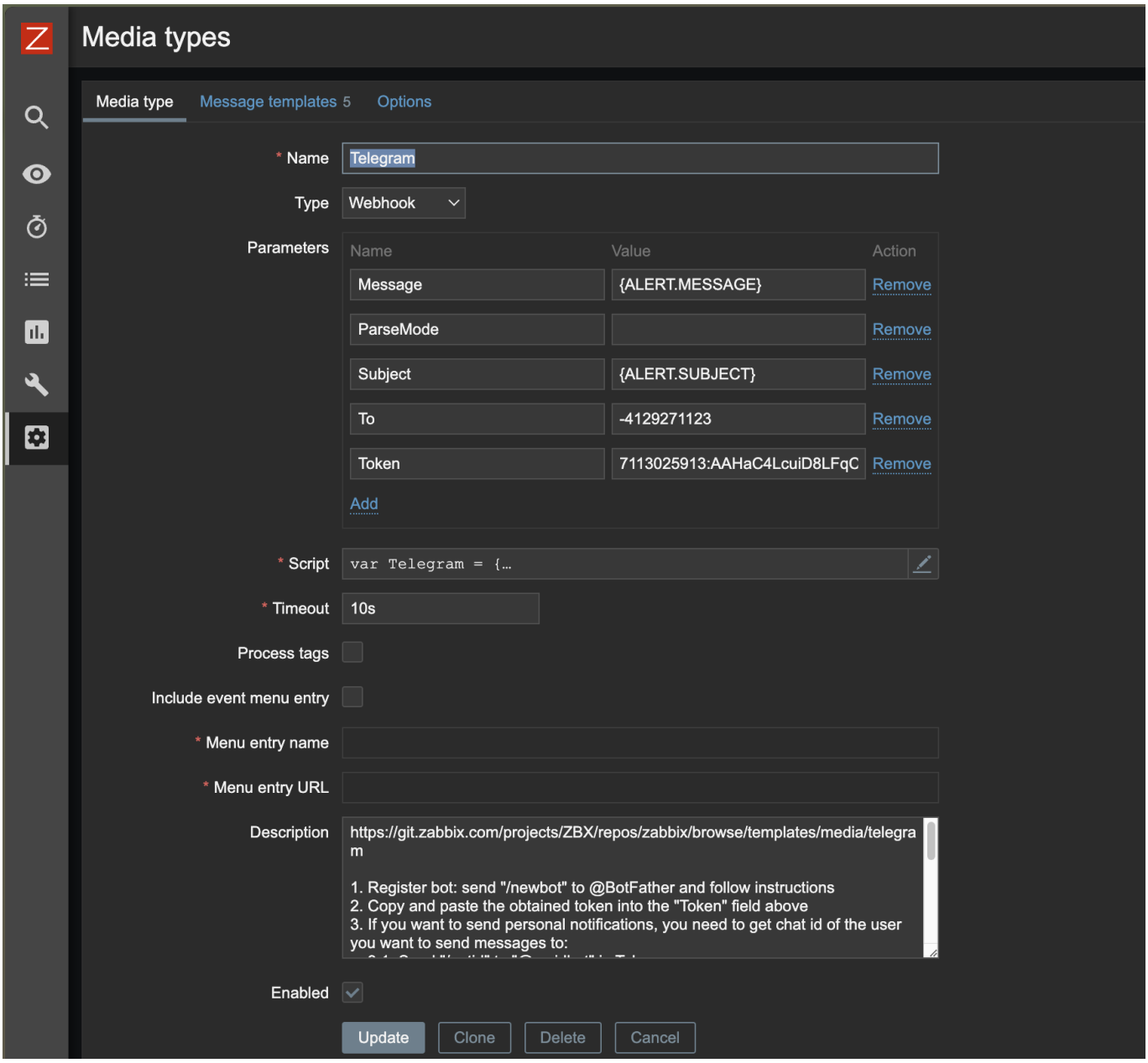
Com o bot criado, o mesmo deverá ser adicionado a um grupo de Telegram com os Administradores do Sistema, neste caso, os integrantes do grupo.



1.1 Configuração do Zabbix

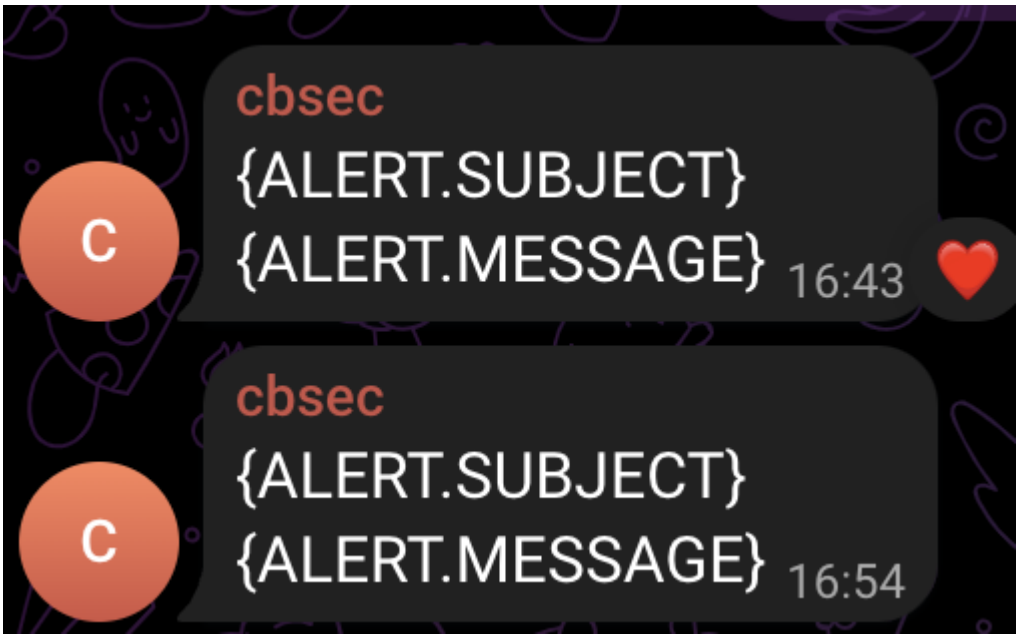
1.1.0 Criação de Media Types

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.



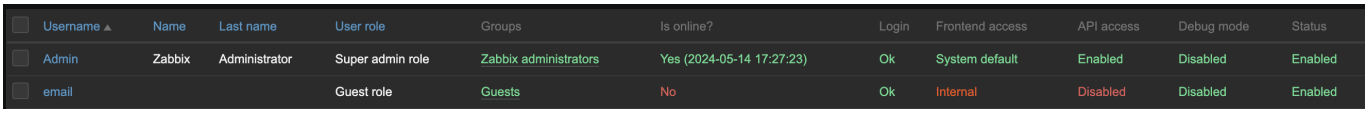
É importante destacar que o Token utilizado é o mesmo token recebido pelo BotFather, e o To é referente ao identificador único do grupo de Telegram.

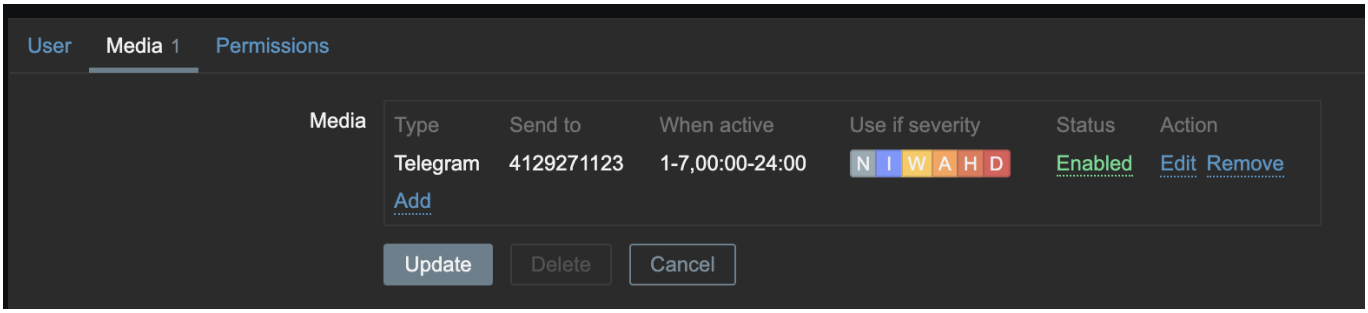
Para verificar se a integração foi feita corretamente, é possível enviar uma mensagem de teste.

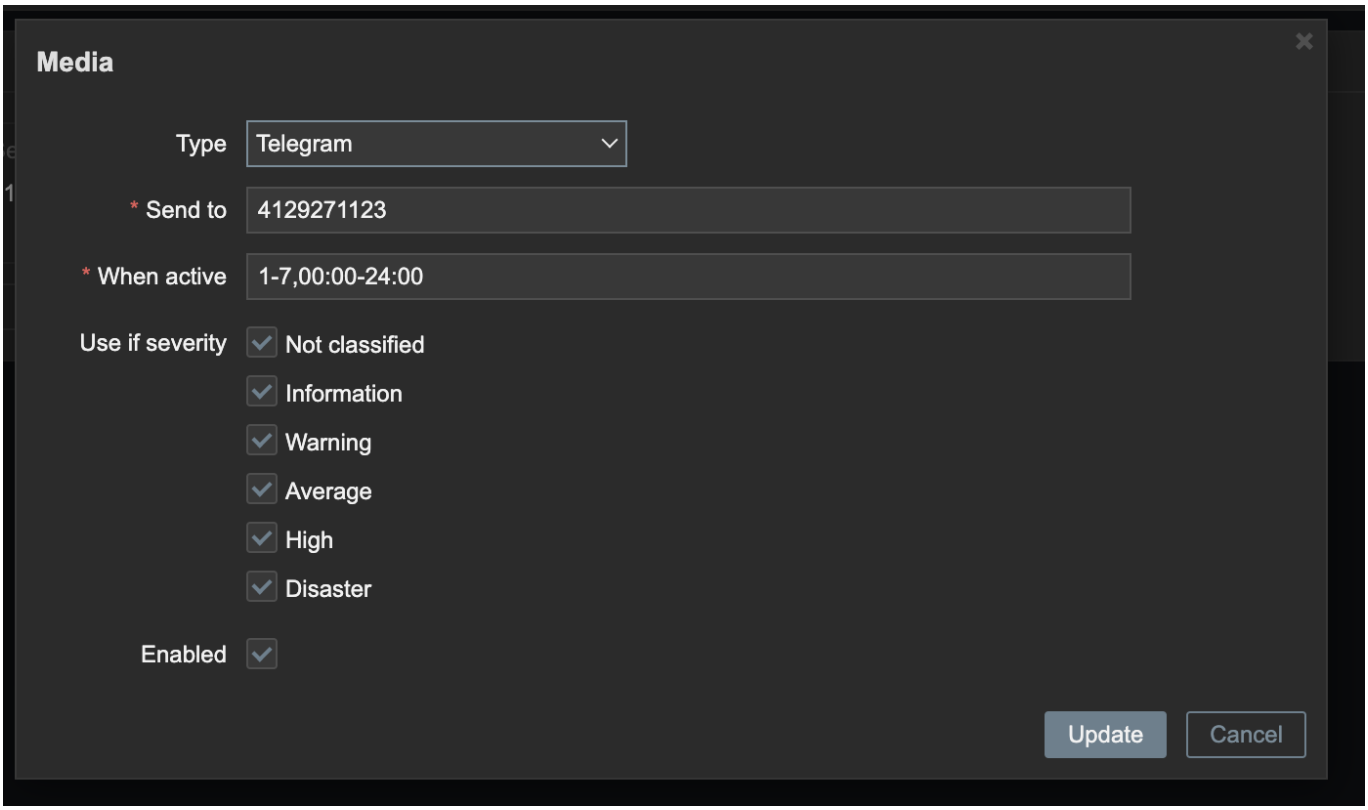


1.1.1 Adição de Media em Usuário Administrador

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

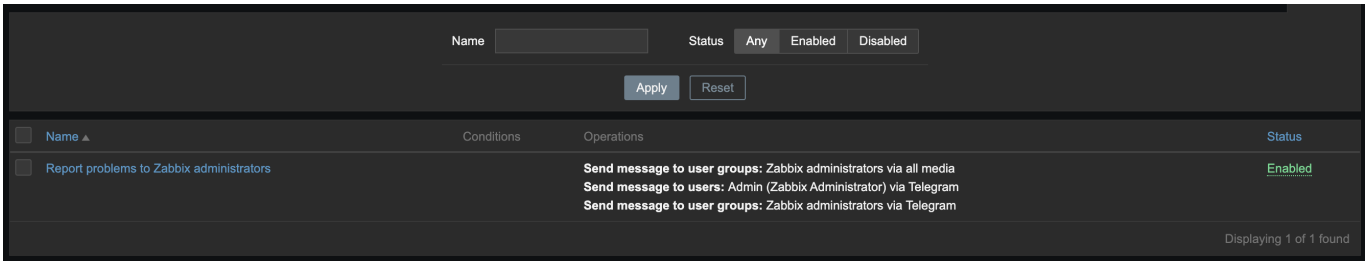


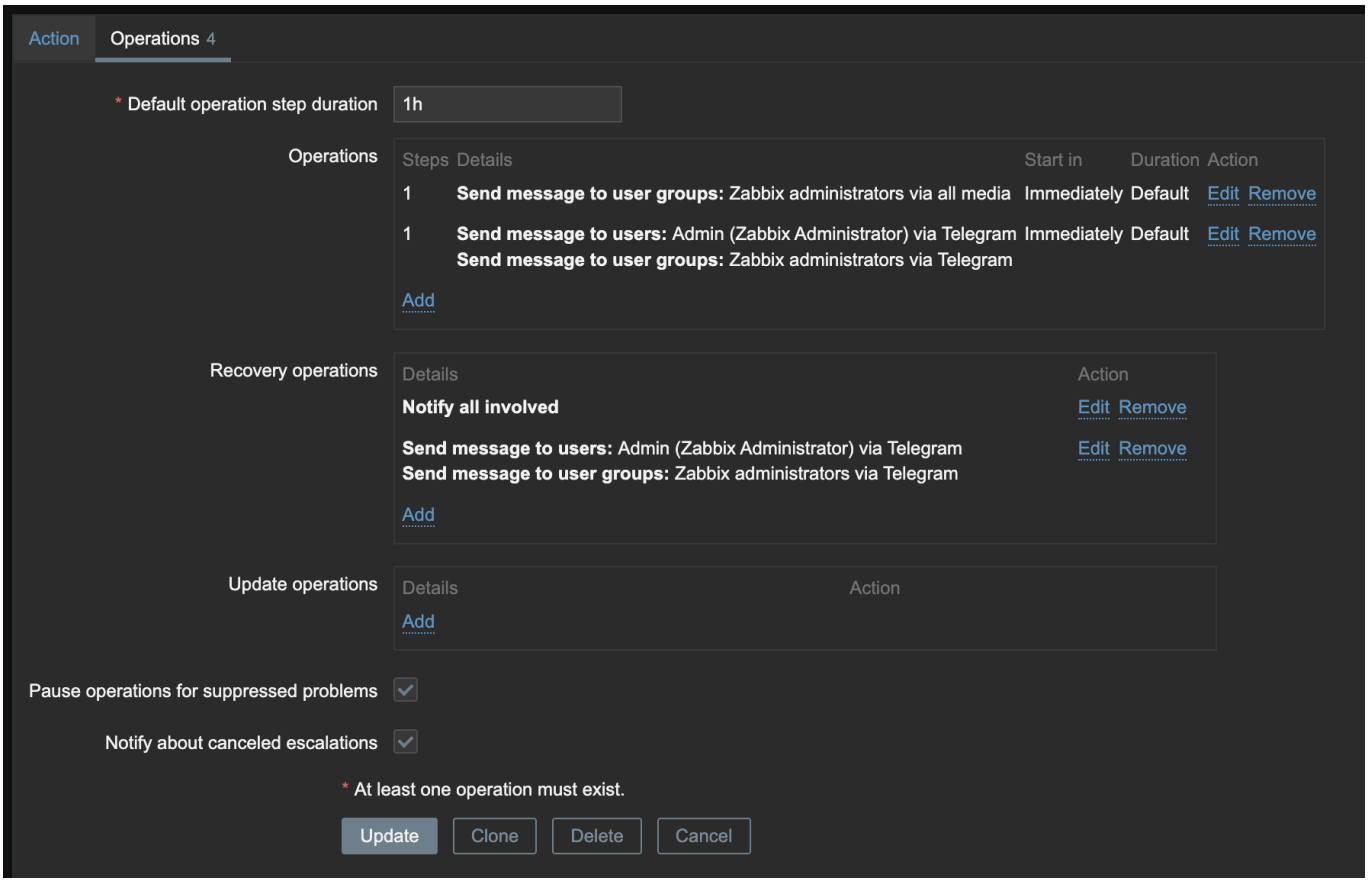




1.1.2 Zabbix Actions

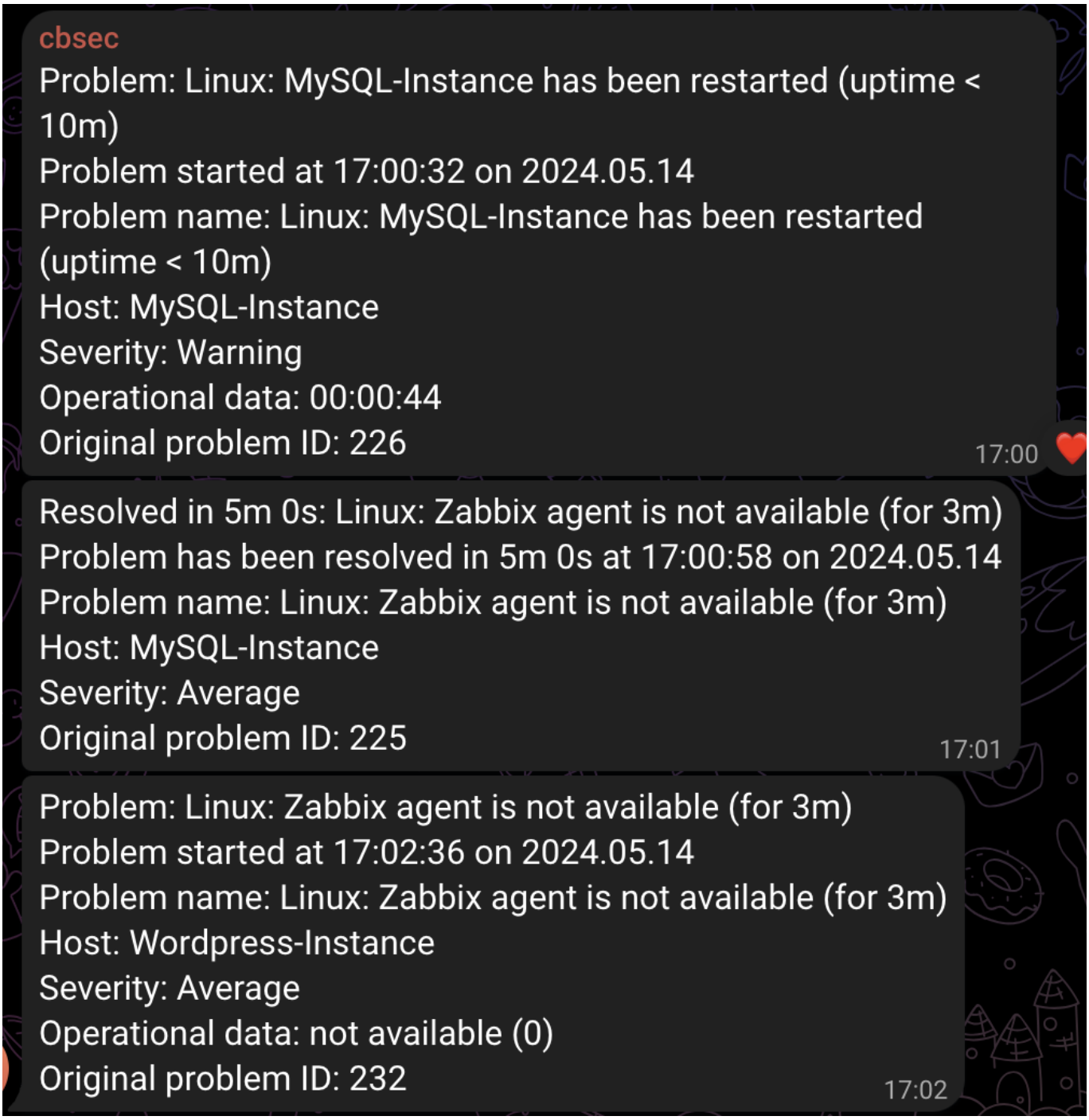
Para que o Zabbix envie mensagens para o Telegram, é necessário criar uma nova ação, que irá ser acionada quando um alerta for disparado.



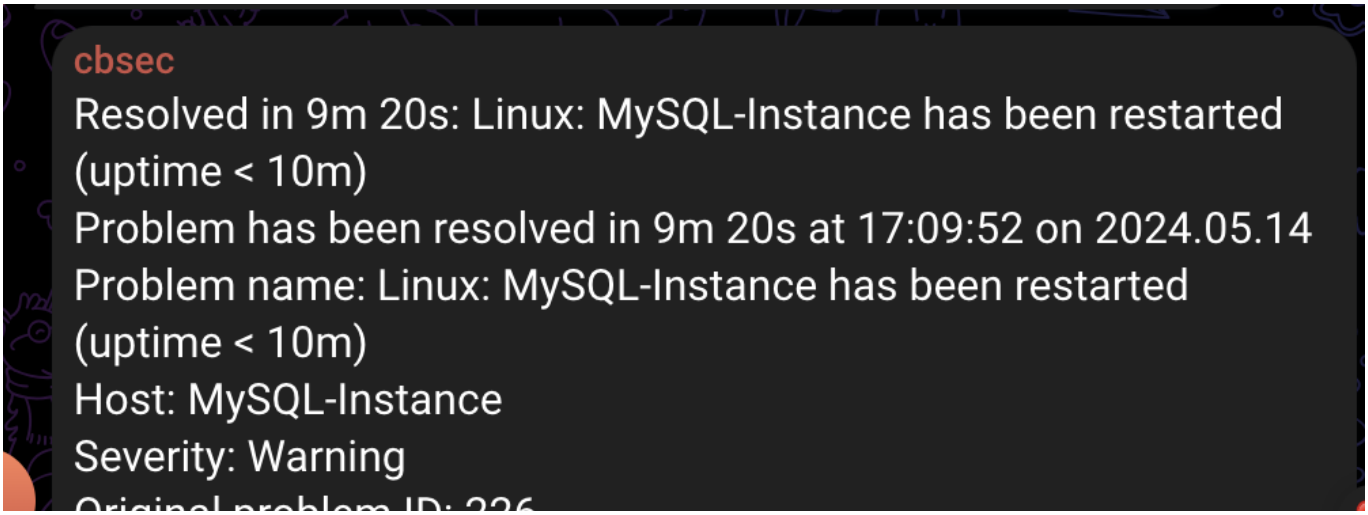


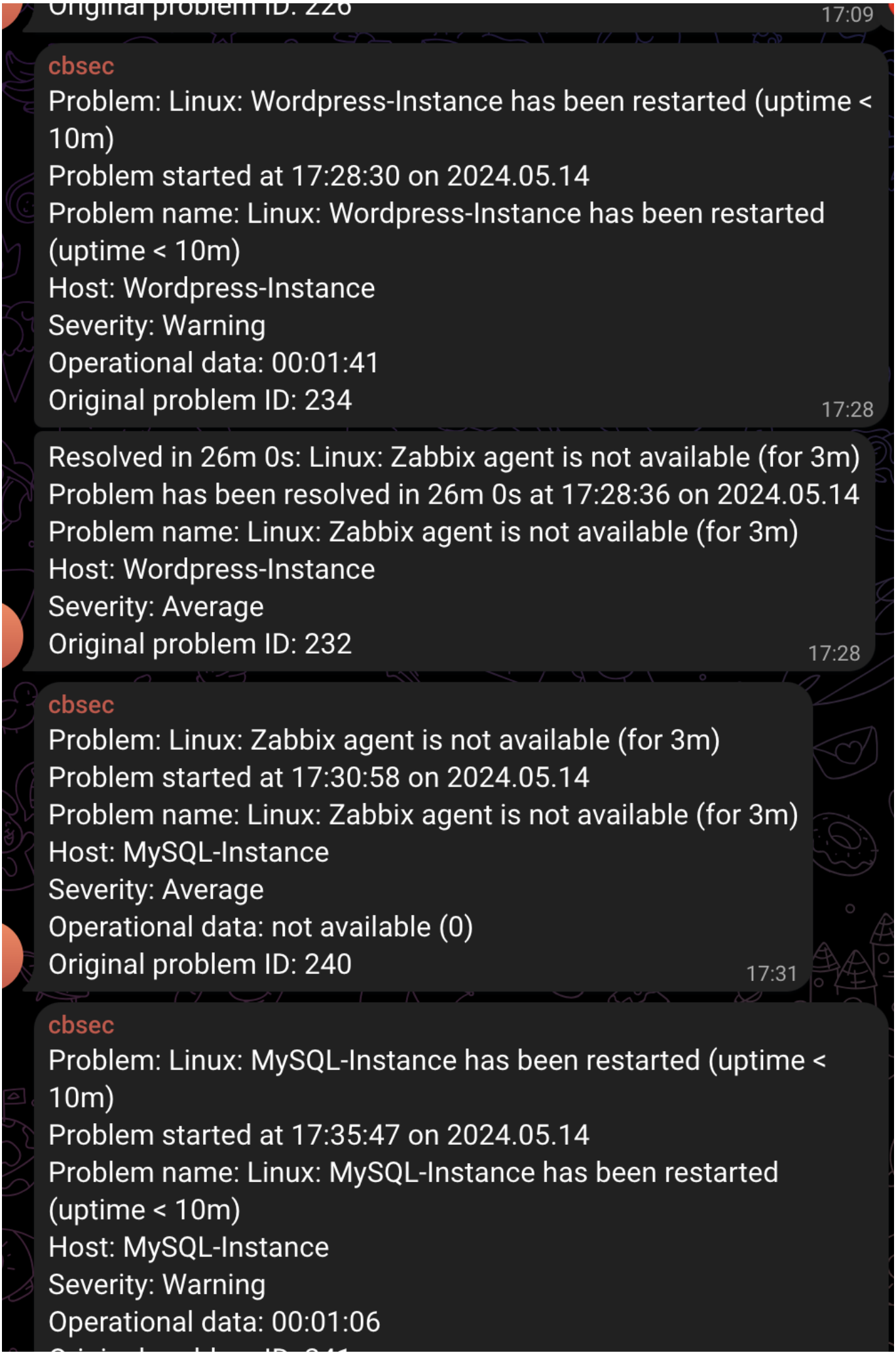
1.1.3 Teste de Integração com Telegram

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



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:





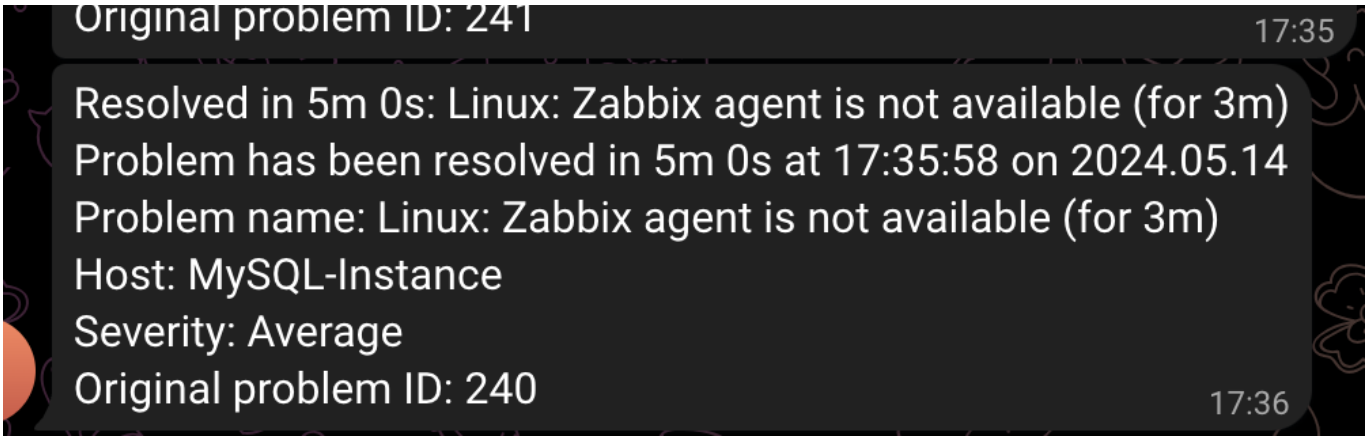
Original problem ID: 226 17:09

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

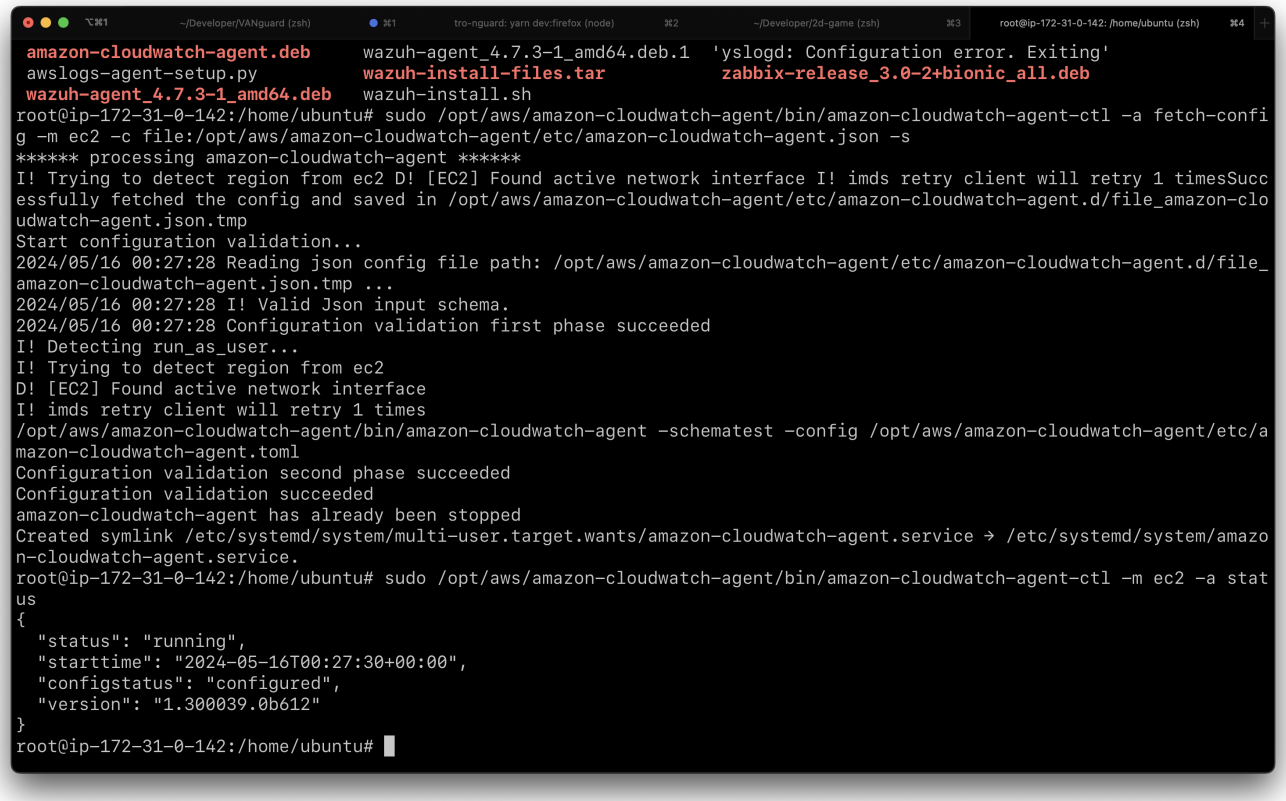
cbsec
Problem: Linux: MySQL-Instance has been restarted (uptime < 10m)
Problem started at 17:35:47 on 2024.05.14
Problem name: Linux: MySQL-Instance has been restarted (uptime < 10m)
Host: MySQL-Instance
Severity: Warning
Operational data: 00:01:06

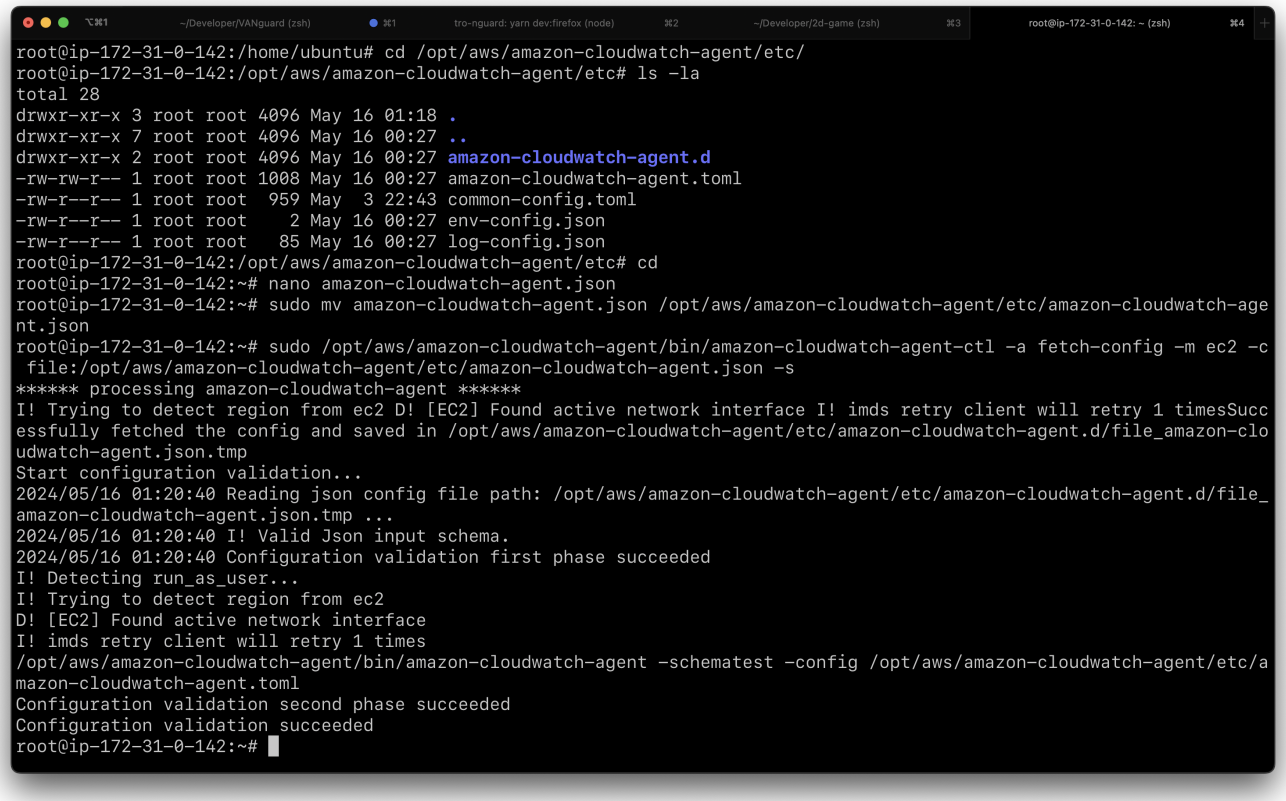


2. Integração com CloudWatch

2.1 Configuração do CloudWatch para o Wazuh

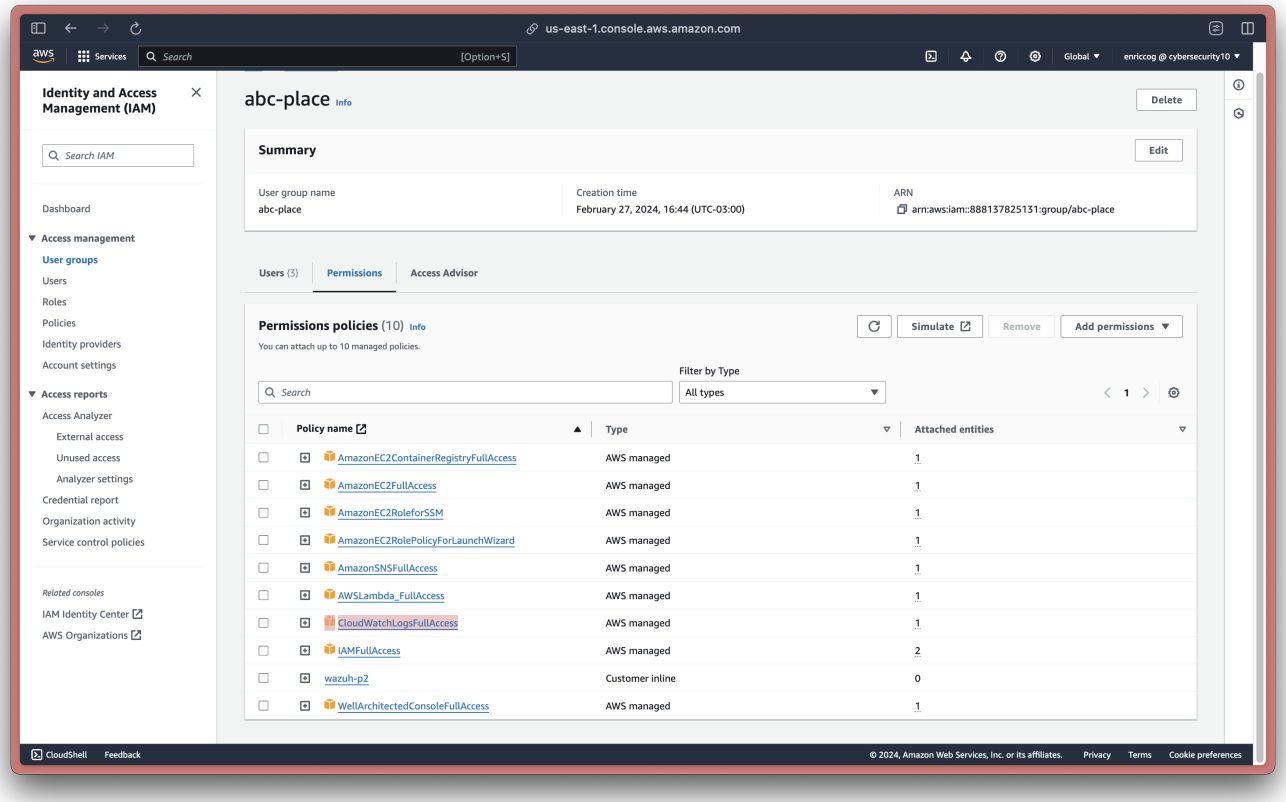
Conforme solicitado, instalou-se e configurou-se os agentes do CloudWatch para enviar logs das instâncias ao serviço titular. Verifica-se isto nas screenshots a seguir:





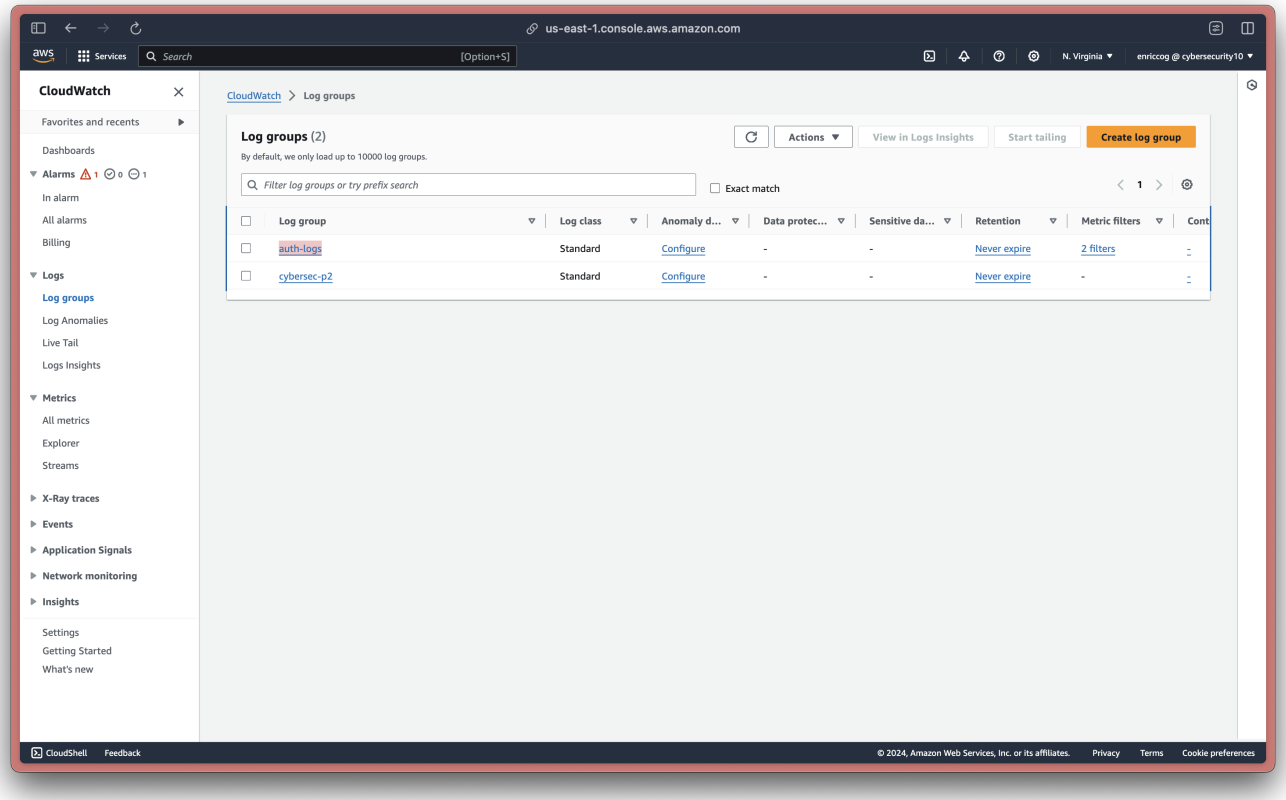
2.2 IAM para o CloudWatch

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

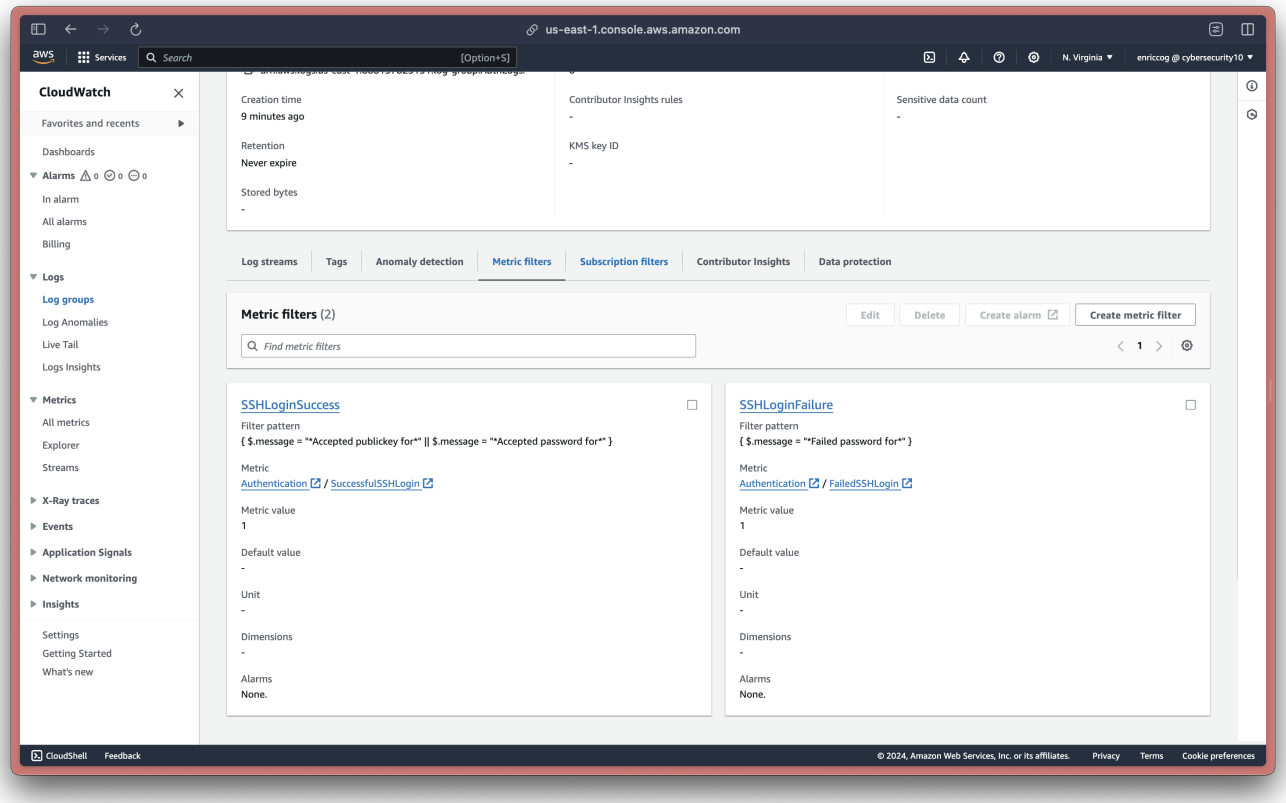


2.3 Métricas e filtros no CloudWatch para tentativas de autenticação SSH (sucesso ou falha)

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

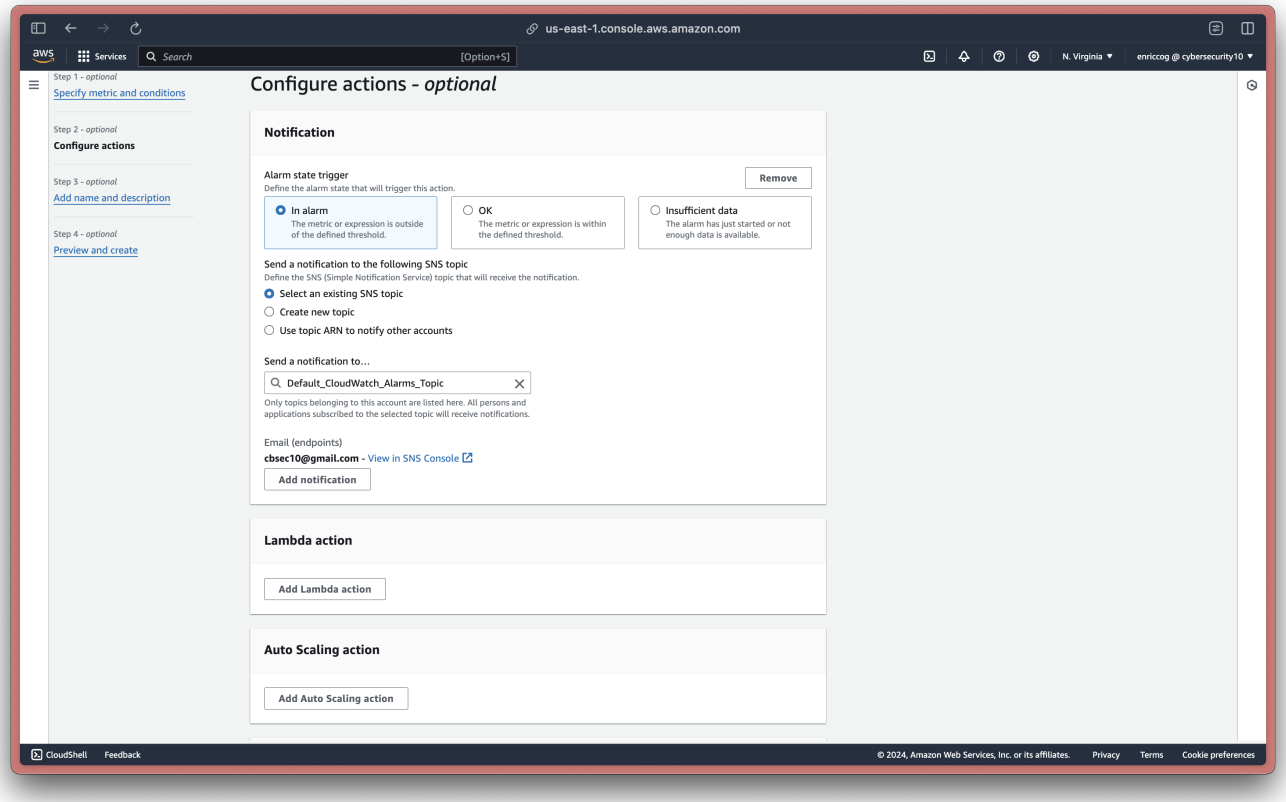


Criaram-se duas métricas associadas a `auth-logs`. Um deles reconhece padrões de logins SSH bem-sucedidos nos logs, enquanto o outro reconhece tentativas falhas.

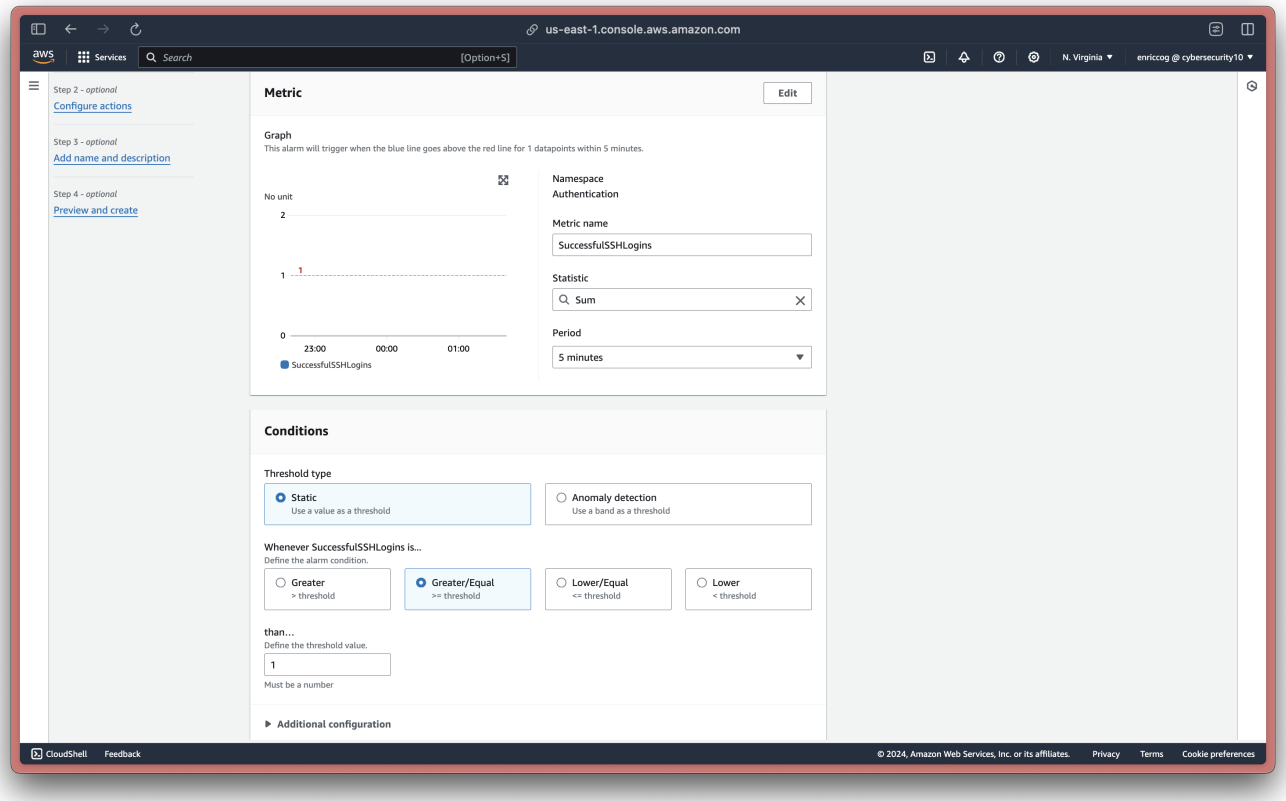


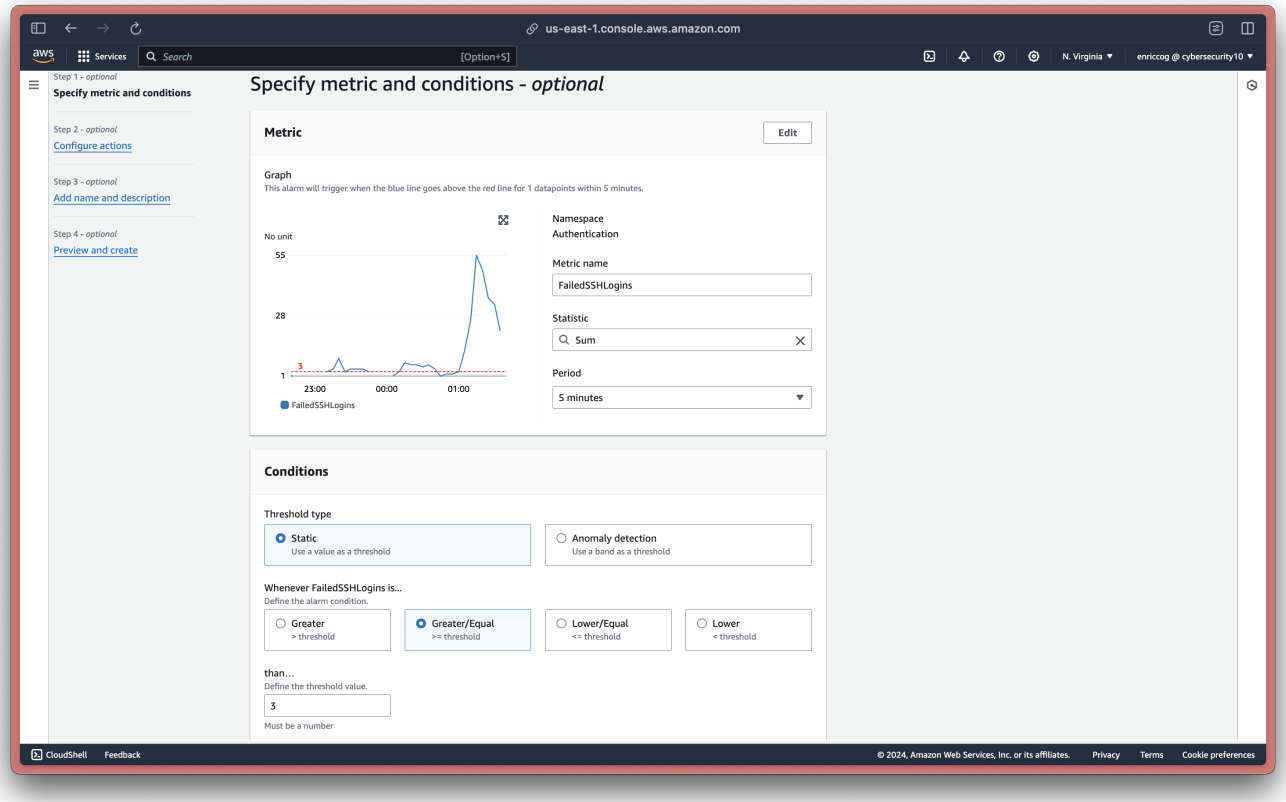
2.4 Alarme no CloudWatch para tentativas de autenticação SSH

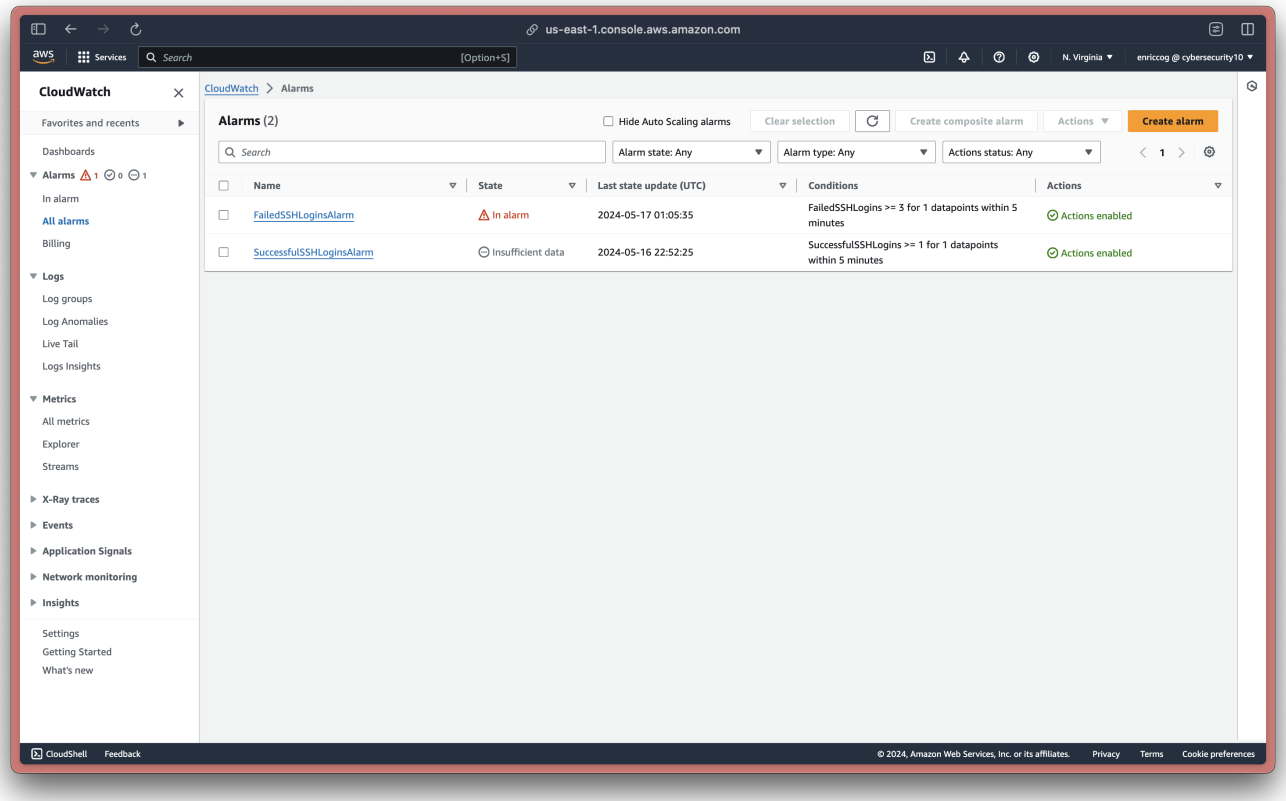
Definiu-se um tópico SNS (Simple Notification Service), atrelado a *cbsec10@gmail.com*, que fará a notificação via e-mail dos alarmes, como se atesta abaixo:



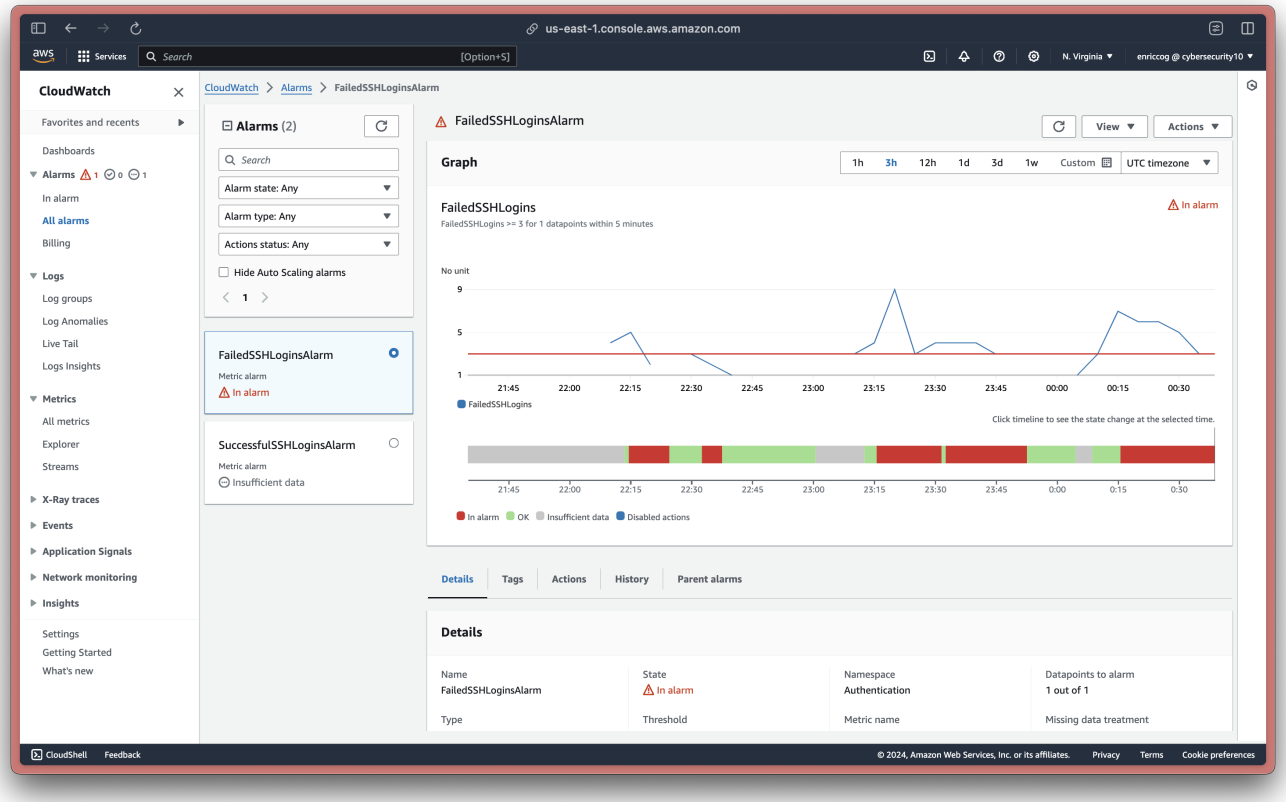
Em seguida, configuram-se propriamente os alarmes, um disparando após 3 tentativas falhas dentro de uma janela de 5 minutos, e outro a cada 1 tentativa bem-sucedida de autenticação.

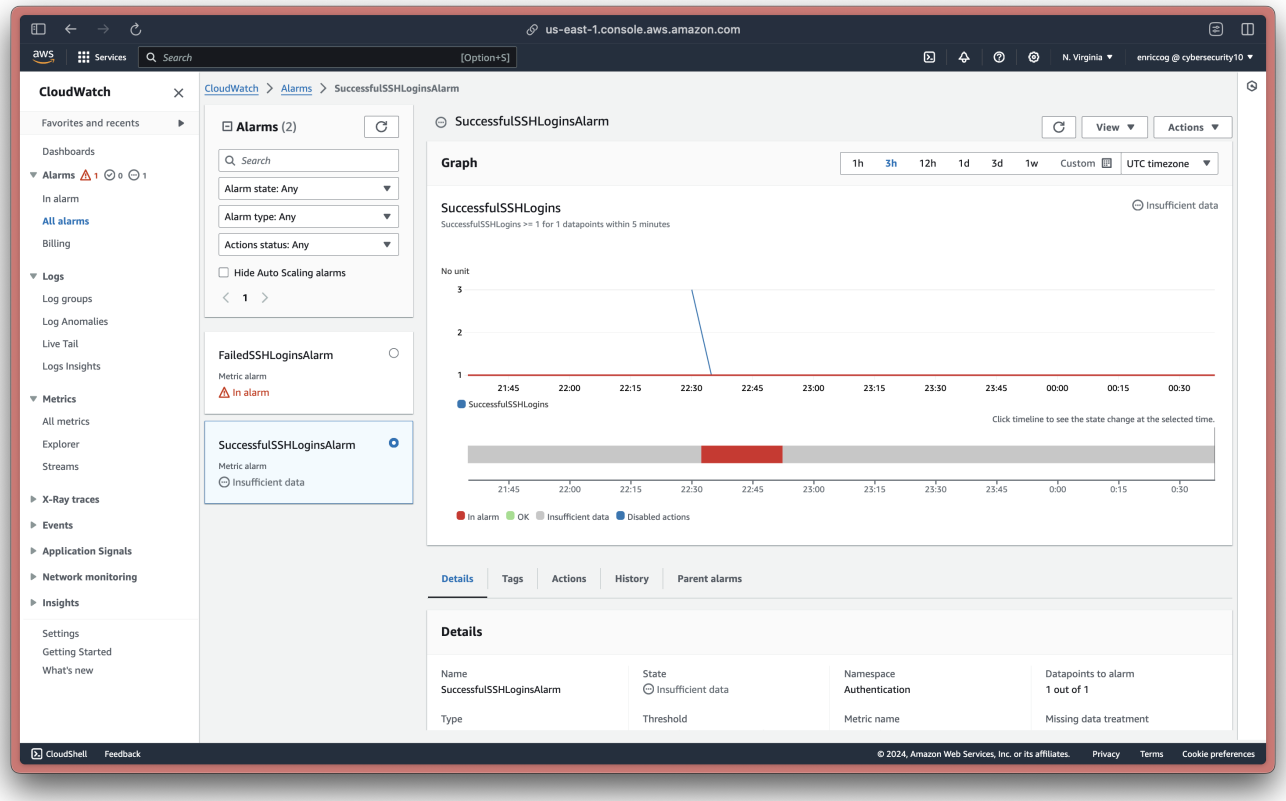

us-east-1.console.aws.amazon.com
Step 2 - optional
Configure actions
Step 3 - optional
Add name and description
Step 4 - optional
Preview and create
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
No unit
2
1
0
23:00
00:00
01:00
SuccessfulSSHLogins
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
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com
Step 1 - optional
Specify metric and conditions
Specify metric and conditions - optional
Step 2 - optional
Configure actions
Step 3 - optional
Add name and description
Step 4 - optional
Preview and create
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
No unit
55
28
1
3
23:00
00:00
01:00
FailedSSHLogins
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
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

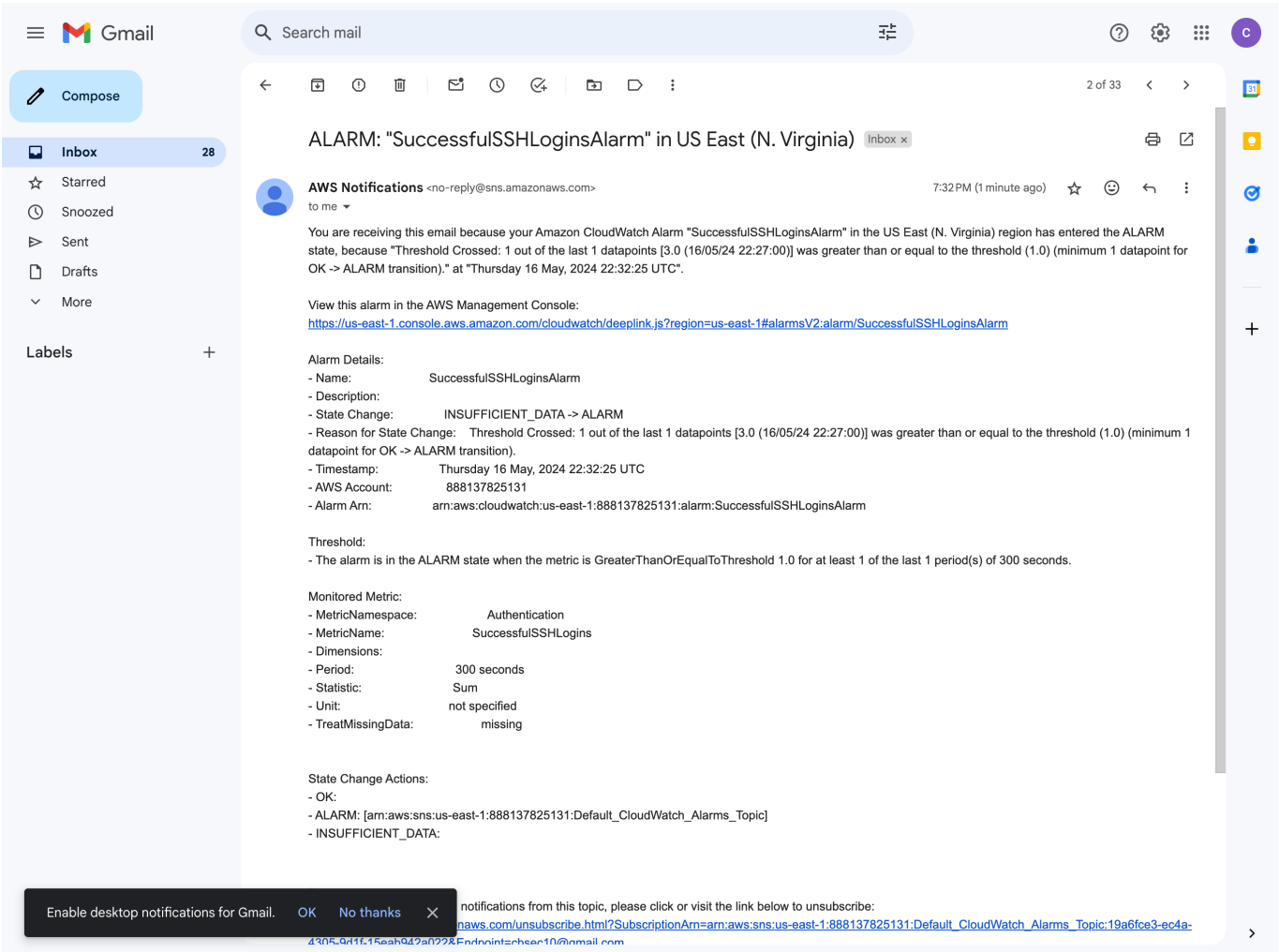


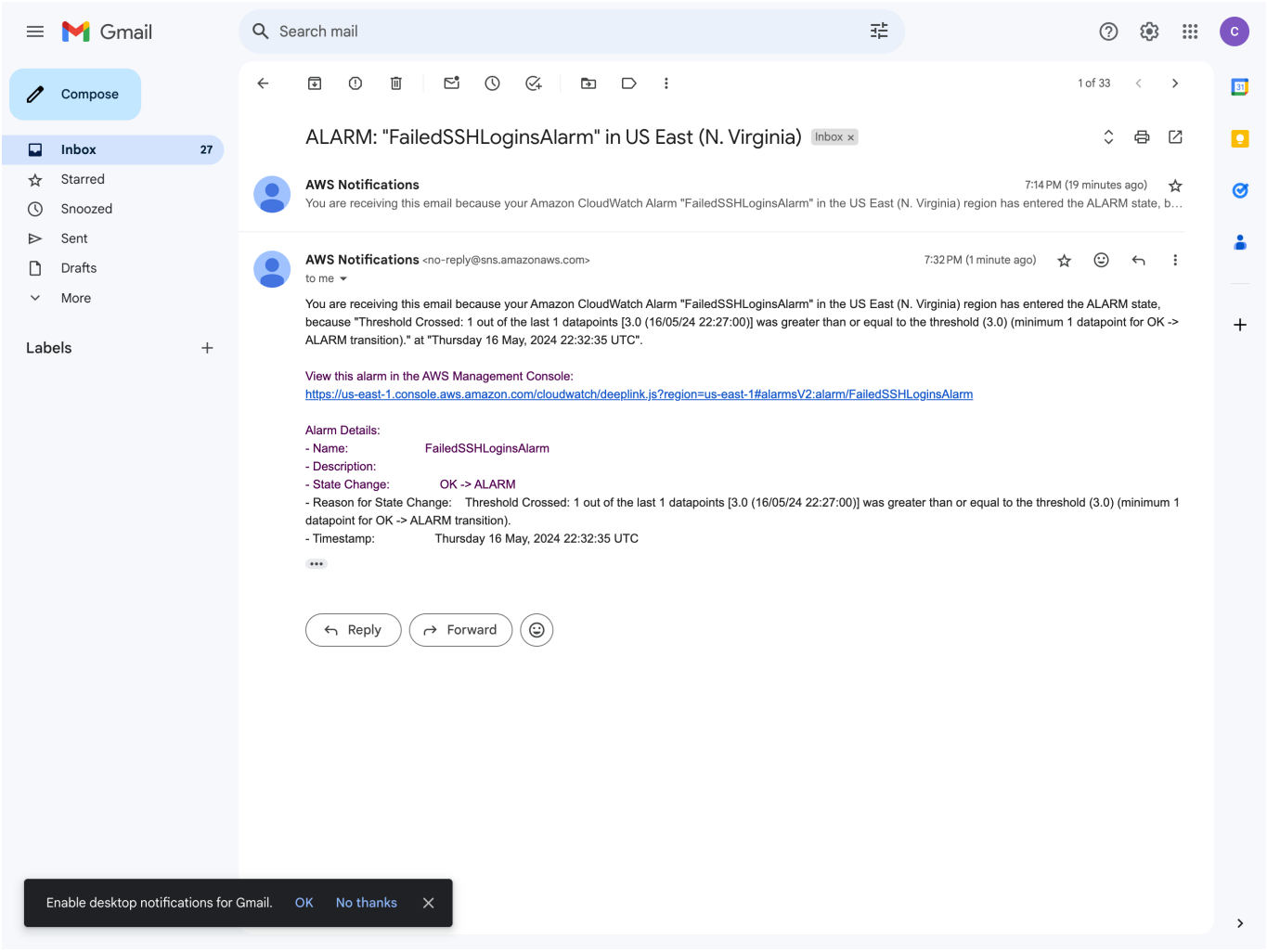
Com isso, pode-se observar nos gráficos o fluxo de tentativas, bem e mal-sucedidas.





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





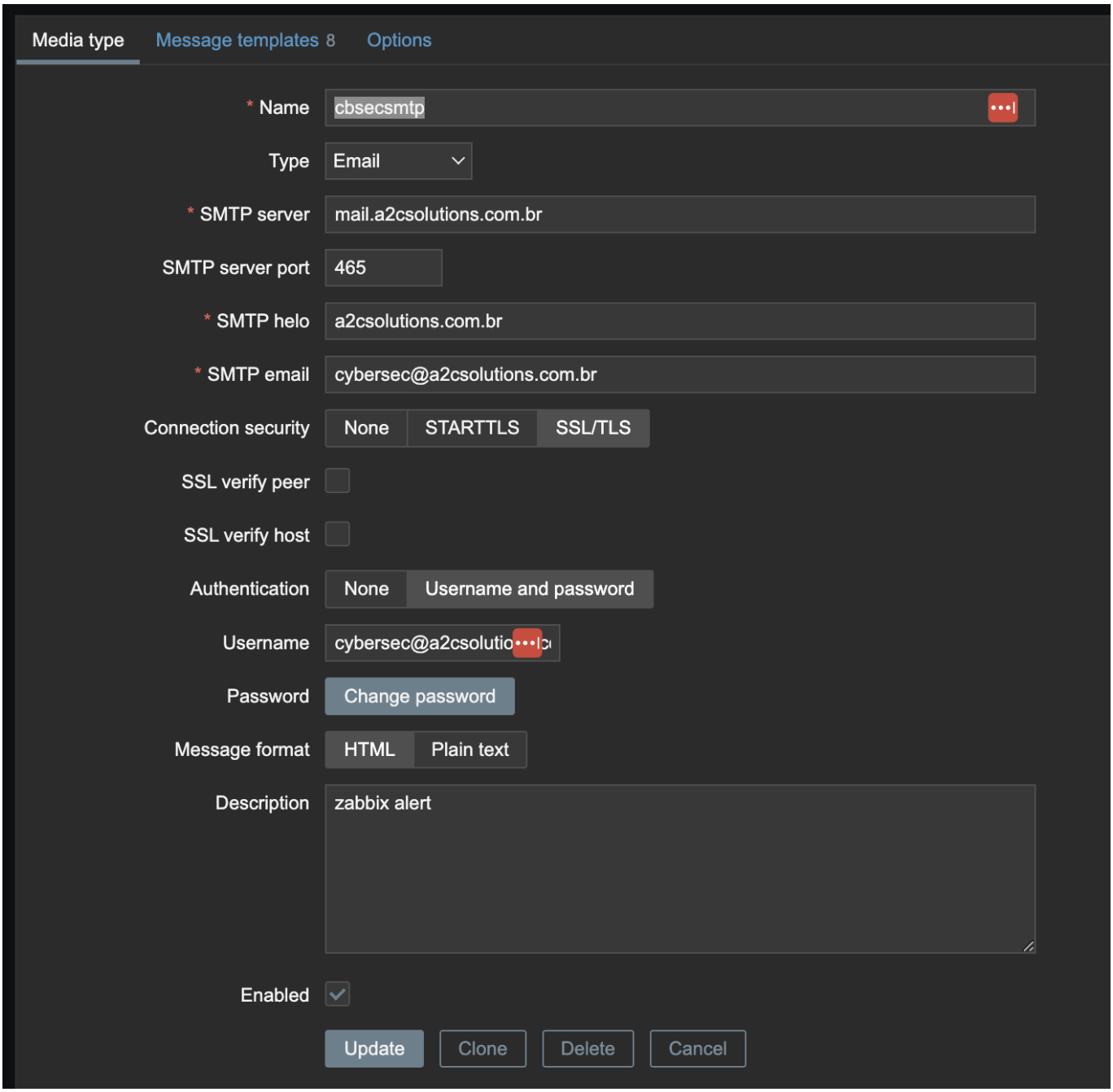
3. Integração do Zabbix com Email

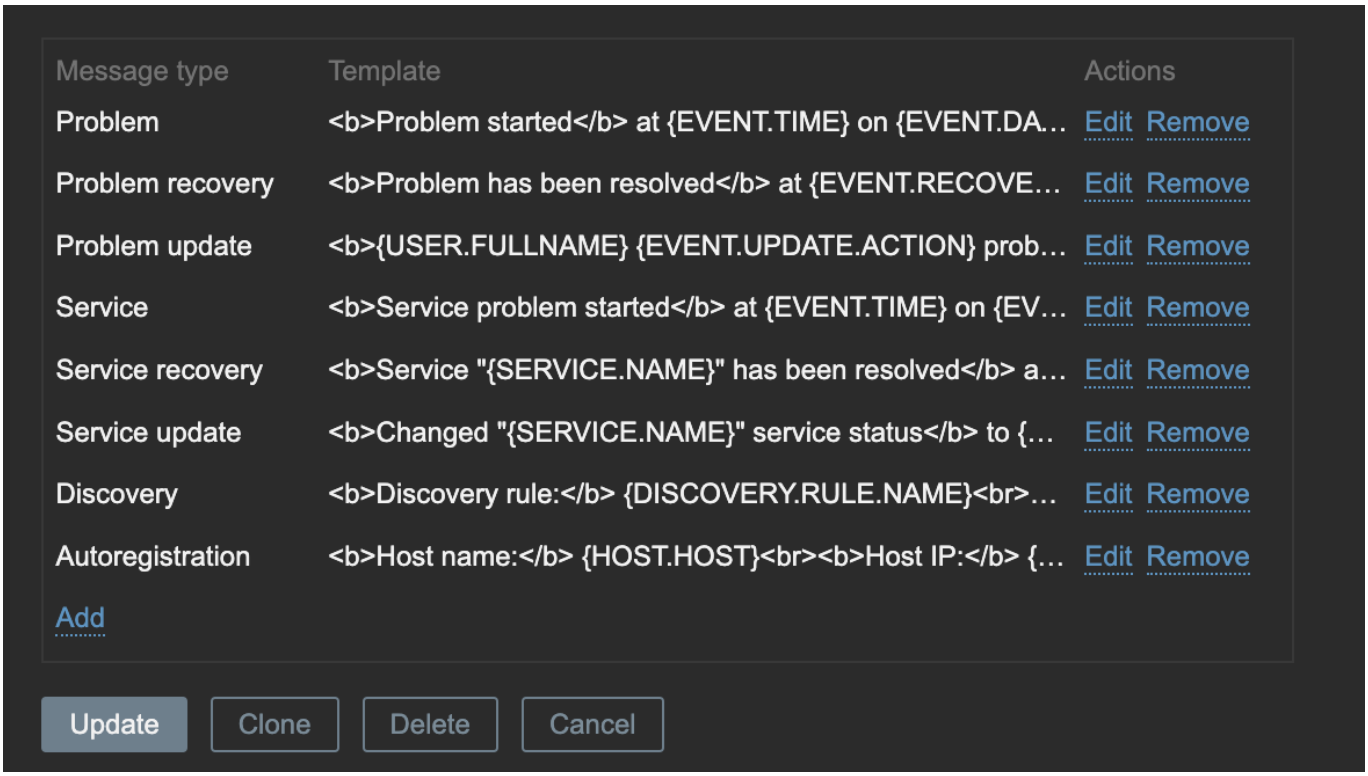
3.0 Configuração do Servidor SMTP

Para a integração com o servidor SMTP, foi utilizado o serviço da A2C Solutions, hospedado no endereço `mail.a2csolutions.com.br`, com a porta `465` para envio de mensagens.

3.1 Configuração de Media Type

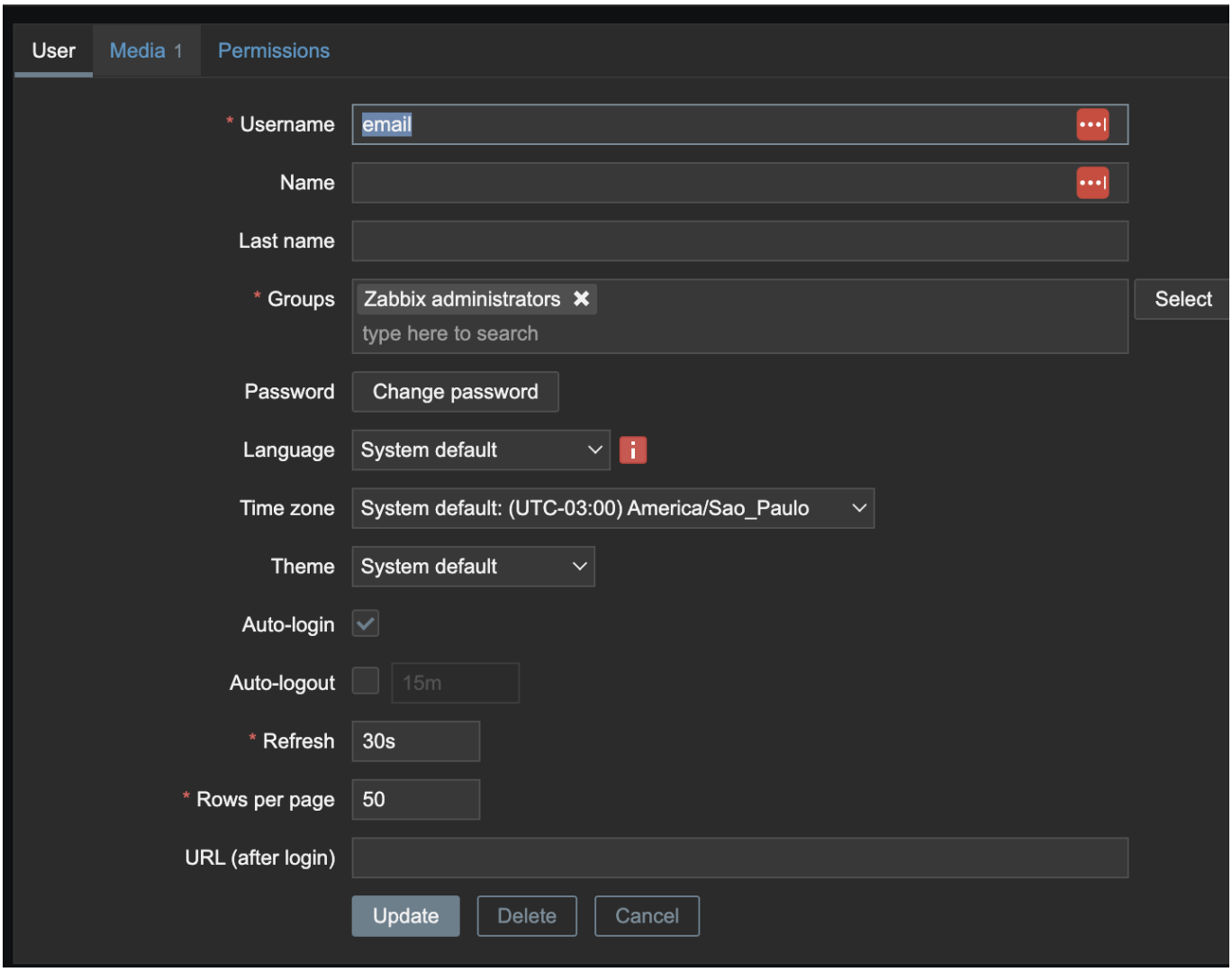
Foi criada um Media Type específico para envio de mensagens por email, com as configurações do servidor SMTP, e o email de destino, com o nome `cbsecsmtp`.


Media type
Message templates 8
Options
* Name
cbsecsmtp
Type
Email
* SMTP server
mail.a2csolutions.com.br
SMTP server port
465
* SMTP helo
a2csolutions.com.br
* SMTP email
cybersec@a2csolutions.com.br
Connection security
None
STARTTLS
SSL/TLS
SSL verify peer
SSL verify host
Authentication
None
Username and password
Username
cybersec@a2csolutio
Password
Change password
Message format
HTML
Plain text
Description
zabbix alert
Enabled
Update
Clone
Delete
Cancel

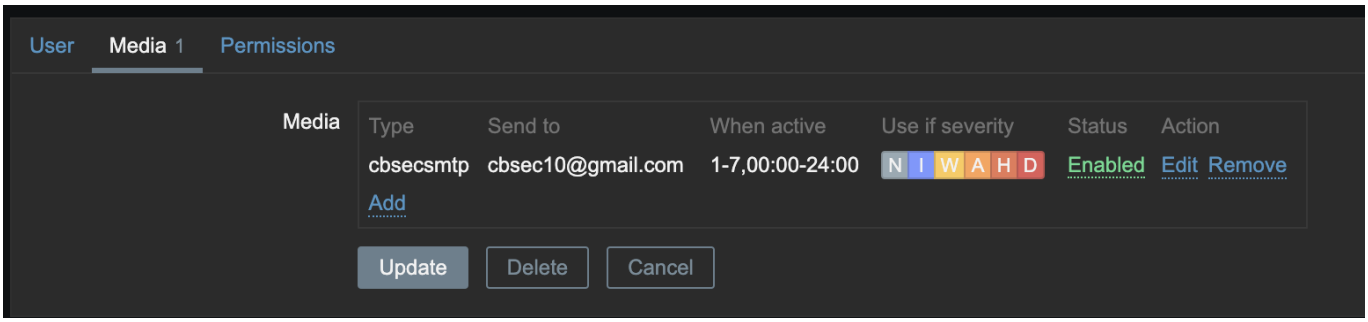


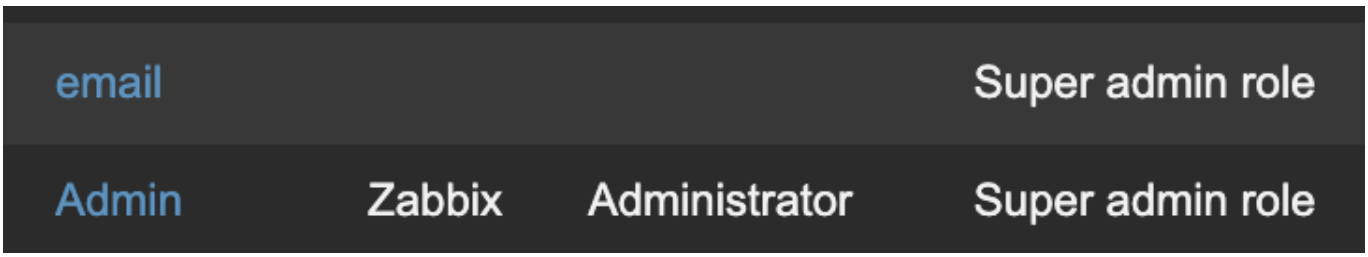
3.2 Configuração de Usuário

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



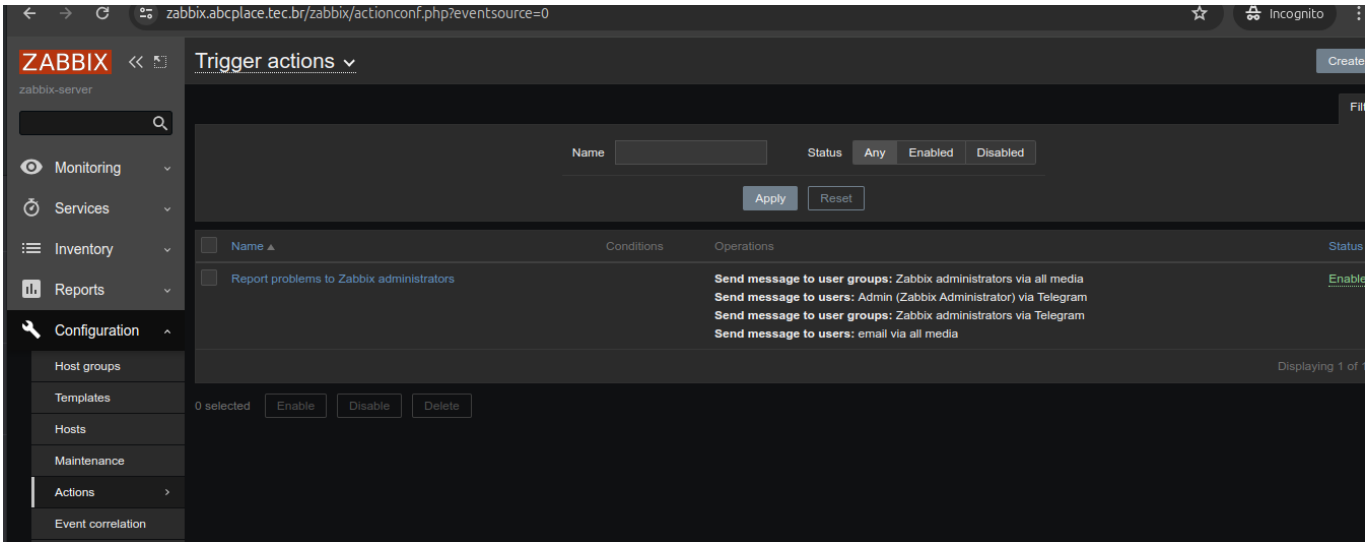
Para este usuário conseguir realizar o envio de emails e ter acesso a actions, há a necessidade de dar a ele permissões de superadmin, e alterar sua Media.





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.


zabbix.abcplace.tec.br/zabbix/actionconf.php?eventsource=0
Incognito
ZABBIX
zabbix-server
Trigger actions
Create
Name
Status
Any
Enabled
Disabled
Apply
Reset
Monitoring
Services
Inventory
Reports
Configuration
Host groups
Templates
Hosts
Maintenance
Actions
Event correlation
Name
Conditions
Operations
Status
Report problems to Zabbix administrators
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
Send message to users: email via all media
0 selected
Enable
Disable
Delete