

Orquestrando Ambiente de Monitoramento Autônomo de Clouds (AWS e Azure)



Bernardo Lankheet



Congresso de TI

WHO AM I

- +10 anos atuando com TI e a 3 anos como consultor
- Ciclista, trilheiro e corredor de rua nas horas vagas
- Eterno Aprendiz e Homelab
- Especialista em Monitoramento e DevOps na JLCP



OPERAÇÃO E MONITORIA TRADICIONAL

ZABBIX

Debian | Ubuntu
CentOS | RHEL

Microsoft

Linux

Data Center 24/7
VSphere / HyperV

Rede

Ambientes
Críticos

Active Directory | Endpoint
File Server | DNS | DHCP

Routing | Switching
Firewall | VPN

OPERAÇÃO E MONITORIA CLOUD

ZABBIX

Debian | Ubuntu
CentOS | RHEL

Data Center 24/7
VSphere / HyperV

Containers
Docker | Kubernetes

Microsoft

Linux

Rede

**Ambientes
Criticos**

Cloud

Microservicos

Active Directory | Endpoint
File Server | DNS | DHCP

Routing | Switching
Firewall | VPN

Azure | AWS |
GCP ...

CONHECIMENTOS NECESSARIOS

O que precisamos conhecer para trabalhar
com o monitoramento de clouds?

- Zabbix;
- Clouds;
- Javascript;
- API's;
- Json;



<https://www.zabbix.com/br/integrations/azure>

Virtual Machines

Azure Cosmos DB for MongoDB

Azure Database for MySQL

Azure Database for Microsoft SQL

Azure Database for PostgreSQL

Storage Accounts

API AZURE

JAVASCRIPT

```
if (!('auth' in data.errors)) {
    try {
        for (var i in types) {
            if (types[i].method === "Microsoft.Sql/servers") {
                mssql_servers = Azure.request('https://management.azure.com/subscriptions/' +
                    + encodeURIComponent(Azure.params.subscription_id) + '/providers/' + types[i].method +
                    '?api-version=' + types[i].version);

                if ('nextLink' in mssql_servers) {
                    mssql_servers = Azure.nextlink(mssql_servers);
                }

                if ('value' in mssql_servers && mssql_servers.value.length > 0) {
                    for (j in mssql_servers.value) {
                        mssql_dbs = Azure.request('https://management.azure.com' +
                            mssql_servers.value[j].id + '/databases?api-version=' + types[i].version);

                        if ('nextLink' in mssql_dbs) {
                            mssql_dbs = Azure.nextlink(mssql_dbs);
                        }
                    }
                }
            }
        }
    }
}
```

API AZURE JAVASCRIPT

Test item

Get value from host

Host address Port

Proxy (no proxy)

Value {"errors": "", "resources": {"value": [{"name": "VM-GRAFANA-01", "id": "/subscriptions/2..."}]}} Time now

Not supported

Previous value Prev. time

End of line sequence LF CRLF

Macros

{\$AZURE.APP.ID}	= 0c
{\$AZURE.DATA.TIMEOUT}	= 15s
{\$AZURE.PASSWORD}	= 1B1'
{\$AZURE.PROXY}	= value
{\$AZURE.SUBSCRIPTION.ID}	= 2c
{\$AZURE.TENANT.ID}	= 002f5a09-d885

Result Result converted to Text

```
{"errors": "", "resources": {"value": [{"name": "VM-GRAFANA-01", "id": "/subscriptions/2..."}]}}
```

Clone Execute now Test Clear history and trends Delete

Result converted to Text

```
{"errors": "", "resources": {"value": [{"name": "VM-GRAFANA-01", "id": "/subscriptions/2..."}]}}
```

VM-GRAFANA-01/providers/Microsoft.Compute/virtualMachines/VM-GRAFANA-01", "type": "Microsoft.Compute/virtualMachines", "location": "eastus2", "properties": {"hardwareProfile": {"vmSize": "Standard_B1ms"}, "provisioningState": "Succeeded", "vmId": "c330f843-8917-43ca-b5bd-f9e4df1d4204", "storageProfile": {"imageReference": {"publisher": "canonical", "offer": "0001-com-ubuntu-server-focal", "sku": "20_04-lts-gen2", "version": "latest", "exactVersion": "20.04.202305150"}, "osDisk": {"osType": "Linux", "name": "VM-GRAFANA-01_OsDisk_1_0846945236914018aada93c3515c8b5f", "createOption": "FromImage", "caching": "ReadWrite", "managedDisk": {"id": "/subscriptions/3ce73c9ec8/resourceGroups/RG-GAFANA-01/providers/Microsoft.Compute/disks/VM-GRAFANA-01_OsDisk_1_0846945236914018aada93c3515c8b5f"}, "deleteOption": "Delete", "dataDisks": [], "diskControllerType": "SCSI"}, "osProfile": {"computerName": "VM-GRAFANA-01", "adminUsername": "", "linuxConfiguration": {"disablePasswordAuthentication": false, "provisionVMAgent": true, "patchSettings": {"patchMode": "ImageDefault", "assessmentMode": "ImageDefault"}, "enableVMAgentPlatformUpdates": false}, "secrets": [], "allowExtensionOperations": true, "requireGuestProvisionSignal": true}, "securityProfile": {"uefiSettings": {"secureBootEnabled": true, "vTpmEnabled": true}, "securityType": "TrustedLaunch"}, "networkProfile": {"networkInterfaces": []}}}}

Virtual Machines



Availability



OS/Data Disk



Networking



CPU and Memory

...

Azure Cosmos DB for MongoDB

Azure Database for MySQL

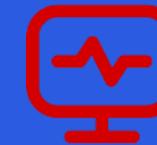
Azure Database for Microsoft SQL

Azure Database for PostgreSQL

Storage Accounts

Virtual Machines

Azure Cosmos DB for MongoDB



Availability



Data, Document, Index and Partition usage



Latency and Requests



Errors

...

Azure Database for MySQL

Azure Database for Microsoft SQL

Azure Database for PostgreSQL

Storage Accounts

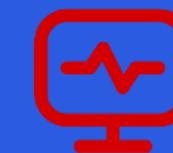
Virtual Machines

Azure Cosmos DB for MongoDB

Azure Database for MySQL

Azure Database for Microsoft SQL

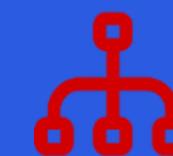
Azure Database for PostgreSQL



Availability and Connections



CPU, Memory and Storage



Networking



Errors

...



Single Server and
Flexible Server

Storage Accounts

Virtual Machines

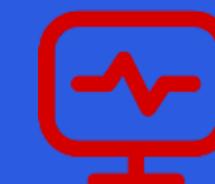
Azure Cosmos DB for MongoDB

Azure Database for MySQL

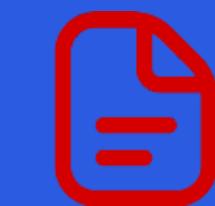
Azure Database for Microsoft SQL

Azure Database for PostgreSQL

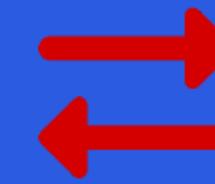
Storage Accounts



Availability and Capacity



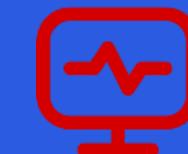
Blobs, Files, Queues and Tables



Transactions

...

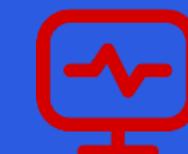
IP Externos



Disponibilidade

Validação Segurança principais portas

API Gateway



Taxa de Erros

Zabbix Agent



Criação de Scripts para instalação
automática de Agents

Tags



jsonpath para identificação de recursos e conta

LLD Override para template



Override para Template de S.O com base na tag de S.O

Azure service principal

```
bernardo@Azure:~$ az ad sp create-for-rbac --name zabbix --role reader --scope /subscriptions/2dde4b29-XXXXXXXXXX-5297-4042-8175-086ce73c9ec8
Found an existing application instance: (id) e589d1a6-b1e7-43f0-a809-5febb5ad5102. We will patch it.
Creating 'reader' role assignment under scope '/subscriptions/2dde4b29-5297-4042-8175-086ce73c9ec8'
  Role assignment already exists.
```

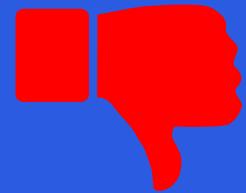
The output includes credentials that you must protect. Be sure that you do not include these credentials in your code or check the credentials into your source control. For more information, see <https://aka.ms/azadsp-cli>

```
{
  "appId": "0d5178fc-XXXXXXXXXX-b42eb8731dda",
  "displayName": "zabbix",
  "password": "v.A8Q~d2TXXXXXXXXXXg097TxwkVrPpzak.",
  "tenant": "002f5a09-XXXXXXXXXX-b40924e5b486"
}
```

<https://www.zabbix.com.br/integrations/azure>

DEMO

LIMITE DE REQUISIÇÕES API



Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
Information					Azure: There are errors in requests to API	21s	No		AZU
Information	17:03:20	RESOLVED			Azure: There are errors in requests to API			Zabbix has received errors in response to API requests.	
Warning	17:03:20	RESOLVED			Azure: Virtual machine is in unknown state			Zabbix has received errors in response to API requests.	

Failed to receive data:

Premium%20Data%20Disk%20Cache%20Read%20Miss , Premium%200S%20Disk%20Cache%20Read%20Hit , Premium%200S%20Disk%20Cache%20Read%20Miss , VM%20Cached%20Bandwidth%20Consumed%20Percentage , VM%20Cached%20IOPS%20Consumed%20Percentage , VM%20Uncached%20Bandwidth%20Consumed%20Percentage , VM%20Uncached%20IOPS%20Consumed%20Percentage , Network%20In%20Total , Network%20Out%20Total , Available%20Memory%20Bytes : Error: cannot get URL: Timeout was reached.

AZURE



<https://www.zabbix.com/br/integrations/aws>

ECS (Elastic Compute Cloud)

RDS (Relational Database Service)

S3 (Simple Storage Service)

ECS Cluster (Elastic Container Service)

Cost Explorer



```
1      canonical_uri = '/' + uri,
2      canonical_headers = 'content-encoding:amz-1.0\n' + 'host:' + host + '\n' +
3      'x-amz-date:' + amzdate + '\n',
4      signed_headers = 'content-encoding;host;x-amz-date',
5      canonical_request = method + '\n' + canonical_uri + '\n' + params + '\n' +
6      canonical_headers + '\n' + signed_headers + '\n' + sha256(data),
7      credential_scope = date + '/' + region + '/' + service + '/' + 'aws4_request',
8      request_string = 'AWS4-HMAC-SHA256' + '\n' + amzdate + '\n' + credential_scope
9      + '\n' + sha256(canonical_request),
10     key = AwsEC2.sign('AWS4' + AwsEC2.params.secret_key, date);
11
12     key = AwsEC2.sign(key, region);
13     key = AwsEC2.sign(key, service);
14     key = AwsEC2.sign(key, 'aws4_request');
15
16     var request = new HttpRequest(),
17     url = 'https://' + host + canonical_uri + '?' + params;
18
19     if (typeof AwsEC2.params.proxy !== 'undefined' && AwsEC2.params.proxy !== '') {
20         request.setProxy(AwsEC2.params.proxy);
21     }
22     request.addHeader('x-amz-date: ' + amzdate);
23     Zabbix.log(4, '[ AWS EC2 ] Sending request: ' + url);
```

CANONICAL_URI = '/' + URI

Test item

Get value from host

Host address Port

+ SHA256 Proxy PRX-MOB2CON-AW...

Value Time now

Previous value Prev. time

End of line sequence LF CRLF

Macros

{\$AWS.ACCESS.KEY.ID}	⇒ <input type="text"/>
{\$AWS.PROXY}	⇒ <input type="text" value="value"/>
{\$AWS.REGION}	⇒ <input type="text" value="us-west-2"/>
{\$AWS.SECRET.ACCESS.KEY}	⇒ <input type="text" value="40Sl"/>

Result Result converted to Text

HEADERS + '\n'

ST),

.....

ECS (Elastic Compute Cloud)



Availability



CPU and CPU Credits



Disk



EBS and CloudWatch



Networking

...

RDS (Relational Database Service)

S3 (Simple Storage Service)

ECS Cluster (Elastic Container Service)

Low Level Discovery



Alarms Discovery



Alarm State and Reason



Read, Write, Throughput



Status



ECS (Elastic Compute Cloud)

RDS (Relational Database Service)



Availability



CPU and CPU Credits



Disk



EBS and CloudWatch



Networking



Memory



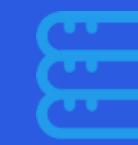
S3 (Simple Storage Service)

ECS Cluster (Elastic Container Service)

Low Level Discovery



Aurora Metrics Discovery



Aurora MySQL Metrics Discovery



Alarms Discovery



Events Discovery



ECS (Elastic Compute Cloud)

RDS (Relational Database Service)

S3 (Simple Storage Service)



Alarms



Latency



Replication



Requests

...

ECS Cluster (Elastic Container Service)

Cost Explorer

Low Level Discovery



Bucket Alarms Discovery



Alarm State and
Reason



ECS (Elastic Compute Cloud)

RDS (Relational Database Service)

S3 (Simple Storage Service)

ECS Cluster (Elastic Container Service)

 Container instance count

 CPU utilization

 Memory utilization

 Network utilization

 Service, task count

Cost Explorer

 Cluster services Discovery

 Alarms Discovery



ECS (Elastic Compute Cloud)

RDS (Relational Database Service)

S3 (Simple Storage Service)

ECS Cluster (Elastic Container Service)

Cost Explorer



IP Externos

Disponibilidade

Validação Segurança principais portas

Agente SSM (Systems Manager)

Validações de instâncias sem Agente de SSM

Billing-Costs

Comparativo de gastos de recursos

Zabbix Agent

Criação de Scripts para instalação
automática de Agents



IAM policy Zabbix

The screenshot shows the 'Create New Policy' wizard in the AWS IAM console. The current step is 'Etapa 1: Especifique permissões' (Specify permissions). The title is 'Especifique permissões' with a 'Informações' link. A note says 'Adicione permissões selecionando serviços, ações, recursos e condições. Crie instruções de permissão usando o editor JSON.' Below is the 'Editor de políticas' (Policy Editor) with the 'JSON' tab selected. The JSON code is:

```
1 Version: "2012-10-17",
2 Statement: [
3   {
4     Action: [
5       "cloudwatch:DescribeAlarms",
6       "cloudwatch:GetMetricData",
7       "ec2:DescribeInstances",
8       "ec2:DescribeVolumes",
9       "ec2:DescribeRegions",
10      "rds:DescribeEvents",
11      "rds:DescribeDBInstances",
12      "ecs:DescribeClusters",
13      "ecs>ListServices",
14      "ecs>ListTasks",
15      "ecs>ListClusters",
16      "s3>ListAllMyBuckets",
17      "s3:GetBucketLocation"
18    ],
19    Effect: "Allow",
20    Resource: "*"
21  }
22 ]
23 ]
24 ]
```

The right panel has tabs for 'Visual' (disabled), 'JSON' (selected), 'Ações' (Actions), and a copy icon. It includes sections for 'Editar instrução' (Edit instruction), 'Selecionar uma instrução' (Select an instruction), and a button '+ Adicionar nova instrução' (Add new instruction).

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create-console.html

IAM policy Zabbix

The screenshot shows the AWS IAM 'Create access key' page. At the top, a green banner displays the message: 'Access key created' with a checkmark icon. Below it, a sub-banner states: 'This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' The navigation path is: IAM > Users > zabbix > Create access key. On the left, there are three steps: Step 1 (Access key best practices & alternatives), Step 2 - optional (Set description tag), and Step 3 (Retrieve access keys). The main content area is titled 'Retrieve access keys' and contains an 'Access key' section. It includes a note: 'If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.' Below this, the Access key and Secret access key are listed. The Access key is 'AI/RRUFF' and the Secret access key is 'p7JPcbiO3'. A 'Hide' link is next to the secret key. At the bottom, there's a section titled 'Access key best practices' with the following bullet points:

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

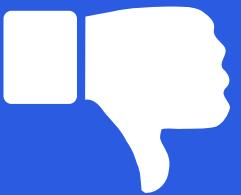
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

At the bottom right, there are two buttons: 'Download .csv file' and 'Done'.

DEMO

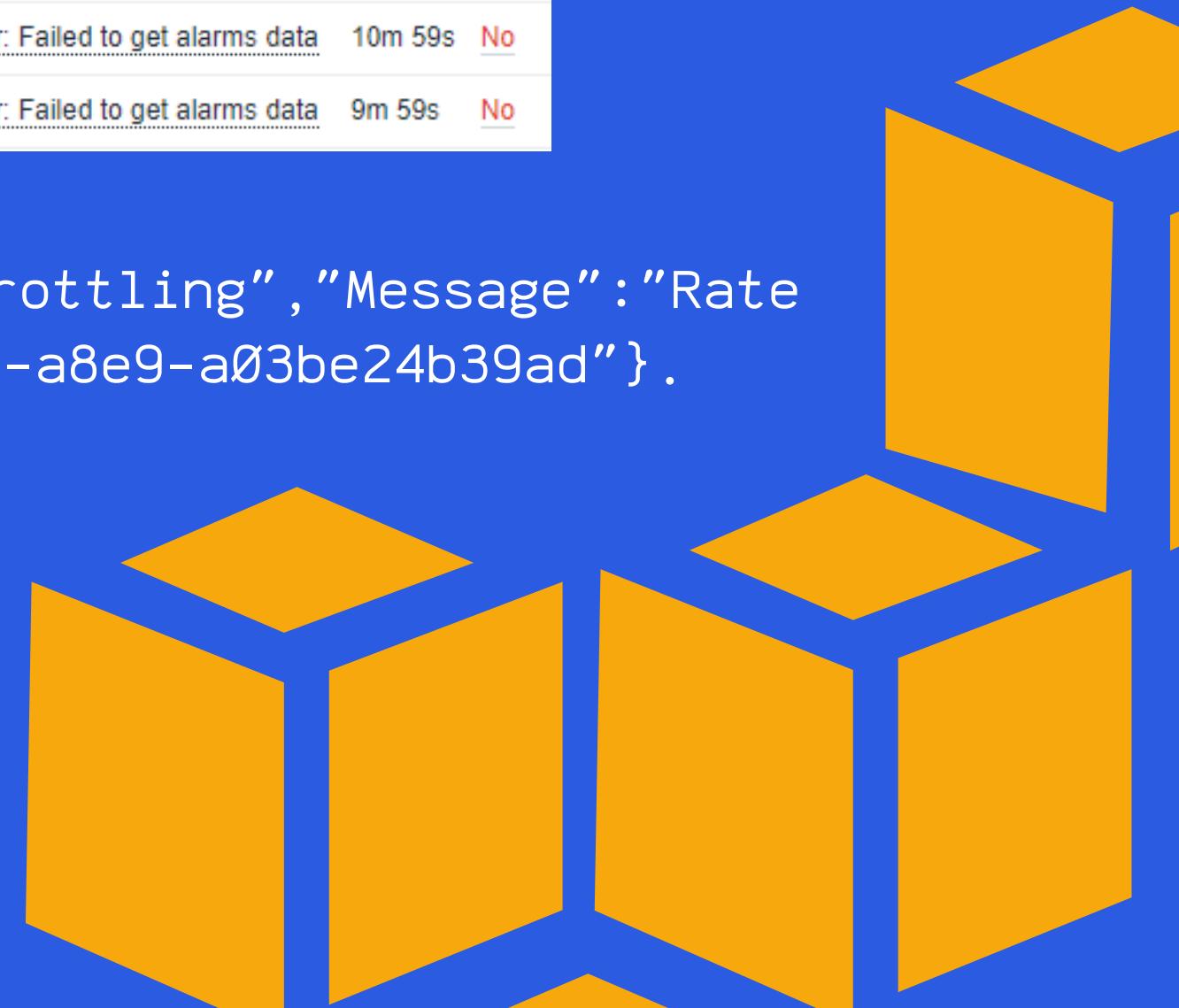


LIMITE DE REQUISIÇÕES API



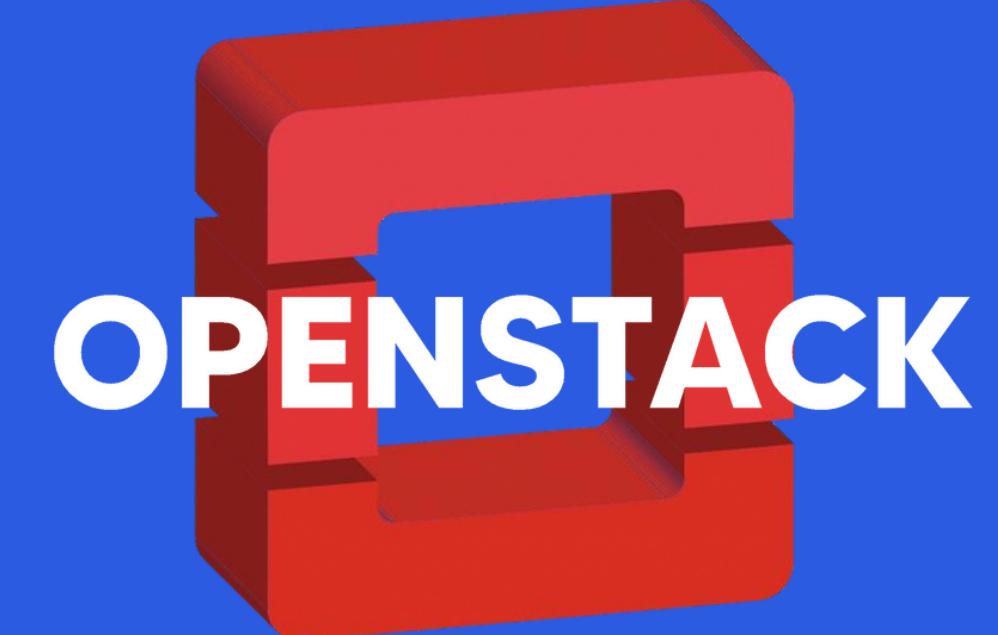
PROBLEM	AWS ECS Cluster: Failed to get alarms data	13m 54s	No
PROBLEM	AWS EC2: Failed to get alarms data	13m 54s	No
17:05:01 RESOLVED	AWS ECS Cluster: Failed to get alarms data	10m 59s	No
17:04:01 RESOLVED	AWS ECS Cluster: Failed to get alarms data	9m 59s	No

Request failed with status code 400: {"Error":{"Code":"Throttling","Message":"Rate exceeded","Type":"Sender"},"RequestId":"f0c97dc0-7511-438e-a8e9-a03be24b39ad"}.



CLOUDS
SUPORTADAS
NATIVAMENTE

ZABBIX



<https://www.zabbix.com/br/integrations>



Obrigado!

✓ Bernardo Lankheet

✓ JLCP

⌚ @bernardolankheet

linkedin @bernardolankheet

facebook @bernardolankheet

