

*Essa atividade é necessária quando precisamos integrar o Dynatrace com a cloud pública da AWS.*

## Guia passo a passo

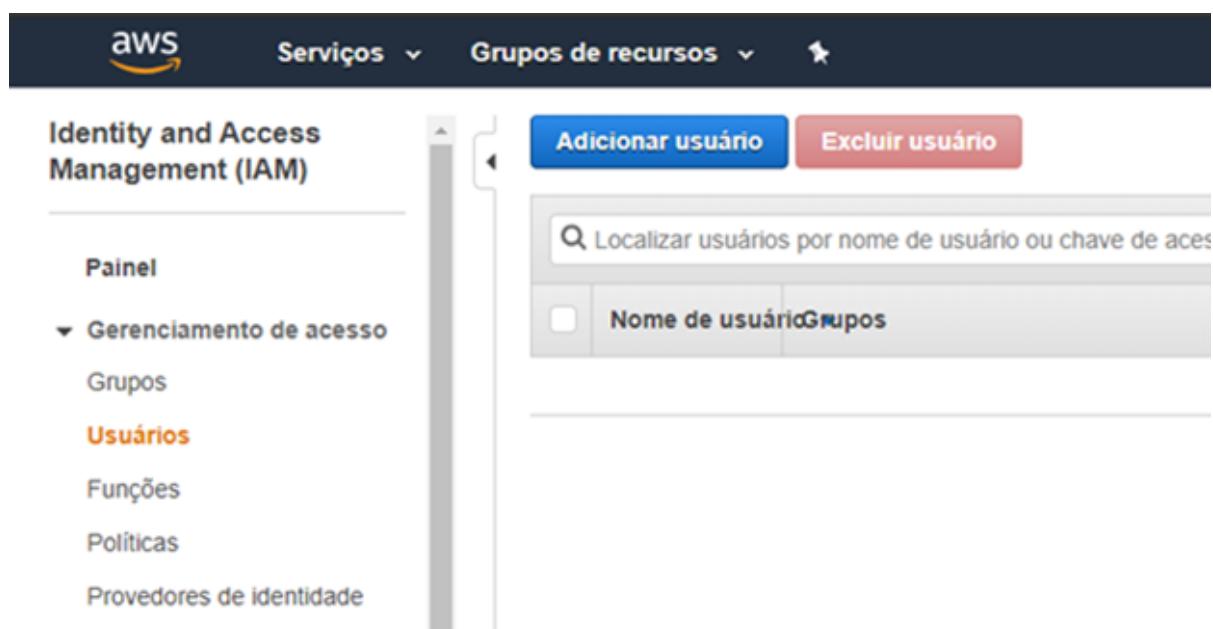
Etapas necessárias:

1. Configurações AWS
2. Configurações no Dynatrace

As configurações na console do IAM AWS devem ser seguidas igualmente como o tutorial, para evitar falhas de acesso/coleta.

## Configurações AWS:

Criar usuário para o Dynatrace.



Dentro da Console da AWS em IAM criar um usuário para o Dynatrace.

Clicar em adicionar usuário

Colocar por Exemplo o nome: “Dynatrace\_monitoring\_user”, para uma melhor identificação.

Adicionar usuário

Definir detalhes do usuário

Você pode adicionar vários usuários de uma só vez com o mesmo tipo de acesso e permissões. [Saiba mais](#)

Nome de usuário\*

Adicionar outro usuário

Selezione o tipo de acesso à AWS

Selezione como esses usuários vão acessar a AWS. As chaves de acesso e as senhas geradas automaticamente são fornecidas na última etapa. [Saiba mais](#)

Tipo de acesso\*  Acesso programático  
Habilita uma **ID da chave de acesso** e **chave de acesso secreta** para a API da AWS, CLI, SDK, e outras ferramentas de desenvolvimento.

Acesso ao Console de Gerenciamento da AWS  
Habilita uma **senha** que permite que os usuários façam login no Console de Gerenciamento da AWS.

\* Obrigatório

[Cancelar](#) [Próximo: Permissões](#)

Na parte de definir limite de permissões configure conforme sua regra de negócio.

## Informação

A partir deste ponto será criada uma nova police para acesso.

Obs.: Neste ambiente de testes não existiam polices de usuário criadas.

## Adicionar usuário

1 2 3 4 5

### Definir permissões



Adicionar usuário ao grupo



Copiar as permissões de um usuário existente



Anexar políticas existentes de forma direta

#### Conceitos básicos de grupos

Você ainda não criou nenhum grupo. Usar grupos é uma prática recomendada para gerenciar as permissões dos usuários por função de trabalho, acesso ao serviço da AWS, ou suas permissões personalizadas. Comece a criar um grupo. [Saiba mais](#)

[Criar um grupo](#)

### Definir limite de permissões

Defina um limite de permissões para controlar o máximo de permissões que este user pode ter. Este é um recurso avançado usado para delegar o gerenciamento de permissões para outros. [Saiba mais](#)

- Criar user sem limite de permissões
- Usar um limite de permissões para controlar o máximo de permissões de user

[Cancelar](#)

[Anterior](#)

[Próximo: Tags](#)

## Adicionar usuário

1 2 3 4 5

### Definir permissões



Adicionar usuário ao grupo



Copiar as permissões de um usuário existente



Anexar políticas existentes de forma direta

[Criar política](#)



[Filtrar políticas](#)

Pesquisar

Exibindo 516 resultados

	Nome da política	Digite	Usado como
<input type="checkbox"/>	AdministratorAccess	Função de trabalho	Nenhum
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	Gerenciado pela AWS	Nenhum
<input type="checkbox"/>	AlexaForBusinessFullAccess	Gerenciado pela AWS	Nenhum
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	Gerenciado pela AWS	Nenhum
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	Gerenciado pela AWS	Nenhum
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	Gerenciado pela AWS	Nenhum

[Cancelar](#)

[Anterior](#)

[Próximo: Tags](#)

Observe que nesta parte é possível dar permissão ao serviço que se deseja liberar o acesso. Abaixo estou concedendo acesso para a EC2, API Gateway, S3, CloudWatch, Lambda.

## Criar política

A política define as permissões da AWS que você pode atribuir a um usuário, um grupo ou uma função. É possível criar e editar uma política no editor visual e usar JSON. Saiba mais.

[Editor visual](#) [JSON](#) [Importar política gerenciada](#)

[Expandir todos](#) [Recolher todos](#)

» API Gateway (1 ação)	<a href="#">Clonar</a>   <a href="#">Remover</a>
» EC2 (16 ações)	<a href="#">Clonar</a>   <a href="#">Remover</a>
» CloudWatch (12 ações)	<a href="#">Clonar</a>   <a href="#">Remover</a>
» S3 (41 ações)	<a href="#">Clonar</a>   <a href="#">Remover</a>
» Lambda (12 ações)	<a href="#">Clonar</a>   <a href="#">Remover</a>

[Adicionar permissões adicionais](#)

Contagem de caracteres: 2.998 de 6.144.

[Cancelar](#) [Revisar política](#)

Para esta política defini o nome para: "Dynatrace\_monitoring\_policy".

## Criar política

### Revisar política

Nome\*

Use caracteres alfanuméricos e "\w\-\\_". Máximo de 128 caracteres.

Descrição

Máximo de 1000 caracteres. Use caracteres alfanuméricos e "\w\-\\_".

#### Resumo

Esta política define algumas ações, recursos ou condições que não fornecem permissões. Para conceder acesso, as políticas devem ter uma ação que tenha um recurso ou condição aplicável. Para obter detalhes, escolha Exibir restantes. [Saiba mais](#)

Serviço	Nível de acesso	Recurso	Condição para solicitação
Permitir (5 de 224 serviços) <a href="#">Exibir restantes 219</a>			
API Gateway	Tela cheia: Leitura	Todos os recursos	Nenhum
CloudWatch	Tela cheia: Leitura, Atribuição de tags (tagging)	Vários	Nenhum
EC2	Tela cheia: Leitura	Todos os recursos	Nenhum

\* Obrigatório

[Cancelar](#) [Anterior](#) [Criar política](#)

Em seguida basta clicar em criar.

Essa será a saída:

Adicionar usuário

1 2 3 4 5

Definir permissões

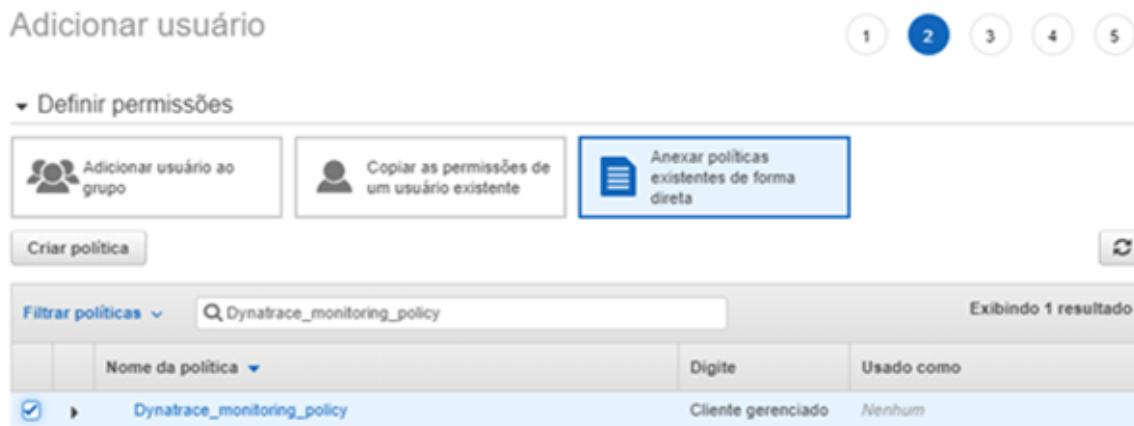
Anexar políticas existentes de forma direta

Criar política

Filtrar políticas ▾

Nome da política	Digite	Usado como
Dynatrace_monitoring_policy	Cliente gerenciado	Nenhum

Exibindo 1 resultado



Se achar pertinente colocar uma TAG para identificar o usuário e suas funções ficara a critério.

Podemos usar estes dados para controlar recursos ou mesmo permissões.

Recomendado usar essa TAG

Chave: dynatrace-monitored

Value: true

Adicionar usuário

1 2 3 4 5

e-mail, ou podem ser descritivas, como um cargo. Você pode usar as tags para organizar, rastrear ou controlar o acesso para esse usuário. [Saiba mais](#)

Chave	Valor (opcional)	Remover
dynatrace-monitored		



Agora adicione o usuário

## Adicionar usuário

1 2 3 4 5

### Revisar

Revise suas escolhas. Depois de criar o usuário, você pode visualizar e fazer download da senha e da chave de acesso geradas automaticamente.

#### Detalhes do usuário

Nome de usuário	Dynatrace_monitoring_user
Tipo de acesso AWS	Acesso programático: com uma chave de acesso
Limite de permissões	Limite de permissões não definido

#### Resumo de permissões

As políticas a seguir serão anexadas ao usuário mostrado acima.

Digite	Nome
Política gerenciada	<a href="#">Dynatrace_monitoring_policy</a>

#### Tags

O novo usuário receberá a seguinte tag

Chave	Valor
dany	Ferramenta de monitoramento usada pela producao

[Cancelar](#) [Anterior](#) [Criar usuário](#)

## Adicionar usuário

1 2 3 4 5

### ✓ Éxito

Você criou com êxito os usuários mostrados abaixo. Você pode visualizar e fazer download das credenciais de segurança do usuário. Você também pode enviar um e-mail aos usuários com as instruções para fazer login no Console de Gerenciamento da AWS. Esta é a última vez que essas credenciais estarão disponíveis para download. No entanto, você pode criar novas credenciais a qualquer momento.

Os usuários com acesso ao Console de Gerenciamento da AWS podem fazer login em:  
<https://832652334502signin.aws.amazon.com/console>

 Fazer download .csv

	Usuário	ID da chave de acesso	Chave de acesso secreta
▼	 Dynatrace_monitoring_user	AKIA4DXPSKWTLM777OZU	***** <a href="#">Exibir</a>

-  Usuário Dynatrace\_monitoring\_user criado
-  Política anexada Dynatrace\_monitoring\_policy ao usuário Dynatrace\_monitoring\_user
-  Chave de acesso criada para o usuário Dynatrace\_monitoring\_user

Copie as respectivas chaves!

É possível definir o que será monitorado com a criação de chaves, conforme exemplo.

Abaixo segue exemplo de configuração

New EC2 Experience  
Tell us what you think

EC2 Dashboard [New](#)

Events [New](#)

Tags

Reports

Limits

**INSTANCES**

**Instances**

Instance Types

Launch Templates [New](#)

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

**IMAGES**

AMIs

Launch Instance

Filter by tags and attributes or search by keyword

Name Instance ID Instance Type Availability Zone Instance State Status Checks

i-05b0d8e7f27613c18 t2.micro us-east-2c running 2/2 checks ...

Instance: i-05b0d8e7f27613c18 Public DNS: ec2-18-222-101-46.us-east-2.compute.amazonaws.com

Description Status Checks Monitoring Tags

Add/Edit Tags

Key	Value
This resource currently has no tags	

**Add/Edit Tags**

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value
dynatrace-monitored	true

Create Tag Cancel Save

Add/Edit Tags

Key	Value
This resource currently has no tags	



Aqui segue um arquivo .json com todas as regras necessárias para obter as métricas da AWS.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "autoscaling:DescribeAutoScalingGroups",  
        "cloudwatch:GetMetricData",  
        "ec2:DescribeAvailabilityZones",  
        "ec2:DescribeInstances",  
        "ec2:DescribeVolumes",  
        "elasticloadbalancing:DescribeLoadBalancers",  
        "elasticloadbalancing:DescribeTags",  
        "elasticloadbalancing:DescribeInstanceHealth",  
        "elasticloadbalancing:DescribeListeners",  
        "elasticloadbalancing:DescribeRules",  
        "elasticloadbalancing:DescribeTargetHealth",  
        "rds:DescribeDBInstances",  
        "rds:DescribeEvents",  
        "rds>ListTagsForResource",  
        "dynamodb>ListTables",  
        "dynamodb>ListTagsOfResource",  
        "lambda>ListFunctions",  
        "lambda>ListTags",  
        "elasticbeanstalkDescribeEnvironments".  
      ]  
    }  
  ]  
}
```

```
"elasticbeanstalk:DescribeEnvironmentResources",
"s3>ListAllMyBuckets",
"sts:GetCallerIdentity",
"cloudformation>ListStackResources",
>tag:GetResources",
>tag:GetTagKeys",
"cloudwatch>ListMetrics",
"kinesisvideo>ListStreams",
"sns>ListTopics",
"sqs>ListQueues",
"ec2>DescribeNatGateways",
"ec2>DescribeSpotFleetRequests",
"kinisis>ListStreams",
"es>ListDomainNames",
"cloudfront>ListDistributions",
"firehose>ListDeliveryStreams",
"elasticmapreduce>ListClusters",
"kinisisanalytics>ListApplications",
"elasticache>DescribeCacheClusters",
"elasticfilesystem>DescribeFileSystems",
"ecs>ListClusters",
"redshift>DescribeClusters",
"rds>DescribeDBClusters",
"apigateway>GET"
],
"Resource": "*"
}
]
}
```

## Configurações no Dynatrace

Para realizar a configuração no Dynatrace basta acessar:

Settings→Cloud and Virtualization→AWS Logo em seguida configurar conforme imagem abaixo:

The screenshot shows the 'Cloud and virtualization' section of the Dynatrace configuration interface. On the left, there's a sidebar with several options: 'Cloud and virtualization' (selected), 'Connect cloud and virtualization types', 'Overview', 'AWS' (selected), 'VMware', 'Azure', 'Cloud Foundry', and 'Kubernetes'. Below these are sections for 'Server-side service monitoring' and 'Log Monitoring'. Under 'Log Monitoring', there's a sub-section for 'Anomaly detection'. On the right, the main configuration area is shown for the 'AWS' connection. It includes fields for 'Name this connection' (set to 'AWS teste Instance Lab'), 'Access Key ID' (set to 'AKIA4DXPSKWTLM777OZU'), 'Secret access key' (left empty), 'AWS partition' (set to 'Default'), and 'Resources monitoring method' (set to 'Monitor resources selected by tag'). Below this, there's a section for monitoring resources tagged with 'dynatrace-monitored': a key field contains 'dynatrace-monitored' and a value field contains 'true'. There are also empty fields for additional keys and values.

Cloud and virtualization

Connect cloud and virtualization types

Overview

AWS

VMware

Azure

Cloud Foundry

Kubernetes

Server-side service monitoring

Manage and customize service monitoring

Log Monitoring

Set up management of logs

Anomaly detection

Configure detection sensitivity

Name this connection

AWS teste Instance Lab

Access Key ID

AKIA4DXPSKWTLM777OZU

Secret access key

Leave empty if you don't want to change existing key

AWS partition

Default

Resources monitoring method

Monitor resources selected by tag

Monitor resources tagged with any of the following tags (up to 10 entries):

key dynatrace-monitored value true

key value

Aqui é necessário informar

Nome da Conexão: {Colocar um nome logico conforme a subscription}

Access Key ID: {Pertinente ao usuário criado nos passos anteriores}

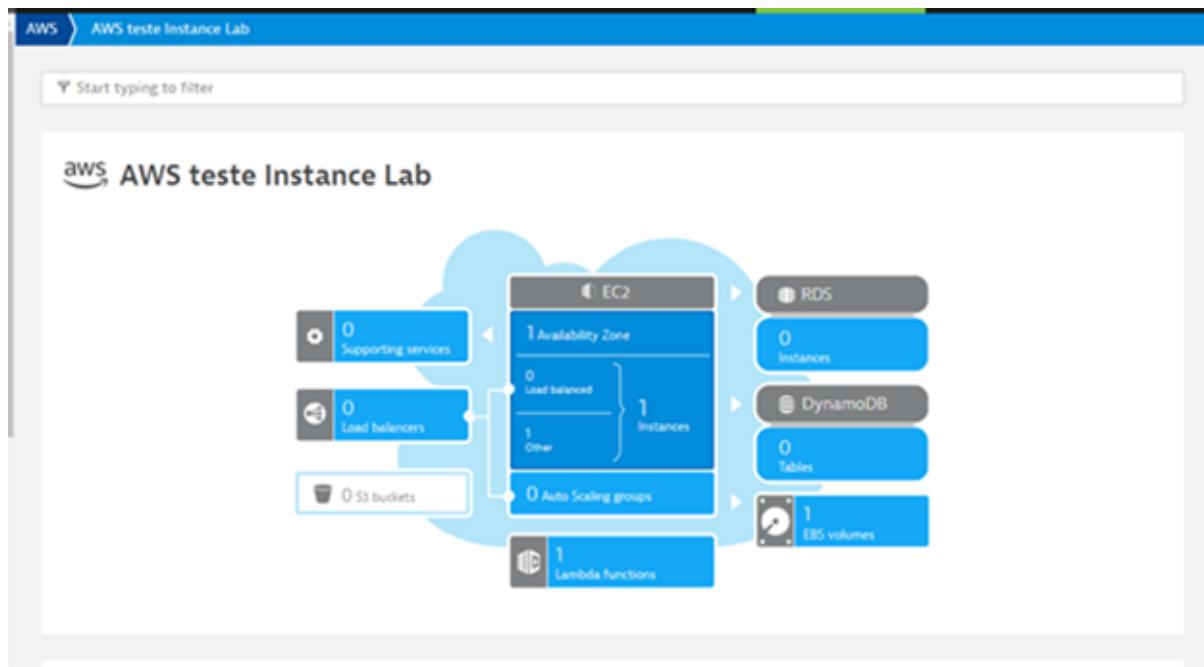
Secret access Key: {Criada nos passos anteriores}

Resources monitoring method: {Alterar para, Monitor resources selected by tag}

Essa opção define que somente componentes que tenham essa TAG serão monitoradas.

Ao finalizar clique em salvar.

Após alguns minutos já teremos as métricas capturadas.



Agora o ambiente AWS já está disponível e eventos a nível cloud serão identificados.