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

Guia passo a passo

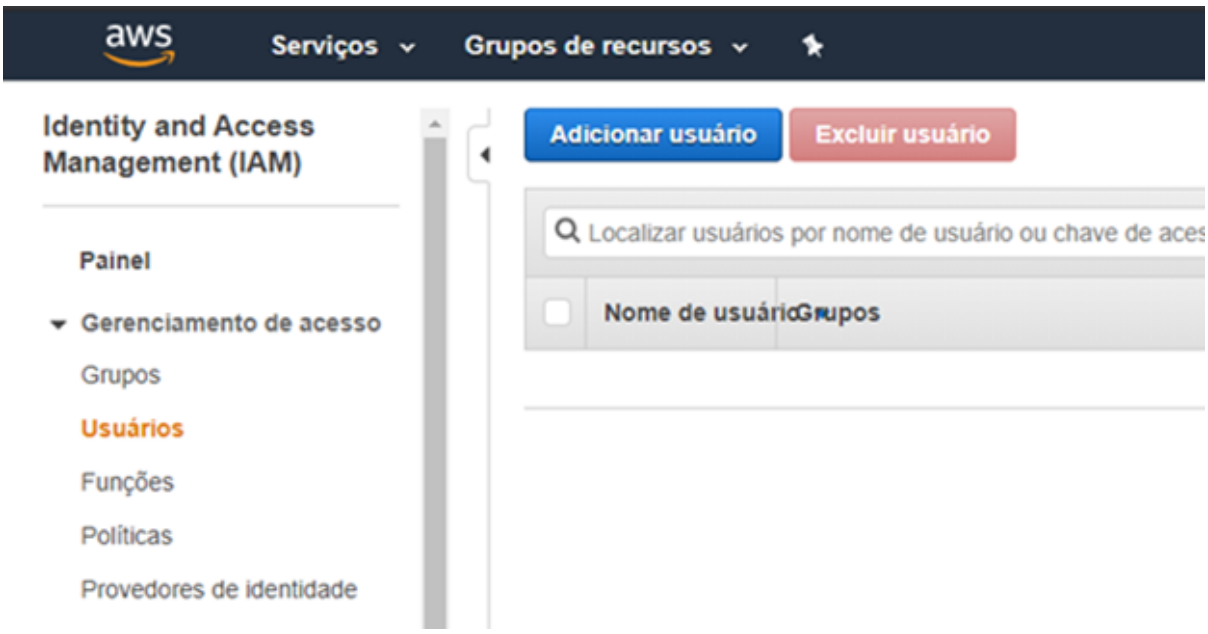
Etapas necessárias:

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:

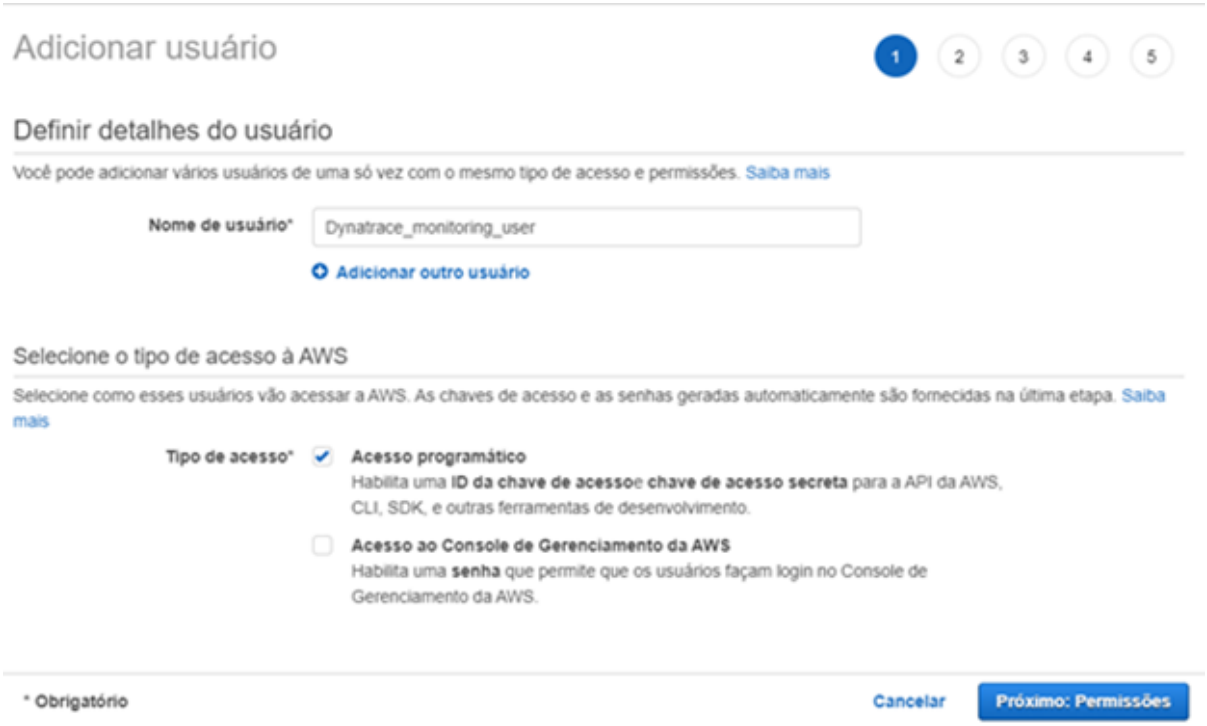
Criar usuário para o Dynatrace.



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.

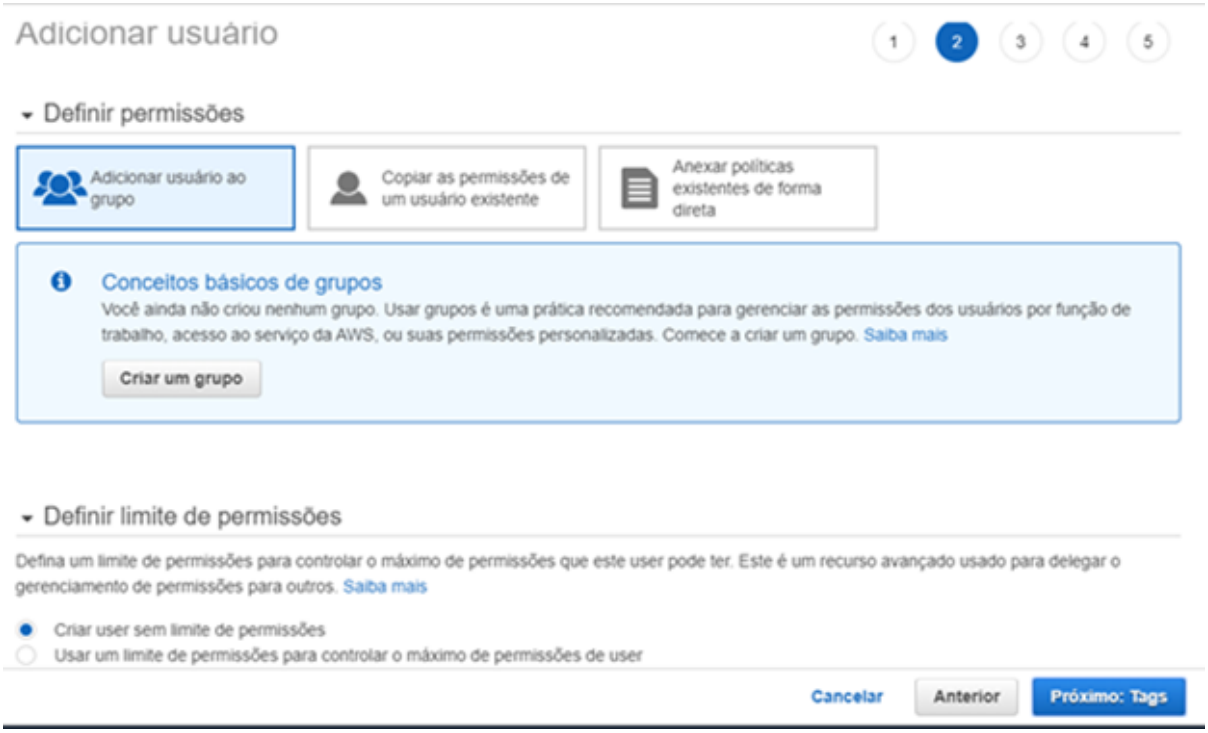


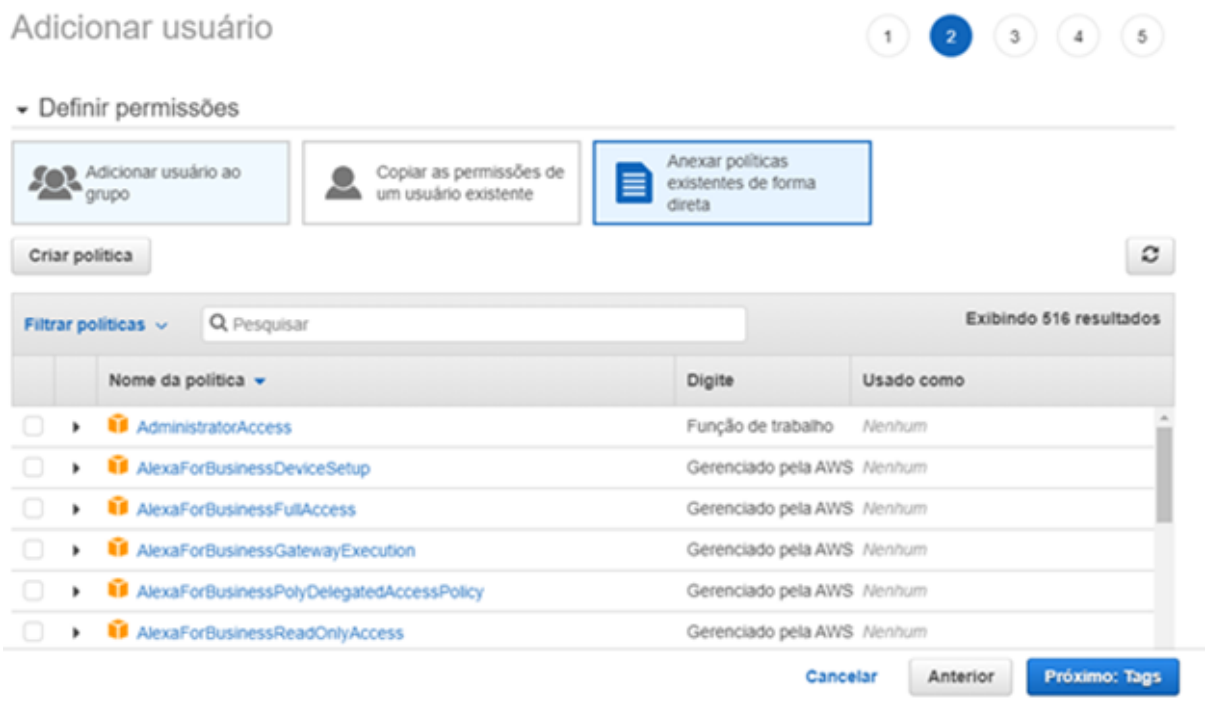
Na parte de definir limite de permissões configure conforme sua regra de negócio.

Informação

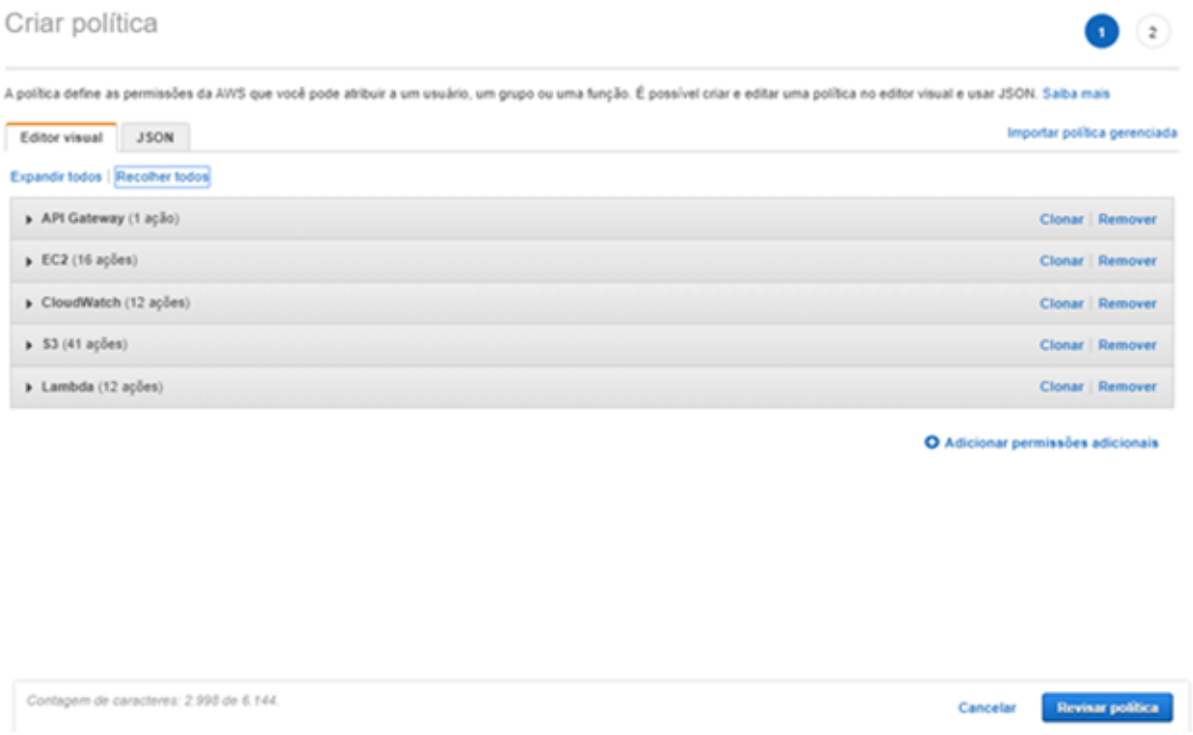
A partir deste ponto será criada uma nova police para acesso.

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

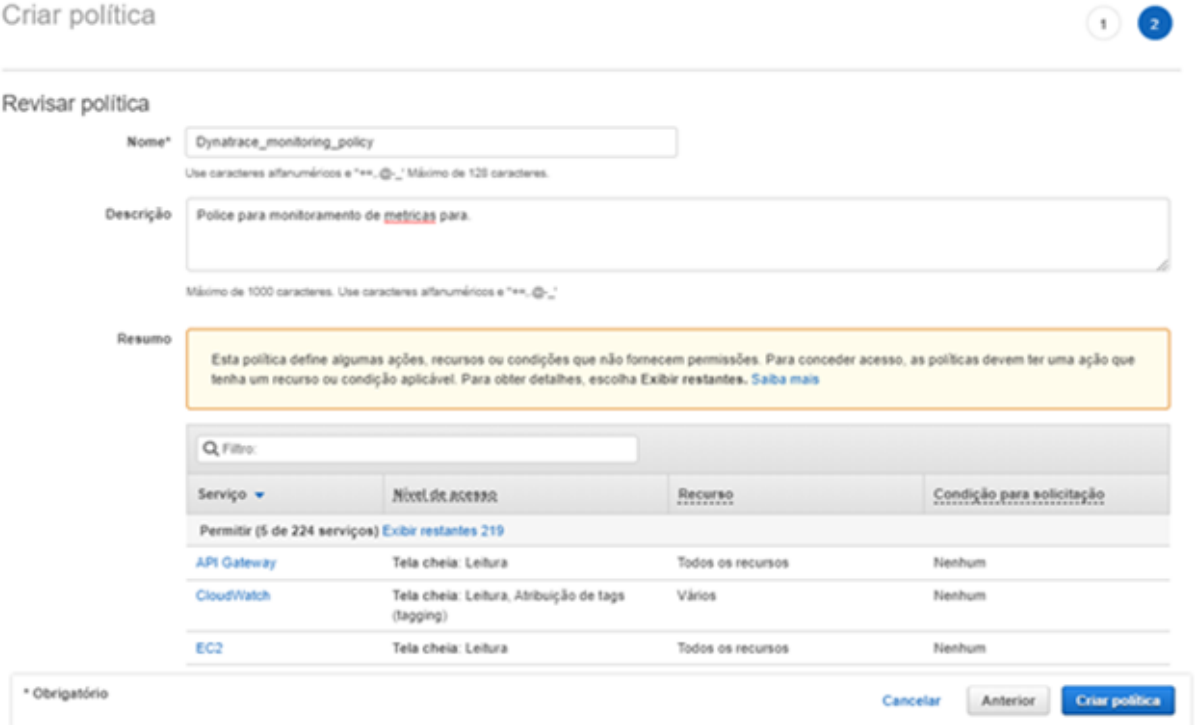




Observe que nesta parte é possível dar permissão ao serviço que se deseja liberar o acesso. Abaixo estou concedendo acesso para a EC2, API Gateway, S3, CloudWatch, Lambda.



Para está politica defini o nome para: “Dynatrace_monitoring_policy”.



Em seguida basta clicar em criar.

Essa será a saída:

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

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.

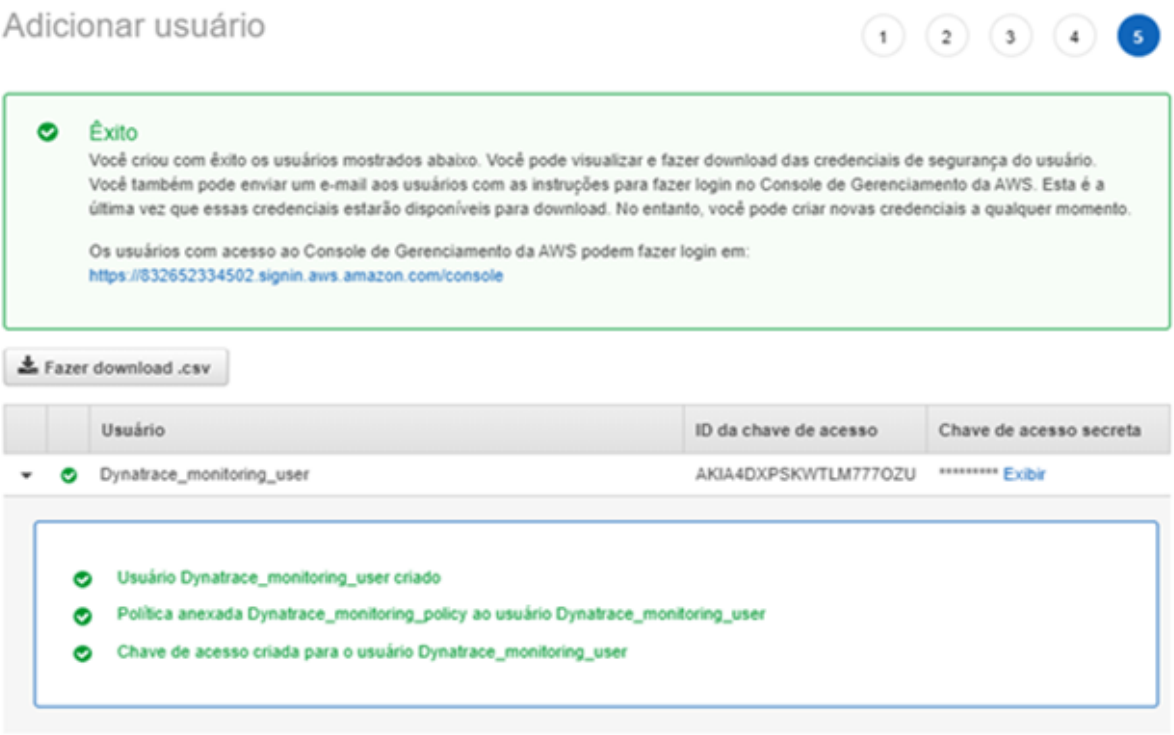
Digite	Nome
Política gerenciada	Dynatrace_monitoring_policy

Tags

O novo usuário receberá a seguinte tag

Chave	Valor
dany	Ferramenta de monitoramento usada pela producao

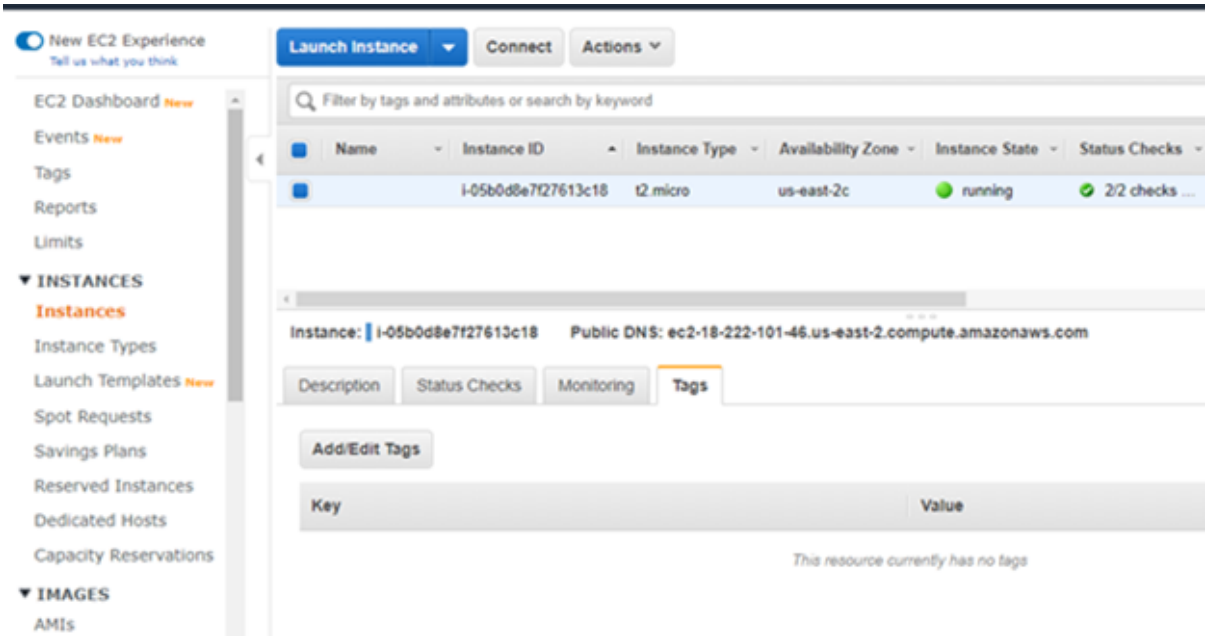
Cancelar Anterior Criar usuário

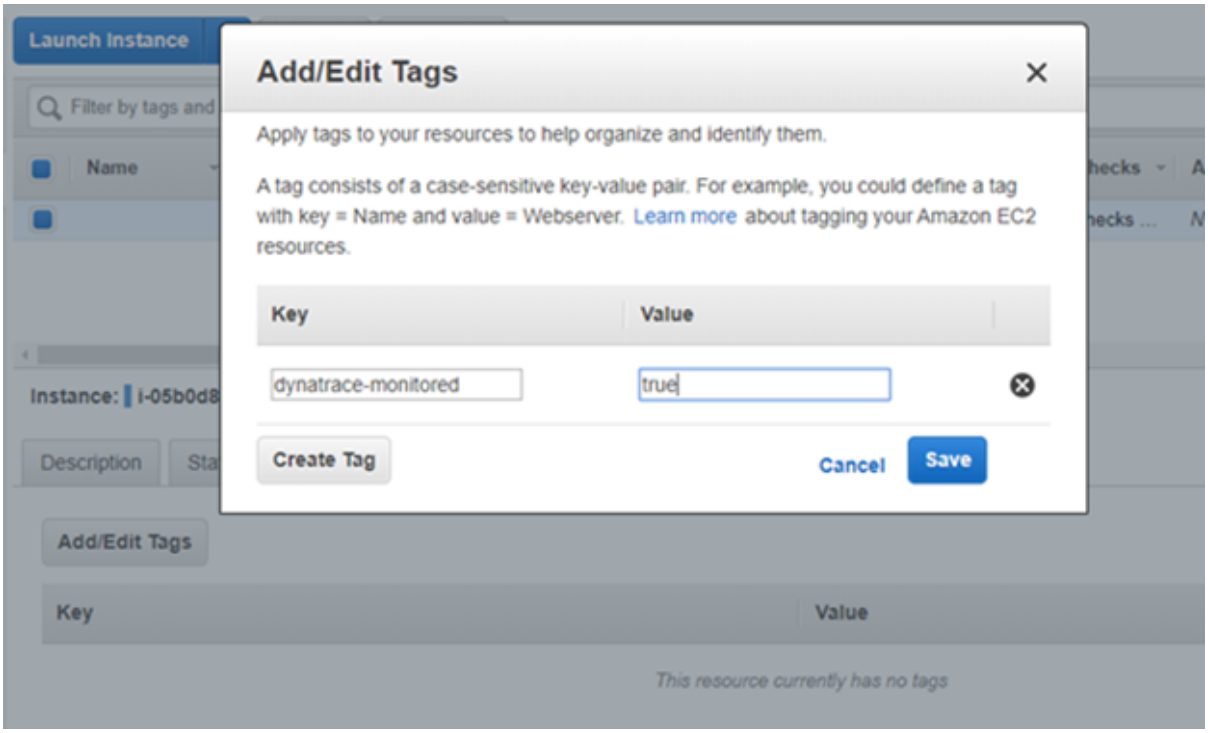


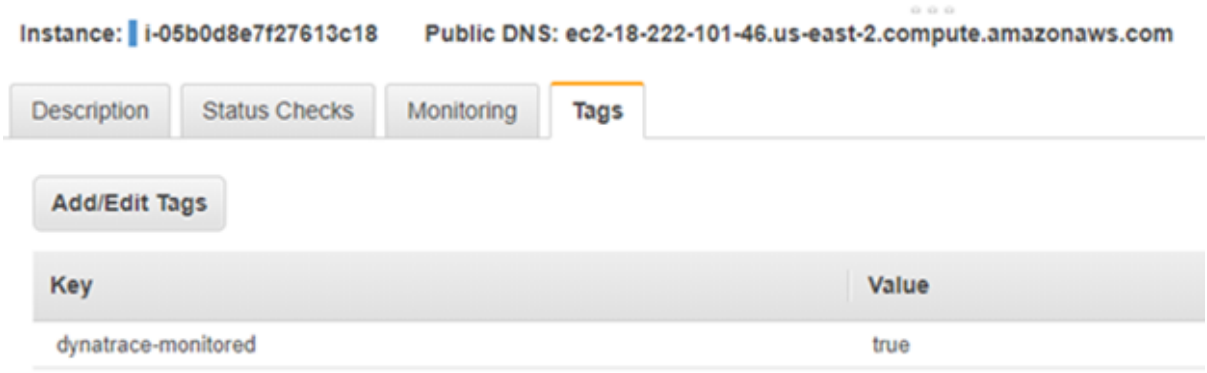
Copie as respectivas chaves!

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
Connect
Actions
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


Launch Instance
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.

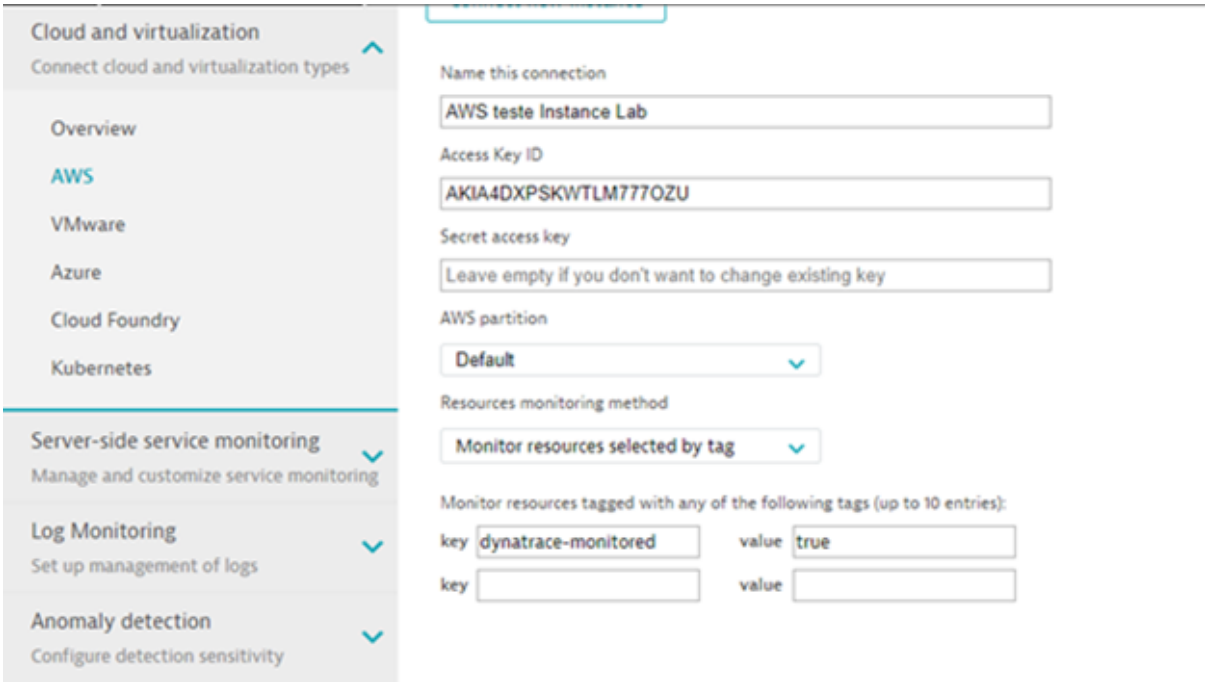
{
“Version”: “2012-10-17”,
“Statement”: [
{
“Effect”: “Allow”,
“Action”: [
“autoscaling:DescribeAutoScalingGroups”,
“cloudwatch:GetMetricData”,
“ec2:DescribeAvailabilityZones”,
“ec2:DescribeInstances”,
“ec2:DescribeVolumes”,
“elasticloadbalancing:DescribeLoadBalancers”,
“elasticloadbalancing:DescribeTags”,
“elasticloadbalancing:DescribeInstanceHealth”,
“elasticloadbalancing:DescribeListeners”,
“elasticloadbalancing:DescribeRules”,
“elasticloadbalancing:DescribeTargetHealth”,
“rds:DescribeDBInstances”,
“rds:DescribeEvents”,
“rds:ListTagsForResource”,
“dynamodb:ListTables”,
“dynamodb:ListTagsOfResource”,
“lambda:ListFunctions”,
“lambda:ListTags”,
“elasticbeanstalk:DescribeEnvironments”,

“elasticbeanstalk:DescribeEnvironmentResources”,
“s3:ListAllMyBuckets”,
“sts:GetCallerIdentity”,
“cloudformation:ListStackResources”,
“tag:GetResources”,
“tag:GetTagKeys”,
“cloudwatch:ListMetrics”,
“kinesisvideo:ListStreams”,
“sns:ListTopics”,
“sqs:ListQueues”,
“ec2:DescribeNatGateways”,
“ec2:DescribeSpotFleetRequests”,
“kinesis:ListStreams”,
“es:ListDomainNames”,
“cloudfront:ListDistributions”,
“firehose:ListDeliveryStreams”,
“elasticmapreduce:ListClusters”,
“kinesisanalytics: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:



Aqui é necessário informar

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

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

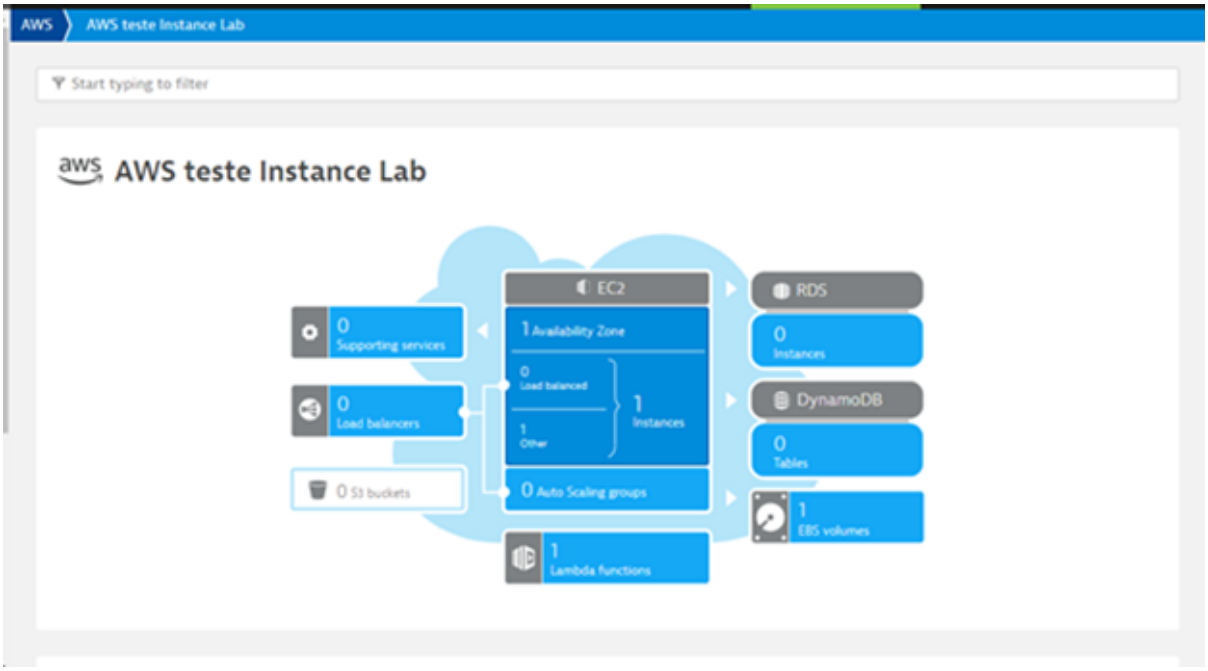
Secret access Key: {Criada nos passos anteriores}

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.