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.

aws Serviço	os v	Grup	pos de recursos 🗸	*	
Identity and Access Management (IAM)	^	ſ	Adicionar usuário	Excluir usuário	
Painel Gerenciamento de acess Grupos	50		Q Localizar usuários	por nome de usuário	ou chave de aces
Usuários					
Funções Políticas					
Provedores de identidade					

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			1	2 3 4 5
Definir detalhes do usuá	rio			
Você pode adicionar vários usuários d	le um	a só vez com o mesmo tipo de acesso e permissões. Saiba mais		
Nome de usuário"	D	/natrace_monitoring_user		
	0	Adicionar outro usuário		
Selecione o tipo de acesso à Selecione como esses usuários vão a mais	AWS	\$ Ir a AWS. As chaves de acesso e as senhas geradas automaticamer	nte são fornec	idas na última etapa. Saiba
Tipo de acesso"	•	Acesso programático Habilita uma ID da chave de acessoe chave de acesso secreta ; CLI, SDK, e outras ferramentas de desenvolvimento.	para a API da	AWS,
		Acesso ao Console de Gerenciamento da AWS Habilita uma senha que permite que os usuários façam login no Co Gerenciamento da AWS.	onsole de	
* Obriostária				

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 recomenda trabalho, acesso ao serviço da AWS, ou suas permissões personalizadas.	ada para gerenciar as permissões dos usuários por função de Comece a criar um grupo. Salba 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. Salba mais

		Cano	elar Anterior Próximo: Tag
\dic	ionar usuário		1 2 3 4 5
- Defi	inir permissões		
æ	Adicionar usuário ao grupo Copiar as permissões de um usuário existente	Anexar políticas existentes de forma direta	
Criar p	politica		0
Filtrar	politicas ~ Q Pesquisar		Exibindo 516 resultados
	Nome da política 👻	Digite	Usado como
	Nome da política 👻	Digite Função de trabalho	Usado como
•	Nome da política 👻 i AdministratorAccess AlexaForBusinessDeviceSetup	Digite Função de trabalho Gerenciado pela AWS	Usado como Nenhum Nenhum
) •	Nome da política	Digite Função de trabalho Gerenciado pela AWS Gerenciado pela AWS	Usado como Nenhum Nenhum Nenhum
)))))	Nome da política • II AdministratorAccess II AlexaForBusinessDeviceSetup II AlexaForBusinessFutIAccess II AlexaForBusinessGatewayExecution	Digite Função de trabalho Gerenciado pela AWS Gerenciado pela AWS Gerenciado pela AWS	Usado como Nenhum Nenhum Nenhum Nenhum Nenhum
· · · · · · · · · · · · · · · · · · ·	Nome da política • Image: AdministratorAccess Image: AdexaForBusinessDeviceSetup Image: AdexaForBusinessFullAccess Image: AdexaForBusinessGatewayExecution Image: AdexaForBusinessGatewayExecution Image: AdexaForBusinessPolyDelegatedAccessPolicy	Digite Função de trabalho Gerenciado pela AWS Gerenciado pela AWS Gerenciado pela AWS Gerenciado pela AWS	Usado como Nenhum Nenhum Nenhum Nenhum Nenhum Nenhum

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		1	2
A política define as permissõe	os 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. Saib	mais	
Editor visual JSON	Importar p	olitica g	erenciada
Expandir todos Recolher to	dos		
 API Gateway (1 ação) 	Cion	ar Re	nover
▶ EC2 (16 ações)	Clos	ar Re	nover
CloudWatch (12 ações	0) Clon	er Re	nover
▶ \$3 (41 ações)	Clos	ar Re	nover
 Lambda (12 ações) 	Clon	ar Rei	nover
Contigen de canademe	29944144 Center	winar p	olitica
Criar política	term o nome para. Dynatrace_monitoring_poney .	1	2
Revisar política			
Nome*	Dynatrace_monitoring_policy		
Descrição	Police para monitoramento de <u>metricas</u> para.		
	Máximo de 1000 caracteres. Use caracteres alfanuméricos e "++, @"		li

	Máximo de 1000 caracteres	Use caracteres alfanuméricos e "++, @'					
Resu	Esta política define tenha um recurso o	algumas ações, recursos ou condições que não for u condição aplicável. Para obter detalhes, escolha E	ecem permissões. Para conceder xibir restantes. Saiba mais	acesso, as políticas devem ter uma ação que			
	Q, Filtro:						
	Serviço 👻	Nixel de acessa	Recurso	Condição para solicitação			
	Permitir (5 de 224 se	Permitir (5 de 224 serviços) Exibir restantes 219					
	API Galeway	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				Country Antonias Councetting			

Em seguida basta clicar em criar.

Essa será a saída:

Adicionar us	suário				1 2 3 4 5
- Definir permis	sões				
Adicionar usu grupo	iário ao	Copiar as permissões de um usuário existente	An exider	exar políticas stentes de forma eta	
Criar política					2
Filtrar políticas 🐱	Q Dynatrae	e_monitoring_policy			Exibindo 1 resultado
Nome da	política 👻			Digite	Usado como
🕗 🕨 Dynati	race_monitoring	g_policy		Cliente gerenciado	Nenhum

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



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.

Valor

Digite Nome

Política gerenciada Dynatrace_monitoring_policy

Tags

O novo usuário receberá a seguinte tag

Chave

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	Launch Instance Connect	Actions Y			
EC2 Dashboard New	Q. Filter by tags and attributes or sea	rch by keyword			
Events New	Name y Instance ID	 Instance Type 	- Availability Zone -	Instance State	Status Charles
Tags		- insumce type	Presidently Lone	manance state	Status Checks
Reports	- 1-05b0d0e7f2	7613c18 t2.micro	us-east-2c	running	2/2 checks
Limits					
▼ INSTANCES					
Instances					
Instance Types	Instance: i-05b0d8e7f27613c18	Public DNS: ec2-18-222	2-101-46.us-east-2.com	pute.amazonaws.	com
Launch Templates New	Description Status Checks	Monitoring Tags			
Spot Requests					
Savings Plans	Add/Edit Tags				
Reserved Instances					
Dedicated Hosts	Кеу			Value	
Capacity Reservations			This resource curre	intly has no tags	
AMIS	Add/Edit Tags Apply tags to your resources to h A tag consists of a case-sensitive with key = Name and value = We resources.	elp organize and iden e key-value pair. For ex observer. Learn more a Value	tify them. kample, you could o about tagging your.	X define a tag Amazon EC2	hecks ~ A hecks N
4	durations maritered	Inced			
Instance: 1-05b0d8	dynatrace-monitored	true		8	

Key

This resource currently has no tags

Value

Instance: i-08	5b0d8e7f27613c18	c18 Public DNS: ec2-18-222-101-46.us-east-2.compute.amazonaws.com		aws.com		
Description	Status Checks	Monitoring	Tags			
Add/Edit Ta	igs					
Кеу				v	/alue	
dynatrace-m	onitored			t	rue	

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:ListDelivervStreams", "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 \rightarrow Cloud and Virtualization \rightarrow AWS Logo em seguida configurar conforme imagem abaixo:

Cloud and virtualization Connect cloud and virtualization types	^	Name this connection				
Overview		AWS teste Instance Lab				
AWS		Access Key ID				
0113		AKIA4DXPSKWTLM777OZU				
VMware		Secret access key				
Azure		Leave empty if you don't want to change existing key				
Cloud Foundry		AWS partition				
Kubernetes		Default 🗸				
		Resources monitoring method				
Server-side service monitoring	~	Monitor resources selected by tag				
Manage and customize service monitor	ring	Monitor resources tasked with any of the following task (up to 10 entries)				
Log Monitoring		key dynatrare-monitored value true				
Set up management of logs	~	internet internet				
Annesely detection		key value				
Anomaly detection	\mathbf{v}					
configure detection sensitivity						

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.