



Redução de custos e segurança na AWS

Ações que podem evitar prejuízos para o negócio

IMPULSO TALKS COM A COTEMINAS



com **Dionizio
Ferreira**,
coordenador de
infraestrutura

 /IN/DIONIZIOAF



com **André
Fialkowski**,
gerente de
engenharia

 /IN/ANDREFELIPEFIALKOWSKI

Projetos que já implementamos

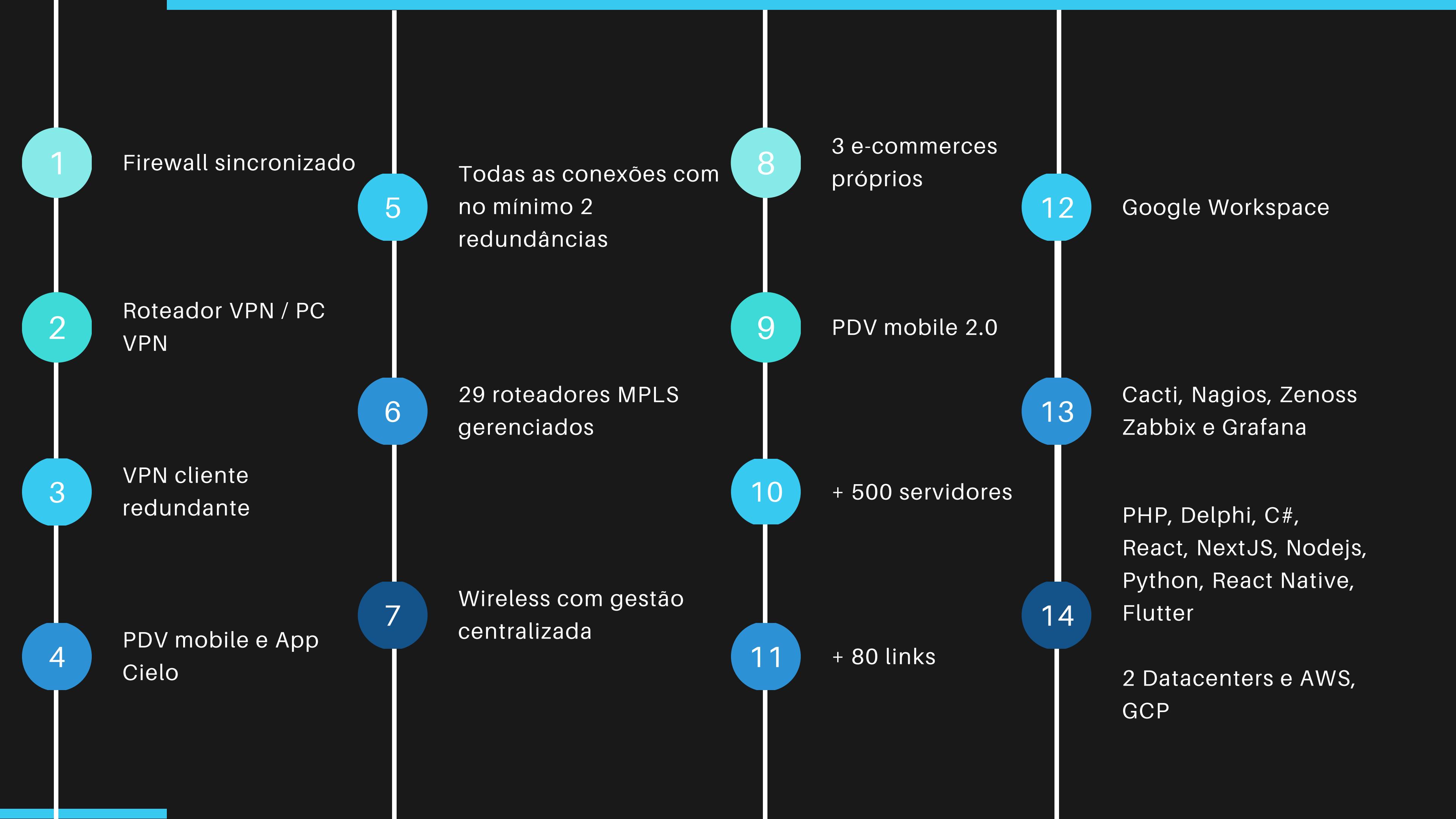


Persono
Beta Edition

O primeiro travesseiro
que monitora o sono.

Recomendado por







- 01 RESPONSABILIDADE COMPARTILHADA
- 02 REDUÇÃO DE CUSTOS
- 03 SEGURANÇA
- 04 REFERÊNCIAS
- 05 RESPONDER A PERGUNTAS

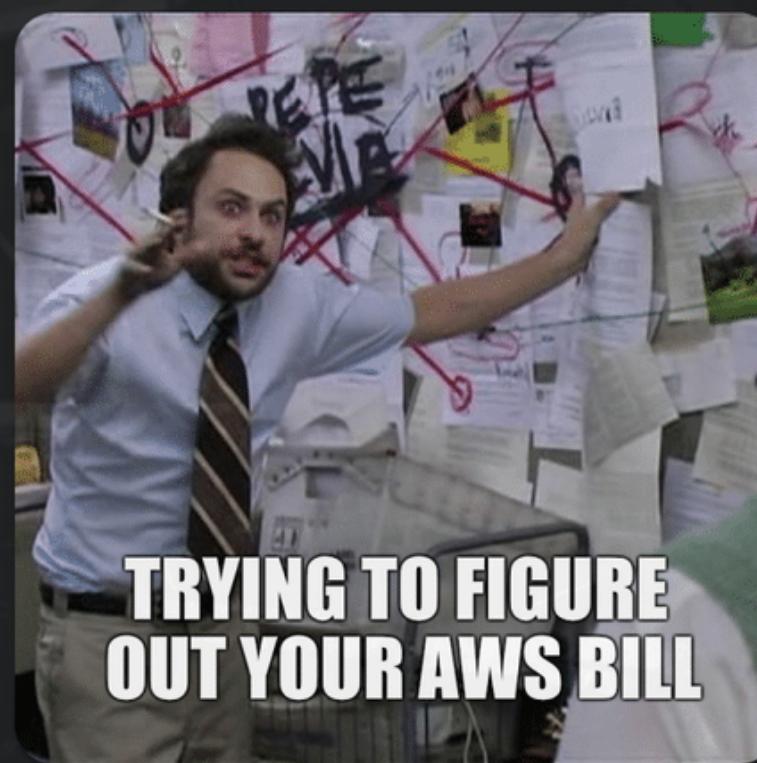
Modelo de Responsabilidade Compartilhada



REDUÇÃO DE CUSTOS



QUER SABER COMO
REDUZIR CUSTOS NA AWS?



IMPULSO TALKS COM COTEMINAS: AWS | 01DEZ19h30

01 SUPER DIMENSIONAMENTO

02 CONTROLE POR TAG

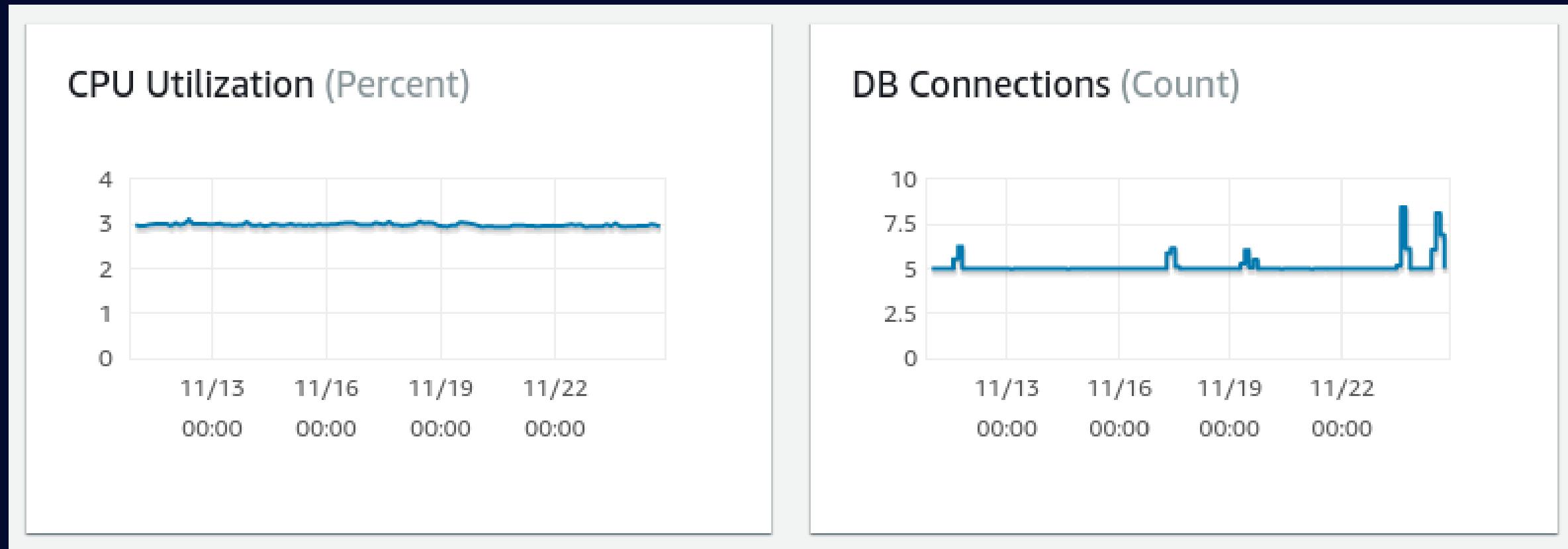
03 TIPO DE INSTÂNCIA

04 RELATÓRIOS

05 CONTRATOS

Problema: Serviços superdimensionados

RDS T2.MEDIUM



Solução:
T2.MEDIUM : \$ 56,74
T2.SMALL: \$ 29,73

DIFERENÇA: \$ 27,01 | 48%

Recomendação de alteração de tamanho

AWS BILLING > AWS COST MANAGEMENT > RIGHTSIZING RECOMMENDATIONS

AWS Cost Management > Rightsizing recommendations

Rightsizing recommendations Info

Amazon EC2 console 

Rightsizing recommendations review your historical Amazon EC2 usage for the past 14 days to identify opportunities for greater cost and usage efficiency.

Recommendation parameters

Display recommendations	Finding types	Advanced options
<input checked="" type="radio"/> Within the same instance family	<input checked="" type="checkbox"/> Idle instances	<input checked="" type="checkbox"/> Include Savings Plans and Reserved Instances
<input type="radio"/> Across instance families	<input checked="" type="checkbox"/> Underutilized instances	

Recommendations

Optimization opportunities	Estimated monthly savings	Estimated savings (%)
10	\$150.96	50.02%

Findings

Download CSV 

Filter by region and tag 

Instance ID	Estimated savings 	Finding	Finding reason(s)	Account ID	Instance type	Recommended instance type	CPU	Platform differen
I-0f9ae5151820a6528	\$62.05/month	Underutilized Instance	CPUOverprovisioned, +4 more	484541199542	c5.xlarge	c5.large	16.9%	-
I-0d81f954a53c60e15	\$24.53/month	Underutilized Instance	-	484541199542	t3.medium	t3.small	5.1%	-
I-04f4415b84ed0c421	\$17.08/month	Underutilized Instance	-	484541199542	t2.medium	t2.small	1.6%	-
I-0c737a1c0b3755427	\$8.52/month	Underutilized Instance	-	484541199542	t2.small	t2.micro	8.7%	-



01 SUPER DIMENSIONAMENTO

02 CONTROLE POR TAG

03 TIPO DE INSTÂNCIA

04 RELATÓRIOS

05 CONTRATOS

Identificar gastos por recursos ou identificações próprias

POR RECURSO

Você poderá olhar para cada recurso/serviço da AWS onde está ocorrendo os seus maiores gastos e então trabalhar na redução do custo.

- S3 standard pode ser convertido para S3 Glacier
- RDS (Postgre, Mysql, Sql) pode ser convertido para Aurora (estudo adicional deve ser realizado para validar se no seu caso será gerado redução)
- Recurso gerando gasto sem o seu conhecimento.

POR AMBIENTE / IDENTIFICAÇÃO

Identificar qual ambiente (desenvolvimento, homologação, produção) está gerando o maior custo.
Identificar os seus serviços da maneira que desejar e então identificar onde o custo não está ideal.

- Poderá entender qual o ambiente (desenvolvimento, homologação, produção) está gerando mais custo e então realizar ações focadas.
- Ex: homologação e desenvolvimento: desligar a noite e final de semana.
- Ex: Software X está gastando muito de transferência de dados e precisará ser repensado algum funcionamento da aplicação.

Configuração de TAG



- 01** Definir as tags que serão utilizadas

- 02** Configurar no billing para que seja gerado dados dos gastos

- 03** Gerar relatórios dos recursos sem tags e corrigir

Definir as tags que serão utilizadas

IREMOS COLOCAR ALGUNS LINKS DE DOCUMENTAÇÃO SOBRE O ASSUNTO, MAS SEGUE ALGUMAS QUE ACHAMOS IMPORTANTES.

- AMBIENTE (DEV, PROD)
- NOME DO PRODUTO (E-COMMERCE, RETAGUARDA, PDV)
- TIME (DEVOPS, INFRAESTRUTURA, PDV)
- ADMIN
- GERENTE
- E-MAIL DO TIME
- DETALHES
- UPTIME
- LEVEL DE CRITICIDADE (BAIXO, MÉDIO, ALTO)

Configurar no billing para que seja gerado dados dos gastos

1. ATIVE A POLÍTICA DE TAGS

A. AWS ORGANIZATIONS > POLICIES > TAG POLICIES > ENABLE TAG POLICIES

The screenshot shows the 'Create new tag policy' interface in the AWS Organizations console. On the left, the 'Details' section includes fields for 'Policy name' (set to 'Sandbox') and 'Policy description - optional' (containing 'e.g Sandbox'). Below these are sections for 'Tags' and 'Visual editor/JSON'. The 'Tags' section shows 'No tags are associated with the resource.' and an 'Add tag' button. The 'Visual editor' tab is selected, showing a single tag key 'New tag key 1' with its value also set to 'New tag key 1'. On the right, the 'New tag key 1' configuration panel is expanded, showing options for 'Tag key capitalization compliance' (checked for 'Use the capitalization that you've specified above for the tag key'), 'Tag value compliance' (checked for 'Specify allowed values for this tag key'), and 'Resource types to enforce' (checked for 'Prevent noncompliant operations for this tag').

AWS Organizations > Policies > Tag policies > Create new tag policy

Create new tag policy

A tag policy enables you to define tag compliance rules to help you maintain consistency in the tags attached to your organization's resources. You can use tag policies to enforce your tag strategy across all of your resources. [Learn more](#)

Details

Policy name

Sandbox

A policy name can be up to 128 characters and can include the following characters: a-z, A-Z, 0-9, and .,*=@_-

Policy description - optional

e.g Sandbox

A description can have up to 512 characters and can include the following characters: a-z, A-Z, 0-9, and .,*=@_-

Tags

Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

No tags are associated with the resource.

Add tag

You can add 50 more tags.

Visual editor JSON Policy size: 29 / 10000 characters | [Tag policies syntax reference](#)

New tag key 1

Remove tag key

Tag key

New tag key 1

Tag key capitalization compliance

Use the capitalization that you've specified above for the tag key.

By default, tag key capitalization is inherited from the parent policy. If the parent policy does not exist or does not specify capitalization, then an all-lowercase tag key is considered compliant. [Learn more](#)

Tag value compliance

Specify allowed values for this tag key.

Only specified values are allowed for the tag key, including the specified capitalization. [Learn more](#)

Specify values

Resource types to enforce

Prevent noncompliant operations for this tag.

By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types not listed in the parent policy, select this option and then specify the resource types. [Learn more](#)

Specify resource types

Add tag key

Configurar no billing para que seja gerado dados dos gastos

1. VINCULE A TAG A UM RECURSO E AGUARDE 24 HORAS
2. ACESSE AWS BILLING > COST ALLOCATION TAGS

The screenshot shows the AWS Billing Cost allocation tags interface. The top navigation bar includes 'AWS Billing' and 'Cost allocation tags'. Below the navigation, there are two tabs: 'User-defined cost allocation tags' (highlighted in orange) and 'AWS-generated cost allocation tags'. The main area displays a table titled 'User-defined cost allocation tags (1/152)'. The table has columns for 'Tag key', 'Status', and a search/filter section at the top. The table lists four entries:

Tag key	Status
elasticbeanstalk:environment-id	Inactive
elasticbeanstalk:environment-name	Inactive
environment	Active

A search bar at the top of the table allows filtering by tag key. Buttons for 'Undo', 'Deactivate', and 'Activate' are located above the table. The status column indicates the current status of each tag key.

AGUARDE 24 HORAS

Listar recursos sem tags

RESOURCE GROUPS & TAG EDITOR > TAG EDITOR

Tag Editor

Find resources to tag
You can search for resources that you want to tag across regions. Then, you can add, remove, or edit tags for resources in your search results. [Learn more](#)

Regions

Resource types

Tags – Optional
 Type the tag key and optional values shared by the resources you want to search for, and then choose Add or press Enter.

Resource search results (- Loading resources)
Choose up to 500 resources for which you want to edit tags.

<input type="checkbox"/>	Identifier <small>(C)</small>	Tag: Name	Service	Type	Region	Tags
<input type="checkbox"/>	AWSControlTowerBP-BASELINE-CLOUDT...	(not tagged)	CloudFormation	Stack	us-east-2	-
<input type="checkbox"/>	AWSControlTowerBP-BASELINE-CONFIG-...	(not tagged)	CloudFormation	Stack	us-east-2	-

Consultar e corrigir tags

AWS RESOURCE GROUPS > TAG POLICIES > ACCOUNT #*****

Details

Account name	Meet up	Compliance status
Meet up		⚠ Noncompliant (updated 10 hours ago)
Account ID		
0000000		
Primary email account		

Tagged noncompliant resources

Full scan of this account for noncompliant resources was completed 10 hours ago. View status of individual region scans
To correct tags on these resources, sign in to this AWS account. [Learn more](#) 

Filter by region / service / noncompliant tag

Region	Service	Resource type	Tagged resources
sa-east-1	rds	snapshot	35 noncompliant
sa-east-1	elasticloadbalancing	loadbalancer	4 noncompliant
sa-east-1	ecr	repository	26 noncompliant
sa-east-1	rds	db	8 noncompliant
us-east-1	cloudfront	distribution	38 noncompliant
us-east-1	iam	policy	3 noncompliant
us-west-2	rds	snapshot	19 noncompliant
us-west-2	rds	db	5 noncompliant



01 SUPER DIMENSIONAMENTO

02 CONTROLE POR TAG

03 TIPO E REGIÃO DA INSTÂNCIA

04 RELATÓRIOS

05 CONTRATOS

Escolhendo a região dos serviços

Usamos a frase acima muitas vezes no ambiente de servidores, mas quando pensamos em custo pode não ser a melhor decisão.

Amazon EC2	Região: América do Sul (São Paulo)	<button>Editar</button>	<button>Ação</button>
Estimativa rápida			
Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (Instâncias sob demanda), Quantidade de armazenamento (100 GB), Tipo de instância (t2.large)	Mensal:	127,62 USD	
Amazon EC2			
Região: América do Sul (São Paulo)	<button>Editar</button>	<button>Ação</button>	
Estimativa rápida			
Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (Instâncias sob demanda), Quantidade de armazenamento (100 GB), Tipo de instância (t3.large)	Mensal:	117,11 USD	

t2.large	2	36	8	Somente EBS	Baixa a moderada
t3.large	2	36	8	Somente EBS	Até 5

Produção vs. Desenvolvimento

Queremos sempre que os servidores e serviços sejam o mais rápido possível para os nossos clientes, mas em ambiente de desenvolvimento ou com ferramentas internas podemos ter um pouco mais de latência para acesso.

Amazon EC2 Região: Leste dos EUA (Norte da Virgínia)	Estimativa rápida Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (Instâncias sob demanda), Quantidade de armazenamento (100 GB), Tipo de instância (t3.large)	Mensal: 70,74 USD	Editar Ação
Amazon EC2 Região: América do Sul (São Paulo)	Estimativa rápida Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (Instâncias sob demanda), Quantidade de armazenamento (100 GB), Tipo de instância (t3.large)	Mensal: 117,11 USD	Editar Ação
Amazon EC2 Região: Oeste dos EUA (Oregon)	Estimativa rápida Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (Instâncias sob demanda), Quantidade de armazenamento (100 GB), Tipo de instância (t3.large)	Mensal: 70,74 USD	Editar Ação

Lembre-se de analisar Data Transfer.

SPOT

Existe um tipo de instância na AWS chamada SPOT que pode chegar até 90% de redução no custo de uso, mas em média fica perto de 70%.

Spot Instance Advisor

Região: América do Sul (São Paulo) SO: Linux/UNIX

Filtro do tipo de instância:

vCPU (min.): 4 Memória GiB (min.): 16 Tipos de instância sustentadas pelo EMR

Memória	Frequência da interrupção
Economia em relação aos preços sob demanda*	<5%
Tipos de instância vCPU GiB	70%
t3.xlarge 4 16	

Mas SPOT não é para todos os cenários, pois como podem ver na imagem temos as interrupções.

Recomendamos o uso nestas situações:
Kubernetes (DEV), Rotinas de processamento (DEV e PROD)

ARMAZENAR DADOS NO DISCO

Temos várias situações em que precisamos realizar backup, armazenar dados de aplicação ou logs e muitas vezes criamos um disco EBS e armazenamos os dados dentro do próprio servidor. O que irei mostrar abaixo não se encaixa para todos os cenários mas deve ser levado em consideração.

Services (3)			
Amazon Simple Storage Service (S3) Região: América do Sul (São Paulo)	Editar	Ação ▾	
Tamanho médio do objeto do S3 Glacier (16 MB), Armazenamento no S3 Glacier (100 GB por mês)	Mensal:	0,05 USD	
Amazon Simple Storage Service (S3) Região: América do Sul (São Paulo)	Editar	Ação ▾	
Armazenamento S3 Standard (100 GB por mês)	Mensal:	4,05 USD	
Amazon Elastic Block Store (EBS) Região: América do Sul (São Paulo)	Editar	Ação ▾	
Amazon Elastic Block Storage (EBS) Número de instâncias (1), Duração média de cada execução da instância (750 horas por mês), Quantidade de armazenamento (100 GB), Frequência de snapshots (Sem armazenamento de snapshots)	Mensal:	19,00 USD	

Dicas para créditos



- 01 Sempre verificar se o serviço que quer utilizar não possui 1 ano de uso grátis em algumas situações.
- 02 Requisitar ao seu gerente de contas créditos de bonificação, principalmente para testes com produtos.
- 03 Para startups normalmente nas aceleradoras existem bônus. Um exemplo é a ABStartup, que possui bônus das principais Clouds e no caso da AWS possui um bônus de até 5k dólares.

FIZ AS CONTAS

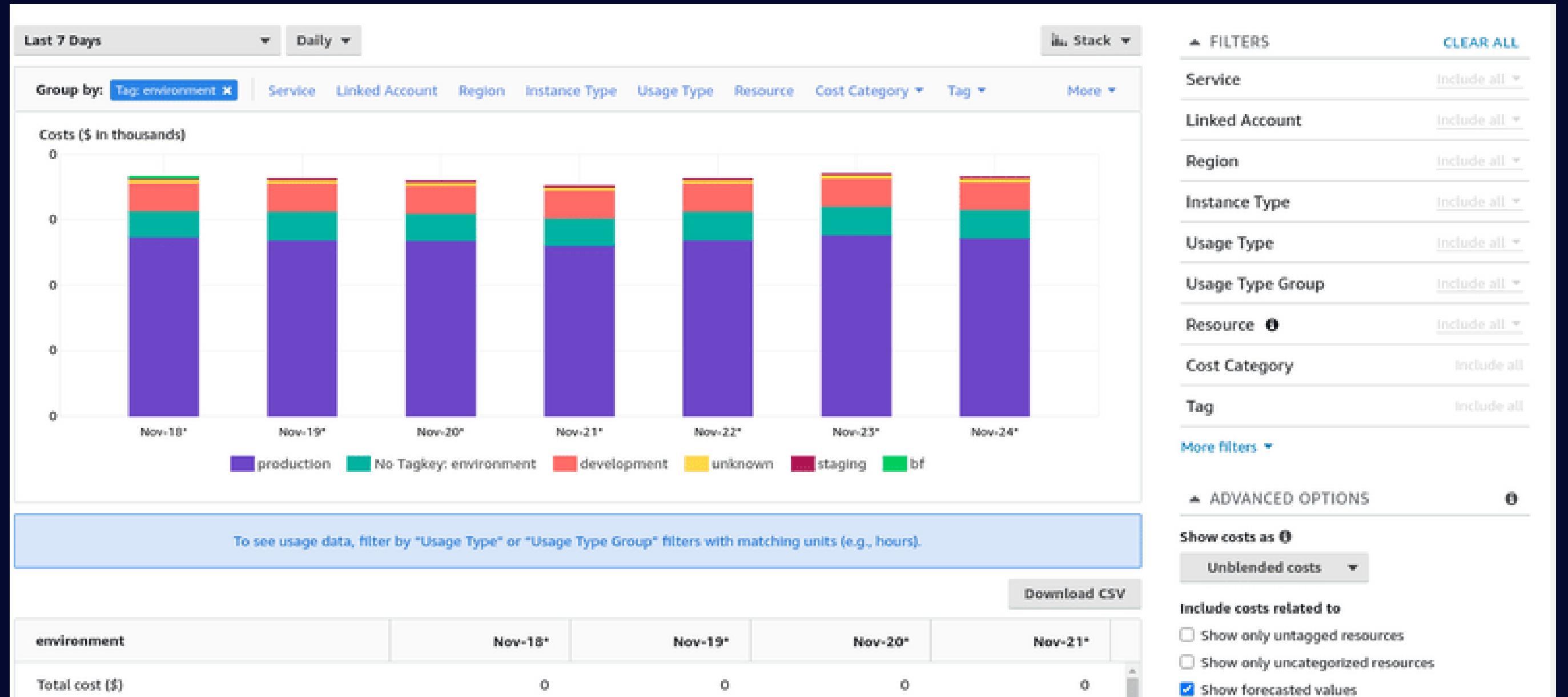


NÃO VOU PRECISAR VENDER
MEUS AMIGOS

- 01 SUPER DIMENSIONAMENTO
- 02 CONTROLE POR TAG
- 03 TIPO DE INSTÂNCIA
- 04 RELATÓRIOS
- 05 CONTRATOS

Visualizar os valores

ACESSE AWS BILLING > COST EXPLORER > LAUNCH COST EXPLORER



Controlar os gastos

ACESSE AWS BILLING > BUDGET > CREATE BUDGET

Choose budget type Info

Budget types

Cost budget - Recommended
Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met. Using cost budgets, the budgeted amount you set represents your expected cloud spend. For example, you can set a cost budget for a business unit and then add additional parameters such as the associated member accounts.

Usage budget
Monitor your usage of one or more specified usage types or usage type groups or to monitor the usage of certain services such as Amazon EC2 and Amazon S3.

Savings Plans budget
Track the utilization or coverage associated with your Savings Plans and receive a utilization target lets you see if your Savings Plans are unused or underutilized.

Reservation budget
Track the utilization or coverage associated with your reservations and receive a utilization target lets you see if your reservations are unused or underutilized. Re

Set budget amount

Period
Daily budgets do not support enabling forecasted alerts, or daily budget planning.

Monthly

Budget effective date

Recurring budget
Recurring budgets renew on the first day of every monthly billing period.

Expiring budget
Expiring monthly budgets stop renewing at the end of the selected expiration month.

Start month
Nov 2021

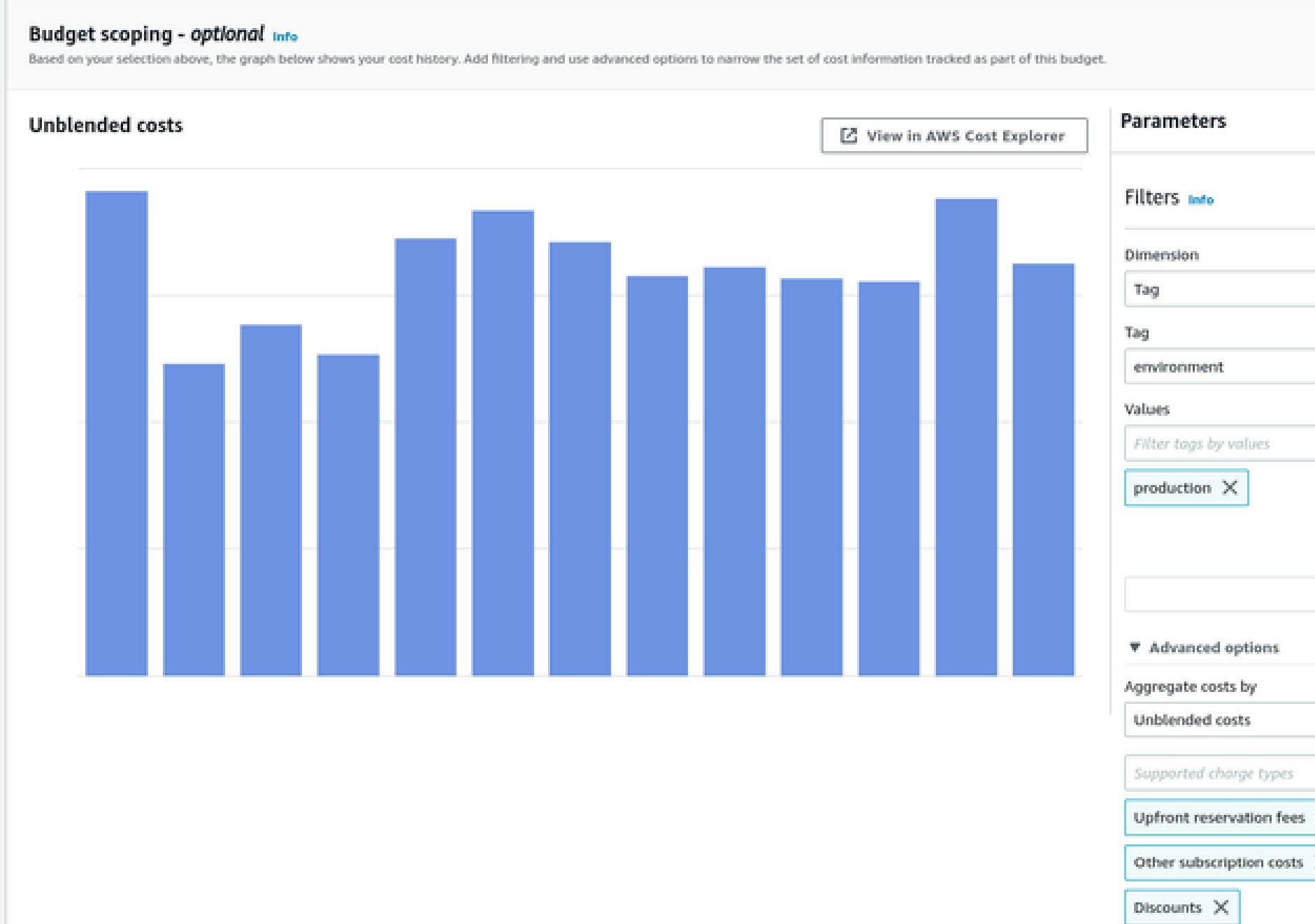
Choose how to budget

Fixed
Create a budget that tracks against a single monthly budgeted amount.

Monthly budget planning
Specify your budgeted amount for each budget period.

Enter your budgeted amount (\$)
Last month's cost: \$56,475.27

Recursos



- Na tela inicial do Budget você irá ver o uso real Vs planejado
- Ao clicar nele poderá ver detalhes como o valor mês a mês entre outros
- Poderá criar alarme quando chegar a x valor utilizado



- 01 SUPER DIMENSIONAMENTO
- 02 CONTROLE POR TAG
- 03 TIPO DE INSTÂNCIA
- 04 RELATÓRIOS
- 05 CONTRATOS

É para você?

- Vai usar o recurso por pelo menos 1 ano?
- A sua necessidade de recurso em questão de potência será igual ou maior?
- Caso este uso não seja mais necessário consegue reutilizar para outra coisa?

Em quais serviços?

- Computação (EC2, EKS, LAMBDA)
- Banco de dados (RDS, Elastic Cache)

*Colocamos os que iremos trazer exemplos

EC2

EC2 > RESERVED INSTANCES

Amazon EC2 Descrição: Sem reserva Região: Oeste dos EUA (Oregon)	Editar	Ação ▾
Estimativa rápida		
Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (Instâncias sob demanda), Quantidade de armazenamento (30 GB), Tipo de instância (t3.large)	Mensal: Pagamento adiantado:	63,74 USD 0,00 USD

ANUAL
\$ 764,88

Amazon EC2 Descrição: Reserva - Sem pagamento adiantado Região: Oeste dos EUA (Oregon)	Editar	Ação ▾
Estimativa rápida		
Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (EC2 Instance Savings Plans 1 ano Sem pagamento adiantado), Quantidade de armazenamento (30 GB), Tipo de instância (t3.large)	Mensal: Pagamento adiantado:	41,11 USD 0,00 USD

ANUAL
\$ 493,32

EC2

EC2 > RESERVED INSTANCES

Amazon EC2 Descrição: Reserva - pagamento parcial Região: Oeste dos EUA (Oregon)	Editar	Ação ▾
Estimativa rápida		
Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (EC2 Instance Savings Plans 1 ano Pagamento adiantado parcial), Quantidade de armazenamento (30 GB), Tipo de instância (t3.large)	Mensal: Pagamento adiantado:	21,14 USD 217,69 USD

ANUAL
\$ 471,37

Amazon EC2 Descrição: Reserva - Sem pagamento total Região: Oeste dos EUA (Oregon)	Editar	Ação ▾
Estimativa rápida		
Sistema operacional (Linux), Quantidade (1), Estratégia de definição de preço (EC2 Instance Savings Plans 1 ano Integral adiantado), Quantidade de armazenamento (30 GB), Tipo de instância (t3.large)	Mensal: Pagamento adiantado:	3,00 USD 426,61 USD

ANUAL
\$ 462,61

ANUAL - SEM RESERVA
\$ 764,88

ANUAL - RESERVA
\$ 493,32

RDS

Amazon RDS for PostgreSQL	Editar	Ação ▾
Região: Oeste dos EUA (Oregon)		
RDS para PostgreSQL		
Volume de armazenamento (SSD de uso geral (gp2)), Quantidade de armazenamento (30 GB por mês), Nós (1), Tipo de instância (db.m5.large), Utilização (somente sob demanda) (100 %Utilized/Month), Opção de implantação (Single-AZ), Modelo de definição de preço (OnDemand)	Mensal:	133,39 USD
Amazon RDS for PostgreSQL	Editar	Ação ▾
Região: América do Sul (São Paulo)		
RDS para PostgreSQL		
Volume de armazenamento (SSD de uso geral (gp2)), Quantidade de armazenamento (30 GB por mês), Nós (1), Tipo de instância (db.m5.large), Utilização (somente sob demanda) (100 %Utilized/Month), Opção de implantação (Single-AZ), Modelo de definição de preço (Reserved), Prazo de oferta de locação (1yr), Opção de compra (No Upfront)	Mensal:	109,13 USD
		Pagamento adiantado: 0,00 USD

Segurança





01 BÁSICO

02 PONTO DE ENTRADA

03 PORTAS E PROTOCOLOS

04 FIREWALL E AMEAÇAS

05 FERRAMENTAS POR ETAPAS

06 OUTRAS FERRAMENTAS

Primeira ação em seu ambiente



Como iremos mostrar, habilitar o MFA pode ser muito importante para garantir que não ocorra invasão e prejuízo.

HABILITAR O MFA

HABILITAR O MFA DEVE SER MANDATÓRIO PARA CONTAS COM ACESSO ADMIN

Someone accessed my AWS account and now I have charges and "irregular activities" emails coming in

discussion

For the last couple week prompting me to update ago and spent a total of logged back in until the

Lacking AWS Support after Account was hacked

security

Hello,

Clearly AWS sees some s to drop the charges and emails which doesn't ad

first of all, my AWS main user/ account root did not had 2 Factor Authentication, which defently is my fault and I will enable immediately :)

AWS Account Hacked | billed 15k USD

How do I actually get a n can see the illegal activit and I can't dispute it app

So this AWS Account was hacked, th changed the Account e-mail and Pa not had an button like "report abuse"

Any help on how to navi

I detectet that my AWS Account got

I lost approximately 10.000 USD in t AWS.

security

Hi guys someone hacked into my AWS account which I made 3 years back and have never used since then.

I just got a mail from AWS saying that there is some unauthorised login in my account. I logged into the account and found out that it has an invoice of 15K USD.

I am just a fresher and I haven't seen this amount of money in my entire life.

Can someone help me with how should I approach this issue?

CASO O MFA NÃO SEJA PARA TODOS

SABEMOS QUE ÀS VEZES DEVIDO A INÚMEROS MOTIVOS VOCÊ PODE ESCOLHER NÃO HABILITAR MFA PARA TODOS DA ORGANIZAÇÃO DE MANEIRA MANDATÓRIA.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with the following items:

- Identity and Access Management (IAM)
- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
- Account settings

The main content area is titled "Password policy". It contains the following text:
A password policy is a set of rules that define the type of password an IAM user can set. [Learn more](#)

Below this, it says "This AWS account uses the following default password policy:" followed by a list of rules:

- Minimum password length is 8 characters
- Include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # \$ % ^ & * () _ + - = [] { } | ^
- Must not be identical to your AWS account name or email address

A blue button labeled "Change password policy" is visible. At the bottom of the main content area, there's another section header: "Security Token Service (STS)".

SUPER PODERES



TEMOS A CONTA ROOT QUE SERIA A PRIMEIRA COM OS MAIORES PRIVILÉGIOS POSSÍVEIS, ESTA CONTA NÃO DEVE SER UTILIZADA NO DIA A DIA, RECOMENDAMOS A CRIAÇÃO DE CONTAS ADICIONAIS, POIS DEVEMOS TER UMA CONTA ONDE NO PIOR CENÁRIO SEJA POSSÍVEL ACESSAR ELA.

E TEMOS QUE LEMBRAR, NA CONTA ROOT:

- HABILITAR MFA
- SENHA COMPLEXA

EX:

(RDEM@Y7KN1N@KQ5FDG5EPL7RBX@LKI
9M@W)

CONTAS DE SERVIÇO

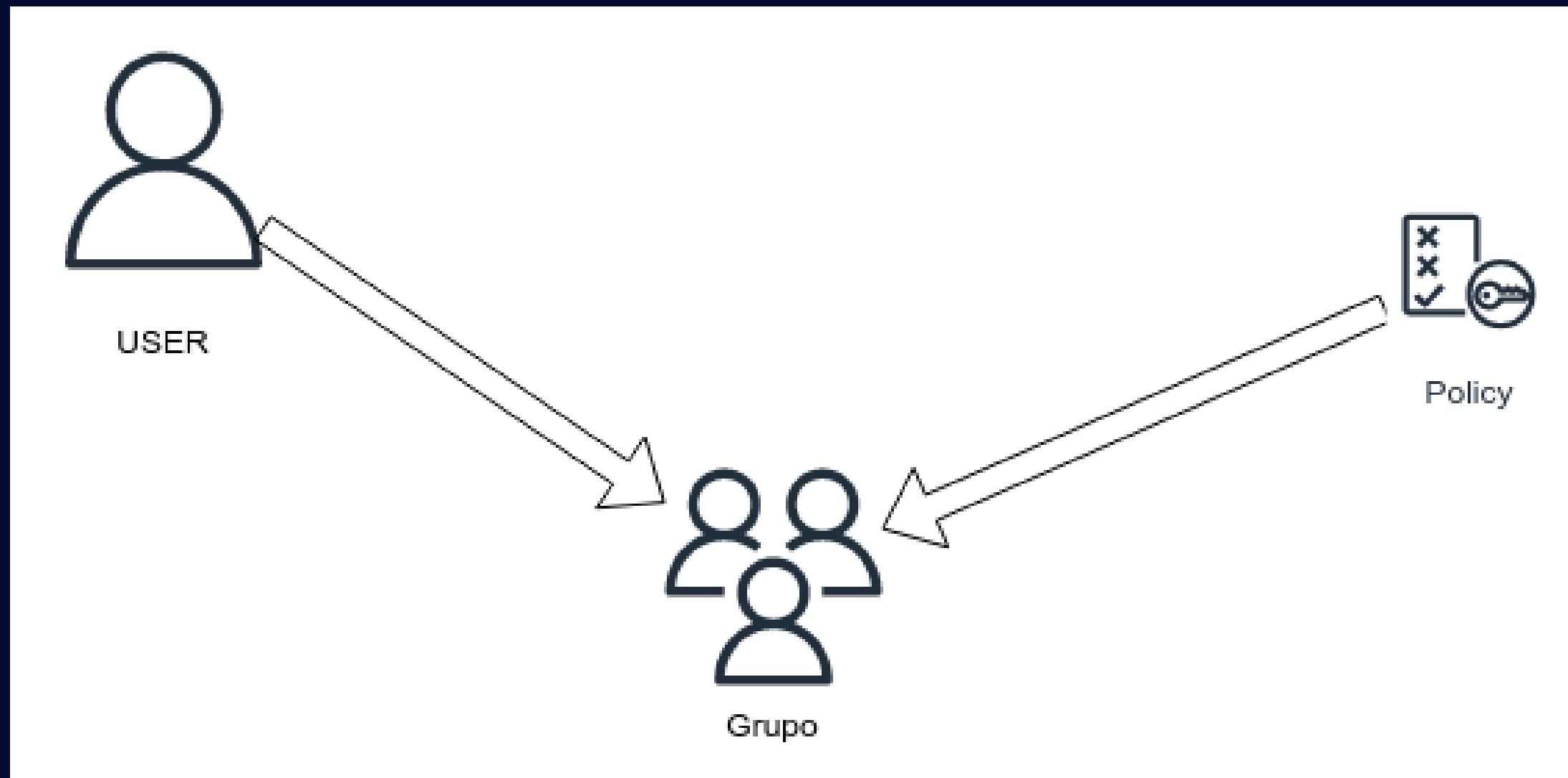
PRECISA CONFIGURAR CONTAS EM SERVIÇOS COMO GRAFANA, BITBUCKET, GITHUB ENTRE OUTROS?

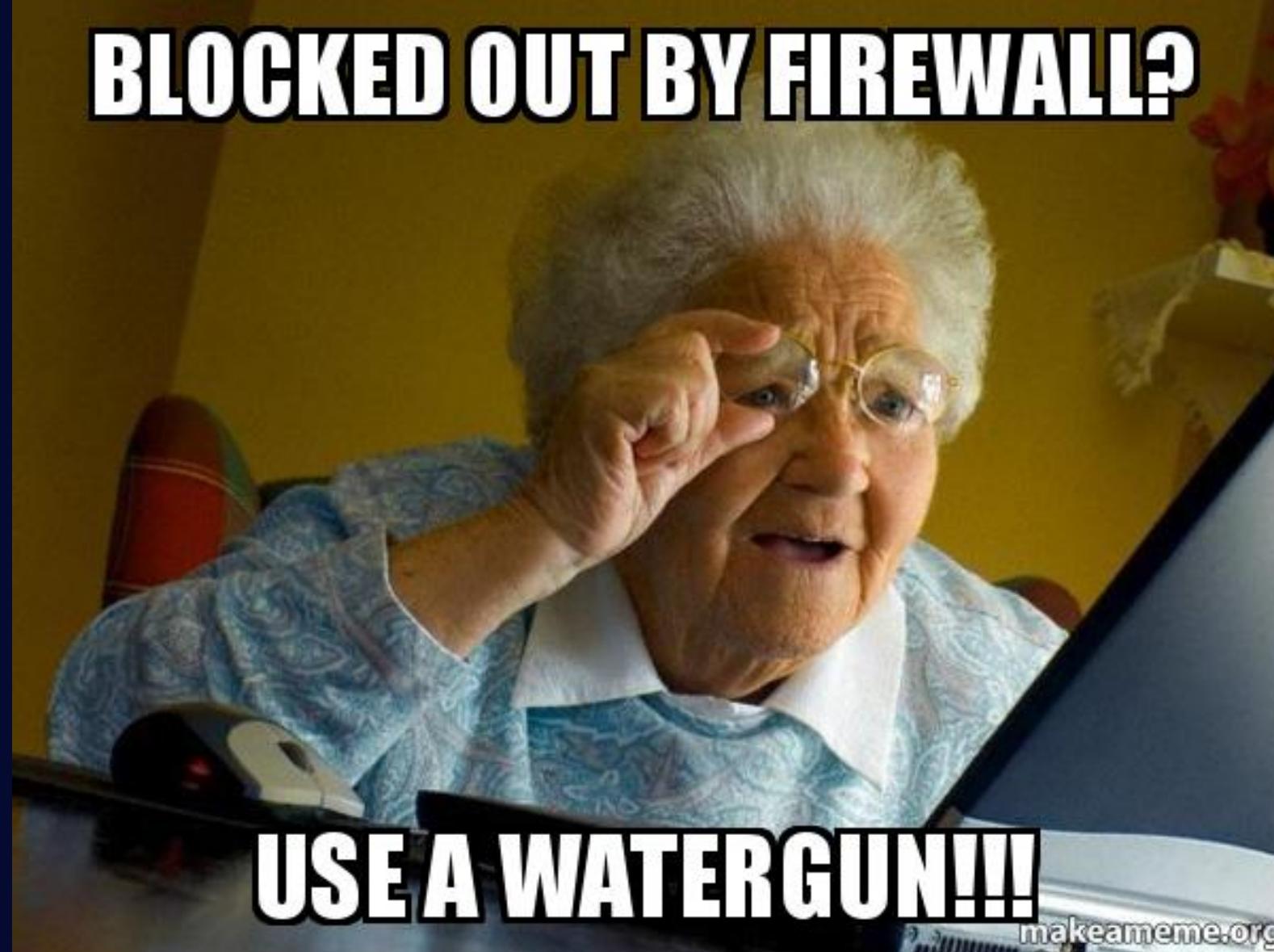
PRECISA QUE O EC2 TENHA ACESSO A ALGUM RECURSO DA AWS?

UTILIZE CONTA DE SERVIÇO OU ROLES

Permissões de acesso

NÓS APLICAMOS A POLÍTICA E O USUÁRIO AO GRUPO. NÃO IMPLEMENTE POLÍTICA AO USUÁRIO OU IN-LINE POLICY.





- 01 BÁSICO
- 02 PONTO DE ENTRADA
- 03 PORTAS E PROTOCOLOS
- 04 FIREWALL E AMEAÇAS
- 05 FERRAMENTAS POR ETAPAS
- 06 OUTRAS FERRAMENTAS

Ponto de entrada

CLOUDFRONT

Melhore a segurança com criptografia de tráfego e controles de acesso e use o AWS Shield Standard para se defender contra ataques de DDoS sem custo adicional.

API GATEWAY

Autorize o acesso às suas APIs com o AWS Identity and Access Management (IAM) e o Amazon Cognito. Se usar tokens OAuth, o API Gateway oferecerá suporte nativo a OIDC e OAuth2.

ELASTIC LOAD BALANCING

Proteja suas aplicações com gerenciamento integrado de certificados, autenticação de usuário e descriptografia SSL/TLS.

FIREWALL

O AWS Network Firewall é um serviço gerenciado que facilita a implantação de proteções básicas de rede para todas as suas Amazon Virtual Private Clouds (VPCs).

DNS FIREWALL

Um firewall gerenciado que permite aos clientes bloquear consultas DNS feitas para domínios mal-intencionados conhecidos e autorizar consultas para domínios confiáveis

AWS SHIELD

Proteção gerenciada contra DDoS.

- Versão básica é disponível para todos.
- Advanced possui custo.



- 01 BÁSICO
- 02 PONTO DE ENTRADA
- 03 PORTAS E PROTOCOLOS
- 04 FIREWALL E AMEAÇAS
- 05 FERRAMENTAS POR ETAPAS
- 06 OUTRAS FERRAMENTAS

Portas e protocolos

TODO MUNDO DE TECNOLOGIA JÁ ESCUTOU QUE A MELHOR PRÁTICA É LIBERAR APENAS AS PORTAS NECESSÁRIAS. ENTÃO QUERO FALAR APENAS DE SSL E ICMP.

SSL

Protocolo de conexão via terminal por padrão utilizado para conexão em linux.

Na AWS o acesso SSL é feito através de um certificado digital.

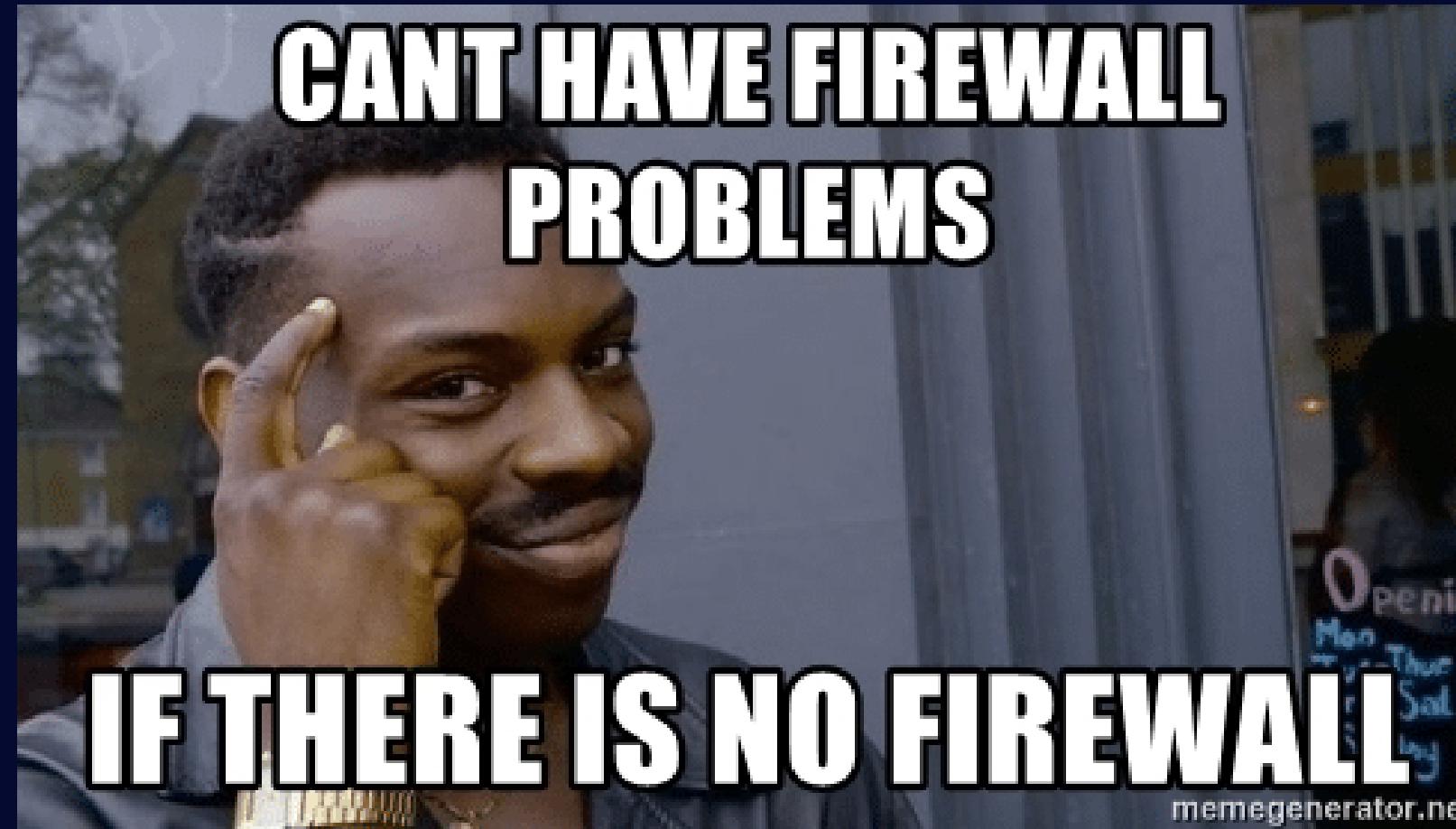
ICMP

Protocolo que responde a comandos de ping e tracert.

EC2 INSTANCE CONNECT

- Amazon Linux 2 (any version)
- Ubuntu 16.04 or later

IAM DEVE SER BEM CONFIGURADA



- 01 BÁSICO
- 02 PONTO DE ENTRADA
- 03 PORTAS E PROTOCOLOS
- 04 FIREWALL E AMEAÇAS
- 05 FERRAMENTAS POR ETAPAS
- 06 OUTRAS FERRAMENTAS

Amazon GuardDuty

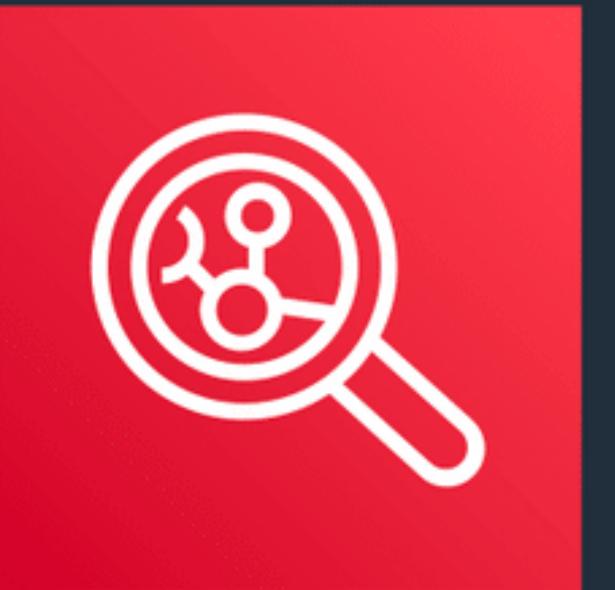
O AMAZON GUARDDUTY É UM SERVIÇO GERENCIADO DE DETECÇÃO DE AMEAÇAS QUE MONITORA CONTINUAMENTE O COMPORTAMENTO MAL-INTENCIONADO OU NÃO AUTORIZADO PARA AJUDÁ-LO A PROTEGER SUAS CONTAS E CARGAS DE TRABALHO DA AWS USANDO ML.



Amazon Inspector

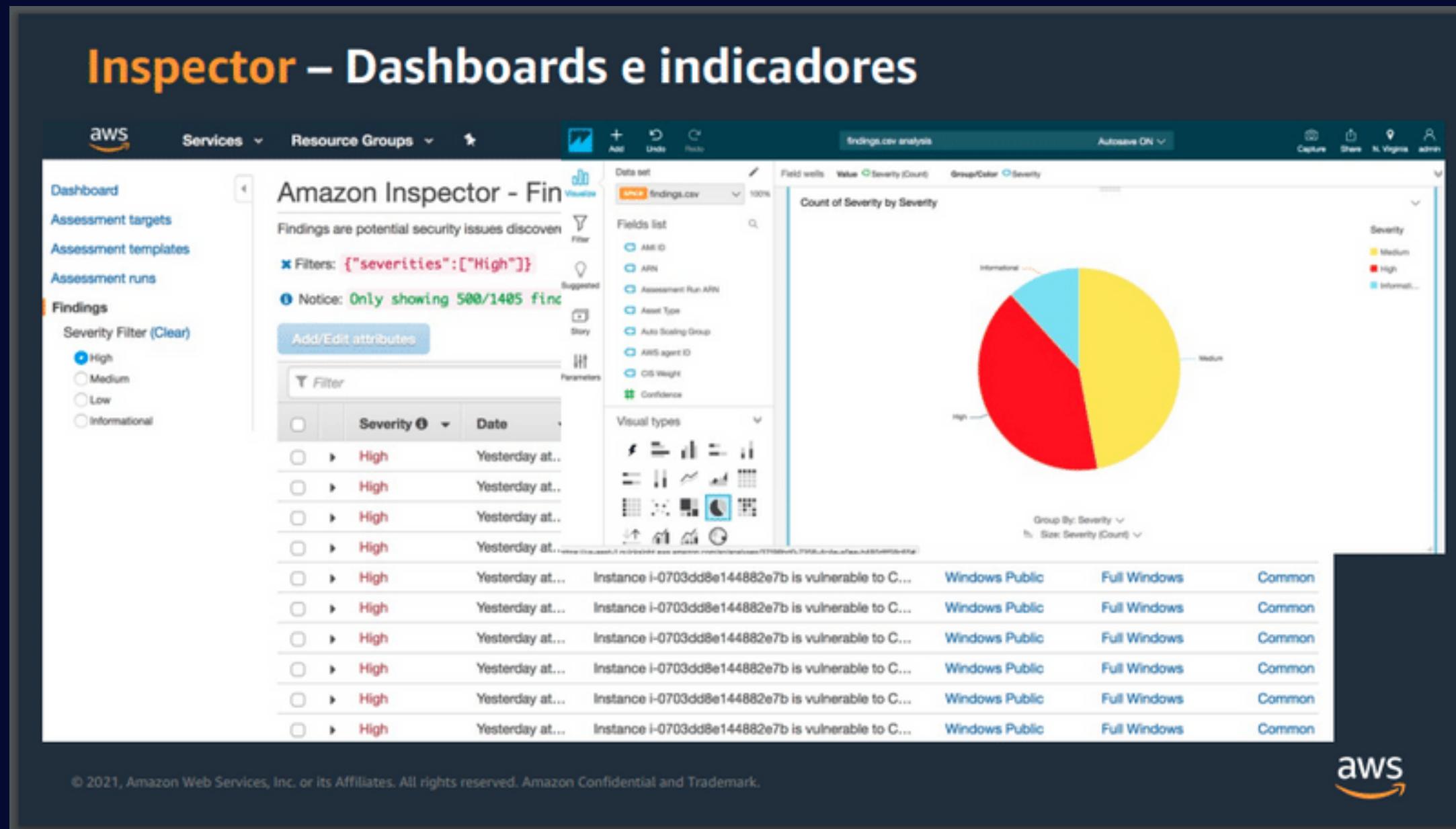
Inspector – Mapeie continuamente possíveis vulnerabilidades

- Serviço de Gestão de Vulnerabilidades integrado com o ambiente de nuvem
- Automatizado via API
- Integrado com CI / CD
- Diferentes pacotes de análise
 - CIS
 - CVE
 - Comportamento
 - Melhores práticas AWS
- **New** Alcance de rede
- Geração e controle de findings



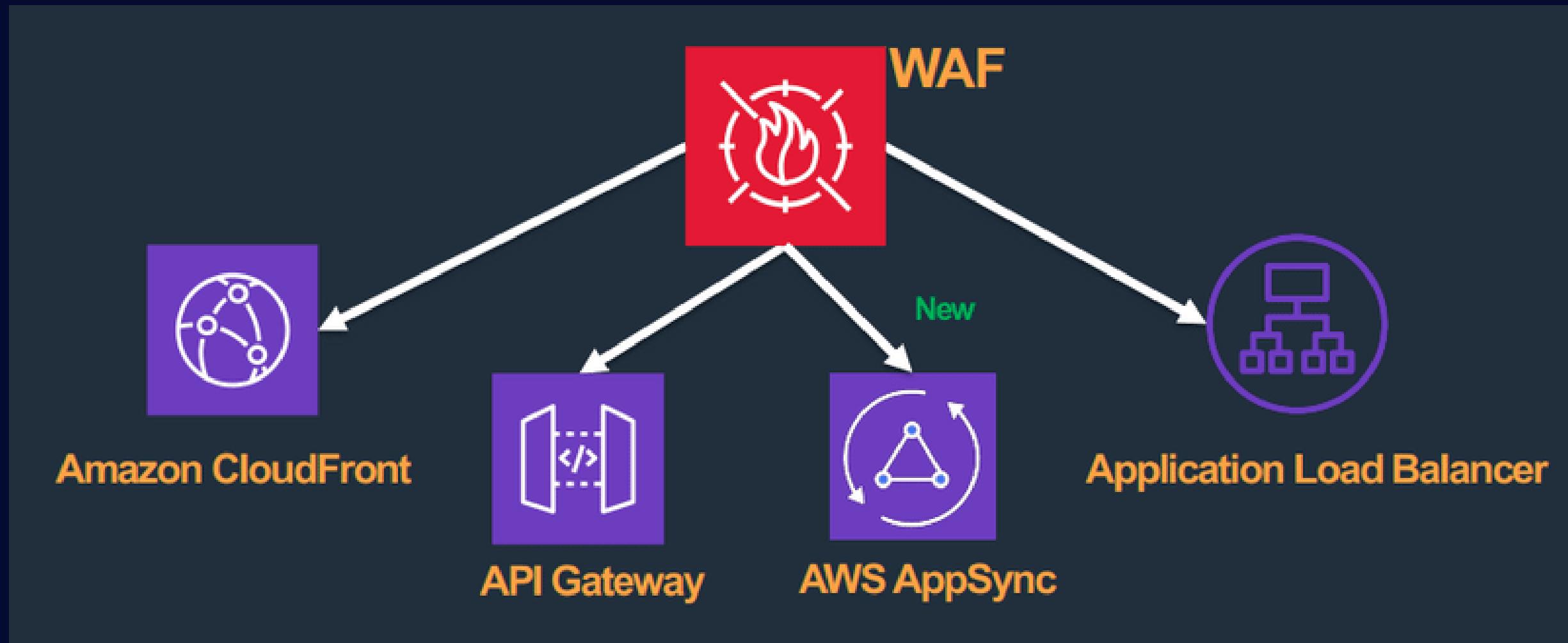
© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.

Amazon Inspector



WAF

FIREWALL DE APLICAÇÃO



WAF

FIREWALL DE APLICAÇÃO

AWS WAF – Automação de criação de regras

The slide illustrates the capabilities of AWS WAF by listing several types of threats it can detect and prevent:

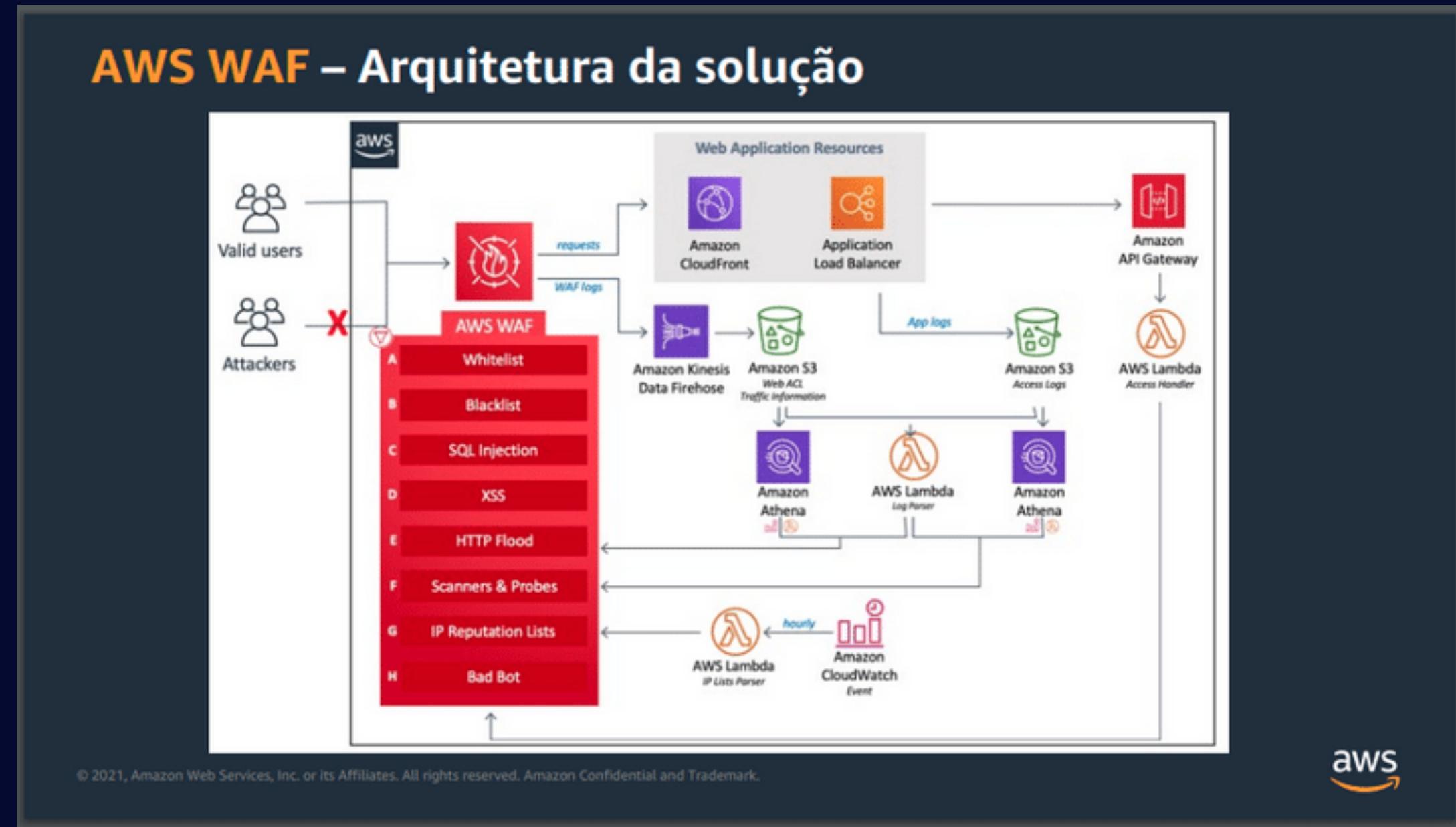
- IP reputation lists (represented by a clipboard icon)
- HTTP floods (represented by a person icon sending multiple requests to a server)
- Scanners and probes (represented by a computer monitor displaying a document with an exclamation mark)
- Bots and scrapers (represented by a magnifying glass over a bug icon)
- SQL injection (represented by a magnifying glass over a database schema icon)
- Cross-site scripting (represented by two overlapping squares with an upward arrow between them)

AWS WAF Security Automations
<https://aws.amazon.com/answers/security/aws-waf-security-automations/>

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.

WAF

FIREWALL DE APLICAÇÃO



AWS Network Firewall e outros serviços de segurança AWS

	AWS Network Firewall	VPC Security Group	Network ACL	AWS WAF
Onde a proteção é aplicada?	Nível de rota, baseado nas rotas de VPC	EC2 – nível de instância	Nível de subrede	Nível de Endpoint (API Gateway, ALB, CloudFront)
Stateful ou Stateless	Ambos	Stateful	Stateless	Stateless
Quais fluxos são protegidos?	Todo fluxo de ingresso/egresso no perímetro da VPC (e.g. IGW, VGW, DX, VPN, VPC-VPC)	Todo fluxo de ingresso/egresso no nível de instância (EC2-EC2, EC2-IGW, EC2-DX, etc.)	Todo fluxo de ingresso/egresso no nível de subredes (subnet-subnet, subnet-IGW, subnet-DX, etc.)	Apenas Ingresso da internet para o API Gateway, ALB ou CloudFront
Qual a camada OSI?	L3-7	L4	L3	L7
Features	Stateless/ Regras ACL L3, Regras stateful/L4, Regras IPS-IDS/L7, filtro FQDN, Detecção de Protocolo, Deep packet inspection, Listas IP block/allow largas	Filtro IP Porta Protocolo	Filtro IP Porta Protocolo	Filtragem profunda da camada de aplicativo, regras gerenciadas
Comportamento Padrão	Allow	Deny	Allow	Cliente escolhe



- 01 BÁSICO
- 02 PONTO DE ENTRADA
- 03 PORTAS E PROTOCOLOS
- 04 FIREWALL E AMEAÇAS
- 05 FERRAMENTAS POR ETAPAS
- 06 OUTRAS FERRAMENTAS

Soluções de Segurança NA Nuvem AWS



Gestão de Acessos e Identidade

AWS Identity & Access Management (IAM)

AWS Organizations

AWS Control Tower

AWS Cognito

AWS Directory Service

AWS Resource Access Manager

AWS Single Sign-On

Conformidade

AWS Audit Manager*(new)

AWS Artifact



Controles de Detecção

AWS CloudTrail

AWS Security Hub

Amazon Inspector

AWS Config

Amazon CloudWatch

Amazon GuardDuty

VPC Flow Logs

Trusted Advisor

IAM Access Analyzer

AWS IoT Device Defender



Segurança em Infraestrutura

AWS Systems Manager

AWS Shield

AWS Web Application Firewall (WAF)

Amazon Virtual Private Cloud (VPC)

EC2 Image Builder

Bastion Host

AWS Firewall Manager

AWS Network Firewall*(new)



Proteção de Dados

AWS Key Management Service (KMS)

AWS CloudHSM

Amazon Macie

Certificate Manager

Server Side Encryption

S3 Block Public Access

AWS Signer*(new)

AWS Secrets Manager



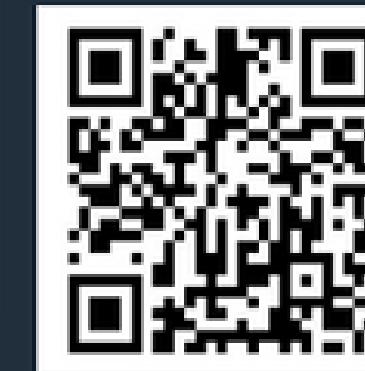
Resposta a Incidentes

AWS Config Rules

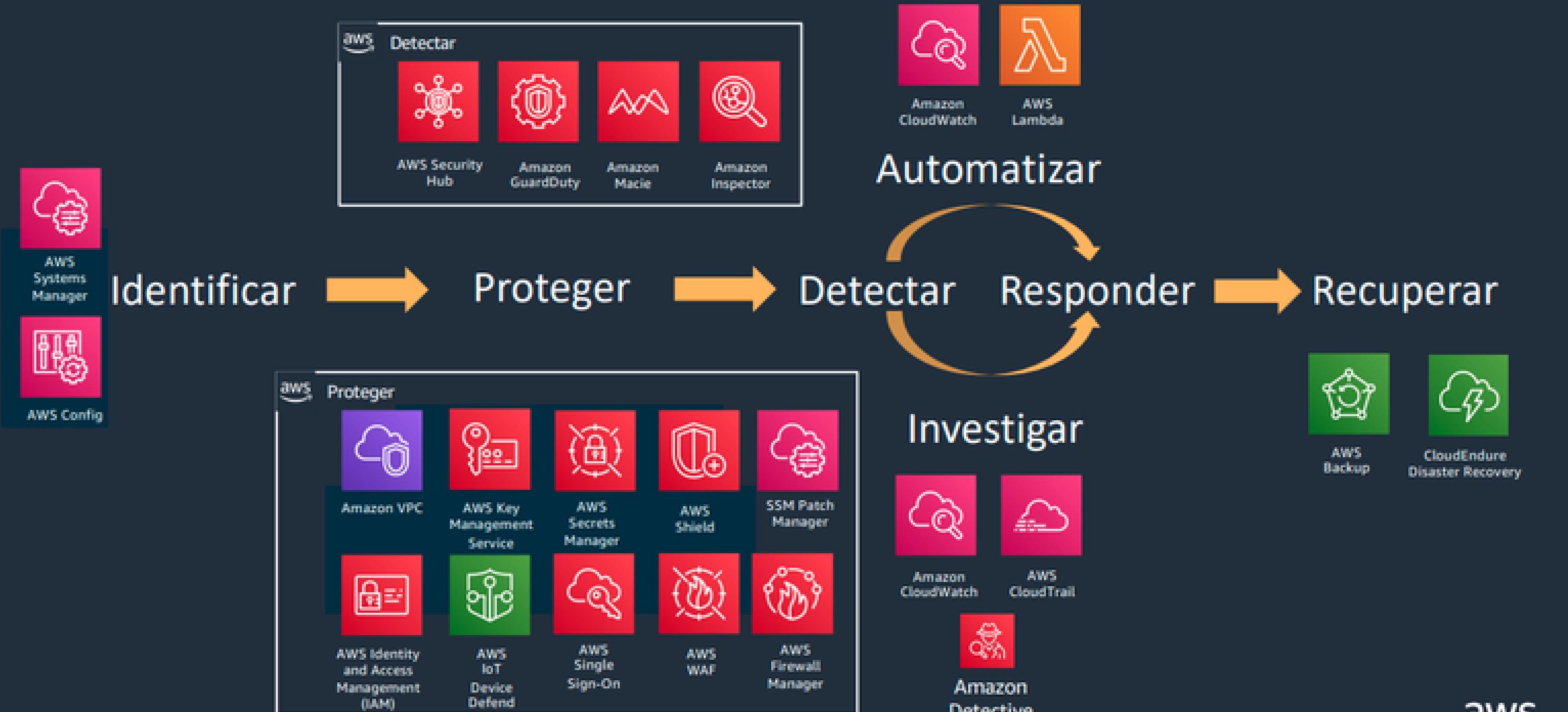
Amazon Detective

AWS Lambda

CloudEndure Disaster Recovery



Serviços AWS para mitigar ransomware

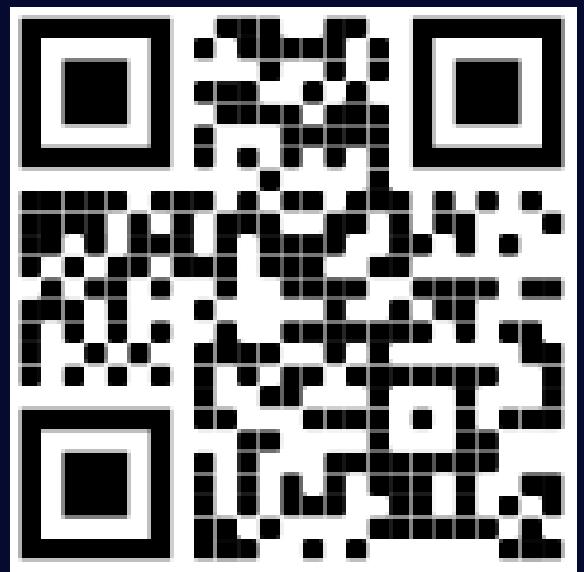




- 01 BÁSICO
- 02 PONTO DE ENTRADA
- 03 PORTAS E PROTOCOLOS
- 04 FIREWALL E AMEAÇAS
- 05 FERRAMENTAS POR ETAPAS
- 06 OUTRAS FERRAMENTAS

SECURITY SCORECARD

C 70 NETWORK SECURITY Detecting insecure network settings	7 findings  View findings
A 90 DNS HEALTH Detecting DNS insecure configurations and vulnerabilities	2 findings  View findings
D 67 PATCHING CADENCE Out of date company assets which may contain vulnerabilities or risks	64 findings  View findings
A 100 ENDPOINT SECURITY Detecting unprotected endpoints or entry points of us	CUBIT SCORE Proprietary algorithms checking for implementation of common security best practices No findings  View findings
A 100 IP REPUTATION Detecting suspicious activity, such as malware or spam	HACKER CHATTER Monitoring hacker sites for chatter about your company No findings  View findings
C 77 APPLICATION SECURITY Detecting common website application vulnerabilities	INFORMATION LEAK Potentially confidential company information which may have been inadvertently leaked No findings  View findings
	SOCIAL ENGINEERING Measuring company awareness to a social engineering or phishing attack 8 findings  View findings





DOWNLOAD GRATUITO
Verifica 16 IPs

- ✓ Alta velocidade, avaliações profundas;
- ✓ Treinamentos e orientações gratuitos;
- ✓ Suporte por meio da Comunidade Tenable;
- ✓ [Treinamentos sob demanda disponíveis.](#)

Ideal para: educadores, alunos e pessoas em início de carreira na área de segurança cibernética. [Saiba mais sobre o uso do Essentials em sala de aula com o programa Tenable para Educação.](#)



<https://tenable.com/products/nessus>



OpenVAS by Greenbone

Open Vulnerability Assessment Scanner

<https://www.openvas.org/>



REFERÊNCIAS



LINKS

Mais algumas ações de redução (em inglês)

<https://george-51059.medium.com/reduce-aws-costs-74ef79f4f348>

Dimensionamento de máquinas

<https://aws.amazon.com/pt/ec2/instance-types/>

<https://instances.vantage.sh/>

<https://aws.amazon.com/pt/ec2/spot/instance-advisor/>

Você pode configurar para forçar o MFA nas contas utilizando uma política.

https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html

Jornada de Segurança na AWS

<https://maturitymodel.security.aws.dev/pt/>

0. Engatinhar (Quick Wins)

Segurança do root (MFA, AK)

Contatos da conta

Alarme de Billing

Habilitar IAM Access Analyzer c/ notificação

GuardDuty c/ notificação p/ eventos alta severidade

S3 Block Public Access

Regras AWS Config (portas críticas publicas, etc)

Uso de múltiplas contas com SCPs:

- Proteção CloudTrail
- Limitação de regiões em uso
- S3 Block Public Access

1. Andar

SSO para usuários / Federação IAM

+ Remoção/Rotacionamento Access-Keys

Bastion Host / Session Manager

Resolver Descobertas Trusted Advisor

Criptografia em trânsito

Plano de treinamento e certificação em segurança

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.

2. Correr

Habilitar SecHub com avaliações AWS Foundational+CIS

Estender regras AWS Config

Uso de múltiplas contas / Control Tower

Web Application Firewall

Criptografia em repouso

Iniciar automatização de resposta a incidentes

Hardening de Imagens

Rotacionamento de segredos

Coleta de logs (Security Data Lake) / SIEM

Mapeamento de dados críticos

3. Voar

Automatização de resposta a incidentes

Segurança no pipeline CI/CD

• Modelamento de Ameaças (Threat Modelling)

• (SAST, DAST, Fuzzing)

• Verificação (Linting) infra-as-code

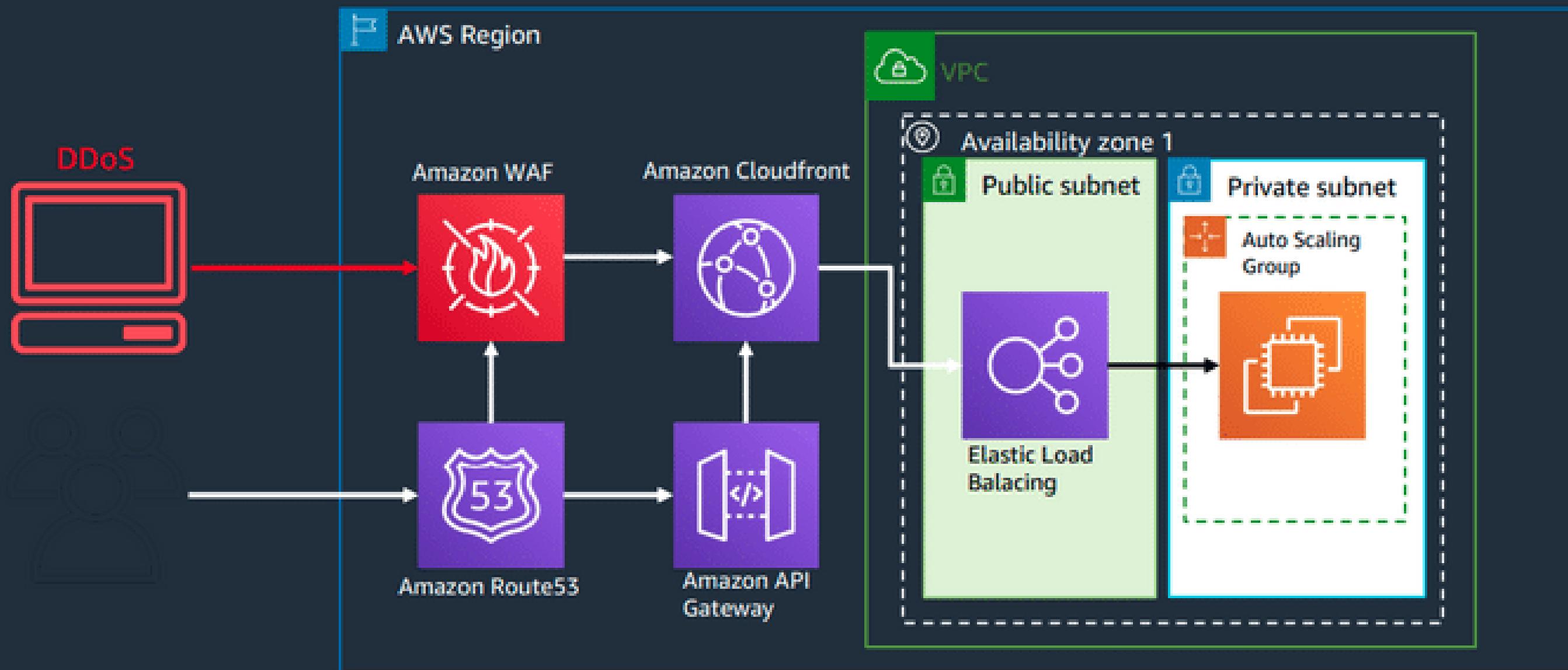
Security as Code

• IAM Policies

• Playbooks, etc.



Proteção de DDoS – Boas práticas e camadas de proteção



https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.



Use as melhores práticas como base

WA Security Pillar



<https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>

Use as melhores práticas como base WA Tool

The screenshot shows the AWS Well-Architected Tool landing page. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, a search bar, and user account information ('admin @ mailto', 'N. Virginia', and 'Support'). Below the navigation, a 'Management Tools' section is visible. The main feature is the 'AWS Well-Architected Tool' card, which includes the title, a subtitle ('Learn, measure, and build using architectural best practices'), and a descriptive paragraph about the tool's purpose. To the right of the main card is a white callout box titled 'Define a workload' with a sub-instruction and an orange 'Define workload' button.

<https://aws.amazon.com/well-architected-tool/>

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.

aws

Use as melhores práticas como base

CIS AWS Foundations



https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

Use as melhores práticas como base

Recursos de Segurança

Recursos de segurança

Segurança Teste de penetração Boletins de segurança Recursos Conformidade Parceiros

Blog de segurança da AWS
[Saiba mais »](#)

Para obter as informações e atualizações mais recentes sobre a segurança da AWS, acesse o blog de segurança da AWS.

Boletins de segurança da AWS
[Saiba mais »](#)

Veja os boletins mais recentes sobre eventos de segurança e privacidade com serviços da AWS.



<https://aws.amazon.com/pt/security/security-resources/>

Aprendizado de Segurança na AWS

AWS Ramp-Up Guide: Security



AWS Training and Certification has created this and other AWS Ramp-Up Guides to help build your knowledge of the AWS Cloud. Each expertly curated guide features free digital training, classroom courses, videos, whitepapers, certifications, and other information you're looking for. To enroll in training and certification exams, and track your progress, visit aws.training and set up a free account. To provide suggestions on Ramp-Up Guides, please contact rampupguides@amazon.com.

Learn the fundamentals of AWS Cloud

LEARNING RESOURCE	DURATION	TYPE
AWS Ramp-Up Guide: Cloud Practitioner	10 minutes	Ramp-Up Guide »

Step 1: Learn the cloud security fundamentals

LEARNING RESOURCE	DURATION	TYPE
How Should We All Think About Security (from AWS re:Invent)	1 hour	Video »
AWS Fundamentals: Securing your AWS Cloud	50 minutes	Digital Training »
AWS Philosophy of Security (from AWS re:Invent)	1 hour	Video »
AWS Shared Responsibility Model	5 minutes	Digital Training »
Getting Started with AWS Security, Identity, & Compliance	3 hours	Digital Training »
AWS Security Fundamentals (Second Edition)	2 hours	Digital Training »
AWS Security Essentials	1 day	Classroom Training »

https://d1.awsstatic.com/training-and-certification/ramp-up_guides/Ramp-Up_Guide_Security.pdf

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.





Ficou alguma dúvida?

Esperamos que você tenha aprendido algo novo.



 /IN/DIONIZIOAF



 /IN/ANDREFELIPEFIALKOWSKI