**Oficina de Projetos - Projeto 7**

Implantação do sistema UpperMed em ambiente Cloud AWS pela empresa Cloud Solução

Local: São Paulo – SP

Data: 08/12/2022

Proposta: 221208-1

Versão: V1

# Integrantes do Grupo 1

Adriano Braganca de Oliveira

Allyson Ribeiro de Moura

Arlindo Ramos

Danilo Henrique Silva Dias

Danilo Marcus Santos Ribeiro

Eduardo C. Vilaro

Eduardo de Jesus Gomes

Galdino Neto de Oliveira Junior

Giovani Grippo

Jeam Martins Alves

Joao Paulo Vieira de Andrade

Jony dos Santos BArbosa

Milena Santana

Renaldo Baur Filho

Rene Salomão

Ricardo Evangelista Santana

Ulisses Fadini

Valdir Aparecido Da Silva

William dos Santos

Willian Gabriel de Mello Gois

# Sumário

[**Integrantes do Grupo 1**](#_dklvgcs0umh2) **2**

[**Sumário**](#_3tr7y8llysre) **3**

[**Institucional**](#_dgehullfzirb) **4**

[Quem somos](#_je4py2io5377) 4

[Portfólio](#_1k989n8b3387) 4

[**Implementação**](#_amj3n8k8ubkt) **4**

[Escopo](#_a0tztz77fwsj) 4

[Cronograma](#_1vurxu3s8ese) 4

[**Cenário atual**](#_sn5jjubx9ql0) **6**

[**Proposta Técnica**](#_w8awhcb06crg) **7**

[Arquitetura Proposta](#_2lkk1i7m3b40) 7

[Requisitos da aplicação](#_h2jb15r97bds) 8

[VPC e Sub Redes](#_curvbx9l1ky1) 8

[Tabela de Rotas](#_9zrco183j6om) 8

[Network ACLs](#_opb5lic5yt43) 9

[Grupos de Segurança](#_iqxjtjxlvqor) 9

[Internet Gateway](#_bq6fjsb4pipu) 10

[Amazon ELB (Elastic Load Balancer)](#_bu1fi29zwewj) 10

[Target Group](#_p1ru521z5dgh) 12

[Amazon Route 53](#_eirzc2k3m09y) 12

[Amazon CloudFront](#_varrbfdz06mb) 13

[AWS WAF - WAF to CloudFront](#_5qvmz034mdjj) 14

[Amazon Auto scaling](#_xr9f9vmhbssz) 15

[Ligar e Desligar (Agendamento automático)](#_huxq687rk1po) 16

[Amazon Simple Storage Service (Amazon S3)](#_hk89dvui0e0) 16

[Amazon Elastic Compute Cloud (Amazon EC2)](#_o01cpt6bn5g9) 17

[Amazon Relational Database Service (Amazon RDS)](#_ub7v9t1zmiy0) 18

[Teste de Estresse nas instâncias](#_8evfdfdqed7n) 19

[**Proposta Comercial**](#_hhk2bnd1ge1r) **21**

[**Anexos**](#_119pm3ir0x19) **23**

# Institucional

## Quem somos

A Cloud Solução é uma empresa especializada em Tecnologia da Informação que atende em todo o território nacional fornecendo serviços em cloud, como implantação, migração e consultoria. O principal provedor de serviços em cloud utilizado pela empresa atualmente é a AWS, simplesmente pelo fato de ser a maior plataforma, com uma grande quantidade de serviços disponíveis, o que possibilita oferecer aos clientes um serviço de qualidade e diverso.

Atuamos apenas no Brasil com todos os colaboradores em formato de *home office.* Oferecemos o serviço de consultoria mensal para diversos tipos de clientes, onde é possível fazer uma POC (proof of concept) por 15 dias.

## Portfólio

Temos clientes em todo o Brasil, especialmente nos estados de SP, MG, BA, MS, ES e PA.

# Implementação

## Escopo

A ideia deste projeto é realizar a criação de uma infraestrutura em cloud AWS e por conseguinte fazer a migração do sistema MediaWiki utilizado pela UpperMed, que atualmente está rodando on-premise. O servidor de aplicação e de banco do cliente atualmente se encontram defasados e não mais atendem aos requisitos mínimos de qualidade, pois vem sofrendo problemas de indisponibilidade e lentidão.

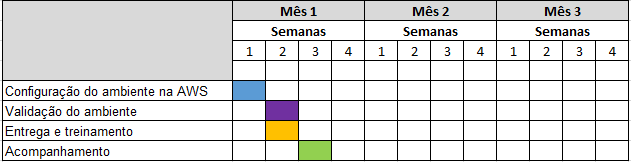
No intuito de resolver os problemas supracitados, foi proposta uma arquitetura moderna e escalável em AWS que irá prover recursos de forma dinâmica e sob demanda, isto é, pagamento apenas pelo recurso utilizado, onde o cliente terá um maior controle da qualidade dos serviços, do custo e também garantir que sua estrutura de servidores sejam sempre atuais e facilmente escalável.

## 

## 

## 

## Cronograma



\* Configuração do ambiente na AWS( abertura de conta e etc…) Migração de dados

# Cenário atual

Foi informado pela TI do cliente que há uma máquina virtual que comporta a solução, porém está com poucos recursos de memória e processador, fazendo com que a VM trave ou tenha alguns períodos de lentidão.

A empresa possui 30 lojas e o sistema é acessado por até oito colaboradores, muitas das vezes necessitando acessar dados de fora no local físico onde estão os servidores, por exemplo, quando é necessário fazer algum atendimento local em alguma das lojas, se o funcionário da TI precisar consultar alguma informação ou procedimento da Wiki ele não consegue, seja por indisponibilidade de rede, internet ou mesmo lentidão.

Atualmente a MediaWiki está rodando em uma VM com sistema operacional CentOS na versão 7.0.1406, possui 12 GB de memória RAM e 2 vCPU. O banco de dados utilizado é o MariaDB 10.1 e também está instalado nesta mesma VM. Utiliza como Web Server o Apache para atender o sistema que é em PHP.

O banco de dados consome 20 GB de armazenamento e ainda possui cerca de 30 GB de armazenamento em arquivos de todas as lojas.

O horário de funcionamento do setor de TI é das 09:00 às 19:00 de segunda a sexta-feira e das 09:00 às 13:00 aos sábados.

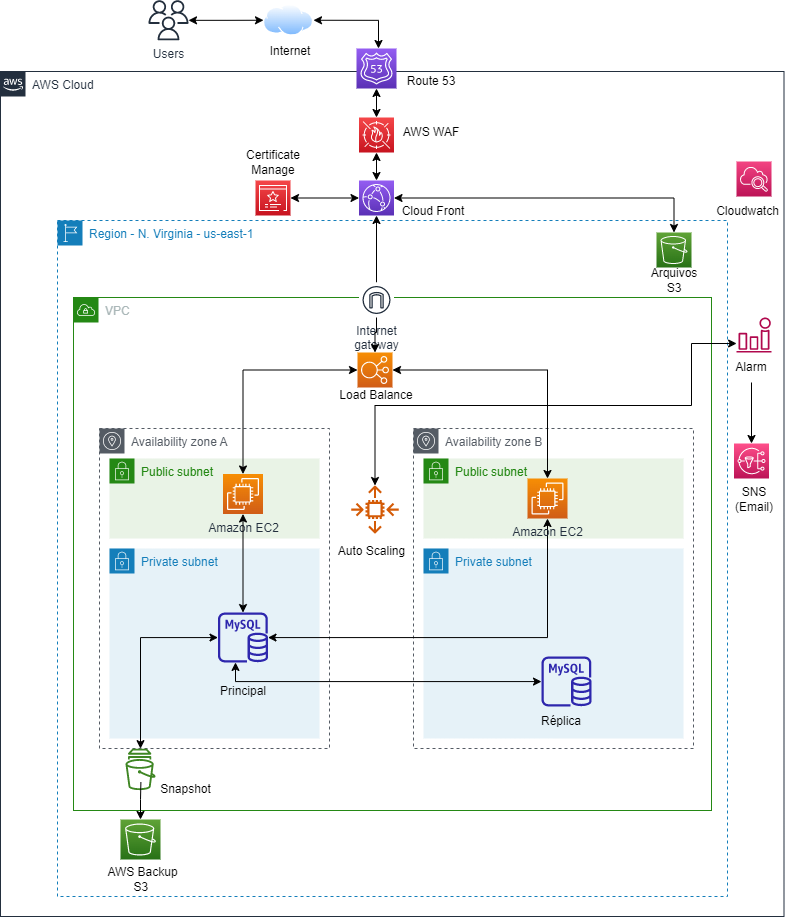
# 

# Proposta Técnica

## Arquitetura Proposta

A arquitetura proposta se baseia em nuvem utilizando recursos disponibilizados pela AWS (Amazon Web Services) visando garantir segurança, disponibilidade, velocidade e escalabilidade sob demanda. E para isso foi montado o diagrama a seguir.

Diagrama da solução:



## Requisitos da aplicação

* Instância com servidor Linux Ubuntu (20), Apache e PHP (7.4.3+)
* Banco de dados MySQL na versão mais atual disponível
* API para conectar a mediaWiki ao S3

## VPC e Sub Redes

No projeto será utilizado 1 (uma) VPC contendo quatro sub-redes, onde duas são públicas e duas privadas. As instâncias EC2 ficarão nas sub-redes públicas, protegidas por firewall de borda e aplicação. As instâncias EC2 acessarão outros serviços da AWS, tais como o banco de dados MySQL e o armazenamento de objetos S3, onde serão armazenados todos os arquivos atuais (30 GB) e futuros.

A VPC será criada na região da Virgínia, onde os custos dos serviços são menores, pois a aplicação não tem restrição de ser hospedada no Brasil e não tem demanda para baixa latência a ponto de precisar usar uma região em SP. Para minimizar a latência utilizaremos o CloudFront que é um serviço de entrega de conteúdo (CDN), a sua função é fazer um cache na região de São Paulo para os usuários do Brasil terem uma melhor performance.

VPC

Nome: wiki-vpc

IPv4 CIDR: 10.1.0.0/16

Habilitamos o DNS hostnames e DNS Resolution



SUBNET

2 públicas e 2 privadas conforme imagem abaixo



## Tabela de Rotas

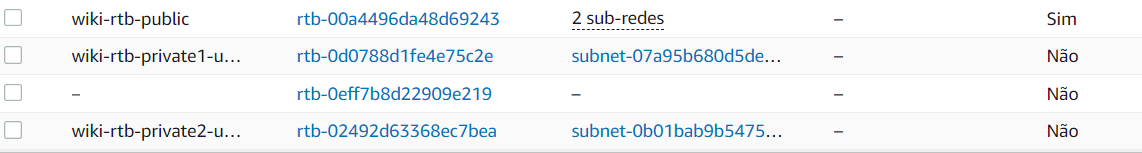
As rotas foram definidas para atender à necessidade das subnets públicas e privadas, onde apenas a subnet pública tem acesso à internet.

Rota pública:

* A rota pública foi associada às subnets públicas.
* Na edição de rotas liberamos qualquer destino para o nosso internet gateway.

Rota privada:

* A rota privada foi associada às subnets privadas.



## Network ACLs

Serão utilizados Network ACLs para fornecer uma camada de segurança em toda a VPC, controlando todo tráfego de entrada e saída das sub-redes.

Uma *network access control list* (ACL) permite, ou nega, tráfego específico de entrada (*inbound*) ou saída (*outbound*) no nível de sub-rede. Você pode usar a ACL de rede padrão para sua VPC, ou pode criar uma ACL de rede personalizada para sua VPC com regras semelhantes às regras de seus grupos de segurança para adicionar uma camada adicional de segurança à sua VPC.

ACL

Pública: acl-publica

Associamos na mesma as duas subnets públicas

Criamos regras de entrada (inbound rules) e saída (outbound rules) liberando o acesso HTTP e SSH para qualquer destino.

Criamos regras de acesso à portas efêmeras 1024-65535 para se ter tráfego interno e externo aplicando tais regras para entrada e saída

Privada: acl-privada

Associamos na mesma as duas subnets públicas

Criamos regra de saída liberando todo o tráfego

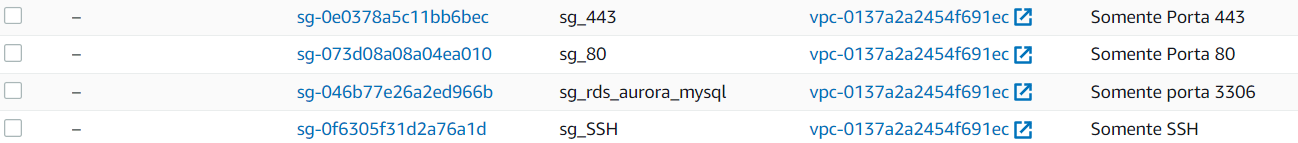
Criamos regra de entrada liberando somente a faixa da VPC (10.1.0.0/16)

## Grupos de Segurança

Um grupo de segurança controla o tráfego que tem permissão para acessar e sair dos recursos aos quais está associado. Por exemplo, depois de associar um grupo de segurança a uma instância do EC2, ele controla o tráfego de entrada e saída da instância.

Um grupo de segurança ou *security group* atua como firewall virtual para as instâncias do EC2 visando controlar o tráfego de entrada e de saída.

Criou-se um security group dentro da VPC para liberar acesso a instância Linux e com algumas regras específicas para a necessidade do cliente conforme pode ser conferido nas imagens abaixo.



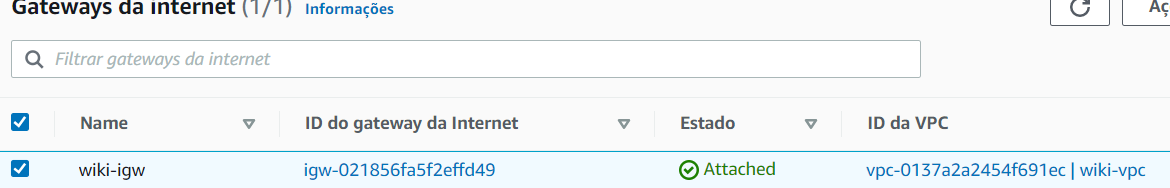
## 

## Internet Gateway

Internet Gateway é um componente da VPC horizontalmente dimensionado, redundante e altamente disponível que permite a comunicação entre a VPC e a Internet.

Se uma sub-rede estiver associada a uma tabela de rotas que tem o direcionamento para um gateway da Internet, ela é conhecida como sub-rede pública. Se uma sub-rede estiver associada a uma tabela de rotas que não tem um direcionamento para um gateway da Internet, ela é conhecida como sub-rede privada.

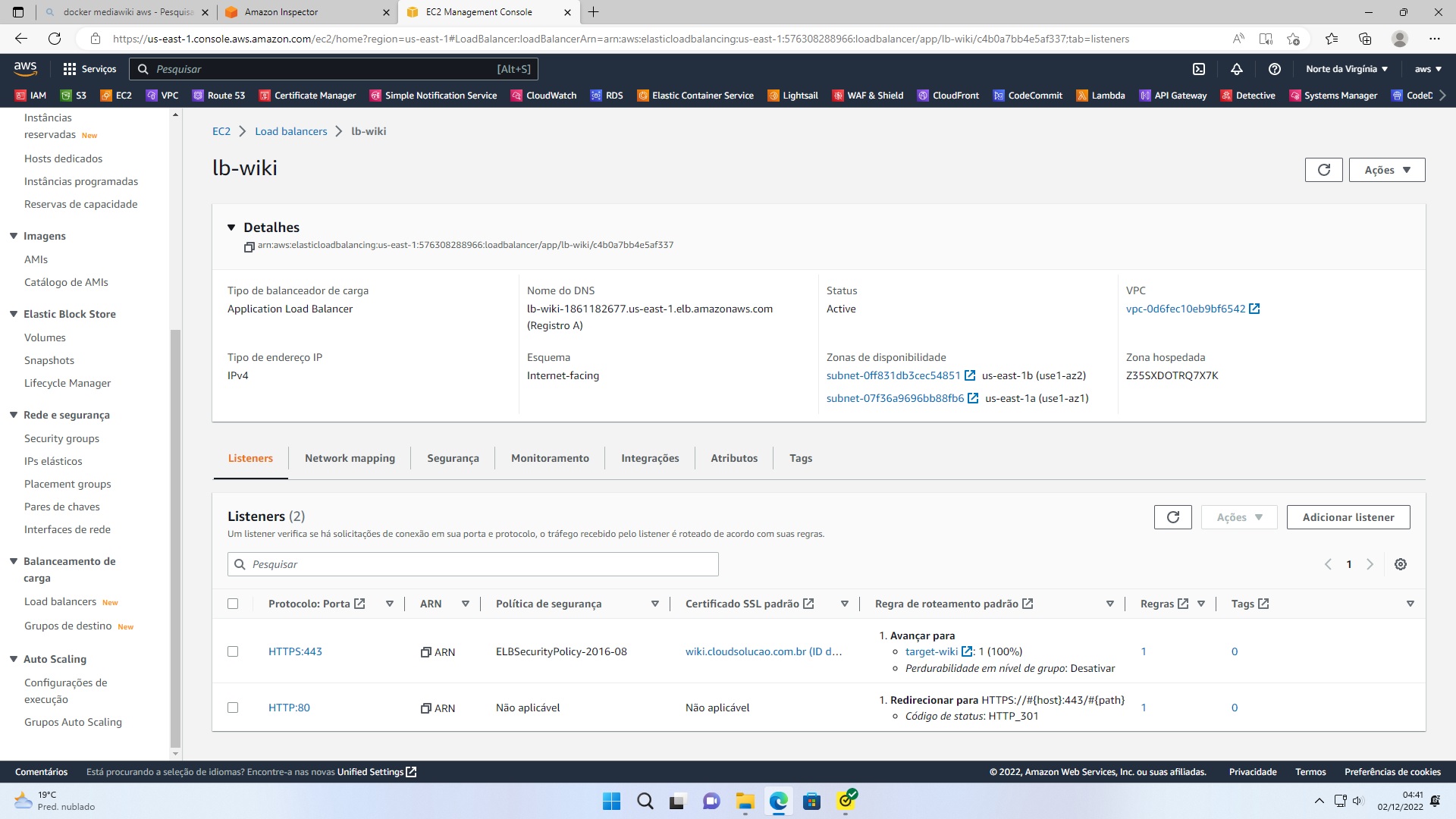
Foi criado um gateway de internet e associado à VPC para permitir acesso à internet, conforme imagem abaixo.

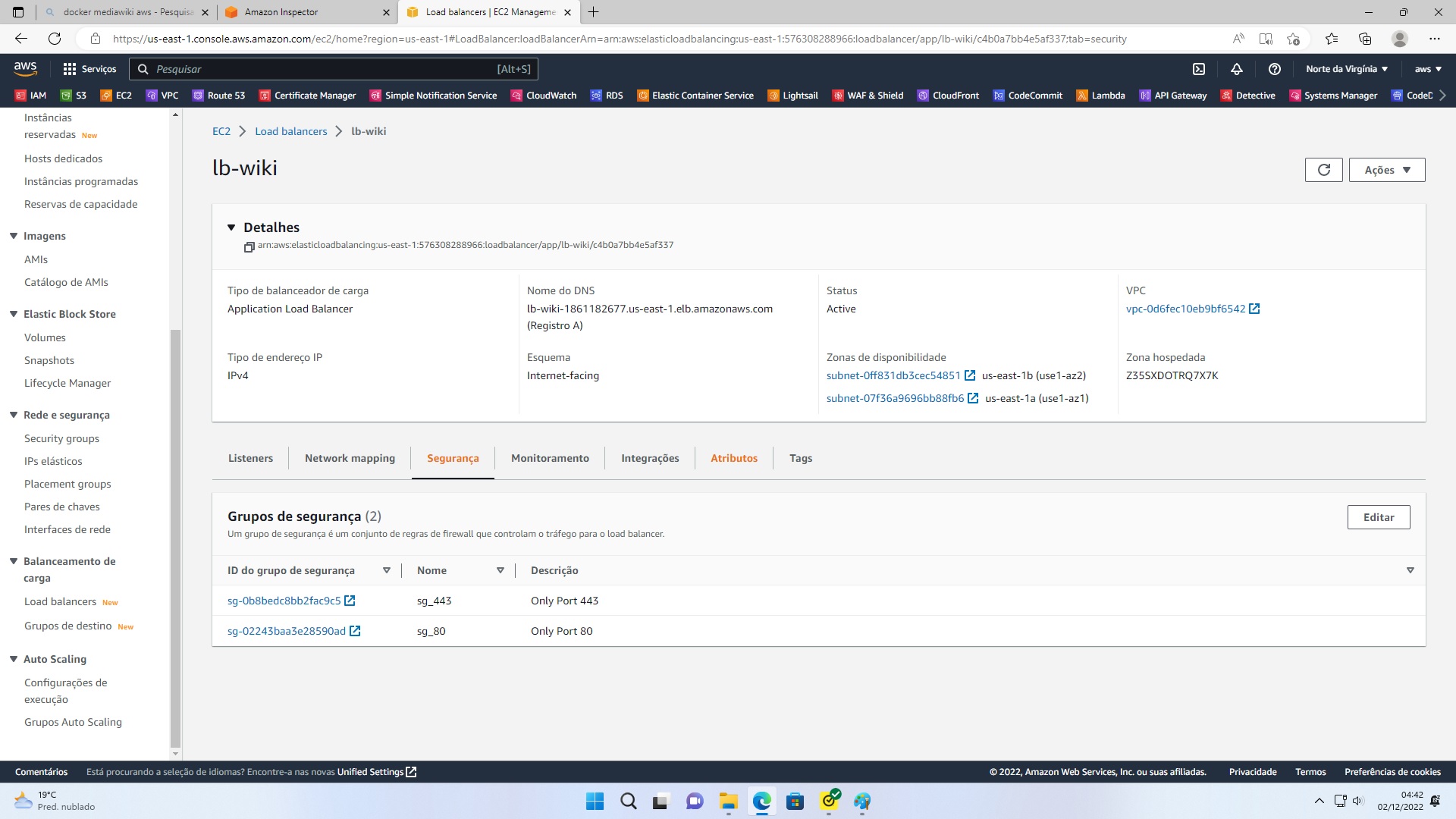


## Amazon ELB (Elastic Load Balancer)

Amazon Elastic Load Balancer distribui automaticamente as requisições externas para as instâncias (servidores), mantendo o equilíbrio distribuindo a carga entre os servidores, monitorando a saúde das instâncias e aplicações que estiverem disponíveis no cluster no momento em que as requisições são recebidas.

Seguem algumas imagens do load balancer aplicado, configurados para acesso por HTTP (80) e HTTPS (443).





## 

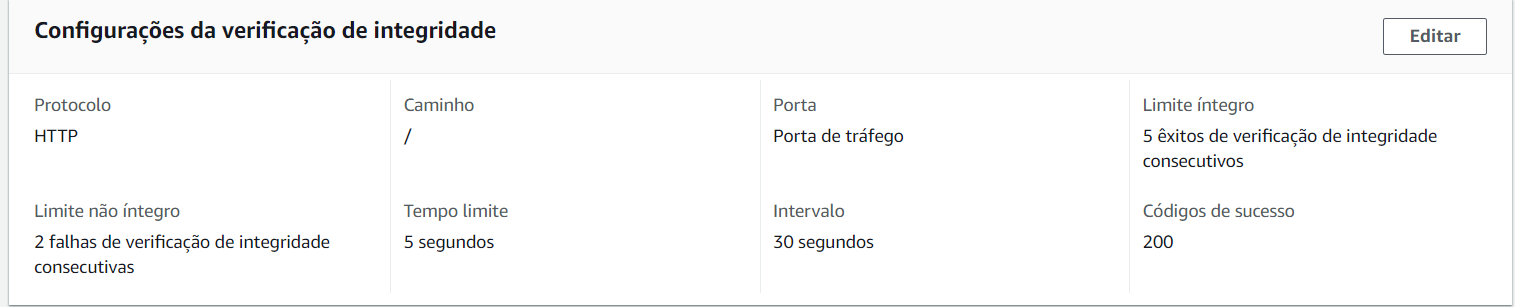
## Target Group

Cada grupo de destino é usado para rotear solicitações para um ou mais destinos registrados. Ao criarmos cada regra do listener, especificamos um grupo de destino e condições. Quando uma condição da regra é atendida, o tráfego é encaminhado para o grupo de destino correspondente. Podemos criar grupos de destino diferentes para tipos de solicitações diferentes. Por exemplo, podemos criar um grupo de destino para solicitações gerais e outros grupos de destino para solicitações para os microsserviços do aplicativo.

Definimos as configurações de verificação de integridade para o load balancer por grupo de destino. Após especificar um grupo de destino em uma regra para um listener, o load balancer monitora continuamente a integridade de todos os destinos registrados com o grupo de destino que estiverem em uma Zona de disponibilidade habilitada para o mesmo. O load balancer roteia solicitações para os destinos registrados que estão íntegros.



## 



## 

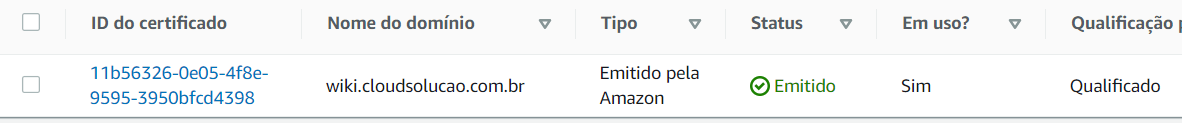
## Amazon Route 53

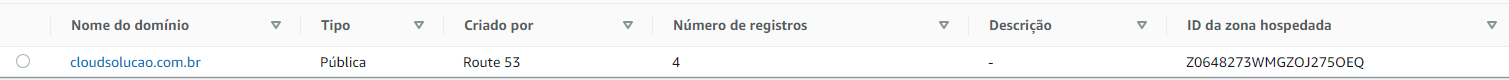
O Amazon Route 53 é um serviço web *Domain Name System* (DNS) na nuvem, com nível muito alto de disponibilidade e escalável. Projetado para oferecer aos desenvolvedores e empresas um meio altamente confiável e econômico de direcionar os usuários finais aos aplicativos de Internet, convertendo nomes para endereços IP numéricos, usados pelos computadores para se conectarem entre si.

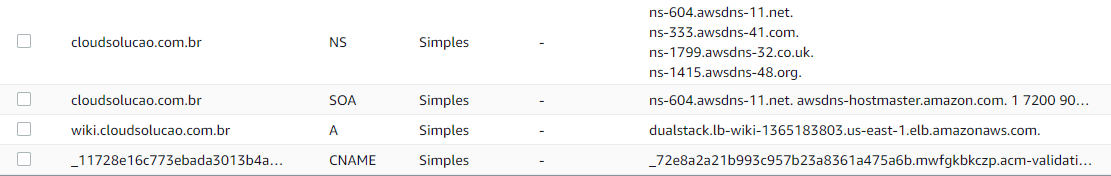
Publicação pelo domínio: cloudsolucao.com.br

Certificate Manager - DNS validation

Certificado que contempla os acessos abaixo: wiki.cloudsolucao.com.br



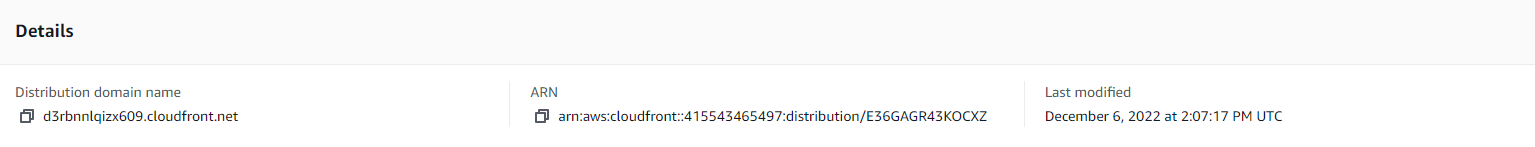


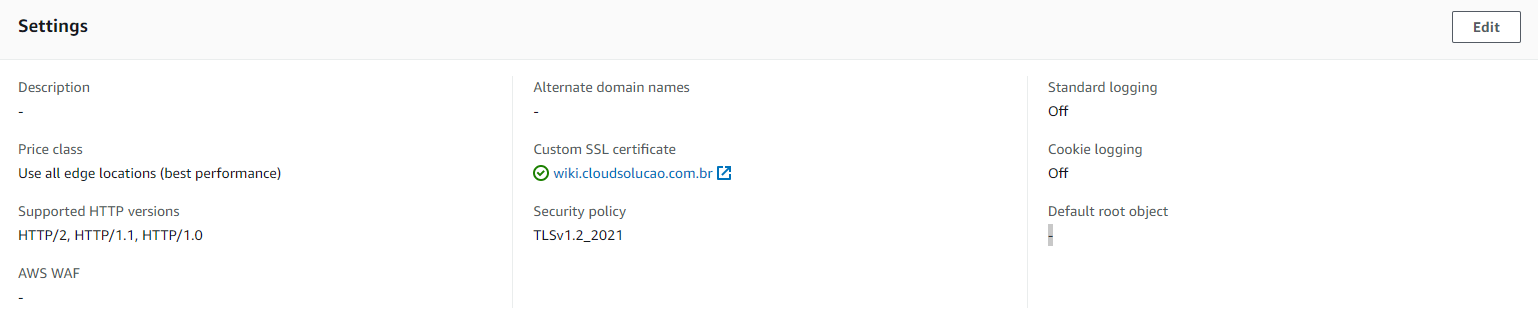


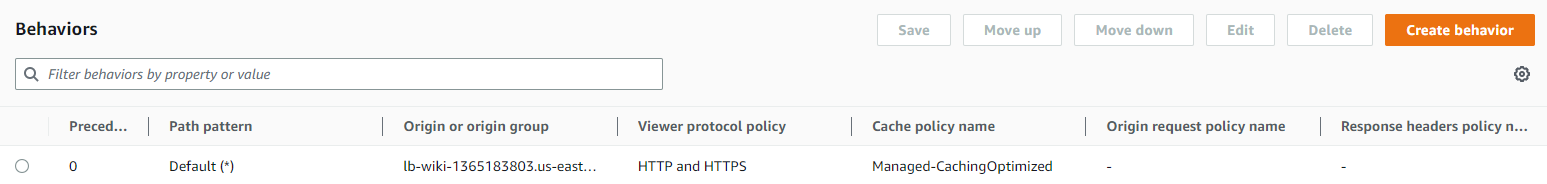
## Amazon CloudFront

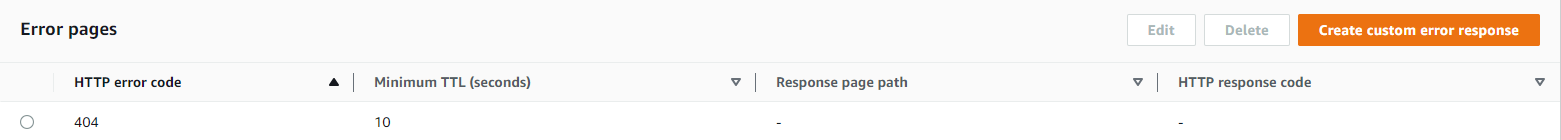
O Amazon CloudFront é um serviço de rede de entrega de conteúdo (CDN) criado para alta performance, segurança e conveniência do desenvolvedor. Acelera a distribuição de conteúdo estático e dinâmico da web, reduz a latência entregando dados através de mais de 410 pontos de presença (PoPs) dispersos globalmente com mapeamento de rede automatizado e roteamento inteligente.

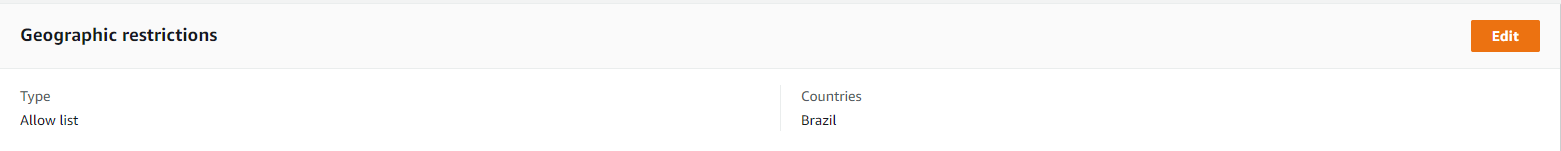
O cloudfront foi utilizado para criar um cache dos dados comuns acessados na aplicação.





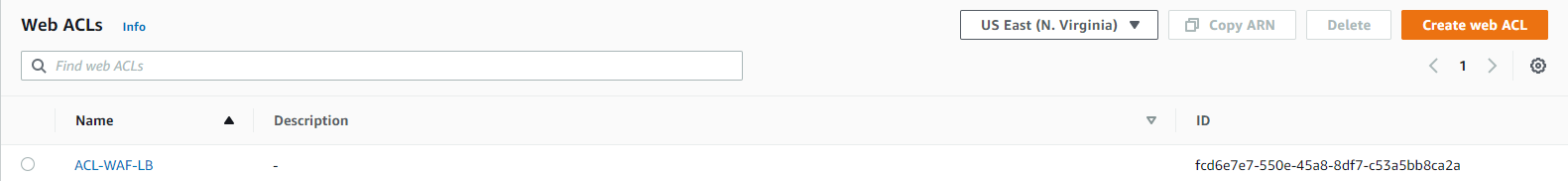


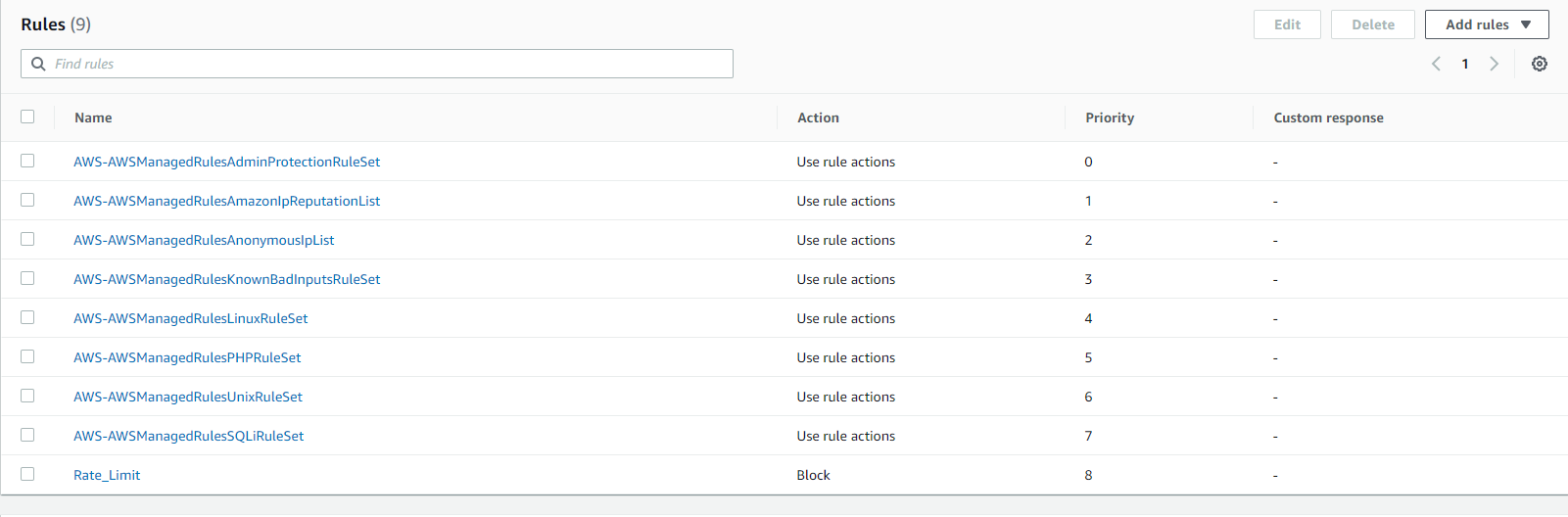


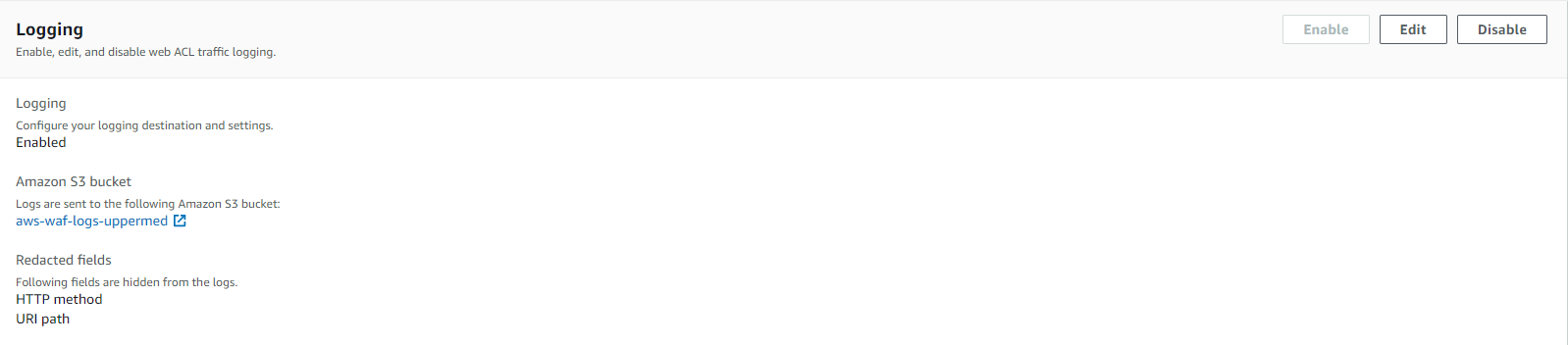


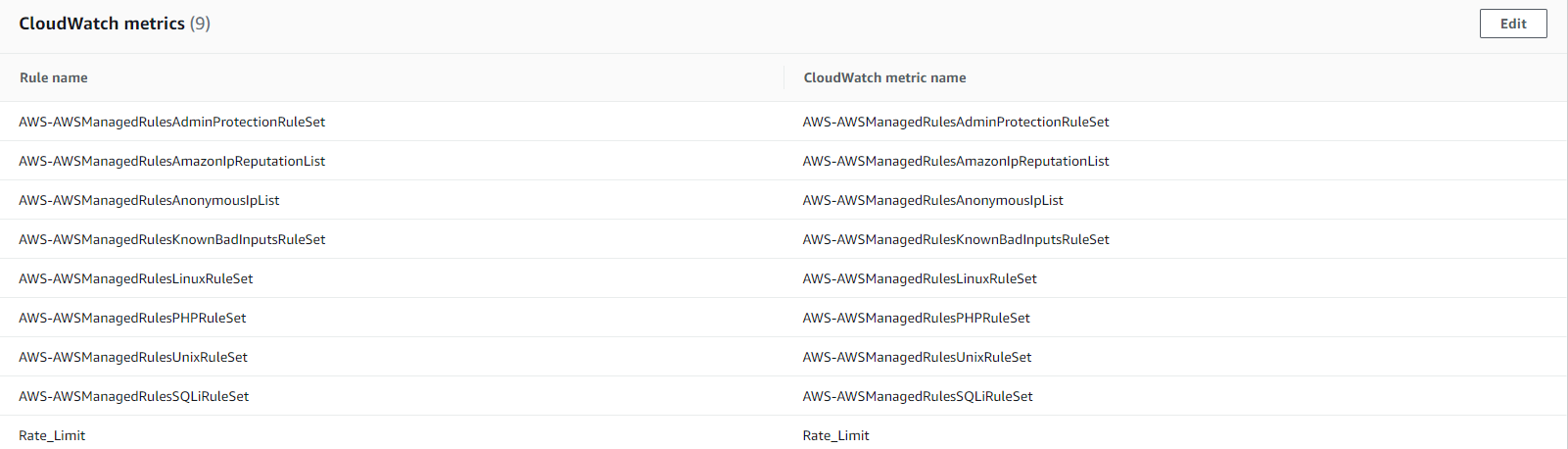
## AWS WAF - WAF to CloudFront

O AWS WAF é um firewall de aplicações Web que ajuda a proteger suas aplicações Web ou APIs contra bots e exploits comuns na Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos em excesso. Oferece controle sobre como o tráfego atinge suas aplicações, permitindo que criemos regras de segurança que controlam o tráfego de bots e bloqueiam padrões de ataque comuns. Agiliza a propagação e as atualizações de regras de segurança permitindo atualizarmos rapidamente a segurança em seu ambiente quando surgirem problemas.







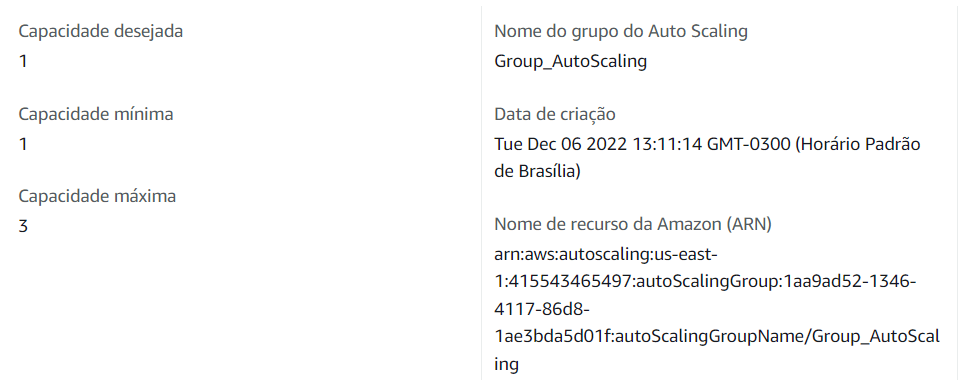


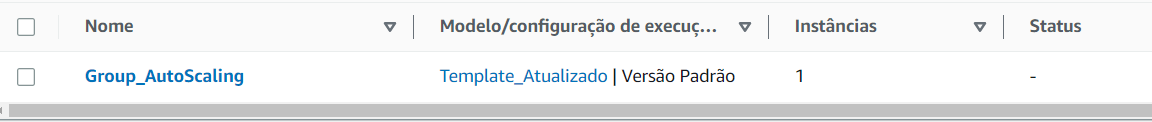
## Amazon Auto scaling

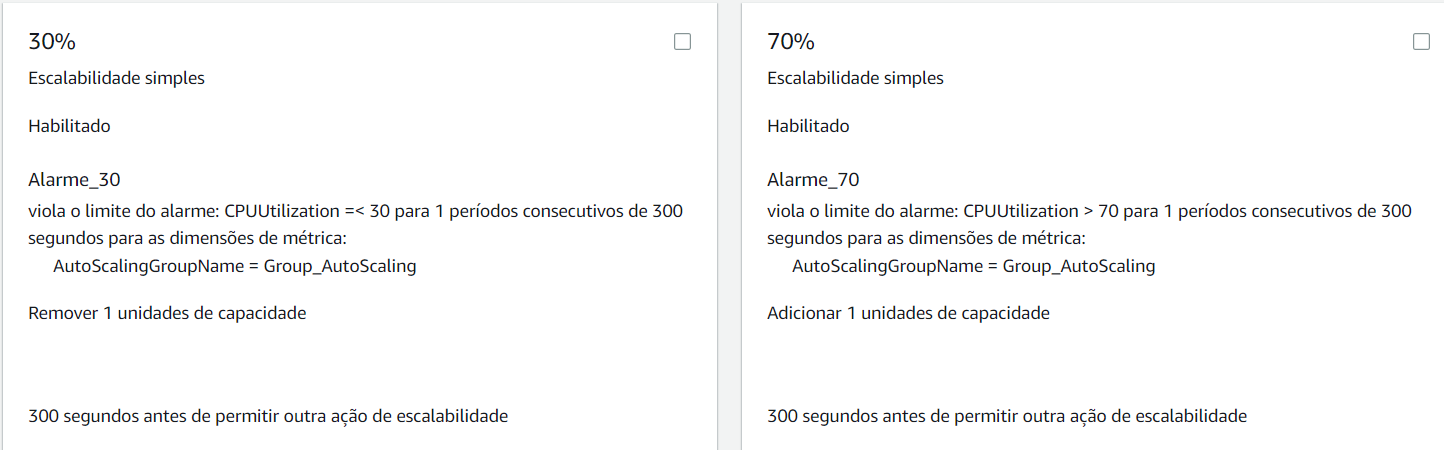
O AWS Auto Scaling monitora os recursos das instâncias e ajusta automaticamente a capacidade para manter um desempenho constante e previsível pelo menor custo possível.

Permite definir os níveis de utilização pretendidos para vários recursos, além de criar planos de escalabilidade que automatizam a forma como grupos de recursos diferentes respondem às flutuações de demanda, priorizando disponibilidade, custos ou um equilíbrio entre os dois. Com AWS Auto Scaling, é fácil configurar a escalabilidade de recursos de EC2 em questão de minutos.

AutoScaling - com base no template







## 

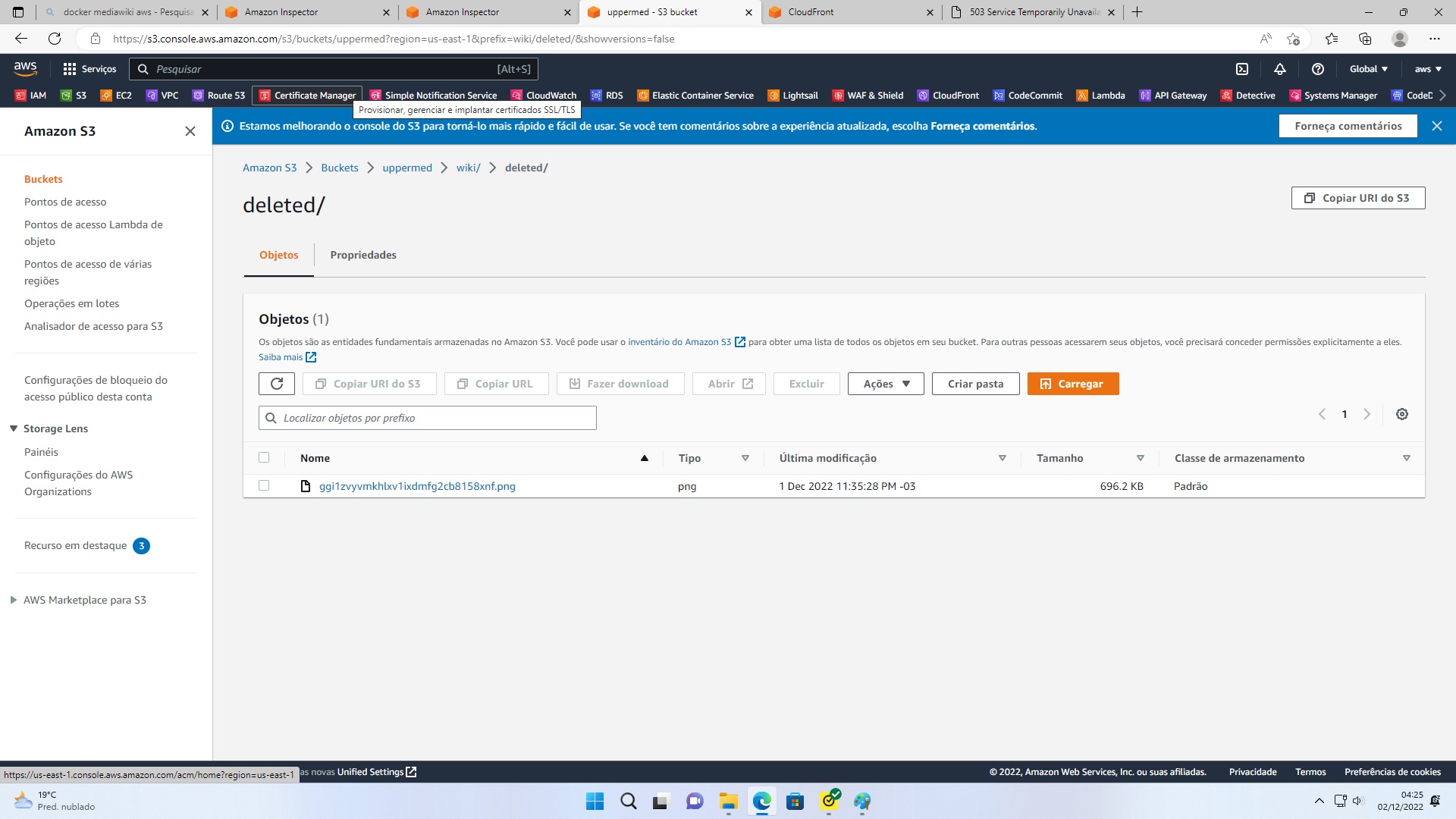
## Ligar e Desligar (Agendamento automático)

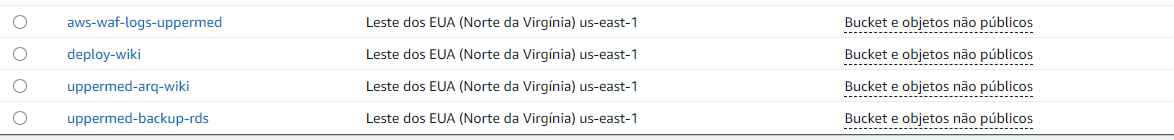
## 

## 

## Amazon Simple Storage Service (Amazon S3)

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade, disponibilidade de dados, segurança e performance líderes do setor. Clientes de todos os portes e setores podem armazenar e proteger qualquer quantidade de dados de praticamente qualquer caso de uso, como data lakes, aplicações nativas da nuvem e aplicações móveis. Com classes de armazenamento econômicas e recursos de gerenciamento fáceis de usar, podemos otimizar custos, organizar dados e configurar controles de acesso ajustados para atender a requisitos específicos de negócios, organizacionais e de conformidade.





## Amazon Elastic Compute Cloud (Amazon EC2)

O Amazon Elastic Compute Cloud (Amazon EC2) oferece a plataforma de computação mais ampla e profunda, com mais de 500 instâncias e opções do processador, armazenamento, redes, sistema operacional e modelo de compra mais recentes para ajudar a atender melhor às necessidades da sua workload. A AWS é o primeiro grande provedor de nuvem a oferecer suporte para processadores Intel, AMD e Arm, a única nuvem com instâncias Mac do EC2 sob demanda e a única nuvem com redes Ethernet de 400 Gbps.

Escolhemos uma instância Linux com o Ubuntu 20.04. O tipo da mesma inicialmente foi uma t2.micro para ficarmos dentro do *freetier*.



Nome da imagem do EC2: t3a.small

Tarefas realizadas na instância:

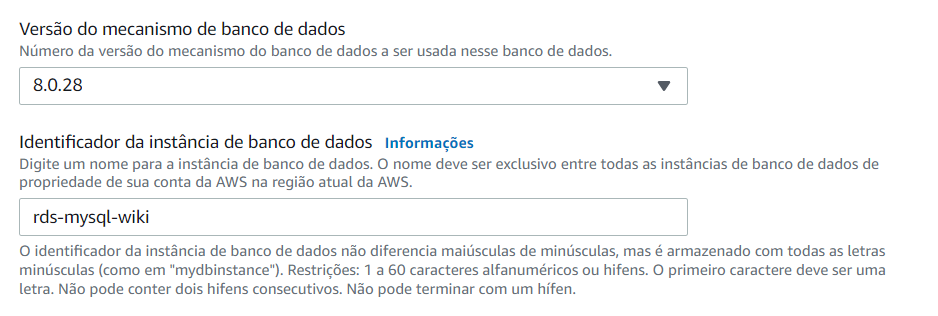
* A instância foi vinculada à VPC
* Escolheu a subnet pública 1
* Vinculou ao security group para permitir:

O storage foi configurado inicialmente com 8GB.

## Amazon Relational Database Service (Amazon RDS)

O Amazon Relational Database Service (Amazon RDS) é um serviço da web que facilita a configuração, a operação e escalabilidade de um banco de dados relacional na nuvem. Ele fornece capacidade econômica e redimensionável para um banco de dados relacional padrão do setor e gerencia tarefas comuns de administração de banco de dados.





## 

## 

## Teste de Estresse nas instâncias

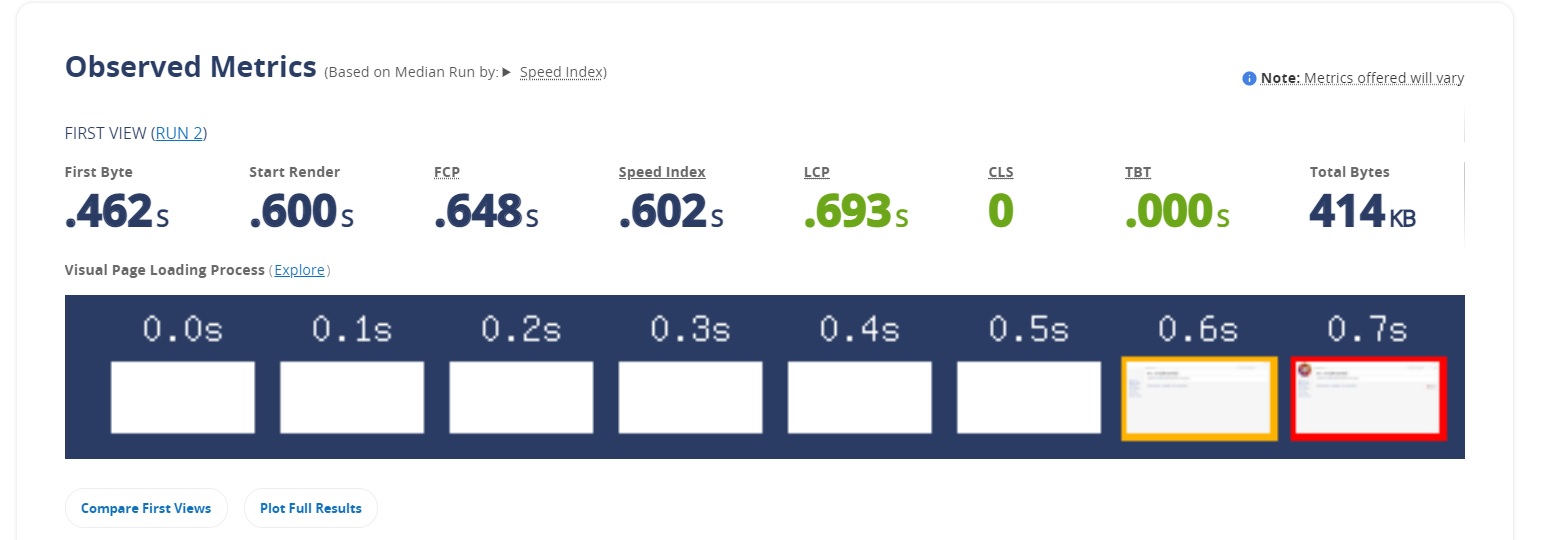
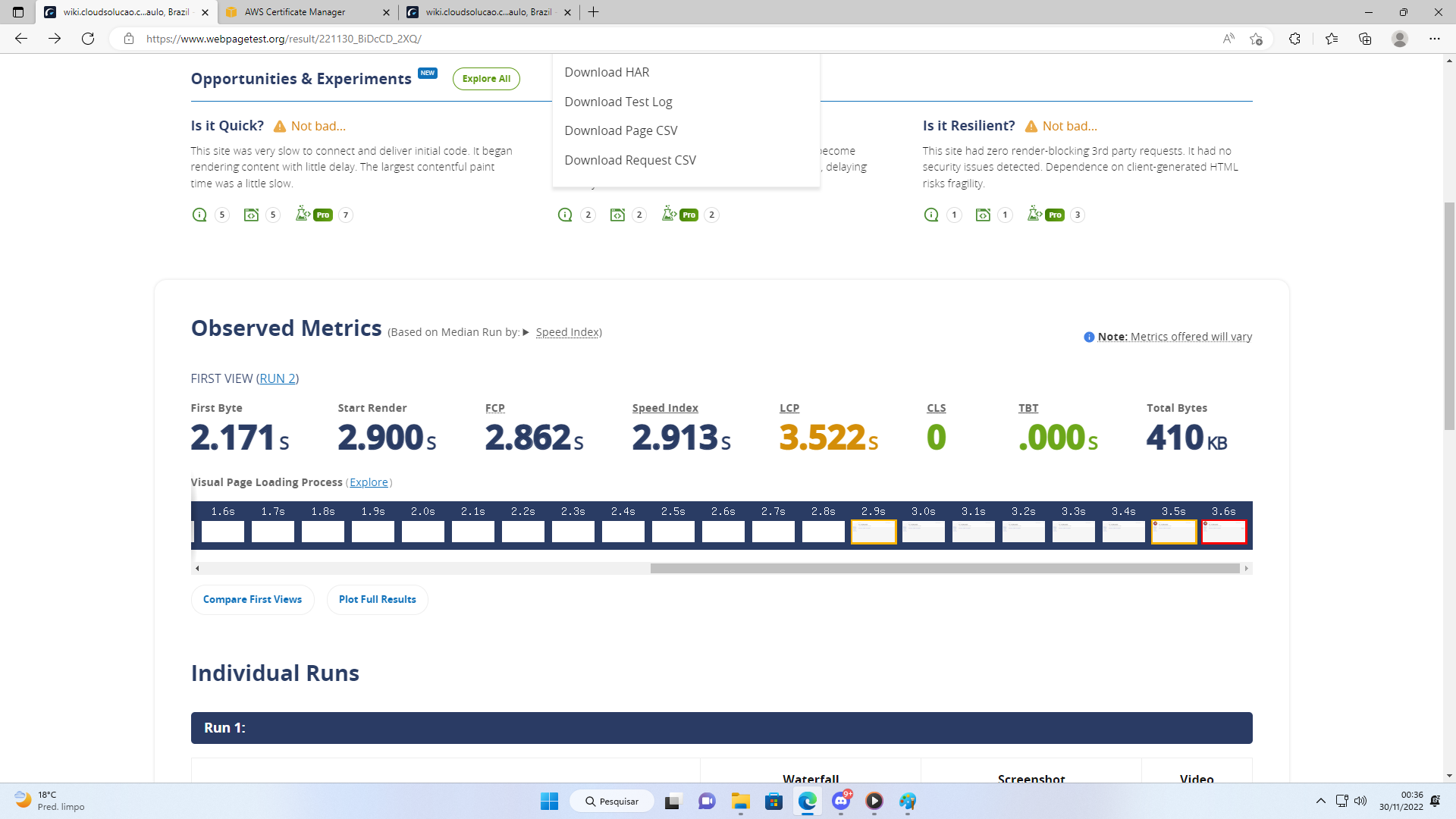
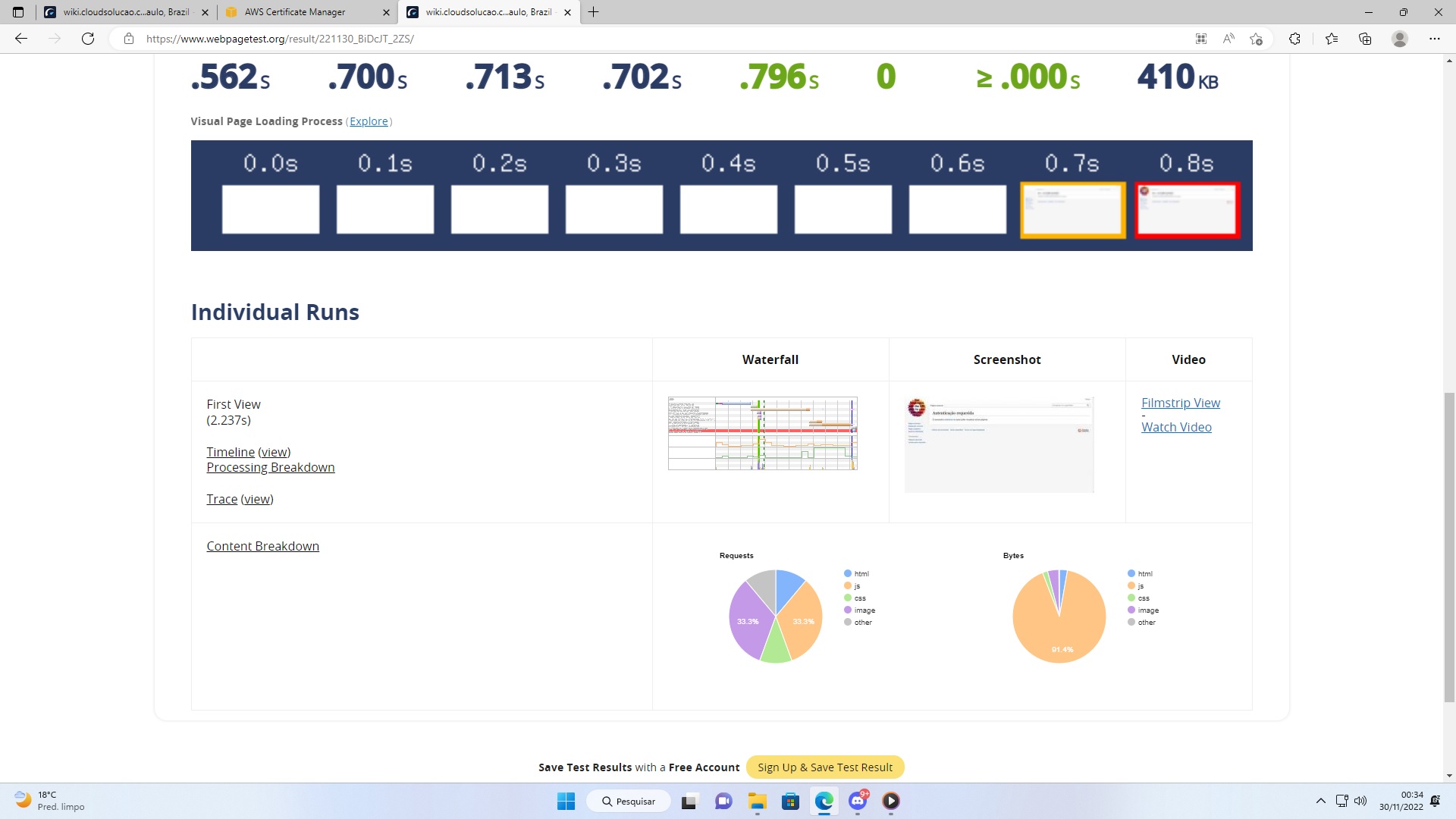
Método 1: Por código

Executamos na instância o seguinte comando:

while 2>1; do cd ~ ; done

Este teste é realizado para sobrecarregar a CPU forçando a atuação do auto scaling fazendo com que novas instâncias sejam criadas.

Método 2: Teste de latência entre as regiões de SP e Virgínia



# Proposta Comercial

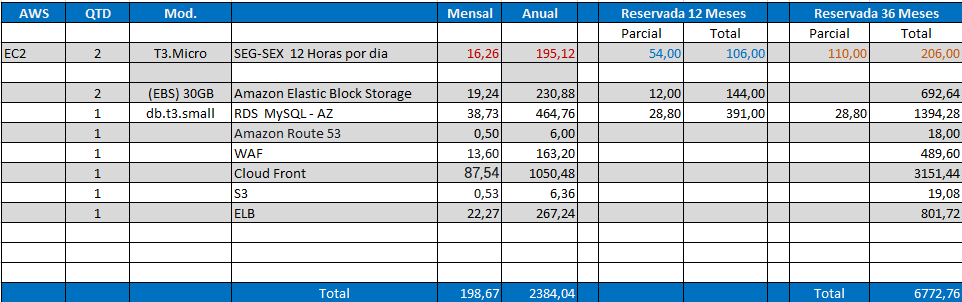
**Comparativo Financeiro Anual - Nuvem x Local**

Abaixo demonstramos o custo, mensal, anual e por reserva de instâncias por período, do cliente ao manter o sistema localmente, e a vantagem financeira em migrar para a nuvem da AWS.

| **Projeto + Plano de Gestão** | | |
| --- | --- | --- |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
| Para melhorar ainda mais  Projeto + Gestão 12x R$ 1.924,60 | |  |
|  |  |  |
|  |  |  |

**Serviços AWS**

Também apresentamos um detalhamento dos custos com os serviços da AWS na tabela abaixo. A conta na AWS será criada sob responsabilidade total do cliente, ou seja, os custos poderão ser gerenciados pela Cloud Solução, mas os valores dos serviços são da UpperMed. Poderemos ser consultado caso queiram antecipar o pagamento de máquinas virtuais (EC2).



Obs.: Os valores acima foram calculados com base no dólar a R$ 5,21