**Six-Cloud Solutions**

****

**Documentação Técnica**

**Oficina 20**

**GLPI**

02/05/2024

A/C Sr. Leandro Porciuncula.

REF: Migrar aplicação GLPI

Prezado Leandro,

Conforme solicitação, segue abaixo a proposta para migração da aplicação GLPI para a AWS, atendendo a Upper Trends, empresa que desenvolve pigmentos para plásticos, que atualmente está enfrentando problemas de lentidão no acesso ao sistema de gerenciamento de chamados de helpdesk – GLPI.

A Six-Cloud Solutions agradece a confiança e a oportunidade de participação no presente projeto, reafirmamos nosso compromisso com a utilização das melhores práticas em conformidade aos pilares do Well Architect framework da AWS, em implantação dos recursos da AWS e nas soluções para nossos clientes, baseada nos mais altos padrões de qualidade, inovação e transparência.

Colocamo-nos à disposição para quaisquer esclarecimentos que forem necessários.

Atenciosamente,

| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Gerente de Contas  Telefone: +55 11 91888-0022  gc@sixcloudsolutions.com.br | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Pré-vendas / Pós-vendas  Telefone: +55 11 92888-0033  cm@sixcloudsolutions.com.br |
| --- | --- |
|  | |

**Identificação do Documento**

| **Documento** | Serviço de implantação aplicação na AWS |
| --- | --- |
| **Fornecedor** | Six-Cloud Solutions |
| **Gerente** | Leandro Porciuncula |
| **Product Owner - PO** | Leandro Porciuncula |
| **Objetivo** | O documento descreve as informações técnicas relacionadas à migração da aplicação GLPI utilizada pela Upper Trends, para a estrutura em nuvem AWS, onde aplicação tenha melhor tempo de resposta, alta disponibilidade, escalabilidade ao menor custo possível, cumprindo os pilares do Well Architect framework da AWS. |
| **Criado por** | Victor Cleber |
| **Revisado Por** | Victor Cleber |

**Controle de Versão do Documento**

| **Revisão** | **Data** | **Colaboradore** | **Breve descrição** |
| --- | --- | --- | --- |
| 1.0 | 05/09/2024 | Victor Cleber | Criação do documento |
| 2.0 | 15/09/2024 | Victor Cleber | Revisão do documento |
| 3.0 | 24/09/2024 | Six-Cloud Solutions | Versão Final. |

Sumário

[1 - PROPRIEDADE E CONFIDENCIALIDADE 1](#_heading=h.gjdgxs)

[2 – INSTITUCIONAL 4](#_heading=h.1pxezwc)

[3 - RESUMO EXECUTIVO 8](#_heading=h.1ksv4uv)

[4 - ARQUITETURA DA SOLUÇÃO 10](#_heading=h.2jxsxqh)

[4.1 - Diagrama dos Serviços 10](#_heading=h.1y810tw)

[4.2 - Detalhamento dos Serviços a serem usados 10](#_heading=h.4i7ojhp)

[5 - IMPLANTAÇÃO 21](#_heading=h.2xcytpi)

[6 - FUNCIONAMENTO SERVIÇOS PRINCIPAIS 33](#_heading=h.1ci93xb)

[7 - CRONOGRAMA GERAL 41](#_heading=h.3whwml4)

[8 - TESTES DE CARGA E DESEMPENHO 42](#_heading=h.2bn6wsx)

[9 - CONSIDERAÇÕES FINAIS 46](#_heading=h.qsh70q)

[10 - INTEGRANTES DO GRUPO 2 48](#_heading=h.3as4poj)

# 1 - PROPRIEDADE E CONFIDENCIALIDADE

**Restrições de Uso e Divulgação da Proposta**

Todas as informações contidas nessa proposta são confidenciais e protegidas nos termos da lei, sejam elas de caráter técnico, financeiro ou comercial. As informações apresentadas aos responsáveis da Upper Trends não podem ser usadas ou divulgadas para propósitos que fogem ao objetivo definido nesta documentação e seu uso sem prévia autorização da Six-Cloud Solutions incorrerá nas sanções previstas em lei.

Da mesma forma, a Six-*Cloud Solutions* compromete-se a não divulgar ou fornecer dados e informações constantes desta documentação à terceiros, seja por qualquer meio, digital ou analógico, a menos que seja do interesse das partes e expressamente autorizado pela Upper Trends, reforçando nosso compromisso com a absoluta confidencialidade em relação às atividades desenvolvidas.

A Six-*Cloud Solutions* protege os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo estando 100% aderente à Lei Geral de Proteção de Dados Pessoais (LGPD).

Esta proposta foi registrada sob o número **PTC-00311p27/2024** e uma cópia idêntica foi depositada em nosso Departamento de Compliance. Qualquer dúvida sobre a conduta de nossos profissionais deve ser reportada para os nossos canais de compliance:

* [www.sixcloudsolutions.com.br/compliance](http://www.sixcloudsolutions.com.br/compliance)
* [compliance@](about:blank)sixcloudsolutions.com.br

A validade da presente proposta é de 15 (vinte dias), contados após a data do seu recebimento.

**Termo de confidencialidade**

Este Termo de Confidencialidade é celebrado entre a Empresa Upper Trends doravante denominada "**Contratante**", e a *Six-Cloud Solutions* doravante denominada "**Contratada**".

**Entendendo Informações Confidenciais**

Informações Confidenciais abrangem qualquer dado ou informação compartilhada por uma parte à outra, independentemente do meio (oral, escrito, digital, etc.), que é explicitamente confidencial ou que, dadas as circunstâncias de sua divulgação, deveria naturalmente ser tratado como tal. Isso pode incluir uma ampla gama de informações, como segredos industriais, inovações patenteadas, dados financeiros, estratégias de negócios, detalhes sobre clientes, dados de produtos, planos de projetos, propostas comerciais, conhecimento técnico especializado e outras informações de natureza sensível.

**Responsabilidades da Parte Contratada**

A parte **contratada** se compromete a preservar o sigilo de todas as informações confidenciais recebidas da Upper Trends, tratando-as com o mais alto grau de discrição.

Ela deve adotar todas as precauções necessárias para assegurar que pessoas afiliadas, empregados, representantes, terceirizados, consultores ou qualquer indivíduo que tenha acesso a tais informações sigam rigorosamente os termos de confidencialidade deste acordo.

Além disso, a parte **contratada** se compromete a utilizar as informações confidenciais unicamente com o propósito de cumprir os objetivos estabelecidos no contrato firmado entre as partes envolvidas, abstendo-se de qualquer uso alternativo sem a explícita autorização por escrito da parte contratante.

**Exceções às Regras de Confidencialidade**

Não se espera que a parte **contratada** mantenha em sigilo aquelas informações que:

Já sejam de domínio público quando divulgadas, ou venham a ser sem que haja infração deste acordo;

Já estivessem sob posse da parte contratada antes da divulgação, sem estar atreladas a quaisquer compromissos de manter o sigilo;

Sejam adquiridas de maneira legítima de terceiros que não estejam sob qualquer compromisso de confidencialidade com as partes envolvidas neste acordo;

Sejam criadas de forma independente pela parte contratada, sem qualquer dependência ou referência às informações consideradas confidenciais aqui;

Tenham que ser reveladas por exigência legal, determinação judicial ou por imposição de órgãos reguladores.

**Devolução ou Destruição de Informações Confidenciais**

Após o encerramento ou a rescisão do contrato entre as partes, ou quando solicitado pela **Contratante**, a parte contratada se compromete a entregar de volta todas as Informações Confidenciais recebidas, incluindo quaisquer cópias, duplicatas ou registros relacionados. Como alternativa, a parte contratada pode optar por eliminar de forma segura todas as Informações Confidenciais, contanto que forneça à **Contratante** uma confirmação escrita dessa destruição.

# 

# 3 - RESUMO EXECUTIVO

**Problemas Levantados Junto ao Cliente**

A Upper Trends, trabalha com uma aplicação atualmente na AWS disponibilizada em uma Instância EC2, a qual foi desenvolvida em DotNet core 7, utilizando banco de dados SQLServer, também fazem uso do S3.

Está startup recebeu um aporte para escalar seu negócio, em conformidade ao contrato com os investidores necessita alcançar a marca de dois milhões de usuários em um ano, tendo como estimativa de um milhão de acessos por dia, tendo como previsão de início em duas semanas suas campanhas de marketing.

Diante deste cenário a Upper Trends tem como exigência, através dos investidores, que aplicação seja rápida e não tenha quedas quando iniciarem os primeiros acessos.

Os maiores problemas encontrados pela equipe técnica da Upper Trends foram: lentidão da aplicação e não tolerância a falhas, tendo em vista que a aplicação está hospedada em somente um servidor.

**Escopo da Proposta de Solução**

A Six-Cloud Solutions é o parceiro ideal, com “know how” para endereçar todos os desafios da Upper Trends.

Esta proposta contempla informações técnicas sobre a nova arquitetura que será desenvolvida e implantada em nuvem AWS, contemplando resiliência, segurança, alta disponibilidade e escalabilidade, ao menor custo possível, seguindo as recomendações dos pilares do Well Architect framework da AWS.

Podemos mencionar brevemente alguns recursos utilizados nesta nova arquitetura, como disponibilidade em mais de uma região, por meio de balanceador de carga e replicação do banco de dados RDS em multi AZ e auto scaling da aplicação, em conformidade com o aumento da demanda dos recursos utilizados, e da mesma forma com a redução dos recursos adicionais, quando estes não forem mais necessários.

Contempla também a esteira de CI/CD para a automatização do deploy de novas versões da sua aplicação, e recursos de segurança adotados no desenvolvimento da aplicação, na arquitetura da solução e conta AWS do cliente, conforme será descrito no decorrer desse material.

Descrição sucinta das melhoria identificadas

Segurança > usuário e senha expostos

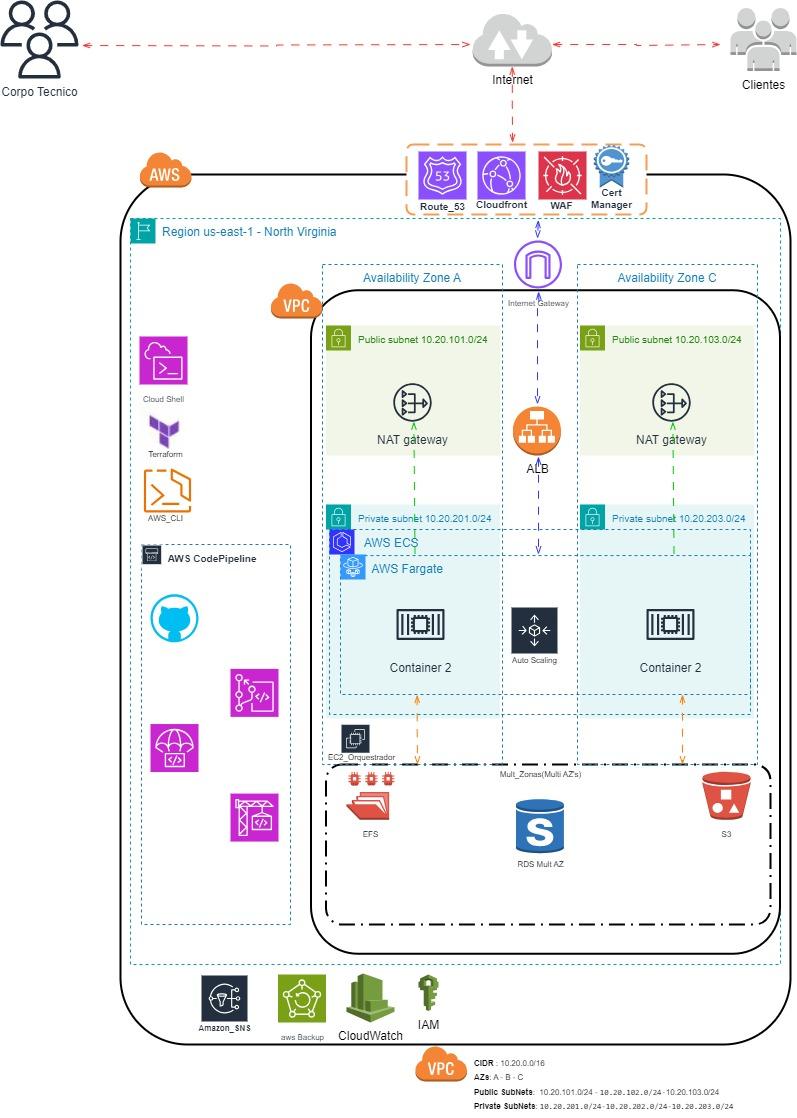
Contas AWS > Segregação de contas

Framework > Upgrade de Framework de desenvolvimento

Automação > Git hub Actions + Terraform

# 4 - ARQUITETURA DA SOLUÇÃO

## 4.1 - Diagrama dos Serviços



## 4.2 - Detalhamento dos Serviços a serem usados

Na tabela que segue temos uma breve descrição dos componentes e serviços propostos para o funcionamento da infraestrutura.

|  | **AWS Route 53**  Serviço de Sistema de Nomes de Domínio (DNS). Fornece serviços de registro de domínio, gerenciamento de DNS e roteamento de tráfego na internet, 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. O gerenciamento de DNS é essencial para a integração com outros serviços da AWS, oferecendo a possibilidade de roteamento inteligente e de alta disponibilidade. |
| --- | --- |
|  | **AWS WAF - Web Application Firewall**  O AWS WAF ajuda a proteger contra *bots* e *exploits* comuns na Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos em excesso. Serviço de segurança que ajuda a proteger aplicativos web contra diferentes tipos de ataques maliciosos. Age como uma camada de segurança entre o tráfego da web e os aplicativos, permitindo o controle e monitoramento das solicitações HTTP e HTTPS que chegam aos seus aplicativos. O serviço permite a criação de regras personalizadas que filtram o tráfego malicioso, o que é particularmente importante para a Cloud Treinamentos. Proteger sua aplicação Web contra ataques comuns, como *SQL Injection* e *Cross-Site Scripting* (XSS), é crucial. |
|  | **Amazon CloudFront**  Serviço de CDN (Content Delivery Network). O CloudFront distribui o conteúdo por meio de uma rede global de datacenters denominados locais da borda. Criado para alta performance, agiliza a entrega de conteúdo pela web, aproximando o cliente final melhorando a comunicação entre as aplicações e seus dados, aproximando os pontos de distribuição espalhados pelo mundo. Ele entrega dados, vídeos, aplicações e APIs com velocidades de transferência elevadas e baixa latência. Melhora a experiência do usuário, reduz a carga nos seus servidores de origem e aumenta a segurança do seu conteúdo. Ele é uma parte fundamental na arquitetura de muitas aplicações web modernas. |
|  | **AWS Virtual Private Cloud - VPC**  O AWS VPC possibilita a criação de uma rede virtual segregada na nuvem, personalizando o ambiente de rede. Oferece controle total sobre a configuração da rede, incluindo a criação de sub-redes, definição de regras de firewall através de Security Groups e NACLs, e estabelecimento de rotas e conexões de rede. Por meio da VPC adicionamos e conectamos recursos como AWS EC2 e RDS. A segregação do ambiente permite distribuir os recursos a partir de uma ou mais regiões e diferentes zonas de disponibilidade garantindo segurança e flexibilidade na arquitetura de rede  Alguns serviços associados a VPC serão utilizados: |
|  | **INTERNET GATEWAY**  INTERNET GATEWAY - O Gateway de Internet da AWS é um serviço de rede da Amazon Web Services (AWS) que permite a comunicação bidirecional entre a Internet pública e a sua Virtual Private Cloud (VPC). Em outras palavras, o Internet Gateway é o ponto de entrada e saída para o tráfego de rede entre a Internet e os recursos da sua VPC.  Quando uma sub-rede estiver associada a uma tabela de rotas que tenha uma rota para um gateway da Internet, ela será conhecida como sub-rede pública. Quando uma sub-rede estiver associada a uma tabela de rotas que não possui uma rota para um gateway de Internet, ela será conhecida como sub-rede privada. |
| Application Load Balancer resource icon for the Elastic Load Balancing service. | **Application Load Balancer**  Serviço destinado a distribuição e controle de tráfego entre as EC2 que permitem a infraestrutura crescer quando for necessário, devido ao aumento de fluxo de usuários, e diminuir quando os recursos não estão sendo utilizados, para otimização de custos com a infraestrutura. Estes serviços atuam em conjunto com o balanceador de carga (Load Balancer) distribuindo as solicitações homogeneizando as chamadas entre as instâncias disponíveis, e o Autoscaling lança novas instâncias integrando o poder computacional existente quando a demanda por recursos for exigida e desliga instâncias quando elas não estão sendo solicitadas. |
| Amazon Elastic Container Service (Amazon ECS) service icon. | **Amazon Elastic Container Service (ECS) Fargate**  O Amazon Elastic Container Service (ECS) é um serviço totalmente gerenciado de orquestração de contêineres que ajuda a implantar, gerenciar e escalar aplicações em contêineres de maneira mais eficiente. Ele se integra totalmente ao ambiente da AWS para fornecer uma solução fácil de usar para executar workloads de contêineres na nuvem e on-premises com atributos de segurança avançados. |
|  | **Amazon Relational Database Service - RDS**  A Amazon Relational Database Service (Amazon RDS) é uma coleção de serviços gerenciados que facilita a configuração, operação e escalabilidade de bancos de dados na nuvem. A funcionalidade de Multi-AZ (Multi Zona de Disponibilidade) cria automaticamente uma instância de banco de dados (BD) primária e replica os dados de forma síncrona para uma instância em uma AZ diferente, permanecendo na mesma região da outra instância. Quando detecta uma falha, o Amazon RDS executa automaticamente o failover para uma instância secundária sem nenhuma intervenção manual. Este serviço é necessário para armazenamento dos dados persistentes da aplicação e simplifica a administração do banco de dados, oferecendo backups automatizados, patching e escalabilidade.  O Amazon RDS para SQL Server facilita a configuração, a operação e a escalabilidade de implantações do SQL Server na nuvem. Com o Amazon RDS, você pode implantar várias edições do SQL Server (2014, 2016, 2017, 2019 e 2022), incluindo Express, Web, Standard e Enterprise, em poucos minutos, com economia e capacidade computacional redimensionável. |
|  | **Amazon Simple Storage Service - S3**  Serviço de armazenamento de objetos para armazenamento de mídias (fotos e vídeos). Usar o S3 para armazenar mídia (fotos, vídeos) não só otimiza os custos de armazenamento, mas também se integra bem com o CloudFront para entrega de conteúdo. |
|  | **SECURITY GROUPS**  Um security group atua como firewall virtual para as instâncias do EC2 visando controlar o tráfego de entrada e de saída. As regras de entrada controlam o tráfego de entrada para a instância e as regras de saída controlam o tráfego de saída da instância. |
|  | **AWS Identity and Access Management - IAM**  O AWS IAM é um serviço essencial para qualquer projeto implementado na Amazon Web Services - AWS. O serviço desempenha um papel crucial na gestão de acesso seguro a todos os recursos da AWS, permitindo o controle de quem está autenticado (logado) e autorizado (tem permissões) para usar recursos. |
|  | **AWS Certificate Manager**  O AWS Certificate Manager é um serviço que permite provisionar, gerenciar e implantar facilmente certificados Secure Sockets Layer/Transport Layer Security (SSL/TLS) para uso com os serviços da AWS. Os certificados SSL/TLS são usados para proteger comunicações de rede e estabelecer a identidade de sites na Internet e de recursos em redes privadas. O AWS Certificate Manager elimina processos manuais demorados como compra, upload e renovação de certificados SSL/TLS. O serviço irá desempenhar um papel crítico em garantir a segurança da comunicação entre os usuários finais e a aplicação Web, bem como entre os diversos componentes da infraestrutura na nuvem. |
|  | **AWS Systems Manager**  É o hub de operações para as aplicações e os recursos da AWS e uma solução segura de gerenciamento unificado da infraestrutura da AWS, automatizando tarefas, gerenciando patches e aplicando configurações, para simplificar o gerenciamento, aumentar a confiabilidade e reduzir custos. É dividido em quatro grupos de recursos principais, e outros recursos que são continuamente disponibilizados. |
| Parameter Store resource icon for the AWS Systems Manager service. | **Parameter Store**  O AWS Systems Manager oferece um armazenamento centralizado para gerenciar os dados de configuração em texto simples, como strings de bancos de dados, ou secretos, como senhas. Assim, pode-se separar dados secretos e de configuração do código. Os parâmetros podem ser marcados com tags e organizados em hierarquias para facilitar seu gerenciamento. |
|  | **AWS CodePipeline**  Entrega contínua que automatiza o processo de desenvolvimento, teste e implantação de código, para aumentar a velocidade e a confiabilidade da entrega de software, além de reduzir o risco de erros e falhas. |
| AWS CodeBuild service icon. | **AWS CodeBuild**  O AWS CodeBuild é um serviço de integração contínua totalmente gerenciado que compila código-fonte, executa testes e produz pacotes de software prontos para implantação. |
|  | **AWS CodeDeploy**  Serviço de implantação automatizada de aplicações para instâncias EC2 e grupos de Auto Scaling, simplificando o processo de implantação, monitorando-o e fornecendo relatórios detalhados |
| Endpoints resource icon for the Amazon VPC service. | **VPC ENDPOINTS**  VPC ENDPOINTS- “Ponto de Extremidade de VPC” é um serviço da Amazon Web Services (AWS) que permite que os recursos dentro de uma Virtual Private Cloud (VPC) acessem de forma privada e segura os serviços da AWS sem a necessidade de roteamento de tráfego pela Internet pública**.**  Existem vários tipos de VPC *endpoints*:  a) *interface endpoints*  Esses *endpoints* são para serviços da AWS hospedados em uma região específica. Eles são representados por interfaces de rede elásticas em uma sub-rede específica da VPC.  b) *GatewayLoadBalancer*  Crie um endpoint do Gateway Load Balancer para enviar tráfego a uma frota de dispositivos virtuais usando endereços IP privados. Encaminhe o tráfego da VPC ao endpoint do Gateway Load Balancer usando tabelas de rotas. O Gateway Load Balancer distribui o tráfego aos dispositivos virtuais e pode ser escalado conforme a demanda.  c) *gateway endpoints*:  Esses *endpoints* são para serviços da AWS que usam Amazon S3 e DynamoDB. Eles são associados diretamente à VPC e permitem que os recursos dentro da VPC acessem esses serviços sem usar a Internet pública. |
| VPN connection resource icon for the Amazon VPC service. | **VPN connection**  Você pode conectar sua VPC a redes remotas e usuários usando as seguintes opções de conectividade VPN  AWS Client VPN é um serviço client-based VPN que permite acessar com segurança seus recursos da AWS ou sua rede local. Com o AWS Client VPN, você configura um endpoint ao qual seus usuários podem se conectar para estabelecer uma sessão VPN TLS segura. Isso permite que os clientes acessem recursos na AWS ou no local a partir de qualquer local usando um cliente VPN baseado em OpenVPN. |
|  | **Virtual Private Gateway**  Você pode usar um gateway do AWS Direct Connect para conectar sua conexão do AWS Direct Connect por meio de uma interface virtual privada a uma ou mais VPCs em qualquer conta localizada na mesma região ou em regiões diferentes. Você associa um gateway Direct Connect ao gateway privado virtual da VPC. Em seguida, você cria uma interface virtual privada para sua conexão do AWS Direct Connect com o gateway Direct Connect. Você pode anexar diversas interfaces virtuais privadas ao gateway Direct Connect. |
| AWS Fargate service icon. | **AWS Fargate**  O AWS Fargate é um mecanismo de computação com tecnologia serverless que permite ao desenvolvedor se concentrar no desenvolvimento de aplicações sem a necessidade de gerenciar servidores. Mover tarefas como gerenciamento de servidores, alocação de recursos e escalabilidade para a AWS não só melhora sua postura operacional, mas também acelera o processo de passar da ideia à produção na nuvem e reduz o custo total de propriedade.  O AWS Fargate gerencia necessidades de capacidade, atualizações de sistema operacional (SO), requisitos de conformidade, resiliência e muito mais. |
| Amazon Elastic Container Registry (Amazon ECR) Service icon. | **Amazon Elastic Container Registry (ECR)**  O Amazon Elastic Container Registry (Amazon ECR) é um registro de contêiner totalmente gerenciado que oferece hospedagem de alta performance para que você possa implantar imagens e artefatos de aplicações de forma confiável em qualquer lugar.  Envie imagens de contêiner ao Amazon ECR sem instalar ou escalar a infraestrutura e extraia imagens usando qualquer ferramenta de gerenciamento. |
| Amazon Simple Notification Service (Amazon SNS) service icon. | **Amazon SNS (Simple Notification Service)**  O Amazon Simple Notification Service (Amazon SNS) é um serviço de mensagens totalmente gerenciado para a comunicação de aplicação para aplicação (A2A) e de aplicação para pessoa (A2P). A funcionalidade pub/sub de A2A fornece tópicos para sistemas de mensagens de alta taxa de transferência baseados em push e de muitos para muitos entre sistemas distribuídos, micros serviços e aplicações sem servidor orientadas por eventos. Usando tópicos do Amazon SNS, seus sistemas editores podem repassar mensagens para um grande número de sistemas de assinantes, incluindo filas do Amazon SQS, funções do AWS Lambda e endpoints HTTPS e o Amazon Kinesis Data Firehose para processamento paralelo. A funcionalidade A2P permite enviar mensagens para usuários em grande escala por SMS, push de dispositivos móveis e e-mail.  Notificação escalável e flexível entre aplicativos, serviços e dispositivos, com alta escalabilidade, confiabilidade e integração com outros serviços da AWS |
|  | **Cloud Trail**  Auditoria e rastreamento de todas as atividades da conta da AWS, para melhor segurança, conformidade e investigação de problemas. |
|  | **AWS CloudWatch**  O AWS CloudWatch é um serviço de monitoramento e observabilidade oferecido pela AWS que fornece dados e insights acionáveis para monitorar suas aplicações, responder a mudanças no sistema e otimizar a eficiência de recursos e aplicações. Ele é projetado para que a equipe de manutenção da infraestrutura possa coletar e rastrear métricas, coletar e monitorar arquivos de log, definir alarmes e visualizar dados em painéis para obter uma visão unificada da saúde operacional da infraestrutura na AWS. Além de monitorar a infraestrutura será possível fornecer dados sobre o tráfego da aplicação Web, por meio da análise das solicitações HTTP/HTTPS recebidas é possível entender padrões de tráfego, picos de visitantes e possíveis ataques DDoS. É possível ainda definir alarmes que disparam e-mails para os gestores informando qualquer anomalia na infraestrutura e tráfego da aplicação. |
|  | **AWS Billing Conductor**  Monitore suas cobranças estimadas da AWS usando o Amazon CloudWatch. Quando o monitoramento de cobranças estimadas para sua conta da AWS está habilitado, as cobranças estimadas são calculadas e enviadas diversas vezes ao dia para o CloudWatch como dados métricos.  Esses dados incluem as cobranças estimadas para cada serviço da AWS em utilização, além do total geral estimado das cobranças da AWS.  O alarme é acionado quando o faturamento da sua conta excede o limite especificado. Ele é acionado somente quando o faturamento atual excede o limite. Ele não usa projeções com base no seu uso até o momento no mês. |
|  | **AWS Backup**  O AWS Backup é um serviço centralizado de backup que oferece uma solução simplificada e automatizada para proteger os dados da Cloud Treinamentos, incluímos o serviço para proteger os dados do banco no AWS Relational Database Service. o AWS Backup desempenha um papel vital na estratégia de continuidade de negócios e recuperação de desastres. |

## 

# 5 - IMPLANTAÇÃO

**Pesquisa de campo e levantamento dos requisitos**

O objetivo desta etapa é levantar os requisitos específicos de configuração para a implantação da aplicação, sejam eles uso de templates ou plugins específicos, informações sobre banco de dados em utilização e quaisquer outras informações relevantes que permitam estabelecer ajustes finos no ambiente, ou seja, na nova infraestrutura e serviços da AWS que compõem essa proposta.

Nesta etapa, será necessário o contato direto com o time de TI e editores da Upper Trends para melhor entender a operação e configuração atual da aplicação atual e seu banco de dados. A ideia é que o time da Upper Trends possa trabalhar em conjunto com os analistas e técnicos da Six-Cloud Solutions trocando informações e definindo a estratégia da nova infraestrutura que ocorrerá na fase seguinte.

As principais tarefas desta etapa são:

* Refinar detalhes da plataforma e objetos para incorporar nos requisitos técnicos do projeto;
* Determinar método de replicação de dados e janela para cutover;
* Confirmar os serviços da AWS necessários para o projeto;
* Designar a equipe de desenvolvimento e suas responsabilidades;
* Revisar o documento de arquitetura apresentado detalhado quais necessidades de mudança atualizando o diagrama dos serviços.

**Setup do ambiente e da aplicação**

Nesta etapa será iniciada a configuração do ambiente. O primeiro passo será analisar a atual conta da Upper Trends na AWS, adequando os níveis de acesso definindo nome e os dados de acesso do usuário raiz ou root. O usuário raiz será proprietário da conta e tem acesso irrestrito a todos os recursos na conta AWS, sendo o único usuário com permissão para excluir a conta.

Seguindo as boas práticas, o usuário raiz deve ser utilizado apenas para questões de configuração da conta e controle de faturamento na AWS. Desta maneira outros usuários com permissões específicas serão criados, de acordo com as necessidades levantadas.

As principais tarefas a partir da criação da conta e usuário root são:

* Configurar a conta da AWS e definir políticas de acesso e permissões. Definir região e quantidade de zonas de disponibilidade
* Definir escopo de rede e políticas de segurança.
* Criação de recursos de rede, sub-redes, tabelas de rotas
* Criação de containers/Fargate
* Criação de Banco de Dados Multi A/Z
* Implementar a aplicação através do código disponibilizado pela Upper Trends;
* Criar imagem AMI da aplicação;
* Implementar a plataforma em um ambiente produtivo.
* Implementar sistema de armazenamento de objeto S3;
* Implementação de estrutura de alta disponibilidade, como ELB, Auto Scaling, Cloud Front
* Criação esteira CI/CD para deploy das atualizações da aplicação conforme novas versões do código via AWS Pipeline e AWS Code Deploy;
* Integração repositório Git externo com trigger para iniciar a esteira buscando última versão do código conforme nova versão no repositório (push);
* Configuração tópico SNS para envio email para comunicação/aprovação deploy aplicação.

Abaixo segue o detalhamento de configurações previamente definidas para o correto setup do ambiente.

**Virtual Private Cloud - VPC**

Uma rede virtual na cloud AWS

| **Nome:** vpc\_uppertrends |
| --- |
| **Região:** Leste dos EUA (Norte da Virgínia)  **ID região:** us-east-1  **CIDR IPv4:** 10.0.0.0/16 |

**Configuração de Sub-redes - Subnets**

Uso de doze sub-redes, sendo duas privadas e duas públicas distribuídas nas zonas de disponibilidade atuais da região: Leste dos EUA (Norte da Virgínia) - us-east-1

| **Nome:** Subnet-pub01-uppertrends  **CIDR IPv4:** 10.0.16.0/20  **(AZ):** us-east-1a | **Nome:** Subnet-priv01-uppertrends  **CIDR IPv4:** 10.0.144.0/20  **(AZ):** us-east-1a |
| --- | --- |
| **Nome:** Subnet-pub02-uppertrends  **CIDR IPv4:** 10.0.0.0/0  **(AZ):** us-east-1b | **Nome:** Subnet-priv02-uppertrends  **CIDR IPv4:** 10.0.128.0/20  **(AZ):** us-east-1b |

**Internet Gateway**

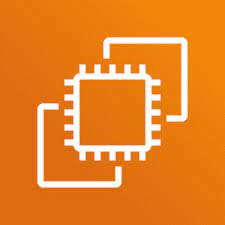
Uso de um gatewayde internet nomeado como**:** igw-uppertrends

**Router Tables:**

| **Tabelas de rotas nome:** rt\_pub\_uppertrends |
| --- |
| **Associações de Sub-rede:**  Subnet-pub01-uppertrends  Subnet-pub02-uppertrends |
| **Rotas:**  **Destino:** 10.0.0.0/16 → **Alvo:** local  **Destino:** 0.0.0.0/0 → **Alvo:** igw-uppertrends |

Duas tabelas de rotas

| **Tabelas de rotas nome:** rt\_priv\_uppertrends |
| --- |
| **Associações de Sub-rede**  Subnet-priv01-uppertrends  Subnet-priv02-uppertrends |
| **Rotas:**  **Destino:** 10.0.0.0/16 → **Alvo:** local |

**EC2 Instance Connect Endpoint:**

Somente um Endpoint, para acesso aos usuários do Ti terem acesso as EC2.

| **Nome:** EC2\_Endpoint |
| --- |
| **Grupo de Segurança:** sg\_endpoint |

**VPC Security Groups**

Grupos de segurança para uso específico

| **Nome:** sg\_uppertrends | | | |
| --- | --- | --- | --- |
| **Regras de entrada:** | | | |
| **Tipo** | **Protocolo** | **Porta** | **Origem** |
| HTTPS  HTTP  SSH | TCP  TCP  TCP | 443  80  22 | sg-alb-uppertrends  sg-alb-uppertrends  sg-endpoint |
| **Regras de saída:** | | | |
| Todo o tráfego | Todos | Todas | 0.0.0.0/0 |

| **Nome:** sg\_banco\_rds | | | |
| --- | --- | --- | --- |
| **Regras de entrada:** | | | |
| **Tipo** | **Protocolo** | **Porta** | **Origem** |
| MYSQL/Aurora | TCP | 3306 | sg\_uppertrends |
| **Regras de saída:** | | | |
| Todo o tráfego | Todos | Todas | 0.0.0.0/0 |

| **Nome:** sg\_alb-uppertrends | | | |
| --- | --- | --- | --- |
| **Regras de entrada:** | | | |
| **Tipo** | **Protocolo** | **Porta** | **Origem** |
|  | | | |
| HTTP  HTTPS | TCP  TCP | 80  443 | 0.0.0.0/0  0.0.0.0/0 |
| **Regras de saída:** | | | |
| Todo o tráfego | Todos | Todas | 0.0.0.0/0 |

| **Nome:** sg\_endpoint | | | |
| --- | --- | --- | --- |
| **Regras de entrada:** | | | |
| **Tipo** | **Protocolo** | **Porta** | **Origem** |
| N/D | N/D | N/D | N/D |
| **Regras de saída:** | | | |
| SSH | TCP | 22 | sg\_uppertrends |

**Router 53** 

Um domínio em zona hospedada pública com os devidos registros para acesso da aplicação via registro DNS público. No ambiente de teste foi utilizado o domínio: almasystemscorp.com

**Criação da zona hospedada:**

| **Nome**: oficina17.taskhere.com |
| --- |
| **Tipo:** Pública |

**Registros:**

| **Nome** | **Tipo** | | **Alias** |
| --- | --- | --- | --- |
| uppertrends.almasystemscorp.com | NS | | não |
| **Valor:** ns-1049.awsdns-03.org.  ns-567.awsdns-06.net.  ns-120.awsdns-15.com.  ns-1689.awsdns-19.co.uk. | | | |
| **TTL:**  172800 | | **Política de roteamento:**  Simples | |

**Relational Database Service - RDS**

Banco de dados relacional utilizando mecanismo MySQL

| **Nome do db:** db\_uppertrends |
| --- |
| **Mecanismo:** Microsoft SQL Server 2019  **Versão do Mecanismo:** 15.00.4355.3.v1  **Classe de Instância:** db.t3.small  **Modelo de preço:** OnDemand  **Disponibilidade:** Multi-AZ  **Insights de performance:** 7 dias (nível gratuito)  **Backups automatizados Habilitado:** 2 vezes ao dia |

**Simple Storage Service - S3**

| **Bucket: uppertrends.g2** |
| --- |
| **Região** us-east-1  **Bloquear todo o acesso público** ativado |

**Elastic Load Balance - ELB**

| **Nome** ALB-uppertrends | | |
| --- | --- | --- |
| **Tipo** Application Load Balance  **Esquema** voltado para internet  **Tipo de endereçamento IP** IPv4 | | |
| **VPC:** vpc\_uppertrends  **Grupo de segurança:** sg\_uppertrends  **Sub-redes:**  Subnet-pub01-uppertrends  Subnet-pub02-uppertrends | | |
| **Listeners e roteamento:** | | |
| **protocolo** | **porta** | **Ação padrão** |
| HTTP | 80 | Forward to target group |
| HTTPS | 443 | Forward to target group |
| **DefaultSSL/TLScertificate** \*.taskhere.com  **Security policy ELBSecurityPolicy-TLS13-1-2-2021-06** | | |

**Grupo de destino - Target Group para ELB**

| **Nome** tg-uppertrends |
| --- |
| **Tipo** Instance  **Protocolo: Porta** HTTP: 80  **Versão do protocolo** HTTP1  **Tipo endereçamento IP** IPv4  **Zonas de disponibilidade:** us-east-1a / us-east-1b / us-east-1c / us-east-1d / us-east-1e / us-east-1f |
| **Verificação de Integridade:**  **Protocolo** HTTP  **Path** /  **Porta** de trafego  **Limite integro** 2 êxitos consecutivos de verificação de integridade  **limite não íntegro** 2 falhas consecutivas de verificação de integridade  **Tempo limite** 2 seconds  **intervalo** 5 seconds  **Código de sucesso** 200-301 |
| **Atributos:**  Atraso de cancelamento de registro 60 seconds  **Duração da iniciação lenta** 0 seconds  **Algoritmo do balanceamento de carga** Ida e Volta  **Perdurabilidade** Off  **Balanceamento de carga entre zonas:** Herdar configurações de atributos do balanceador de carga |

**Grupo de Auto Scaling**

| **Nome** as\_uppertrends |
| --- |
| **Capacidade desejada** 2  **Capacidade mínima** 2  **Capacidade máxima** 3 |
| **Tipo de verificação de integridade** EC2,ELB  **Período de tolerância da verificação de integridade:** 120  **Protegido contra a redução da escala na horizontal:** Não  **Políticas de término:** Default  **Aquecimento de instâncias padrão:** 120 segundos |

**Modelo de execução**

| **Nome:** AMI-Uppertrends |
| --- |
| **Tipo de instância** t3a.small  **Versão** 2 |
| **Security Group** sg\_uppertrends  **Subnets:**  Subnet-priv01- uppertrends  Subnet-priv02- uppertrends |
| **Escala automática:**  **Tipo Políticas de escalabilidade** dinâmica  **Métricas:**  **Nome** add\_instance  **Escalabilidade de monitoramento do objetivo** Habilitado  Aplicar Métrica Média de utilização da CPU acima de 70%  **Nome** rmv\_instance  **Escalabilidade de monitoramento do objetivo** Habilitado  Aplicar Métrica Média de utilização da CPU inferior a 30%  **\***Será adicionada ou removida unidades de capacidade conforme necessário em 120 segundos para aquecer antes de incluir na métrica habilitada. |



**Identity and Access Management - IAM**

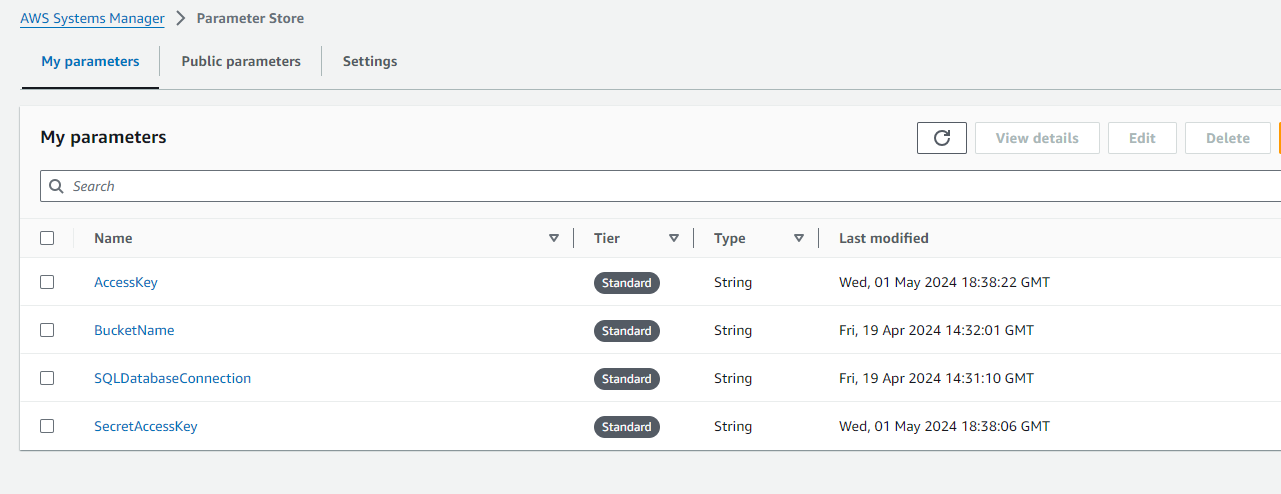
Dois usuários para manutenção da infraestrutura e uso específico de recursos S3

| **Usuário U**pperTrends |
| --- |
| **Acesso ao console:** Habilitado  **Credenciais** Login / Senha, MFA  **Políticas de permissão** AdministratorAccess |
| **Permissões**  {  "Version": "2024-02-06",  "Statement": [  {  "Effect": "Allow",  "Action": "\*",  "Resource": "\*"  }  ]  } |

| **Usuário** s3\_ UpperTrends |
| --- |
| **Acesso ao console:** Desabilitado  **Credenciais** Chave de acesso  **Políticas de permissão** AmazonS3FullAccess |
| **Permissões**  {  "Version": "2024-02-06",  "Statement": [  {  "Effect": "Allow",  "Action": [  "s3:\*",  "s3-object-lambda:\*"  ],  "Resource": "\*"  }  ]  } |

**AWS Systems Management**

**Parameter Store**



# 6 - FUNCIONAMENTO SERVIÇOS PRINCIPAIS

A seguir, serão detalhados o funcionamento e os serviços habilitados para integração e deploy da aplicação na infraestrutura e serviços de segurança para mitigação de ameaças no ambiente.

**AWS Code Pipeline:**

O AWS CodePipeline é um serviço de entrega contínua (CI/CD) totalmente gerenciado que automatiza o processo de liberar com segurança e rapidez do código para produção. Ele elimina o trabalho manual de mover o código entre as etapas de desenvolvimento, teste e implantação, permitindo que você se concentre na criação de software de qualidade.

O AWS CodePipeline oferece uma interface visual para criar pipelines com etapas sequenciais ou paralelas, integrando-se a diversos provedores de código como GitHub, Bitbucket e AWS CodeCommit. Ele permite a compilação e o teste automatizados com AWS CodeBuild, GitHub Actions ou ferramentas personalizadas, além da integração com serviços de teste como AWS CodeDeploy e Lambda. O CodePipeline oferece implantação automatizada em diversos targets como EC2, Lambda, ECS e Elastic Beanstalk, com opções de implantação manual ou automática e controle de aprovação. O serviço também fornece monitoramento completo do pipeline com logs e métricas detalhadas, além de visualização do status do pipeline em tempo real e histórico. Por fim, o CodePipeline garante segurança e conformidade com controle de acesso granular via IAM e políticas personalizadas, além de conformidade com diversos padrões de segurança e auditoria.

**Pipeline da Upper Trends:**

Desenvolvemos esteira CI/CD para automatizar a implementação de novas versões do código da aplicação na infraestrutura da AWS. Através de webhook no repositório do GitHub, conseguimos integrar com o AWS CodePipeline para iniciar o processo de deploy quando um novo push acontecer no repositório do código.

Para controle e governança quanto ao lançamento da nova versão da aplicação para o ambiente de produção, configuramos um tópico SNS que possui uma subscription de email que irá comunicar a área responsável para aprovação do deploy, onde o usuário aprovador terá acesso a pipeline para aprovação do lançamento.

Havendo a aprovação, o AWS CodeDeploy dará início ao deploy da aplicação na infraestrutura, utilizando imagem pré configurada da instância virtual que possui o sistema operacional, aplicação apache e dependências já instaladas, apenas atualizando os arquivos da aplicação no diretório do servidor.

Para garantir disponibilidade do serviço e escalabilidade, a aplicação será implementada em grupo de instâncias distribuídas com recurso de escala horizontal entre zonas de disponibilidade, com balanceador de carga para distribuir o tráfego entre as instâncias. Durante o deploy, será utilizando implantação azul/verde, onde o tráfego de produção continuará na implementação atual até que as novas instâncias com a nova versão da aplicação estejam totalmente implementadas, com virada do tráfego do conjunto de tarefas original para o conjunto de tarefas atualizado de uma só vez (R ll-at-once).

**AWS Web Application Firewall**

O AWS WAF ajuda a manter as aplicações seguras contra as ameaças web mais comuns e vulnerabilidades de segurança, seguindo padrões como os Top 10 da OWASP. As solicitações bloqueadas pelo WAF são interrompidas antes de chegarem aos servidores web, o que ajuda a preservar os recursos e a segurança da aplicação.

**Modo de Monitoramento**

O AWS WAF oferece um modo de monitoramento que permite aos usuários avaliar quantas solicitações seriam bloqueadas pela configuração atual do WAF sem efetivamente bloqueá-las. Esse modo é útil para fins de teste e ajuste fino das regras de segurança, permitindo que os administradores vejam o impacto das regras antes de ativá-las para o bloqueio real.

**Proteções de Segurança Incluídas**

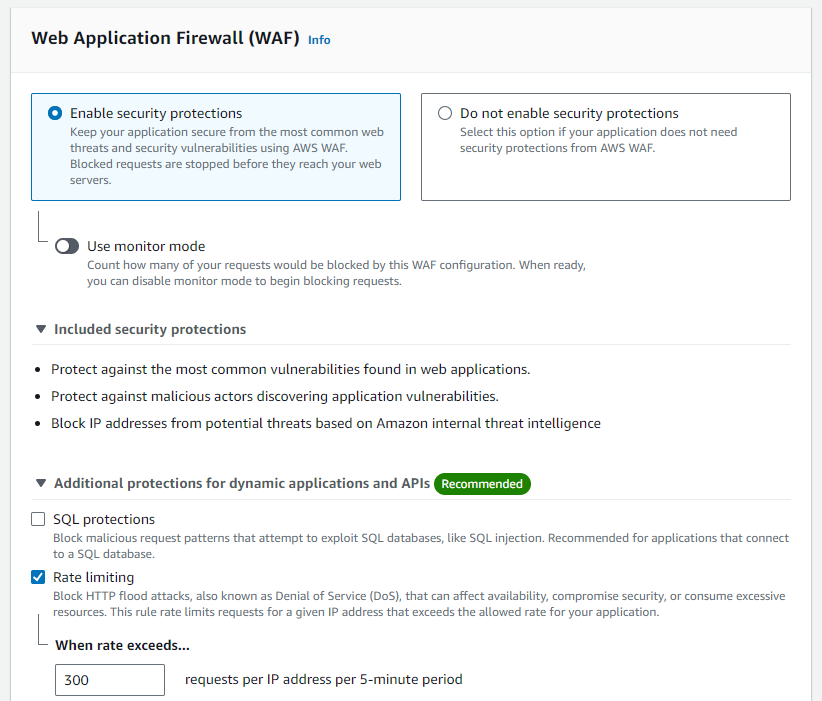
O AWS WAF fornece proteção contra vulnerabilidades comuns encontradas em aplicações web e protege contra atores mal-intencionados que tentam descobrir vulnerabilidades na aplicação. Ele permite o bloqueio de endereços IP com base em inteligência interna de ameaças da Amazon, aumentando a segurança contra ataques conhecidos e potenciais ameaças.

**Rate Limiting**

Um aspecto crucial do AWS WAF é sua capacidade de implementar rate limiting, que é essencial para bloquear ataques de HTTP flood, também conhecidos como ataques de Denial of Service (DoS). Esses ataques podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos. O rate limiting permite limitar as solicitações de um determinado endereço IP que excede a taxa permitida para a aplicação.

**Considerações sobre o Rate Limit**

A configuração do rate limit no AWS WAF deve ser cuidadosamente analisada e adaptada às necessidades específicas da aplicação. Uma taxa muito restritiva pode bloquear usuários legítimos, especialmente em aplicações com alta interatividade ou em eventos de pico de tráfego. Por outro lado, uma configuração muito permissiva pode não oferecer proteção suficiente contra ataques de DoS. É recomendável começar com configurações conservadoras e ajustá-las com base no monitoramento do tráfego e no comportamento dos usuários.



Implementamos também o Amazon CloudFront para a distribuição de conteúdo HTML e o Amazon S3 para o armazenamento de mídia e outros arquivos, conforme detalhado anteriormente. Essa configuração minimiza a carga nas instâncias EC2 ao distribuir o tráfego através do CloudFront e reduz as requisições GET ao S3, contribuindo para uma notável redução de custos. O TTL do CloudFront para conteúdo HTML foi ajustado para um valor baixo, permitindo atualizações frequentes sem a necessidade de invalidações constantes de cache, enquanto para o S3, estabelecemos um TTL mais alto para minimizar as requisições e os custos associados. É importante destacar que aproveitamos o tier gratuito (*Free tier[[1]](#footnote-0)*) do CloudFront, que inclui até 1 TB de transferência de dados por mês, otimizando o custo-benefício.

**Regras e ACLs**

Foram utilizadas 1 ACL e 6 Regras conforme a seguir.

ACL: Gerada pelo CloudFront

Regras:

AWS-RateBasedRule-IP-300-CreatedByCloudFront

(Regra para bloquear uma lista de IPs já identificados pela AWS)

AWS-AWSManagedRulesAmazonIpReputationList

(Este grupo contém regras baseadas na inteligência de ameaças da Amazon. Isso é útil se você quiser bloquear fontes associadas a bots ou outras ameaças.)

AWS-AWSManagedRulesKnownBadInputsRuleSet

(Contém regras que permitem bloquear padrões de solicitação conhecidos como inválidos e associados à exploração ou descoberta de vulnerabilidades. Isso pode ajudar a reduzir o risco de um agente mal-intencionado descobrir um aplicativo vulnerável)

AWS-AWSManagedRulesSQLiRuleSet

(Contém regras que permitem bloquear padrões de solicitação associados à exploração de bancos de dados SQL, como ataques de injeção SQL. Isso pode ajudar a evitar a injeção remota de consultas não autorizadas.)

AWS-AWSManagedRulesBotControlRuleSet

(Fornece proteção contra bots automatizados que podem consumir recursos excessivos, distorcer as métricas de negócios, causar tempo de inatividade ou realizar atividades maliciosas. O Bot Control fornece visibilidade adicional por meio do Amazon CloudWatch e gera rótulos que você pode usar para controlar o tráfego de bots para seus aplicativos.)

**AWS Systems Manager**

O AWS Systems Manager permite a automatização segura de tarefas de operações e gerenciamento de TI comuns e repetitivas em várias contas e regiões da AWS. É o hub de operações para aplicações e recursos da AWS e é dividido em quatro grupos de recursos principais, e outros recursos que são continuamente disponibilizados

| Gerenciamento de operações | Gerenciamento de aplicações | Gerenciamento de alterações | Gerenciamento de nós | Miscelânia |
| --- | --- | --- | --- | --- |
| Explorer | Application Manager | Automação | Fleet Manager | Conformidade |
| OpsCenter | AppConfig | Change Manager | Session Manager | Inventário |
| Incident Manager | **Armazenamento de parâmetros** | Janelas de manutenção | Patch Manager | Run Command |
|  |  |  |  | State Manager |
|  |  |  |  | Distribuidor |

**Parameter Store**

O AWS Systems Manager oferece um armazenamento centralizado para gerenciar os dados de configuração em texto simples, como strings de bancos de dados, ou secretos, como senhas. Assim, pode-se separar dados secretos e de configuração do código. Os parâmetros podem ser marcados com *tags* e organizados em hierarquias para facilitar seu gerenciamento. Por exemplo, pode-se usar o mesmo nome de parâmetro, “db-string”, com um caminho hierárquico diferente, “dev/db-string” ou “prod/db-string”, para armazenar valores diferentes. O Systems Manager é integrado ao AWS Key Management Service (KMS), o que permite criptografar automaticamente os dados armazenados. Também pode-se controlar o acesso de usuários e recursos aos parâmetros usando o AWS Identity and Access Management (IAM). Os parâmetros podem ser indicados por meio de outros serviços da AWS, como Amazon ECS, AWS Lambda e AWS CloudFormation.

**Backup e segurança de dados**

Ao ser ativado o serviço da AWS Backup será propiciado uma proteção abrangente, garantindo que todos os componentes críticos do Upper Trends estejam protegidos, incluindo arquivos de configuração, temas, plugins e uploads de mídia.

O Serviço permite a rápida recuperação em casos críticos. A capacidade de restauração rápida de arquivos específicos, diretórios ou sistemas completos, reduz o tempo de inatividade em caso de problemas.

O serviço tem um design que preza pela simplicidade operacional com redução considerável da complexidade na gestão de backups, automatizando tarefas rotineiras e centralizando a administração de backups.

Integrar o AWS Backup em sua infraestrutura AWS proporciona uma camada adicional de segurança e resiliência, assegurando backups confiáveis e acessíveis para uma recuperação rápida e eficaz quando necessário.

**Validação das funcionalidades e Testes**

Nesta etapa estaremos saindo de um ambiente de desenvolvimento para um ambiente de homologação e produção. O objetivo é garantir que a aplicação da Upper Trends tenha a melhor experiência possível, com escalabilidade e segurança conforme demanda com observabilidade, seguindo etapas abaixo:

* Realizar testes intensivos de integração e usabilidade, com teste de carga.
* Validar se métricas e alertas estão sendo coletados corretamente.
* Acompanhar se os alertas estão sendo enviados corretamente pelos métodos de notificação.
* Lançar a plataforma para um grupo restrito de usuários para um período de testes.
* Coletar feedback dos usuários e fazer ajustes finais.

**Ajustes finais, monitoramento e entrega da solução**

* Definir serviços de monitoramento, como o Amazon CloudWatch, para coletar métricas de desempenho.
* Monitorar o desempenho da plataforma em produção.
* Manter uma equipe de suporte pronta para lidar com problemas e solicitações dos usuários.
* Realizar uma avaliação final do projeto, para identificar possíveis melhorias e garantir que todas expectativas foram atendidas.

**Itens Não Inclusos (fora do escopo)**

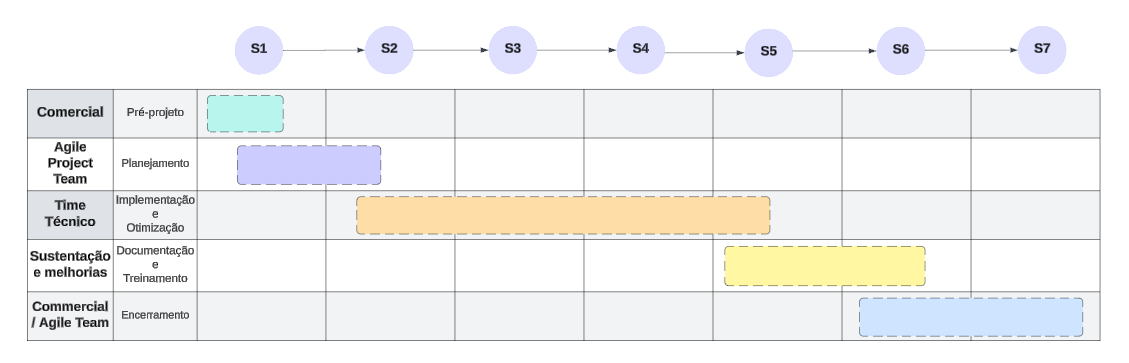
Posterior a instalação e disponibilidade de aplicação, não será fornecido qualquer suporte à utilização da aplicação, ficando definido que a equipe de TI e editores Upper Trends possuem conhecimento e capacidade técnica para lidar com as questões relativas à operação da sua aplicação.

Outros itens que não estejam explicitamente relacionados no resumo executivos, implantação e suporte e demais situações não previstas neste documento serão tratadas como projetos específicos, cujo esforço, escopo, prazo e valor serão discutidos oportunamente.

# 7 - CRONOGRAMA GERAL

Para otimizar a gestão do projeto, ficou estabelecido que as reuniões terão duração de 1 hora e 40 minutos, proporcionando um tempo eficiente para discutir progressos, desafios e estratégias. Além disso, reconhecendo a possibilidade de necessidade de horas técnicas adicionais em situações específicas, informamos que essas solicitações resultarão em custos adicionais, visando uma transparência financeira e uma gestão eficiente dos recursos. Essa abordagem visa maximizar a eficácia do tempo dedicado às reuniões, garantindo que sejam focadas e produtivas. Essa abordagem estruturada visa assegurar um equilíbrio entre a alocação de tempo para discussões essenciais e a flexibilidade para abordar desafios técnicos específicos, contribuindo para a eficiência global do projeto e a satisfação do cliente.

O cronograma estabelecido representa nossa abordagem detalhista e centrada na obtenção de resultados consistentes.

****

**Pré-projeto:**

* Marcar reunião inicial
* Contrato
* Documentação dos Requisitos de negócio

**Planejamento:**

* Definição de Objetivos e Escopo
* Avaliação de Viabilidade
* Análise de Riscos
* Design da Arquitetura
* Provisionamento de Recursos
* Preparação de Dados

**Implementação e Otimização:**

* Migração de Aplicações
* Otimização de Desempenho
* Testes de Desempenho
* Backup e Recuperação
* Ajustes pós teste de desempenho e recuperação
* Implantação completa

**Documentação e Treinamento:**

* Documentação
* Treinamento da equipe

**Encerramento do Projeto:**

* Revisão Pós-Implementação
* Encerramento formal

# 8 - TESTES DE CARGA E DESEMPENHO

Realizamos testes de carga progressivos, utilizando a ferramenta [loader.io](https://loader.io/), para avaliar o desempenho da aplicação rodando no ECS Fargate da AWS. O cenário simulou 700 usuários simultâneos. Os resultados obtidos foram extremamente satisfatórios conforme demonstrado:

**Características do teste**

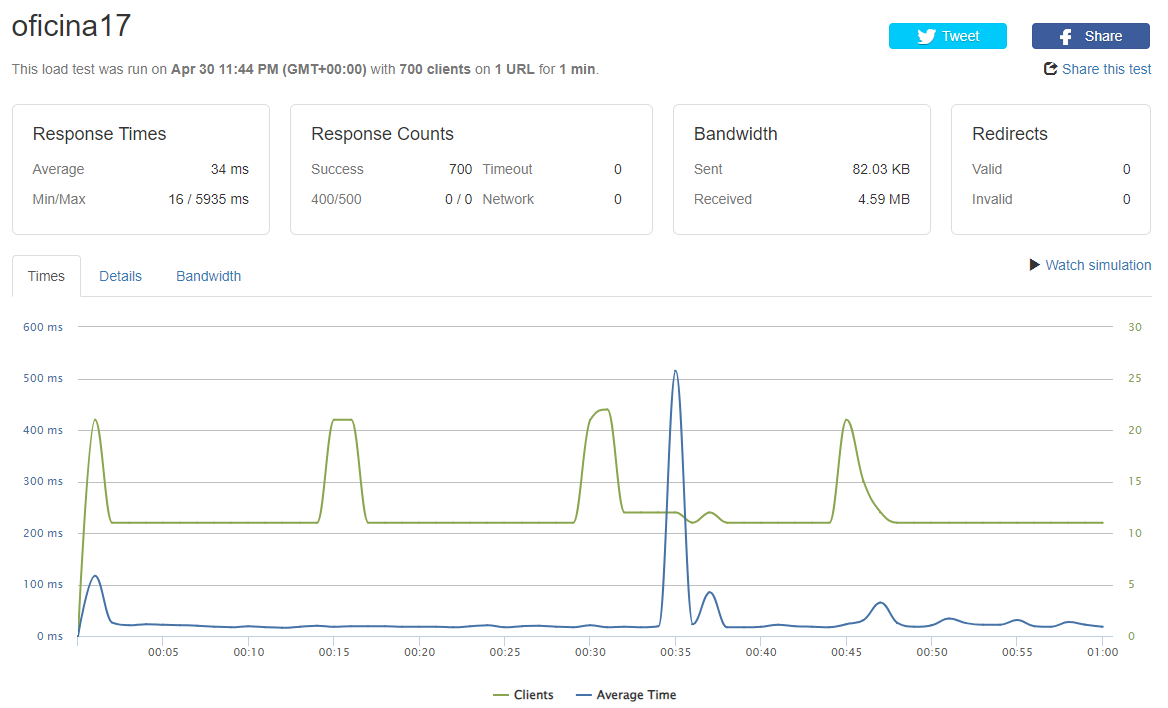
Para a realização dos testes, simulamos uma carga de 700 usuários durante um período de 30 minutos através da ferramenta [loader.io](https://loader.io/), ferramenta de teste on-line que permite realizar testes de carga em sistemas e APIs.

**Resultado dos testes**

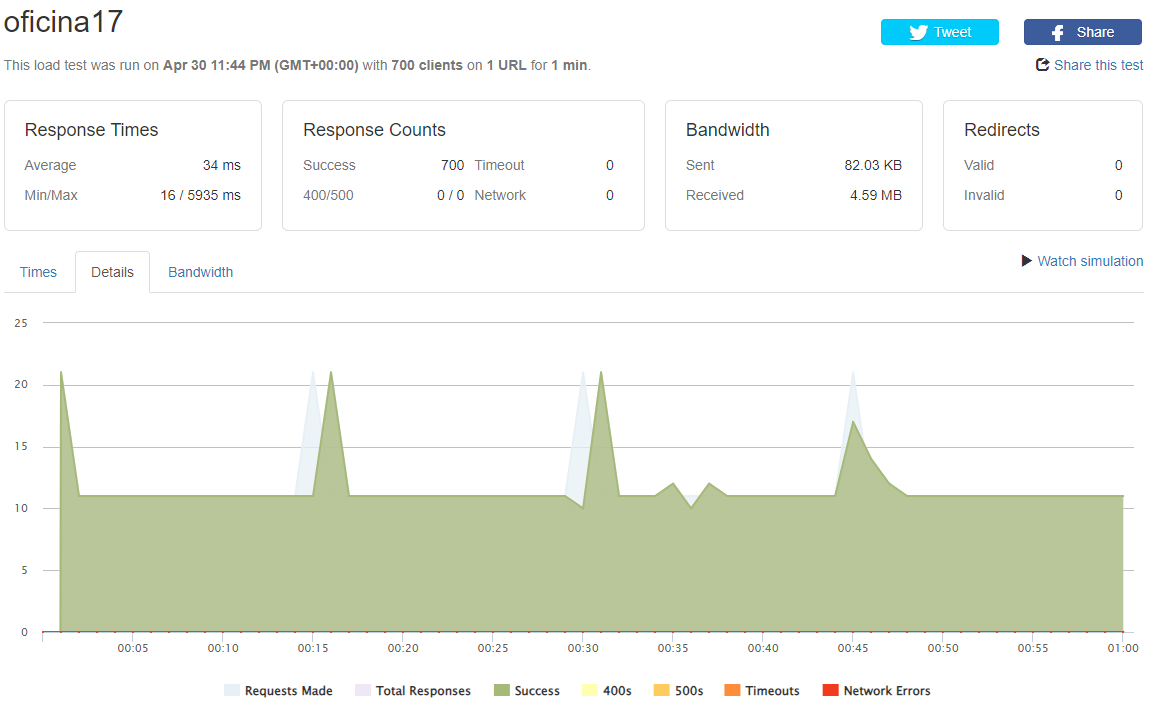
Após os diversos testes realizados e com a infraestrutura no ambiente de teste completamente definida, realizamos o teste final para validação da arquitetura.

O resultado apresentado pela *Six-Cloud Solutions*, como veremos mais abaixo trabalhou em um cenário de 700 requisições por segundo, desta maneira podemos concluir que a solução atende com folga a necessidade uma vez que 700 requisições por segundo representam mais de 1.000.000 de requisições por dia.

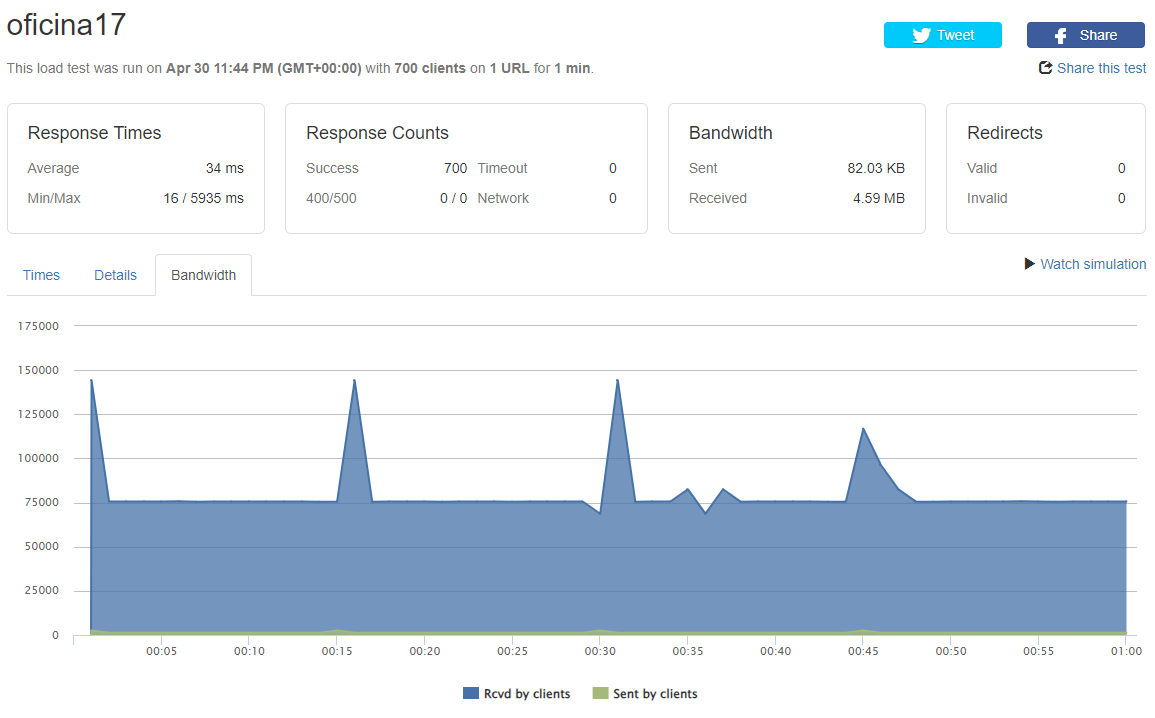
A próxima figura exibe os resultados do teste realizado em que é possível observar por exemplo que mesmo sustentando as requisições por segundo acima de 700 as chamadas não apresentaram nenhuma falha e o tempo de resposta foi menor que 0.5 segundos, lembrando que o tempo de resposta médio ficou em 34 ms.

****

A próxima imagem descreve em detalhes o total de requisições realizadas e os tipos de respostas. É possível observar que mesmo com 700 requisições por segundo, a aplicação apresentou nenhuma falha ao exibir as páginas.

****

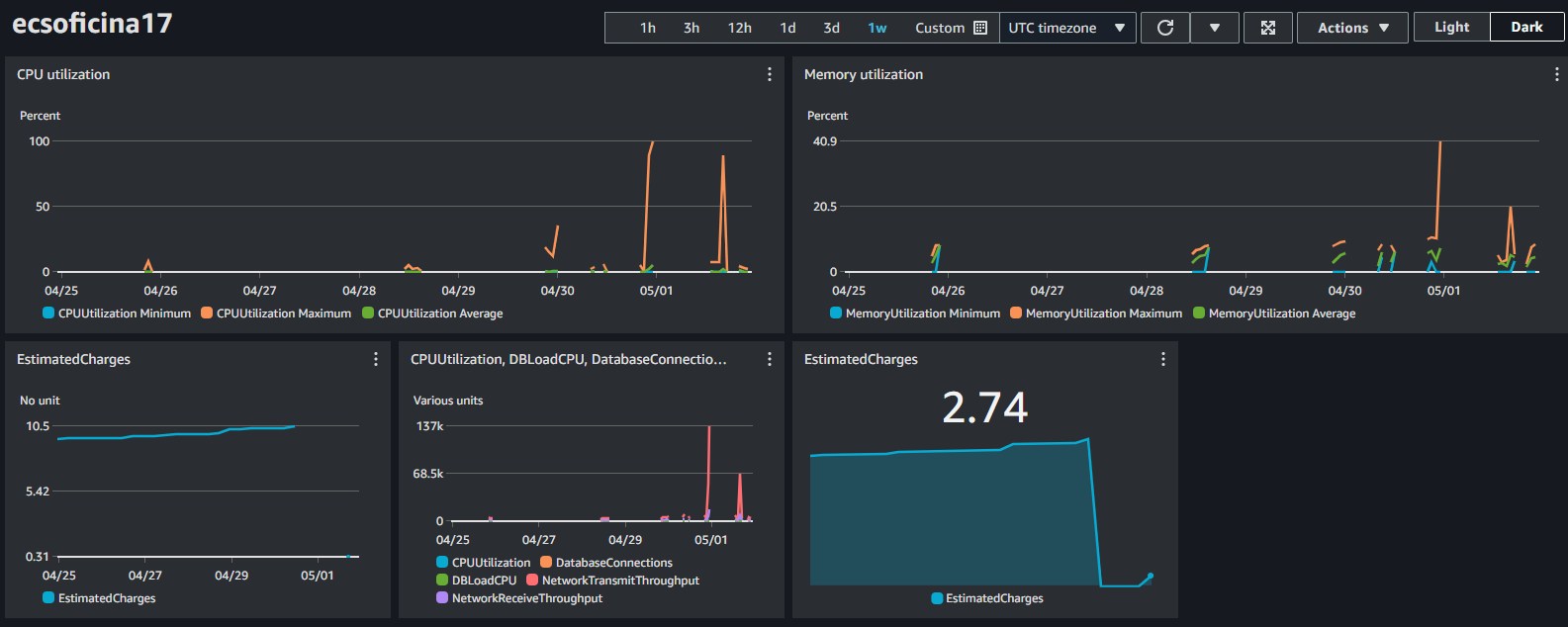
A próxima imagem detalha a conexão de banda utilizada para atender as 700 requisições por segundo, em detalhes o total de requisições realizadas e os tipos de respostas. É possível observar que em alguns momentos mesmo com o aumento de requisições a largura de banda configurada não alcançou o máximo disponível para a aplicação resultando numa navegação mais amigável sem tempos de espera.

****

**Painel de Monitoramento**

Abaixo os painéis de monitoramento de:

* Utilização de CPU
* Utilização de memória
* Estimativas de cobrança em Gráfico
* Gráfico de CPU Utilization, DBLoadCPU, NetworkReceiveThroughput, DBAConnections, NetworkTransitThroughput
* Estimativas de cobrança em Valor

****

# 9 - CONSIDERAÇÕES FINAIS

Após a conclusão da implementação e disponibilidade da aplicação na infraestrutura da AWS, várias vantagens serão alcançadas. Representando uma jornada significativa na modernização da infraestrutura de hospedagem e na utilização de serviços gerenciados na nuvem para garantir escalabilidade, segurança e desempenho.

As principais realizações incluem elasticidade e escalabilidade, gerenciamento eficiente de recursos, segurança e conformidade e desempenho aprimorado e alguns desafios superados incluem a migração de dados e a otimização de custos.

Em resumo, a implementação bem-sucedida da aplicação na AWS representa não apenas um marco, mas também uma base sólida para futuras inovações e melhorias contínuas.

# 10 - INTEGRANTES DO GRUPO 2

| Carlos Junior |  |
| --- | --- |
| Edilson Bezerra |  |
| Victor Cleber | <https://www.linkedin.com/in/victor-cleber/?locale=en_US> |

1. *Free Tier* - em português conhecido como Nível Gratuito AWS é um conjunto de incentivos fornecido pela AWS que inclui período de 12 meses (para novas contas), alguns serviços com períodos de teste ou volumes menores de gratuidade e outros serviços que serão sempre gratuitos. [↑](#footnote-ref-0)