



PROPOSTA TÉCNICA



A/C Sr. Leandro Porciuncula.

24/09/2024

REF: Migrar o sistema de gerenciamento de chamados de helpdesk – GLPI para a infraestrutura na AWS

Prezado Leandro,

Conforme solicitação, segue abaixo a proposta para migração da aplicação GLPI para a AWS, atendendo a Upper Plan, 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,

Victor Cleber

Gerente de Contas

Telefone: +55 11 91888-0022

gc@sixcloudsolutions.com.br

Carlos Junior

Pré-vendas / Pós-vendas

Telefone: +55 11 92888-0033

cm@sixcloudsolutions.com.br

Edilson Bezerra

AWS Architect

Telefone: +55 11 9188-0123

ar@sixcloudsolutions.com.br

Identificação do Documento

Documento	Prestação de serviço de migração de aplicação – GLPI
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 Plan, para a estrutura em nuvem AWS, para melhorar o tempo de resposta, prover 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
2 - RESUMO EXECUTIVO	4
3 - ARQUITETURA DA SOLUÇÃO	6
3.1 - Diagrama dos Serviços.....	6
3.2 - Detalhamento dos Serviços a serem usados	7
4 - IMPLANTAÇÃO	14
5 - OVERVIEW DOS PRINCIPAIS SERVIÇOS	24
6 - CRONOGRAMA GERAL	30
7 - CONSIDERAÇÕES FINAIS.....	32
8 - INTEGRANTES DO GRUPO.....	32

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 Plan 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 Plan, 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
- compliance@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 Plan 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 Plan, 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.

2 - RESUMO EXECUTIVO

Problemas Levantados Junto ao Cliente

A Upper Plan é uma empresa que desenvolve pigmentos para plásticos e trabalha com sistema de gerenciamento de chamados de helpdesk – GLPI. A empresa Upper Plan possui quatro colaboradores na área de TI: um gerente de TI, um analista de infraestrutura e dois analistas de suporte. No total, a empresa tem 200 colaboradores, porém, apenas 60 utilizam o GLPI para abertura de chamados.

O time de TI tem enfrentado problemas de lentidão no acesso ao GLPI e foi observado que o servidor atual que hospeda o GLPI está com os recursos de memória e CPU no limite. A atual infraestrutura que suporta o GLPI é composta por uma máquina virtual com o sistema operacional CentOS 7, com 10 GB de memória RAM e 4 vCPUs. O banco de dados é o MariaDB, que utiliza 30 GB.

A iniciativa de migrar para a Cloud partiu do gerente de TI, que avaliou ser mais benéfico migrar a solução de chamados para a Cloud, considerando que, no planejamento estratégico de TI para 2025, está prevista a migração de outros serviços e sistemas, como o ERP.

Escopo da Proposta de Solução

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

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 melhorias identificadas

Segurança > usuário e senha de administração configurada no arquivo php da aplicação

Contas AWS > Segregação de contas

Sistema Operacional > Sistema Operacional CentOS para Amazon Linux

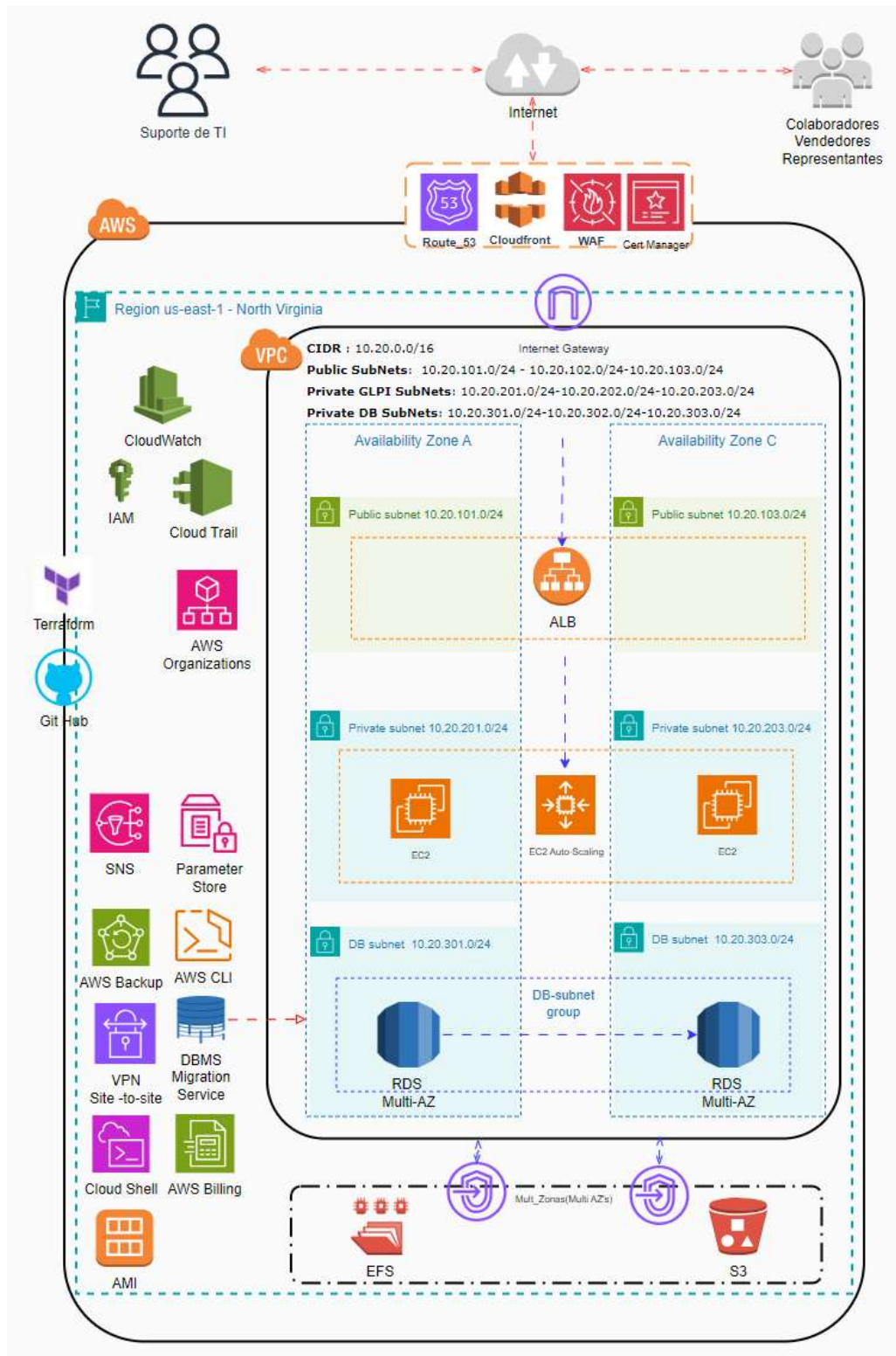
Escalabilidade > uso do balanceador de carga nativo da AWS

Resiliência > replicação do banco de dados RDS em multi AZ

Alta disponibilidade > uso de TRÊS regiões




3 - ARQUITETURA DA SOLUÇÃO



3.1 - Diagrama dos Serviços






3.2 - Detalhamento dos Serviços a serem usados




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


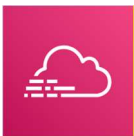

	<p>AWS Route 53</p> <p>Serviço de Sistema de Nomes de Domínio (DNS). Fornece serviços de registro de domínio, gerenciamento de DNS e roteamento de tráfego na internet, com nível muito alto de disponibilidade e escalável. Projetado para oferecer aos desenvolvedores e empresas um meio altamente confiável 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.</p>
	<p>AWS WAF - Web Application Firewall</p> <p>O AWS WAF ajuda a proteger contra <i>bots</i> e <i>exploits</i> 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 <i>SQL Injection</i> e <i>Cross-Site Scripting</i> (XSS), é crucial.</p>
	<p>Amazon CloudFront</p> <p>Serviço de CDN (Content Delivery Network). O CloudFront distribui o conteúdo por meio de uma rede global de datacenters denominados</p>




	<p>loais 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.</p>
	<p>AWS Virtual Private Cloud - VPC</p> <p>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</p> <p>Alguns serviços associados a VPC serão utilizados:</p>
	<p>AWS Organizations</p> <p>Serviço de gerenciamento de contas que permite consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente. AWS Organizations inclui recursos de gerenciamento de contas e faturamento consolidado que permitem que você atenda melhor às necessidades orçamentárias, de segurança e de conformidade de sua empresa. Como um administrador de uma organização, você pode criar contas em sua organização e convidar contas existentes a participarem da organização.</p>

	<p>INTERNET GATEWAY</p> <p>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.</p> <p>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.</p>
	<p>Application Load Balancer</p> <p>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.</p>
	<p>Elastic Cloud Computing (EC2)</p> <p>A EC2 é o serviço de computação da AWS que oferece a facilidade de rodar os serviços na nuvem pública da AWS. O EC2 reduz o tempo de inicialização de novos servidores e oferece a capacidade de dimensionamento com base em alterações nos requisitos de computação dinamicamente. Além de possuir segurança integrada, que te dá controle total dos servidores, possui também a flexibilidade para você escolher entre diferentes sistemas operacionais dependendo da sua necessidade de negócio.</p>

	<p>Amazon Relational Database Service - RDS</p> <p>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.</p>
	<p>Amazon Simple Storage Service - S3</p> <p>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.</p>
	<p>SECURITY GROUPS</p> <p>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.</p>
	<p>AWS Identity and Access Management - IAM</p> <p>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.</p>

	<p>AWS Certificate Manager</p> <p>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.</p>
	<p>Parameter Store</p> <p>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.</p>
	<p>VPC ENDPOINTS</p> <p>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.</p> <p>Existem vários tipos de VPC <i>endpoints</i>:</p> <p>a) <i>interface endpoints</i></p> <p>Esses <i>endpoints</i> 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.</p> <p>b) <i>Gateway Load Balancer</i></p>

	<p>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.</p> <p>c) <i>gateway endpoints</i>:</p> <p>Esses <i>endpoints</i> 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.</p>
	<p>Amazon SNS (Simple Notification Service)</p> <p>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 pubsub 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. A funcionalidade A2P permite enviar mensagens para usuários em grande escala por SMS, push de dispositivos móveis e e-mail.</p>
	<p>Cloud Trail</p> <p>Auditoria e rastreamento de todas as atividades da conta da AWS, para melhor segurança, conformidade e investigação de problemas.</p>
	<p>AWS CloudWatch</p> <p>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,</p>

	<p>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.</p>
	<p>AWS Billing</p> <p>O AWS Billing é um serviço de monitoramento das cobranças estimadas da AWS usando o Amazon CloudWatch. As suas cobranças estimadas para cada serviço da AWS em utilização são calculadas e enviadas diversas vezes ao dia para o CloudWatch como dados métricos.</p> <p>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.</p>
	<p>AWS Backup</p> <p>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.</p>
	<p>VPN site-to-site</p> <p>O serviço VPN site-to-site, será usado sua rede interna se comunicar-se com sua rede na AWS. Você pode habilitar o acesso à sua rede remota pela VPC criando uma conexão AWS Site-to-Site VPN (Site-to-Site VPN) e configurando o roteamento para transmitir o tráfego pela conexão.</p>

4 - IMPLANTAÇÃO

Pesquisa de campo e levantamento dos requisitos

O objetivo desta etapa é levantar os requisitos específicos de configuração para a migração da aplicação para a AWS, 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 diretores da Upper Plan para melhor entender a operação e configuração atual da aplicação atual e seu banco de dados. A ideia é que o time da Upper Plan 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 da Landing Page da Upper Plan. O primeiro passo será analisar e adequar 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 Landing Zone e o AWS Organizations
- 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 Banco de Dados Multi A/Z
- Configurar sistema de armazenamento de objeto S3
- Configurar o sistema de arquivos EFS
- Criação e configuração da EC2
- Implementar a aplicação GLPI através do código disponibilizado pela Upper Plan
- Criar imagem AMI da aplicação
- Implementar a plataforma em um ambiente produtivo
- Implementação de estrutura de alta disponibilidade, como ELB, Auto Scaling, Cloud Front
- Configuração tópico SNS para envio email para comunicação

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_glpi

Região: Leste dos EUA (Norte da Virgínia)

ID região: us-east-1

CIDR IPv4: 172.20.0.0/20

Configuração de Sub-redes - Subnets

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

Nome: glpi-web-1 CIDR IPv4: 172.20.1.0/24 (AZ): us-east-1a	Nome: glpi-web-2 CIDR IPv4: 172.20.2.0/24 (AZ): us-east-1b	Nome: glpi-web-3 CIDR IPv4: 172.20.3.0/24 (AZ): us-east-1c
Nome: glpi-app-1 CIDR IPv4: 172.20.4.0/24 (AZ): us-east-1a	Nome: glpi-app-2 CIDR IPv4: 172.20.5.0/24 (AZ): us-east-1b	Nome: glpi-app-3 CIDR IPv4: 172.20.6.0/24 (AZ): us-east-1c
Nome: glpi-db-1 CIDR IPv4: 172.20.7.0/24 (AZ): us-east-1a	Nome: glpi-db-2 CIDR IPv4: 172.20.8.0/24 (AZ): us-east-1b	Nome: glpi-db-3 CIDR IPv4: 172.20.9.0/24 (AZ): us-east-1c

Internet Gateway

Uso de um gateway de internet nomeado como: igw-glpi

Router Tables:

Tabelas de rotas nome: rt_web_glpi
Associações de Sub-rede: glpi-web-1 glpi-web-2 glpi-web-3
Rotas: Destino: 172.20.0.0/20 → Target: local Destino: 0.0.0.0/0 → Target: igw-glpi

Tabelas de rotas nome: rt_app_glpi
Associações de Sub-rede

glpi-app-1 | glpi-app-2 | glpi-app-3

Rotas:

Destino: 172.20.0.0/20 → **Target:** local

Tabelas de rotas nome: rt_db_glpi

Associações de Sub-rede

glpi-db-1 | glpi-db-2 | glpi-db-3

Rotas:

Destino: 172.20.0.0/20 → **Target:** local

VPC Security Groups

Nome: glpi-web-sg

Regras de entrada:

Tipo	Protocolo	Porta	Origem
HTTPS	TCP	443	alb-glpi
HTTP	TCP	80	alb-glpi

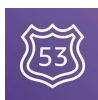
Regras de saída:

Todo o tráfego	Todos	Todas	0.0.0.0/0
----------------	-------	-------	-----------

Grupos de segurança para uso específico

Nome: glpi_app_sg			
Regras de entrada:			
Tipo	Protocolo	Porta	Origem
HTTPS	TCP	443	glpi-web-sg
HTTP	TCP	80	glpi-web-sg
Regras de saída:			
Todo o tráfego	Todos	Todas	0.0.0.0/0

Nome: glpi_db_sg			
Regras de entrada:			
Tipo	Protocolo	Porta	Origem
MYSQL/Aurora	TCP	3306	glpi-app-sg
Regras de saída:			
Todo o tráfego	Todos	Todas	0.0.0.0/0

**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: insights4.cloud
Tipo: Pública

Registros:

Nome	Tipo	Alias
insights4.cloud.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_glpi
Mecanismo: MariaDb Versão do Mecanismo: 10.11.8 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: upperplan.s3.glpi.alb
Região us-east-1
Bloquear todo o acesso público: ativado
Encriptação Ativa: Server Side encriptação com SSE-S3



Elastic Load Balancer - ELB

Nome ALB-glpi
Tipo Application Load Balance
Esquema voltado para internet
Tipo de endereçamento IP IPv4
VPC: vpc_glpi
Grupo de segurança: sg-web-glpi
Sub-redes:
 glpi-web-1 | glpi-web-2 | glpi-web-3

Listeners e roteamento:

protocolo	porta	Ação padrão
HTTP	80	Forward to target group
HTTPS	443	Forward to target group

DefaultSSL / TLSertificate *.upperplan.com Security policy ELBSecurityPolicy-TLS13-1-2-2021-06

Grupo de destino - Target Group para ELB

Nome tg-glpi
Tipo Instance Protocolo: Porta HTTP: 80 Versão do protocolo HTTP 1 Tipo endereçamento IP IPv4 Zonas de disponibilidade: us-east-1a / us-east-1b / us-east-1c
Verificação de Integridade: Protocolo HTTP Path / Porta de tráfego Limite inteiro 2 êxitos consecutivos de verificação de integridade limite não inteiro 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_glpi
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: AML-glpi
Tipo de instância t2.medium Versão 3
Security Group glpi-app-sg Subnets: glpi-app-1 glpi-app-2 glpi-app-3
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: upperplan

Acesso ao console: Habilitado

Credenciais Login / Senha, MFA

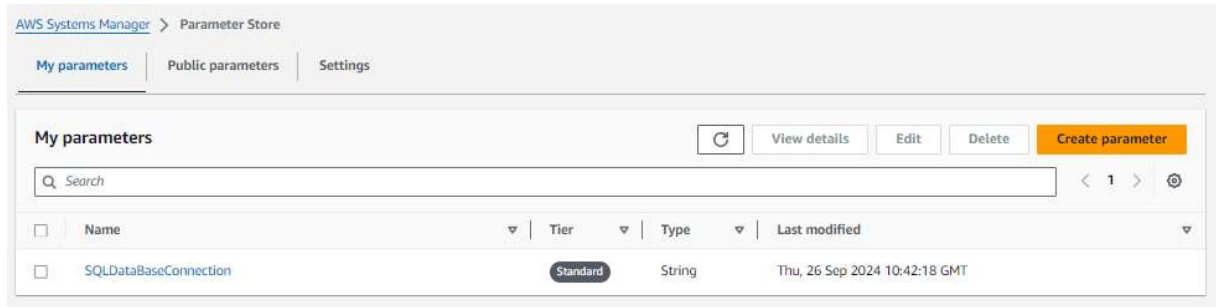
Políticas de permissão AdministratorAccess

Permissões:

```
{
  "Version": "2024-02-06",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

AWS Systems Management

Parameter Store



5 - OVERVIEW DOS PRINCIPAIS SERVIÇOS

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 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.

The screenshot shows the 'Web Application Firewall (WAF)' configuration page in the AWS console. At the top, there's a title 'Web Application Firewall (WAF)' with an 'Info' link. Below this, there are two main sections for enabling security protections. The first section, 'Enable security protections', is selected with a radio button and includes a description: 'Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.' The second section, 'Do not enable security protections', is unselected and includes a description: 'Select this option if your application does not need security protections from AWS WAF.' Below these, there's a section for 'Use monitor mode' with a radio button and a description: 'Count how many of your requests would be blocked by this WAF configuration. When ready, you can disable monitor mode to begin blocking requests.' Further down, there's a section titled 'Included security protections' with a list of three items: 'Protect against the most common vulnerabilities found in web applications.', 'Protect against malicious actors discovering application vulnerabilities.', and 'Block IP addresses from potential threats based on Amazon internal threat intelligence.' Below this, there's a section titled 'Additional protections for dynamic applications and APIs' with a 'Recommended' badge. This section contains two checkboxes: 'SQL protections' (unchecked) and 'Rate limiting' (checked). The 'Rate limiting' checkbox is checked, and its description reads: 'Block HTTP flood attacks, also known as Denial of Service (DoS), that can affect availability, compromise security, or consume excessive resources. This rule rate limits requests for a given IP address that exceeds the allowed rate for your application.' Below the 'Rate limiting' checkbox, there's a section titled 'When rate exceeds...' with a text input field containing '300' and a label 'requests per IP address per 5-minute period'.

Web Application Firewall (WAF) [Info](#)

☒ **Enable security protections**
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

☐ **Do not enable security protections**
Select this option if your application does not need security protections from AWS WAF.

☐ **Use monitor mode**
Count how many of your requests would be blocked by this WAF configuration. When ready, you can disable monitor mode to begin blocking requests.

▼ **Included security protections**

- Protect against the most common vulnerabilities found in web applications.
- Protect against malicious actors discovering application vulnerabilities.
- Block IP addresses from potential threats based on Amazon internal threat intelligence

▼ **Additional protections for dynamic applications and APIs** **Recommended**

☐ **SQL protections**
Block malicious request patterns that attempt to exploit SQL databases, like SQL injection. Recommended for applications that connect to a SQL database.

☒ **Rate limiting**
Block HTTP flood attacks, also known as Denial of Service (DoS), that can affect availability, compromise security, or consume excessive resources. This rule rate limits requests for a given IP address that exceeds the allowed rate for your application.

When rate exceeds...

requests per IP address per 5-minute period

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) do

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.

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.)

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 segredos, 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 Plan 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 Plan 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.

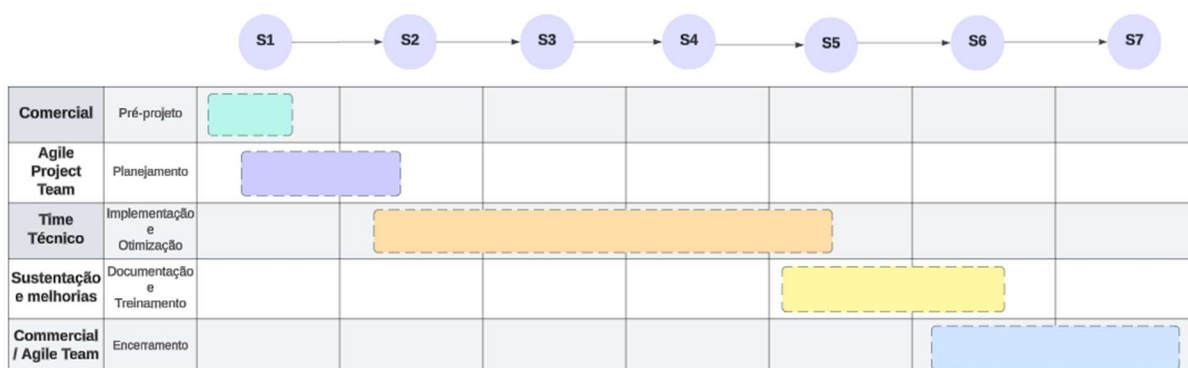
Itens Não Inclusos (fora do escopo)

Posterior a instalação e disponibilidade de aplicação, não será fornecido qualquer suporte à utilização da aplicação, ficando definido que a equipe de TI da Upper Plan possui 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.

6 - CRONOGRAMA GERAL

Para otimizar a gestão do projeto, ficou estabelecido que as reuniões terão duração de 2 horas, 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.



Pré-projeto:

- Reunião inicial
- Assinatura do Contrato
- Elaboração da 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 dos Dados
- Otimização de Desempenho
- Testes de Desempenho
- Backup e Recuperação
- Ajustes pós teste de desempenho e recuperação

Documentação e Treinamento:

- Documentação
- Treinamento da equipe

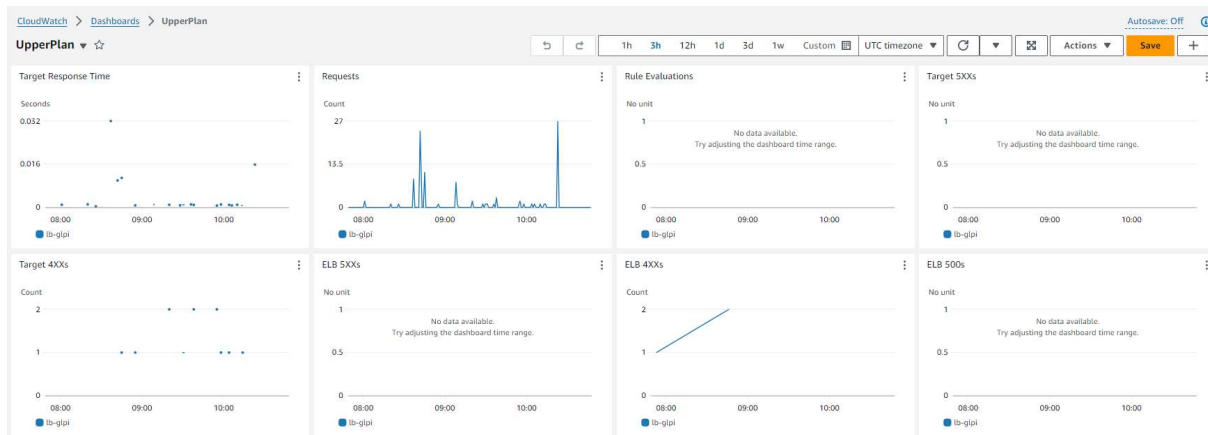
Encerramento do Projeto:

- Revisão Pós-Implementação
- Encerramento formal

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



7 - 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.

8 - INTEGRANTES DO PROJETO

Carlos Junior <https://www.linkedin.com/in/junior-fernandes-35006228/>

Edilson Bezerra <https://www.linkedin.com/in/edilson-bezerra-a0933137/>

Victor Cleber https://www.linkedin.com/in/victor-cleber/?locale=en_US

www.sixcloudsolutions.com.br

@sixcloudsolutions_oficial



+55 11 4000-1111