

RELATÓRIO SIMPLIFICADO ACERCA
DE PROCESSOS DE CONFIABILIDADE E
DISPONIBILIDADE

SPEEDIO

Declaro de antemão que todos os dados em posse da SPEEDIO são originados de fontes públicas e terminantemente não fazemos o trato de dados pessoais.

Tecnologias

Na SPEEDIO é usada principalmente duas ferramentas quando estamos falando de armazenamento de dados.

Para dados da plataforma (ATLAS) é usado o banco de dados não relacional **MongoDB**, para o armazenamento de informações relacionadas a usabilidade da plataforma, alguns exemplos são: sessão, infosets, informações cadastrais, credenciais de usuário e etc.

Para a **BIGDATA** usamos o ELASTICSEARCH como motor de busca e armazenamento de dados tratados, tais como: informações cadastrais de empresas, assim como decisores, websites e quaisquer outros meios de contato.

Todas as ferramentas citadas acima rodam em distribuições Linux.

Fluxo

Todos os servidores contendo bases de dados de produção, são estritamente isolados da rede externa pelo **Firewall**. É proibido nas regras de **Firewall** qualquer fluxo de entrada e saída de informações que não seja destinada à usabilidade da nossa plataforma.

É explicitamente proibido, a colaboradores da empresa, o acesso direto á base de dados ou a serviços de produção, sendo necessário em casos de emergência/manutenção a solicitação de acesso junto a justificativa do líder do time solicitante. Se aprovado, será feita a liberação temporária de um usuário sem permissão de escrita. O acesso se dá por meio de uma conexão VPN com chaves de identificação pessoal.

Sendo assim, o usuário final tem acesso aos dados contidos nessas bases apenas através de uma API, a qual restringe a aplicação a fornecer somente as informações devidas.

Para clientes finais que desejam se cadastrar na plataforma ATLAS, é necessário a criação de senhas igual ou maior a 12 dígitos, contendo obrigatoriamente caracteres especiais, letras e números.

Todos os servidores, independentemente se são de produção, são acessados somente através do Secure Shell (SSH), usando apenas as chaves pessoais autorizadas.

Criptografia e Ofuscação

Algumas de nossas metodologias de ofuscação, sejam para segurança ou para anonimato de informações pessoais, levam em consideração as seguintes metodologias.

Todos os backups sejam da base de dados ou de configurações de aplicações são criptografados e comprimidos com o algoritmo ZipCrypto, e armazenados em um servidor de posse somente do time DevOps.

Todas as senhas e tokens de acesso contidos nesses arquivos são mantidos em forma de HASH com a criptografia md5.

Quaisquer dados pessoais, como por exemplo, nome de decisores contido nos dados buscados pelo nosso motor de busca (ELASTICSEARCH) são ofuscados pelos nossos algoritmos buscando o anonimato do sujeito em questão.

Disponibilidade

O frontend de produção está em rede CDN para facilitar o fluxo de disponibilidade e agilidade para nossos usuários. A api da nossa aplicação funciona por meio de load balance com o objetivo de dividir a carga do usuário entre servidores.

Nossos bancos de dados e motores de busca trabalham de forma clusterizadas, para o caso de falhas estarmos sempre disponíveis

Redundância

~ Main Backup = Nosso principal servidor de armazenamentos de backups

~ Mongo Main = Banco de dados responsável pelo armazenamento de informações coletadas pelos mais diversos scripts.

~ Site de vendas = WebSite principal da Speedio.

~ Outros Servidores = Servidores menos relevantes que não são de produção

Para o MongoDB temos 2 Réplicas + Snapshot dos servidores (4 a cada 2 horas; 3 diários; 1 semanal; 1 mensal) e backups contínuos no **Main Backup**.

Para o Elasticsearch temos backups contínuos no **Main Backup**, com redundância de backup para AWS e AZURE

Para o Mongo Main temos apenas backups contínuos no **Main Backup**.

Para o Site de vendas temos apenas snapshots do servidor.

Para os Outros Servidores temos apenas snapshots servidor.

Prevenção

É estabelecido com periodicidade uma auditoria interna para analisar qualquer inconsistência nos nossos processos de backup, redundância e segurança.