FACULDADE SÃO PAULO TECH SCHOOL

Arthur Ramos dos Santos - 04241008

Fabricio Prudente Ferreira - 04241070

Luís Henrique Ribeiro Alves - 04241047

Luiza Câmara Moreira - 04241065

Victor Hugo Ribeiro Braga - 04241015

1-CCO/A – 2º Semestre

PROJETO SEMESTRAL – 2º SEMESTRE

Política de Gestão de Acessos

GATEWATCH

São Paulo – SP

2024

SUMÁRIO

1. Plataforma em Nuvem AWS

A equipe GateWatch utiliza a AWS (*Amazon Web Service*) para aplicar uma camada de segurança no controle de acesso e manipulação de dados das máquinas e dos usuários. A utilização da AWS busca proteger as instâncias da EC2 (*Elastic Compute Cloud*), usadas para a criação de máquinas virtuais que, por sua vez, isolam os dados na nuvem.

2. Criação da Instância EC2

As instâncias necessárias para o armazenamento e coleta de dados devem ser, inicialmente, criadas, contendo o sistema operacional do Ubuntu ou Amazon Linux. A instância também necessitará de um par de chaves (uma pública e outra privada) da extensão *.pem* criptografadas por RSA. O arquivo gerado contendo o par de chaves deverá ser armazenado em um local seguro.

3. Configuração de Acesso da Instância EC2

No sistema da GateWatch, o usuário que terá acesso aos dados das máquinas e dos usuários será, exclusivamente, o **Gerente de TI da Azul**. Com isso, torna-se relevante o controle de acesso às instâncias na nuvem AWS para que apenas pessoas autorizadas possam ter acesso às chaves e à instância da EC2, privando os dados contidos neste serviço.

Para garantir com que apenas o gerente de TI tenha acesso ao par de chaves, é necessário abrir o terminal no diretório do arquivo e executar o seguinte comando em uma máquina contendo distro Linux:

chmod 400 <nome do arquivo .pem>

A execução desse código permite apenas a leitura do arquivo para o proprietário destas chaves. Outros usuários não terão acesso para executar, ler ou escrever este arquivo.

Desta forma, possibilita-se a conexão com a instância da EC2 via SSH (*Secure Shell*), estabelecendo uma comunicação remota entre as máquinas de

forma segura. Para fazer esta conexão, é necessário efetuar o seguinte código no terminal:

ssh -i “<nome do arquivo .pem>” <DNS Pública>

Nota de observação: O código acima para a conexão fica disponível após a criação da instância na aba “Cliente SSH”.

Com isso, o usuário poderá ter acesso remoto aos dados dos componentes *hardware* via SSH, através da instância oferecida pelo serviço da AWS.