Autenticação Única nos Ambientes em Nuvem da Amazon Web Services com Integração de Usuários do Google Suite

Pedro Silveira Pisa[1,2], **Diogo Menezes Ferrazani Mattos**[2]

[1]Solvimm
[2]MídiaCom - PPGEET/TET/UFF
Universidade Federal Fluminense (UFF)

Resumo. *A gestão de identidade nos diversos sistemas de uma organização é um desafio cada vez maior, pois novos sistemas introduzem bases de usuários individualizadas e diferentes modelos de autenticação não federados. Esse cenário é ainda mais desafiador em organizações com alta rotatividade de colaboradores e em negócios sensíveis a vazamentos de dados, principalmente com a adoção de leis de privacidade de dados. Este artigo apresenta uma solução de integração entre bases de usuários do Google Suite, utilizada pela organização nos ativos de tecnologia da informação, com o ambiente em nuvem, servidores, bancos de dados e interfaces de aplicação. O estudo visa apresentar um cenário prático de integração da identificação provida pelo Google com serviços de nuvem providos pela Amazon. Com este estudo, conclui-se que a integração de acesso, mesmo em cenários de nuvens heterogêneas, traz grande benefício de gestão do ambiente para as organizações, pois um único usuário pode ser utilizado para todos os ativos de tecnologia, facilitando, sobretudo, a revogação ampla e imediata em caso de rescisão do contrato do colaborador.*

Abstract. *Identity and access management across a wide range of organizational systems is a growing challenge as new systems and devices are adopted by departments, which require greater security. This scenario is even more challenging in fast-moving organizations as well as in data-sensitive businesses, especially with the proliferation of data privacy laws around the world. This article presents a Google Suite user-base integration solution used by the organization for information technology assets such as cloud environment, servers, databases, and APIs. This study concludes that access integration, even in heterogeneous cloud scenarios, as presented hereafter, brings great environmental management benefit to organizations because a single user can be used for all technology assets, allowing especially the immediate revogation of employee access in the event of resignation.*

1. Introdução

Com o avanço da modernização e da automatização das empresas, cada vez mais sistemas são adotados pelos departamentos ou por toda a organização. Além disso, os mais diversos dispositivos são integrados nas infraestruturas das organizações e os colaboradores da empresa precisam acessá-los e operá-los diariamente. Nesse cenário, a gestão de identidade e, especificamente, o controle de acesso nos sistemas da organização são cada vez mais desafiadores.

Este trabalho foi realizado com recursos do CNPq, CAPES, RNP e FAPERJ.

Em organizações que possuem alta rotatividade de colaboradores, há um número maior de eventos de concessão e revogação de identidade e privilégios de acessos nos sistemas da empresa e, em cada um dos eventos, introduz a possibilidade de erro ou atraso na execução. Como consequência, colaboradores já desligados da empresa podem ainda possuir acesso aos sistemas, gerando um ponto de vulnerabilidade e possíveis acessos indevidos. A adoção de leis e regulamentos de privacidade de dados ao redor do mundo, como a Lei Geral de Proteção de Dados do Brasil, tendem a enrijecer as punições aos acessos indevidos a dados de sistemas e dispositivos [Mattos et al., 2019] e, portanto, fomentam a demanda por soluções integradas de gestão de identidade mesmo em ambientes de nuvens heterogêneas.

Este artigo apresenta uma solução de integração das bases de usuário do *Google Suite* com a nuvem da *Amazon Web Services* (AWS) utilizando a linguagem de marcação para asserção de segurança 2.0 (*Security Assertion Markup Language 2.0* - SAML 2.0). No estudo de caso apresentado, após a integração da infraestrutura da nuvem da AWS com o domínio do cliente no *Google Suite*, torna-se possível a utilização do usuário do Google para acesso ao ambiente de configuração da conta da AWS, a servidores Linux e Windows, bancos de dados MySQL e PostgreSQL e, também, em aplicações personalizadas desenvolvidas pela empresa e hospedadas na AWS.

No estudo apresentado, conclui-se que a integração da gestão de identidade e o controle de acesso para as aplicações da organização em um único diretório de usuários, mesmo em cenários de nuvens heterogêneas, traz benefícios de gestão do ambiente de tecnologia da informação das organizações. Um único usuário pode ser utilizado para todos os ativos de tecnologia, oferecendo precisão, agilidade e assertividade na concessão e revogação de privilégios de acessos aos diversos sistemas em poucos passos, principalmente quando o evento de alteração é a revogação ampla e imediata dos acessos em caso de rescisão do colaborador.

Este artigo é organizado da seguinte maneira. A Seção 2 apresenta os trabalhos relacionados referentes a mecanismos e estudos sobre a integração de mecanismos de autenticação e a relação desses mecanismos com a nuvem. Na Seção 3, apresenta-se o cenário do problema solucionado com o estudo de caso do artigo. A formulação da solução é o foco da Seção 4 e a Seção 5 discute o estudo de caso em detalhes para a autenticação no ambiente em nuvem, servidores, bancos de dados e aplicações nativas da nuvem. Por fim, na Seção 6 conclui-se o trabalho e enumera-se ações futuras de evolução do estudo para outros cenários.

2. Trabalhos Relacionados

A computação em nuvem é cada vez mais importante para cumprir os requisitos organizacionais de colaboração entre os diferentes departamentos de uma organização ou entre várias organizações. As organizações são obrigadas a guardar dados ou informações em um ambiente de fácil acesso pelos interessados ou pessoas autorizadas [I. et al., 2017]. Para minimizar os riscos de privacidade e segurança em serviços web na nuvem, as organizações precisam de um sistema de gerenciamento de identidades (IdM) forte, flexível, escalável e responsável [Sharma et al., 2015, Singh e Chatterjee, 2015]. Os provedores de serviços de nuvem (CSPs) fornecem serviço de gerenciamento baseado em acesso por identidade para os clientes em sua infraestrutura de nuvem. As questões de

perda de controle e transparência são criadas ao armazenar e processar informações de identidade por terceiros ou fora dos limites organizacionais [I. et al., 2017].

Os serviços web na nuvem confirmam a identidade dos usuários para fornecer gerenciamento de segurança e experiência de usuário personalizada em ambientes com várias nuvens [Nicanfar et al., 2014]. Os protocolos *Single Sign On* (SSO) são integrados em serviços web para acessar vários serviços a qualquer momento pelos usuários finais dos provedores de identidade. Os provedores de identidade (*Identity Providers* - IdPs) utilizam ferramentas de integração que permitem aos desenvolvedores implementar o SSO em poucos minutos [Lewis e Lewis, 2009]. A linguagem de marcação para asserção de segurança 2.0 (*Security Assertion Markup Language 2.0* - SAML 2.0) é uma das principais ferramentas para o mecanismo de autenticação única de domínio cruzado. SAML é um padrão aberto baseado em XML (*Extensible Markup Language*) que é usado para trocar autenticação e informações de autorização de um sistema de gerência de identidade para a aplicação de destino. A autenticação é realizada através de um *token* de segurança que não armazena as informações da credencial do usuário, mas garante ao provedor de serviço a capacidade de verificar com o provedor de identidade os metadados relativos à identificação do usuário.

Os protocolos existentes para SSO são, principalmente, o SAML e o Open ID, que sofrem de vulnerabilidades na autenticação. Wang formalizou um modelo de sistema baseado em identidade para o gerenciamento de certificados, melhorando a flexibilidade e a eficiência para realizar a verificação privada, a verificação pública e a verificação delegada com base na autorização do cliente [Wang, 2015]. Indu e Anand propõem extensões para o SAML 2.0 a fim de adotar diferentes métodos de controle de acesso em conjunto com o SAML 2.0, como controle de acesso discricionário, controle de acesso baseado em papéis e controle de acesso baseado em atributos [Indu e Anand, 2016]. Celesti *et al.* propõem a integração do padrão de identificação SAML 2.0 com o protocolo extensível de mensagens e presença (*eXtensible Messaging and Presence Protocol* – XMPP) para adequar o padrão ao cenário de Internet das Coisas [Celesti et al., 2017]. Hernandez *et al.* propõem um mecanismo de autenticação e autorização leve para incorporar a funcionalidade de autenticação e autorização em objetos inteligentes restritos [Hernández-Ramos et al., 2015]. Outros trabalhos realizam pesquisas sobre diferentes arquiteturas de federação de nuvem e suas avaliações com base em suas propriedades funcionais e não funcionais para o tratamento de tráfego e evidenciam a demanda recente da federação de nuvens [Assis e Bittencourt, 2016, Kritikos et al., 2017].

Sistemas de nuvem federada são instâncias de sistemas distribuídos e, portanto, incorporam muitos aspectos fundamentais da computação distribuída que geralmente diferem nas propriedades de organização, acesso e escala. Com base nessas propriedades, Lee identifica seis modelos de implantação de federação: i) federação simples emparelhada, ii) federação hierárquica, iii) centralização em uma terceira parte confiável, iv) federações distribuídas e federações ponto a ponto, v) federações com intermediários, *proxies* ou *gateways* e vi) federação entre nuvens. Embora os casos de uso de federação possam diferir em seu escopo e escala de operação, todos compartilham o requisito de um provedor de identidade de terceiros (IdP) emitindo credenciais para um usuário, que um provedor de serviços (SP) deve validar antes de conceder acesso ao usuário [Lee, 2016].

Este trabalho, por sua vez, foca no gerenciamento de identidade entre serviços

distintos de nuvens e apresenta o estudo de caso da integração do provedor de identidade do Google para o controle de acesso em um ambiente de desenvolvimento e produção da AWS. Vale ressaltar que a federação das identidades providas pelo Google no ambiente Amazon é de amplo interesse comercial e permite uma melhor gestão do controle de acesso dos usuários de serviço Amazon, já que os privilégios de acesso passam a serem associados à conta Google pessoal em contraposição a identidades de grupo usadas para o gerenciamento de serviços Amazon.

3. O problema da Identificação na Nuvem

Em grandes organizações, a gestão da identidade dos colaboradores, parceiros, clientes e fornecedores é um grande desafio que permeia diversas setores, como Recursos Humanos, Tecnologia da Informação, Operações, Segurança e Conformidade. Sempre que há uma alteração no quadro de pessoas, é necessário alterar seu nível de acesso aos diversos sistemas e ambientes da empresa, sendo os dois eventos de alteração mais importantes a admissão e a demissão ou, no caso de não funcionários, o início e o término da relação contratual. Nesses eventos, torna-se necessário a gestão dos acessos e permissões dos usuários em todos os sistemas e seções da empresa, assim como a correta remoção em todos os pontos no momento do término da relação contratual. Essa obrigatoriedade é fundamental para garantir a segurança da organização e se configura um desafio enorme, que cresce com o aumento do número de colaboradores e de sistemas. Outro ponto importante de se destacar é que muitas vezes, por simplicidade de configuração, o controle de acesso a serviços críticos da organização é realizado por senhas de grupo, não identificando o real usuário. A senha de grupo, em especial, é crítica no momento de desligamento de um dos colaboradores que a conhece, pois a revogação do acesso do colaborador desligado implica a mudança da credencial de acesso do grupo.

Quando se adiciona a velocidade de inovação que os ambientes em nuvem proporcionam e a integração de todas as equipes que os métodos ágeis pregam,a gestão de identidade se torna ainda mais desafiadora, pois as aplicações, servidores, bancos de dados são mais voláteis e exigem um processo rápido e automatizado para garantir tanto o acesso de todos os colaboradores que precisam acessar um ambiente que acabou de ser criado quanto a revogação imediata em todos os ambientes de um colaborador que foi desligado.

4. A Solução de Gerenciamento de Identidades em Ambientes em Nuvens

A solução para esse cenário é garantir que a gestão dos acesso utilize uma entidade centralizada para gerir a identidade dos colaboradores e conectar esta entidade aos diversos sistemas e recursos da organização. Dessa forma, pode-se realizar os eventos de controle de acesso e permissões na entidade centralizada e ter a certeza de que este evento foi propagado para os diversos sistemas da organização, garantindo a segurança da informação e a conformidade. Diversas possibilidades podem ser utilizadas para atingir esse objetivo. Considerando-se ambientes em nuvem, pode-se utilizar soluções baseadas em *Active Directory*, seja em modelo replicado na nuvem ou através do Serviços de Federação do *Active Directory* (AD FS) ou, ainda, por soluções genéricas que utilizem a linguagem *Security Assertion Markup Language* (SAML) 2.0.

Este artigo apresenta um estudo com avaliação qualitativa da utilização de recursos em nuvem da *Amazon Web Services* (AWS) conectado para autenticação de login

único com o *Google Suite*, usando o protocolo SAML 2.0. Através da solução, é possível utilizar os usuários do *Google Suite* para autenticação nos ambientes em nuvem da AWS, bem como nos diversos recursos criados na solução, como servidores, bancos de dados e estruturas de diretórios e arquivos. Além disso, a solução analisada ainda apresenta um registro para auditoria de todos os acessos a qualquer dos recursos em tempo real, para garantir rastros de acesso e utilização necessários para conformidade com diversas certificações e regulações, como por exemplo o *Payment Card Industry – Data Security Standard* (PCI-DSS) e o *Health Insurance Portability and Accountability Act* (HIPAA), obrigatórios para empresas globais nos mercados financeiro e de saúde.

5. Avaliação Qualitativa

Nesta Seção, são apresentados os elementos da análise qualitativa apresentados no estudo de caso de autenticação em ambiente em nuvem da AWS utilizando usuários federados do *Google Suite*. A Seção5.1 apresenta a solução para conexão do ambiente de gerenciamento da AWS através de usuários do Provedor de Identidade do Google. Na Seção 5.2, apresenta-se a conexão nos servidores virtuais e na Seção 5.3, a autenticação em bases de dados MySQL e PostgreSQL em ambiente AWS. Por fim, a Seção 5.4 mostra como a solução pode ser estendida para qualquer aplicação construída sobre a nuvem da *Amazon Web Services* (AWS) e garantir que a Organização possa gerenciar facilmente seus usuários, acessos e permissões.

É importante ressaltar que, em todos os cenários apresentados nesta Seção, os acessos são registrados em *logs* de auditoria em tempo real usando o serviço *AWS Cloudtrail*. Este serviço registra todas as chamadas às APIs da AWS, possibilitando um rastro completo dos usuários que acessaram quaisquer recursos em cada momento. Por registrar todas as chamadas à API e as credenciais usadas serem sempre temporárias, é possível, inclusive, estimar o tempo em que o usuário ficou conectado, uma vez que todas as chamadas para renovação da chave de acesso são também registradas.

O registro de auditoria é armazenado em arquivos de texto no formato JSON dentro do ambiente de armazenamento do serviço Amazon S3, que é barato, durável e com espaço de armazenamento ilimitado. Dessa forma, por serem arquivos estruturados, é possível utilizar ferramentas de análise de dados para realizar consultas nos dados e responder perguntas das equipes de segurança. A estrutura mais simples que pode ser criada é a utilização do serviço Amazon Athena para realizar consultas SQL nestes arquivos. O Amazon Athena é um produto da AWS que encapsula o Apache Presto', solução de código aberto.

5.1. Conexão da AWS com o Google Suite

A solução cria um Provedor de Identidade (IdP) SAML no serviço de Identidade e Gerenciamento de Acesso da AWS (*Identity and Access Management* - IAM) para estabelecer a relação de confiança com o Provedor de Identidade (IdP) do Google (Google IdP), permitindo que os usuários do *Google Suite* da organização possam acessar o console de gerenciamento da conta da AWS. O processo é iniciado com o administrador da conta da AWS delegando a responsabilidade pela autenticação para o IdP confiável, no caso o Google Suite, e usa SAML 2.0. Esta configuração permite que um papel do IAM (*role*) obtenha as permissões do usuário federado para se autenticar no Console de Gerenciamento da Conta AWS e acessar os recursos.

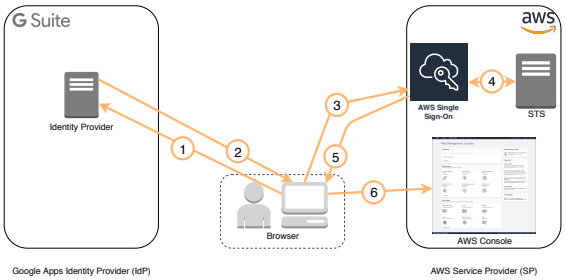

Figura 1. Diagrama da estratégia proposta para autenticação na AWS com usuário do *Google Suite*

Após a configuração da solução apresentada, o processo seguirá os passos enumerados na Figura 1:

1. O usuário federado clica no botão de conexão com a AWS dentro do seu painel de aplicativos federados na conta do *Google Suite*. Se o usuário não estiver autenticado no Google, será redirecionado para o portal de autenticação do *Google Suite*.
2. O portal autentica as credenciais do usuário do *Google Suite* e gera a resposta de autenticação SAML, que inclui as validações que identificam o usuário e atributos relevantes sobre o usuário. Essa resposta é enviada para o navegador do usuário.
3. O navegador do usuário redireciona para o ponto de conexão do *AWS Single Sign-On* e envia as validações do SAML recebidas do provedor de identidade.
4. AWS chama a interface do *AssumeRoleWithSAML* para solicitar credenciais seguras de acesso temporário e cria um endereço específico do Console de Gerenciamento usando essas credenciais temporárias.
5. AWS envia a URL de acesso para o navegador do usuário.
6. Navegador do usuário redireciona para o Console de Gerenciamento da Conta AWS. Observa-se que se o usuário tiver múltiplos papéis de acesso, é apresentada uma janela para que o usuário selecione o papel que deseja utilizar no acesso.

Da perspectiva do usuário federado, o processo ocorre transparentemente: o usuário inicia a partir do portal do *Google Suite* e termina no Console de Gerenciamento da AWS, sem ter que fornecer nenhum novo usuário e senha. As políticas de permissão associadas ao papel que o usuário assumiu determinam quais as suas permissões no console da AWS.

5.2. Autenticação para Servidores Virtuais

Enquanto ferramentas de Infraestrutura como Código (IaC), como *Chef* e *Puppet*, têm se tornado comuns na indústria para configuração de servidores, é frequentemente necessário que os usuários administradores acessem os servidores para ajustes finos, consultar *logs* de sistema ou mesmo inspecionar e localizar falhas nas aplicações. Para isso, a ferramenta mais comum para conectar em servidores Linux é o *Secure Shell* (SSH), que foi criado em 1995 e está instalado em quase todas as distribuições Linux.

Ao conectar nos servidores via SSH, chaves de acesso podem ser utilizadas para conceder autorização individual para cada usuário. Como resultado, as empresas têm que armazenar, compartilhar, gerenciar acesso e manter essas chaves de SSH para cada um dos usuários, além de renová-las e revogá-las para evitar acessos não autorizados.

Em alguns cenários, servidores bastiões são utilizados e ajudam a limitar a superfície de ataque dos servidores a apenas um único ponto de entrada. Esses servidores podem prover registro de atividades e adicionar camadas adicionais de segurança de rede. No entanto, os servidores bastiões trazem novos desafios, pois é necessário manter as chaves de cada usuário instaladas, lidar com as rotações de chaves e ter certeza de que o servidor bastião estará sempre disponível e seguro.

Quando se utiliza a nuvem da AWS, é possível utilizar o serviço *Amazon EC2 Instance Connect*, que é estudado nesta avaliação, para se conectar nos servidores virtuais sem precisar realizar todo o processo de gestão, distribuição e renovação das chaves. O serviço simplifica o desafio de gerenciar as chaves SSH e o servidor bastião enquanto possui os benefícios abaixo, que melhoram a segurança de todo o ambiente.

Controle de Acesso Centralizado. Provê controle de acesso centralizado a todos os servidores virtuais com granularidade de configuração por servidor e por usuário. As políticas de permissões do serviço IAM removem a necessidade de compartilhar e gerenciar os pares de chaves de SSH.

Chaves Temporárias de Vida Curta. As chaves SSH não são persistentes nos servidores virtuais, pois são efêmeras em sua natureza, uma vez que são acessíveis pela instância no momento que o usuário conecta, tornando fácil o fornecimento ou a revogação do acesso em tempo real. Além disso, permite que a organização deixe de usar chaves de longa duração, que são arriscadas, adotando chaves de uso único geradas no momento em que o usuário se conecta com o servidor. Essa abordagem elimina a necessidade de rastrear e manter as chaves de acesso.

Auditável. Todas as conexões dos usuários aos servidores usando o *EC2 Instance Connect* são registradas pelo serviço *AWS CloudTrail*, que provê a visibilidade necessária para manter a conformidade com regulações e certificações que a organização esteja submetida, facilmente auditando todas as requisições de conexão.

Acesso Ubíquo. A usabilidade é simples, pois é possível usar os clientes de SSH já existentes. Além disso, para facilitar as comunicações de rede, a conexão pode ser feita através de um cliente SSH baseado em navegador Web, dentro do Console de Gerenciamento do Serviço EC2 da AWS, responsável pela gestão dos servidores virtuais.

Quando o serviço está habilitado no servidor virtual, o serviço do SSH (sshd) é configurado para utilizar um *script* personalizado para a ação *AuthorizedKeysCommand*. Este *script* fornecido pela Amazon Web Services (AWS) obtém as chaves públicas para este servidor através dos metadados da instância durante o processo de autenticação SSH. Os metadados da instância são um recurso disponível em todas as instâncias na AWS em que a infraestrutura disponibiliza informações relevantes do servidor, como, por exemplo, a região em que está alocado e o tamanho da instância, dentro deste servidor através da consulta a uma URL em uma rede especial de controle.

As chaves públicas do SSH ficam disponíveis nos metadados da instância para uso único por até 60 segundos. A conexão somente é bem-sucedida se o usuário se conectar à instância dentro dessa janela de tempo após o envio da chave pública para o servidor virtual. Como a chave expira automaticamente, não existe a necessidade de rastrear ou gerenciar as chaves diretamente, como é necessário sem o uso da ferramenta.

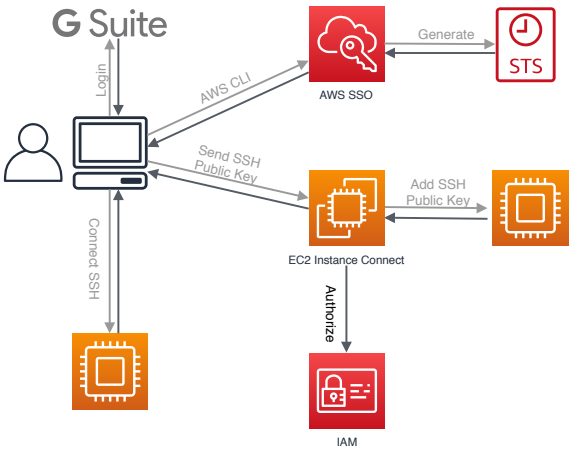

Figura 2. Diagrama da estratégia proposta para autenticação em servidores virtuais hospedados na AWS com usuário do Google Suite

A configuração do serviço é simples e envolve permitir que um usuário IAM possa enviar suas chaves públicas de SSH para os servidores virtuais. Isso é feito incluindo essa permissão às políticas de acesso do usuário criado a partir da autenticação SAML 2.0 realizada na integração com o *Google Suite*.

Para instâncias Amazon Linux 2, quando solicitado o nome do usuário de sistema, utiliza-se *ec2-user* para que os metadados da instância utilizados na conexão sejam disponibilizados corretamente para este usuário no sistema operacional, necessário para a validação no momento da autenticação do SSH. Após essas configurações, basta conectar usando qualquer cliente SSH normalmente seguindo os passos abaixo ou a interface em navegador oferecida pela AWS.

1. Gera-se um novo par de chaves pública e privada, respectivamente $mynew\_key$ e $mynew\_key.pub$
2. Usa-se o comando abaixo para autorizar o usuário do perfil AWS na seu computador e distribuir sua nova chave pública do SSH para o servidor virtual.

```
$ aws ec2-instance-connect send-ssh-public-key \
--region us-east-1 --instance-id INSTANCEID \
--availability-zone us-east-1a \
--instance-os-user ec2-user \
--ssh-public-key file://mynew_key.pub
```

3. Após a distribuição, a chave pública é disponibilizada nos metadados do servidor virtual por 60 segundos. Durante este tempo, o usuário deve conectar ao servidor usando a chave privada associada.

```
$ ssh -i mynew_key INSTANCEIP
```

Para cada tentativa de conexão, é possível visualizar os detalhes deste evento, que incluem marcações de data e hora, o identificador da instância, nome do usuário no sistema operacional e a chave pública utilizada. Essas informações são registradas dentro do AWS CloudTrail quando a chamada *SendSSHPublicKey* é acionada. Caso o serviço EC2 Instance Connect esteja em uso, é possível visualizar os registros dos usuários realizando

esta operação de API para enviar as chaves públicas de SSH para o servidor de destino e realizar a conexão em até 60 segundos.

Dessa forma, o serviço EC2 Instance Connect, aliado a integração dos usuários do IAM com o Google Suite apresentada na Seção 5.1, oferece um método inteligente e seguro de gerenciamento de chaves SSH de acesso aos servidores, incluindo um serviço nativo de auditoria com o CloudTrail. A integração com o *Google Suite*, os metadados dentro dos servidores e as chaves de curta duração apresentam uma forma segura de acesso aos servidores, garantindo sempre que apenas os usuários com a devida autorização tenham seus acessos autorizados e evitando, inclusive, vazamentos de senhas e chaves de acesso por funcionários já demitidos.

5.3. Autenticação para Bancos de Dados MySQL e PostgreSQL

Outro componente importante da infraestrutura de tecnologia da informação das empresas são os bancos de dados (BD), cuja proteção do acesso e autorização a cada uma das bases de dados é fundamental na garantia da privacidade dos dados das empresas. No contexto do estudo de caso apresentado neste artigo, é possível autenticar nos servidores de banco de dados usando a base de dados para autenticação do Gerenciamento de Identidade e Acesso (*Identity and Access Management - IAM*) da AWS em bancos de dados MySQL e PostgreSQL. Com esse método de autenticação, não é necessário usar uma senha para conectar em uma instância de BD. Considerando o cenário completo exposto no estudo caso, os usuários do Google Suite da organização podem também ser utilizados para acessos aos bancos de dados, uma vez que estão vinculados ao IAM da AWS.

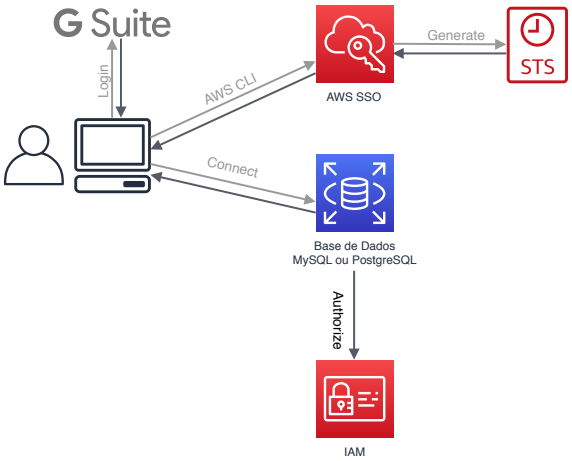

Figura 3. Diagrama da estratégia proposta para autenticação em bases de dados MySQL ou PostgreSQL hospedadas e gerenciadas na AWS com usuário do Google Suite

Para o banco de dados, ao invés das credenciais de usuário e senha tradicionais, utiliza-se um *token* de autenticação, que é uma sequência única de caracteres que o serviço Amazon RDS gera sob demanda. Os *tokens* de autenticação são gerados usando o método AWS Signature Version 4 e cada *token* tem uma vida útil de 15 minutos. Dessa forma, não é necessário guardar credenciais de usuário na base de dados porque a autenticação é gerenciada externamente usando o IAM, que por sua vez está vinculado via protocolo SAML com o *Google Suite*.

A utilização da base de dados de autenticação da AWS provê os seguintes benefícios:

1. O tráfego de rede entre base de dados e os servidores é encriptado usando *Secure Sockets Layer* (SSL).
2. É possível usar a base de dados de usuários da AWS para gerenciar centralizadamente o acesso aos seus recursos de base de dados, em vez de fazer tal gerenciamento individualmente a partir de cada instância de base de dados.
3. Para aplicações em execução nos servidores virtuais da AWS, usando o serviço Amazon EC2, pode-se usar credenciais de perfil específicas de sua instância para acessar sua base de dados em vez de uma senha.

Para habilitar a autenticação do banco de dados via o IAM, deve ser ativada a opção durante a criação do servidor e criar uma política de acesso dando permissões para os usuários o acesso ao servidor de banco de dados criado.

Com as políticas de acesso, os usuários do IAM assumem papéis de acesso dentro do banco de dados, sendo possível definir também quais bases de dados, tabelas, visualizações, entre outros recursos, determinado usuário terá acesso. Assim, se, por exemplo, um servidor de banco de dados possui duas bases de dados, o usuário acessará apenas aquela cujo acesso lhe for concedido.

Para acessos às bases de dados através de um outro serviço de programação da AWS, é possível utilizar a funcionalidade de geração de *tokens* de autenticação temporário, associado aos servidores ou contêineres para se conectar ao Amazon RDS, evitando que credenciais de usuário sejam adicionadas nos códigos fontes ou nas aplicações, o que leva ao benefício de rotações automáticas de senhas. As ferramentas de desenvolvimento que a AWS fornece para as diversas linguagens de programação suportam essa funcionalidade, facilitando o desenvolvimento de aplicações seguras.

5.4. Autenticação para Aplicações dentro da conta da AWS

A solução de autenticação única pode ser estendida para todas as aplicações construídas na nuvem e, não somente ao ambiente em nuvem, aos servidores e aos bancos de dados. É também possível utilizar os recursos do IAM para oferecer acesso aos usuário federados a partir do Google Suite, utilizando a mesma estrutura de Políticas de Permissões que foram usados para garantir acesso aos servidores virtualizados e às bases de dados. No entanto, a solução pode ser utilizada de forma mais ampla, envolvendo, inclusive, as aplicações criadas dentro da estrutura da Amazon Web Services. Nesta Seção, apresenta-se a análise da solução de dados federados para uma aplicação Web criada sobre a conta da AWS utilizando serviços de computação, armazenamento de arquivos e Gateway de API.

O cenário abaixo descreve um serviço simples Web que utiliza uma estrutura de *gateway* de API e funções AWS Lambda para processamento das requisições, de tal maneira que o retorno da função Lambda é o corpo da resposta do *gateway* de API. Nesse contexto, é possível adicionar um usuário ou papel do IAM da AWS para fazer a autenticação desse serviço Web. Como os usuários, no estudo de caso em questão, estão integrados ao *Google Suite*, o usuário é o responsável pelas chamadas de API das aplicações criadas.

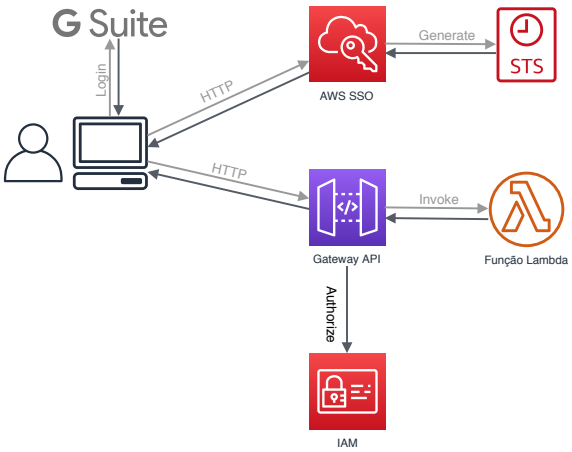

Figura 4. Diagrama da estratégia para autenticação com usuário do *Google Suite* em aplicações da Organização criadas em ambiente da nuvem da AWS

A forma como os clientes acessam os serviços web é através da geração de uma chave temporária de acesso a essa API fornecida pela aplicação, usando o serviço *AWS Secure Token Service*, integrado ao *Google Sign-in*. Dessa forma, é possível utilizar as credenciais de acesso do *Google Suite* para autorizar a conexão em qualquer aplicativo construído sobre a AWS usando o *gateway* de API, que pode ser posicionado na frente como *proxy* de qualquer aplicação Web.

6. Conclusão

A gestão dos usuários e dos acessos é um desafio cada vez maior nas organizações, sobretudo em cenários de maior rotatividade de colaboradores. Uma falha na revogação de acesso a um ambiente pode deixar vulnerável os servidores, as aplicações e os dados da organização. Esse artigo apresentou um estudo de caso de cenário que pode ser implementado através do uso da nuvem da *Amazon Web Services* (AWS) com o diretório de usuário do *Google Suite*, implementando o mecanismo de *Single Sign-on atavés* da SAML 2.0.

Nesse estudo de caso, apresentou-se a solução para a autenticação através dos usuários do *Google Suite* para todo o ambiente em nuvem, incluindo o acesso ao ambiente de configuração da nuvem da AWS, aos servidores virtuais no ambiente, aos bancos de dados MySQL e PostgreSQL disponibilizados na nuvem e também para aplicações construídas dentro da nuvem utilizando recursos computacionais oferecidos como serviços, como *gateways* de API.

Dessa forma, o principal benefício da solução é a agilidade e garantia de atualização na gestão das identidades e acessos dos sistemas da corporação. Isso é importante para assegurar a privacidade das informações confidenciais e, sobretudo após as vigências das leis de proteção de dados no mundo, se torna significativo no retorno financeiro das corporações, pois as leis preveem muitas altas em caso de vazamento ou acesso não autorizado aos dados.

Como trabalhos futuros, pode-se citar a construção de estudo de caso utilizando o diretório de usuários da Microsoft, o *Active Directory* ou o Serviço de Federação do *Active Directory* (AD FS). Além disso, é previsto expandir o estudo de caso para soluções

de redes híbridas entre o cenário na nuvem e e um centro de dados tradicional, além de integrar a autenticação com aplicações móveis corporativas.

Referências

[Assis e Bittencourt, 2016] Assis, M. e Bittencourt, L. (2016). A survey on cloud federation architectures: Identifying functional and non-functional properties. *Journal of Network and Computer Applications*, 72:51 – 71.

[Celesti et al., 2017] Celesti, A., Fazio, M. e Villari, M. (2017). Enabling secure xmpp communications in federated iot clouds through xep 0027 and saml/sasl sso. *Sensors*, 17(2).

[Hernández-Ramos et al., 2015] Hernández-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F. e Ladid, L. (2015). Toward a lightweight authentication and authorization framework for smart objects. *IEEE Journal on Selected Areas in Communications*, 33(4):690–702.

[I. et al., 2017] I., I., P.M., R. A. e Bhaskar, V. (2017). Encrypted token based authentication with adapted saml technology for cloud web services. *Journal of Network and Computer Applications*, 99:131 – 145.

[Indu e Anand, 2016] Indu, I. e Anand, P. M. R. (2016). Hybrid authentication and authorization model for web based applications. Em *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, p. 1187–1191.

[Kritikos et al., 2017] Kritikos, K., Kirkham, T., Kryza, B. e Massonet, P. (2017). Towards a security-enhanced paas platform for multi-cloud applications. *Future Generation Computer Systems*, 67:206 – 226.

[Lee, 2016] Lee, C. A. (2016). Cloud federation management and beyond: Requirements, relevant standards, and gaps. *IEEE Cloud Computing*, 3(1):42–49.

[Lewis e Lewis, 2009] Lewis, K. D. e Lewis, James E., P. (2009). Web single sign-on authentication using saml. *International Journal of Computer Science Issues (IJCSI)*, 2:41–48.

[Mattos et al., 2019] Mattos, D. M. F., Velloso, P. B. e Duarte, O. C. M. B. (2019). An agile and effective network function virtualization infrastructure for the Internet of Things. *Journal of Internet Services and Applications*, 10(1):6.

[Nicanfar et al., 2014] Nicanfar, H., Jokar, P., Beznosov, K. e Leung, V. C. M. (2014). Efficient authentication and key management mechanisms for smart grid communications. *IEEE Systems Journal*, 8(2):629–640.

[Sharma et al., 2015] Sharma, A., Sharma, S. e Dave, M. (2015). Identity and access management- a comprehensive study. Em *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, p. 1481–1485.

[Singh e Chatterjee, 2015] Singh, A. e Chatterjee, K. (2015). Identity management in cloud computing through claim-based solution. Em *2015 Fifth International Conference on Advanced Computing Communication Technologies*, p. 524–529.

[Wang, 2015] Wang, H. (2015). Identity-based distributed provable data possession in multicloud storage. *IEEE Transactions on Services Computing*, 8(2):328–340.