Navegando na conformidade com a LGPD na AWS

Março de 2020

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento (a) é fornecido apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no "estado em que se encontram", sem qualquer garantia, declaração ou condição de qualquer tipo, explícita ou implícita. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.

Índice

Resumo

Este documento fornece informações sobre serviços e recursos que a Amazon Web Services (AWS) oferece aos clientes a fim de ajudá-los a estabelecer o alinhamento com os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira que possam ser aplicáveis a suas atividades. Isso inclui aderência a padrões de segurança de TI, controles de acesso a dados, ferramentas de monitoramento e registro em log, criptografia, além de gerenciamento de chaves.

Visão geral da Lei Geral de Proteção de Dados brasileira

A Lei Geral de Proteção de Dados Pessoais brasileira (Lei n.º 13.709 de 14 de agosto de 2018, alterada pela Lei n.º 13.853 de 8 de julho de 2019) ou LGPD é a primeira regulamentação abrangente de proteção de dados do Brasil e está amplamente alinhada ao General Data Protection Regulation (GDPR – Regulamento Geral sobre a Proteção de Dados) da Europa. A LGPD entrará em vigor em agosto de 2020. A LGPD é aplicável a qualquer operação de processamento de *dados pessoais* (definidos como informações relacionadas a uma pessoa física identificada ou identificável) executada por indivíduos ou pessoas jurídicas do setor público ou privado, independentemente do meio usado para o processamento ou o país no qual o controlador ou os dados estejam localizados, desde que: 1) a operação de processamento seja executada no Brasil; 2) a atividade de processamento tenha como finalidade oferecer ou fornecer bens ou serviços a indivíduos no Brasil; ou 3) os dados pessoais tenham sido coletados no Brasil.

A LGPD instituiu uma agência de proteção de dados, a Autoridade Nacional de Proteção de Dados (ANPD), que supervisiona a proteção de dados pessoais e publica regulamentações e procedimentos relacionados à proteção de dados pessoais. Até a data de publicação do presente documento, os membros da ANPD ainda não haviam sido indicados.

Mudanças que a LGPD introduz para organizações que operam no Brasil

Ao estabelecer regras para a coleta, uso, processamento e armazenamento de dados pessoais, a LGPD transformou significativamente o sistema de proteção de dados no Brasil. As organizações precisam ter a capacidade de demonstrar continuamente a segurança dos dados que estão processando e a aderência à LGPD, implementando e revisando frequentemente medidas técnicas e organizacionais robustas. Isso exige a definição e a aplicação de políticas compatíveis aplicáveis ao processamento de dados pessoais. Quem violar a LGPD pode estar sujeito a diversas penalizações, entre elas: avisos, suspensão ou bloqueio das atividades de processamento que violam a lei, além de multas de até 2% da receita bruta do infrator no Brasil no ano anterior, com o valor máximo de 50 milhões de reais.

Sob a LGPD, controladores e processadores (conforme definidos na LGPD) precisam adotar medidas de segurança, tanto técnicas quanto administrativas, para proteger dados pessoais contra acesso não autorizado, situações acidentais ou ilegais de destruição, perda, alteração, comunicação ou qualquer tipo de processamento inadequado ou ilegal. Além disso, a LGPD concede à ANPD a autoridade para estabelecer padrões técnicos mínimos que devem ser

implementados por controladores e processadores. Por ocasião da redação deste texto, a ANPD ainda não publicou esses padrões técnicos mínimos.

Preparação da AWS para a LGPD

Os especialistas em conformidade, proteção de dados e segurança da AWS têm trabalhado com clientes em todo o mundo para responder dúvidas e ajudá-los a se preparar para a execução de cargas de trabalho na nuvem após a LGPD entrar em vigor. Essas equipes também estão revisando as operações e as responsabilidades da AWS em relação aos requisitos da LGPD a fim de garantir que os serviços da AWS possam ser usados em conformidade com a LGPD assim que a lei entrar em vigor.

Função da AWS segundo a LGPD

De acordo com a LGPD, a AWS pode atuar tanto como um *controlador de dados* quanto como um *processador de dados*. Na LGPD, um *controlador de dados* é definido como a pessoa física ou jurídica, pública ou privada, que é responsável por decisões relacionadas ao processamento de dados pessoais. Na LGPD, um *processador de dados* é definido como a pessoa física ou jurídica, pública ou privada, que executa o processamento de dados pessoais em nome do controlador.

A AWS como um controlador de dados

Quando a AWS coleta dados pessoais e determina os fins e os meios de processamento desses dados pessoais (por exemplo, quando a AWS coleta e armazena informações de seus clientes diretos para registro de contas, administração, acesso a serviços, atributos de serviço ou informações de contato para a conta da AWS com o objetivo de fornecer auxílio por meio de atividades de suporte ao cliente), ela atua como um controlador de dados.

A AWS como um processador de dados

Quando clientes e provedores de soluções da AWS usam os serviços da AWS para processar dados no conteúdo de seus respectivos clientes, a AWS atua como um processador de dados. Clientes e provedores de soluções da AWS podem usar os controles disponíveis nos serviços da AWS, inclusive controles de configuração de segurança, para processar e armazenar dados pessoais. Nessas circunstâncias, o próprio cliente ou parceiro do APN pode atuar como um controlador de dados ou processador de dados, e a AWS atua como um processador ou um subprocessador de dados.

Modelo de responsabilidade compartilhada de segurança

Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Quando o cliente transfere seus dados e sistemas de computação para a nuvem, as responsabilidades de privacidade e segurança são compartilhadas entre o cliente e o provedor de serviços de nuvem. Quando os clientes migram para a Nuvem AWS, a AWS é responsável pela proteção da infraestrutura subjacente que oferece suporte à nuvem, e os clientes são responsáveis por tudo aquilo que colocam na nuvem ou conectam à nuvem. Normalmente essa diferenciação da responsabilidade é mencionada como segurança *da* nuvem vs. segurança *na* nuvem.

Esse modelo compartilhado pode ajudar a reduzir a carga operacional do cliente e oferecer a flexibilidade e o controle necessários para implantar a infraestrutura dele na Nuvem AWS. A AWS opera, gerencia e controla os componentes de infraestrutura, desde o sistema operacional de hospedagem e a camada de virtualização até a implementação de serviços com abstração e a segurança física das instalações nas quais os serviços operam. Os clientes assumem a responsabilidade e o gerenciamento pelo sistema operacional convidado (inclusive por atualizações e patches de segurança), por outros aplicativos de software associados e pela configuração do firewall do grupo de segurança fornecido pela AWS. Para mais informações, consulte o Modelo de responsabilidade compartilhada da AWS.

Solidez na estrutura de conformidade e nos padrões de segurança

A LGPD concede à ANPD a autoridade para estabelecer padrões técnicos mínimos que devem ser implementados por controladores de dados ou processadores de dados. Até a data de publicação deste documento, a ANPD não tinha estabelecido os padrões técnicos mínimos, mas a AWS já oferece aos clientes capacidades sólidas de estrutura de conformidade e segurança avançada que atendem às necessidades dos padrões modernos de segurança e conformidade em todo o mundo.

Programa de conformidade da AWS

O programa de conformidade da AWS ajuda os clientes a entender os controles robustos existentes na AWS para manter a segurança e a proteção de dados na nuvem. À medida em que os sistemas são construídos tendo a infraestrutura da Nuvem AWS como base, as responsabilidades de conformidade serão compartilhadas. Ao integrar recursos de serviços com foco em governança e facilmente auditáveis a padrões de auditoria ou conformidade aplicáveis, os capacitadores de conformidade da AWS aproveitam os programas tradicionais, ajudando clientes a estabelecerem e operarem em um ambiente de controle de segurança da AWS. A infraestrutura de TI que a AWS fornece aos seus clientes é projetada e gerenciada em total

alinhamento com as melhores práticas de segurança e diversos padrões de segurança de TI, entre eles:

- SOC 1/SSAE 16/ISAE 3402 (antigo SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP e FedRAMP (EUA)
- DoD SRG (EUA)
- IRAP (Austrália)
- MTCS nível 3 (Singapura)
- C5 (Alemanha)
- ENS High (Espanha)
- PCI DSS nível 1
- ISO 9001
- ISO/IEC 27001 / ABNT NBR ISO/IEC 27001
- ISO/IEC 27017/ABNT NBR ISO/IEC 27017
- ISO/IEC 27018/ABNT NBR ISO/IEC 27018[1]
- FIPS 140-2 (EUA e Canadá)

Além disso, a flexibilidade e o controle oferecidos pela infraestrutura da AWS permitem que os clientes implantem soluções que atendem a diversos padrões específicos dos setores.

Por meio de whitepapers, relatórios, certificações, credenciamentos e outros atestados de terceiros, a AWS fornece aos clientes uma ampla variedade de informações relacionadas ao seu ambiente de controle de TI. Para mais informações, consulte o whitepaper sobre risco e conformidade.

Controles de acesso a dados

A LGPD determina que controladores e processadores precisam adotar medidas de segurança, tanto técnicas quanto administrativas, para proteger dados pessoais contra acesso não

[1]Até a data de publicação deste whitepaper, a AWS havia apresentado o pedido, mas ainda não havia recebido a certificação oficial nas versões brasileiras desses padrões.

autorizado. Os seguintes mecanismos de controle de acesso da AWS podem ajudar os clientes a cumprir esse requisito, permitindo o acesso exclusivo de administradores, usuários e aplicativos autorizados aos recursos e aos dados do cliente na AWS:

AWS Identity and Access Management

Quando você cria uma conta da AWS, um usuário root principal é criado automaticamente para sua conta da AWS. Esse usuário principal tem acesso completo a todos os seus serviços e recursos da AWS em sua conta da AWS. Em vez de usar esse root principal para as tarefas cotidianas, você só deve usá-lo para criar inicialmente funções e contas de usuário adicionais, e para um número restrito de atividades administrativas que precisam dele. A AWS recomenda que você aplique o princípio de privilégio mínimo desde o início: defina diferentes funções e contas de usuário para diferentes tarefas, e especifique o conjunto mínimo de permissões necessário para concluir cada tarefa. O AWS Identity and Access Management (IAM) é um serviço web que você pode usar para controlar com segurança o acesso a seus recursos da AWS.

Usuários e funções definem as identidades do IAM com permissões específicas. Usuários do IAM são provisionados diretamente na AWS e fornecem um conjunto avançado de recursos e capacidades. Com funções do IAM, você pode permitir que usuários executem tarefas específicas para assumir a função e fazer uso de credenciais temporárias durante a sessão da função. É possível usar as funções do IAM para acessar sua conta usando identidades de usuário existentes por meio da SAML ou federação do OIDC, ou ainda usando o serviço AWS Single Sign-On (SSO). Você também pode usar funções para fornecer de modo seguro credenciais temporárias a aplicativos executados no Amazon Elastic Compute Cloud (Amazon EC2), Elastic Container Service (ECS) ou AWS Lambda, permitindo que esses aplicativos acessem outros recursos da AWS, como Amazon Simple Storage Service (Amazon S3 ou buckets do Amazon S3) e bancos de dados Amazon RDS ou DynamoDB.

Tokens de acesso temporário por meio do AWS STS

Você pode usar o AWS Security Token Service (AWS STS) para criar e fornecer credenciais temporárias de segurança que permitem que usuários confiáveis acessem seus recursos da AWS. As credenciais temporárias de segurança funcionam de maneira praticamente idêntica às credenciais de longo prazo que você pode fornecer aos seus usuários do IAM, com as seguintes diferenças:

- As credenciais temporárias de segurança servem apenas para uso em curto prazo. É possível configurar o tempo durante o qual elas permanecem válidas, variando de poucos minutos a várias horas. Após as credenciais temporárias expirarem, a AWS não as reconhece nem permite nenhum tipo de acesso proveniente de solicitações de API feitas com elas; e

- As credenciais temporárias de segurança não são armazenadas na conta do usuário. Em vez disso, elas são geradas de maneira dinâmica e fornecidas ao usuário mediante solicitação. Quando (ou antes de) as credenciais temporárias de segurança expirarem, o usuário poderá solicitar novas credenciais, caso tenha permissão para fazer isso.

Essas diferenças proporcionam as seguintes vantagens quando você usa credenciais temporárias:

- Não é necessário distribuir ou incorporar credenciais de segurança de longo prazo da AWS em um aplicativo;
- As credenciais temporárias são a base da federação de funções e identidades. Ao definir uma identidade temporária da AWS aos usuários, você pode permitir que eles acessem seus recursos da AWS; e
- As credenciais temporárias de segurança têm uma vida útil personalizável limitada. Por causa disso, não é necessário fazer rodízio delas ou revogá-las de maneira explícita quando não forem mais necessárias. Após a expiração das credenciais temporárias de segurança, elas não podem ser reutilizadas. É possível especificar o tempo máximo durante o qual as credenciais permanecem válidas.

Autenticação multifator

Para segurança adicional, é possível acrescentar autenticação de dois fatores ao root principal de sua conta e a contas específicas de usuário do IAM. Com a Multi-Factor Authentication (MFA – Autenticação multifator) ativada, ao acessar um site da AWS, você é solicitado a fornecer seu nome do usuário e senha (o primeiro fator), bem como uma resposta de autenticação de seu dispositivo MFA da AWS (o segundo fator). É possível ativar a MFA para sua conta da AWS e para usuários específicos do IAM criados em sua conta. Também é possível usar a MFA para controlar o acesso a APIs de serviços da AWS.

Por exemplo, é possível definir uma política que permita acesso completo a todas as operações de API da AWS no Amazon EC2, mas negue explicitamente o acesso a operações específicas de API, como *StopInstances* e *TerminateInstances*, caso o usuário não esteja autenticado com MFA.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllActionsForEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

Você pode obter resultados semelhantes mesmo que seus usuários acessem os recursos da AWS por meio de federação. Nesse caso, a autenticação multifator seria usada para fazer a autenticação no provedor de identidade. Em seguida, é possível transformar a atribuição do provedor de identidade em tags do principal no IAM e analisá-la no contexto da autorização.

Acesso a recursos da AWS

Para implementar acesso granular aos seus objetos da AWS, é possível conceder diferentes níveis de permissões a diferentes usuários para recursos diferentes. Por exemplo, é possível permitir que apenas alguns usuários tenham acesso completo ao Amazon EC2, Amazon S3, Amazon DynamoDB, Amazon Redshift e a outros serviços AWS.

Para outros usuários, você pode definir acesso do tipo somente leitura a apenas alguns buckets do Amazon S3, permissão para administrar apenas algumas instâncias do EC2 ou para acessar somente suas informações de faturamento.

A política apresentada a seguir é um exemplo de um método que você pode usar para permitir todas as ações em um bucket específico do Amazon S3 e negar explicitamente acesso a todos os serviços da AWS que não sejam o Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

É possível vincular uma política a uma função ou a uma conta de usuário. Para outros exemplos de políticas do IAM, consulte Exemplo de políticas do IAM baseadas em identidade.

Acesso a dados operacionais e de configuração

Você pode usar o AWS Systems Manager para visualizar e gerenciar as operações de sua infraestrutura da AWS. É possível auditar e obrigar a conformidade com estados definidos. O Parameter Store do AWS Systems Manager pode gerenciar centralmente parâmetros de definição de dados. Isso permite que você implemente acesso granular a dados de parâmetro, sejam eles dados em texto sem formatação (como cadeias de caracteres de banco de dados) ou segredos (como senhas). Usando permissões personalizadas, você pode fornecer esse controle de acesso a usuários e recursos (como instâncias) para acesso a parâmetros e para usar a integração com o IAM. Por exemplo, frequentemente as credenciais são integradas ao código em um ambiente de desenvolvimento. Em vez de integrar suas credenciais ao código, é possível usar o Parameter Store para salvar senhas e permitir que seus desenvolvedores obtenham acesso às credenciais usando o get-parameter de API da AWS.

O exemplo de trecho de código de API abaixo mostra o *get-parameter* para recuperação de senha:

```
Password=$(aws ssm get-parameters --region us-east-1 --names MySecureSQLPassword
```

O AWS Secrets Manager representa outra opção disponível para proteger segredos necessários para acessar seus aplicativos, serviços e recursos de TI. O serviço permite a você alternar, gerenciar e recuperar facilmente credenciais de banco de dados, chaves de API e outros segredos durante os ciclos de vida deles. Usuários e aplicativos recuperam segredos

com uma chamada para APIs do Secrets Manager, eliminando a necessidade de usar informações confidenciais integradas ao código em texto simples.

O Secrets Manager oferece rodízio de segredo com integração interna para Amazon RDS, Amazon Redshift e Amazon DocumentDB.

Restrições geográficas

Você pode usar restrições geográficas, também conhecidas como bloqueio geográfico, para evitar que usuários em locais geográficos específicos acessem conteúdo que você esteja distribuindo por meio de uma distribuição web do Amazon CloudFront.

Há duas opções para o uso de restrições geográficas:

- **Recurso de restrição geográfica do CloudFront** – os clientes podem selecionar essa opção para restringir o acesso a todos os arquivos associados a uma distribuição do CloudFront e para restringir o acesso em nível nacional.
- **Serviço de geolocalização de terceiros** – os clientes podem selecionar essa opção para restringir o acesso a um subconjunto dos arquivos que estão associados a uma distribuição ou para restringir o acesso a um nível mais detalhado de granularidade do que em nível nacional.

Além dessas duas opções, há capacidades de limitação geográfica para regiões lançadas recentemente. Por um lado, as regiões da AWS lançadas antes de 20 de março de 2019 são habilitadas por padrão. Já as regiões disponibilizadas após 20 de março de 2019, como Ásia-Pacífico (Hong Kong) e Oriente Médio (Bahrein), são desabilitadas por padrão. É necessário habilitar essas regiões antes que seja possível usá-las. Caso uma região da AWS seja desabilitada por padrão, é possível usar o Console de Gerenciamento da AWS para habilitar e desabilitar a região. A habilitação e desabilitação das regiões da AWS permitem que você controle se os usuários em sua conta da AWS podem acessar recursos na respectiva região.

Controle de acesso a aplicativos web e aplicativos móveis

A AWS oferece serviços para gerenciar o controle de acesso a dados nos aplicativos dela. Caso precise adicionar recursos de login de usuário e controle de acesso aos seus aplicativos web e aplicativos móveis, você pode usar o Amazon Cognito. Os grupos de usuários do Amazon Cognito disponibilizam um diretório seguro de usuários que pode escalar para centenas de milhões de usuários. Para proteger a identidade dos usuários, é possível adicionar a Multi-Factor Authentication (MFA – Autenticação multifator) aos seus grupos de usuários. Também é possível usar autenticação adaptativa, que emprega um modelo baseado em risco para prever quando você precisará de outro fator de autenticação.

Com o Amazon Cognito, é possível visualizar quem acessou seus recursos e a origem do acesso (aplicativo móvel ou aplicativo web). Você pode usar essa informação para criar

políticas de segurança que permitam ou neguem acesso a um recurso com base no tipo de origem do acesso (aplicativo móvel ou aplicativo web).

Monitoramento e registro em log

O monitoramento e o registro em log são elementos cruciais de uma arquitetura de segurança robusta, e a AWS oferece diversos serviços e recursos de monitoramento e registro em log, entre eles:

Gerencie e configure ativos com o AWS Config

O AWS Config oferece uma exibição detalhada da configuração atual, bem como do histórico de recursos da AWS em sua conta da AWS. Isso inclui como os recursos se relacionam entre si e como foram configurados anteriormente, permitindo que você visualize a evolução das configurações e dos relacionamentos ao longo do tempo.

Figura 1 – Use o AWS Config para monitorar as alterações de configuração ao longo do tempo

Um recurso da AWS é uma entidade com a qual você pode trabalhar na AWS, como uma instância do EC2, um volume do Amazon Elastic Block Store (Amazon EBS), um grupo de segurança ou uma Amazon Virtual Private Cloud (Amazon VPC). Para uma lista completa dos recursos da AWS compatíveis com o AWS Config, consulte
Tipos de recurso da AWS compatíveis.

Com o AWS Config, você pode:

- Avaliar as configurações de seu recurso da AWS para verificar se elas estão corretas;
- Obter um snapshot das configurações atuais dos recursos compatíveis associados à sua conta da AWS;

- Obter configurações de um ou mais recursos existentes em sua conta;
- Obter configurações históricas de um ou mais recursos;
- Receber uma notificação quando um recurso for criado, modificado ou excluído; e
- Visualizar os relacionamentos entre os recursos. Por exemplo, talvez você queira encontrar todos os recursos que usam um determinado grupo de segurança
- Executar código automaticamente por meio de regras do Config em resposta a qualquer alteração na configuração, seja notificando um administrador ou até mesmo corrigindo automaticamente qualquer alteração indesejada.

Auditoria de conformidade e análises de segurança com o AWS CloudTrail

Com o AWS CloudTrail, é possível monitorar continuamente a atividade da conta da AWS. O serviço captura um histórico de chamadas de APIs da AWS para sua conta, incluindo chamadas de APIs feitas usando o Console de Gerenciamento da AWS, os SDKs da AWS, as ferramentas da linha de comando e outros serviços de nível superior da AWS. Você pode identificar quais usuários e contas chamaram APIs da AWS para serviços que dão suporte ao CloudTrail, o endereço IP de origem dessas chamadas e quando as chamadas ocorreram. É possível integrar o CloudTrail a aplicativos usando a API, automatizar a criação de trilhas para a sua organização, verificar o status de suas trilhas e controlar como os administradores ativam e desativam o registro em log do CloudTrail. Você pode organizar e armazenar logs do CloudTrail em um bucket do Amazon S3 para fins de auditoria ou atividades de solução de problemas.

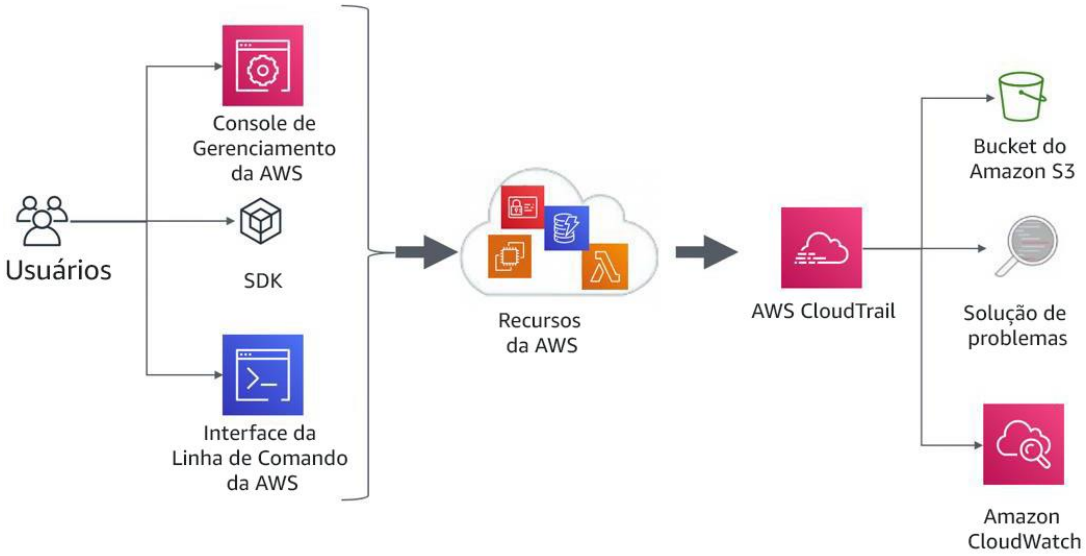

Figura 2 – Exemplo de arquitetura para auditoria de conformidade e análise de segurança com o AWS CloudTrail

Os logs do AWS CloudTrail também podem acionar eventos previamente configurados do Amazon CloudWatch. Você pode usar esses eventos para notificar usuários ou sistemas sobre a ocorrência de um evento ou para ações de correção. Por exemplo, caso deseje monitorar atividades em suas instâncias do Amazon EC2, é possível criar uma regra do CloudWatch Event. Quando uma atividade específica acontece em relação a uma instância do Amazon EC2 e o evento é capturado nos logs, a regra aciona uma função do AWS Lambda, que envia um e-mail de notificação sobre o evento (quando aconteceu, qual usuário executou a ação, detalhes do Amazon EC2 etc.) para o administrador. O diagrama a seguir mostra a arquitetura da notificação de eventos.

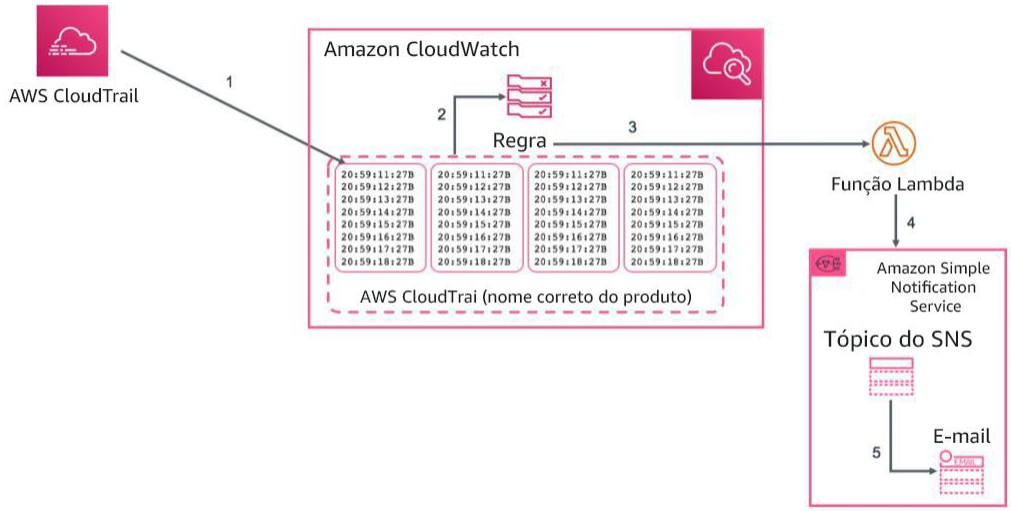

Figura 3 – Exemplo da notificação de evento do AWS CloudTrail

Outros recursos de registro em log

Além do registro de API em log do CloudTrail, há vários outros tipos e fontes importantes de log que permitem manter seu ambiente AWS seguro. Por exemplo, ao habilitar o registro em log do S3, é possível obter logs detalhados de acesso para as solicitações que são feitas ao seu bucket do Amazon S3. Um registro de log de acesso contém detalhes sobre a solicitação, como o tipo de solicitação, os recursos especificados na solicitação e a data e a hora na qual a solicitação foi processada. Para mais informações sobre o conteúdo de uma mensagem de log, consulte o formato de log de acesso a servidor do Amazon S3 no *Guia do desenvolvedor do Amazon Simple Storage Service*.

Outros tipos de fontes importantes de log além do CloudTrail e do S3 incluem:

- Informações detalhadas sobre todos os fluxos de rede em sua rede virtual por meio do VPC Flow Logs;
- Logs de solicitação de seus Elastic Load Balancers;

- Filtragem e monitoramento do acesso HTTP a aplicativos com funções do WAF no CloudFront; e
- Logs de sistema operacional reunidos centralmente e passíveis de análise usando o CloudWatch Logs e o agente de registro em log do EC2.

Os logs também são uma fonte útil de informações para a detecção de ameaças. O serviço de detecção de ameaças do GuardDuty analisa logs do AWS CloudTrail, VPC Flow Logs e AWS DNS, habilitando você a monitorar continuamente suas contas e cargas de trabalho da AWS. Esse serviço usa machine learning, inteligência de ameaças e detecção de anomalias para fornecer alertas detalhados e práticos sempre que houver o registro de uma atividade maliciosa ou comportamento não autorizado.

Gerenciamento centralizado de segurança

Muitas organizações enfrentam desafios relacionados à visibilidade e ao gerenciamento centralizado de seus ambientes. A menos que você analise seus projetos de segurança, esse desafio pode se agravar conforme sua área de alcance operacional cresce. Falta de conhecimento, com gerenciamento descentralizado e desigual de processos de governança e segurança podem tornar seu ambiente vulnerável.

A AWS fornece as ferramentas que ajudam você a abordar alguns dos requisitos mais desafiadores para gerenciamento e governança de TI, além de ferramentas para apoiar uma abordagem de proteção de dados inerente ao projeto.

O **AWS Organizations** ajuda você a gerenciar e dirigir centralmente ambientes muito complexos. Ele permite que você controle o acesso, a conformidade e a segurança em um ambiente multicontas. O AWS Organizations é compatível com a Service Control Policy (SCP – Política de controle de serviço), que define as ações de serviço da AWS disponíveis para uso com diferentes contas em uma organização.

O **AWS Control Tower** fornece um método fácil de configurar e administrar um ambiente da AWS novo, protegido e multicontas. Ele automatiza a configuração de uma landing zone, que é um ambiente multicontas baseado em diagramas de melhores práticas e habilita a governança usando proteções que você pode escolher em uma lista predefinida. As proteções implementam regras de governança para segurança, conformidade e operações. O AWS Control Tower oferece gerenciamento de identidade usando o diretório padrão do AWS Single Sign-On (SSO) e habilita a auditoria entre contas usando AWS SSO e AWS IAM. Ele também centraliza logs provenientes do Amazon CloudTrail e do AWS Config, que são armazenados no Amazon S3.

O **AWS Security Hub** é outro serviço compatível com centralização e que pode aprimorar a visibilidade de uma organização. O Security Hub centraliza e prioriza os achados de segurança e conformidade de contas e serviços da AWS, e pode ser integrado a softwares de segurança

de parceiros terceirizados visando ajudar você a analisar tendências de segurança e identificar os problemas de segurança prioritários.

O **Amazon CloudWatch Events** permite que você configure sua conta da AWS para enviar eventos a outras contas da AWS ou passar a ser uma receptora de eventos de outras contas ou organizações. Esse mecanismo pode ser bastante útil para a implementação de cenários de resposta a incidentes entre contas ao adotar ações corretivas em tempo hábil (p. ex., chamando uma função Lambda ou executando um comando na instância do EC2) conforme necessário e sempre que ocorrer um evento de incidente de segurança.

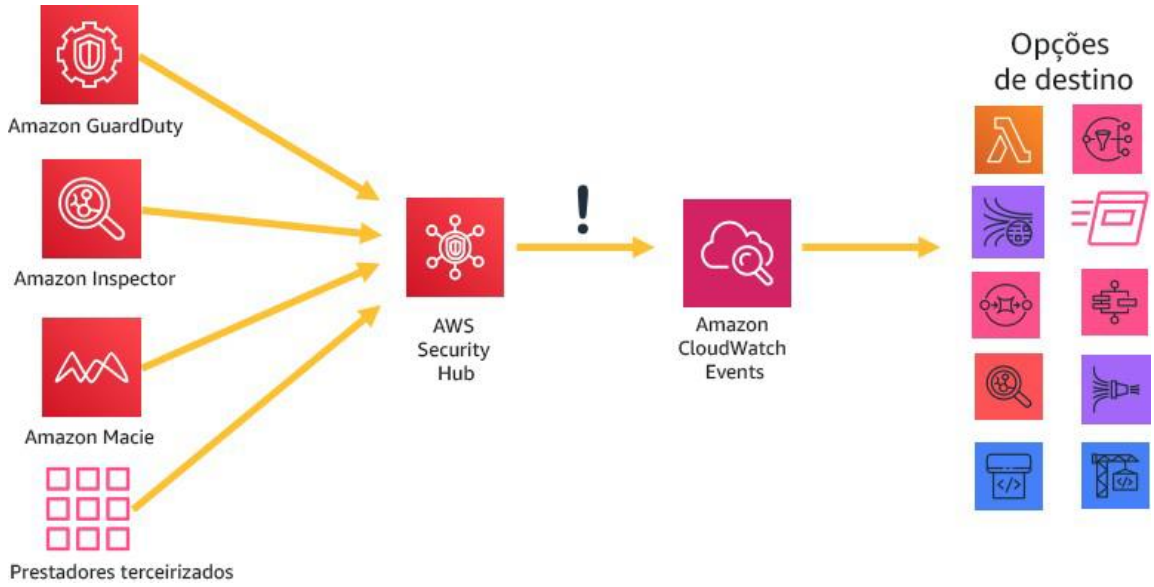

Figura 4 – Adotando medidas com o AWS Security Hub e o Amazon CloudWatch Events

Protegendo seus dados na AWS

A LGPD exige que os negócios adotem medidas de segurança técnicas e administrativas capazes de proteger dados pessoais contra acesso não autorizado ou situações acidentais ou ilegais de destruição, perda, alteração, comunicação, disseminação ou qualquer forma de tratamento inadequado ou ilegal. Nesse aspecto, a AWS oferece vários mecanismos altamente escaláveis e seguros de criptografia de dados para ajudar a proteger os dados do cliente armazenados e processados na AWS.

A criptografia reduz os riscos associados ao armazenamento de dados pessoais porque os dados não podem ser lidos sem a chave correta. Uma estratégia detalhada de criptografia pode ajudar a mitigar o impacto de vários eventos de segurança, inclusive determinados tipos de violações de segurança.

Criptografar dados em repouso

Criptografar dados em repouso é crucial para a conformidade regulatória e a proteção de dados. Isso ajuda a garantir que os dados confidenciais salvos em armazenamento persistente não sejam passíveis de leitura por nenhum usuário ou aplicativo sem a autorização adequada, que inclui uma chave válida. A AWS fornece diversas opções para criptografia em repouso e gerenciamento de chave de criptografia. Por exemplo, é possível usar o AWS Encryption SDK com uma Customer Master Key (CMK – Chave mestra do cliente) criada e gerenciada no AWS Key Management Service (AWS KMS) para criptografar dados arbitrários. Muitos serviços da AWS também oferecem criptografia automática em repouso enquanto permitem que o cliente controle, alterne ou revogue as CMKs no AWS KMS.

Os dados criptografados podem ser armazenados em repouso com segurança e só podem ser descriptografados por uma parte com acesso autorizado à CMK. Como resultado, você obtém dados confidenciais com criptografia de envelope, mecanismos de política para autorização e criptografia autenticada, além de registro de auditoria em log por meio do AWS CloudTrail. Conforme mencionado, a maioria dos serviços de armazenamento e banco de dados da AWS tem recursos internos de criptografia em repouso, oferecendo a opção de criptografar dados antes que eles sejam gravados em armazenamento não volátil. Por exemplo, é possível configurar sua conta para criptografar automaticamente todos os volumes do Amazon Elastic Block Store (Amazon EBS) usando chaves de dados protegidas por uma chave mestra no KMS. Também é possível configurar buckets do Amazon S3 para Server-Side Encryption (SSE – Criptografia no servidor) usando criptografia AES-256. O Amazon Relational Database Service (Amazon RDS) também é compatível com Transparent Data Encryption (TDE – Criptografia de dados transparente).

Outro método para criptografar dados em volumes de armazenamento do EC2 é mediante o uso de bibliotecas integradas do Linux ou Windows. Esses métodos criptografam arquivos de maneira transparente, o que protege os dados confidenciais. Como resultado, os aplicativos que processam os dados não tomam ciência da criptografia em nível de disco.

É possível usar dois métodos para criptografar arquivos em armazenamentos de instância. O primeiro método é a *criptografia de disco*, no qual um disco inteiro (ou um bloco no disco) é criptografado usando uma ou mais chaves de criptografia. A criptografia de disco opera abaixo do nível de sistema de arquivos, funciona independentemente do sistema operacional e oculta informações de diretórios e arquivos, como nome e tamanho. Por exemplo, o Encrypting File System é uma extensão da Microsoft para o NTFS (New Technology File System) do sistema operacional Windows que fornece criptografia de disco.

O segundo método é a *criptografia do sistema de arquivos*. Com esse método, arquivos e diretórios são criptografados, mas não a partição ou o disco inteiro. A criptografia do sistema de arquivos opera acima do sistema de arquivos e permite a portabilidade entre sistemas operacionais.

Para volumes de armazenamento de instâncias SSD NVMe (Non-Volatile Memory Express) no EC2, a criptografia acelerada por hardware sempre está ativada. Os dados em um armazenamento de instâncias NVMe são criptografados usando uma codificação de bloco XTS-AES-256 implementada em um módulo de hardware chamado de controlador Nitro na própria instância. As chaves de criptografia são geradas usando o módulo de hardware e são exclusivas para cada dispositivo de armazenamento de instâncias NVMe. Todas as chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Ao contrário do que acontece com volumes do EBS, nesse caso, não é possível usar suas próprias chaves de criptografia.

Criptografar dados em trânsito

A AWS recomenda energicamente criptografar dados em trânsito de um sistema para outro, incluindo recursos dentro e fora da AWS.

Quando você cria uma conta da AWS e utiliza um recurso de serviço de máquina virtual do EC2, uma seção da Nuvem AWS isolada logicamente, a Amazon Virtual Private Cloud (Amazon VPC), é provisionada para a conta. Nela, é possível executar recursos da AWS em uma rede virtual definida por você. Você tem controle total sobre seu ambiente de rede virtual, incluindo a seleção do seu próprio intervalo de endereços IP, criação de sub-redes e configuração de tabelas de rotas e gateways de rede. Também é possível criar uma conexão de Virtual Private Network (VPN – Rede virtual privada) com criptografia IPSec entre seu datacenter corporativo e seu Amazon VPC para poder usar a Nuvem AWS como uma extensão de seu datacenter corporativo.

Para proteger a comunicação entre seu Amazon VPC e seu datacenter corporativo, você pode selecionar entre várias opções de conectividade de VPN e escolher a que melhor atende às suas necessidades. Você pode usar o AWS Client VPN para habilitar o acesso seguro aos seus recursos da AWS usando serviços de VPN baseados em aplicativo. Também é possível usar um appliance de VPN por software de terceiros, que você pode instalar em uma instância do Amazon EC2 em seu Amazon VPC. Como alternativa, você pode criar uma conexão de VPN IPSec para proteger a comunicação entre seu VPC e sua rede remota. É possível usar o AWS Direct Connect para criar uma conexão privada dedicada com base em uma rede remota para seu Amazon VPC. É possível combinar essa conexão com um AWS Site-to-Site VPN visando criar uma conexão com criptografia IPSec.

A AWS fornece endpoints HTTPS usando o protocolo TLS (Transport Layer Security) para comunicação, proporcionando criptografia em trânsito quando você usar APIs da AWS. É possível usar o serviço AWS Certificate Manager (ACM) para gerar, gerenciar e implantar os certificados privados e públicos que você usa para estabelecer transporte criptografado entre sistemas para suas cargas de trabalho. Diversos serviços da AWS compatíveis com TLS, como Amazon Elastic Load Balancing, são integrados ao ACM para fornecer certificados X.509 públicos e privados e, em alguns casos, para alternar automaticamente os certificados em seu

nome. Caso seu conteúdo seja distribuído por meio do Amazon CloudFront, ele também é compatível com endpoints criptografados e certificados gerenciados pelo ACM.

Ferramentas de criptografia

A AWS oferece vários serviços, ferramentas e mecanismos altamente escaláveis de criptografia de dados para ajudar a proteger seus dados armazenados e processados na AWS. Para informações sobre a funcionalidade e a privacidade do serviço da AWS, consulte Capacidades do serviço da AWS em questões de privacidade.

Os serviços criptográficos da AWS usam uma ampla gama de tecnologias de criptografia e armazenamento que são projetadas para manter a integridade de seus dados em repouso ou em trânsito.

A AWS oferece quatro ferramentas principais para operações criptográficas.

- O **AWS Key Management Service (AWS KMS)** é um serviço gerenciado da AWS que gera e gerencia tanto chaves mestras quanto chaves de dados. O AWS KMS está integrado a muitos serviços da AWS para fornecer criptografia de dados no servidor usando chaves do KMS de contas de cliente. Os Hardware Security Modules (HSM – Módulo de segurança de hardware) do KSM têm validação FIPS 140-2 nível 2.
- O **AWS CloudHSM** oferece HSMs com validação FIPS 140-2 nível 3. Ele armazena com segurança uma diversidade de chaves criptográficas autogerenciadas, inclusive chaves mestras e chaves de dados.
- **Ferramentas e serviços criptográficos da AWS**
  - O **AWS Encryption SDK** fornece uma biblioteca de criptografia no cliente para implementação de operações de criptografia e descriptografia em *todos* os tipos de dados.
  - O **Amazon DynamoDB Encryption Client** fornece uma biblioteca de criptografia no cliente para criptografar tabelas de dados antes de enviá-las para um serviço de banco de dados, como o Amazon DynamoDB.

AWS Key Management Service

O **AWS Key Management Service** (AWS KMS) é um serviço gerenciado que facilita a criação e o controle de chaves de criptografia usadas para criptografar seus dados, e usa Hardware Security Modules (HSM – Módulos de segurança de hardware) para proteger a segurança de suas chaves. O AWS KMS é integrado a dezenas de outros serviços da AWS para ajudar você a proteger os dados que armazena nesses serviços. O AWS KMS também é integrado ao AWS CloudTrail para fornecer logs contendo toda a utilização de suas chaves para fins regulatórios e de conformidade.

Você pode criar, importar e alternar chaves com facilidade, além de definir políticas de uso e auditar a utilização no Console de Gerenciamento da AWS ou usando o AWS SDK ou Interface da Linha de Comando da AWS (ILC da AWS).

As chaves mestras no KMS, sejam elas importadas por você ou criadas em seu nome pelo AWS KMS e conhecidas como CMKs, são armazenadas em um formato criptografado em um armazenamento resiliente para ajudar a garantir que possam ser usadas quando necessário. Você pode solicitar que o AWS KMS faça automaticamente o rodízio das CMKs criadas no KMS uma vez por ano sem a necessidade de criptografar novamente os dados que já foram criptografados com sua chave mestra. Não é necessário monitorar as versões anteriores de suas CMKs, pois o AWS KMS as mantém disponíveis para descriptografar automaticamente dados criptografados anteriormente.

Para qualquer CMK no KMS, é possível controlar quem tem acesso às respectivas chaves e em quais serviços elas podem ser usadas com diversos controles de acesso, inclusive concessões, e condições de política de chave nas políticas de chave ou políticas do IAM. Você também pode importar chaves de sua própria infraestrutura de gerenciamento de chaves e usá-las no KMS.

Por exemplo, a política abaixo usa a condição *kms:ViaService* para permitir que uma CMK gerenciada pelo cliente seja usada nas ações específicas exclusivamente quando a solicitação tiver origem do Amazon EC2 ou Amazon RDS em uma região específica (*us-west-2*) e em nome de um usuário específico (*ExampleUser*).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "ec2.us-west-2.amazonaws.com",
        "rds.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

Integração a serviços da AWS
O AWS KMS foi integrado a vários serviços da AWS (aproximadamente sessenta até a publicação deste texto). Essas integrações permitem que você use facilmente CMKs do AWS KMS para criptografar os dados armazenados nesses serviços. Além de usar uma CMK gerenciada pelo cliente, vários dos serviços integrados permitem que você use uma CMK gerenciada pela AWS que é criada e gerenciada automaticamente para você, mas que só pode ser usada no serviço específico que a criou.

Capacidades de auditoria
Se o AWS CloudTrail estiver habilitado para sua conta da AWS, cada utilização de uma chave que você armazene no KMS é registrado em um arquivo de log que é enviado para o bucket do Amazon S3 que você especificou quando habilitou o AWS CloudTrail. As informações registradas incluem detalhes de usuário, hora, data e a chave usada.

Segurança
O AWS KMS foi projetado para garantir que ninguém tenha acesso às suas chaves mestras. O serviço é criado com base em sistemas projetados para proteger suas chaves mestras com técnicas abrangentes de proteção, como nunca armazenar chaves mestras em texto simples em disco, não as manter na memória e limitar quais sistemas podem acessar hosts que usam as chaves. Todo o acesso para atualização de software no serviço é administrado por um controle de acesso para vários participantes que é auditado e revisado por um grupo independente na Amazon.

Para mais informações sobre o AWS KMS, consulte o whitepaper sobre o AWS Key Management Service.

AWS CloudHSM
O serviço AWS CloudHSM ajuda você a satisfazer os requisitos corporativos, contratuais e normativos de conformidade para segurança de dados ao usar appliances dedicados do HSM na Nuvem AWS. Com o CloudHSM, você controla as chaves de criptografia e as operações criptográficas executadas pelo HSM.

Os parceiros da AWS e do AWS Marketplace oferecem diversas soluções para a proteção de dados confidenciais na infraestrutura da AWS, porém, ocasionalmente é necessário oferecer proteção adicional para aplicativos e dados sujeitos a requisitos mais rígidos, contratuais ou normativos, de gerenciamento de chaves criptográficas. Anteriormente, talvez datacenters locais fossem a única opção para armazenar dados confidenciais (ou as chaves de criptografia que protegiam os dados confidenciais). Isso pode ter impedido você de migrar esses aplicativos para a nuvem ou atrasado consideravelmente a performance deles. Com o AWS CloudHSM, você pode proteger suas chaves criptográficas em HSMs projetados e validados de acordo com padrões governamentais de gerenciamento seguro de chaves. É possível gerar, armazenar e gerenciar com segurança as chaves criptográficas usadas na criptografia de

dados a fim de garantir que só você tenha acesso a elas. O AWS CloudHSM ajuda a cumprir requisitos rigorosos de gerenciamento de chaves sem sacrificar a performance dos aplicativos.

O serviço AWS CloudHSM funciona com o Amazon Virtual Private Cloud (Amazon VPC). As instâncias do CloudHSM são provisionadas dentro do seu Amazon VPC com o endereço IP que você especificar, fornecendo conectividade de rede simples e privada às suas instâncias do EC2. Ao posicionar suas instâncias do CloudHSM perto de suas instâncias do Amazon EC2, você diminui a latência da rede, o que pode aprimorar o desempenho do aplicativo. A AWS fornece acesso dedicado e exclusivo (único locatário) a instâncias do CloudHSM, que ficam isoladas de outros clientes da AWS.

Disponível em várias regiões e Availability Zones (AZ – Zona de disponibilidade), o CloudHSM permite que você adicione um armazenamento de chaves seguro e resiliente aos seus aplicativos.

Integração a serviços da AWS e aplicativos de terceiros
Você pode usar o CloudHSM com Amazon Redshift, Amazon Relational Database Service (Amazon RDS) for Oracle ou aplicativos de terceiros (como SafeNet Virtual KeySecure) para atuar como sua raiz de confiança, Apache (terminação de SSL) ou Microsoft SQL Server (criptografia de dados transparente). Também é possível usar o CloudHSM enquanto cria seus próprios aplicativos e continuar a usar as bibliotecas de criptografia padrão que já conhece, inclusive PKCS#11, Java JCA/JCE e Microsoft CAPI e CNG.

Auditar atividades
Se precisar rastrear alterações de recursos ou auditar atividades para fins de segurança e conformidade, você pode revisar todas as chamadas de API do CloudHSM feitas de sua conta por meio do AWS CloudTrail. Além disso, é possível auditar operações no appliance HSM usando o syslog ou enviar mensagens de log do syslog para seu próprio coletor de logs.

Ferramentas e serviços criptográficos da AWS
A AWS oferece mecanismos compatíveis com uma ampla variedade de padrões criptográficos de segurança que você pode usar para implementar as melhores práticas criptográficas. O AWS Encryption SDK é uma biblioteca de criptografia no cliente, disponível para Java, Python, C e JavaScript, além de uma interface da linha de comando compatível com Linux, macOS e Windows. O AWS Encryption SDK oferece recursos avançados de proteção de dados, inclusive pacotes seguros, autenticados e simétricos de algoritmo de chave, como 256-bit AES-GCM com derivação e assinatura de chave. Como foi especialmente desenvolvido para aplicativos que usam o Amazon DynamoDB, o DynamoDB Encryption Client permite que os usuários protejam os dados de suas tabelas antes que eles sejam enviados para o banco de dados. Ele também verifica e descriptografa dados quando eles são recuperados. O cliente está disponível em Java e Python.

Infraestrutura para Linux DM-Crypt

O **dm-crypt** é um mecanismo de criptografia de kernel do Linux que permite aos usuários montar um sistema de arquivos criptografado. A montagem de um sistema de arquivos é um processo no qual um sistema de arquivos é vinculado a um diretório (ponto de montagem), disponibilizando-o para o sistema operacional. Após a montagem, todos os arquivos no sistema de arquivos ficam disponíveis para aplicativos sem nenhuma interação adicional. No entanto, esses arquivos ficam criptografados quando armazenados em disco.

O **mapeador de dispositivos** é uma infraestrutura do kernel 2.6 e 3.x do Linux que oferece um método genérico de criar camadas virtuais de dispositivos de blocos. O destino de criptografia do mapeador de dispositivos oferece criptografia transparente de dispositivos de blocos por meio da API de criptografia do kernel. A solução desta publicação usa dm-crypt juntamente com um sistema de arquivos baseado em disco mapeado a um volume lógico pelo Logical Volume Manager (LVM – Gerenciador de volumes lógicos). O LVM oferece gerenciamento de volumes lógicos para o kernel do Linux.

Proteção de dados inerente ao projeto e por padrão

Uma solicitação é enviada para a AWS sempre que o usuário ou um aplicativo tenta usar o Console de Gerenciamento da AWS, a API da AWS ou a ILC da AWS. O serviço da AWS recebe a solicitação e executa um conjunto de diversas etapas para determinar se deve permitir ou negar a solicitação, tudo seguindo uma lógica específica de avaliação de política. Todas as solicitações na AWS são negadas por padrão (a política *negar* padrão é aplicada). Isso significa que tudo que não está explicitamente permitido pela política é negado. Na definição de políticas e como uma melhor prática, a AWS sugere que você aplique o princípio de privilégio mínimo, o que significa que todos os componentes (como usuários, módulos ou serviços) precisam ter a capacidade de acessar exclusivamente os recursos necessários para a conclusão de suas respectivas tarefas.

A AWS também fornece ferramentas para implementar *infraestrutura como código*, que é um mecanismo poderoso para incluir segurança desde o início da concepção de uma arquitetura. O AWS CloudFormation oferece uma linguagem comum para descrever e provisionar todos os recursos de infraestrutura, inclusive processos e políticas de segurança. Com essas ferramentas e páticas, a segurança passa a fazer parte de seu código e pode passar por versionamento, monitoramento e modificação (com um sistema de versionamento) de acordo com os requisitos de sua organização.

Isso viabiliza a abordagem de *proteção de dados inerente ao projeto*, pois você pode incluir políticas e processos de segurança na definição de sua arquitetura, e esses processos e políticas também podem ser monitorados continuamente por medidas de segurança em sua organização.

Colaboradores

Os colaboradores desse documento incluem:

- Stacy Shelhorse, garantia de segurança, Amazon Web Services
- Fernando Gebara Filho, garantia de segurança, Amazon Web Services
- Cristiane Moncau, consultora jurídica corporativa, Amazon Web Services
- Diane Young, consultora jurídica corporativa, Amazon Web Services
- Debra Farber, especialista setorial, Amazon Web Services

Revisões do documento

Data	Descrição
Março de	Primeira publicação