Whitepaper da AWS

Entendendo a conformidade com o GDPR na AWS

Entendendo a conformidade com o GDPR na AWS: Whitepaper da AWS

Table of Contents

Resumo 1
Resumo 1
Visão geral do Regulamento Geral de Proteção de Dados 2
Alterações que o RGPD introduz para organizações que operam na UE 2
Preparação da AWS para o RGPD 2
Data Processing Addendum (DPA – Adendo de processamento de dados) da AWS 3
O papel da AWS nos termos do RGPD 3
A AWS como um processador de dados 4
A AWS como um controlador de dados 4
Modelo de responsabilidade compartilhada de segurança 4
Solidez na framework de conformidade e nos padrões de segurança 6
Programa AWS Compliance 6
Cloud Computing Compliance Controls Catalog 6
Controles de acesso a dados 8
AWS Identity and Access Management 8
Tokens de acesso temporário por meio do AWS STS 9
Autenticação multifator 10
Acesso a recursos da AWS 11
Definir limites para acesso a serviços regionais 12
Controle de acesso a aplicações Web e aplicativos móveis 14
Monitoramento e registro em log 15
Gerenciar e configurar ativos com o AWS Config 15
Auditoria de conformidade e análise de segurança 16
Coletar e processar logs 18
Descobrir e proteger dados em escala 20
Gerenciamento centralizado de segurança 21
Proteger seus dados na AWS 24
Criptografar dados em repouso 24
Criptografar dados em trânsito 25
Ferramentas de criptografia 26
AWS Key Management Service 27
Ferramentas e serviços criptográficos da AWS 30
Proteção de dados inerente ao projeto e por padrão 31
Como a AWS pode ajudar 32

Colaboradores 35
Revisões do documento 36
Avisos 37

Entendendo a conformidade com o GDPR na AWS

Data de publicação: dezembro de 2020 (Revisões do documento)

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 do Regulamento Geral de Proteção de Dados (RGPD) que possam ser aplicáveis às respectivas atividades deles. Esses serviços e recursos incluem as normas de segurança de TI, o atestado do Cloud Computing Compliance Controls Catalog (C5) da AWS, cumprimento do código de conduta da Cloud Infrastructure Services Providers in Europe (CISPE – Provedores de serviços de infraestrutura de nuvem da Europa), controles de acesso a dados, ferramentas de monitoramento e registro em log, criptografia e gerenciamento de chaves.

Visão geral do Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD) é uma lei europeia de privacidade (Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016) que entrou em vigor em 25 de maio de 2018. O RGPD substitui a Diretiva de Proteção de Dados da UE, (Diretiva 95/46/EC) e destina-se a unificar as leis de proteção de dados em toda a União Europeia ao aplicar uma única lei de proteção de dados vinculativa em cada um dos estados membro da UE.

O RGPD se aplica a todo o processamento de dados pessoais por organizações que têm um estabelecimento na UE ou a organizações que processam dados pessoais de residentes da UE ao oferecer produtos ou serviços a indivíduos na UE ou monitorar o comportamento dos residentes da UE na UE. Os dados pessoais são qualquer informação relacionada a uma pessoa física identificada ou identificável.

Alterações que o RGPD introduz para organizações que operam na UE

Um dos principais aspectos do RGPD é que ele cria uma uniformidade entre os estados membro da UE com relação a como os dados pessoais podem ser processados, usados e trocados com segurança. As organizações precisam demonstrar continuamente a segurança dos dados que processam e sua conformidade com o RGPD por meio da implementação e a revisão frequente de medidas técnicas e organizacionais e políticas de conformidade aplicáveis ao processamento de dados pessoais. As autoridades de supervisão da UE podem emitir multas de até EUR 20 milhões, ou 4% do volume de negócios anual mundial, o que for maior, por violação do RGPD.

Preparação da AWS para o RGPD

Especialistas em conformidade, proteção de dados e segurança da AWS trabalham com clientes em todo o mundo para responder às suas perguntas e ajudá-los a se preparar para executar workloads na nuvem sob o RGPD. Essas equipes também analisam a prontidão da AWS em relação aos requisitos do RGPD.

> **Note**
>
> Confirmamos que todos os serviços da AWS podem ser usados em conformidade com o RGPD.

Data Processing Addendum (DPA – Adendo de processamento de dados) da AWS

A AWS oferece um anexo de processamento de dados em conformidade com o RGPD (DPA do RGPD), que permite aos clientes cumprir suas obrigações contratuais em relação a esse regulamento. O DPA do RGPD é incorporado aos Termos de Serviço da AWS e se aplica automaticamente a todos os clientes em todo o mundo que exigem a conformidade da AWS com o RGPD.

Em 16 de julho de 2020, o Tribunal de Justiça da União Europeia (TJUE) emitiu uma decisão sobre a Proteção de Privacidade UE-EUA e as Cláusulas Contratuais Padrão (SCCs), também conhecidas como “cláusulas modelo”. O TJUE determinou que a Proteção de Privacidade UE-EUA não é mais válido para a transferência de dados pessoais da União Europeia (UE) para os Estados Unidos (EUA). No entanto, na mesma decisão, o TJUE confirmou que as empresas podem continuar a usar as SCCs como um mecanismo para transferir dados para fora da UE.

Seguindo essa decisão, os clientes e parceiros da AWS podem continuar a usar a AWS para transferir seu conteúdo da Europa para os EUA e outros países, em conformidade com as leis de proteção de dados da UE, incluindo o Regulamento Geral de Proteção de Dados (RGPD). Os clientes da AWS poderão confiar nas SCCs incluídas no DPA da AWS se optarem por transferir seus dados para fora da União Europeia em conformidade com o RGPD. Conforme o cenário regulatório e legislativo evoluir, sempre trabalharemos para garantir que nossos clientes e parceiros possam continuar aproveitando os benefícios da AWS onde quer que operem. Para obter informações adicionais, consulte as Perguntas frequentes sobre a Proteção de Privacidade UE-EUA.

O papel da AWS nos termos do RGPD

Nos termos do RGPD, a AWS atua como um processador e um controlador de dados.

Nos termos do artigo 32, os controladores e os processadores precisam “...implementar medidas técnicas e organizacionais adequadas” que consideram “o nível tecnológico e o custo da implementação, bem como a natureza, o escopo, o contexto e as finalidades do processamento, além do risco das semelhanças e gravidades variáveis dos direitos e liberdades das pessoas físicas”. O RGPD oferece sugestões específicas sobre os tipos de ações de segurança que podem ser necessários, incluindo:

- A pseudonimização e a criptografia de dados pessoais.

- A capacidade de garantir continuamente a confidencialidade, a integridade, a disponibilidade e a resiliência de sistemas e serviços de processamento;
- A capacidade de restaurar a disponibilidade e o acesso a dados pessoais em tempo hábil em casos de incidentes físicos ou técnicos.
- Um processo para testar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento.

A AWS como um processador de dados

Quando os clientes e os parceiros da Rede de Parceiros da AWS (APN) usam serviços da AWS para processar dados pessoais em seu conteúdo, a AWS atua como um processador de dados. Os clientes e os parceiros da APN podem usar os controles disponíveis nos serviços da AWS, incluindo os controles de configuração de segurança para o processamento de dados pessoais. Nessas circunstâncias, o cliente ou os parceiros da APN podem atuar como um controlador ou processador de dados, e a AWS atua como um processador ou subprocessador de dados. O DPA da AWS em conformidade com o RGPD da AWS incorpora os compromissos da AWS como processador de dados.

A AWS como um controlador de dados

Quando a AWS coleta dados pessoais e determina as finalidades e os meios de processamento desses dados pessoais, ela atua como controladora de dados. Por exemplo, quando a AWS processa informações de conta para registro de conta, administração, acesso a serviços ou informações de contato da conta da AWS para fornecer assistência por meio de atividades de atendimento ao cliente, ela atua como controladora de dados.

Modelo de responsabilidade compartilhada de segurança

Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Quando os clientes transferem seus dados e sistemas de computação para a nuvem, as responsabilidades de 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 por proteger a infraestrutura global que executa todos os serviços oferecidos na Nuvem AWS. Para serviços abstratos, como o Amazon S3 e o Amazon DynamoDB, a AWS também é responsável pela segurança do sistema operacional e da plataforma. Os clientes e os parceiros da APN, atuando como controladores ou processadores de dados, são responsáveis por tudo o que colocam na nuvem ou conectam a ela. 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. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada da AWS.

O RGPD não altera o modelo de responsabilidade compartilhada da AWS, que continua relevante para clientes e parceiros da APN que se dedicam a usar serviços de computação em nuvem. O modelo de responsabilidade compartilhada é uma abordagem útil para ilustrar as diferentes responsabilidades da AWS (como processadora ou subprocessadora de dados) e dos clientes ou parceiros da APN (como controladores ou processadores de dados) nos termos do RGPD.

Estrutura de conformidade e padrões de segurança sólidos

De acordo com o RGPD, medidas técnicas e organizacionais adequadas podem precisar incluir "...a capacidade de garantir continuamente a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de processamento", bem como processos confiáveis de restauração, testes e gerenciamento de riscos gerais.

Programa AWS Compliance

A AWS mantém continuamente um patamar elevado de segurança e conformidade em todas as suas operações globais. A segurança sempre foi nossa maior e mais importante prioridade. A AWS passa regularmente por auditorias independentes de certificação de terceiros para garantir que as atividades de controle estejam operando conforme o esperado. Mais especificamente, a AWS é auditada em relação a uma variedade de frameworks de segurança globais e regionais dependentes da região e do setor. Atualmente, a AWS participa de mais de 50 programas de auditoria diferentes.

Os resultados dessas auditorias são documentados pelo órgão avaliador e disponibilizados para todos os clientes da AWS por meio do AWS Artifact. O AWS Artifact é um portal de autoatendimento gratuito para acesso sob demanda aos relatórios de conformidade da AWS. Quando novos relatórios são lançados, eles são disponibilizados no AWS Artifact, permitindo que os clientes monitorem continuamente a segurança e a conformidade da AWS com acesso imediato a novos relatórios.

Os clientes podem aproveitar certificações e credenciamentos reconhecidos internacionalmente, demonstrando conformidade com rigorosos padrões internacionais, como ISO 27017 para segurança na nuvem, ISO 27018 para privacidade na nuvem, SOC 1, SOC 2 e SOC 3, PCI DSS Nível 1 e outros. A AWS também ajuda os clientes a atender a padrões de segurança locais, como o Common Cloud Computing Controls Catalogue (C5) do BSI, que é um atestado apoiado pelo governo alemão.

Para obter informações mais detalhadas sobre os programas de certificação da AWS, relatórios e atestados de terceiros, consulte Programas de conformidade da AWS. Para obter informações específicas do serviço, consulte Serviços da AWS no escopo.

Cloud Computing Compliance Controls Catalog

O Cloud Computing Compliance Controls Catalog (C5) é um esquema de atestado apoiado pelo governo alemão que foi introduzido na Alemanha pelo Escritório Federal de Segurança da Informação (BSI). Ele foi criado para ajudar as organizações a demonstrar segurança operacional

contra ataques cibernéticos comuns no contexto das Security Recommendations for Cloud Providers (Recomendações de segurança do governo alemão para provedores de nuvem).

As medidas técnicas e organizacionais de proteção de dados e as medidas de segurança da informação visam a segurança dos dados para garantir confidencialidade, integridade e disponibilidade. O C5 define requisitos de segurança que também podem ser relevantes para a proteção de dados. Os clientes da AWS e seus consultores de conformidade podem usar o atestado do C5 como um recurso para compreender a gama de serviços de garantia de segurança de TI oferecida pela AWS na movimentação de workloads para a nuvem. O C5 adiciona um nível de segurança de TI definido normativamente, equivalente ao IT-Grundschutz com a adição de controles específicos para a nuvem.

O C5 acrescenta mais controles que fornecem informações sobre localização de dados, provisionamento de serviços, jurisdição, certificações existentes, obrigações de divulgação de informações e uma descrição completa dos serviços. Usando essas informações, você pode avaliar como regulamentos legais (por exemplo, privacidade de dados), suas próprias políticas ou o ambiente de ameaças se relacionam com o uso de serviços de computação em nuvem.

Controles de acesso a dados

O artigo 25 do RGPD declara que o controlador “deverá implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, somente serão processados os dados pessoais necessários para cada finalidade específica do processamento”. Os mecanismos de controle de acesso da AWS a seguir podem ajudar os clientes a cumprir esse requisito, permitindo o acesso exclusivo de administradores, usuários e aplicações autorizados aos recursos e aos dados do cliente na AWS.

AWS Identity and Access Management

Quando você cria uma conta da AWS, uma conta de usuário raiz é criada automaticamente para sua conta da AWS. Essa conta de usuário tem acesso completo a todos os serviços e recursos da AWS em sua conta da AWS. Em vez de usar essa conta para as tarefas cotidianas, você só deve usá-la para criar inicialmente funções e contas de usuário adicionais, e para atividades administrativas que precisam dela. A AWS recomenda que você aplique o princípio de menor privilégio 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. Essa abordagem é um mecanismo para ajustar um conceito-chave introduzido no RGPD: proteção de dados por design. O AWS Identity and Access Management(IAM) é um serviço da Web que você pode usar para controlar com segurança o acesso aos seus recursos da AWS.

Usuários e funções definem as identidades do IAM com permissões específicas. Um usuário autorizado pode assumir uma função do IAM para realizar tarefas específicas. Credenciais temporárias são criadas quando a função é assumida. Por exemplo, você pode usar funções do IAM para, de forma segura, fornecer às aplicações executadas no Amazon Elastic Compute Cloud (Amazon EC2) as credenciais temporárias necessárias para acessar outros recursos da AWS, como buckets do Amazon S3 e bancos de dados Amazon Relational Database Service (Amazon RDS) ou Amazon DynamoDB. Da mesma forma, as funções de execução fornecem às funções do AWS Lambda as permissões necessárias para acessar outros serviços e recursos da AWS, como o Amazon CloudWatch Logs, para a transmissão de logs ou a leitura de uma mensagem de uma fila do Amazon Simple Queue Service (Amazon SQS). Ao criar uma função, você adiciona políticas a ela para definir autorizações.

Para ajudar os clientes a monitorar políticas de recursos e identificar recursos com acesso não intencional, público ou entre contas, o IAM Access Analyzer pode ser habilitado para gerar

descobertas abrangentes que identificam recursos que podem ser acessados de fora de uma conta da AWS. O IAM Access Analyzer avalia políticas de recursos usando lógica matemática e inferência a fim de determinar os possíveis caminhos de acesso permitidos pelas políticas. O IAM Access Analyzer monitora continuamente as políticas novas ou atualizadas e analisa as permissões concedidas usando políticas para funções do IAM, mas também para recursos de serviços como buckets do Amazon S3, chaves do AWS Key Management Service (AWS KMS), filas do Amazon SQS e funções do Lambda.

O Access Analyzer para S3 alerta quando os buckets são configurados para permitir o acesso a qualquer pessoa na Internet ou a outras contas da AWS, incluindo contas da AWS fora da organização. Ao revisar um bucket em risco no Access Analyzer para Amazon S3, você pode bloquear todo o acesso público ao bucket com um único clique. A AWS recomenda que você bloqueie todo o acesso aos buckets, a menos que exija acesso público para dar suporte a um caso de uso específico. Antes de bloquear todo o acesso público, as aplicações devem continuar funcionando corretamente sem acesso público. Para obter mais informações, consulte Usar o Amazon S3 para bloquear o acesso público.

O IAM também fornece as últimas informações acessadas para ajudar a identificar permissões não utilizadas para que você possa removê-las das entidades principais associadas. Usando as informações acessadas pela última vez, é possível refinar suas políticas e permitir o acesso apenas aos serviços e às ações necessários. Isso ajuda a seguir e a aplicar melhor as práticas recomendadas de privilégio mínimo. É possível visualizar as informações acessadas pela última vez para entidades ou políticas existentes no IAM ou em todo o ambiente do AWS Organizations.

Tokens de acesso temporário por meio do AWS STS

É possível usar o AWS Security Token Service (AWS STS) para criar e fornecer aos usuários confiáveis credenciais temporárias de segurança que concedam acesso aos seus recursos da AWS. As credenciais temporárias de segurança funcionam de maneira praticamente idêntica às credenciais de chave de acesso 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. Você pode configurar a quantidade de tempo que elas permanecem válidas, de 15 minutos até, no máximo, 12 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 identidade. 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 obter segurança extra, você pode adicionar a autenticação de dois fatores à sua conta da AWS e aos usuários do IAM. Com a autenticação multifator (MFA) habilitada, ao fazer login no Console de Gerenciamento da AWS, é solicitado que você forneça seu nome do usuário e senha (o primeiro fator), bem como uma resposta de autenticação de seu dispositivo com 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": "*",
                "Conditions": {
                    "BoolIfExists": {"aws:MultiFactorAuthPresent":false}
                }
            }
        }
}
```

Para adicionar uma camada extra de segurança aos buckets do Amazon S3, você pode configurar a Exclusão de MFA, que requer autenticação adicional para alterar o estado de versionamento de um bucket e excluir permanentemente uma versão do objeto. A Exclusão de MFA oferece segurança adicional caso suas credenciais de segurança sejam comprometidas.

Para usar a Exclusão de MFA, você pode usar um dispositivo de hardware ou com MFA virtual para gerar um código de autenticação. Consulte a página Autenticação multifator para obter uma lista de dispositivos com MFA virtuais ou de hardware compatíveis.

Acesso a recursos da AWS

Para implementar acesso granular aos seus recursos 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, ao Amazon S3, ao DynamoDB, ao Amazon Redshift e a outros serviços da AWS.

Para outros usuários, você pode definir acesso somente leitura a apenas alguns buckets do Amazon S3, permissão para administrar apenas algumas instâncias do Amazon 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.

Definir limites para acesso a serviços regionais

Como cliente, você mantém a propriedade sobre o seu conteúdo e seleciona quais serviços da AWS podem processar, armazenar e hospedar esse conteúdo. A AWS não acessa nem usa o seu conteúdo para nenhum finalidade sem o seu consentimento. Com base no modelo de responsabilidade compartilhada, você escolhe as regiões da AWS nas quais seu conteúdo é armazenado, permitindo que você implante serviços da AWS nos locais de sua escolha, de acordo com seus requisitos geográficos específicos. Por exemplo, se você quiser garantir que seu conteúdo esteja localizado apenas na Europa, você poderá optar por implantar serviços da AWS exclusivamente em uma das regiões europeias da AWS.

As políticas do IAM fornecem um mecanismo simples para limitar o acesso a serviços em regiões específicas. Você pode adicionar uma condição global (`aws:RequestedRegion`) às políticas do

IAM anexadas às suas entidades principais do IAM para aplicá-la a todos os serviços da AWS. Por exemplo, a política a seguir usa o elemento `NotAction` com o efeito `Deny`, que nega explicitamente o acesso a todas as ações não listadas na instrução se a região solicitada não for na Europa. As ações nos serviços CloudFront, IAM, Amazon Route 53 e AWS Support não devem ser negadas porque são serviços globais populares da AWS.

```
{
   “Version”: “2012-10-17”,
   “Statement”: [
       {
          “Sid”: “DenyAllOutsideRequestedRegions”,
          “Effect”: “Deny”,
          “NotAction”: [
               “cloudfront:*”,
               “iam:*”,
               ”route53:*”,
               “support:*”
           ],
           “Resource”: “*”,
           “Condition”: {
              “StringNotLike”: {
                  “aws:RequestedRegion”: [
                        “eu-*”
                  ]
               }
            }
      }
    ]
}
```

Esse exemplo de política do IAM também pode ser implementado como uma Política de Controle de Serviço (SCP) no AWS Organizations, que define os limites de permissão aplicados a contas específicas da AWS ou unidades organizacionais (OUs) em uma organização. Isso permite que você controle o acesso do usuário a serviços regionais em ambientes complexos de várias contas.

Existem recursos de limitação geográfica para regiões recém-lançadas. As regiões introduzidas após 20 de março de 2019 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 a

desabilitação das regiões da AWS permitem que você controle se os usuários em sua conta da AWS podem acessar recursos na região em questão. Para obter mais informações, consulte Gerenciar regiões da AWS.

Controle de acesso a aplicações Web e aplicativos móveis

A AWS oferece serviços para gerenciar o controle de acesso a dados nas aplicações do cliente. Caso precise adicionar recursos de login de usuário e controle de acesso às suas aplicações 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 os grupos de identidades do Amazon Cognito (identidades federadas), você pode ver quem acessou seus recursos e de onde o acesso se originou (aplicativo móvel ou aplicação Web). Você pode usar essa informação para criar políticas e funções do IAM que permitam ou neguem acesso a um recurso com base no tipo de origem do acesso (aplicativo móvel ou aplicação Web) e provedor de identidade.

Monitoramento e registro em log

O artigo 30 do RGPD estabelece que “...cada controlador e, se for o caso, o representante do controlador, deverão manter um registro das atividades de processamento sob sua responsabilidade”. Este artigo também inclui detalhes sobre quais informações devem ser registradas quando você monitora o processamento de todos os dados pessoais. Os controladores e os processadores também precisam enviar notificações de violação em tempo hábil, portanto, detectar incidentes rapidamente é importante. Para ajudar os clientes a cumprir essas obrigações, a AWS oferece os serviços de monitoramento e registro em log a seguir.

Gerenciar e configurar ativos com o AWS Config

O AWS Config oferece uma exibição detalhada da configuração dos muitos tipos 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.

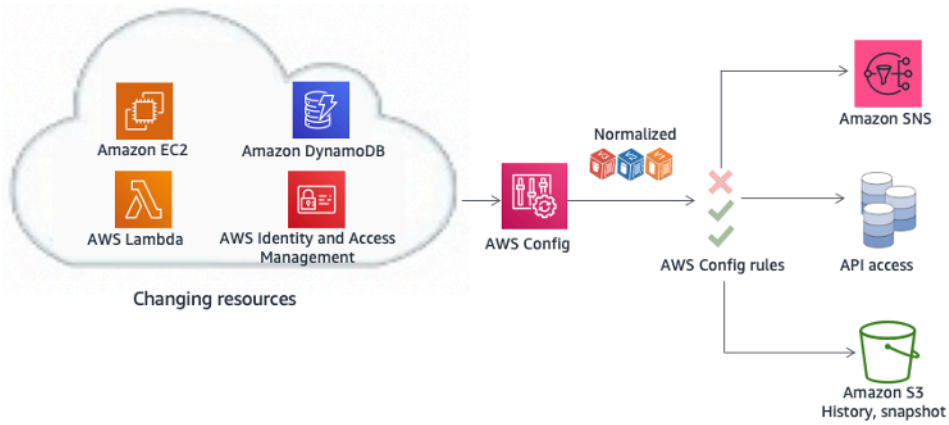

Figura 1: monitorar as alterações de configuração ao longo do tempo com o AWS Config

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 obter uma lista completa dos recursos da AWS compatíveis com o AWS Config, consulte Tipos de recurso da AWS compatíveis.

Com o AWS Config, é possível fazer o seguinte:

- 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.
- Visualizar os relacionamentos entre os recursos. Por exemplo, encontrar todos os recursos que usam um determinado grupo de segurança.

Auditoria de conformidade e análise de segurança

Com o AWS CloudTrail, você pode 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 compatíveis com o CloudTrail, o endereço IP de origem dessas chamadas e quando as chamadas ocorreram. É possível integrar o CloudTrail a aplicações usando a API, automatizar a criação de trilhas para a sua organização, verificar o status de suas trilhas e controlar como os administradores habilitam e desabilitam o registro em log do CloudTrail.

Os logs do CloudTrail podem ser agregados de várias regiões e várias contas da AWS em um único bucket do Amazon S3. A AWS recomenda que você grave registros, especialmente registros do AWS CloudTrail, em um bucket do Amazon S3 com acesso restrito em uma conta da AWS designada para registro em log (conta de arquivamento de logs). As permissões no bucket devem impedir a exclusão dos logs e também devem ser criptografadas em repouso usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) ou chaves gerenciadas pelo AWS KMS (SSE-KMS). É possível usar a validação de integridade de arquivos de log do CloudTrail para determinar se um arquivo de log foi modificado, excluído ou permaneceu inalterado depois de fornecido pelo CloudTrail. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Desse modo, é computacionalmente difícil modificar, excluir ou forjar arquivos de log do CT; sem detecção. Você pode usar a AWS Command Line Interface (AWS CLI) para validar os arquivos no local onde o CloudTrail os entregou.

Os logs do CloudTrail agregados em um bucket do Amazon S3 podem ser analisados para fins de auditoria ou para atividades de solução de problemas. Depois que os logs estiverem centralizados, você poderá fazer a integração com soluções de Security Information and Event Management (SIEM)

ou usar serviços da AWS, como o Amazon Athena ou o CloudTrail Insights, para analisá-los e visualizá-los usando os painéis do Amazon QuickSight . Depois de centralizar os logs do CloudTrail, você também pode usar a mesma conta do Log Archive para centralizar logs de outras fontes, como CloudWatch Logs e AWS Load Balancers.

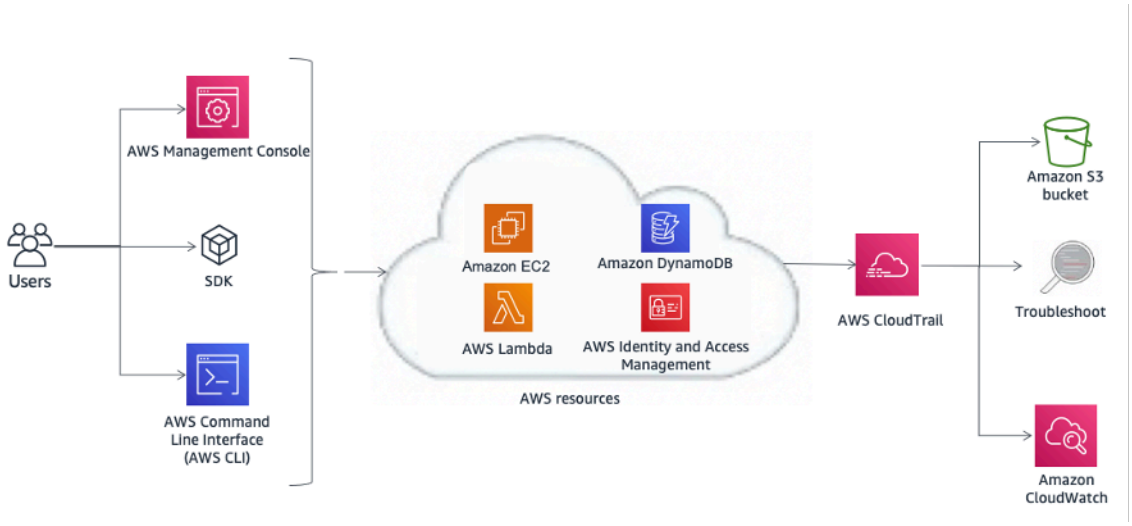

Figura 2: exemplo de arquitetura para auditoria de conformidade e análise de segurança com o AWS CloudTrail

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 na 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 para o administrador. (Ver Figura 3.) O e-mail inclui detalhes como quando o evento aconteceu, qual usuário executou a ação, detalhes do Amazon EC2 e muito mais. O diagrama a seguir mostra a arquitetura da notificação de eventos.

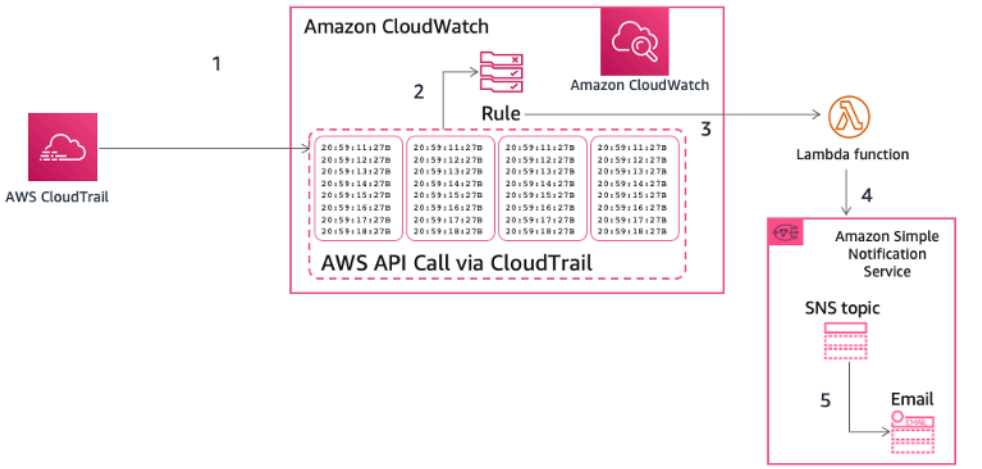

Figura 3: exemplo de notificação de evento do AWS CloudTrail

Coletar e processar logs

O CloudWatch Logs pode ser usado para monitorar, armazenar e acessar seus arquivos de log de instâncias do Amazon EC2, do AWS CloudTrail, do Route 53 e de outras fontes. Consulte a página de documentação dos Serviços da AWS que publicam logs no CloudWatch Logs.

As informações de logs incluem, por exemplo:

- Registro em log de acesso detalhado a objetos do Amazon S3
- Informações detalhadas sobre fluxos na rede por meio dos logs de fluxo da VPC
- Verificação de configuração baseada em regras e ações com regras do AWS Config
- Filtragem e monitoramento de acesso HTTP a aplicações com funções de firewall de aplicação Web (WAF) no CloudFront

Métricas e logs de aplicações personalizados também podem ser publicados no CloudWatch Logs instalando o CloudWatch Agent em instâncias do Amazon EC2 ou em servidores on-premises.

Os logs podem ser analisados interativamente usando o CloudWatch Logs Insights, realizando consultas para ajudar você a responder de forma mais eficiente e eficaz a problemas operacionais.

O CloudWatch Logs pode ser processado praticamente em tempo real configurando filtros de assinatura e entregue a outros serviços, como um cluster do Amazon OpenSearch Service (OpenSearch Service), um stream do Amazon Kinesis, um stream do Amazon Kinesis Data Firehose ou Lambda para processamento personalizado, análise ou carregamento para outros sistemas.

Os filtros de métrica do CloudWatch podem ser usados para definir padrões a serem procurados em dados de log, transformá-los em métricas numéricas do CloudWatch e configurar alarmes com base em seus requisitos de negócios. Por exemplo, seguindo a recomendação da AWS de não usar o usuário raiz para tarefas diárias, é possível configurar um filtro de métrica específico do CloudWatch em um log do CloudTrail (entregue ao CloudWatch Logs) para criar uma métrica personalizada e configurar um alarme para notificar as partes interessadas quando as credenciais raiz são usadas para acessar sua conta da AWS.

Logs como logs de acesso ao servidor do Amazon S3, logs de acesso do Elastic Load Balancing, logs de fluxo da VPC e logs de fluxo do AWS Global Accelerator podem ser entregues diretamente a um bucket do Amazon S3. Por exemplo, quando você habilita os logs de acesso ao servidor do Amazon Simple Storage Service, você pode obter informações detalhadas sobre as solicitações 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 obter mais informações sobre o conteúdo de uma mensagem de log, consulte o Formato de log de acesso a servidor do Amazon Simple Storage Service no Guia do desenvolvedor do Amazon Simple Storage Service. Logs de acesso ao servidor são úteis para muitas aplicações, porque fornecem aos proprietários de buckets insights sobre a natureza das solicitações feitas por clientes fora de seu controle. Por padrão, o Amazon S3 não coleta logs de acesso ao serviço. No entanto, quando você habilita o registro em log, o Amazon S3 geralmente fornece logs de acesso ao bucket em algumas horas. Se você precisar de uma entrega mais rápida ou precisar entregar logs para vários destinos, considere usar logs do CloudTrail ou uma combinação de logs do CloudTrail e do Amazon S3. Os logs podem ser criptografados em repouso configurando a criptografia de objeto padrão no bucket de destino. Os objetos são criptografados usando a criptografia no lado do servidor com as chaves gerenciadas pelo Amazon S3 (SSE-S3) ou as chaves primárias de cliente (CMKs) armazenadas no AWS Key Management Service (AWS KMS).

Os logs armazenados em um bucket do Amazon S3 podem ser consultados e analisados usando o Amazon Athena. O Amazon Athena é um serviço de consultas interativas que permite analisar dados no S3 usando SQL. Você pode usar o Athena para executar consultas pontuais com ANSI SQL, sem necessidade de agregar ou carregar os dados no Athena. O Athena pode processar conjuntos de dados não estruturados, semiestruturados e estruturados e integra-se ao Amazon QuickSight para facilitar a visualização.

Os logs também são uma fonte útil de informações para a detecção de ameaças automatizada. O Amazon GuardDuty é um serviço de monitoramento contínuo de segurança que analisa e processa eventos de várias fontes, como logs de fluxo da VPC, logs de eventos de gerenciamento do CloudTrail, logs de eventos de dados do Amazon S3 do CloudTrail e logs de DNS. Ele usa feeds de

inteligência contra ameaças, como listas de endereços IP e domínios mal-intencionados, e machine learning para identificar atividades inesperadas, maliciosas e possivelmente não autorizadas no seu ambiente da AWS. Quando você habilita o GuardDuty em uma região, ele começa imediatamente a analisar seus logs de eventos do CloudTrail. Ele consome o gerenciamento do CloudTrail e os eventos de dados do Amazon S3 diretamente do CloudTrail por meio de um fluxo de eventos independente e duplicado.

Descobrir e proteger dados em escala com o Amazon Macie

O artigo 32 do RGPD declara que “... o controlador e o processador devem implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança apropriado ao risco, incluindo, inter alia, conforme apropriado: [...]

(b) a capacidade de garantir continuamente a confidencialidade, a integridade, a disponibilidade e a resiliência de sistemas e serviços de processamento;

[...]

(d) um processo para testar, avaliar e aferir a eficácia de medidas técnicas e organizacionais a fim de garantir a segurança do processamento”.

Ter um processo contínuo de classificação de dados é fundamental para ajustar o processamento de dados de segurança à natureza dos dados. Se sua organização gerencia dados sigilosos, monitore onde eles residem, proteja-os adequadamente e forneça evidências de que você está aplicando a segurança e a privacidade dos dados conforme necessário para atender aos requisitos de conformidade regulatória. Para ajudar o cliente a identificar e proteger seus dados sigilosos em escala, a AWS oferece o Amazon Macie, um serviço totalmente gerenciado de segurança e privacidade de dados que usa modelos de correspondência de padrões e machine learning para detecção de informações de identificação pessoal (PII) a fim de descobrir e proteger dados confidenciais armazenados em buckets do S3. O Amazon Macie verifica esses buckets e fornece uma categorização de dados deles usando identificadores de dados gerenciados projetados para detectar várias categorias de dados sigilosos. O Macie pode detectar PII, como nome completo, endereço de e-mail, data de nascimento, número de identificação nacional, número de identificação do contribuinte ou número de referência e muito mais. O cliente pode definir identificadores de dados personalizados que refletem os cenários específicos de sua organização (por exemplo, números de contas de clientes ou classificação de dados internos).

O Amazon Macie avalia continuamente o objeto dentro dos buckets e fornece automaticamente um resumo das descobertas (Figura 4) para quaisquer dados descobertos não criptografados ou

acessíveis publicamente que correspondam à categoria de dados definida. Esses dados podem incluir alertas para quaisquer objetos ou buckets não criptografados e acessíveis publicamente compartilhados com contas da AWS fora daqueles que você definiu no AWS Organizations. O Amazon Macie é integrado a outros serviços da AWS, como o AWS Security Hub, por exemplo, para gerar descobertas de segurança que levem a ações concretas e fornecer uma ação automática e reativa à descoberta (Figura 5).

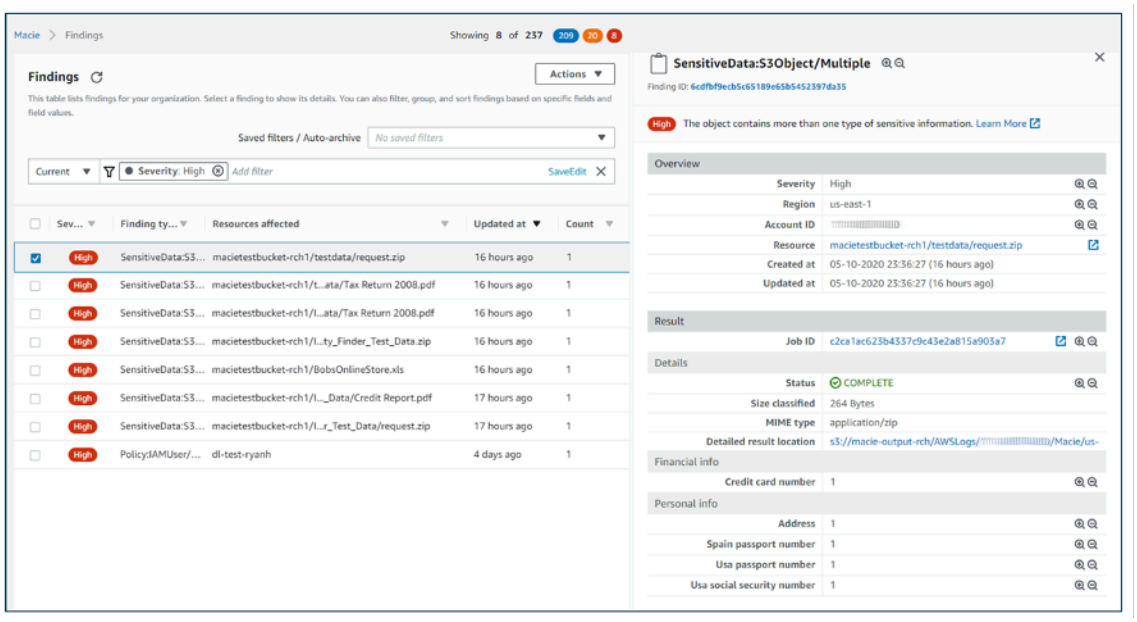

Figura 4: inspeções de dados e exemplo de descoberta

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, combinado com gerenciamento descentralizado e desigual de processos de governança e segurança, pode 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 Control Tower é um método para configurar e administrar um ambiente novo, seguro e com várias contas da AWS. Ele automatiza a configuração de uma zona de aterrissagem, que é um ambiente de várias contas com base em esquemas de práticas recomendadas 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 fornece gerenciamento de identidades usando o diretório padrão AWS IAM Identity Center (IAM Identity Center) e permite auditorias entre contas usando o IAM Identity Center e o IAM. Ele também centraliza os logs provenientes do CloudTrail e os logs 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, como o Amazon GuardDuty e o Amazon Inspector, e pode ser integrado a softwares de segurança de parceiros terceiros visando ajudar você a analisar tendências de segurança e identificar os problemas de segurança prioritários.

O Amazon GuardDuty é um serviço inteligente de detecção de ameaças que pode ajudar os clientes a monitorar e proteger com mais precisão e facilidade suas contas, workloads e dados da AWS armazenados no Amazon S3. O GuardDuty analisa bilhões de eventos em suas contas da AWS de várias fontes, incluindo eventos de gerenciamento do AWS CloudTrail, eventos de dados do Amazon S3 do CloudTrail, logs de fluxo da Amazon Virtual Private Cloud e logs de DNS. Por exemplo, ele detecta chamadas de API incomuns, comunicações de saída suspeitas com endereços IP mal-intencionados conhecidos ou possível roubo de dados usando consultas de DNS como mecanismo de transporte. O GuardDuty é capaz de fornecer descobertas mais precisas aproveitando a inteligência contra ameaças baseada em machine learning e parceiros de segurança terceiros.

O Amazon Inspector é um serviço automatizado de avaliação de segurança que ajuda a aprimorar a segurança e a conformidade das aplicações implantadas em instâncias do Amazon EC2. O Amazon Inspector avalia automaticamente aplicações em busca de exposição, vulnerabilidades e desvios das práticas recomendadas. Depois de fazer uma avaliação, o Amazon Inspector gera uma lista detalhada dos problemas de segurança encontrados priorizados por nível de gravidade.

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 (por exemplo, chamando uma função do Lambda ou executando um comando na instância do Amazon EC2) conforme necessário e sempre que ocorrer um evento de incidente de segurança.

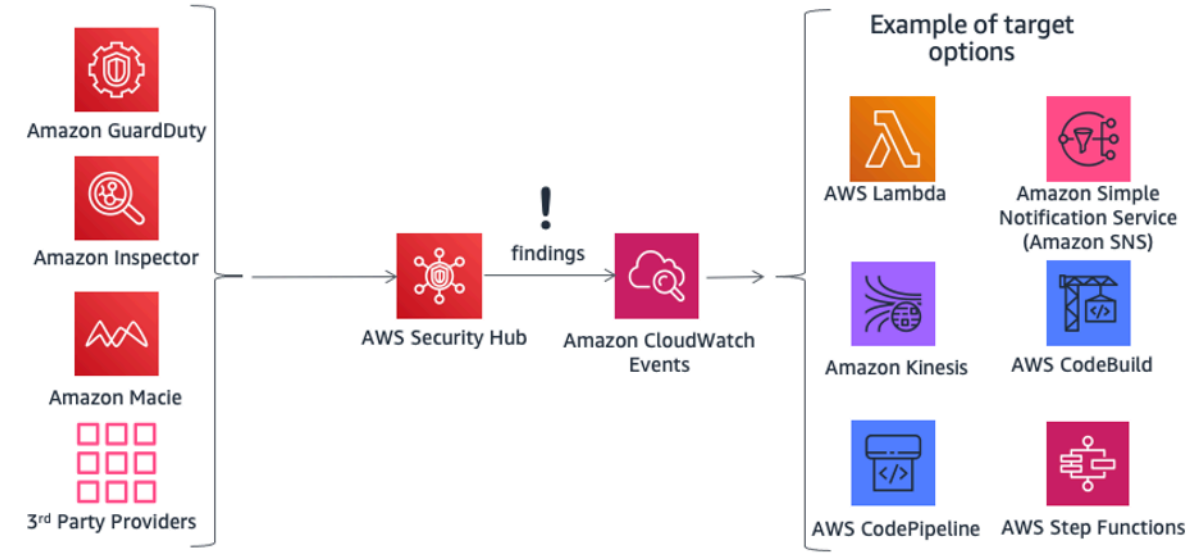

Figura 5: adotar medidas com o AWS Security Hub e o Amazon CloudWatch Events

O AWS Organizations ajuda você a gerenciar e administrar de forma centralizada ambientes complexos. Ele permite que você controle o acesso, a conformidade e a segurança em um ambiente de várias contas. O AWS Organizations é compatível com Políticas de controle de serviço (SCPs), que definem as ações de serviço da AWS disponíveis para uso com contas específicas ou unidades organizacionais (OUs) em uma organização.

O AWS Systems Manager oferece visibilidade e controle da sua infraestrutura na AWS. Você pode visualizar dados operacionais de vários serviços da AWS em um console unificado e automatizar tarefas operacionais entre eles. É possível ter informações sobre atividades recentes da API, alterações na configuração de recursos, alertas operacionais, inventário de software e status de conformidade de patches. Usando a integração com outros serviços da AWS, você também pode tomar medidas em relação aos recursos, dependendo de suas necessidades operacionais, para ajudar a tornar seu ambiente em um status de conformidade.

Por exemplo, ao integrar o Amazon Inspector com o AWS Systems Manager, as avaliações de segurança são simplificadas e automatizadas, pois você pode instalar o agente do Amazon Inspector automaticamente usando o Amazon Elastic Compute Cloud Systems Manager quando uma instância do Amazon EC2 é iniciada. Você também pode executar correções automáticas para descobertas do Amazon Inspector usando as funções do Amazon EC2 System Manager e do Lambda.

Proteção de dados na AWS

O artigo 32 do RGPD exige que as organizações “...implementem medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado para o risco, incluindo ...a pseudonimização e a criptografia de dados pessoais[...]”. Além disso, as organizações devem se proteger contra a divulgação ou o acesso não autorizado de dados pessoais”.

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 amenizar o impacto de vários eventos de segurança, inclusive algumas 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 sigilosos salvos em discos não sejam legíveis por nenhum usuário ou aplicação sem uma chave válida. A AWS fornece diversas opções para criptografia em repouso e gerenciamento de chave de criptografia. Por exemplo, você pode usar o AWS Encryption SDK com uma CMK criada e gerenciada no AWS KMS para criptografar dados arbitrários.

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. Alguns serviços básicos da AWS têm 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 criptografar volumes do Amazon EBS e configurar buckets do Amazon S3 para criptografia Server-Side Encryption (SSE – Criptografia do lado do servidor) usando criptografia AES-256. O Amazon S3 também é compatível com criptografia do lado do cliente, que permite criptografar dados antes de enviá-los para o Amazon S3. Os SDKs da AWS são compatíveis com a criptografia do lado do cliente para facilitar as operações de criptografia e descriptografia de objetos. O Amazon RDS também é compatível com a criptografia transparente de dados (TDE).

É possível criptografar dados em armazenamentos de instâncias Linux do Amazon EC2 usando bibliotecas Linux incorporadas. Esse método criptografa arquivos de forma transparente, o que protege os dados confidenciais. Como resultado, os aplicativos que processam os dados não estão cientes da criptografia de disco.

É possível usar dois métodos para criptografar arquivos em armazenamentos de instância:

- Criptografia no nível do disco: com esse método, todo o disco, ou um bloco dentro do 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 New Technology File System (NTFS) do sistema operacional Windows NT que fornece criptografia de disco.
- Criptografia no nível do sistema de arquivos: com esse método, arquivos e diretórios são criptografados, mas não a partição ou o disco inteiro. A criptografia no nível do sistema de arquivos opera acima do sistema de arquivos e permite a portabilidade entre sistemas operacionais.

Para volumes de armazenamento de instâncias SSD com Non-Volatile Memory Express (NVMe), a criptografia no nível do disco é a opção padrão. Os dados no armazenamento de instâncias de NVMe são criptografados usando uma criptografia de bloco XTS-AES-256 implementada em um módulo de hardware na instância. As chaves de criptografia são geradas usando o módulo de hardware e são exclusivas para cada dispositivo de armazenamento de instâncias de NVMe. Todas as chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Você não pode usar suas próprias chaves de criptografia.

Criptografar dados em trânsito

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

Quando você cria uma conta da AWS, uma seção isolada logicamente da Nuvem AWS, a Amazon Virtual Private Cloud (Amazon VPC), é provisionada para ela. 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 rede privada virtual (VPN) de hardware 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 equipamento

de software VPN de terceiros disponível no AWS Marketplace, que você pode instalar em uma instância do Amazon EC2 em sua Amazon VPC. Como alternativa, você pode criar uma conexão VPN IPSec para proteger a comunicação entre sua 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 sua Amazon VPC. Combine essa conexão com o AWS Site-to-Site VPN para criar uma conexão privada criptografada por IPsec.

A AWS fornece endpoints HTTPS usando o protocolo TLS para comunicação, que proporciona criptografia em trânsito quando você usa 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 workloads. O Elastic Load Balancing é integrado ao ACM e é usado para oferecer suporte a protocolos HTTPS. Se seu conteúdo for distribuído por meio do Amazon CloudFront, ele será compatível com endpoints criptografados.

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 obter 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 AWS Managed Service que gera e gerencia chaves primárias e chaves de dados. O AWS KMS está integrado ao com muitos serviços da AWS para fornecer criptografia de dados no lado do servidor usando chaves do AWS KMS de contas de clientes. Os AWS KMS Hardware Security Modules (HSMs – Módulo de segurança de hardware) 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 primárias e chaves de dados.
- Ferramentas e serviços criptográficos da AWS
  - O AWS Encryption SDK fornece uma biblioteca de criptografia do lado do 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 do lado do 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

AWS Key Management Service é um serviço gerenciado que facilita a criação e o controle das chaves de criptografia usadas para criptografar seus dados e usa módulos de segurança de hardware (HSMs) para proteger a segurança de suas chaves. O AWS KMS está integrado a vários outros serviços da AWS para ajudar você a proteger os dados armazenados com esses serviços. O AWS KMS também é integrado ao AWS CloudTrail para fornecer logs de todo o uso de chaves para suas necessidades regulatórias e de conformidade.

Você pode criar, importar e alternar facilmente as chaves, além de definir políticas de uso e fazer auditoria da utilização por meio do AWS Management Console ou usando o AWS SDK ou a AWS CLI.

As CMKS no AWS KMS, tanto as importadas quanto as criadas em seu nome pelo KMS, são armazenadas em um formato criptografado em um armazenamento altamente durável, o que ajuda a garantir que elas possam ser usadas quando necessário. Você pode solicitar que o KMS alterne automaticamente as CMKs criadas no KMS uma vez por ano sem a necessidade de criptografar novamente os dados que já foram criptografados com sua chave primária. Não é necessário monitorar as versões anteriores de suas CMKs, pois o KMS as mantém disponíveis para descriptografar automaticamente dados criptografados anteriormente.

Para qualquer CMK no AWS 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 do Amazon RDS em uma região específica (us-west-2) em nome de um usuário específico (`ExampleUser`).

```
{
 “Version”: “2012-10-17”,
```

```
        “Statement”: [
            {
               “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”: {
                   “ForAnyValue: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. Consulte o site do KMS para obter uma lista completa de serviços integrados. 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

O AWS CloudTrail registra cada uso de uma chave armazenada no AWS KMS em um arquivo de log que é entregue ao bucket do Amazon S3 que você especificou na configuração do CloudTrail. As informações registradas incluem detalhes de usuário, hora, data, operação executada e a chave usada.

Segurança

O AWS KMS foi projetado para garantir que ninguém tenha acesso às suas chaves primárias. O serviço é criado com base em sistemas projetados para proteger suas chaves primárias com técnicas abrangentes de proteção, como nunca armazenar chaves primárias 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 várias partes que é auditado e revisado por um grupo independente na AWS.

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

AWS CloudHSM

O AWS CloudHSM é um módulo de segurança de hardware (HSM) baseado em nuvem que ajuda você a atender aos requisitos de conformidade corporativa, contratual e regulatória para segurança de dados, permitindo que você gere e use suas chaves de criptografia em um hardware validado FIPS 140-2 nível 3.

Com o AWS CloudHSM, você controla as chaves de criptografia e as operações criptográficas executadas pelo HSM.

A AWS e os parceiros do AWS Marketplace oferecem diversas soluções para a proteção de dados sigilosos dentro da plataforma da AWS. No entanto, ocasionalmente, pode ser necessário oferecer proteção adicional para aplicações e dados sujeitos a rigorosos requisitos contratuais ou normativos de gerenciamento de chaves criptográficas. Anteriormente, talvez datacenters on-premises fossem a única opção para armazenar dados sigilosos (ou as chaves de criptografia que protegiam os dados confidenciais). Isso pode ter impedido você de migrar essas aplicações para a nuvem ou atrasado consideravelmente a performance delas. 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 de forma segura as chaves de criptografia usadas na criptografia de dados, garantindo que somente você terá acesso a elas. O AWS CloudHSM ajuda a cumprir requisitos rigorosos de gerenciamento de chaves sem sacrificar a performance das aplicações.

O serviço AWS CloudHSM funciona com a Amazon VPC. As instâncias do AWS CloudHSM são provisionadas dentro da sua Amazon VPC com o endereço IP que você especificar, fornecendo conectividade de rede simples e privada às suas instâncias do Amazon EC2. Ao posicionar suas instâncias do HSM perto de suas instâncias do Amazon EC2, você diminui a latência da rede, o

que pode aprimorar a performance da aplicação. A AWS fornece acesso dedicado e exclusivo (locatário único) a instâncias do HSM, que ficam isoladas de outros clientes da AWS. Disponível em várias regiões e zonas de disponibilidade, o AWS CloudHSM permite que você adicione um armazenamento de chaves seguro e resiliente às suas aplicações.

Integração a serviços da AWS e aplicações de terceiros

Você pode usar o CloudHSM com o Amazon Redshift, o Amazon RDS for Oracle ou aplicações 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 AWS CloudHSM enquanto cria suas próprias aplicações e continuar a usar as bibliotecas de criptografia padrão, inclusive PKCS#11, Java JCA/JCE e Microsoft CAPI e CNG.

Atividades de auditoria

Se você precisar rastrear alterações de recursos ou atividades de auditoria para fins de segurança e conformidade, poderá revisar as chamadas de API de gerenciamento pelo AWS CloudHSM feitas na sua conta usando o AWS CloudTrail. Além disso, é possível auditar operações no equipamento 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. Ele oferece recursos avançados de proteção de dados, inclusive pacotes seguros, autenticados e simétricos de algoritmo de chave, como AES-GCM de 256 bits 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

Sempre que um usuário ou uma aplicação tenta usar o AWS Management Console, a API da AWS ou a AWS CLI, uma solicitação é enviada para a 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. Exceto para solicitações de credencial raiz, todas as solicitações na AWS são negadas por padrão (a política de negação 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.

Essa abordagem se alinha ao artigo 25 do RGPD, que declara que o controlador “deverá implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, somente serão processados os dados pessoais necessários para cada finalidade específica do processamento”.

A AWS também fornece ferramentas para implementar a infraestrutura como código, que é um mecanismo poderoso para incluir a segurança desde o início do projeto de uma arquitetura. O AWS CloudFormation fornece uma linguagem comum para descrever e provisionar todos os recursos de infraestrutura, incluindo políticas e processos de segurança. Com essas ferramentas e práticas, 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 permite a proteção de dados inerente ao projeto, porque os processos e as políticas de segurança podem ser incluídos na definição de sua arquitetura e também podem ser monitorados continuamente por medidas de segurança em sua organização.

Como a AWS pode ajudar

Tabela 1: como a AWS pode ajudar você a navegar pela conformidade com o RGPD

Área	Descrição	Serviços e ferramentas da AWS
Estrutura de conformidade forte	Medidas técnicas e organizacionais apropriadas podem precisar incluir “a capacidade de garantir a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e dos serviços de processamento”.	SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS 70)/SOC 2/SOC 3 PCI DSS nível 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5)
Controle de acesso a dados	O controlador “...deverá implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, somente serão processados os dados pessoais	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield e AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail

Área	Descrição	Serviços e ferramentas da AWS
	necessários para cada finalidade e específica do processamento”.	
Monitoramento e registro em log	“Cada controlador e, se for o caso, o representante do controlador, deverão manter um registro das atividades de processamento sob sua responsabilidade”. “... o controlador e o processador devem implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco [...]”	AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub Ferramentas e SDKs da AWS

Área	Descrição	Serviços e ferramentas da AWS
Proteger seus dados na AWS	As organizações devem “implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado para o risco, incluindo a pseudonimização e a criptografia de dados pessoais”.	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

Colaboradores

Os colaboradores desse documento incluem:

- Tim Anderson, especialista técnico do setor da Amazon Web Services
- Carmela Gambardella, arquiteta de soluções do setor público da Amazon Web Services
- Giuseppe Russo, gerente de garantia de segurança da Amazon Web Services
- Marta Taggart, gerente sênior de programas da Amazon Web Services
- Luca Iannario, arquiteto de soluções do setor público da Amazon Web Services

Revisões do documento

Data	Descrição
Novembro de 2017	Primeira publicação
Dezembro de 2020	Atualizado para incluir a adição de novos serviços e funcionalidades da AWS.

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento é: (a) fornecido apenas para fins informativos, (b) representa as ofertas e as 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 os serviços da AWS são fornecidos no “estado em que se encontram”, sem garantias, declarações ou condições de qualquer tipo, explícitas ou implícitas. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte, nem modifica, qualquer contrato entre a AWS e seus clientes.