Entendendo a conformidade com o GDPR na AWS

Setembro de 2018

Avisos

Este documento é disponibilizado apenas para fins informativos. Ele relaciona as atuais ofertas de produtos e práticas da AWS a contar da data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento e de qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido “como está”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais, condições ou seguros da AWS, suas afiliadas, fornecedores ou licenciadores. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos dela, e este documento não é parte, nem modifica, qualquer contrato entre a AWS e seus clientes.

Sumário

Resumo

Este documento tem o objetivo de responder a várias perguntas, dentre elas: “Como a AWS ajuda os clientes a estar em conformidade com o General Data Protection Regulation (GDPR – Regulamento geral de proteção de dados)?” A Amazon Web Services (AWS) fornece aos clientes serviços e recursos para ajudar a cumprir os requisitos do GDPR que podem ser aplicáveis às suas operações. Esses serviços e recursos incluem o código de conduta da Cloud Infrastructure Services Providers in Europe (CISPE – Provedores de serviços de infraestrutura de nuvem da Europa), controles detalhados de acesso a dados, ferramentas de monitoramento e registro em log, criptografia, gerenciamento de chaves, recursos de auditoria, cumprimento de normas de segurança de TI e os atestados do Cloud Computing Compliance Controls Catalog (C5) da AWS.

O regulamento geral de proteção de dados: uma visão geral

O GDPR é uma nova lei de privacidade europeia. O GDPR pretende harmonizar as leis de proteção de dados de toda a União Europeia (UE) aplicando uma única lei de proteção de dados obrigatória em todos os estados-membro.

O GDPR se aplica a todas as organizações que têm um estabelecimento na UE ou que oferecem mercadorias ou serviços a indivíduos na UE e que processam "dados pessoais" de residentes da UE. Os dados pessoais são qualquer informação relacionada a uma pessoa física identificada ou identificável.

Mudanças introduzidas pelo GDPR nas organizações que operam na UE

Um dos principais aspectos do GDPR é que ele pretende criar consistência entre os estados-membro da UE com relação a como os dados pessoais podem ser processados, usados e trocados com segurança. As organizações precisarão demonstrar continuamente a segurança dos dados que processam e sua conformidade com o GDPR por meio da implementação e revisão frequente de medidas técnicas e organizacionais rigorosas e políticas de conformidade. As autoridades fiscalizadoras poderão emitir multas de até 20 milhões de euros ou 4% do volume de negócios global anual, o que for mais alto.

Preparação da AWS para o GDPR

Os especialistas em conformidade, proteção de dados e segurança da AWS têm trabalhado com clientes em todo o mundo para responder às suas perguntas e ajudá-los a se preparar para a execução de cargas de trabalho na nuvem após o GDPR entrar em vigor. Essas equipes também estão revisando tudo o que a AWS já faz para garantir o cumprimento dos requisitos do GDPR.

> **Podemos confirmar que os serviços da AWS cumprem o GDPR.**

Nos termos do artigo 32, os controladores e os processadores têm de "implementar medidas técnicas e organizacionais adequadas" considerando "o nível tecnológico e o custo da implementação, bem como a natureza, o contexto e as finalidades do processamento, além do risco das semelhanças e severidades variáveis dos direitos e liberdades das pessoas físicas". O GDPR 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, avaliar e aferir a eficácia de medidas técnicas e organizacionais a fim de garantir a segurança do processamento.

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

A AWS oferece um anexo de processamento de dados em conformidade com o GDPR (DPA do GDPR) para que você possa cumprir suas obrigações contratuais em relação ao GDPR. O DPA do GDPR 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 GDPR.

Função da AWS nos termos do GDPR

A AWS atua como um processador de dados e um controlador de dados nos termos do GDPR.

- **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 do 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 parceiro do APN pode atuar como um controlador de dados ou processador de dados em si, e a AWS atua como um processador ou um subprocessador de dados. A AWS oferece um anexo de processamento de dados (DPA) em conformidade com o GDPR que incorpora os compromissos da AWS como processador de dados.
- **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 armazena informações de contas para registro de contas, administração, acesso a serviços ou informações de contato da conta da AWS com o objetivo de fornecer ajuda por meio de atividades de suporte ao cliente), atua como um controlador de dados.

O código de conduta da CISPE

O GDPR prevê a aprovação de códigos de conduta para ajudar controladores e processadores a demonstrar conformidade e melhores práticas. Um desses códigos que aguardam aprovação oficial é o código de conduta da CISPE para provedores de serviço de infraestrutura de nuvem (o “Código”). O Código oferece aos clientes a

tranquilidade de que seu provedor de nuvem usa padrões adequados de proteção de dados consistentes com o GDPR.
Alguns dos principais benefícios do Código incluem:

- Esclarecer quem é responsável quando se trata da proteção de dados: o Código de conduta explica a função do provedor e do cliente nos termos do GDPR, especificamente no contexto de serviços de infraestrutura em nuvem.
- O Código de conduta estabelece os princípios a serem seguidos pelos provedores: o Código de conduta desenvolve princípios fundamentais no âmbito do GDPR sobre ações e compromissos claros a serem assumidos pelos provedores para ajudar os clientes a manter a conformidade. Os clientes podem confiar nesses benefícios concretos de sua própria conformidade e suas próprias estratégias de proteção de dados.
- O Código de conduta fornece aos clientes as informações de segurança de que precisam para tomar decisões sobre a conformidade: o Código de conduta exige que os provedores sejam transparentes sobre as medidas tomadas para cumprir os compromissos de segurança. Alguns exemplos dessas etapas são a notificação de violações de dados, a exclusão de dados e o subprocessamento por terceiros, bem como solicitações de autoridades policiais e governamentais. Os clientes podem usar essas informações para compreender integralmente os altos níveis de segurança oferecidos.

Em 13 de fevereiro de 2017, a AWS declarou que os serviços Amazon EC2, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail, e Amazon Elastic Block Store (Amazon EBS) estão em total conformidade com o Código (consulte https://cispe.cloud/publicregister). Essa conformidade proporciona aos clientes garantias adicionais de que controlam totalmente seus dados em um ambiente seguro, protegido e em conformidade quando usam a AWS. A nossa conformidade com o Código complementa a longa lista de certificações e credenciamentos reconhecidos internacionalmente e já obtidos pela AWS, incluindo ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3 e PCI DSS nível 1, entre muitos outros.

Controles de acesso a dados

O artigo 25 do GDPR 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 ajudam os clientes a cumprir esse requisito, permitindo que somente administradores, usuários e aplicativos autorizados acessem os recursos e os dados do cliente da AWS:

- **Acesso detalhado a objetos da AWS em buckets do S3, SQS, SNS e outros –** Você pode conceder permissões diferentes para pessoas e recursos distintos. Por exemplo, você pode conceder a alguns usuários acesso completo aos serviços Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB e Amazon Redshift, entre

outros serviços da AWS. Para outros usuários, você pode conceder acesso somente leitura para apenas alguns buckets do S3, permissões de administração de apenas algumas instâncias do EC2 ou acesso às informações de faturamento e nada mais.

- **Multi-Factor-Authentication (MFA) –** Você pode adicionar autenticação de dois fatores à sua conta e a usuários individuais para aumentar a segurança. Com a MFA, além de fornecer uma senha ou chave de acesso para trabalhar com uma conta, você ou os usuários devem informar um código gerado por um dispositivo especialmente configurado.
- **Autenticação por solicitação de API –** Você pode usar recursos do IAM para fornecer com segurança a aplicativos executados em instâncias do EC2 as credenciais necessárias para acessar outros recursos da AWS, como buckets do S3 e RDS ou bancos de dados do DynamoDB.
- **Restrições geográficas –** Você pode usar restrições geográficas, também conhecidas como bloqueios geográficos, para evitar que usuários em locais geográficos específicos acessem conteúdo de uma distribuição web do CloudFront. Você tem duas opções para usar restrições geográficas:
  - Use o recurso de restrição geográfica do CloudFront. Use esta opção para restringir o acesso a todos os arquivos associados a uma distribuição e restringir o acesso por país.
  - Use um serviço de geolocalização de terceiros. Use esta opção para restringir o acesso a um subconjunto dos arquivos associados a uma distribuição ou para restringir o acesso em um nível mais detalhado que por país.
- **Tokens de acesso temporário por meio do STS –** Você pode usar o AWS Security Token Service (AWS STS) para criar e fornecer aos usuários confiáveis credenciais de segurança temporárias que podem controlar o acesso a recursos da AWS. As credenciais de segurança temporárias funcionam de forma praticamente idêntica às credenciais de chave de acesso de longo prazo usadas pelos usuários do IAM, com as seguintes diferenças:
  - As credenciais de segurança temporárias têm curta duração, como indicado pelo nome. Elas podem ser configuradas para durar por alguns minutos ou várias horas. Após a expiração das credenciais, a AWS deixa de reconhecê-las e não permite qualquer tipo de acesso de solicitações de API com essas credenciais.
  - As credenciais de segurança temporárias não são armazenadas com o usuário, mas são geradas dinamicamente e fornecidas ao usuário mediante solicitação. Quando as credenciais de segurança temporárias expiram (ou até mesmo antes disso), o usuário pode solicitar novas credenciais, desde que ainda tenha permissões para fazê-lo.

  Essas diferenças do uso de credenciais temporárias oferecem as seguintes vantagens:

- Não é necessário distribuir ou incorporar credenciais de segurança de longo prazo da AWS em um aplicativo.
- Você pode conceder aos usuários acesso a recursos da AWS sem necessidade de definir uma identidade da AWS para esses usuários. As credenciais temporárias são a base da federação de funções e identidades.
- As credenciais de segurança temporárias têm um ciclo de vida limitado. Portanto, não é preciso mudá-las frequentemente ou revogá-las quando deixam de ser necessárias. Após a expiração das credenciais de segurança temporárias, elas não podem ser reutilizadas. Você pode especificar o período de validade das credenciais, até um limite máximo.

Monitoramento e registro em log

O GDPR exige que "cada controlador e, se aplicável, o representante do controlador, deve manter um registro de atividades de processamento sob sua responsabilidade". Esse artigo também inclui detalhes sobre as informações que precisam ser registradas. Em outras palavras, o GDPR exige o monitoramento do processamento de dados de PII. Além disso, as obrigações de notificação de violação em tempo hábil exigem a detecção dos incidentes praticamente em tempo real. Para ajudar os clientes a cumprir essas obrigações, a AWS oferece diversos serviços de monitoramento e registro em log:

- **Gerenciamento e configuração de ativos com o AWS Config –** O AWS Config oferece uma visualização detalhada da configuração dos recursos da AWS em uma conta da AWS. Essa visualização inclui a forma como os recursos se relacionam entre si e como foram configurados anteriormente, o que permite ver a evolução das configurações e dos relacionamentos ao longo do tempo.
  Um recurso da AWS é uma entidade com a qual você pode trabalhar na AWS como, por exemplo, uma instância do Amazon Elastic Compute Cloud (EC2), um volume do Amazon Elastic Block Store (EBS), um grupo de segurança ou uma Amazon Virtual Private Cloud (VPC). Para obter uma lista dos recursos da AWS com suporte do AWS Config, consulte Tipos de recursos da AWS com suporte.
  Com o AWS Config, você pode:
  - Avaliar as configurações de recursos da AWS e as definições desejadas.
  - Obter um snapshot das configurações atuais dos recursos com suporte associados à sua conta da AWS.
  - Recuperar configurações de um ou mais recursos existentes em sua conta.
  - Recuperar configurações históricas de um ou mais recursos.
  - Receber uma notificação sempre que um recurso é criado, modificado ou excluído.
  - Ver os relacionamentos entre os recursos. Por exemplo, você pode encontrar todos os recursos que usam um determinado grupo de segurança.

- **Auditoria de conformidade e análise de segurança com o AWS CloudTrail –** Com o AWS CloudTrail, você pode monitorar as implantações da AWS na nuvem obtendo um histórico de chamadas das APIs da AWS na sua conta, incluindo as efetuadas pelo Console de Gerenciamento da AWS, pelos AWS SDKs, pelas ferramentas da linha de comando e pelos serviços da AWS de nível mais alto. Você também pode identificar quais usuários e contas chamaram APIs da AWS para serviços que oferecem 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 em sua organização, verificar o status das trilhas e controlar como os administradores ativam e desativam o registro em log do CloudTrail.
- **Identificação de desafios de configuração por meio do Trusted Advisor –** O registro em log oferece uma forma de entregar logs de acesso detalhados para dados armazenados em um bucket do S3. Um registro de acesso contém detalhes sobre a solicitação, tais como o tipo da solicitação, os recursos especificados na solicitação e a data e hora em que a solicitação foi processada. Para obter mais informações sobre o conteúdo de um log, consulte o formato de log de acesso a servidor no Guia do desenvolvedor do Amazon Simple Storage Service.
- Registros de acesso ao servidor são úteis para muitos aplicativos porque fornecem aos proprietários de buckets uma visão das solicitações feitas por clientes fora de seu controle. Por padrão, o Amazon S3 não coleta registros de acesso ao serviço. No entanto, quando você habilita o registro em log, o Amazon S3 fornece logs de acesso ao bucket a cada hora.
- Registro em log detalhado de acesso a objetos do S3
- Informações detalhadas sobre fluxos na rede por meio dos logs de fluxo da VPC
- Verificações e ações de configuração baseadas em regras com o AWS Config Rules
- Filtragem e monitoramento do acesso HTTP a aplicativos com funções do WAF no CloudFront

Proteção de dados na AWS

O GDPR 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. Por fim, quando ocorre uma violação de dados pessoais e o resultado provável é um risco alto para os direitos e as liberdades de pessoas físicas, mas o controlador implementou “medidas de proteção técnicas e organizacionais adequadas (...) como criptografia”, o controlador não precisa notificar os titulares de dados afetados pela violação, evitando dessa forma os custos administrativos e os danos à reputação. 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:

Criptografia: criptografar dados na AWS

- **Criptografia de dados em repouso com AES-256 (EBS/S3/Glacier/RDS) –** A criptografia de dados ociosos é essencial para a conformidade normativa e garante que dados confidenciais salvos em disco não possam ser lidos por nenhum usuário ou aplicativo sem uma chave válida. A AWS oferece opções de dados em repouso e gerenciamento de chaves para oferecer suporte ao processo de criptografia. 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. Além disso, o Amazon RDS oferece suporte à Transparent Data Encryption (TDE – Criptografia transparente de dados).

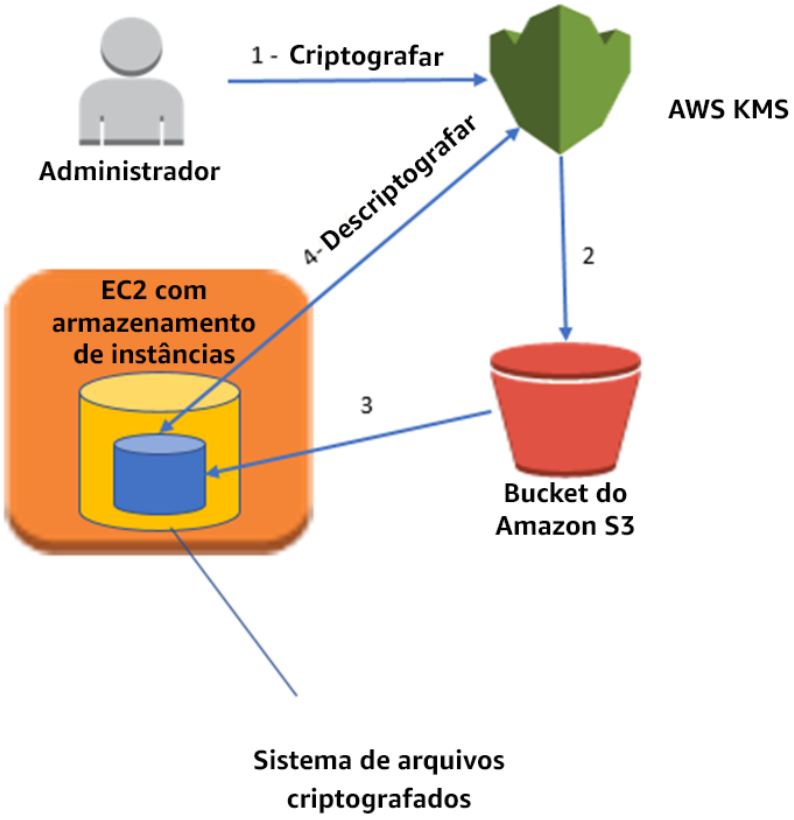
  O armazenamento de instâncias oferece armazenamento temporário de blocos para instâncias do Amazon EC2. Esse armazenamento é localizado em discos conectados fisicamente ao computador host. O armazenamento de instâncias é ideal para armazenamento temporário de informações que mudam frequentemente, como buffers, caches e dados de trabalho. Por padrão, os arquivos armazenados nesses discos não são criptografados. Um método para criptografar dados em armazenamentos de instância do EC2 no Linux é usar as bibliotecas incorporadas do Linux. 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.

  - **Criptografia de discos e sistema de arquivos** – Você pode usar dois métodos para criptografar arquivos em armazenamentos de instância. O primeiro método é a criptografia de disco, em que um disco ou bloco inteiro dentro do disco é criptografado usando uma ou mais chaves de criptografia. A criptografia de disco opera abaixo do nível de sistema de arquivos, é independente 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.

    O segundo método é a criptografia de sistema de arquivos. Os arquivos e diretórios são criptografados, mas não a partição ou o disco inteiro. A criptografia de sistema de arquivos opera com base no sistema de arquivos e permite a portabilidade entre sistemas operacionais.
  - **A infraestrutura Linux dm-crypt** – O dm-crypt é um mecanismo de criptografia de kernel do Linux que permite que os usuários montem um sistema de arquivos criptografado. A montagem de um sistema de arquivos é um processo em que um sistema de arquivos é conectado a um diretório (ponto de montagem), disponibilizando-o ao sistema operacional. Após a montagem, todos os arquivos do sistema de arquivos estão disponíveis para

aplicativos sem interações adicionais. No entanto, esses arquivos são criptografados quando armazenados no disco.
O mapeador de dispositivos é uma infraestrutura do kernel 2.6 e 3.x do Linux que oferece uma forma genérica de criar camadas virtuais de dispositivos de blocos. A criptografia de destino 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.

- **Visão geral de arquitetura** – O diagrama de arquitetura resumido a seguir mostra a solução proposta para possibilitar a criptografia do armazenamento de instâncias do EC2. Veja na próxima seção um plano de implementação



detalhado.

1. O administrador criptografa uma senha secreta usando o KMS. A senha criptografada é salva em um arquivo.
2. O administrador coloca o arquivo que contém a senha criptografada em um bucket do S3.

3. Quando é inicializada, a instância copia o arquivo criptografado para um disco interno.
4. Em seguida, a instância do EC2 descriptografa o arquivo usando o KMS e recupera a senha em texto simples. A senha é usada para configurar o sistema de arquivos criptografado do Linux com o LUKS. Todos os dados gravados no sistema de arquivos criptografado são criptografados usando um algoritmo de criptografia AES-256 quando armazenados em disco.

- **Gerenciamento de chaves centralizado (por região)** – O AWS Key Management Service (KMS) é um serviço gerenciado que facilita a criação e o controle de chaves de criptografia usadas para criptografar dados, além de usar módulos de segurança de hardware (HSMs) para proteger a segurança das chaves. O AWS Key Management Service é integrado a vários outros serviços da AWS para ajudar você a proteger os dados que armazena nesses serviços. O AWS Key Management Service também é integrado com o AWS CloudTrail para fornecer logs contendo toda a utilização das chaves para ajudar a cumprir requisitos normativos e de conformidade.
  - **Gerenciamento de chaves centralizado** – O AWS Key Management Service fornece controle centralizado de chaves de criptografia. Você pode criar, importar e mudar facilmente as chaves, além de definir políticas de uso e auditar a utilização por meio do Console de Gerenciamento da AWS ou usando o AWS SDK ou a ILC. As chaves mestras no KMS, tanto as importadas quanto as criadas em seu nome pelo KMS, são armazenadas em um formato criptografado em um armazenamento altamente resiliente, o que ajuda a garantir sua recuperação quando necessário. Você pode solicitar que o KMS mude automaticamente as chaves mestras criadas no KMS uma vez por ano sem a necessidade de criptografar novamente os dados que já foram criptografados com a chave mestra, uma ação conhecida por rotação de chaves. Você não precisa monitorar as versões anteriores das chaves mestras, pois o KMS as mantém disponíveis para descriptografar dados anteriormente criptografados. Você pode criar novas chaves mestras e controlar quem tem acesso a essas chaves e com quais serviços elas podem ser usadas sempre que você quiser. Você também pode importar chaves da sua própria infraestrutura de gerenciamento de chaves e usá-las no KMS.
  - **Integração a serviços da AWS** – O AWS Key Management Service é totalmente integrado a vários outros serviços da AWS. Essa integração significa que você pode usar facilmente as chaves mestras do AWS KMS para criptografar os dados armazenados nesses serviços. É possível usar uma chave mestra padrão criada automaticamente para você e que só pode ser utilizada no serviço integrado, ou selecionar uma chave mestra

personalizada criada no KMS ou importada da sua própria infraestrutura de gerenciamento de chaves para a qual você tem permissão de uso.

- **Recursos de auditoria** – Se o AWS CloudTrail estiver habilitado para sua conta da AWS, cada utilização de uma chave que você armazenar no KMS será registrada em um arquivo de log que será enviado para o bucket do Amazon S3 que você especificou quando habilitou o AWS CloudTrail. As informações registradas incluem detalhes do usuário, hora, data e a chave usada.
- **Escalabilidade, resiliência e alta disponibilidade** – O AWS Key Management Service é um serviço gerenciado. Não é necessário comprar infraestrutura de gerenciamento de chaves adicional para acompanhar o crescimento do uso das chaves de criptografia do AWS KMS. O AWS KMS oferece escalabilidade automática para atender às suas necessidades de chaves de criptografia.
  As chaves mestras criadas em seu nome pelo AWS KMS ou importadas por você não podem ser exportadas do serviço. O AWS KMS armazena várias cópias de versões criptografadas das chaves em sistemas projetados para ter resiliência de 99,999999999%, o que ajuda a garantir a disponibilidade das chaves quando for necessário acessá-las. Se você importar chaves para o KMS, deverá manter de modo seguro uma cópia das chaves para que possa importá-las novamente a qualquer momento.
  O AWS KMS é implantado em várias zonas de disponibilidade dentro de uma região da AWS para proporcionar alta disponibilidade para as chaves de criptografia.
- **Seguro** – O AWS KMS foi projetado para que ninguém tenha acesso às suas chaves mestras. O serviço é criado com base em sistemas projetados para proteger as chaves mestras com técnicas de proteção abrangentes, como nunca armazenar chaves mestras em texto simples em disco, não as manter na memória e controlar quais sistemas podem acessar hosts que usam as chaves. Todo 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 saber mais sobre como o AWS KMS funciona, leia o whitepaper sobre o AWS Key Management Service.

- **Túneis IPsec para a AWS com gateways VPN** – A Amazon VPC permite provisionar uma seção logicamente isolada da nuvem da Amazon Web Services (AWS). Nessa seção, você pode executar recursos da AWS em uma rede virtual que você mesmo define. Você tem controle total sobre seu ambiente de rede virtual, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub-redes e configuração de tabelas de rotas e gateways de rede. Além disso, você pode criar uma conexão de Virtual Private Network (VPN) por hardware entre o datacenter corporativo e a VPC e usar a Nuvem AWS como uma extensão desse datacenter.

É possível personalizar facilmente a configuração da rede para a Amazon VPC. Por exemplo, você pode criar uma sub-rede pública para os servidores web que têm acesso à Internet e dispor os sistemas back-end como bancos de dados ou servidores de aplicativos em uma sub-rede privada sem acesso à Internet. Você pode aproveitar várias camadas de segurança, como grupos de segurança e listas de controle de acesso à rede, para ajudar a controlar o acesso às instâncias do Amazon EC2 em cada sub-rede.

- **Módulos HSM dedicados na nuvem com o CloudHSM –** O serviço AWS CloudHSM ajuda a cumprir requisitos de conformidade corporativos, contratuais e normativos para a segurança de dados usando dispositivos Hardware Security Module (HSM – Módulo de segurança de hardware) dedicados dentro da Nuvem AWS. Com o CloudHSM, você controla as chaves e as operações de criptografia executadas pelo HSM.
  Os parceiros da AWS e do AWS Marketplace oferecem diversas soluções para a proteção de dados confidenciais dentro da AWS. No entanto, ocasionalmente, pode ser necessário oferecer proteção adicional para aplicativos e dados sujeitos a rigorosos requisitos contratuais ou normativos de gerenciamento de chaves criptográficas. Até agora, a única opção disponível era armazenar os dados confidenciais (ou as chaves de criptografia que protegem os dados confidenciais) em datacenters locais. Infelizmente, essa opção impedia a migração desses aplicativos para a nuvem ou reduzia consideravelmente sua performance. O serviço AWS CloudHSM permite que você proteja suas chaves de criptografia dentro de HSMs designados e validados de acordo com padrões governamentais para o gerenciamento seguro de chaves. É possível gerar, armazenar e gerenciar as chaves de criptografia usadas na criptografia de dados de tal forma que somente 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 a Amazon Virtual Private Cloud (VPC). As instâncias de CloudHSM são provisionadas dentro da sua VPC com o endereço IP que você especificar, oferecendo conectividade a redes simples e privadas para instâncias do Amazon Elastic Compute Cloud (EC2). O posicionamento das instâncias do CloudHSM perto das instâncias do EC2 reduz a latência de rede, o que pode aumentar a performance do aplicativo. A AWS fornece acesso dedicado e exclusivo (single tenant – único locatário) a instâncias do CloudHSM de forma isolada dos outros clientes da AWS. Disponível em várias regiões e zonas de disponibilidade (AZs), o AWS CloudHSM permite que você adicione aos aplicativos um armazenamento de chaves seguro e resiliente.
    - **Integrado** – Você pode usar o CloudHSM com o Amazon Redshift, o Amazon Relational Database Service (RDS) Oracle ou aplicativos de terceiros, como SafeNet Virtual KeySecure, para atuar como uma raiz de confiança, Apache (terminação de SSL) ou Microsoft SQL Server (criptografia de dados transparente). Você também pode usar o CloudHSM para escrever seus próprios aplicativos e continuar a usar as

bibliotecas de criptografia padrão que já conhece, incluindo PKCS#11, Java JCA/JCE e Microsoft CAPI e CNG.

- **Auditável** – Se você precisar rastrear alterações de recursos ou auditar atividades para fins de segurança e conformidade, poderá usar o CloudTrail para revisar todas as chamadas de API do CloudHSM efetuadas em sua conta. Além disso, é possível auditar operações no dispositivo HSM usando o syslog ou enviando mensagens de log do syslog ao seu próprio coletor.

Estrutura de conformidade e padrões de segurança sólidos

De acordo com o GDPR, 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. A AWS oferece aos clientes uma estrutura de conformidade sólida e padrões de segurança avançados.

Modelo de responsabilidade de segurança compartilhada

Antes de detalharmos como a AWS protege os dados, devemos analisar o que torna a segurança na nuvem um pouco diferente da segurança em datacenters locais. Quando você transfere sistemas e dados para a nuvem, a responsabilidade pela segurança passa a ser compartilhada entre você e seu provedor de serviços de nuvem. Neste caso, a AWS é responsável pela proteção da infraestrutura subjacente que oferece suporte à nuvem, e você é responsável por tudo aquilo que coloca na nuvem ou conecta à nuvem. Esse modelo de responsabilidade de segurança compartilhada pode reduzir a carga operacional de muitas formas e, em alguns casos, até melhorar a postura habitual de segurança sem que você precise fazer nada.

Responsabilidades de segurança da AWS

A Amazon Web Services é responsável pela proteção da infraestrutura global que executa todos os serviços oferecidos na Nuvem AWS. Essa infraestrutura abrange o hardware, o software, as redes e as instalações que executam os serviços da AWS. Proteger essa infraestrutura é a maior prioridade da AWS. Embora você não possa visitar nossos escritórios e datacenters para ver essa proteção diretamente, nós disponibilizamos vários relatórios de auditores independentes que verificaram nossa conformidade com diversas normas e padrões de segurança em computação. Para obter mais informações, acesse aws.amazon.com/compliance.

Além de proteger essa infraestrutura global, a AWS é responsável pela configuração de segurança dos produtos considerados serviços gerenciados que oferece. Entre os exemplos desses tipos de serviços incluem-se o Amazon DynamoDB, o Amazon RDS, o Amazon Redshift, o Amazon Elastic MapReduce, o Amazon WorkSpaces e vários

outros. Eles permitem a escalabilidade e a flexibilidade dos recursos baseados na nuvem com o benefício adicional de serem gerenciados. No caso desses serviços, a AWS cuidará das tarefas básicas de segurança, como aplicação de patches a bancos de dados e sistemas operacionais (SOs) convidados, configuração de firewalls e recuperação de desastres. No caso da maioria desses serviços gerenciados, você só precisa configurar controles de acesso lógico aos recursos e proteger as credenciais de sua conta. Alguns deles podem exigir tarefas adicionais, como configurar contas de usuário do banco de dados. Entretanto, no geral a configuração da segurança é executada pelo serviço.

Responsabilidades de segurança do cliente

Com a nuvem AWS, você pode provisionar servidores virtuais, armazenamento, bancos de dados e desktops em minutos, em vez de semanas. Além disso, pode usar ferramentas de fluxo de trabalho e análise baseadas na nuvem para processar seus dados e armazená-los em seus próprios datacenters ou na nuvem. Os serviços da AWS que você usar é que vão determinar o volume de trabalho de configuração que estará entre suas responsabilidades de segurança.

Os produtos da AWS que se inserem na conhecida categoria de Infrastructure as a Service (IaaS, Infraestrutura como serviço), como o Amazon EC2, a Amazon VPC e o Amazon S3, ficam inteiramente sob seu controle, exigindo que você execute todas as tarefas de configuração e gerenciamento de segurança necessárias. No caso das instâncias do EC2, por exemplo, você é responsável pelo gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança) e de todos os utilitários ou aplicativos de software que instalar nas instâncias, bem como pela configuração do firewall fornecido pela AWS (security group – grupo de segurança) em cada instância. Essas são basicamente as mesmas tarefas de segurança que você já está habituado a executar, independentemente da localização de seus servidores.

Os AWS Managed Services, como o Amazon Relational Database Service (RDS) ou o Amazon Redshift, fornecem todos os recursos que você precisa para executar uma determinada tarefa, só que sem o trabalho de configuração que geralmente os acompanham. Com eles, você não precisa se preocupar com execução e manutenção de instâncias, correção de bancos de dados e SOs convidados nem com replicação de bancos de dados: a AWS cuida disso tudo para você. Porém, como em todos os serviços, você deve proteger as credenciais de sua conta da AWS e configurar a conta de cada usuário com o Amazon Identity and Access Management (IAM) para que eles tenham suas próprias credenciais e você possa implementar a segregação de tarefas. Recomendamos também o uso de multi-factor authentication (MFA) em todas as contas, que requer SSL/TLS para comunicação com seus recursos na AWS, e a configuração de um registro em log de atividades da API e dos usuários com o AWS CloudTrail. Para obter informações sobre as medidas adicionais que você pode adotar, consulte o whitepaper Melhores práticas de segurança da AWS e as leituras recomendadas na página Recursos de segurança da AWS.

Programa de conformidade da AWS

O programa de conformidade da Amazon Web Services permite que os clientes entendam os rígidos controles que existem na AWS para manter a segurança e a proteção de dados na nuvem. À medida que os sistemas são construídos com base na infraestrutura da Nuvem AWS, as responsabilidades de conformidade são 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. Projetada e gerenciada conforme as melhores práticas de segurança, a infraestrutura de TI da AWS obedece a vários padrões de segurança do setor, entre os quais:

- SOC 1/SSAE 16/ISAE 3402 (antigo SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP e FedRAMP
- SRG do DoD
- PCI DSS nível 1
- ISO 9001/ISO 27001
- ITAR
- FIPS 140-2
- MTCS nível 3

Além disso, a flexibilidade e o controle que os produtos e serviços da AWS oferecem aos clientes permitem implantar soluções que atendem a diversos padrões específicos do setor, entre os quais:

- Serviços de Informação da Justiça Criminal (CJIS)
- Cloud Security Alliance (CSA)
- Lei da privacidade e dos direitos educacionais da família (FERPA)
- Lei de Portabilidade e Responsabilidade de Provedores de Saúde (HIPAA)
- Motion Picture Association of America (MPAA)

A AWS fornece aos seus clientes uma ampla variedade de informações relacionadas ao seu ambiente de controle de TI por meio de whitepapers, relatórios, certificações e declarações de terceiros. Para obter mais informações, consulte o whitepaper Risco e conformidade.

Cloud Computing Compliance Controls Catalog (C5 – Esquema de credenciamento baseado no governo alemão)

O Cloud Computing Compliance Controls Catalog (C5) é um credenciamento apoiado pelo governo alemão, introduzido na Alemanha pelo departamento federal de segurança das informações (BSI) para ajudar as organizações a demonstrar segurança

operacional contra ataques cibernéticos comuns dentro do contexto do documento Security Recommendations for Cloud Providers do governo alemão.
O credenciamento C5 pode ser usado por clientes da AWS e seus consultores de conformidade para compreender a gama de serviços de garantia de segurança de TI oferecida pela AWS na movimentação de cargas de trabalho 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 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, os clientes podem avaliar como regulamentos legais (por exemplo, privacidade de dados), suas próprias políticas ou o ambiente de ameaças se relacionam ao uso de serviços de computação em nuvem.

Revisões do documento

Data	Descrição
Setembro de 2018	Pequenas atualizações.
Novembro de 2017	Primeira publicação