Separação lógica

Uma avaliação das exigências de segurança de nuvem para cargas de trabalho sensíveis do Departamento de Segurança dos EUA

Maio de 2018

[Série de Guias Governamentais da AWS]

Avisos

Este documento é fornecido 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 obrigações da AWS para com seus clientes são controladas por contratos da AWS, e este documento não modifica nem faz parte de qualquer contrato entre a AWS e seus clientes.

Índice

Finalidade

Este documento examina a equivalência de segurança da separação lógica para clientes que usam a infraestrutura como serviço (IaaS) da Amazon Web Services (AWS) para atender às exigências de separação apresentadas no Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG). Analisa também uma abordagem tríplice — utilização de virtualização, criptografia e implantação de computação em hardware dedicado — que os governos do mundo inteiro podem usar para migrar com segurança para a nuvem cargas de trabalho sensíveis mas não confidenciais (*por exemplo*, de alto impacto) sem a necessidade de uma infraestrutura física específica.

Introdução

A tecnologia de nuvem tira proveito das técnicas transformativas da tecnologia da informação (TI). Os clientes que utilizam a nuvem podem se beneficiar de um datacenter e uma arquitetura de rede criados para atender às organizações mundiais com as maiores exigências de segurança. Os novos modelos operacionais e as novas abstrações fornecidos pelas tecnologias de nuvem contribuem para a criação de um ambiente de TI seguro. Os provedores de serviço em nuvem (CSPs) como a AWS usam a nuvem para inovar e, desse modo, entregar aos clientes recursos de segurança novos e aprimorados. A AWS fornece serviços prontamente disponíveis e comporta recursos de "defesa em profundidade" e de "defesa em amplitude" com mecanismos de segurança intrínsecos para projetos e operações de serviços em nuvem.

A AWS oferece intencionalmente aos clientes domínio e controle sobre seu conteúdo por meio de ferramentas que lhes permitem determinar onde esse conteúdo será armazenado. Com os recursos fornecidos pela AWS, os clientes podem proteger seu conteúdo em trânsito e repouso e gerenciar o acesso de seus usuários aos serviços e recursos da AWS. Os clientes da AWS têm total controle sobre o acesso a seu conteúdo, o que impede que usuários e clientes não autorizados acessem a conta de outros clientes. A AWS fornece serviços multilocatário com a melhor segurança de separação de locatários do setor. Essa separação lógica entre ambientes de cliente fornecida pela AWS oferece uma segurança mais eficaz e mais confiável do que a oferecida por infraestruturas físicas dedicadas.

Plano de fundo

Em dezembro de 2011, o diretor executivo de informação federal dos Estados Unidos instituiu uma ampla política governamental exigindo que os órgãos federais usem o Programa Federal de Gerenciamento de Risco e Autorização (FedRAMP), um programa padronizado de âmbito federal destinado à autorização de segurança de serviços em nuvem. A abordagem "do once, use many times" (faça uma vez para usar sempre) do FedRAMP foi concebida para oferecer benefícios significativos, como aumentar a consistência e confiabilidade da avaliação de controles de segurança, reduzir os custos dos provedores de serviço e clientes governamentais e otimizar as avaliações de autorização duplicativa entre as agências do governo que adquirem o mesmo serviço. O principal órgão de governança e tomada de decisões do FedRAMP é o Conselho de Autorização Conjunta (JAB), composto pelos diretores executivos de informação (CIOs) da Administração de Serviços Gerais, do Departamento de Segurança Nacional e do DoD.

Atualmente, o FedRAMP tem três parâmetros de segurança padronizados — baixo, moderado e alto impacto —, que se baseiam nas categorizações da publicação 199 do Federal Information Processing Standard (FIPS). Esses parâmetros foram desenvolvidos com a colaboração de especialistas em segurança cibernética do setor privado e do governo dos Estados Unidos (incluindo o DoD). Embora o DoD tenha estabelecido reciprocidade com o parâmetro moderado do FedRAMP, não a estabeleceu com o parâmetro alto do FedRAMP. Em vez disso, o DoD desenvolveu e implementou o que efetivamente constitui um conjunto de controles e exigências de segurança, o "FedRAMP plus", por meio do DoD Cloud Computing Security Requirements Guide (SRG).

Particularmente, o DoD requer por meio do SRG a separação entre locatários/missões do DoD e do governo federal mediante meios físicos e lógicos. Mais especificamente, o SRG estabelece que os "CSPs devem apresentar evidência de sólidos controles de separação virtual e monitoramento e capacidade para atender a solicitações de 'busca e captura' sem divulgar informações e dados do DoD". Mais do que isso, para sistemas com impacto de nível 5 (IL5),[1] o DoD requer a "separação física (por exemplo, infraestrutura dedicada) de locatários não pertencentes ao DoD/governo federal". Essas exigências do DoD baseiam-se em suas preocupações quanto à mesclagem de dados do DoD com dados de outros locatários, em virtude de vazamento ou derramamento de dados e do acesso não autorizado ou da adulteração de dados do DoD por locatários que não pertencem ao DoD.

Para implementar melhores práticas direcionadas a resultados, o SRG reconhece o uso da separação lógica como uma abordagem viável para atender às exigências de separação IL5 do DoD:

> *"Um CSP pode oferecer soluções alternativas que forneçam uma segurança equivalente em relação aos requisitos estabelecidos. A aprovação será avaliada caso a caso durante o processo de avaliação de autorização provisória."*

---

1 5.2.2.2 Exigências de localização e separação de impacto de nível 5

As informações que devem ser processadas e armazenadas de acordo com o impacto de nível 5 só podem ser processadas em uma infraestrutura dedicada, local ou externa, em qualquer modelo de implantação de nuvem que restrinja a localização física das informações tal como descrito na seção 5.2.1, "Exigências de jurisdição/localização". Isso exclui produtos e serviços do setor público.

O seguinte se aplica:

- Somente as nuvens privadas do DoD, da comunidade do DoD ou da comunidade do governo federal são qualificadas para o impacto de nível 5.
- Um modelo de implantação pode comportar várias missões ou locatários/missões de cada organização de cliente.
- A separação virtual/lógica entre locatários/missões do DoD e do governo federal é permitida.
- A separação virtual/lógica entre sistemas de locatários/missões é uma exigência mínima.
- A separação física (por exemplo, infraestrutura dedicada) de locatários não pertencentes ao DoD/governo federal é obrigatória.

OBSERVAÇÃO: um CSP pode oferecer soluções alternativas que forneçam uma segurança equivalente em relação aos requisitos estabelecidos. A aprovação será avaliada caso a caso durante o processo de avaliação de autorização provisional.

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

Quais são as desvantagens das exigências de separação física?

As exigências de ofertas de nuvem fisicamente dedicadas são determinadas principalmente por preocupações com o acesso de terceiros ou outros tipos de acesso não autorizado a aplicativos, conteúdo ou dados, incluindo o acesso imposto para aplicação da lei e o acesso não autorizado de terceiros. Entretanto, com relação a sistemas que podem ser acessados por rede ou via Internet, a separação física desses sistemas, como colocá-los em compartimentos trancados ou em uma instalação de datacenter separada, não aumenta a segurança nem o controle sobre o acesso. Em suma, todos os controles de acesso direcionados a sistemas conectados são gerenciados por meio de controles de acesso lógicos, gerenciamento de permissões, tráfego de rede e criptografia. A AWS trata qualquer preocupação de separação física por meio dos recursos de segurança lógica que fornecemos a todos os nossos clientes e dos controles de segurança que temos atualmente para proteger os dados do cliente, descritos mais detalhadamente abaixo na abordagem de separação lógica em três vertentes.

Ambientes menores e fisicamente separados não têm paridade com ambientes de nuvem disponíveis de maneira geral. Assim, qualquer requisito de separação física pode limitar ou atrasar a capacidade de um cliente de utilizar investimentos inovadores (incluindo inovações em recursos de segurança) feitos em nome de todos os clientes que usam os serviços da AWS. As desvantagens também incluem estrutura de maior custo e menor utilização resultantes do uso menos eficiente do espaço, bem como opções e recursos de redundância limitada em comparação à diversidade geográfica das regiões comerciais do datacenter.

De que maneira a separação lógica é mais eficiente que a separação física?

Os clientes podem utilizar a abordagem de três vertentes abaixo para atender com êxito os resultados de segurança equivalentes à separação física, conforme exigido pelo IL5 do DoD.

1. Virtual Private Cloud (VPC) – demonstração suficiente de que a VPC cria o equivalente de domínios de rede completamente separados para cada locatário;
2. Criptografia de dados em repouso e em trânsito – utilização de recursos de criptografia de dados intrínsecos ou fornecidos pelo usuário dos serviços de nuvem AWS, como EBS, S3 e DynamoDB, com chaves de criptografia geradas e armazenadas pelo AWS Key Management Service (KMS) e/ou AWS Cloud Hardware Security Module (CloudHSM); e
3. Hosts dedicados, instâncias dedicadas e bare metal – proprietários de missões do DoD podem provisionar os hosts físicos da AWS para processar instâncias de máquina hipervisionadas e não hipervisionadas atribuídas e as cargas de trabalho correspondentes.

1. Virtual Private Cloud (VPC)

A VPC da AWS possibilita a criação de um enclave de rede logicamente separado dentro da rede do AWS Elastic Cloud Compute (Amazon EC2), que pode hospedar recursos de computação e armazenamento. Esse ambiente pode ser conectado a uma infraestrutura existente do cliente por uma conexão de rede privada virtual (VPN) pela Internet, ou pelo AWS Direct Connect, um serviço que fornece conectividade privada dentro da nuvem AWS. O uso de uma VPC oferece aos proprietários de missões flexibilidade, segurança e controle completo de sua presença de rede na nuvem. Permite uma transição controlada para a nuvem usando um modelo de datacenter e um esquema de gerenciamento existentes do cliente. O cliente controla o ambiente privado, incluindo endereços IP, sub-redes, listas de controle de acesso à rede, security groups, firewalls de sistemas operacionais, tabelas de rotas, VPNs e/ou gateways da Internet. A Amazon VPC fornece isolamento lógico robusto de todos os recursos do cliente. Por exemplo, cada fluxo de pacotes na rede é autorizado individualmente para validar a fonte e o destino corretos antes de transmitido e entregue. Não é possível que as informações sejam passadas entre diversos locatários sem serem especificamente autorizadas tanto pelo cliente que está transmitindo, como pelo que está recebendo. Se um pacote estiver sendo roteado para um destino sem uma regra que corresponda a ele, o pacote será descartado. Ademais, apesar de pacotes Address Resolution Protocol (ARP – Protocolo de resolução do endereço) acionarem uma pesquisa autenticada de banco de dados, pacotes ARP nunca chegam à rede, já que não são necessários para descobrir a topologia de rede virtual. Assim, a falsificação do ARP é impossível. Além disso, o modo promíscuo não revela nenhum tráfego além daquele vinculado ao sistema operacional do cliente. Esses conjuntos precisos de regras de entrada e saída de tráfego definidos pelo cliente não só permitem aumentar a flexibilidade da conectividade, mas permitem maior controle do cliente sobre a segmentação e o roteamento do tráfego.

Por exemplo, opções de conectividade da VPC[2] incluem a capacidade do cliente de:

- Conectar-se à Internet usando a Conversão de endereços de rede (sub-redes privadas) – sub-redes privadas podem ser utilizadas para instâncias que não deveriam ter acesso direto à ou da Internet. As instâncias em uma sub-rede privada podem acessar a Internet sem expor seu endereço IP privado ao rotear seu tráfego por um gateway da Conversão de endereços de rede (NAT) em uma sub-rede pública.
- Conectar-se com segurança ao datacenter corporativo – todo o tráfego de e para instâncias na VPC pode ser roteado para o datacenter corporativo por uma conexão VPN criptografada de hardware IPsec padrão do setor.
- Conectar-se de maneira privada a outras VPCs – una VPCs para compartilhar recursos entre várias redes virtuais pertencentes às suas contas da AWS.
- Conecte de maneira privada seus serviços internos entre diferentes contas e VPCs dentro de suas organizações, simplificando significativamente sua arquitetura de rede interna.

---

2 Observação: o uso da VPC com um gateway privado para uma solução aprovada do Cloud Access Point (CAP) ou Secure Cloud Computing Architecture (SCCA) do DoD é obrigatório para todos os clientes que usam cargas de trabalho IL5 do SRG na região AWS GovCloud (EUA), a menos que seja dispensada pelo CIO do DoD.

2. Criptografar dados em repouso e em trânsito

Para dados que proprietários de missões estejam armazenando nos serviços de armazenamento da AWS ou que estejam transitando em nossas redes, é altamente recomendável que dados em repouso e em trânsito sejam criptografados. Para ficar mais fácil e seguro para nossos clientes, fornecemos um número de ferramentas e recursos que os permitem criptografar dados, bem como diversas opções de infraestrutura de gerenciamento de chaves de criptografia. Esses recursos de criptografia e controle de acesso a dados já estão integrados nas ofertas de serviços básicos, como o Amazon Simple Storage Service (Amazon S3), um serviço de armazenamento de objetos altamente escalável, o Amazon Elastic Block Store (Amazon EBS), que fornece armazenamento anexado à rede para instâncias do EC2, e o Amazon Relational Database Service (Amazon RDS), que fornece mecanismos de banco de dados gerenciados. Esses recursos estão prontos e fornecem uma vasta documentação para ajudar os clientes a entenderem como seus dados estão sendo protegidos e as opções de configurações que podem controlar para personalizar quem pode acessar os sistemas. Os serviços nativos da AWS têm recursos de segurança em evolução que, em ambientes herdados, só foram alcançáveis por uma junção de outros fornecedores. Agora esses recursos estão cada vez mais disponíveis, permitindo que os clientes se concentrem na inovação dos serviços.

A combinação do AWS Key Management Service (KMS) e do AWS CloudHSM é a peça central de uma rigorosa solução de criptografia. O AWS KMS é um serviço regional totalmente gerenciado e altamente disponível que usa módulos de segurança de hardware (HSMs) validados pelo FIPS 140-2 nível 3 (segurança física)[3] em sua base, com um sofisticado software de escalabilidade horizontal que pode atender centenas de milhares de solicitações de API por segundo. Ele dá aos clientes a capacidade de realizar as principais funções de gerenciamento de uma maneira profundamente integrada a outros serviços da AWS. O AWS CloudHSM fornece um HSM dedicado do FIPS 140-2 nível 3 (geral) sob seu controle exclusivo, diretamente em sua Amazon Virtual Private Cloud (VPC).[4] O serviço do CloudHSM fornece backup, replicação e disponibilidade automatizada dos HSMs dedicados e de cliente único nas zonas de disponibilidade. Ele se integra aos aplicativos de propriedade do cliente usando APIs de criptografia padrão do setor. Embora aplicável em diferentes contextos, ambos os serviços servem para garantir que o algoritmo de criptografia seja robusto o bastante para tornar os dados ininteligíveis e as chaves suficientemente protegidas, para que assim o texto cifrado fique ilegível para pessoas não autorizadas. Em outras palavras, o armazenamento de dados apropriadamente criptografados com chaves devidamente gerenciadas e protegidas pode ser uma garantia de que os dados estão totalmente protegidos. Essa abordagem é igualmente relevante, aplicável e eficaz, independentemente de ser implantada em um ambiente de nuvem comercial fisicamente ou logicamente isolado.

3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139

4 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3108

Por meio da criptografia, a confidencialidade das chaves criptográficas do proprietário da missão é crucial. A segurança depende de onde os dados foram criptografados e de quem tem acesso a eles e está protegendo as chaves. Se os dados forem criptografados pelo proprietário da missão antes de serem incorporados na nuvem, não há motivo para os CSPs terem acesso às chaves — o proprietário da missão tem total controle e responsabilidade. Entretanto, se os dados forem criptografados usando serviços nativos dos CSPs, tanto os CSPs quanto o proprietário da missão estarão na cadeia de custódia das chaves. O AWS KMS foi desenvolvido para que ninguém, inclusive os funcionários da AWS, consiga recuperar chaves em texto simples do serviço. O serviço usa HSMs validados pelo FIPS 140-2 para proteger a confidencialidade e integridade de suas chaves, independentemente de você solicitar que o KMS crie as chaves em seu nome ou de importá-las para o serviço. As chaves em texto simples nunca são gravadas no disco e somente são usadas na memória volátil dos HSMs durante o tempo necessário para realizar a operação criptográfica solicitada. As chaves do KMS nunca são transmitidas para fora da região da AWS na qual foram criadas. As atualizações do firmware do KMS HSM são controladas por acesso de quorum auditado e revisto por um grupo independente da Amazon. Esses processos, procedimentos e políticas foram auditados independentemente e reconhecidos pelo FedRAMP e pelo DoD. A seção a seguir resume os recursos do AWS KMS e do AWS CloudHSM. Os clientes podem consultar os links incorporados sobre recursos adicionais no AWS KMS e AWS CloudHSM.

AWS Key Management Service (KMS)

o AWS Key Management Service (KMS) fornece aos clientes controle centralizado sobre as chaves de criptografia usadas para proteger seus dados. Por meio do AWS KMS, os clientes podem criar, alternar, desabilitar, excluir e definir políticas de chaves de criptografia e auditar o uso dessas chaves para criptografar dados dos clientes. O AWS KMS é integrado aos serviços da AWS para facilitar a criptografia de dados armazenados nesses serviços com chaves de criptografia gerenciadas pelo cliente (ou por meio de chaves de criptografia padrão que o serviço da AWS gerencia em nome do cliente). Esse serviço está incluído entre os cinco serviços fundamentais reconhecidos para atender às exigências IL5 do DoD para habilitar a criptografia de dados em repouso e em trânsito e fornecer separação lógica suficiente de dados do DoD que transitam pela infraestrutura da AWS e estão localizados no mesmo hardware que os dados de clientes não relacionados ao DoD. Por exemplo, no caso de dados em repouso, o uso de algoritmos criptográficos robustos para separação lógica de dados de clientes é o princípio para estabelecer equivalência com a separação física de dados em repouso, uma exigência do IL5.

A fronteira de segurança interna do AWS KMS é o módulo de segurança de hardware (HSM). O HSM tem uma API interna limitada baseada na web e sem nenhuma outra interface física em seu estado operacional. Um HSM operacional é configurado e carregado com as chaves criptográficas apropriadas durante a inicialização. O material criptográfico sensível do HSM é armazenado somente na memória volátil e apagado quando o HSM sai do estado operacional, inclusive de encerramentos não intencionais ou reinicializações. Quando se encontra no estado operacional, nenhum operador humano pode acessar o HSM. Somente os hosts de serviço que lidam com solicitações dos clientes podem fazer conexões por meio da API limitada. As APIs do HSM estão disponíveis em uma sessão confidencial mutuamente autenticada por operadores humanos (quando não operacional) ou hosts de serviço (quando operacional).

O sistema foi desenvolvido para que vários operadores humanos que usam autenticação de dois fatores sejam obrigados a atualizar o firmware ou a configuração de software, por meio de um processo de quorum, de qualquer HSM no KMS, mas até mesmo nesse caso somente depois que é posto em estado não operacional e não contém nenhum material importante.

> **Observação:** Agora, o AWS Key Management Service (KMS) usa módulos de segurança de hardware (HSMs) validados pelo FIPS 140-2 e comporta endpoints validados pelo FIPS 140-2, que fornecem garantias independentes quanto à confidencialidade e integridade de suas chaves.

HSM da Nuvem AWS

O AWS CloudHSM oferece um eficiente gerenciamento de chaves de hardware em escala de nuvem para cargas de trabalho confidenciais e regulamentadas. O CloudHSM permite que os proprietários de missão forneçam e utilizem chaves criptográficas para criptografar seus dados dentro dos serviços da AWS, bem como seus aplicativos residentes. O CloudHSM permite que os clientes gerenciem suas chaves de criptografia usando o HSM validado pelo FIPS 140-2 nível 3 e lhes oferece flexibilidade para se integrar a seus aplicativos usando APIs padrão do setor, como PKCS#11, Java Cryptography Extensions (JCE) e bibliotecas Microsoft CryptoNG (CNG). Ele também é compatível com os padrões estabelecidos e permite que os proprietários de missão exportem todas as chaves para a maioria dos outros HSMs disponíveis no mercado. O CloudHSM é um serviço gerenciado que automatiza tarefas administrativas demoradas, como provisionamento de hardware, aplicação de patches de software, alta disponibilidade e backups. Para proteger e isolar seu CloudHSM de outros clientes da Amazon, ele deve ser provisionado dentro de uma VPC.

A separação de controle de acesso baseado em responsabilidades e funções é inerente no projeto do CloudHSM. A AWS tem um acesso limitado ao HSM que nos permite monitorar e manter a integridade e disponibilidade do HSM, fazer backups criptografados e extrair e publicar logs de auditoria em seu CloudWatch Logs. A AWS não pode visualizar, acessar ou suar suas chaves ou fazer com que seu HSM realize qualquer operação criptográfica usando suas chaves.

3. Hosts dedicados, instâncias dedicadas e bare metal

Além de fornecer serviços de computação altamente seguros, logicamente isolados e para vários locatários, a AWS também oferece três meios para implantar computação em hardware dedicado usando instâncias dedicadas, hosts dedicados e bare metal. Essas opções de implantação podem ser usadas para executar instâncias do Amazon EC2 em servidores físicos dedicados para seu uso. Instâncias dedicadas são instâncias do Amazon EC2 hipervisionadas que são executadas em uma nuvem privada virtual (VPC) em hardware dedicado a um único cliente. As instâncias dedicadas são isoladas fisicamente no nível de hardware de host das instâncias pertencentes a outras contas da AWS. As instâncias dedicadas podem compartilhar hardware com outras instâncias da mesma conta da AWS que não sejam dedicadas. Um host dedicado também é um servidor físico dedicado para seu uso. Com um host dedicado, você tem visibilidade e controle sobre como as instâncias hipervisionadas são colocadas no servidor. As instâncias bare metal são dispositivos de hardware host não hipervisionados. Ao usar a tecnologia do AWS Nitro para descarregamento de armazenamento e rede, além do chip de segurança do Nitro para eliminar os riscos associados à locação única em bare metal, os clientes têm acesso direto ao hardware do Amazon EC2. Essas instâncias bare metal são membros completos do serviço do Amazon EC2 e têm acesso a serviços como a Amazon VPC e o Amazon Elastic Block Store (EBS).[5]

5 No momento, as instâncias bare metal do Amazon EC2 podem ser experimentadas na família de instâncias I3 no formato do tipo de

Não há diferenças físicas, de segurança ou de desempenho entre instâncias dedicadas e instâncias implantadas em hosts dedicados. No entanto, os hosts dedicados oferecem aos proprietários de missão controle adicional em relação ao modo como as instâncias são inseridas em um servidor físico e como esse servidor é utilizado. Quando você usa hosts dedicados, tem controle sobre o posicionamento da instância no host usando as configurações de afinidade de host e posicionamento automático de instância. Se sua organização quer usar a AWS e tem uma licença de software existente, isso requer que o software seja executado em uma parte específica do hardware por um período mínimo de tempo. Hosts dedicados permitem visibilidade dentro do hardware do host, possibilitando que os requisitos da licença sejam atendidos.

Como a nuvem de locação múltipla atende aos requisitos de aplicação da lei para dados sem divulgar dados do DoD?

A AWS cumpre os requisitos de aplicação da lei para dados. Enquanto sistemas no local normalmente permitem que autoridades confisquem ou acessem diretamente o hardware físico do proprietário dos dados, a computação em nuvem apresenta um modelo diferente, já que os dados são hospedados em um ambiente de locação múltipla. Não é possível apreender ou acessar fisicamente um hardware físico na AWS, pois os dados de um cliente são distribuídos por vários dispositivos físicos, obrigando todas as solicitações de dados a passarem por um processo lógico de recuperação aprovado e autorizado. Por nosso credenciamento de FedRAMP, a AWS cumpre os controles do NIST 800-53, englobando o parâmetro moderado do FedRAMP, incluindo os controles de segurança "Retenção e manuseio de informações" e "Integridade de informações e sistema". Isso significa, entre outras coisas, que os serviços da AWS são definidos entre os limites das diferentes contas de clientes, impedem a combinação cruzada de contas de clientes, e resultam no controle total dos clientes sobre os conteúdos e operações de suas contas individuais da AWS. Os clientes do DoD, como todos os clientes, podem ter certeza de que qualquer solicitação legal de execução da lei será aplicada somente aos dados dentro da conta do cliente sujeito à solicitação. Também cumprimos os controles "Integridade de informações e sistema", que exigem que os CSPs compatíveis concedam aos clientes acesso aos seus dados e ordenam que agências compatíveis mantenham seus próprios dados consistentes com as leis vigentes. Além disso, os controles "Auditoria e prestação de contas" exigem que as organizações retenham registros de auditoria para oferecer suporte a investigações a posteriori de incidentes de segurança e que atendam aos requisitos organizacionais e regulatórios de retenção de informações. Os clientes podem recuperar os registros e relatórios de auditoria em nuvem utilizando o CloudTrail e o CloudWatch Logs, os quais podem ser então fornecidos às autoridades apropriadas. Essas soluções permitem que o DoD responda diretamente às solicitações do inspetor geral ou de agentes da lei para obtenção de informações, permitindo que oficiais do governo tenham acesso direto a informações que possam exigir sem confiscar o hardware.

instância i3.metal.

A AWS também aplica sérios controles e políticas em relação à higienização e destruição. Por exemplo, a AWS rastreia, documenta e verifica ações de descarte e higienização de mídia. Em nenhum momento um cliente tem acesso físico à mídia mapeada ao seu objeto ou volume lógico. Todo descarte e remoção de mídia são feitos pelo corpo de funcionários indicados da AWS. O conteúdo das unidades é tratado no nível máximo da classificação, de acordo com a política de classificação de dados da AWS. Toda mídia fica ilegível ou é destruída ao fim do ciclo de vida da mídia antes de sair de uma sala de datacenter da AWS, de acordo com os padrões de segurança da AWS, como parte do processo de desativação.

Como a nuvem de locação múltipla protege contra o acesso não autorizado de terceiros, incluindo o acesso de funcionários do CSP, aos dados do DoD?

Uma preocupação relacionada à amplitude da capacidade dos agentes de execução da lei de solicitar legalmente dados de clientes é o potencial do acesso não autorizado por parte de terceiros ao conteúdo do cliente e a adequação das medidas de controle de acesso para impedir o acesso não autorizado pelo corpo de funcionários do CSP. Não acessamos ou usamos o conteúdo do cliente para nenhuma outra finalidade que não a legalmente necessária e para manter os serviços da AWS e fornecê-los a nossos clientes e a seus usuários finais.

O acesso por parte de funcionários aos sistemas da AWS é concedido com base no princípio de privilégio mínimo, aprovado por uma pessoa autorizada antes de ser provisionado e supervisionado por um funcionário da AWS. Os deveres e as áreas de responsabilidade (por exemplo, a solicitação e aprovação do acesso, a solicitação e aprovação do gerenciamento de alterações etc.) devem ser distribuídos entre pessoas distintas para reduzir as chances de uma modificação não autorizada ou não intencional, ou o uso indevido dos sistemas da AWS. Os funcionários da AWS que possuem necessidades comerciais de acessar o plano de gerenciamento são obrigados a usar a autenticação multifator, diferente de suas credenciais corporativas da Amazon, para obter acesso a determinados hosts administrativos. Esses hosts administrativos são sistemas especificamente projetados, criados, configurados e reforçados para proteger o plano de gerenciamento. Todo esse acesso é registrado e auditado. Quando um funcionário não tem mais a necessidade comercial de acessar o plano de gerenciamento, os privilégios e o acesso a esses hosts e sistemas relevantes são revogados. A AWS implementou uma política de bloqueio de sessão que é aplicada sistematicamente. O bloqueio de sessão é mantido até que os procedimentos de identificação e autenticação sejam realizados.

Os clientes gerenciam o acesso ao conteúdo do cliente e serviços e recursos da AWS. Fornecemos um conjunto avançado de recursos de acesso, criptografia e registro em log (como AWS CloudTrail, CloudWatch, CloudHSM e AWS KMS, conforme descrito acima) para ajudá-lo a ser eficaz nesse gerenciamento.

Quais são as recomendações da AWS aos governos considerando os requisitos de separação física?

Durante o processo de autorização do SRG de computação em nuvem do DoD, a AWS demonstrou a suficiência da separação lógica para atender ao objetivo por trás de uma solicitação de uma infraestrutura dedicada e fisicamente isolada para as cargas de trabalho não confidenciais mais restritas do DoD. Nossa abordagem confirma que ambientes de locação múltipla logicamente separados que atendem a severos controles de segurança podem fornecer um nível de segurança superior a implantações na nuvem privada dedicada, enquanto oferecem vantagens significativas na disponibilidade, escalabilidade e menor custo. A tecnologia de nuvem moderna de provedores consagrados oferece soluções originais que podem atender ao objetivo de segurança da tecnologia tradicional, contanto que as abordagens de credenciamento sejam flexíveis o suficiente para acomodar implementações de alternativas.

Embora a revisão dos controles de segurança possa ser valiosa para demonstrar conformidade, nossa experiência demonstrou que as organizações que se concentram principalmente (e, em alguns casos, exclusivamente) na implementação de controles tradicionais podem limitar inadvertidamente seu acesso às melhores soluções de segurança. Enquanto os governos avaliam se os CSPs atendem aos requisitos com base em conceitos que vêm de um legado, eles devem articular claramente o resultado de segurança desejado e permitir que os CSPs desenvolvam as técnicas ideais para atender (se não exceder) esses resultados. Concentrar-se no objetivo de segurança desejado por trás de um requisito específico pode ajudar as agências federais a se concentrarem corretamente nos resultados que desejam alcançar, e não nos detalhes da implementação.

À medida que os programas de garantia de segurança amadurecem e são dimensionados para acompanhar o ritmo acelerado do recurso de nuvem e da inovação em segurança, os detalhes de implementação de controle se tornarão cada vez mais irrelevantes em relação às capacidades atuais dos CSPs. O estado final desejado – segurança robusta na nuvem, com base em uma estrutura definida pelos resultados de segurança do cliente e técnicas de segurança determinadas pelo CSP para atender a esses resultados – só pode ser resultado de um diálogo contínuo entre a comunidade das partes interessadas na garantia da nuvem. Acreditamos que essa abordagem ofereceria melhorias significativas na manutenção da garantia de uma postura de segurança do CSP.

Além de fornecer uma solução alternativa seguindo a mesma lógica, a AWS utilizou uma abordagem integral e realizou análises profundas para tratar totalmente das preocupações de segurança prioritárias do Departamento de Defesa dos Estados Unidos (DoD). A começar pelas necessidades do cliente relatadas no Guia dos requisitos de segurança de computação em nuvem do Departamento de Defesa, a AWS realizou diversas sessões de conhecimento para instruir o DoD sobre como nossa abordagem de três vertentes atende ao objetivo do requisito de separação física. O avaliador externo que validou nossos serviços também participou dessas sessões para atestar a precisão de nossas afirmações e oferecer sua avaliação baseada em riscos. Essas sessões colaborativas serviram como um meio valioso e eficiente de garantir a segurança, acelerar o credenciamento e, por fim, avançar com as metas de modernização de TI do DoD.

Somos encorajados pela evolução do DoD em aceitar soluções inovadoras e adaptadas à nuvem para atingir ao objetivo por trás dos requisitos de separação física na nuvem. Estamos comprometidos com a colaboração contínua com governos do mundo todo que estão avaliando os méritos e as melhores práticas da abordagem de equivalência da separação lógica do DoD.