Whitepaper da AWS

Visão geral de segurança do AWS Lambda

Visão geral de segurança do AWS Lambda: Whitepaper da AWS

Table of Contents

Visão geral de segurança do AWS Lambda

Data de publicação: 12 de fevereiro de 2021 (Revisões do documento)

Resumo

Este whitepaper apresenta uma análise profunda do serviço AWS Lambda por meio da perspectiva de segurança. Ele fornece uma imagem completa do serviço, o que é útil para novos usuários, e aprofunda a compreensão do Lambda para os usuários atuais.

Este whitepaper tem como público-alvo responsáveis pela segurança da informação (CISOs), engenheiros de segurança da informação, arquitetos empresariais, equipes de conformidade e quaisquer outros interessados em entender os fundamentos do AWS Lambda.

Introdução

Atualmente, mais workloads estão usando o AWS Lambda para alcançar escalabilidade, performance e economia, sem gerenciar a infraestrutura subjacente. Essas workloads são escalonadas para milhares de solicitações simultâneas por segundo. O Lambda é um dos muitos serviços importantes oferecidos pela AWS atualmente. O Lambda é usado por centenas de milhares de clientes da Amazon Web Services (AWS) para atender trilhões de solicitações todos os meses.

O Lambda é adequado para aplicações essenciais à missão em muitos setores. Uma ampla variedade de clientes, de mídia e entretenimento a serviços financeiros e outros setores regulamentados, usam o Lambda. Esses clientes diminuem o tempo de lançamento no mercado, otimizam os custos e melhoram a agilidade, concentrando-se no que fazem de melhor: administrar os negócios.

O modelo de ambiente do tempo de execuçãogerenciado permite que o Lambda gerencie muitos dos detalhes de implementação da execução de workloads sem servidor. Esse modelo reduz ainda mais a superfície de ataque e torna a segurança na nuvem mais simples. Este whitepaper apresenta os fundamentos desse modelo, além das práticas recomendadas, para desenvolvedores, analistas de segurança, equipes de segurança e conformidade e outras partes interessadas.

Sobre o AWS Lambda

AWS Lambda é um serviço computacional sem servidor orientado por eventos que estende outros serviços da AWS com lógica personalizada ou cria outros serviços de backend que operam com escala, performance e segurança. O Lambda pode executar código automaticamente em resposta a vários eventos, como solicitações de HTTP por meio do Amazon API Gateway, de modificações de objetos em buckets do Amazon S3, atualizações de tabela no Amazon DynamoDB e transições de estado no AWS Step Functions. Você também pode executar o código diretamente de qualquer aplicativo da web ou móvel. O Lambda executa seu código em uma infraestrutura computacional de alta disponibilidade e realiza toda a administração da plataforma adjacente, inclusive a manutenção do servidor e do sistema operacional, o provisionamento da capacidade e a escalabilidade automática, a aplicação de patches, o monitoramento de código e o registro em log.

Com o Lambda, basta carregar seu código e configurar quando ele deve ser invocado. O Lambda cuida de todo o restante necessário para executar seu código com alta disponibilidade. O Lambda se integra a muitos outros serviços da AWS e permite que você crie aplicações sem servidor ou serviços de backend, desde tarefas de automação simples, acionadas periodicamente, até aplicações de microsserviços completos.

O Lambda também pode ser configurado para acessar recursos em sua Amazon Virtual Private Cloud e, por extensão, seus recursos on-premises.

Você pode concluir facilmente o Lambda com um procedimento de segurança forte usando o AWS Identity and Access Management (IAM) e outras técnicas discutidas neste whitepaper para manter um alto nível de segurança e auditoria e atender às suas necessidades de conformidade.

Tópicos

Benefícios do Lambda

Clientes que desejam liberar a criatividade e a velocidade de suas organizações de desenvolvimento, sem comprometer a capacidade de sua equipe de TI de fornecer uma infraestrutura escalável, econômica e gerenciável, descobrem que o AWS Lambda lhes permite negociar a complexidade operacional por agilidade e melhores preços, sem comprometer a escala ou a confiabilidade.

O Lambda oferece muitos benefícios, incluindo os seguintes:

Nenhum servidor para gerenciar

O Lambda executa seu código em uma infraestrutura altamente disponível e tolerante a falhas espalhada por várias zonas de disponibilidade (AZs) em uma única região, implantando código sem problemas e fornecendo toda a administração, manutenção e patches da infraestrutura. O Lambda também oferece registro integrado e monitoramento, incluindo integração com Amazon CloudWatch, CloudWatch Logs e AWS CloudTrail.

Escalabilidade contínua

O Lambda gerencia com precisão a escalabilidade de suas funções (ou aplicação) executando o código acionado por eventos em paralelo e processando cada evento individualmente.

Medição em milissegundos

Com o AWS Lambda, a cobrança é feita por cada 1 milissegundo (ms) que seu código é executado e o número de vezes que é acionado. Você paga pela taxa de transferência consistente ou duração da execução, em vez de por unidade de servidor.

Aumenta a inovação

Assumindo o gerenciamento da infraestrutura, o Lambda libera seus recursos de programação, permitindo, assim, que eles se concentrem mais na inovação e no desenvolvimento da lógica de negócios.

Modernize suas aplicações

O Lambda permite que você use funções com modelos de machine learning pré-treinados para injetar inteligência artificial em aplicações com facilidade. Uma única solicitação de Interface do Programa da Aplicação (API) pode classificar imagens, analisar vídeos, converter fala em texto, executar processamento de linguagem natural e muito mais.

Ecossistema rico

O Lambda oferece suporte a desenvolvedores por meio do AWS Serverless Application Repository para descobrir, implantar e publicar aplicações sem servidor, AWS Serverless Application Model para criar aplicações sem servidor e integrações com vários ambientes de desenvolvimento (IDEs),

como AWS Cloud9, AWS Toolkit for Visual Studio, AWS Tools for Visual Studio Team Services e vários outros. O Lambda é integrado a serviços da AWS adicionais para fornecer um ecossistema avançado para a criação de aplicações sem servidor.

Custo para executar aplicações baseadas em Lambda

O Lambda oferece um modelo granular de pagamento conforme o uso. Com esse modelo, você é cobrado com base no número de invocações de função e sua duração (o tempo que leva para o código ser executado). Além desse modelo de preços flexível, o Lambda também oferece 1 milhão de solicitações perpetuamente gratuitas por mês, o que permite que muitos clientes automatizem seus processos sem nenhum custo.

Modelo de responsabilidade compartilhada

Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Esse modelo de responsabilidade compartilhada pode auxiliar a reduzir as preocupações operacionais, pois a AWS opera, gerencia e controla os componentes do sistema operacional do host e camada de virtualização, indo até a segurança física das instalações nas quais o serviço opera.

Para o AWS Lambda, a AWS gerencia a infraestrutura subjacente e os serviços básicos, o sistema operacional e a plataforma da aplicação. Você é responsável pela segurança de seu código e pelo gerenciamento de identidade e acesso (IAM) no serviço Lambda e dentro de sua função.

A Figura 1 mostra o modelo de responsabilidade compartilhada conforme se aplica aos componentes comuns e distintos do AWS Lambda. As responsabilidades da AWS aparecem abaixo da linha pontilhada em laranja e as responsabilidades do cliente aparecem acima da linha pontilhada em azul.

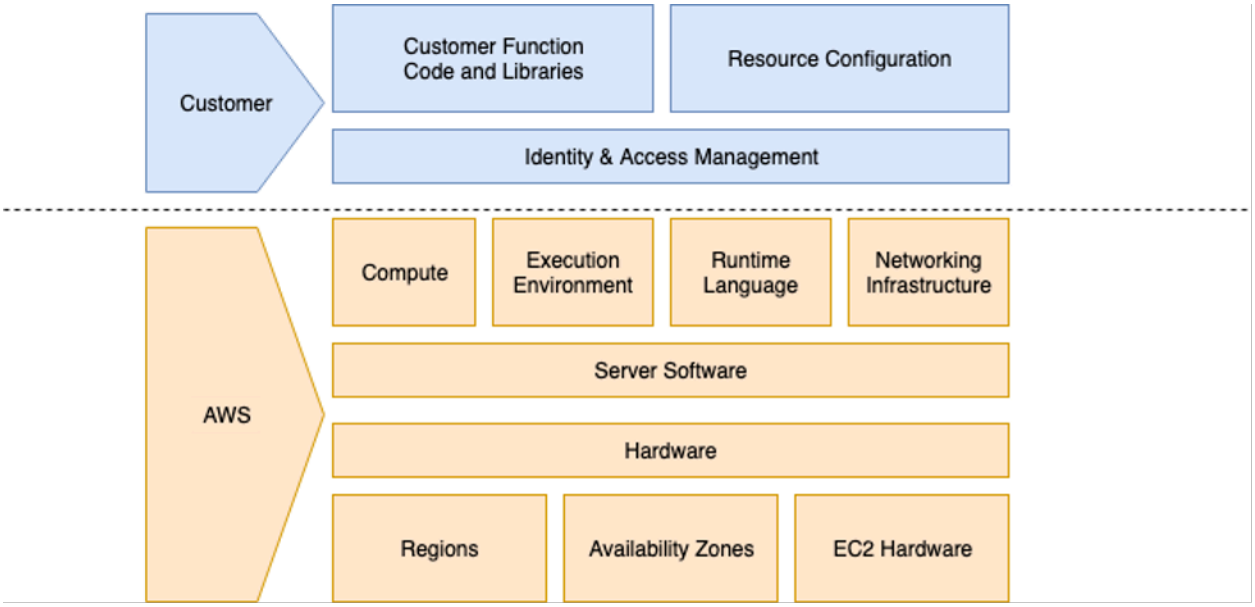

Figura 1: Modelo de responsabilidade compartilhada para AWS Lambda

Funções e camadas do Lambda

Com o Lambda, você pode executar código virtualmente sem administração da infraestrutura subjacente. Você é responsável apenas pelo código fornecido ao Lambda e pela configuração de como o Lambda deve executar esse código em seu nome. Atualmente, o Lambda oferece suporte a dois tipos de recursos de código: Funções e Camadas.

Uma função é um recurso que pode ser chamado para executar seu código no Lambda. As funções podem incluir um recurso comum ou compartilhado chamado Camadas. As camadas podem ser usadas para compartilhar código ou dados comuns entre diferentes funções ou contas da AWS. Você é responsável pelo gerenciamento de todo o código contido em suas funções ou camadas. Quando o Lambda recebe o código de função ou camada de um cliente, ele protege o acesso a esse código criptografando-o em repouso por meio do AWS Key Management Service (AWS KMS) e em trânsito usando o TLS 1.2+.

Você pode gerenciar o acesso às suas funções e camadas por meio de políticas do AWS Lambda ou por meio de permissões baseadas em recursos. Para obter uma lista completa dos recursos compatíveis do IAM no IAM, consulte Serviços da AWS que funcionam com o IAM.

Você também pode controlar todo o ciclo de vida de suas funções e camadas por meio das APIs do ambiente de gerenciamento do Lambda. Por exemplo, você pode escolher excluir sua função chamando `DeleteFunction` ou revogar permissões de outra conta chamando `RemovePermission`.

Modos de chamada do Lambda

A API Invoke pode ser chamada de duas maneiras: modo de evento e modo de requisição-resposta.

- O modo evento coloca na fila a carga útil para uma chamada assíncrona.
- O modo requisição-resposta chama de forma síncrona a função com a carga útil fornecida e retorna uma resposta imediatamente.

Em ambos os casos, a execução da função é sempre executada em um ambiente de execução do Lambda, mas a carga útil vai por caminhos diferentes. Para obter mais informações, consulte “Ambientes de execução do Lambda” neste documento.

Você também pode usar outros serviços da AWS que executam invocações em seu nome. O modo de chamada usado depende de qual serviço da AWS você está usando e de como ele está configurado. Para obter informações adicionais sobre como outros serviços da AWS se integram ao Lambda, consulte Uso do AWS Lambda com outros serviços.

Quando o Lambda recebe uma chamada de requisição-resposta, ela é passada diretamente para o serviço de invocação. Se o serviço de invocação não estiver disponível, os responsáveis pela chamada poderão colocar temporariamente a carga útil na fila do lado do cliente para repetir a ação um determinado número de vezes. Se o serviço de invocação receber a carga útil, o serviço tentará identificar um ambiente de execução disponível para a solicitação e passará a carga útil para esse ambiente de execução para concluir a chamada. Se não existirem ambientes de execução adequados, será criado um de forma dinâmica em resposta à solicitação. Enquanto em trânsito, as cargas úteis enviadas para o serviço de chamada são protegidas com TLS 1.2+. O tráfego dentro do serviço Lambda (do balanceador de carga para baixo) passa por uma virtual private cloud (VPC) interna isolada, de propriedade do serviço Lambda, na região da AWS para a qual a solicitação foi enviada.

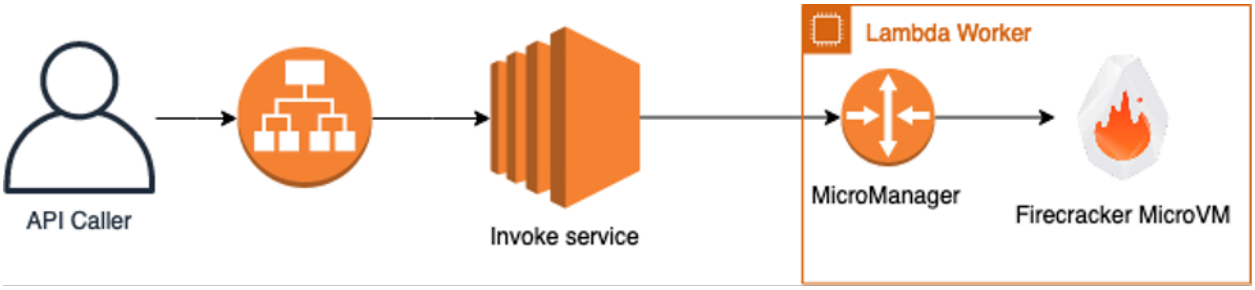

Figura 2: Modelo de chamada para requisição-resposta do AWS Lambda

As cargas úteis do modo de chamada evento são sempre colocadas na fila para processamento antes da chamada. Todas as cargas úteis são colocadas em fila para processamento em uma fila Amazon Simple Queue Service (Amazon SQS). Os eventos em fila são sempre protegidos em trânsito com o TLS 1.2+, mas, atualmente, não são criptografados em repouso. As filas do Amazon SQS usadas pelo Lambda são gerenciadas pelo serviço Lambda e não são visíveis para você como cliente. Os eventos em fila podem ser armazenados em uma fila compartilhada, mas podem ser migrados ou atribuídos a filas dedicadas, dependendo de vários fatores que não podem ser controlados diretamente pelos clientes (por exemplo, taxa de chamada, tamanho dos eventos e assim por diante).

Os eventos em fila são recuperados em lotes pela frota de sondagem do Lambda. A frota de sondagem é um grupo de instâncias do EC2 cuja finalidade é processar invocações de eventos em fila que ainda não foram processadas. Quando a frota de sondagem recupera um evento que está em fila e que precisa processar, isso é feito transferindo-o para o serviço de chamada, da mesma forma que um cliente faria em um modo de requisição-resposta.

Se a chamada não puder ser executada, a frota de sondagem armazenará temporariamente o evento, na memória, no host, até que seja capaz de concluir com êxito a execução, ou até que o número de tentativas de repetição de execução tenha sido excedido. Nenhum dado de carga útil é gravado em disco na própria frota de sondagem. A frota de sondagem pode ser atribuída aos clientes da AWS, permitindo o menor tempo de invocação. Para obter mais informações sobre quais serviços podem usar o modo de invocação de evento, consulte Uso do AWS Lambda com outros serviços.

Execuções do Lambda

Quando o Lambda executa uma função em seu nome, ele gerencia o provisionamento e a configuração dos sistemas subjacentes necessários para executar seu código. Isso permite que seus desenvolvedores se concentrem na lógica de negócios e na escrita de código, não administrando e gerenciando sistemas subjacentes.

O serviço Lambda é dividido no ambiente de gerenciamento e no plano de dados. Cada ambiente serve a um propósito distinto no serviço. O ambiente de gerenciamento fornece as APIs de gerenciamento (por exemplo, `CreateFunction`, `UpdateFunctionCode`, `PublishLayerVersion` e assim por diante) e gerencia integrações com todos os serviços da AWS. As comunicações com o ambiente de gerenciamento do Lambda são protegidas em trânsito pelo TLS. Todos os dados do cliente armazenados no ambiente de gerenciamento do Lambda são criptografados em repouso por meio do uso do AWS KMS, que foi projetado para protegê-los contra divulgação não autorizada ou adulteração.

O plano de dados é a API Invoke do Lambda que aciona a invocação de funções do Lambda. Quando uma função do Lambda é invocada, o plano de dados aloca um ambiente de execução em um operador do AWS Lambda (ou simplesmente operador, um tipo de instância do Amazon EC2) para essa versão de função, ou escolhe um ambiente de execução existente que já foi configurado para essa versão da função, que usa para concluir a invocação. Para obter mais informações, consulte a seção “MicroVMs e operador do AWS Lambda)” deste documento.

Ambientes de execução do Lambda

Cada invocação é roteada pelo serviço de invocação do Lambda para um ambiente de execução em um operador capaz de atender à solicitação. Além do plano de dados, os clientes e outros usuários não podem iniciar diretamente comunicações de rede de entrada com um ambiente de execução. Isso ajuda a garantir que as comunicações com o ambiente de execução sejam autenticadas e autorizadas.

Os ambientes de execução são reservados para uma versão de função específica e não podem ser reutilizados entre versões de função, funções ou contas da AWS. Isso significa que uma única função que pode ter duas versões diferentes resultaria em pelo menos dois ambientes de execução exclusivos.

Cada ambiente de execução só pode ser usado para uma invocação simultânea por vez, e eles podem ser reutilizados em várias invocações da mesma versão de função por motivos de

performance. Dependendo de vários fatores (por exemplo, taxa de invocação, configuração de função e assim por diante), um ou mais ambientes de execução podem existir para determinada versão da função. Com essa abordagem, o Lambda é capaz de fornecer isolamento no nível da versão da função para seus clientes.

No momento, o Lambda não isola invocações dentro do ambiente de execução de uma versão de função. Isso quer dizer que uma invocação pode deixar um estado que pode afetar a próxima invocação (por exemplo, arquivos gravados em /tmp ou dados na memória). Se você quiser garantir que uma invocação não afete outra, o Lambda recomenda que você crie funções distintas adicionais. Por exemplo, você pode criar funções distintas para operações de análise complexas que são mais propensas a erros e reutilizar funções que não executam operações confidenciais de segurança. No momento, o Lambda não limita o número de funções que os clientes podem criar. Para obter mais informações sobre limites, consulte a página de cotas do Lambda.

Os ambientes de execução são monitorados e gerenciados continuamente pelo Lambda e podem ser criados ou destruídos por vários motivos, incluindo, entre outros:

- Uma nova invocação chega e não existe um ambiente de execução adequado
- Ocorre um tempo de execução interno ou uma implantação de software do operador
- Uma nova configuração de simultaneidade provisionada é publicada
- O tempo de concessão no ambiente de execução, ou no operador, está se aproximando ou excedeu a vida útil máxima
- Outros processos internos de reequilíbrio da workload

Os clientes podem gerenciar o número de ambientes de execução pré-provisionados existentes para uma versão de função configurando a simultaneidade provisionada em sua configuração de função. Quando configurado para isso, o Lambda criará, gerenciará e garantirá que o número configurado de ambientes de execução sempre exista. Isso garante que os clientes tenham maior controle sobre a performance de suas aplicações sem servidor em qualquer escala.

Além de uma configuração de simultaneidade provisionada, os clientes não podem controlar deterministicamente o número de ambientes de execução que são criados ou gerenciados pelo Lambda em resposta a invocações.

Função de execução

Cada função do Lambda também deve ser configurada com uma função de execução, que é uma função do IAM que é assumida pelo serviço Lambda ao executar operações do ambiente de gerenciamento e plano de dados relacionados à função. O serviço Lambda assume essa função para buscar credenciais de segurança temporárias que ficam disponíveis como variáveis de ambiente durante a invocação de uma função. Por motivos de performance, o serviço Lambda armazenará em cache essas credenciais e poderá reutilizá-las em diferentes ambientes de execução que usam a mesma função de execução.

Para garantir a adesão ao princípio de privilégio mínimo, o Lambda recomenda que cada função tenha sua própria função exclusiva e que seja configurada com o conjunto mínimo de permissões necessárias.

O serviço Lambda também pode assumir a função de execução para executar determinadas operações do ambiente de gerenciamento, como aquelas relacionadas à criação e configuração de funções das interfaces de rede elásticas (ENI) para funções de VPC, envio de logs para o Amazon CloudWatch Application Insights, envio de rastreamentos para AWS X-Ray ou outras operações relacionadas que não sejam de invocação. Os clientes sempre podem analisar e auditar esses casos de uso analisando os registros de auditoria no AWS CloudTrail.

Para obter mais informações sobre esse assunto, consulte a página de documentação da função de execução do AWS Lambda.

MicroVMs e operadores do Lambda

O Lambda criará seus ambientes de execução em uma frota de instâncias do Amazon EC2 chamada Operadores do AWS Lambda. Operadores são instâncias bare metal do EC2 Nitro que são executadas e gerenciadas pelo Lambda em uma conta separada e isolada da AWS que não seja visível para os clientes. Os operadores têm uma ou mais micromáquinas virtuais (MVM) virtualizadas por hardware criadas pelo Firecracker. Firecracker é um monitor de máquina virtual (VMM) de código aberto que usa a máquina virtual baseada em kernel (KVM) do Linux para criar e gerenciar MVMs. Ele foi desenvolvido especificamente para criar e gerenciar contêineres seguros e multilocatários e serviços baseados em funções que fornecem modelos operacionais sem servidor. Para obter mais informações sobre o modelo de segurança do Firecracker, consulte o site do projeto Firecracker.

Como parte do modelo de responsabilidade compartilhada, o Lambda é responsável por manter a configuração de segurança, os controles e o nível de aplicação de patches dos operadores. A equipe

do Lambda usa o Amazon Inspector para descobrir possíveis problemas de segurança conhecidos, bem como outros mecanismos personalizados de notificação de problemas de segurança e listas de pré-divulgação, para que os clientes não precisem gerenciar o procedimento de segurança subjacente de seu ambiente de execução.

Figura 3: Modelo de isolamento para operadores do AWS Lambda

Os operadores têm uma vida útil máxima de locação de 14 horas. Quando um operador se aproxima do tempo máximo de concessão, nenhuma outra invocação é roteada para ele, os MVMs são normalmente encerrados e a instância subjacente do operador é encerrada. O Lambda monitora e emite alertas de forma contínua sobre as atividades do ciclo de vida da frota.

Todas as comunicações do plano de dados com os operadores são criptografadas usando o Advanced Encryption Standard with Galois/Counter Mode (AES-GCM). Além de operações de plano de dados, os clientes não podem interagir diretamente com um operador, pois ele está hospedado em uma rede isolada da Amazon VPC gerenciada pelo Lambda nas contas de serviço do Lambda.

Quando um operador precisa criar um ambiente de execução, ele recebe autorização por tempo limitado para acessar artefatos de função do cliente. Esses artefatos são otimizados especificamente para o ambiente de execução e os operadores do Lambda. O código de função, que é carregado usando o formato ZIP, é otimizado uma vez e, depois, armazenado em um formato criptografado usando uma chave gerenciada pela AWS e AES-GCM.

As funções carregadas no Lambda usando o formato de imagem de contêiner também são otimizadas. A imagem do contêiner é primeiramente baixada de sua fonte original, otimizada em partes distintas e apenas depois armazenada e criptografada em blocos usando um método de criptografia convergente que usa uma combinação de AES-CTR, AES-GCM e SHA-256 MAC. O método de criptografia convergente permite que o Lambda elimine duplicações de blocos criptografados com segurança. Todas as chaves necessárias para descriptografar os dados do cliente são protegidas por meio da AWS KMS chave mestra do cliente (CMK) gerenciada pelo cliente. O uso da CMK pelo serviço Lambda está disponível para os clientes em logs do AWS CloudTrail para rastreamento e auditoria.

Tecnologias de isolamento do Lambda

O Lambda usa uma variedade de tecnologias de isolamento proprietárias e de código aberto para proteger os operadores e os ambientes de execução. Cada ambiente de execução contém uma cópia dedicada dos seguintes itens:

- O código da versão da função específica
- Quaisquer camadas do AWS Lambda selecionadas para sua versão de função
- O tempo de execução da função escolhida (por exemplo, Java 11, NodeJS 12, Python 3.8 e assim por diante) ou o tempo de execução personalizado da função
- Um diretório /tmp gravável
- Um espaço mínimo de usuário Linux baseado no Amazon Linux 2

Os ambientes de execução são isolados uns dos outros usando várias tecnologias semelhantes a contêineres incorporadas ao kernel do Linux, juntamente com tecnologias de isolamento proprietárias da AWS. Essas tecnologias incluem:

- cgroups: usado para restringir o acesso da função à CPU e à memória.
- namespaces: cada ambiente de execução é executado em um namespace dedicado. Fazemos isso tendo IDs de processo de grupo exclusivos, IDs de usuário, interfaces de rede e outros recursos gerenciados pelo kernel do Linux.
- seccomp-bpf: para limitar as chamadas do sistema (syscalls) que podem ser usadas de dentro do ambiente de execução.
- iptables e tabelas de roteamento: para evitar comunicações de rede de entrada e isolar conexões de rede entre MVMs.
- chroot: fornece acesso com escopo ao sistema de arquivos subjacente.
- Configuração do Firecracker: usada para limitar a taxa de transferência do dispositivo de blocos e do dispositivo de rede.
- Recursos de segurança do Firecracker: para obter mais informações sobre o design de segurança atual do Firecracker, consulte o documento de design mais recente do Firecracker.

Usados com as tecnologias de isolamento proprietárias da AWS, esses mecanismos fornecem um forte isolamento entre os ambientes de execução.

Armazenamento e estado

Os ambientes de execução nunca são reutilizados em diferentes versões de função ou clientes, mas um único ambiente pode ser reutilizado entre invocações da mesma versão de função. Isso significa que os dados e o estado podem persistir entre as invocações. Os dados e/ou o estado podem continuar a persistir por horas antes de serem destruídos como parte do gerenciamento normal do ciclo de vida do ambiente de execução. Por motivos de performance, as funções podem tirar proveito desse comportamento para melhorar a eficiência, mantendo e reutilizando caches locais ou conexões de longa duração entre invocações. Dentro de um ambiente de execução, essas várias invocações são manipuladas por um único processo. Portanto, qualquer estado de todo o processo (como um estado estático em Java) pode estar disponível para futuras invocações para reutilização, se a invocação ocorrer em um ambiente de execução reutilizado.

Cada ambiente de execução do Lambda também inclui um sistema de arquivos gravável, disponível em `/tmp`. Esse armazenamento não é acessível nem compartilhado entre os ambientes de execução. Assim como no estado do processo, os arquivos gravados em `/tmp` permanecem durante toda a vida útil do ambiente de execução. Isso permite que operações de transferência caras, como o download de modelos de machine learning (ML), sejam amortizadas em várias invocações. As funções que não desejam manter os dados entre invocações não devem gravar em /tmp ou excluir seus arquivos de /tmp entre invocações. O diretório `/tmp` é apoiado por um armazenamento de instância do Amazon EC2 e é criptografado em repouso.

Os clientes que desejam manter os dados no sistema de arquivos fora do ambiente de execução devem considerar o uso da integração do Lambda com o Amazon Elastic File System (Amazon EFS). Para obter mais informações, consulte Uso do Amazon EFS com o AWS Lambda.

Se os clientes não quiserem manter os dados ou o estado em todas as invocações, o Lambda recomenda que eles não usem o contexto de execução ou o ambiente de execução para armazenar dados ou estado. Se os clientes quiserem impedir ativamente o vazamento de dados ou estado nas invocações, o Lambda recomenda que eles criem funções distintas para cada estado. O Lambda não recomenda que os clientes usem ou armazenem o estado confidencial de segurança no ambiente de execução, pois ele pode sofrer mutação entre invocações. Recomendamos recalcular o estado em cada invocação.

Manutenção de tempo de execução no Lambda

O Lambda oferece suporte a esses tempos de execução verificando e implantando continuamente atualizações e patches de segurança compatíveis e executando outras atividades de manutenção em tempo de execução. Isso permite que os clientes se concentrem apenas na manutenção e segurança de qualquer código incluído em sua função e camada. A equipe do Lambda usa o Amazon Inspector para descobrir problemas de segurança conhecidos, bem como outros mecanismos de notificação de problemas de segurança personalizados e listas de pré-divulgação para garantir que nossas linguagens de tempo de execução e ambiente de execução permaneçam corrigidas. Se novos patches ou atualizações forem identificados, o Lambda testará e implantará as atualizações de tempo de execução sem qualquer envolvimento dos clientes. Para obter mais informações sobre o programa de conformidade do Lambda, consulte a seção “Lambda e conformidade” deste documento.

Normalmente, nenhuma ação é necessária para selecionar os patches mais recentes para os tempos de execução do Lambda compatíveis. Porém, às vezes pode ser necessária uma ação para testar os patches antes de serem implantados (por exemplo, patches de tempo de execução incompatíveis conhecidos). Se qualquer ação for exigida dos clientes, o Lambda entrará em contato com eles por meio do Personal Health Dashboard, pelo e-mail da conta da AWS ou por outros meios, com as ações específicas necessárias a serem tomadas.

Os clientes podem usar outras linguagens de programação no Lambda implementando um tempo de execução personalizado. Para tempos de execução personalizados, a manutenção do tempo de execução se torna responsabilidade do cliente, incluindo garantir que o tempo de execução personalizado inclua os patches de segurança mais recentes. Para obter mais informações, consulte Tempos de execução personalizados do AWS Lambda no Guia do desenvolvedor do AWS Lambda.

Quando os mantenedores de linguagem de tempo de execução upstream marcam sua linguagem End-Of-Life (EOL), o Lambda não oferecerá mais suporte à versão da linguagem de tempo de execução. Quando as versões de tempo de execução são marcadas como obsoletas no Lambda, o Lambda deixa de oferecer suporte à criação de novas funções e atualizações para funções existentes que foram criadas no tempo de execução obsoleto. Para alertar o cliente sobre futuras descontinuidades em tempos de execução, o Lambda envia notificações aos clientes sobre a próxima data de descontinuidade e o que eles podem esperar. O Lambda também não fornecerá atualizações de segurança, suporte técnico nem hotfixes para tempos de execução obsoletos e se reserva o direito de desativar as invocações de funções configuradas para execução em um tempo de execução obsoleto a qualquer momento. Se os clientes quiserem continuar a executar versões

de tempo de execução obsoletas ou sem suporte, eles poderão criar seu próprio tempo de execução personalizado do AWS Lambda. Para obter detalhes sobre quando os tempos de execução serão descontinuados, consulte a política de suporte do tempo de execução do AWS Lambda.

Monitoramento e auditoria de funções do Lambda

Você pode monitorar e auditar funções do Lambda com muitos serviços e métodos da AWS, incluindo os seguintes:

Amazon CloudWatch

O AWS Lambda monitora automaticamente as funções do Lambda em seu nome. Por meio do Amazon CloudWatch, ele relata métricas como o número de solicitações, a duração da execução por solicitação e o número de solicitações que resultam em um erro. Essas métricas são expostas no nível da função, que você pode aproveitar para definir alarmes do CloudWatch. Para obter uma lista de métricas expostas pelo Lambda, consulte AWS Lambda Métricas.

Amazon CloudTrail

Usando o AWS CloudTrail, você pode implementar governança, conformidade, auditoria operacional e auditoria de risco de toda a sua conta da AWS, incluindo o Lambda. O CloudTrail permite que você registre, monitore continuamente e retenha atividades da conta relacionadas a ações em toda a infraestrutura da AWS, fornecendo um histórico completo de eventos das ações realizadas por meio do AWS Management Console, dos SDKs da AWS, das ferramentas da linha de comando e de outros serviços da AWS. Usando o CloudTrail, outra opção é criptografar os arquivos de log usando o AWS KMS e usar a validação da integridade do arquivo de log do CloudTrail para confirmação.

AWS X-Ray

Usando o AWS X-Ray, você pode analisar e depurar a produção e as aplicações baseadas em Lambda distribuídas, o que permite compreender a performance da aplicação e serviços subjacentes dela, para que você possa identificar e solucionar a raiz dos problemas de performance e erros. A visualização completa das solicitações de X-Ray à medida que elas percorrem a aplicação mostra um mapa dos componentes subjacentes da aplicação, para que você possa analisar as aplicações durante o desenvolvimento e a produção.

AWS Config

Com o AWS Config, é possível rastrear alterações de configuração nas funções do Lambda (incluindo funções excluídas), ambientes do tempo de execução, etiquetas, nome de quem

manuseou, tamanho do código, alocação de memória, configurações de tempo limite e configurações de simultaneidade, juntamente com a função de execução do IAM do Lambda, sub-rede e associações de grupos de segurança. Isso oferece uma visão holística do ciclo de vida da função do Lambda e permite que você exiba esses dados para possíveis requisitos de auditoria e conformidade.

Arquitetura e operação de funções do Lambda

Esta seção discute a arquitetura e as operações do Lambda. Para obter informações sobre as práticas recomendadas padrão para aplicações sem servidor, consulte o whitepaper Perspectivas de aplicativos sem servidor, que define e explora os pilares do AWS Well-Architected Framework em um contexto sem servidor.

- Pilar de excelência operacional: a capacidade de executar e monitorar sistemas para entregar valor empresarial e melhorar continuamente os processos e procedimentos de suporte.
- Pilar de segurança: a capacidade de proteger informações, sistemas e ativos, ao mesmo tempo em que agrega valor empresarial por meio de avaliações de risco e estratégias de mitigação.
- Pilar de confiabilidade: a capacidade de um sistema se recuperar de interrupções de infraestrutura ou de serviço, adquirir dinamicamente recursos computacionais para atender à demanda e mitigar transtornos, como configurações incorretas ou problemas transitórios de rede.
- Pilar de eficiência de performance: concentra-se no uso eficiente de recursos computacionais para cumprir os requisitos e a manutenção dessa eficiência conforme a demanda muda e as tecnologias evoluem.
- Pilar de otimização de custos: o processo contínuo de refinamento e melhoria para garantir que os resultados dos negócios sejam alcançados, minimizando os custos à medida que a demanda muda e as tecnologias evoluem.

O whitepaper Serverless Applications Lens (Perspectivas de aplicações sem servidor) inclui tópicos como registro de métricas e alarmes, controle de utilização e limites, atribuição de permissões a funções do Lambda e disponibilização de dados sigilosos para funções do Lambda.

Lambda e conformidade

Conforme mencionado na seção “Modelo de responsabilidade compartilhada”, você é responsável por determinar qual regime de conformidade se aplica aos seus dados. Depois de determinar suas necessidades de regime de conformidade, você pode usar os vários recursos do Lambda para corresponder a esses controles. Você pode entrar em contato com especialistas da AWS (como arquitetos de soluções, especialistas da área, gerentes de conta técnicos e outros recursos humanos) para obter assistência. No entanto, a AWS não pode aconselhar os clientes sobre se (ou quais) regimes de conformidade são aplicáveis a um caso de uso específico.

Desde novembro de 2020, o Lambda está no escopo dos relatórios SOC 1, SOC 2 e SOC 3, que são relatórios de exames independentes de terceiros que demonstram como a AWS atinge os principais controles e objetivos de conformidade. Para obter uma lista atualizada de informações de conformidade, consulte a página Serviços da AWS no escopo por programa de conformidade.

Devido à natureza sensível de alguns relatórios de conformidade, eles não podem ser compartilhados publicamente. Para acessar esses relatórios, você pode fazer login no AWS Management Console e usar o AWS Artifact, um portal de autoatendimento gratuito para acesso sob demanda aos relatórios de conformidade da AWS.

Fontes de eventos do Lambda

O Lambda se integra a mais de 140 serviços da AWS por meio de integração direta e do barramento de eventos do Amazon EventBridge. As fontes de eventos do Lambda comumente usadas são:

- Amazon API Gateway
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- Amazon DynamoDB Streams
- Amazon EventBridge
- Amazon Kinesis Data Streams
- Amazon S3
- Amazon SNS
- Amazon SQS
- AWS Step Functions

Com essas fontes de eventos, você pode:

- Usar o AWS Identity and Access Management para gerenciar o acesso ao serviço e aos recursos com segurança.

- Criptografar seus dados em repouso. *Todos os serviços criptografam dados em trânsito.
- Acessar a partir de sua Amazon Virtual Private Cloud usando endpoints da VPC (com tecnologia AWS PrivateLink
- Use o Amazon CloudWatch Application Insights para coletar, relatar e emitir alertas sobre métricas.
- Use AWS CloudTrail para registrar, monitorar continuamente e reter a atividade da conta relacionada a ações em toda a infraestrutura da AWS, fornecendo um histórico completo de eventos das ações realizadas por meio dos AWS Management Console > AWS SDKs , ferramentas da linha de comando e outros serviços da AWS.

*No momento da publicação, a criptografia de dados em repouso não estava disponível para o Amazon EventBridge. Continue monitorando as páginas iniciais do serviço para atualizações sobre esses recursos.

Conclusão

AWS Lambda oferece um poderoso toolkit para criar aplicações seguras e escaláveis. Muitas das práticas recomendadas de segurança e conformidade no Lambda são as mesmas de todos os serviços da AWS, mas algumas são específicas do Lambda. Este whitepaper descreveu os benefícios do Lambda, sua adequação para aplicações e o ambiente do tempo de execução gerenciado pelo Lambda. Também inclui informações sobre monitoramento e auditoria, além de práticas recomendadas de segurança e conformidade. Ao pensar em sua próxima implementação, considere o que aprendeu sobre o AWS Lambda e como isso pode melhorar sua próxima solução de workload.

Colaboradores

Os colaboradores desse documento incluem:

- Mayank Thakkar, arquiteto de soluções globais de ciências biológicas
- Marc Brooker, engenheiro-chefe sênior (sem servidor)
- Osman Surkatty, engenheiro de segurança sênior (sem servidor)

Leitura adicional

Para obter informações adicionais, consulte:

- Modelo de responsabilidade compartilhada, que explica como a AWS pensa sobre a segurança em geral.
- Práticas recomendadas de segurança da AWS, que abrange recomendações para o serviço AWS Identity and Access Management (IAM).
- Perspectivas de aplicações sem servidor abrange a AWS Well-Architected framework e identifica os principais elementos para garantir que suas workloads sejam arquitetadas de acordo com as práticas recomendadas.
- Introduction to AWS Security (Introdução à segurança da AWS) oferece uma ampla introdução ao pensamento sobre segurança na AWS.
- AWS Risk and Compliance (Risco e conformidade da AWS) fornece uma visão geral da conformidade na AWS.

Revisões do documento

Para ser notificado sobre atualizações deste whitepaper, inscreva-se no RSS feed.

update-history-change	update-history-description	update-history-date
Atualizado	Atualizações significativas	15 de fevereiro de 2021
Publicação inicial	Primeira publicação do whitepaper	3 de janeiro de 2019

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 práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no “estado em que se encontram”, sem garantias, declarações ou condições de qualquer tipo, explícitas ou implícitas. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.