Os 7 Pilares de segurança na AWS

COMECE A PROTEGER SUA NUVEM

GUILHERME TELES

Contents

Segurança na AWS

Modelo de Responsabilidade Compartilhada

Antes de entrarmos nos detalhes de como a AWS protege seus recursos, devemos falar sobre como a segurança na nuvem é um pouco diferente da segurança nos seus datacenters locais.

Quando você move dados e sistemas de computador para a nuvem, as responsabilidades de segurança são compartilhadas entre você e seu provedor de serviços em nuvem. Nesse caso, a AWS é responsável por proteger a infraestrutura subjacente que suporta a nuvem, e você é responsável por qualquer coisa que você colocar na nuvem ou conectar-se à nuvem.

Esse modelo de responsabilidade compartilhada pode reduzir sua carga operacional de várias maneiras e, em alguns casos, pode até melhorar sua postura de segurança padrão sem ação adicional de sua parte

Programa de conformidade da AWS

A conformidade da AWS permite que os clientes entendam os controles robustos em vigor na AWS para manter a segurança e a proteção de dados na nuvem.

Ao criar sistemas sobre a infraestrutura em nuvem da AWS, você compartilha responsabilidades de conformidade com a AWS. Ao vincular os recursos de serviço amigáveis e focados em governança com os padrões de conformidade ou auditoria aplicáveis, os facilitadores de conformidade da AWS se baseiam em programas tradicionais, ajudando você a estabelecer e operar em um ambiente de controle de segurança da AWS.

A infraestrutura de TI fornecida pela AWS é projetada e gerenciada em alinhamento com as melhores práticas de segurança e uma variedade de padrões de segurança de TI, incluindo (no momento da redação deste documento):

- Controle da organização de serviços (SOC) 1 / Declaração sobre normas para compromissos de atestado (SSAE) 16 / Normas internacionais para compromissos de garantia nº 3402 (ISAE) 3402 (anteriormente Declaração sobre normas de auditoria [SAS] 70)
- SOC 2
- SOC 3
- Lei Federal de Gerenciamento de Segurança da Informação (FISMA)
- Departamento de Defesa (DoD)
- Processo de Certificação e Acreditação de Garantia da Informação (DIACAP)
- Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP)
- Guia de Requisitos de Segurança (SRG) do DoD Cloud Computing Níveis 2 e 4
- Padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS) Nível 1
- Organização Internacional de Normalização (ISO) 9001 e ISO 27001
- Regulamentos sobre o tráfego internacional de armas (ITAR)
- Padrão Federal de Processamento de Informações (FIPS) 140-2

Além disso, a flexibilidade e o controle fornecidos pela plataforma da AWS permitem que os clientes implantem soluções que atendem a vários padrões específicos do setor, incluindo:

- Serviços de Informação da Justiça Criminal (CJIS)
- Aliança de Segurança na Nuvem (CSA)
- Lei de Privacidade e Direitos Educacionais da Família (FERPA)
- Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA)
- Associação de Cinema da América (MPAA)

A AWS fornece uma ampla gama de informações sobre seu ambiente de controle de TI para os clientes por meio de whitepapers, relatórios, certificações, acreditações e outros atestados de terceiros.

Segurança de infraestrutura global da AWS

A AWS opera a infraestrutura de nuvem global usada para provisionar uma variedade de recursos básicos de computação, como processamento e armazenamento. A infraestrutura global da AWS inclui as instalações, a rede, o hardware e o software operacional (por exemplo, host operacional, sistema e software de virtualização) que oferecem suporte ao provisionamento e uso desses recursos.

A infraestrutura global da AWS é projetada e gerenciada de acordo com as melhores práticas de segurança, bem como com uma variedade de padrões de conformidade de segurança. Como cliente da AWS, você pode ter certeza de que está construindo arquiteturas da Web sobre algumas das infraestruturas de computação mais seguras do mundo.

Segurança Física e Ambiental

Os data centers da AWS são avançados, usando abordagens inovadoras de arquitetura e engenharia. A Amazon tem muitos anos de experiência no design, construção e operação de data centers em larga escala. Essa experiência foi aplicada à plataforma e infraestrutura da AWS.

Os datacenters da AWS estão alojados em instalações não-descritas. O acesso físico é estritamente controlado tanto no perímetro quanto nos pontos de entrada da construção pela equipe de segurança profissional, usando videovigilância, sistemas de detecção de intrusão e outros meios eletrônicos.

A equipe autorizada deve passar pela autenticação de dois fatores no mínimo duas vezes para acessar os andares do datacenter. Todos os visitantes e contratados são obrigados a apresentar identificação e são assinados e acompanhados continuamente por pessoal autorizado.

A AWS fornece apenas acesso e informações ao datacenter a funcionários e contratados que possuem uma necessidade legítima dos negócios por esses privilégios. Quando um funcionário não tem mais uma necessidade comercial desses privilégios, seu acesso é imediatamente revogado, mesmo se continuar sendo funcionário da Amazon ou da AWS. Todo o acesso físico aos datacenters pelos funcionários da AWS é registrado e auditado rotineiramente.

Detecção e Supressão de Incêndio

Os datacenters da AWS possuem equipamentos automáticos de detecção e supressão de incêndio para reduzir riscos. O sistema de detecção de incêndio utiliza sensores de detecção de fumaça em todos os ambientes de data center, espaços de infraestrutura mecânica e elétrica, salas de resfriadores e salas de equipamentos de gerador.

Essas áreas são protegidas por sistemas de tubulação úmida, pré-ação com bloqueio duplo ou aspersores gasosos.

Energia

Os sistemas de energia elétrica do datacenter da AWS foram projetados para serem totalmente redundantes e mantidos sem impacto nas operações, 24 horas por dia e 7 dias por semana. As unidades de fonte de alimentação ininterrupta (UPS) fornecem energia de backup no caso de uma falha elétrica para cargas críticas e essenciais nas instalações. Os datacenters da AWS usam geradores para fornecer energia de backup para toda a instalação.

Clima e Temperatura

O controle climático é necessário para manter uma temperatura operacional constante para servidores e outros hardwares, o que evita o superaquecimento e reduz a possibilidade de interrupções no serviço.

Os data centers da AWS são criados para manter as condições atmosféricas em níveis ideais. O pessoal e os sistemas monitoram e controlam a temperatura e a umidade em níveis adequados.

Gerenciamento

A AWS monitora sistemas e equipamentos elétricos, mecânicos e de suporte à vida, para que quaisquer problemas sejam identificados imediatamente. A equipe da AWS realiza manutenção preventiva para manter a operacionalidade contínua dos equipamentos.

Desativação do dispositivo de armazenamento

Quando um dispositivo de armazenamento atinge o fim de sua vida útil, os procedimentos da AWS incluem um processo de descomissionamento desenvolvido para impedir que os dados do cliente sejam expostos a pessoas não autorizadas.

Gestão de Continuidade de Negócios

A infraestrutura da Amazon tem um alto nível de disponibilidade e fornece aos clientes os recursos para implantar uma arquitetura de TI resiliente. A AWS projetou seus sistemas para tolerar falhas de sistema ou hardware com impacto mínimo no cliente.

Continuidade de negócios do data center

O gerenciamento da AWS está sob a direção do Amazon Infrastructure Group.

Disponibilidade

Os datacenters são construídos em clusters em várias regiões globais. Todos os data centers estão online e atendem aos clientes; nenhum data center está "frio".

Em caso de falha, processos automatizados afastam o tráfego de dados da área afetada.

Os aplicativos principais são implantados em uma configuração N + 1, para que, no caso de uma falha no data center, haja capacidade suficiente para permitir que o tráfego seja balanceado por carga nos sites restantes.

A AWS oferece a seus clientes a flexibilidade de colocar instâncias e armazenar dados em várias regiões geográficas e também em várias zonas de disponibilidade em cada região.

Cada zona de disponibilidade é projetada como uma zona de falha independente.

Isso significa que as zonas de disponibilidade são fisicamente separadas dentro de uma região metropolitana típica e localizadas em planícies de inundação de menor risco (a categorização específica das zonas de inundação varia de acordo com a região). Além de possuir instalações discretas de geração de no-break e backup no local, elas são alimentadas por diferentes grades de utilidades independentes para reduzir ainda mais os pontos únicos de falha. As zonas de disponibilidade são todas redundantemente conectadas a vários provedores de transporte de nível 1

Você deve arquitetar o uso da AWS para tirar proveito de várias regiões e zonas de disponibilidade. A distribuição de aplicativos em várias zonas de disponibilidade oferece a capacidade de permanecer resiliente diante da maioria dos modos de falha, incluindo desastres naturais ou falhas no sistema.

Resposta a Incidentes

A equipe de gerenciamento de incidentes da Amazon emprega procedimentos de diagnóstico padrão do setor para direcionar a resolução durante eventos com impacto nos negócios.

Os operadores da equipe oferecem cobertura 24 × 7 × 365 para detectar incidentes e gerenciar o impacto e a resolução.

Comunicação

A AWS implementou vários métodos de comunicação interna em nível global para ajudar os funcionários a entender suas funções e responsabilidades individuais e comunicar eventos significativos em tempo hábil.

Esses métodos incluem programas de orientação e treinamento para funcionários recém-contratados, reuniões regulares de gerenciamento para atualizações sobre o desempenho dos negócios e outros assuntos e meios eletrônicos, como videoconferência, mensagens de correio eletrônico e postagem de informações pela intranet da Amazon.

A AWS também implementou vários métodos de comunicação externa para apoiar sua base de clientes e a comunidade.

Existem mecanismos para permitir que a equipe de suporte ao cliente seja notificada sobre problemas operacionais que afetam a experiência do cliente. Um painel de integridade do serviço está disponível e é mantido pela equipe de suporte ao cliente para alertar os clientes sobre quaisquer problemas que possam ter amplo impacto.

O Centro de segurança da AWS está disponível para fornecer detalhes de segurança e conformidade sobre a AWS. Os clientes também podem se inscrever nas ofertas de suporte da AWS, que incluem comunicação direta com a equipe de suporte ao cliente e alertas proativos para quaisquer problemas que impactem o cliente.

Segurança em Rede

A AWS fornece uma gama de serviços de rede que permitem criar uma rede logicamente isolada que você define, estabelecer uma conexão de rede privada com a AWS Cloud, usar um serviço DNS (Sistema de Nomes de Domínio) altamente disponível e escalável e fornecer conteúdo para seus usuários finais com baixa latência e altas velocidades de transferência de dados com um serviço da Web de entrega de conteúdo.

Segurança de rede

A rede da AWS foi arquitetada para permitir que você selecione o nível de segurança e resiliência apropriado para sua carga de trabalho. Para permitir a criação de arquiteturas da Web geograficamente dispersas e tolerantes a falhas com recursos de nuvem, a AWS implementou uma infraestrutura de rede de classe mundial que é cuidadosamente monitorada e gerenciada.

Arquitetura de rede segura

Dispositivos de rede, incluindo firewall e outros dispositivos de limite, existem para monitorar e controlar as comunicações nos limites externos da rede e nos principais limites internos da rede. Esses dispositivos de limite empregam conjuntos de regras, listas de controle de acesso (ACLs) e configurações para impor o fluxo de informações a serviços específicos do sistema de informações.

As ACLs ou políticas de fluxo de tráfego são estabelecidas em cada interface gerenciada, que gerencia e aplica o fluxo de tráfego. As políticas da ACL são aprovadas pelo Amazon Information Security. Essas políticas são enviadas automaticamente para garantir que essas interfaces gerenciadas apliquem as ACLs mais atualizadas.

Pontos de acesso seguros

A AWS colocou estrategicamente um número limitado de pontos de acesso na nuvem para permitir um monitoramento mais abrangente das comunicações de entrada e saída e do tráfego da rede.

Esses pontos de acesso do cliente são chamados de endpoint API (Application Programming Interface) e permitem acesso HTTP seguro (HTTPS), o que permite estabelecer uma sessão de comunicação segura com suas instâncias de armazenamento ou computação na AWS.

Para oferecer suporte a clientes com requisitos criptográficos do Federal Information Processing Standard (FIPS), os balanceadores de carga que terminam

com Secure Sockets Layer (SSL) no AWS GovCloud (US) são compatíveis com FIPS 140-2.

Além disso, a AWS implementou dispositivos de rede dedicados ao gerenciamento de comunicações de interface com os ISPs (Internet Service Providers). A AWS emprega uma conexão redundante com mais de um serviço de comunicação em cada extremidade da rede da AWS voltada para a Internet. Essas conexões possuem dispositivos de rede dedicados.

Proteção de transmissão

Você pode conectar-se a um ponto de acesso da AWS via HTTP ou HTTPS usando SSL, um protocolo criptográfico desenvolvido para proteger contra interceptação, adulteração e falsificação de mensagens.

Monitoramento e proteção de rede

A rede da AWS fornece proteção significativa contra problemas de segurança de rede tradicionais e você pode implementar mais proteção. A seguir estão alguns exemplos:

Ataques de negação de serviço distribuída (DDoS)

Os endpoint da API da AWS são hospedados em uma grande infraestrutura de classe mundial em escala da Internet, que se beneficia da mesma experiência em engenharia que transformou a Amazon no maior varejista on-line do mundo.

Técnicas proprietárias de mitigação de DDoS são usadas. Além disso, as redes da AWS têm hospedagem múltipla em vários fornecedores para alcançar a diversidade de acesso à Internet.

Ataques intermediários (MITM)

Todas as APIs da AWS estão disponíveis por endpoint protegidos por SSL que fornecem autenticação de servidor.

As AMIs do Amazon Elastic Compute Cloud (Amazon EC2) geram automaticamente novos certificados de host Secure Shell (SSH) na primeira inicialização e os registram no console da instância. Você pode usar as APIs seguras para chamar o console e acessar os certificados de host antes de efetuar login na instância pela primeira vez. A AWS incentiva você a usar SSL para todas as suas interações.

Falsificação de IP

As instâncias do Amazon EC2 não podem enviar tráfego de rede falsificado. A infraestrutura de firewall controlada por host e controlada pela AWS não permitirá que uma instância envie tráfego com um endereço IP ou MAC (Machine Access Control) de origem diferente do seu.

Verificação de porta

Verificações de porta não autorizadas por clientes do Amazon EC2 são uma violação da Política de uso aceitável da AWS. As violações da Política de uso aceitável da AWS são levadas a sério e todas as violações relatadas são investigadas.

Os clientes podem denunciar suspeitas de abuso por meio dos contatos disponíveis no site da AWS. Quando a varredura de porta não autorizada é detectada pela AWS, ela é parada e bloqueada. As verificações de porta das instâncias do Amazon EC2 geralmente são ineficazes porque, por padrão, todas as portas de entrada nas instâncias do Amazon EC2 são fechadas e são abertas apenas pelo cliente.

O gerenciamento rigoroso de grupos de segurança pode reduzir ainda mais a ameaça de varreduras portuárias. Se você configurar o grupo de segurança para permitir o tráfego de qualquer origem para uma porta específica, essa porta específica ficará vulnerável a uma verificação de porta. Nesses casos, você deve usar as medidas de segurança apropriadas para proteger os serviços de escuta que possam ser essenciais para seus serviços de aplicativos sejam descobertos por uma verificação de porta não autorizada.

Por exemplo, um servidor Web deve claramente ter a porta 80 (HTTP) aberta ao mundo, e o administrador deste servidor é responsável pela segurança do software do servidor HTTP, como o Apache. Você pode solicitar permissão para realizar verificações de vulnerabilidade, conforme necessário, para atender aos seus requisitos de conformidade específicos.

Essas verificações devem ser limitadas às suas próprias instâncias e não devem violar a Política de uso aceitável da AWS. A aprovação avançada para esses tipos de verificações pode ser iniciada enviando uma solicitação pelo site da AWS.

Detecção de pacotes

Embora você possa colocar suas interfaces no modo promíscuo, o hipervisor não fornecerá nenhum tráfego para eles que não lhes seja endereçado. Mesmo duas instâncias virtuais pertencentes ao mesmo cliente localizadas no mesmo host físico não podem escutar o tráfego um do outro. Embora o Amazon EC2 forneça ampla proteção contra um cliente que, inadvertidamente ou maliciosamente, tente visualizar os dados de outro cliente, como prática padrão, você deve criptografar o tráfego confidencial.

Recursos de segurança da conta da AWS

A AWS fornece uma variedade de ferramentas e recursos que você pode usar para manter sua conta e recursos da AWS protegidos contra uso não autorizado. Isso inclui credenciais para controle de acesso, endpoint HTTPS para transmissão de dados criptografados, a criação de contas de usuário separadas do AWS Identity and Access Management (IAM) e o registro de atividades do usuário para monitoramento de segurança. Você pode tirar proveito de todas essas ferramentas de segurança, independentemente dos serviços da AWS selecionados.

Credenciais da AWS

Para ajudar a garantir que apenas usuários e processos autorizados acessem sua conta e recursos da AWS, a AWS usa vários tipos de credenciais para autenticação. Isso inclui senhas, chaves criptográficas, assinaturas digitais e certificados. A AWS

também oferece a opção de exigir a autenticação multifator (MFA) para efetuar login na sua conta da AWS ou contas de usuário do IAM.

Por motivos de segurança, se suas credenciais foram perdidas ou esquecidas, você não pode recuperá-las ou fazer o download novamente. No entanto, você pode criar novas credenciais e, em seguida, desabilitar ou excluir o conjunto antigo de credenciais. De fato, a AWS recomenda que você altere (gire) suas chaves de acesso e certificados regularmente.

Para ajudá-lo a fazer isso sem afetar potencialmente a disponibilidade do seu aplicativo, a AWS oferece suporte a várias chaves e certificados de acesso simultâneo.

Com esse recurso, você pode alternar chaves e certificados para dentro e fora de operação regularmente, sem tempo de inatividade para o seu aplicativo. Isso pode ajudar a reduzir o risco de chaves ou certificados de acesso perdidos ou comprometidos.

A API do AWS IAM permite que você gire as chaves de acesso da sua conta da AWS e também das contas de usuário do IAM.

Senhas

As senhas são necessárias para acessar sua conta da AWS, contas de usuário individuais do IAM, fóruns de discussão da AWS e o Centro de suporte da AWS.

Você especifica a senha quando cria a conta e pode alterá-la a qualquer momento, acessando a página Credenciais de segurança.

As senhas da AWS podem ter até 128 caracteres e conter caracteres especiais, permitindo a criação de senhas muito fortes.

Você pode definir uma política de senha para suas contas de usuário do IAM para garantir que senhas fortes sejam usadas e que sejam alteradas com frequência. Uma política de senha é um conjunto de regras que definem o tipo de senha que um usuário do IAM pode definir.

Autenticação multifator da AWS (AWS MFA)

O AWS MFA é uma camada adicional de segurança para acessar os serviços da AWS Cloud. Ao ativar esse recurso opcional, você precisará fornecer um código de uso único de seis dígitos, além das credenciais padrão de nome de usuário e senha, antes que o acesso seja concedido às configurações da sua conta da AWS ou aos serviços e recursos da AWS Cloud.

Você obtém esse código de uso único de um dispositivo de autenticação que você mantém em sua posse física. Esse é o MFA porque mais de um fator de autenticação é verificado antes do acesso ser concedido: uma senha (algo que você sabe) e o código preciso do seu dispositivo de autenticação (algo que você possui).

Você pode ativar os dispositivos MFA para sua conta da AWS e para os usuários que você criou na sua conta da AWS com o AWS IAM. Além disso, você pode adicionar proteção MFA para acesso nas contas da AWS, pois quando você deseja permitir que um usuário criado em uma conta da AWS use uma função do IAM para acessar recursos em outra conta da AWS.

Você pode exigir que o usuário use o MFA antes de assumir a função como uma camada adicional de segurança.

O AWS MFA suporta o uso de tokens de hardware e dispositivos MFA virtuais. Os dispositivos virtuais MFA usam os mesmos protocolos que os dispositivos físicos MFA, mas podem ser executados em qualquer dispositivo de hardware móvel, incluindo um telefone inteligente.

Um dispositivo MFA virtual usa um aplicativo de software que gera códigos de autenticação de seis dígitos que são compatíveis com o padrão TOTP (Time-Based One-Time Password), conforme descrito na RFC 6238.

A maioria dos aplicativos MFA virtuais permite hospedar mais de um dispositivo MFA virtual, o que os torna mais convenientes que os dispositivos MFA de hardware. No entanto, você deve estar ciente de que, como um MFA virtual pode ser executado em um dispositivo menos seguro, como um telefone inteligente, um MFA virtual pode não fornecer o mesmo nível de segurança que um dispositivo MFA de hardware.

Você também pode aplicar a autenticação MFA para as APIs de serviço da AWS Cloud para fornecer uma camada extra de proteção contra ações poderosas ou privilegiadas, como encerrar instâncias do Amazon EC2 ou ler dados confidenciais armazenados no Amazon S3. Você faz isso adicionando um requisito de MFA a uma política de acesso do IAM.

Você pode anexar essas políticas de acesso a usuários, grupos do IAM ou recursos do IAM que suportam ACLs como buckets do Amazon S3, filas do Amazon Simple Queue Service (Amazon SQS) e tópicos do Amazon Simple Notification Service (Amazon SNS).

Chaves de Acesso

As chaves de acesso são criadas pelo AWS IAM e entregues como um par: o ID da chave de acesso (AKI) e a chave de acesso secreta (SAK). A AWS exige que todas as solicitações de API sejam assinadas pela SAK; ou seja, eles devem incluir uma assinatura digital que a AWS possa usar para verificar a identidade do solicitante.

Você calcula a assinatura digital usando uma função de hash criptográfico. Se você usar qualquer um dos SDKs da AWS para gerar solicitações, o cálculo da assinatura digital será feito para você.

O processo de assinatura não apenas ajuda a proteger a integridade da mensagem, impedindo a violação da solicitação enquanto ela está em trânsito, mas também ajuda a proteger contra possíveis ataques de reprodução.

Uma solicitação deve chegar à AWS dentro de 15 minutos do carimbo de data / hora na solicitação. Caso contrário, a AWS nega a solicitação.

A versão mais recente do processo de cálculo de assinatura digital no momento da redação deste documento é a versão 4 da assinatura, que calcula a assinatura usando o protocolo HMAC - Hashed Message Authentication Mode (HMAC) - Algoritmo de hash seguro (SHA) -256. A versão 4 fornece uma medida adicional de proteção em relação às versões anteriores, exigindo que você assine a mensagem

usando uma chave derivada da sua SAK em vez de usar a própria SAK. Além disso, você obtém a chave de assinatura com base no escopo da credencial, o que facilita o isolamento criptográfico da chave de assinatura.

Como as chaves de acesso podem ser mal utilizadas se caírem em mãos erradas, a AWS recomenda que você as salve em um local seguro e não as incorpore ao seu código. Para clientes com grandes frotas de instâncias do Amazon EC2 com escala elástica, o uso de funções do IAM pode ser uma maneira mais segura e conveniente de gerenciar a distribuição de chaves de acesso.

As funções do IAM fornecem credenciais temporárias, que não apenas são carregadas automaticamente na instância de destino, mas também são rotacionadas automaticamente várias vezes ao dia.

O Amazon EC2 usa um perfil de instância como um contêiner para uma função do IAM.

Quando você cria uma função do IAM usando o AWS Management Console, o console cria um perfil de instância automaticamente e atribui o mesmo nome à função à qual corresponde. Se você usar a AWS CLI, API ou um AWS SDK para criar uma função, crie o perfil da função e da instância como ações separadas e poderá atribuir nomes diferentes a eles.

Para iniciar uma instância com uma função do IAM, especifique o nome do seu perfil de instância. Ao iniciar uma instância usando o console do Amazon EC2, você pode selecionar uma função a ser associada à instância; no entanto, a lista exibida é na verdade uma lista de nomes de perfis de instância.

Pares de chaves

O Amazon EC2 suporta chaves SSA RSA 2048 para obter o primeiro acesso a uma instância do Amazon EC2. Em uma instância do Linux, o acesso é concedido mostrando a posse da chave privada SSH. Em uma instância do Windows, o acesso é concedido mostrando a posse da chave privada SSH para descriptografar a senha do administrador.

A chave pública está incorporada à sua instância e você usa a chave privada para entrar com segurança sem uma senha. Depois de criar suas próprias AMIs, você pode escolher outros mecanismos para efetuar logon em suas novas instâncias com segurança.

Você pode ter um par de chaves gerado automaticamente para você ao iniciar a instância ou fazer upload de seu próprio. Salve a chave privada em um local seguro no seu sistema e registre o local onde a salvou.

No Amazon CloudFront, você usa pares de chaves para criar URLs assinados para conteúdo privado, como quando você deseja distribuir conteúdo restrito pelo qual alguém pagou. Você cria pares de chaves do Amazon CloudFront usando a página Credenciais de segurança. Os pares de chaves do Amazon CloudFront podem ser criados apenas pela conta raiz e não podem ser criados pelos usuários do IAM.

Certificados X.509

Os certificados X.509 são usados para assinar solicitações baseadas em SOAP. Os certificados X.509 contêm uma chave pública associada a uma chave privada. Ao criar uma solicitação, você cria uma assinatura digital com sua chave privada e a inclui na solicitação, juntamente com seu certificado.

A AWS verifica se você é o remetente descriptografando a assinatura com a chave pública que está no seu certificado. A AWS também verifica se o certificado que você enviou corresponde ao certificado que você enviou para a AWS.

Para sua conta da AWS, você pode fazer com que a AWS crie um certificado X.509 e uma chave privada que você possa baixar ou fazer upload de seu próprio certificado usando a página Credenciais de segurança.

Para usuários do IAM, você deve criar o certificado X.509 (certificado de assinatura) usando software de terceiros. Ao contrário das credenciais da conta raiz, a AWS não pode criar um certificado X.509 para usuários do IAM.

Depois de criar o certificado, você o anexa a um usuário do IAM usando o IAM. Além das solicitações SOAP, os certificados X.509 são usados como certificados de

servidor SSL / Transport Layer Security (TLS) para clientes que desejam usar HTTPS para criptografar suas transmissões.

Para usá-los para HTTPS, você pode usar uma ferramenta de código aberto como o OpenSSL para criar uma chave privada exclusiva. Você precisará da chave privada para criar a Solicitação de Assinatura de Certificado (CSR) enviada a uma Autoridade de Certificação (CA) para obter o certificado do servidor.

Você usará a CLI da AWS para fazer upload do certificado, chave privada e cadeia de certificados no IAM.

Você também precisará de um certificado X.509 para criar uma AMI do Linux personalizada para instâncias do Amazon EC2. O certificado é necessário apenas para criar uma AMI suportada por instância (em oposição a uma AMI suportada pelo Amazon Elastic Block Store [Amazon EBS]). Você pode fazer com que a AWS crie um certificado X.509 e uma chave privada que você possa baixar ou fazer upload de seu próprio certificado usando a página Credenciais de segurança.

AWS CloudTrail

O AWS CloudTrail é um serviço da web que registra as chamadas de API feitas em sua conta e entrega arquivos de log ao seu bucket do Amazon S3. O benefício do AWS CloudTrail é a visibilidade da atividade da conta, registrando as chamadas de API feitas em sua conta. O AWS CloudTrail registra as seguintes informações sobre cada chamada de API:

- O nome da API
- A identidade do chamador
- A hora da chamada da API
- Os parâmetros de solicitação
- Os elementos de resposta retornados pelo serviço de nuvem da AWS

Essas informações ajudam a rastrear as alterações feitas nos recursos da AWS e a solucionar problemas operacionais. O AWS CloudTrail facilita garantir a conformidade com políticas internas e padrões regulatórios.

O AWS CloudTrail oferece suporte à integridade do arquivo de log, o que significa que você pode provar a terceiros (por exemplo, auditores) que o arquivo de log enviado pelo AWS CloudTrail não foi alterado.

Arquivos de log validados são inestimáveis em investigações forenses e de segurança. Esse recurso foi criado usando algoritmos padrão do setor: SHA-256 para hash e SHA-256 com RSA para assinatura digital.

Isso inviabiliza computacionalmente modificar, excluir ou forjar arquivos de log do AWS CloudTrail sem detecção.

Segurança específica do serviço de nuvem da AWS

Não apenas a segurança é incorporada a todas as camadas da infraestrutura da AWS, mas também a cada um dos serviços disponíveis nessa infraestrutura. Os serviços em nuvem da AWS são projetados para trabalhar de maneira eficiente e segura com todas as redes e plataformas da AWS.

Cada serviço fornece recursos de segurança adicionais para proteger dados e aplicativos confidenciais.

Serviços de computação

A AWS fornece uma variedade de serviços de computação baseados em nuvem que incluem uma ampla seleção de instâncias de computação que podem ser aumentadas e diminuídas automaticamente para atender às necessidades de seu aplicativo ou empresa.

Segurança do Amazon Elastic Compute Cloud (Amazon EC2)

O Amazon EC2 é um componente essencial na infraestrutura como serviço (IaaS) da Amazon, fornecendo capacidade de computação redimensionável usando

instâncias de servidor nos datacenters da AWS. O Amazon EC2 foi desenvolvido para facilitar a computação em escala da Web, permitindo obter e configurar a capacidade com atrito mínimo. Você cria e inicia instâncias, que são coleções de hardware e software da plataforma.

Vários níveis de segurança

A segurança no Amazon EC2 é fornecida em vários níveis: o sistema operacional (SO) da plataforma host, o SO de instância virtual ou SO convidado, um firewall e chamadas de API assinadas. Cada um desses itens se baseia nos recursos dos outros. O objetivo é impedir que os dados contidos no Amazon EC2 sejam interceptados por usuários ou sistemas não autorizados e tornar as instâncias do Amazon EC2 tão seguras quanto possível, sem sacrificar a flexibilidade na configuração exigida pelos clientes.

Hypervisor

Atualmente, o Amazon EC2 usa uma versão altamente personalizada do Xen hypervisor, aproveitando a paravirtualização (no caso de convidados Linux). Como os convidados paravirtualizados contam com o hipervisor para fornecer suporte para operações que normalmente exigem acesso privilegiado, o SO convidado não tem acesso elevado à CPU.

A CPU fornece quatro modos de privilégio separados: 0–3, chamados anéis. O anel 0 é o mais privilegiado e 3 o menos. O sistema operacional host executa no Ring 0. No entanto, em vez de executar no Ring 0 como a maioria dos sistemas operacionais, o SO convidado é executado no Ring 1 com menos privilégios e os aplicativos com menos privilégios no Ring 3.

Essa virtualização explícita dos recursos físicos leva a uma separação clara entre convidado e hipervisor, resultando em separação de segurança adicional entre os dois.

Isolamento de Instância

Diferentes instâncias em execução na mesma máquina física são isoladas uma da outra por meio do hipervisor Xen. A Amazon está ativa na comunidade Xen, que fornece à AWS o conhecimento dos últimos desenvolvimentos. Além disso, o firewall da AWS reside na camada do hipervisor, entre a interface de rede física e a interface virtual da instância.

Todos os pacotes devem passar por essa camada; portanto, os vizinhos de uma instância não têm mais acesso a ela do que qualquer outro host na Internet e podem ser tratados como se estivessem em hosts físicos separados.

A RAM física é separada usando mecanismos semelhantes. As instâncias do cliente não têm acesso aos dispositivos de disco bruto, mas são apresentadas com discos virtualizados. A camada de virtualização de disco proprietária da AWS redefine automaticamente todos os blocos de armazenamento usados pelo cliente, para que os dados de um cliente nunca sejam expostos involuntariamente a outro cliente. Além disso, a memória alocada para os convidados é limpa (definida como zero) pelo hipervisor quando não é alocada para um convidado.

A memória não é retornada ao conjunto de memória livre disponível para novas alocações até que a limpeza da memória seja concluída.

Sistema Operacional Host

Os administradores com uma empresa que precisam acessar o plano de gerenciamento precisam usar o MFA para obter acesso aos hosts de administração criados com finalidade específica. Esses hosts administrativos são sistemas projetados, construídos, configurados e protegidos especificamente para proteger o plano de gerenciamento da nuvem.

Todo esse acesso é registrado e auditado. Quando um funcionário não tem mais uma necessidade comercial de acessar o plano de gerenciamento, os privilégios e o acesso a esses hosts e sistemas relevantes podem ser revogados.

Operador convidado

As instâncias virtuais do sistema são completamente controladas por você, o cliente. Você tem acesso root completo ou controle administrativo sobre contas, serviços e aplicativos.

A AWS não possui direitos de acesso às suas instâncias ou ao SO convidado. A AWS recomenda um conjunto básico de práticas recomendadas de segurança para incluir a desativação do acesso somente por senha aos seus convidados e o uso de alguma forma de MFA para obter acesso às suas instâncias (ou no mínimo, no acesso SSH Versão 2 com base em certificado).

Além disso, você deve empregar um mecanismo de escalonamento de privilégios com o registro por usuário. Por exemplo, se o sistema operacional convidado for Linux, após a proteção, sua instância deverá usar o SSHv2 baseado em certificado para acessar a instância virtual, desabilitar o logon raiz remoto, usar o log da linha de comando e usar o sudo para escalar privilégios.

Você deve gerar seus próprios pares de chaves para garantir que eles sejam exclusivos e não sejam compartilhados com outros clientes ou com a AWS. A AWS também oferece suporte ao uso do protocolo de rede SSH para permitir o login seguro nas instâncias do Amazon EC2 do UNIX / Linux.

A autenticação do SSH usado com a AWS é feita através de um par de chaves pública / privada para reduzir o risco de acesso não autorizado à sua instância. Você também pode conectar-se remotamente às instâncias do Windows usando o RDP (Remote Desktop Protocol) usando um certificado RDP gerado para sua instância. Você também controla a atualização e o patch do sistema operacional convidado, incluindo atualizações de segurança.

As AMIs baseadas em Windows e Linux fornecidas pela Amazon são atualizadas regularmente com os patches mais recentes. Portanto, se você não precisar preservar dados ou personalizações nas instâncias em execução da Amazon AMI, basta reiniciar novas instâncias com a AMI atualizada mais recente. Além disso, são fornecidas atualizações para o Amazon Linux AMI por meio dos repositórios yum do Amazon Linux.

Firewall

O Amazon EC2 fornece um firewall de entrada obrigatório configurado no modo de negar tudo padrão; Os clientes do Amazon EC2 devem abrir explicitamente as portas necessárias para permitir o tráfego de entrada. O tráfego pode ser restrito pelo protocolo, pela porta de serviço e pelo endereço IP de origem (IP individual ou bloco CIDR).

O firewall pode ser configurado em grupos, permitindo que diferentes classes de instâncias tenham regras diferentes. Considere, por exemplo, o caso de um aplicativo da web tradicional de três camadas.

O grupo para os servidores da Web teria a porta 80 (HTTP) e / ou a porta 443 (HTTPS) aberta para a Internet. O grupo para os servidores de aplicativos teria a porta 8000 (específica do aplicativo) acessível apenas ao grupo de servidores da web.

O grupo para os servidores de banco de dados teria a porta 3306 (MySQL) aberta apenas para o grupo de servidores de aplicativos. Todos os três grupos permitiriam acesso administrativo na porta 22 (SSH), mas apenas da rede corporativa do cliente.

O nível de segurança oferecido pelo firewall é uma função de quais portas você abre e por qual duração e finalidade. Gerenciamento de tráfego bem informado e design de segurança ainda são necessários por instância. A AWS ainda recomenda que você aplique filtros de instância adicionais a firewalls baseados em host, como tabelas de IP ou Firewall do Windows e VPNs.

O estado padrão é negar todo o tráfego recebido, e você deve planejar cuidadosamente o que abrirá ao criar e proteger seus aplicativos.

Acesso à API

As chamadas de API para iniciar e encerrar instâncias, alterar parâmetros de firewall e executar outras funções são todas assinadas pela sua Amazon Secret

Access Key, que pode ser a Chave de acesso secreto da conta da AWS ou a Chave de acesso secreto de um usuário criado com o AWS IAM.

Sem acesso à sua chave de acesso secreto, as chamadas da API do Amazon EC2 não podem ser feitas em seu nome. As chamadas de API também podem ser criptografadas com SSL para manter a confidencialidade. A AWS recomenda sempre o uso de terminais de API protegidos por SSL.

Segurança de balanceamento de carga elástico

O Elastic Load Balancing é usado para gerenciar o tráfego em uma frota de instâncias do Amazon EC2, distribuindo o tráfego para instâncias em todas as zonas de disponibilidade em uma região.

O Elastic Load Balancing possui todas as vantagens de um balanceador de carga local, além de vários benefícios de segurança:

Assume o trabalho de criptografia e descriptografia das instâncias do Amazon EC2 e o gerencia centralmente no balanceador de carga.

Oferece aos clientes um único ponto de contato e também pode servir como a primeira linha de defesa contra ataques à sua rede.

Quando usado em um Amazon VPC, oferece suporte à criação e gerenciamento de grupos de segurança associados ao seu Elastic Load Balancing para fornecer opções adicionais de rede e segurança.

Suporta criptografia de tráfego de ponta a ponta usando TLS (anteriormente SSL) nas redes que usam conexões HTTP seguras (HTTPS). Quando o TLS é usado, o certificado do servidor TLS usado para finalizar as conexões do cliente pode ser gerenciado centralmente no balanceador de carga, em vez de em cada instância individual.

HTTPS / TLS usa uma chave secreta de longo prazo para gerar uma chave de sessão de curto prazo a ser usada entre o servidor e o navegador para criar a mensagem criptografada. O Elastic Load Balancing configura seu balanceador de carga com um

conjunto de códigos predefinido usado para negociação TLS quando uma conexão é estabelecida entre um cliente e seu balanceador de carga.

O conjunto de cifras predefinido fornece compatibilidade com uma ampla variedade de clientes e usa algoritmos criptográficos robustos. No entanto, alguns clientes podem ter requisitos para permitir apenas cifras e protocolos específicos (por exemplo, PCI DSS], Sarbanes-Oxley Act [SOX]) dos clientes para garantir que os padrões sejam atendidos. Nesses casos, o Elastic Load Balancing fornece opções para selecionar configurações diferentes para protocolos e cifras TLS. Você pode optar por ativar ou desativar as cifras, dependendo de seus requisitos específicos.

Segurança da nuvem virtual privada da Amazon (Amazon VPC)

Normalmente, cada instância do Amazon EC2 iniciada recebe aleatoriamente um endereço IP público no espaço de endereço do Amazon EC2.

O Amazon VPC permite criar uma parte isolada da nuvem da AWS e iniciar instâncias do Amazon EC2 com endereços privados (RFC 1918) no intervalo de sua escolha (por exemplo, 10.0.0.0/16).

Você pode definir sub-redes no Amazon VPC, agrupando tipos semelhantes de instâncias com base no intervalo de endereços IP e, em seguida, configurar o roteamento e segurança para controlar o fluxo de tráfego dentro e fora das instâncias e sub-redes.

Os recursos de segurança no Amazon VPC incluem grupos de segurança, ACLs de rede, tabelas de roteamento e gateways externos. Cada um desses itens é complementar ao fornecimento de uma rede segura e isolada que pode ser estendida por meio da habilitação seletiva de acesso direto à Internet ou conectividade privada a outra rede.

As instâncias do Amazon EC2 em execução no Amazon VPC herdam todos os benefícios descritos abaixo relacionados ao SO convidado e à proteção contra detecção de pacotes. Observe, no entanto, que você deve criar grupos de segurança especificamente para o Amazon VPC; quaisquer grupos de segurança do Amazon EC2 que você criou não funcionarão dentro do seu Amazon VPC.

Além disso, os grupos de segurança do Amazon VPC possuem recursos adicionais que os grupos de segurança do Amazon EC2 não possuem, como alterar o grupo de segurança após o lançamento da instância e especificar qualquer protocolo com um número de protocolo padrão (em vez de apenas TCP, User Datagram Protocol [UDP] ou Internet Control Message Protocol [ICMP]).

Cada Amazon VPC é uma rede distinta e isolada dentro da nuvem; o tráfego de rede em cada Amazon VPC é isolado de todos os outros Amazon VPCs. No momento da criação, você seleciona um intervalo de endereços IP para cada Amazon VPC. Você pode criar e conectar um gateway da Internet, gateway virtual privado ou ambos para estabelecer conectividade externa, sujeito aos seguintes controles.

Chamadas de acesso à API para criar e excluir Amazon VPCs; alterar os parâmetros de roteamento, grupo de segurança e ACL da rede; e executar outras funções são todas assinadas pela chave de acesso secreto da Amazon, que pode ser a chave de acesso secreto da conta da AWS ou a chave de acesso secreto de um usuário criado com o AWS IAM. Sem acesso à sua chave de acesso secreto, as chamadas à API do Amazon VPC não podem ser feitas em seu nome. Além disso, as chamadas de API podem ser criptografadas com SSL para manter a confidencialidade.

A AWS recomenda sempre o uso de terminais de API protegidos por SSL. O AWS IAM também permite que um cliente controle ainda mais quais APIs um usuário recém-criado tem permissão para chamar.

Sub-redes e tabelas de rotas Você cria uma ou mais sub-redes dentro de cada Amazon VPC; cada instância iniciada no Amazon VPC é conectada a uma sub-rede. Os ataques de segurança tradicionais da camada 2, incluindo falsificação de MAC e falsificação de ARP, são bloqueados. Cada sub-rede em um Amazon VPC é associada a uma tabela de roteamento e todo o tráfego de rede que sai da sub-rede é processado pela tabela de roteamento para determinar o destino.

Firewall (grupos de segurança)

Como o Amazon EC2, o Amazon VPC suporta um firewall de solução completa, permitindo a filtragem no tráfego de entrada e saída de uma instância. O grupo

padrão permite a comunicação de entrada de outros membros do mesmo grupo e a comunicação de saída para qualquer destino.

O tráfego pode ser restringido por qualquer protocolo IP, porta de serviço e endereço IP de origem / destino (bloco individual de IP ou CIDR). O firewall não é controlado pelo sistema operacional convidado; em vez disso, só pode ser modificado através da invocação de APIs do Amazon VPC.

A AWS suporta a capacidade de conceder acesso granular a diferentes funções administrativas nas instâncias e no firewall, permitindo, assim, implementar segurança adicional por meio da separação de tarefas.

O nível de segurança oferecido pelo firewall é uma função de quais portas você abre e por qual duração e finalidade. O gerenciamento de tráfego e o design de segurança bem informados ainda são necessários por instância.

A AWS ainda recomenda que você aplique filtros adicionais por instância com firewalls baseados em host, como IPtables ou Windows Firewall.

ACLs de rede

Para adicionar uma camada adicional de segurança ao Amazon VPC, você pode configurar as ACLs de rede. Esses são filtros de tráfego sem estado que se aplicam a todo o tráfego de entrada ou saída de uma sub-rede no Amazon VPC.

Essas ACLs podem conter regras ordenadas para permitir ou negar tráfego com base no protocolo IP, por porta de serviço e endereço IP de origem / destino.

Como grupos de segurança, as ACLs de rede são gerenciadas por meio de APIs do Amazon VPC, adicionando uma camada adicional de proteção e permitindo segurança adicional por meio da separação de tarefas.

Gateway Privado Virtual

Um gateway privado virtual permite conectividade privada entre o Amazon VPC e outra rede. O tráfego de rede em cada gateway privado virtual é isolado do tráfego de rede em todos os outros gateways privados virtuais.

Você pode estabelecer conexões VPN para o gateway privado virtual a partir de dispositivos de gateway em suas instalações. Cada conexão é protegida por uma chave pré-compartilhada em conjunto com o endereço IP do cliente de dispositivo de gateway.

Gateway de Internet

Um gateway da Internet pode ser anexado a um Amazon VPC para permitir conectividade direta ao Amazon S3, outros serviços da AWS e a Internet. Cada instância que deseja esse acesso deve ter um IP Elastic associado a ele ou rotear o tráfego através de uma instância de Network Address Translation (NAT)

Instâncias dedicadas

Em um Amazon VPC, você pode iniciar instâncias do Amazon EC2 que são fisicamente isolados no nível do hardware do host (ou seja, eles serão executados no hardware de um único inquilino).

Um Amazon VPC pode ser criado com locação "dedicada", para que todas as instâncias iniciadas no Amazon VPC usem esse recurso.

Como alternativa, um Amazon VPC pode ser criado com locação "padrão", mas você pode especificar a locação dedicada para instâncias específicas lançado nele.

Amazon CloudFront Security

O Amazon CloudFront oferece aos clientes uma maneira fácil de distribuir conteúdo para usuários finais com baixa latência e altas velocidades de transferência de dados. Ele fornece conteúdo dinâmico, estático e de streaming usando uma rede global de locais de borda.

As solicitações de objetos dos clientes são roteadas automaticamente para o local da borda mais próximo, para que o conteúdo seja entregue com o melhor desempenho possível.

O Amazon CloudFront é otimizado para trabalhar com outros serviços da AWS, como Amazon S3, Amazon EC2, Elastic Load Balancing e Amazon Route 53. Ele também funciona perfeitamente com qualquer servidor de origem que não seja da AWS que armazene as versões definitivas originais de seus arquivos.

O Amazon CloudFront exige que todas as solicitações feitas à sua API de controle sejam autenticadas, para que apenas usuários autorizados possam criar, modificar ou excluir suas próprias distribuições do Amazon CloudFront. As solicitações são assinadas com uma assinatura HMAC-SHA-1 calculada a partir da solicitação e da chave privada do usuário.

Além disso, a API de controle Amazon CloudFront é acessível apenas por endpoint habilitados para SSL.

Não há garantia de durabilidade dos dados mantidos nos locais de borda do Amazon CloudFront. Às vezes, o serviço pode remover objetos de locais de borda se esses objetos não forem solicitados com frequência. A durabilidade é fornecida pelo Amazon S3, que funciona como servidor de origem do Amazon CloudFront, mantendo as cópias definitivas originais dos objetos entregues pelo Amazon CloudFront.

Se você deseja controlar quem pode baixar o conteúdo do Amazon CloudFront, pode ativar o recurso de conteúdo privado do serviço. Esse recurso tem dois componentes.

A primeira controla como o conteúdo é entregue a partir da localização de borda do Amazon CloudFront para os espectadores na Internet. O segundo controla como os locais de borda do Amazon CloudFront acessam objetos no Amazon S3. O Amazon CloudFront também oferece suporte à restrição geográfica, que restringe o acesso ao seu conteúdo com base na localização geográfica dos seus visualizadores.

Para controlar o acesso às cópias originais de seus objetos no Amazon S3, o Amazon CloudFront permite criar uma ou mais identidades de acesso à origem e associá-las às suas distribuições. Quando uma identidade de acesso de origem é associada a

uma distribuição do Amazon CloudFront, a distribuição usa essa identidade para recuperar objetos do Amazon S3.

Você pode usar o recurso ACL do Amazon S3, que limita o acesso a essa identidade de acesso de origem para que a cópia original do objeto não seja legível publicamente.

Para controlar quem pode baixar objetos de locais de borda do Amazon CloudFront, o serviço usa um sistema de verificação de URL assinado. Para usar esse sistema, primeiro crie um par de chaves público-privado e faça o upload da chave pública em sua conta pelo AWS Management Console.

Em seguida, você configura sua distribuição do Amazon CloudFront para indicar quais contas você autorizaria a assinar solicitações - você pode indicar até cinco contas da AWS nas quais confia para assinar solicitações. Ao receber solicitações, você criará documentos de política indicando as condições sob as quais deseja que o Amazon CloudFront sirva seu conteúdo.

Esses documentos de política podem especificar o nome do objeto solicitado, a data e a hora da solicitação e o IP de origem (ou intervalo CIDR) do cliente que está fazendo a solicitação. Você então calcula o hash SHA-1 do seu documento de política e assina isso usando sua chave privada.

Por fim, você inclui o documento de política codificado e a assinatura como parâmetros da sequência de consulta ao fazer referência a seus objetos. Quando o Amazon CloudFront recebe uma solicitação, ele decodifica a assinatura usando sua chave pública. O Amazon CloudFront atenderá apenas solicitações que tenham um documento de política válido e assinatura correspondente.

Observe que o conteúdo privado é um recurso opcional que deve ser ativado quando você configura sua distribuição do Amazon CloudFront. O conteúdo entregue sem esse recurso ativado será publicamente legível.

O Amazon CloudFront oferece a opção de transferir conteúdo por uma conexão criptografada (HTTPS). Por padrão, o Amazon CloudFront aceita solicitações nos protocolos HTTP e HTTPS. No entanto, você também pode configurar o Amazon

CloudFront para exigir HTTPS para todas as solicitações ou fazer com que o Amazon CloudFront redirecione solicitações HTTP para HTTPS.

Você pode até configurar distribuições do Amazon CloudFront para permitir HTTP para alguns objetos, mas exigir HTTPS para outros objetos.

Armazenamento

A AWS fornece armazenamento de dados de baixo custo com alta durabilidade e disponibilidade. A AWS oferece opções de armazenamento para backup, arquivamento e recuperação de desastres e também para armazenamento de blocos e objetos.

Amazon Elastic Block Storage (Amazon EBS)

O Amazon EBS permite criar volumes de armazenamento de 1 GB a 16 TB que podem ser montados como dispositivos pelas instâncias do Amazon EC2. Os volumes de armazenamento se comportam como dispositivos de bloco não formatados brutos, com nomes de dispositivos fornecidos pelo usuário e uma interface de dispositivo de bloco. Você pode criar um sistema de arquivos sobre os volumes do Amazon EBS ou usá-los de qualquer outra maneira que usaria um dispositivo de bloco (como um disco rígido).

O acesso ao volume Amazon EBS é restrito à conta da AWS que criou o volume e aos usuários da conta da AWS criada com o AWS IAM (se o usuário tiver acesso concedido às operações do EBS). Todas as outras contas e usuários da AWS têm permissão negada para exibir ou acessar o volume.

Os dados armazenados nos volumes do Amazon EBS são redundantemente armazenados em vários locais físicos, como parte da operação normal desses serviços e sem custo adicional. No entanto, a replicação do Amazon EBS é armazenada na mesma zona de disponibilidade, não em várias zonas; portanto, é

altamente recomendável que você realize snapshots regulares no Amazon S3 para durabilidade dos dados a longo prazo.

Para clientes que arquitetaram bancos de dados transacionais complexos usando o Amazon EBS, recomenda-se que os backups do Amazon S3 sejam executados por meio do sistema de gerenciamento de banco de dados, para que as transações e logs distribuídos possam ser verificados.

A AWS não executa automaticamente backups de dados mantidos em discos virtuais conectados a instâncias em execução no Amazon EC2.

Você pode disponibilizar publicamente os snapshots de volume do Amazon EBS para outras contas da AWS para usar como base para a criação de volumes duplicados.

O compartilhamento de snapshots de volume do Amazon EBS não fornece a outras contas da AWS a permissão para alterar ou excluir o snapshot original, pois esse direito é explicitamente reservado para a conta da AWS que criou o volume. Um snapshot do Amazon EBS é uma visualização em nível de bloco de um volume inteiro do Amazon EBS.

Observe que dados que não são visíveis no sistema de arquivos no volume, como arquivos que foram excluídos, podem estar presentes no snapshot do Amazon EBS. Se você deseja criar snapshots compartilhados, faça com tanto cuidado. Se um volume contiver dados confidenciais ou tiver arquivos excluídos, você deverá criar um novo volume do Amazon EBS para compartilhar.

Os dados a serem contidos na captura instantânea compartilhada devem ser copiados para o novo volume e a captura instantânea criada a partir do novo volume.

Os volumes do Amazon EBS são apresentados a você como dispositivos de bloco não formatados brutos que foram limpos antes de serem disponibilizados para uso. A limpeza ocorre imediatamente antes da reutilização, para que você possa ter certeza de que o processo de limpeza foi concluído. Se você tiver procedimentos que exijam a limpeza de todos os dados por meio de um método específico, poderá fazê-lo no Amazon EBS.

Você deve realizar um procedimento de limpeza especializado antes de excluir o volume para conformidade com os requisitos estabelecidos.

A criptografia de dados confidenciais geralmente é uma boa prática de segurança, e a AWS fornece a capacidade de criptografar volumes do Amazon EBS e seus snapshots com o Advanced Encryption Standard (AES) -256. A criptografia ocorre nos servidores que hospedam as instâncias do Amazon EC2, fornecendo criptografia de dados à medida que eles se movem entre as instâncias do Amazon EC2 e o armazenamento do Amazon EBS. Para poder fazer isso de forma eficiente e com baixa latência, o recurso de criptografia do Amazon EBS está disponível apenas nos tipos de instância mais poderosos do Amazon EC2.

Segurança do Amazon Simple Storage Service (Amazon S3)

O Amazon S3 permite fazer upload e recuperar dados a qualquer momento, de qualquer lugar da Web. O Amazon S3 armazena dados como objetos dentro de buckets. Um objeto pode ser qualquer tipo de arquivo: um arquivo de texto, uma foto, um vídeo e muito mais.

Ao adicionar um arquivo ao Amazon S3, você tem a opção de incluir metadados com o arquivo e definir permissões para controlar o acesso ao arquivo. Para cada depósito, você pode controlar o acesso ao depósito (quem pode criar, excluir e listar objetos no depósito), exibir logs de acesso ao depósito e seus objetos e escolher a região geográfica onde o Amazon S3 armazenará o depósito e seus itens. conteúdo.

Acesso de dados

O acesso aos dados armazenados no Amazon S3 é restrito por padrão; somente proprietários de bucket e objeto têm acesso aos recursos do Amazon S3 que eles criam. (Observe que o proprietário do bloco / objeto é o proprietário da conta da

AWS, não o usuário que criou o bloco / objeto.) Existem várias maneiras de controlar o acesso a buckets e objetos:

Políticas do IAM

O AWS IAM permite que organizações com muitos funcionários criem e gerenciem vários usuários em uma única conta da AWS. As políticas do IAM são anexadas aos usuários, permitindo o controle centralizado das permissões dos usuários na sua conta da AWS para acessar buckets ou objetos. Com as políticas do IAM, você só pode conceder usuários em sua própria conta da AWS com permissão para acessar seus recursos do Amazon S3.

ACLs

No Amazon S3, você pode usar ACLs para fornecer acesso de leitura ou gravação em buckets ou objetos a grupos de usuários. Com as ACLs, você só pode conceder a outras contas da AWS (usuários não específicos) acesso aos seus recursos do Amazon S3.

Políticas de bucket

As políticas de bucket no Amazon S3 podem ser usadas para adicionar ou negar permissões em alguns ou todos os objetos em um único bucket. As políticas podem ser anexadas a usuários, grupos ou buckets do Amazon S3, permitindo o gerenciamento centralizado de permissões. Com as políticas de bucket, você pode conceder aos usuários da sua conta da AWS ou de outras contas da AWS acesso aos recursos do Amazon S3.

Autenticação de string de consulta

Você pode usar uma string de consulta para expressar uma solicitação inteiramente em uma URL. Nesse caso, você usa parâmetros de consulta para fornecer informações de solicitação, incluindo as informações de autenticação. Como a assinatura da solicitação faz parte da URL, esse tipo de URL geralmente é chamado

de URL pré-assinado. Você pode usar URLs pré-assinados para incorporar links clicáveis, que podem ser válidos por até sete dias, em HTML.

Você pode restringir ainda mais o acesso a recursos específicos com base em determinadas condições. Por exemplo, você pode restringir o acesso com base no horário da solicitação (Data Condição), se a solicitação foi enviada usando SSL (Condições Booleanas), no endereço IP de um solicitante (Condição de Endereço IP) ou no aplicativo cliente do solicitante (Condições da String). Para identificar essas condições, você usa chaves de política.

O Amazon S3 também oferece aos desenvolvedores a opção de usar a autenticação de string de consulta, o que permite compartilhar objetos do Amazon S3 por meio de URLs válidas por um período predefinido.

A autenticação de cadeia de consulta é útil para fornecer ao HTTP acesso do navegador a recursos que normalmente exigiriam autenticação. A assinatura na cadeia de consulta protege a solicitação.

Transferência de dados

Para segurança máxima, você pode fazer upload / download de dados com segurança para o Amazon S3 através dos endpoint criptografados por SSL. Os endpoint criptografados são acessíveis na Internet e no Amazon EC2, para que os dados sejam transferidos com segurança na AWS e para e de fontes fora da AWS.

Armazenamento de dados

O Amazon S3 fornece várias opções para proteger os dados em repouso. Para os clientes que preferem gerenciar sua própria criptografia, eles podem usar uma biblioteca de criptografia de cliente como o Amazon S3 Encryption Client para criptografar dados antes de fazer o upload para o Amazon S3.

Como alternativa, você pode usar o SSE (Amazon S3 Server Side Encryption) se preferir que o Amazon S3 gerencie o processo de criptografia para você. Os dados

são criptografados com uma chave gerada pela AWS ou com uma chave fornecida, dependendo dos seus requisitos.

Com o Amazon S3 SSE, você pode criptografar dados no upload simplesmente adicionando um cabeçalho de solicitação adicional ao gravar o objeto.

A descriptografia acontece automaticamente quando os dados são recuperados. Observe que os metadados, que você pode incluir no seu objeto, não são criptografados.

O Amazon S3 SSE usa uma das cifras de bloco mais fortes disponíveis: AES-256. Com o Amazon S3 SSE, todos os objetos protegidos são criptografados com uma chave de criptografia exclusiva.

Essa chave de objeto é criptografada com uma chave mestre rotacionada regularmente. O Amazon S3 SSE fornece segurança adicional armazenando os dados criptografados e as chaves de criptografia em diferentes hosts.

O Amazon S3 SSE também possibilita a imposição de requisitos de criptografia.

Por exemplo, você pode criar e aplicar políticas de buckets que exigem que apenas dados criptografados possam ser carregados em seus buckets.

Quando um objeto é excluído do Amazon S3, a remoção do mapeamento do nome público para o objeto inicia imediatamente e geralmente é processada no sistema distribuído em alguns segundos.

Após a remoção do mapeamento, não há acesso remoto ao objeto excluído. A área de armazenamento subjacente é então recuperada para uso pelo sistema.

O Amazon S3 Standard foi projetado para fornecer 99,9999999999% de durabilidade dos objetos em um determinado ano. Esse nível de durabilidade corresponde a uma perda média anual esperada de 0,000000001 por cento dos objetos. Por exemplo, se você armazenar 10.000 objetos no Amazon S3, poderá esperar, em média, a perda de um único objeto a cada 10.000.000 anos.

Além disso, o Amazon S3 foi projetado para sustentar a perda simultânea de dados em duas instalações.

Logs de acesso

Um bucket do Amazon S3 pode ser configurado para registrar o acesso ao bucket e aos objetos dentro dele. O log de acesso contém detalhes sobre cada solicitação de acesso, incluindo o tipo de solicitação, o recurso solicitado, o IP do solicitante e a hora e data da solicitação.

Quando o log é ativado para um bucket, os registros são periodicamente agregados aos arquivos de log e entregues no bucket especificado do Amazon S3.

Compartilhamento de recursos entre origens (CORS)

Os clientes da AWS que usam o Amazon S3 para hospedar páginas da Web estáticas ou armazenar objetos usados por outras páginas da Web podem carregar conteúdo com segurança, configurando um bucket do Amazon S3 para ativar explicitamente solicitações de origem cruzada.

Navegadores modernos usam a política Same Origin para bloquear JavaScript ou HTML5 permite que solicitações carreguem conteúdo de outro site ou domínio como uma maneira de garantir que o conteúdo malicioso não seja carregado de uma fonte menos respeitável (como durante ataques de script entre sites).

Com a política de compartilhamento de recursos de origem cruzada (CORS) ativada, ativos como fontes da web e imagens armazenadas em um bucket do Amazon S3 podem ser referenciados com segurança por páginas da web externas, folhas de estilo e aplicativos HTML5.

Amazon Glacier Security

Como o Amazon S3, o serviço Amazon Glacier fornece armazenamento de baixo custo, seguro e durável.

Onde o Amazon S3 foi projetado para recuperação rápida, no entanto, o Amazon Glacier deve ser usado como um serviço de arquivamento de dados que não são acessados com frequência e para os quais os tempos de recuperação de várias horas são adequados.

O Amazon Glacier armazena arquivos como arquivos dentro de cofres. Os arquivos podem ser quaisquer dados, como uma foto, vídeo ou documento, e podem conter um ou vários arquivos.

Você pode armazenar um número ilimitado de arquivos em um único cofre e criar até 1.000 cofres por região. Cada arquivo pode conter até 40 TB de dados.

Transferência de dados

Para segurança máxima, você pode fazer upload / download de dados com segurança no Amazon Glacier por meio dos endpoint criptografados SSL. Os endpoint criptografados são acessíveis na Internet e no Amazon EC2, para que os dados sejam transferidos com segurança na AWS e para e de fontes externas à AWS.

Recuperação de dados

A recuperação de arquivos do Amazon Glacier requer o início de um trabalho de recuperação, que geralmente é concluído em três a cinco horas. Você pode acessar os dados por meio de solicitações HTTP GET. Os dados permanecerão disponíveis para você por 24 horas.

Você pode recuperar um arquivo inteiro ou vários arquivos de um arquivo. Se você deseja recuperar apenas um subconjunto de um archive, pode usar uma solicitação de recuperação para especificar o intervalo do archive que contém os arquivos nos quais está interessado ou pode iniciar várias solicitações de recuperação, cada uma com um intervalo para um ou mais arquivos.

Você também pode limitar o número de itens de inventário do Vault recuperados filtrando um período de criação de arquivo morto ou definindo um limite máximo de itens.

Seja qual for o método escolhido, ao recuperar partes do arquivo morto, você pode usar a soma de verificação fornecida para ajudar a garantir a integridade dos arquivos, desde que o intervalo recuperado esteja alinhado com o hash da árvore do arquivo morto geral.

Armazenamento de dados

O Amazon Glacier criptografa automaticamente os dados usando o AES-256 e os armazena de forma durável de forma imutável. O Amazon Glacier foi projetado para fornecer durabilidade média anual de 99,9999999999% para um arquivo morto.

Ele armazena cada arquivo em várias instalações e vários dispositivos. Diferentemente dos sistemas tradicionais, que podem exigir verificação de dados trabalhosa e reparo manual, o Amazon Glacier realiza verificações sistemáticas e regulares da integridade dos dados e foi desenvolvido para ser auto-reparável.

Acesso de dados

Somente sua conta pode acessar seus dados no Amazon Glacier. Para controlar o acesso aos seus dados no Amazon Glacier, você pode usar o AWS IAM para especificar quais usuários da sua conta têm direitos para operações em um determinado cofre.

Segurança do AWS Storage Gateway

O serviço AWS Storage Gateway conecta seu dispositivo de software local ao armazenamento baseado em nuvem para fornecer integração perfeita e segura entre seu ambiente de TI e a infraestrutura de armazenamento da AWS.

O serviço permite fazer upload de dados com segurança para o AWS escalável, serviço de armazenamento confiável e seguro do Amazon S3 para backup econômico e recuperação rápida de desastres.

Transferência de dados

Os dados são transferidos de forma assíncrona do seu hardware de armazenamento local para a AWS sobre SSL.

Armazenamento de dados

Os dados são armazenados criptografados no Amazon S3 usando o AES 256, um padrão de criptografia de chave simétrica usando chaves de criptografia de 256 bits. O AWS Storage Gateway apenas carrega dados que foram alterados, minimizando a quantidade de dados enviados pela Internet.

Base de dados

A AWS fornece várias soluções de banco de dados para desenvolvedores e empresas, desde serviços gerenciados de banco de dados relacional e NoSQL a cache de memória como serviço e serviço de armazém de dados em escala de petabytes.

Segurança do Amazon DynamoDB

O Amazon DynamoDB é um serviço de banco de dados NoSQL gerenciado que fornece desempenho rápido e previsível com escalabilidade perfeita. O Amazon DynamoDB permite descarregar os encargos administrativos de operação e dimensionamento de bancos de dados distribuídos para a AWS, para que você não precisa se preocupar com provisionamento de hardware, instalação e configuração, replicação, aplicação de patches de software ou dimensionamento de cluster.

Você pode criar uma tabela de banco de dados que possa armazenar e recuperar qualquer quantidade de dados e atender a qualquer nível de tráfego de solicitação. O Amazon DynamoDB espalha automaticamente os dados e o tráfego para a tabela sobre um número suficiente de servidores para lidar com a capacidade de solicitação especificada e a quantidade de dados armazenados, mantendo um desempenho rápido e consistente.

Todos os itens de dados são armazenados em unidades de estado sólido (SSDs) e são replicados automaticamente em várias zonas de disponibilidade em uma região para fornecer alta disponibilidade e durabilidade de dados.

Você pode configurar backups automáticos usando um modelo especial no AWS Data Pipeline que foi criado apenas para copiar tabelas do Amazon DynamoDB. Você pode escolher backups completos ou incrementais para uma tabela na mesma região ou em uma região diferente.

Você pode usar a cópia para recuperação de desastre no caso de um erro no seu código danificar a tabela original ou federar dados do Amazon DynamoDB entre regiões para oferecer suporte a um aplicativo com várias regiões.

Para controlar quem pode usar os recursos e a API do Amazon DynamoDB, configure as permissões no AWS IAM. Além de controlar o acesso no nível do recurso com o IAM, você também pode controlar o acesso no nível do banco de dados - você pode criar permissões no nível do banco de dados que permitem ou negam o acesso a itens (linhas) e atributos (colunas) com base nas necessidades de sua aplicação.

Essas permissões no nível do banco de dados são chamadas de controles de acesso refinados, e você as cria usando uma política do IAM que especifica sob quais circunstâncias um usuário ou aplicativo pode acessar uma tabela do Amazon DynamoDB. A política do IAM pode restringir o acesso a itens individuais em uma tabela, o acesso aos atributos nesses itens ou a ambos ao mesmo tempo.

Além de exigir permissões de banco de dados e de usuário, cada solicitação ao serviço Amazon DynamoDB deve conter uma assinatura HMAC-SHA-256 válida ou a solicitação é rejeitada.

Os AWS SDKs assinam automaticamente suas solicitações; no entanto, se você quiser escrever suas próprias solicitações HTTP POST, deverá fornecer a assinatura no cabeçalho da sua solicitação ao Amazon DynamoDB. Para calcular a assinatura, você deve solicitar credenciais de segurança temporárias do AWS Security Token Service.

Use as credenciais de segurança temporárias para assinar suas solicitações no Amazon DynamoDB. O Amazon DynamoDB pode ser acessado por terminais criptografados em SSL, e os terminais criptografados podem ser acessados na Internet e no Amazon EC2.

Segurança do Amazon RDS

O Amazon Relational Database Service (Amazon RDS) permite criar rapidamente uma Instância de banco de dados relacional (Instância de banco de dados) e escalar com flexibilidade os recursos de computação associados e a capacidade de armazenamento para atender à demanda de aplicativos.

O Amazon RDS gerencia a instância do banco de dados em seu nome, executando backups, manipulando o failover e mantendo o software do banco de dados.

Até o momento em que este artigo foi escrito, o Amazon RDS estava disponível para os mecanismos de banco de dados MySQL, Oracle, Microsoft SQL Server, MariaDB, Amazon Aurora e PostgreSQL.

O Amazon RDS possui vários recursos que aprimoram a confiabilidade de bancos de dados críticos de produção, incluindo grupos de segurança de banco de dados, permissões, conexões SSL, backups automatizados, snapshots de banco de dados e várias implantações da Zona de Disponibilidade (Multi-AZ).

As instâncias de banco de dados também podem ser implantadas em um Amazon VPC para isolamento adicional da rede.

Controle de acesso

Quando você cria uma Instância de banco de dados pela primeira vez no Amazon RDS, cria uma conta de usuário principal, que é usada apenas no contexto do Amazon RDS para controlar o acesso às suas Instâncias de banco de dados.

A conta de usuário principal é uma conta de usuário nativa do banco de dados que permite fazer logon na sua Instância de Banco de Dados com todos os privilégios do banco de dados.

Você pode especificar o nome de usuário mestre e a senha que deseja associar a cada Instância de banco de dados ao criar a Instância de banco de dados. Depois de criar sua Instância de banco de dados, você pode se conectar ao banco de dados usando as credenciais de usuário principal. Posteriormente, você pode criar contas de usuário adicionais para restringir quem pode acessar sua instância de banco de dados.

Você pode controlar o acesso à instância do Amazon RDS DB via grupos de segurança do DB, que são semelhantes aos grupos de segurança do Amazon EC2, mas não são intercambiáveis. Os grupos de segurança do banco de dados agem como um firewall que controla o acesso da rede à sua instância de banco de dados. Os grupos de segurança do banco de dados são padrão para negar todo o modo de acesso, e os clientes devem autorizar especificamente a entrada na rede.

Há duas maneiras de fazer isso:

- Autorizando um intervalo de IP de rede
- Autorizando um grupo de segurança existente do Amazon EC2

Os grupos de segurança do banco de dados permitem apenas o acesso à porta do servidor de banco de dados (todos os outros estão bloqueados) e podem ser atualizados sem reiniciar a Instância de banco de dados do Amazon RDS, o que fornece controle contínuo do acesso ao banco de dados.

Usando o AWS IAM, você pode controlar ainda mais o acesso às suas instâncias do Amazon RDS DB. O AWS IAM permite controlar as operações do Amazon RDS que cada usuário do AWS IAM tem permissão para chamar.

Isolamento de rede

Para controle de acesso à rede adicional, você pode executar suas instâncias de banco de dados em um Amazon VPC. O Amazon VPC permite isolar suas instâncias de banco de dados especificando o intervalo de IPs que você deseja usar e se conectar à sua infraestrutura de TI existente por meio da VPN IPsec criptografada padrão do setor.

A execução do Amazon RDS em uma VPC permite que você tenha uma instância de banco de dados em uma sub-rede privada. Você também pode configurar um gateway privado virtual que estenda sua rede corporativa à sua VPC e permita acesso à instância do RDS DB nessa VPC.

Para implantações Multi-AZ, a definição de uma sub-rede para todas as zonas de disponibilidade em uma região permitirá que o Amazon RDS crie um novo modo de espera em outra zona de disponibilidade, se necessário. Você pode criar grupos de sub-rede de banco de dados, que são coleções de sub-redes que você pode designar para suas instâncias de banco de dados do Amazon RDS em um Amazon VPC.

Cada grupo de sub-rede de banco de dados deve ter pelo menos uma sub-rede para cada zona de disponibilidade em uma determinada região. Nesse caso, quando você cria uma instância de banco de dados em um Amazon VPC, você seleciona um grupo de sub-rede de banco de dados; O Amazon RDS usa esse grupo de sub-redes do banco de dados e sua Zona de disponibilidade preferida para selecionar uma sub-rede e um endereço IP dentro dessa sub-rede.

O Amazon RDS cria e associa uma interface de rede elástica à sua instância de banco de dados com esse endereço IP.

As instâncias de banco de dados implantadas em um Amazon VPC podem ser acessadas da Internet ou de instâncias do Amazon EC2 fora do Amazon VPC por meio de hosts VPN ou bastiões que você pode iniciar em sua sub-rede pública.

Para usar um host bastião, você precisará configurar uma sub-rede pública com uma instância do Amazon EC2 que atue como bastião SSH. Essa sub-rede pública

deve ter um gateway da Internet e regras de roteamento que permitam direcionar o tráfego através do host SSH, que deve encaminhar solicitações para o endereço IP privado da sua instância do Amazon RDS DB.

Grupos de segurança de banco de dados podem ser usados para ajudar a proteger instâncias de banco de dados dentro de um Amazon VPC. Além disso, o tráfego de rede que entra e sai de cada sub-rede pode ser permitido ou negado por meio de ACLs da rede. Todo o tráfego de rede que entra ou sai do Amazon VPC por meio da conexão VPN IPsec pode ser inspecionado pela infraestrutura de segurança local, incluindo firewalls de rede e sistemas de detecção de intrusão.

Criptografia

Você pode criptografar conexões entre seu aplicativo e sua Instância de banco de dados usando SSL. Para MySQL e SQL Server, o Amazon RDS cria um certificado SSL e instala o certificado na instância do banco de dados quando a instância é provisionada.

Para o MySQL, você inicia o cliente MySQL usando o parâmetro --ssl_ca para referenciar a chave pública para criptografar as conexões. Para o SQL Server, baixe a chave pública e importe o certificado para o sistema operacional Windows. O Oracle RDS usa criptografia de rede nativa Oracle com uma instância de banco de dados.

Você simplesmente adiciona a opção de criptografia de rede nativa a um grupo de opções e associa esse grupo de opções à instância do banco de dados. Depois que uma conexão criptografada é estabelecida, os dados transferidos entre a Instância do banco de dados e seu aplicativo serão criptografados durante a transferência.

Você também pode exigir que sua Instância de banco de dados aceite apenas conexões criptografadas.

O Amazon RDS suporta criptografia de dados transparente (TDE) para SQL Server (SQL Server Enterprise Edition) e Oracle (parte da opção Oracle Advanced Security disponível no Oracle Enterprise Edition).

O recurso TDE criptografa automaticamente os dados antes de serem gravados para armazenamento e descriptografa automaticamente os dados quando são lidos do armazenamento. Se você precisar que seus dados MySQL sejam criptografados enquanto estiver descansando no banco de dados, seu aplicativo deverá gerenciar a criptografia e descriptografia de dados.

Observe que o suporte a SSL no Amazon RDS é para criptografar a conexão entre seu aplicativo e sua instância de banco de dados; não deve ser invocado para autenticar a própria instância do banco de dados. Embora o SSL ofereça benefícios de segurança, lembre-se de que a criptografia SSL é uma operação intensiva em computação e aumentará a latência da sua conexão com o banco de dados.

Backups automatizados e snapshots de banco de dados O Amazon RDS fornece dois métodos diferentes para fazer backup e restaurar suas instâncias de banco de dados: backups automatizados e snapshots de banco de dados (snapshots de banco de dados). Ativado por padrão, o recurso de backup automatizado do Amazon RDS permite a recuperação point-in-time para sua Instância de banco de dados.

O Amazon RDS fará backup do banco de dados e dos logs de transações e armazenará ambos por um período de retenção especificado pelo usuário. Isso permite restaurar a instância do banco de dados a qualquer segundo durante o período de retenção, até os últimos cinco minutos.

Seu período de retenção de backup automático pode ser configurado para até 35 dias. Snapshots de banco de dados são backups iniciados pelo usuário da sua instância de banco de dados.

Esses backups completos do banco de dados são armazenados pelo Amazon RDS até que você os exclua explicitamente. Você pode copiar snapshots de banco de dados de qualquer tamanho e movê-los entre qualquer uma das regiões públicas da AWS ou copiar o mesmo snapshot para várias regiões simultaneamente. Você pode criar uma nova instância de banco de dados a partir de um snapshot de banco de dados sempre que desejar.

Durante a janela de backup, a E / S de armazenamento pode ser suspensa enquanto o backup dos dados está sendo feito. Essa suspensão de E / S normalmente dura

alguns minutos. Essa suspensão de E / S é evitada nas implantações do Multi-AZ DB, porque o backup é retirado do modo de espera.

Replicação de Instância de Banco de Dados

Os recursos de computação em nuvem da AWS estão alojados em instalações de data center altamente disponíveis em diferentes regiões do mundo, e cada região contém vários locais distintos chamados Zonas de Disponibilidade.

Cada zona de disponibilidade é projetada para se isolar de falhas em outras zonas de disponibilidade e fornecer uma rede de baixo custo e baixa latência de conectividade com outras zonas de disponibilidade na mesma região.

Para projetar a alta disponibilidade de seus bancos de dados Oracle, PostgreSQL ou MySQL, você pode executar a instância do Amazon RDS DB em várias zonas de disponibilidade, uma opção chamada implantação Multi-AZ.

Quando você seleciona essa opção, a AWS provisiona e mantém automaticamente uma réplica síncrona em espera da sua Instância de banco de dados em uma zona de disponibilidade diferente.

A instância de banco de dados principal é replicada de forma síncrona nas zonas de disponibilidade para a réplica em espera. No caso de falha da instância do banco de dados ou da zona de disponibilidade, o Amazon RDS fará failover automaticamente no modo de espera, para que as operações do banco de dados possam ser retomadas rapidamente sem intervenção administrativa.

Para clientes que usam o MySQL e precisam escalar além das restrições de capacidade de uma única instância de banco de dados para cargas de trabalho de banco de dados com muita leitura, o Amazon RDS fornece uma opção de réplica de leitura.

Depois de criar uma réplica de leitura, as atualizações do banco de dados na Instância de banco de dados de origem são replicadas para a réplica de leitura usando a replicação assíncrona nativa do MySQL.

Você pode criar várias réplicas de leitura para uma determinada instância de banco de dados de origem e distribuir o tráfego de leitura do seu aplicativo entre elas. As réplicas de leitura podem ser criadas com implantações Multi-AZ para obter benefícios de escala de leitura, além da disponibilidade aprimorada de gravação no banco de dados e durabilidade dos dados fornecidos pelas implantações Multi-AZ.

Correção automática de software

O Amazon RDS garantirá que o software de banco de dados relacional que alimenta sua implantação permaneça atualizado com os patches mais recentes.

Quando necessário, os patches são aplicados durante uma janela de manutenção que você pode controlar. Você pode pensar na janela de manutenção do Amazon RDS como uma oportunidade de controlar quando ocorrem modificações na Instância do banco de dados (como a classe de instância do banco de dados de escala) e correções de software, em que o evento é solicitado ou necessário.

Se um evento de manutenção for agendado para uma determinada semana, ele será iniciado e concluído em algum momento durante a janela de manutenção de 30 minutos que você identificar.

Os únicos eventos de manutenção que exigem que o Amazon RDS coloque sua Instância de banco de dados offline são operações de computação em escala (que geralmente levam apenas alguns minutos do início ao fim) ou aplicação de patches de software.

O patch necessário é agendado automaticamente apenas para patches relacionados à segurança e durabilidade. Essas correções ocorrem com pouca frequência (geralmente uma vez a cada poucos meses) e raramente exigem mais do que uma fração da sua janela de manutenção.

Se você não especificar uma janela de manutenção semanal preferida ao criar sua Instância de banco de dados, um valor padrão de 30 minutos será atribuído. Se você deseja modificar quando a manutenção é executada em seu nome, você pode fazê-lo modificando sua Instância de banco de dados no AWS Management Console ou usando a API ModifyDBInstance.

Cada uma das suas instâncias de banco de dados pode ter diferentes janelas de manutenção preferenciais, se você escolher.

A execução da sua Instância de banco de dados em uma implantação Multi-AZ pode reduzir ainda mais o impacto de um evento de manutenção, pois o Amazon RDS realizará a manutenção através das seguintes etapas:

1. Execute a manutenção no modo de espera.
2. Promova o modo de espera para o primário.
3. Execute a manutenção no primário antigo, que se torna o novo modo de espera.

Quando uma API de exclusão da instância do Amazon RDS DB (DeleteDBInstance) é executada, a instância do banco de dados é marcada para exclusão. Depois que a instância não indica mais o status de exclusão, ela foi removida. Nesse momento, a instância não está mais acessível e, a menos que uma cópia final do snapshot tenha sido solicitada, ela não poderá ser restaurada e não será listada por nenhuma das ferramentas ou APIs.

Amazon Redshift Security

O Amazon Redshift é um serviço de data warehouse SQL em escala de petabytes que é executado em recursos de computação e armazenamento altamente otimizados e gerenciados da AWS.

O serviço foi arquitetado não apenas para aumentar ou diminuir rapidamente, mas também para melhorar significativamente as velocidades de consulta, mesmo em conjuntos de dados extremamente grandes.

Para aumentar o desempenho, o Amazon Redshift usa técnicas como armazenamento colunar, compactação de dados e mapas de zona para reduzir a quantidade de E / S necessária para executar consultas. Ele também possui uma arquitetura MPP (Massively Parallel Processing), paralelizando e distribuindo operações SQL para aproveitar todos os recursos disponíveis.

Acesso ao Cluster

Por padrão, os clusters que você cria são fechados para todos. O Amazon Redshift permite configurar regras de firewall (grupos de segurança) para controlar o acesso de rede ao cluster de data warehouse. Você também pode executar o Amazon Redshift dentro de um Amazon VPC para isolar o cluster de data warehouse em sua própria rede virtual e conectá-lo à sua infraestrutura de TI existente usando a VPN IPsec criptografada padrão do setor.

A conta da AWS que cria o cluster tem acesso total ao cluster. Na sua conta da AWS, você pode usar o AWS IAM para criar contas de usuário e gerenciar permissões para essas contas. Ao usar o IAM, você pode conceder permissão a diferentes usuários para executar apenas as operações de cluster necessárias para o trabalho delas.

Como todos os bancos de dados, você deve conceder permissão no Amazon Redshift no nível do banco de dados, além de conceder acesso no nível do recurso.

Os usuários do banco de dados são denominados contas de usuário que podem se conectar a um banco de dados e são autenticadas quando efetuam login no Amazon Redshift. No Amazon Redshift, você concede permissões de usuário de banco de dados por cluster, em vez de por tabela.

No entanto, os usuários podem ver dados apenas nas linhas da tabela que foram geradas por suas próprias atividades; linhas geradas por outros

os usuários não são visíveis para eles.

O usuário que cria um objeto de banco de dados é seu proprietário. Por padrão, apenas um superusuário ou o proprietário de um objeto pode consultar, modificar ou conceder permissões ao objeto. Para que os usuários usem um objeto, você deve conceder as permissões necessárias ao usuário ou ao grupo que contém o

do utilizador. Além disso, apenas o proprietário de um objeto pode modificá-lo ou excluí-lo.

Backups de dados

O Amazon Redshift distribui seus dados por todos os nós de computação em um cluster. Quando você executa um cluster com pelo menos dois nós de computação, os dados em cada nó sempre serão espelhados em discos em outro nó, reduzindo o risco de perda de dados.

Além disso, é feito backup contínuo de todos os dados gravados em um nó do cluster no Amazon S3 usando snapshots. O Amazon Redshift armazena seus snapshots por um período definido pelo usuário, que pode ser de 1 a 35 dias.

Você também pode tirar suas próprias capturas instantâneas a qualquer momento; esses snapshots aproveitam todos os snapshots do sistema existentes e são mantidos até que você os exclua explicitamente.

O Amazon Redshift monitora continuamente a integridade do cluster e replica automaticamente os dados de unidades com falha e substitui os nós conforme necessário. Tudo isso acontece sem nenhum esforço de sua parte, embora você possa observar uma ligeira degradação do desempenho durante o processo de replicação.

Você pode usar qualquer snapshot do sistema ou do usuário para restaurar seu cluster usando o AWS Management Console ou as APIs do Amazon Redshift.

Seu cluster estará disponível assim que os metadados do sistema forem restaurados e você poderá iniciar a execução de consultas enquanto os dados do usuário estão em spool.

Criptografia de Dados

Ao criar um cluster, você pode optar por criptografá-lo para fornecer proteção adicional aos seus dados em repouso. Quando você ativa a criptografia em seu cluster, o Amazon Redshift armazena todos os dados em tabelas criadas pelo usuário em um formato criptografado usando chaves de criptografia de bloco AES-256 aceleradas por hardware. Isso inclui todos os dados gravados no disco e todos os backups.

O Amazon Redshift usa uma arquitetura baseada em chave de quatro camadas para criptografia. Essas chaves consistem em chaves de criptografia de dados, uma chave de banco de dados, uma chave de cluster e uma chave mestra.

As chaves de criptografia de dados criptografam os blocos de dados no cluster. Cada bloco de dados recebe uma chave AES256 gerada aleatoriamente. Essas chaves são criptografadas usando a chave do banco de dados do cluster.

A chave do banco de dados criptografa as chaves de criptografia de dados no cluster. A chave do banco de dados é uma chave AES-256 gerada aleatoriamente. Ele é armazenado em disco em uma rede separada do cluster Amazon Redshift e criptografado por uma chave mestra. O Amazon Redshift passa a chave do banco de dados por um canal seguro e a mantém na memória no cluster.

A chave do cluster criptografa a chave do banco de dados do cluster Amazon Redshift. Você pode usar a AWS ou um HSM (Hardware Security Module) para armazenar a chave do cluster.

Os HSMs fornecem controle direto da geração e gerenciamento de chaves e tornam o gerenciamento de chaves separado e distinto do aplicativo e do banco de dados.

A chave mestra criptografa a chave do cluster se estiver armazenada na AWS. A chave mestra criptografa a chave de banco de dados criptografada pela chave do cluster se a chave do cluster estiver armazenada em um HSM.

Você pode fazer com que o Amazon Redshift gire as chaves de criptografia dos seus clusters criptografados a qualquer momento. Como parte do processo de rotação, as chaves também são atualizadas para todos os snapshots automáticos e manuais do cluster.

Observe que a ativação da criptografia em seu cluster afetará o desempenho, mesmo que seja acelerado por hardware.

A criptografia também se aplica aos backups. Quando você estiver restaurando a partir de um snapshot criptografado, o novo cluster também será criptografado.

Para criptografar sua tabela, carregue os arquivos de dados ao carregá-los no Amazon S3, você pode usar a criptografia no servidor do Amazon S3. Quando você

carrega os dados do Amazon S3, o comando COPY descriptografa os dados à medida que carrega a tabela.

Log de auditoria de banco de dados

O Amazon Redshift registra todas as operações SQL, incluindo tentativas de conexão, consultas e alterações no seu banco de dados. Você pode acessar esses logs usando consultas SQL em tabelas do sistema ou optar por fazer o download para um bucket seguro do Amazon S3. Em seguida, você pode usar esses logs de auditoria para monitorar seu cluster para fins de segurança e solução de problemas.

Correção automática de software

O Amazon Redshift gerencia todo o trabalho de configurar, operar e dimensionar seu data warehouse, incluindo capacidade de provisionamento, monitoramento do cluster e aplicação de patches e atualizações no mecanismo Amazon Redshift. Os patches são aplicados apenas durante as janelas de manutenção especificadas.

Conexões SSL

Para proteger seus dados em trânsito na nuvem da AWS, Amazon Redshift usa SSL acelerado por hardware para se comunicar com o Amazon S3 ou o Amazon DynamoDB para operações de COPY, UNLOAD, backup e restauração. Você pode criptografar a conexão entre seu cliente e o cluster especificando SSL no grupo de parâmetros associado ao cluster.

Para que seus clientes também autentiquem o servidor Amazon Redshift, você pode instalar a chave pública (arquivo .pem) do certificado SSL em seu cliente e usar a chave para conectar-se aos seus clusters.

O Amazon Redshift oferece os conjuntos de cifras mais novos e mais fortes que usam o protocolo Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). O ECDHE permite que os clientes SSL forneçam o Perfect Forward Secrecy entre o cliente e o cluster do Amazon Redshift.

O Perfect Forward Secrecy usa chaves de sessão efêmeras e não armazenadas em qualquer lugar, o que impede a decodificação de dados capturados por terceiros

não autorizados, mesmo se a própria chave secreta de longo prazo estiver comprometida.

Você não precisa configurar nada no Amazon Redshift para ativar o ECDHE. Se você se conectar a partir de uma ferramenta de cliente SQL que usa ECDHE para criptografar a comunicação entre o cliente e o servidor, o Amazon Redshift usará a lista de criptografia fornecida para estabelecer a conexão apropriada.

Amazon ElastiCache Security

O Amazon ElastiCache é um serviço da Web que facilita a configuração, o gerenciamento e a escalabilidade de ambientes de cache na memória distribuídos na nuvem.

O serviço melhora o desempenho dos aplicativos da Web, permitindo recuperar informações de um sistema de cache em memória gerenciado e rápido, em vez de depender inteiramente de um disco mais lento, baseado em disco de bancos de dados.

Ele pode ser usado para melhorar significativamente a latência e a taxa de transferência para muitas cargas de trabalho de aplicativos pesados (como redes sociais, jogos, compartilhamento de mídia e portais de perguntas e respostas) ou cargas de trabalho intensivas em computação (como um mecanismo de recomendação).

O armazenamento em cache melhora o desempenho do aplicativo, armazenando dados críticos na memória para acesso de baixa latência. As informações em cache podem incluir os resultados de consultas de banco de dados intensivas em E / S ou os resultados de cálculos computacionalmente intensivos.

O serviço Amazon ElastiCache automatiza tarefas de gerenciamento demoradas para ambientes de cache de memória, como gerenciamento de patches, detecção de falhas e recuperação. Funciona em conjunto com outros serviços da AWS Cloud (como Amazon EC2, Amazon CloudWatch e Amazon SNS) para fornecer um cache de memória seguro, de alto desempenho e gerenciado.

Por exemplo, um aplicativo em execução no Amazon EC2 pode acessar com segurança um cluster do Amazon ElastiCache na mesma região com latência muito baixa.

Usando o serviço Amazon ElastiCache, você cria um cluster de cache, que é uma coleção de um ou mais nós de cache, cada um executando uma instância do serviço Memcached. Um nó de cache é um pedaço de tamanho fixo de RAM segura e conectada à rede. Cada nó de cache executa uma instância do serviço Memcached e possui seu próprio nome DNS e porta. Vários tipos de nós de cache são suportados, cada um com quantidades variáveis de memória associada.

Um cluster de cache pode ser configurado com um número específico de nós de cache e um grupo de parâmetros de cache que controla as propriedades de cada nó de cache. Todos os nós de cache em um cluster de cache foram projetados para serem do mesmo tipo de nó e terem as mesmas configurações de parâmetro e grupo de segurança.

Acesso de dados

O Amazon ElastiCache permite controlar o acesso aos seus Clusters de cache usando grupos de segurança de cache. Um grupo de segurança de cache age como um firewall, controlando o acesso da rede ao seu cluster de cache. Por padrão, o acesso à rede está desativado nos seus Clusters de cache.

Se você deseja que seus aplicativos acessem seu cluster de cache, ative explicitamente o acesso de hosts em grupos de segurança específicos do Amazon EC2. Após a configuração das regras de entrada, as mesmas regras se aplicam a todos os Clusters de cache associados a esse grupo de segurança de cache.

Para permitir o acesso da rede ao seu cluster de cache, crie um grupo de segurança de cache e use a API ou o comando CLI de entrada de grupo de segurança de cache de autorização para autorizar o grupo de segurança desejado do Amazon EC2 (que por sua vez especifica as instâncias do Amazon EC2 permitidas). O controle de acesso baseado em IPrange atualmente não está ativado para Clusters de cache.

Todos os clientes de um cluster de cache devem estar na rede Amazon EC2 e autorizados por meio de grupos de segurança de cache.

O Amazon ElastiCache for Redis fornece funcionalidade de backup e restauração, onde é possível criar uma captura instantânea de todo o cluster Redis, como existe em um momento específico. Você pode agendar snapshots diários automáticos e recorrentes ou criar um snapshot manual a qualquer momento.

Para capturas instantâneas automáticas, você especifica um período de retenção; os snapshots manuais são mantidos até que você os exclua. Os snapshots são armazenados no Amazon S3 com alta durabilidade e podem ser usados para inicialização a quente, backups e arquivamento.

Serviços de Aplicação

A AWS oferece uma variedade de serviços gerenciados para uso com seus aplicativos, incluindo serviços que fornecem fluxo de aplicativos, enfileiramento, notificação por push, entrega de email, pesquisa e transcodificação.

Segurança do Amazon Simple Queue Service (Amazon SQS)

O Amazon SQS é um serviço escalável e altamente confiável de enfileiramento de mensagens que permite a comunicação assíncrona baseada em mensagens entre os componentes distribuídos de um aplicativo. Os componentes podem ser computadores ou instâncias do Amazon EC2 ou uma combinação de ambos.

Com o Amazon SQS, você pode enviar qualquer número de mensagens para uma fila do Amazon SQS a qualquer momento a partir de qualquer componente. As mensagens podem ser recuperadas do mesmo componente ou de outro, imediatamente ou posteriormente (em 14 dias).

As mensagens são altamente duráveis; cada mensagem é armazenada persistentemente em filas altamente disponíveis e altamente confiáveis. Vários

processos podem ler / gravar de / para uma fila do Amazon SQS ao mesmo tempo sem interferir um no outro.

Acesso de dados

O acesso ao Amazon SQS é concedido com base em uma conta da AWS ou em um usuário criado com o AWS IAM. Depois de autenticada, a conta da AWS tem acesso total a todas as operações do usuário. Um usuário do IAM, no entanto, só tem acesso às operações e filas para as quais foram acessos concedidos via política.

Por padrão, o acesso a cada fila individual é restrito à conta da AWS que o criou. No entanto, você pode permitir outro acesso a uma fila, usando uma política gerada pelo Amazon SQS ou uma política que você escreve.

Criptografia

O Amazon SQS pode ser acessado por terminais criptografados em SSL. Os terminais criptografados são acessíveis pela Internet e pelo Amazon EC2. Os dados armazenados no Amazon SQS não são criptografados pela AWS; no entanto, o usuário pode criptografar os dados antes de fazer o upload para o Amazon SQS, desde que o aplicativo que usa a fila tenha um meio de descriptografar a mensagem quando ela for recuperada.

A criptografia de mensagens antes de enviá-las ao Amazon SQS ajuda a proteger contra o acesso a dados confidenciais de clientes por pessoas não autorizadas, incluindo a AWS.

Segurança do Amazon Simple Notification Service (Amazon SNS)

O Amazon SNS é um serviço da Web que facilita a configuração, a operação e o envio de notificações da nuvem. Ele fornece aos desenvolvedores um recurso altamente escalável, flexível e econômico para publicar mensagens de um aplicativo e entregá-las imediatamente para assinantes ou outros aplicativos.

O Amazon SNS fornece uma interface simples de serviços da web que pode ser usado para criar tópicos sobre os quais os clientes desejam notificar aplicativos (ou pessoas), inscrever clientes nesses tópicos, publicar mensagens e enviar essas mensagens por protocolo de escolha dos clientes (por exemplo, HTTP / HTTPS, email).

O Amazon SNS entrega notificações aos clientes usando um mecanismo de envio que elimina a necessidade de verificar ou buscar novas informações e atualizações periodicamente.

O Amazon SNS pode ser aproveitado para criar fluxos de trabalho e aplicativos de mensagens altamente confiáveis e controlados por eventos, sem a necessidade de gerenciamento complexo de aplicativos e middleware.

Os usos potenciais para o Amazon SNS incluem aplicativos de monitoramento, sistemas de fluxo de trabalho, atualizações de informações sensíveis ao tempo, aplicativos móveis e muitos outros.

Acesso de dados

O Amazon SNS fornece mecanismos de controle de acesso para que tópicos e mensagens sejam protegidos contra acesso não autorizado. Os proprietários do tópico podem definir políticas para um tópico que restrinja quem pode publicar ou assinar um tópico.

Além disso, os proprietários do tópico podem criptografar a transmissão especificando que o mecanismo de entrega deve ser HTTPS.

O acesso ao Amazon SNS é concedido com base em uma conta da AWS ou em um usuário criado com o AWS IAM. Depois de autenticada, a conta da AWS tem acesso total a todas as operações do usuário.

Um usuário do IAM, no entanto, só tem acesso às operações e tópicos aos quais eles receberam acesso via política.

Por padrão, o acesso a cada tópico individual é restrito à conta da AWS que o criou. No entanto, você pode permitir outro acesso ao Amazon SNS, usando uma política gerada pelo Amazon SNS ou uma política que você escreve.

Serviços de análise

A AWS fornece serviços de análise baseados na nuvem para ajudá-lo a processar e analisar qualquer volume de dados, independentemente de sua necessidade de clusters gerenciados do Hadoop, dados de streaming em tempo real, data warehousing em escala de petabytes ou orquestração.

Segurança do Amazon Elastic MapReduce (Amazon EMR)

O Amazon Elastic MapReduce (Amazon EMR) é um serviço da web gerenciado que você pode usar para executar clusters do Hadoop que processam grandes quantidades de dados, distribuindo o trabalho e os dados entre vários servidores. Ele usa uma versão aprimorada da estrutura do Apache Hadoop em execução na infraestrutura de escala da Web do Amazon EC2 e Amazon S3.

Você simplesmente carrega seus dados de entrada e um aplicativo de processamento de dados no Amazon S3. O Amazon EMR inicia o número de instâncias do Amazon EC2 que você especificar. O serviço inicia a execução do fluxo de trabalho enquanto puxa os dados de entrada do Amazon S3 para as instâncias iniciadas do Amazon EC2.

Após a conclusão do fluxo de trabalho, o Amazon EMR transfere os dados de saída para o Amazon S3, onde você pode recuperá-los ou usá-los como entrada em outro fluxo de trabalho.

Ao iniciar fluxos de trabalho em seu nome, o Amazon EMR configura dois grupos de segurança do Amazon EC2: um para os nós principais e outro para os escravos. O grupo de segurança principal possui uma porta aberta para comunicação com o serviço. Ele também possui a porta SSH aberta para permitir o SSH nas instâncias usando a chave especificada na inicialização.

Os escravos iniciam em um grupo de segurança separado, que permite apenas a interação com a instância principal. Por padrão, os dois grupos de segurança são configurados para não permitir o acesso de fontes externas, incluindo instâncias do Amazon EC2 pertencentes a outros clientes. Como esses grupos são de segurança na sua conta, você pode reconfigurá-los usando as ferramentas ou o painel padrão do EC2. Para proteger os conjuntos de dados de entrada e saída do cliente, o Amazon EMR transfere dados de e para o Amazon S3 usando SSL.

O Amazon EMR fornece várias maneiras de controlar o acesso aos recursos do seu cluster. Você pode usar o AWS IAM para criar contas e funções de usuário e configurar permissões que controlam quais recursos da AWS esses usuários e funções podem acessar. Ao iniciar um cluster, você pode associar um par de chaves do Amazon EC2 ao cluster, que pode ser usado quando você se conecta ao cluster usando SSH.

Você também pode definir permissões que permitam usuários diferentes do padrão de usuário do Hadoop para enviar tarefas ao seu cluster. Por padrão, se um usuário do IAM iniciar um cluster, esse cluster estará oculto de outros usuários do IAM a conta da AWS.

Essa filtragem ocorre em todas as interfaces do Amazon EMR (console de gerenciamento da AWS, CLI, API e SDKs) e ajuda a impedir que os usuários do IAM acessem e alterem inadvertidamente os clusters criados por outros usuários do IAM.

Para uma camada adicional de proteção, você pode iniciar as instâncias do Amazon EC2 do cluster do Amazon EMR em um Amazon VPC, o que é como iniciá-lo em uma sub-rede privada.

Isso permite que você controle o acesso a toda a sub-rede. Você também pode iniciar o cluster em um Amazon VPC e permitir que o cluster acesse recursos em sua rede interna usando uma conexão VPN.

Você pode criptografar os dados de entrada antes de carregá-los no Amazon S3 usando qualquer ferramenta comum de criptografia de dados. Se você criptografar os dados antes do upload, precisará adicionar uma etapa de descriptografia ao

início do seu fluxo de trabalho quando o Amazon EMR buscar os dados do Amazon S3.

Segurança do Amazon Kinesis

O Amazon Kinesis é um serviço gerenciado projetado para lidar com o streaming em tempo real de big data. Ele pode aceitar qualquer quantidade de dados, de qualquer número de fontes, aumentando e diminuindo conforme necessário.

Você pode usar o Amazon Kinesis em situações que exigem ingestão e processamento em larga escala de dados em tempo real, como logs de servidor, mídias sociais ou feeds de dados de mercado e dados de fluxo de cliques na Web.

Os aplicativos leem e gravam registros de dados no Amazon Kinesis em fluxos. Você pode criar qualquer número de fluxos do Amazon Kinesis para capturar, armazenar e transportar dados.

Você pode controlar o acesso lógico aos recursos e funções de gerenciamento do Amazon Kinesis criando usuários na sua conta da AWS usando o AWS IAM e controlando quais operações do Amazon Kinesis esses usuários têm permissão para executar.

Para facilitar a execução de aplicativos produtores ou consumidores em uma instância do Amazon EC2, você pode configurar essa instância com uma função do IAM. Dessa forma, as credenciais da AWS que refletem as permissões associadas à função do IAM são disponibilizadas para aplicativos na instância, o que significa que você não precisa usar suas credenciais de segurança da AWS a longo prazo.

As funções têm o benefício adicional de fornecer credenciais temporárias que expiram dentro de um curto período de tempo, o que adiciona uma medida adicional de proteção.

A API Amazon Kinesis só pode ser acessada por meio de um ponto de extremidade criptografado por SSL (kinesis.us-east-1.amazonaws.com) para ajudar a garantir a transmissão segura de seus dados para a AWS. Você deve se conectar a esse

terminal para acessar o Amazon Kinesis, mas poderá usar a API para direcionar o Amazon Kinesis para criar um fluxo em qualquer região da AWS.

Serviços de implantação e gerenciamento

A AWS fornece uma variedade de ferramentas para ajudar na implantação e gerenciamento de seus aplicativos. Isso inclui serviços que permitem criar contas de usuário individuais com credenciais para acesso aos serviços da AWS.

Ele também inclui serviços para criar e atualizar pilhas de recursos da AWS, implantar aplicativos nesses recursos e monitorar a integridade desses recursos da AWS. Outras ferramentas ajudam a gerenciar chaves criptográficas usando HSMs e registrar a atividade da API da AWS para fins de segurança e conformidade.

Segurança do AWS Identity and Access Management (IAM)

O AWS IAM permite criar vários usuários e gerenciar as permissões para cada um desses usuários na sua conta da AWS. Um usuário é uma identidade (dentro de uma conta da AWS) com credenciais de segurança exclusivas que podem ser usadas para acessar os serviços em nuvem da AWS.

O IAM elimina a necessidade de compartilhar senhas ou chaves e facilita a habilitação ou desabilitação do acesso de um usuário, conforme apropriado.

O AWS IAM permite implementar práticas recomendadas de segurança, como privilégios mínimos, concedendo credenciais exclusivas a todos os usuários da sua conta da AWS e concedendo apenas permissão para acessar os serviços e recursos da AWS Cloud necessários para que os usuários realizem suas tarefas.

O IAM é seguro por padrão; novos usuários não têm acesso à AWS até que as permissões sejam concedidas explicitamente.

O AWS IAM também está integrado ao AWS Marketplace, para que você possa controlar quem em sua organização pode se inscrever no software e serviços oferecidos no AWS Marketplace.

Como a assinatura de um determinado software no AWS Marketplace inicia uma instância do Amazon EC2 para executar o software, esse é um recurso importante de controle de acesso.

O uso do IAM para controlar o acesso ao AWS Marketplace também permite que os proprietários da conta da AWS tenham controle refinado sobre o uso e custos de software. O AWS IAM permite minimizar o uso das credenciais da sua conta da AWS.

Depois de criar contas de usuário do IAM, todas as interações com os serviços e recursos da AWS Cloud devem ocorrer com as credenciais de segurança do usuário do IAM.

Funções

Uma função do IAM usa credenciais de segurança temporárias para permitir que você delegue o acesso a usuários ou serviços que normalmente não têm acesso aos seus recursos da AWS.

Uma função é um conjunto de permissões para acessar recursos específicos da AWS, mas essas permissões não estão vinculadas a um usuário ou grupo específico do IAM. Uma entidade autorizada (por exemplo, usuário móvel ou instância do Amazon EC2) assume uma função e recebe credenciais de segurança temporárias para autenticação nos recursos definidos na função.

As credenciais de segurança temporárias fornecem segurança aprimorada devido à sua curta vida útil (a expiração padrão é de 12 horas) e ao fato de que elas não podem ser reutilizadas depois que expiram. Isso pode ser particularmente útil ao fornecer acesso limitado e controlado em determinadas situações:

Acesso de usuário federado (não pertencente à AWS)

Usuários federados são usuários (ou aplicativos) que não possuem contas da AWS. Com as funções, você pode conceder acesso a seus recursos da AWS por um período limitado.

Isso é útil se você tiver usuários que não são da AWS e que podem se autenticar com um serviço externo, como Microsoft Active Directory, LDAP (Lightweight Directory Access Protocol) ou Kerberos.

As credenciais temporárias da AWS usadas com as funções fornecem federação de identidade entre a AWS e seus usuários não pertencentes à AWS em seu sistema de identidade e autorização corporativa.

Linguagem de Marcação de Asserção de Segurança (SAML) 2.0

Se sua organização oferecer suporte ao SAML 2.0, você poderá criar confiança entre sua organização como um provedor de identidade (IdP) e outras organizações como provedores de serviços.

Na AWS, você pode configurar a AWS como o provedor de serviços e usar o SAML para fornecer aos usuários SSO federado (SSO) no AWS Management Console ou obter acesso federado para chamar as APIs da AWS.

As funções também são úteis se você criar um aplicativo móvel ou baseado na Web que acesse os recursos da AWS. Os recursos da AWS exigem credenciais de segurança para solicitações programáticas; no entanto, você não deve incorporar credenciais de segurança de longo prazo em seu aplicativo, pois elas são acessíveis aos usuários do aplicativo e podem ser difíceis de alternar.

Em vez disso, você pode permitir que os usuários façam login no seu aplicativo usando o Login com Amazon, Facebook ou Google e, em seguida, use as informações de autenticação para assumir uma função e obter credenciais de segurança temporárias.

Acesso entre contas

Para organizações que usam várias contas da AWS para gerenciar seus recursos, você pode configurar funções para fornecer aos usuários que têm permissões em uma conta para acessar recursos em outra conta.

Para organizações que possuem funcionários que raramente precisam acessar recursos em outra conta, o uso de funções ajuda a garantir que as credenciais sejam fornecidas temporariamente e somente quando necessário.

Aplicativos em execução em instâncias EC2 que precisam acessar os recursos da AWS

Se um aplicativo é executado em uma instância do Amazon EC2 e precisa fazer solicitações de recursos da AWS, como buckets do Amazon S3 ou uma tabela do DynamoDB, ele deve ter credenciais de segurança. Usando funções em vez de criar contas individuais do IAM para cada aplicativo em cada instância, pode economizar tempo significativo para os clientes que gerenciam um grande número de instâncias ou uma frota de escala elástica usando o AWS Auto Scaling.

As credenciais temporárias incluem um token de segurança, um ID da chave de acesso e uma chave de acesso secreta. Para conceder ao usuário acesso a determinados recursos, você distribui as credenciais de segurança temporárias ao usuário a quem você está concedendo acesso temporário. Quando o usuário faz chamadas para seus recursos, ele passa o token e o ID da chave de acesso e assina a solicitação com a Chave de acesso secreta. O token não funcionará com chaves de acesso diferentes.

O uso de credenciais temporárias fornece proteção adicional para você, porque você não precisa gerenciar ou distribuir credenciais de longo prazo para usuários temporários. Além disso, as credenciais temporárias são carregadas automaticamente na instância de destino, para que você não precise incorporá-las em algum lugar inseguro como o seu código.

As credenciais temporárias são giradas ou alteradas automaticamente várias vezes ao dia, sem nenhuma ação da sua parte, e são armazenadas com segurança por padrão.

Serviços Móveis

Os serviços móveis da AWS facilitam a criação, o envio, a execução, o monitoramento, a otimização e o dimensionamento de aplicativos para dispositivos móveis baseados na nuvem.

Esses serviços também ajudam a autenticar usuários no seu aplicativo móvel, sincronizar dados e coletar e analisar o uso do aplicativo.

Amazon Cognito Security

O Amazon Cognito fornece serviços de identidade e sincronização para aplicativos móveis e baseados na Web. Ele simplifica a tarefa de autenticar usuários e armazenar, gerenciar e sincronizar seus dados em vários dispositivos, plataformas e aplicativos.

Ele fornece credenciais temporárias com privilégios limitados para usuários autenticados e não autenticados sem precisar gerenciar nenhuma infraestrutura de back-end.

O Amazon Cognito trabalha com provedores de identidade conhecidos como Google, Facebook e Amazon para autenticar usuários finais de seus aplicativos móveis e da Web. Você pode tirar proveito dos recursos de identificação e autorização fornecidos por esses serviços, em vez de precisar criar e manter seus próprios.

Seu aplicativo se autentica com um desses provedores de identidade usando o SDK do provedor. Depois que o usuário final é autenticado com o fornecedor, um token OAuth ou OpenID Connect retornado do provedor é passado pelo seu aplicativo para o Amazon Cognito, que retorna um novo ID do Amazon Cognito para o usuário e um conjunto de credenciais temporárias da AWS com privilégios limitados.

Para começar a usar o Amazon Cognito, você cria um pool de identidades por meio do console do Amazon Cognito. O pool de identidades é um armazenamento de informações de identidade do usuário específicas da sua conta da AWS.

Durante a criação do pool de identidades, você será solicitado a criar uma nova função do IAM ou escolher uma existente para seus usuários finais. Uma função do

IAM é um conjunto de permissões para acessar recursos específicos da AWS, mas essas permissões não estão vinculadas a um usuário ou grupo específico do IAM.

Uma entidade autorizada (por exemplo, usuário móvel, instância do Amazon EC2) assume uma função e recebe credenciais de segurança temporárias para autenticação nos recursos da AWS definidos na função.

As credenciais de segurança temporárias fornecem segurança aprimorada devido à sua curta vida útil (a expiração padrão é de 12 horas) e ao fato de que elas não podem ser reutilizadas depois que expiram.

A função que você seleciona afeta os serviços da AWS Cloud que seus usuários finais poderão acessar com credenciais temporárias. Por padrão, o Amazon Cognito cria uma nova função com permissões limitadas; os usuários finais têm acesso apenas ao serviço Amazon Cognito Sync e Amazon Mobile Analytics. Se seu aplicativo precisar acessar outros recursos da AWS, como Amazon S3 ou Amazon DynamoDB, você poderá modificar suas funções diretamente no console do IAM.

Com o Amazon Cognito, não há necessidade de criar contas individuais da AWS ou mesmo contas do IAM para todos os usuários finais de aplicativos da Web / dispositivos móveis que precisarão acessar seus recursos da AWS.

Em conjunto com as funções do IAM, os usuários móveis podem acessar com segurança a recursos da AWS e recursos de aplicativos e até mesmo salvar dados na nuvem da AWS sem precisar criar uma conta ou fazer login.

Se optarem por criar uma conta ou fazer login posteriormente, o Amazon Cognito mesclará informações de dados e identificação.

Como o Amazon Cognito armazena dados localmente e também no serviço, seus usuários finais podem continuar interagindo com os dados, mesmo quando estão offline. Seus dados offline podem estar obsoletos, mas eles podem recuperar imediatamente qualquer coisa que colocarem no conjunto de dados, estejam eles online ou não.

O SDK do cliente gerencia um armazenamento SQLite local para que o aplicativo possa funcionar mesmo quando não estiver conectado.

O armazenamento SQLite funciona como um cache e é o alvo de todas as operações de leitura e gravação. O recurso de sincronização do Amazon Cognito compara a versão local dos dados à versão em nuvem e aumenta ou diminui os deltas, conforme necessário. Observe que, para sincronizar dados entre dispositivos, seu pool de identidades deve suportar identidades autenticadas.

Identidades não autenticadas estão vinculadas ao dispositivo, portanto, a menos que um usuário final se autentique, nenhum dado poderá ser sincronizado em vários dispositivos.

Com o Amazon Cognito, seu aplicativo se comunica diretamente com um provedor de identidade pública suportado (Amazon, Facebook ou Google) para autenticar usuários. O Amazon Cognito não recebe ou armazena credenciais de usuário, apenas o token OAuth ou OpenID Connect recebido do provedor de identidade.

Depois que o Amazon Cognito recebe o token, ele retorna um novo ID do Amazon Cognito para o usuário e um conjunto de credenciais temporárias da AWS com privilégios limitados. Cada identidade do Amazon Cognito tem acesso apenas a seus próprios dados no armazenamento de sincronização, e esses dados são criptografados quando armazenados. Além disso, todos os dados de identidade são transmitidos por HTTPS.

O identificador exclusivo do Amazon Cognito no dispositivo é armazenado no local seguro apropriado. Por exemplo, no iOS, o identificador do Amazon Cognito é armazenado no chaveiro do iOS. Os dados do usuário são armazenados em cache em um banco de dados SQLite local na caixa de proteção do aplicativo; se você precisar de segurança adicional, poderá criptografar esses dados de identidade no cache local implementando a criptografia no seu aplicativo.

Aplicativos

Os aplicativos da AWS são serviços gerenciados que permitem fornecer a seus usuários áreas de trabalho e armazenamento centralizadas e seguras na nuvem.

Segurança do Amazon WorkSpaces

O Amazon WorkSpaces é um serviço de desktop gerenciado que permite o provisionamento rápido de desktops baseados em nuvem para seus usuários. Basta escolher um pacote do Windows 7 que melhor atenda às necessidades de seus usuários e ao número de WorkSpaces que você deseja iniciar.

Depois que os WorkSpaces estiverem prontos, os usuários receberão um email informando onde podem fazer o download do cliente relevante e efetuar login no WorkSpace.

Eles podem acessar seus desktops baseados na nuvem a partir de uma variedade de dispositivos de terminal, incluindo PCs, laptops e dispositivos móveis.

No entanto, os dados da sua organização nunca são enviados ou armazenados no dispositivo do usuário final porque o Amazon WorkSpaces usa PC-over-IP (PCoIP), que fornece um fluxo de vídeo interativo sem transmitir dados reais.

O protocolo PCoIP compacta, criptografa e codifica a experiência de computação em desktop dos usuários e transmite como pixels apenas em qualquer rede IP padrão para dispositivos do usuário final.

Para acessar o seu WorkSpace, os usuários devem entrar usando um conjunto de credenciais exclusivas ou suas credenciais regulares do Active Directory. Quando você integra o Amazon WorkSpaces ao Active Directory corporativo, cada WorkSpace ingressa no domínio do Active Directory e pode ser gerenciado como qualquer outra área de trabalho da sua organização.

Isso significa que você pode usar diretivas de grupo do Active Directory para gerenciar os espaços de trabalho dos usuários e especificar opções de configuração que controlam a área de trabalho. Se você optar por não usar o Active Directory ou

outro tipo de diretório onpremises para gerenciar seu WorkSpaces do usuário, poderá criar um diretório de nuvem privada no Amazon WorkSpaces que possa ser usado para administração.

Para fornecer uma camada adicional de segurança, você também pode exigir o uso do MFA ao entrar na forma de um token de hardware ou software.

O Amazon WorkSpaces oferece suporte ao MFA usando um servidor RADIUS (Remote Authentication Dial In User Service) ou qualquer provedor de segurança que suporta autenticação RADIUS. Atualmente, ele suporta os protocolos PAP, CHAP, MSCHAP1 e MS-CHAP2, juntamente com proxies RADIUS.

Cada WorkSpace reside em sua própria instância do Amazon EC2 em um Amazon VPC. Você pode criar WorkSpaces em um Amazon VPC que você já possui ou fazer com que o serviço Amazon WorkSpaces crie um para você automaticamente, usando a opção Início rápido do Amazon WorkSpaces.

Quando você usa a opção Início rápido, o Amazon WorkSpaces não apenas cria o Amazon VPC, mas também executa várias outras tarefas de provisionamento e configuração para você, como a criação de um gateway da Internet para o Amazon VPC, a configuração de um diretório no Amazon VPC que é usado para armazenar informações de usuário e espaço de trabalho, criando uma conta de administrador de diretório, criando as contas de usuário especificadas e adicionando-as ao diretório e criando as instâncias do Amazon WorkSpaces.

Ou o Amazon VPC pode ser conectado a uma rede local usando uma conexão VPN segura para permitir o acesso a um Active Directory local existente e outros recursos da intranet. Você pode adicionar um grupo de segurança criado no Amazon VPC a todos os espaços de trabalho que pertencem ao seu Active Directory.

Isso permite controlar o acesso à rede do Amazon WorkSpaces no Amazon VPC para outros recursos no Amazon VPC e na rede local.

O armazenamento persistente do Amazon WorkSpaces é fornecido pelo Amazon EBS e é feito backup automaticamente duas vezes por dia no Amazon S3. Se o Amazon WorkSpaces Sync estiver ativado em um WorkSpace, a pasta que um usuário escolher para sincronizar será continuamente copiada e armazenada no Amazon S3.

Você também pode usar o Amazon WorkSpaces Sync em um Mac ou PC para sincronizar documentos de ou para o seu WorkSpace, para que você possa sempre ter acesso aos seus dados, independentemente do computador que estiver usando.

Por ser um serviço gerenciado, a AWS cuida de várias tarefas de segurança e manutenção, como backups diários e aplicação de patches. As atualizações são entregues automaticamente nos seus WorkSpaces durante uma janela de manutenção semanal.

Você pode controlar como a aplicação de patches é configurada para o espaço de trabalho de um usuário. Por padrão, o Windows Update está ativado, mas você pode personalizar essas configurações ou use uma abordagem alternativa de gerenciamento de patches, se desejar. Para o sistema operacional subjacente, o Windows Update é ativado por padrão no Amazon WorkSpaces e configurado para instalar atualizações semanalmente.

Você pode usar uma abordagem alternativa de patch ou configurar o Windows Update para executar atualizações no momento que você escolher. Você pode usar o IAM para controlar quem em sua equipe pode executar funções administrativas, como criar ou excluir WorkSpaces ou configurar diretórios de usuários.

Você também pode configurar um WorkSpace para administração de diretórios, instalar suas ferramentas de administração favoritas do Active Directory e criar unidades organizacionais e políticas de grupo para aplicar as alterações do Active Directory com mais facilidade a todos os usuários do Amazon WorkSpaces.

Risco e Compliance na AWS

A AWS e seus clientes compartilham o controle sobre o ambiente de TI, para que ambas as partes sejam responsáveis pelo gerenciamento desse ambiente. A parte da AWS nessa responsabilidade compartilhada inclui o fornecimento de seus serviços em uma plataforma altamente segura e controlada e o fornecimento de uma ampla variedade de recursos de segurança que os clientes podem usar.

O cliente é responsável por configurar seu ambiente de TI de maneira segura e controlada para seus propósitos. Embora os clientes não comuniquem seu uso e configurações à AWS, a AWS se comunica com os clientes sobre sua segurança e controle do ambiente, conforme relevante. A AWS divulga essas informações usando três mecanismos principais.

Primeiro, a AWS trabalha diligentemente para obter certificações do setor e atestados independentes de terceiros. Segundo, a AWS publica abertamente informações sobre suas práticas de segurança e controle em whitepapers e conteúdo de sites.

Por fim, a AWS fornece certificados, relatórios e outras documentações diretamente a seus clientes sob os contratos de confidencialidade (NDAs), conforme necessário.

Quando os clientes transferem suas cargas de trabalho de produção para a nuvem da AWS, ambas as partes se tornam responsáveis pelo gerenciamento do ambiente de TI.

Os clientes são responsáveis por configurar seu ambiente de maneira segura e controlada. Os clientes também precisam manter a governança adequada sobre todo o ambiente de controle de TI. Esta seção descreve o modelo de responsabilidade compartilhada da AWS e fornece conselhos sobre como estabelecer uma conformidade forte.

Modelo de Responsabilidade Compartilhada

Esse modelo de responsabilidade compartilhada pode ajudar a diminuir a carga operacional de TI de um cliente, pois é responsabilidade da AWS gerenciar os componentes do sistema operacional host e da virtualização até a segurança física dos datacenters em que esses serviços operam.

O cliente é responsável pelos componentes do sistema operacional convidado para cima (incluindo atualizações, patches de segurança e software antivírus). O cliente também é responsável por qualquer outro software aplicativo, bem como pela configuração de grupos de segurança, Nuvens Privadas Virtuais (VPCs) e assim por diante.

Enquanto a AWS gerencia a segurança da nuvem, a segurança na nuvem é de responsabilidade do cliente. Os clientes mantêm o controle de qual segurança eles escolhem implementar para proteger seu próprio conteúdo, plataforma, aplicativos, sistemas e redes, da mesma forma que seria para aplicativos em um data center no local.

Os clientes precisam estar cientes de quaisquer leis e regulamentos aplicáveis com os quais devem cumprir e, em seguida, devem considerar se os serviços que eles consomem na AWS estão em conformidade com essas leis. Em alguns casos, pode ser necessário melhorar na AWS com medidas de segurança adicionais (como implantar um firewall de aplicativo da web, Sistema de detecção de intrusões [IDS] ou Sistema de prevenção de intrusões [IPS] ou usar alguma forma de criptografia para os dados em repouso)

Esse modelo de responsabilidade compartilhada do cliente / AWS não se limita apenas a considerações de segurança, mas também se estende aos controles de TI.

Por exemplo, o gerenciamento, a operação e a verificação dos controles de TI são compartilhados entre a AWS e o cliente.

Antes de migrar para a Nuvem AWS, os clientes eram responsáveis por gerenciar todos os controles de TI em seus ambientes. A AWS gerencia os controles da infra-estrutura física, levando assim a carga pesada indiferenciada dos clientes, permitindo que eles se concentrem no gerenciamento dos controles de TI relevantes. Como cada cliente é implantado de maneira diferente na AWS, os clientes podem mudar o gerenciamento de determinados controles de TI para a AWS.

Essa mudança no gerenciamento dos controles de TI resulta em um novo ambiente de controle distribuído. Os clientes podem usar a documentação de controle e conformidade da AWS disponível para executar seus procedimentos de avaliação e verificação de controle, conforme necessário.

Forte governança de conformidade

Ainda é responsabilidade dos clientes manter uma governança adequada em todo o ambiente de controle de TI, independentemente de como a TI é implantada (seja no local, na nuvem ou parte de um ambiente híbrido). Ao implantar na nuvem da AWS, os clientes têm opções para aplicar diferentes tipos de controles e vários métodos de verificação.

Para alcançar uma forte conformidade e governança, os clientes podem querer seguir esta metodologia básica:

1. Adote uma abordagem holística. Revise as informações disponíveis na AWS, juntamente com todas as outras informações, para entender o máximo possível do ambiente de TI. Após a conclusão, documente todos os requisitos de conformidade.

2. Projete e implemente objetivos de controle para atender aos requisitos de conformidade da organização.

3. Identifique e documente os controles de propriedade de todos os terceiros.

4. Verifique se todos os objetivos de controle foram alcançados e se todos os controles principais foram projetados e operando com eficiência.

Ao usar essa metodologia básica, os clientes podem entender melhor seu ambiente de controle. Por fim, isso simplificará o processo e ajudará a separar as atividades de verificação que precisam ser executadas.

Avaliando e integrando controles da AWS

A AWS fornece aos clientes uma ampla gama de informações sobre seu ambiente de controle de TI por meio de documentos técnicos, relatórios, certificações e outros atestados de terceiros.

Esta documentação ajuda os clientes a entender os controles em vigor relevantes para os serviços em nuvem da AWS que eles usam e como esses controles foram validados. Essas informações também auxiliam os clientes em seus esforços para contabilizar e validar se os controles em seu ambiente de TI estendido estão operando efetivamente.

Tradicionalmente, o design e a eficácia operacional dos controles e objetivos de controle são validados pelos auditores internos e / ou externos por meio de orientações passo a passo do processo e avaliação de evidências.

Observação direta e verificação, pelo cliente ou auditor externo do cliente, geralmente são realizadas para validar os controles. No caso de fornecedores de serviços como a AWS, empresas solicitam e avaliam atestados e certificações de terceiros a fim de obter garantia razoável do design e da eficácia operacional dos controles e objetivos do controle.

Como resultado, embora os principais controles de um cliente possam ser gerenciados pela AWS, o ambiente de controle ainda pode ser uma estrutura unificada na qual todos os controles são contabilizados e verificados como operando efetivamente. Os atestados e certificações de terceiros da AWS não apenas fornecem um nível mais alto de validação do ambiente de controle, mas também pode aliviar os clientes do requisito de realizar determinados trabalhos de validação.

Informações de controle de TI da AWS

A AWS fornece informações de controle de TI aos clientes das duas maneiras a seguir.

Definição de controle específico

Os clientes da AWS podem identificar os principais controles gerenciados pela AWS. Os controles-chave são críticos para o ambiente de controle do cliente e exigem um atestado externo da eficácia operacional desses controles-chave para atender aos requisitos de conformidade (por exemplo, uma auditoria financeira anual). Para esse fim, a AWS publica uma ampla gama de controles de TI específicos em seu relatório Service Organization Controls 1 (SOC 1) Tipo II.

O relatório SOC 1 Tipo II, anteriormente a Declaração sobre Normas de Auditoria (SAS) Nº 70, é um padrão de auditoria amplamente reconhecido desenvolvido pelo Instituto Americano de Contadores Públicos Certificados

(AICPA). A auditoria SOC 1 é uma auditoria aprofundada da eficácia do projeto e da operação dos objetivos de controle definidos e das atividades de controle da AWS (que incluem objetivos de controle e atividades de controle sobre a parte da infraestrutura que a AWS gerencia). "Tipo II" refere-se ao fato de que cada um dos controles descritos no relatório não é apenas avaliados quanto à adequação do projeto, mas também são testados quanto à eficácia operacional pelo auditor externo. Devido à independência e competência do auditor externo da AWS, os controles identificados no relatório devem fornecer aos clientes um alto nível de confiança no ambiente de controle da AWS.

Os controles da AWS podem ser considerados efetivamente projetados e operacionais para vários fins de conformidade, incluindo auditorias às demonstrações financeiras da Seção 404 da Sarbanes-Oxley (SOX). A utilização de relatórios SOC 1 Tipo II também é geralmente permitida por outros organismos de certificação externos. Por exemplo, os auditores da Organização Internacional de

Normalização (ISO) 27001 podem solicitar um relatório SOC 1 Tipo II para concluir suas avaliações para clientes

Conformidade com o padrão de controle geral

Se um cliente da AWS exigir que um amplo conjunto de objetivos de controle seja alcançado, a avaliação das certificações do setor da AWS poderá ser realizada. Com a certificação ISO 27001, a AWS está em conformidade com um padrão de segurança amplo e abrangente e segue as práticas recomendadas para manter um ambiente seguro. Com a certificação DSS (Data Security Standard) do setor de cartões de pagamento (PCI), a AWS cumpre um conjunto de controles importantes para as empresas que lidam com informações de cartão de crédito.

A conformidade da AWS com os padrões da Federal Information Security Management Act (FISMA) significa que a AWS cumpre uma ampla gama de controles específicos exigidos pelas agências governamentais dos EUA. A conformidade da AWS com esses padrões gerais fornece aos clientes informações detalhadas sobre a natureza abrangente dos controles e processos de segurança em vigor na nuvem da AWS.

Regiões globais da AWS

A infraestrutura da nuvem da AWS é construída em torno de regiões e zonas de disponibilidade. Uma região é um local físico no mundo em que temos várias zonas de disponibilidade. As zonas de disponibilidade consistem em um ou mais data centers distintos, cada um com energia, rede e rede redundantes em conectividade, instalado em instalações separadas. Essas zonas de disponibilidade oferecem aos clientes a capacidade de operar aplicativos e bancos de dados de produção mais altamente disponíveis, tolerantes a falhas e escaláveis do que seria possível usando um único data center.

Até o momento em que este artigo foi escrito, a AWS Cloud opera 33 zonas de disponibilidade em 12 regiões geográficas do mundo. As 12 regiões são Leste dos EUA (Virgínia do Norte), Oeste dos EUA (Oregon), Oeste dos EUA (norte da

Califórnia), AWS GovCloud (EUA) (Oregon), UE (Frankfurt), UE (Irlanda), Ásia-Pacífico (Cingapura), Ásia Pacífico (Tóquio), Ásia-Pacífico (Sydney), Ásia-Pacífico (Seul), China (Pequim) e América do Sul (São Paulo).

Programa de conformidade e risco da AWS

O AWS Risk and Compliance foi desenvolvido para aproveitar os programas tradicionais e ajudar os clientes a estabelecer e operar em um ambiente de controle de segurança da AWS.

A AWS fornece informações detalhadas sobre seu programa de risco e conformidade para permitir que os clientes incorporem os controles da AWS em suas estruturas de governança. Essas informações podem ajudar os clientes a documentar estruturas completas de controle e governança nas quais a AWS está incluída como uma parte importante.

As três áreas principais do programa de riscos e conformidade - gerenciamento de riscos, ambiente de controle e segurança da informação - são descritas a seguir.

Gerenciamento de riscos

A AWS desenvolveu um plano estratégico de negócios que inclui a identificação de riscos e a implementação de controles para mitigar ou gerenciar riscos. Uma equipe de gerenciamento da AWS reavalia o plano de risco comercial pelo menos duas vezes por ano.

Como parte desse processo, os membros da equipe de gerenciamento são obrigados a identificar riscos em suas áreas específicas de responsabilidade e implementar controles projetados para tratar e talvez até eliminar esses riscos.

O ambiente de controle da AWS está sujeito a avaliações de risco internas e externas adicionais. As equipes de conformidade e segurança da AWS estabeleceram uma estrutura e políticas de segurança da informação com base na estrutura COBIT (Objetivos de Controle para Tecnologia da Informação e

Tecnologia Relacionada) e integraram efetivamente a estrutura certificável ISO 27001 com base nos controles ISO 27002, nos Princípios dos Serviços de Confiança da AICPA, O PCI DSS v3.1 e as Publicações 800–53 do Instituto Nacional de Padrões e Tecnologia (NIST), Revisão 3, Controles de segurança recomendados para sistemas de informações federais.

A AWS mantém a política de segurança e fornece treinamento de segurança aos seus funcionários. Além disso, a AWS realiza revisões regulares de segurança de aplicativos para avaliar a confidencialidade, integridade e disponibilidade de dados e conformidade com a política de segurança da informação.

A equipe de segurança da AWS verifica regularmente todos os endereços IP de endpoints voltados para o público em busca de vulnerabilidades. É importante entender que essas verificações não incluem instâncias do cliente. A segurança da AWS notifica as partes apropriadas para corrigir quaisquer vulnerabilidades identificadas. Além disso, empresas de segurança independentes realizam regularmente avaliações externas de ameaças de vulnerabilidade.

As descobertas e recomendações resultantes dessas avaliações são categorizadas e entregues à liderança da AWS. Essas verificações são feitas de maneira a garantir a integridade e a viabilidade da infraestrutura subjacente da AWS e não têm como objetivo substituir as verificações de vulnerabilidade do cliente necessárias para atender aos requisitos de conformidade específicos.

Conforme mencionado, os clientes podem solicitar permissão para realizar suas próprias verificações de vulnerabilidade em seus próprios ambientes. Essas verificações de vulnerabilidades não devem violar a política de uso aceitável da AWS e devem ser solicitadas antes da verificação.

Ambiente de controle

A AWS gerencia um ambiente de controle abrangente que consiste em políticas, processos e atividades de controle. Esse ambiente de controle existe para a entrega segura de ofertas de serviços da AWS.

O ambiente de controle coletivo inclui pessoas, processos e tecnologia necessários para estabelecer e manter um ambiente que ofereça suporte à eficácia operacional da estrutura de controle da AWS. A AWS integrou controles específicos aplicáveis à nuvem identificados pelos principais organismos do setor de computação em nuvem na estrutura de controle da AWS.

A AWS continua a monitorar esses grupos do setor em busca de idéias sobre quais práticas líderes podem ser implementadas para ajudar melhor os clientes no gerenciamento de seus ambientes de controle.

O ambiente de controle da AWS começa no nível mais alto da empresa. A liderança executiva e sênior desempenha papéis importantes no estabelecimento do tom e dos valores essenciais da empresa.

Todos os funcionários recebem o código de conduta e ética comercial da empresa e concluem o treinamento periódico. As auditorias de conformidade são realizadas para que os funcionários entendam e sigam as políticas estabelecidas.

A estrutura organizacional da AWS fornece uma estrutura para planejar, executar e controlar operações de negócios. A estrutura organizacional atribui funções e responsabilidades para fornecer pessoal adequado, eficiência das operações e segregação de funções.

A gerência também estabeleceu autoridade e linhas de relatório apropriadas para o pessoal-chave. Como parte dos processos de verificação de contratação da empresa, estão incluídos educação, emprego anterior e, em alguns casos, verificações de antecedentes permitidas por lei para funcionários compatíveis com a posição e o nível de acesso do funcionário às instalações da AWS.

A empresa segue um processo de integração estruturado para familiarizar os novos funcionários com as ferramentas, processos, sistemas, políticas e procedimentos da Amazon.

Segurança da Informação

A AWS usa um programa formal de segurança da informação desenvolvido para proteger a confidencialidade, a integridade e a disponibilidade dos sistemas e dados dos clientes. A AWS publica vários documentos técnicos de segurança disponíveis no site principal da AWS. Estes documentos técnicos são de leitura recomendada.

Conclusão

Normalmente, os sistemas de produção vêm com requisitos definidos ou implícitos em termos de tempo de atividade.