Npo SISTEMAS A RICOH COMPANY | nposecurity

Segurança na Núvem AWS

Do 0 ao Avançado

ÍNDICE

INTRODUÇÃO

A segurança é um ponto essencial na sua jornada para a nuvem, uma das partes que devem ter mais atenção para que você e seus clientes se sintam confiantes com a arquitetura que está sendo utilizada.

A AWS possui um vasto acervo de serviços dedicados tanto para a segurança quanto para a conformidade do seu ambiente, além de interessantes definições de responsabilidades.

Nesse E-book vamos tratar sobre alguns dos principais tópicos de segurança na Nuvem AWS.

ABRAÇANDO A IDEIA DA MIGRAÇÃO

Primeiros passos

Abrace a ideia, entenda os benefícios e não "paralise" com excessos. Comece pequeno, você não precisa de uma equipe com 50 pessoas para inicializar a sua familiarização com a nuvem. Dedique duas ou três pessoas para começar a entender um pouco da console, usar o free tier para ver as possibilidades e comece a ver o real valor de Cloud.

Antes de olharmos para a segurança, ainda na fase de planejamento, é importante se conseguir um patrocinador, pois em todas as mudanças irão ocorrer resistências pelo receio do "novo." A maneira mais rápida de dissipar essa resistência é obter o apoio de um líder sênior disposto a assumir o programa e fornecer uma direção estratégica. Por exemplo, um CIO que irá lidar com os aspectos críticos do negócio, alinhar ações estratégicas, definir metas e ajudar com a negociação entre as partes interessadas.

Ainda na fase de planejamento, é muito importante que se alinhe todas as dúvidas, ideias e o roadmap com o parceiro AWS, tenha sempre em vista que você deve possuir um "Trust Advisor" na sua jornada cloud, não tente seguir sem ajuda, pois esse pode ser um risco muito alto que prejudique seu negócio.

Crie um inventário de todas as suas aplicações, hardwares e ferramentas. Garanta sua política de backup, RTOs e RPOs. Pense em como aproveitar essa janela de migração para transformar o seu negócio, tente modernizar\melhorar aquele sistema monolítico que nunca pode parar para um "update”. Invista em treinamento internos para capacitar sua equipe ou mesmo adquira alguns novos recursos.

Após esse passo, tenha um roteiro, vá aos poucos, planeje o que será migrado primeiro e a partir daí mergulhe no entendimento, estudo e uso das ferramentas e dos frameworks de boas práticas da AWS.

AWS CAF

O AWS CAF identifica recursos organizacionais específicos e fornece orientações de práticas recomendadas que ajudam a melhorar sua preparação para a nuvem. O AWS CAF agrupa seus recursos em seis perspectivas:

A perspectiva de negócios ajuda a garantir que seus investimentos em nuvem acelerem suas ambições de transformação digital e resultados de negócios. As partes interessadas comuns incluem diretor executivo (CEO), diretor financeiro (CFO), diretor de operações (COO), diretor de informações (CIO) e diretor de tecnologia (CTO).

A perspectiva das pessoas serve como uma ponte entre tecnologia e negócios, acelerando a jornada para a nuvem para ajudar as organizações a evoluir mais rapidamente para uma cultura de crescimento contínuo, aprendizado e onde a mudança se torna normal, com foco na cultura, estrutura organizacional, liderança, e força de trabalho. As partes interessadas comuns incluem CIO, COO, CTO, diretor de nuvem e líderes multifuncionais e corporativos.

A perspectiva de governança ajuda você a orquestrar suas iniciativas de nuvem enquanto maximiza os benefícios organizacionais e minimiza os riscos relacionados à transformação. As partes interessadas comuns incluem diretor de transformação, CIO, CTO, CFO, diretor de dados (CDO) e diretor de risco (CRO).

A perspectiva da plataforma ajuda você a criar uma plataforma de nuvem híbrida, escalável e de nível empresarial, modernizar as cargas de trabalho existentes e implementar novas soluções nativas da nuvem. As partes interessadas comuns incluem CTO, líderes de tecnologia, arquitetos e engenheiros.

A perspectiva de segurança ajuda você a alcançar a confidencialidade, integridade e disponibilidade de seus dados e cargas de trabalho na nuvem. As partes interessadas comuns incluem o diretor de segurança da informação (CISO), diretor de conformidade (CCO), líderes de auditoria interna e arquitetos e engenheiros de segurança.

A perspectiva de operações ajuda a garantir que seus serviços de nuvem sejam entregues em um nível que atenda às necessidades de seus negócios. As partes interessadas comuns incluem líderes de infraestrutura e operações, engenheiros de confiabilidade do site e gerentes de serviços de tecnologia da informação.

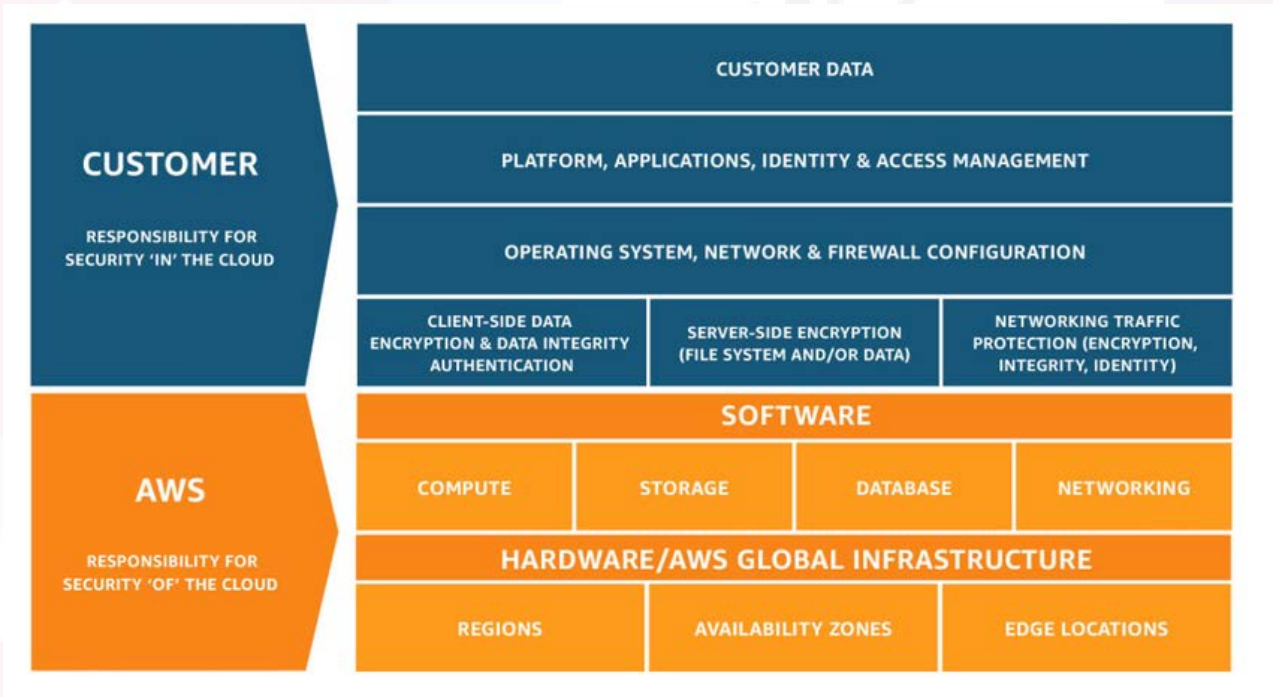
Cada perspectiva compreende um conjunto de recursos que as partes interessadas relacionadas funcionalmente possuem ou gerenciam na jornada de transformação da nuvem. Use o AWS CAF para identificar e priorizar oportunidades de transformação, avaliar e melhorar sua preparação para a nuvem e evoluir iterativamente seu roteiro de transformação.

MODELO DE RESPONSABILIDADE COMPARTILHADA AWS

Muitos clientes acreditam que o fato de usarem AWS em si, os deixa protegido e compliance com as normas de segurança. De fato, ao migrar para nuvem AWS, muitos certificados de seguranças e compliances da AWS são automaticamente atribuídos ao cliente, a segurança DA nuvem é de responsabilidade da AWS e a segurança NA nuvem é de responsabilidade do cliente, basicamente é isto o que o modelo de responsabilidade compartilhada nos explica ao longo de sua documentação.

Em uma breve explicação, a AWS é responsável pela infraestrutura que executa os serviços que ela oferece. Isso vai de hardware, software até refrigeração, energia e etc. Já a responsabilidade do cliente vai depender dos serviços que vai utilizar. Em um serviço IaaS (Infrastructure as a Service) como o EC2 (Elastic Compute Cloud), onde você pode criar suas máquinas virtuais, a AWS oferece a infraestrutura e o cliente cuida do Sistema Operacional e regras de firewall que serão aplicadas à máquina, por exemplo.

É aconselhável estudar também sobre IaaS, PaaS e SaaS.

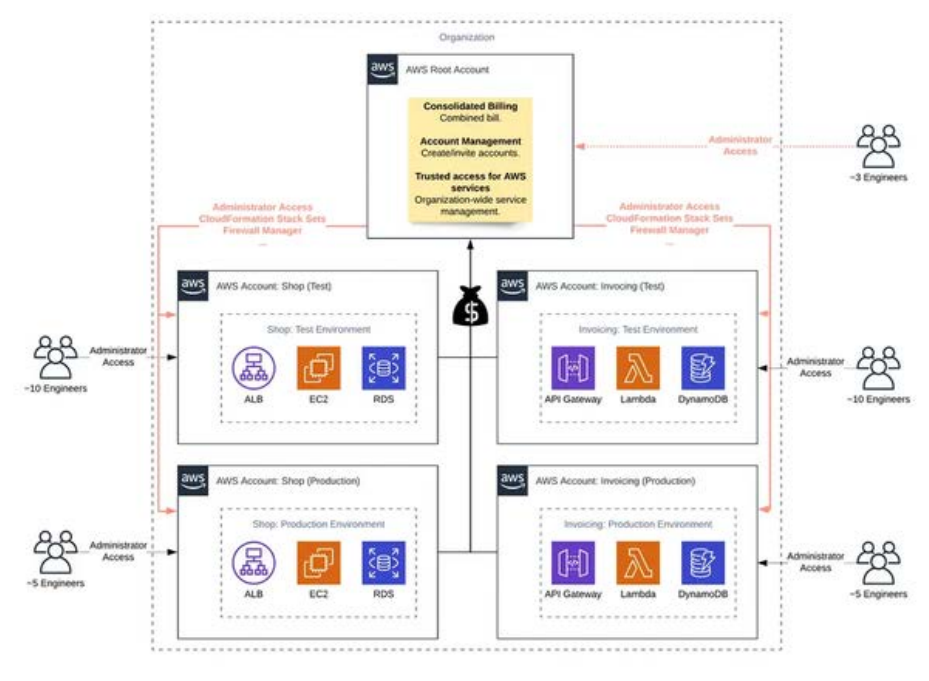


PROCESSO DE CRIAÇÃO DE CONTAS

As contas da AWS servem como o limite fundamental de segurança em nuvem. Elas servem como um contêiner de recursos isolados, essa capacidade de isolar recursos e usuários é um requisito fundamental para estabelecer um ambiente seguro e bem governado. Obviamente a interação entre contas e recursos é algo viável e também utilizado, porém devem seguir delimitações e controles necessários para manter a segurança dos workloads.

Por que necessáriamente preciso de multi contas?

- **Controle de segurança**— Aplicativos diferentes podem ter perfis de segurança diferentes, exigindo diferentes políticas de controles e mecanismos ao seu redor. Por exemplo, é muito mais fácil falar com um auditor e poder apontar para uma única conta da AWS que hospeda todos os elementos da sua carga de trabalho que estão sujeitos a atender o PCI (Payment Card Industry) como padrão de segurança;
- **Isolamento**— Uma Conta da AWS é uma unidade de proteção de segurança. Riscos potenciais e ameaças à segurança devem estar contidos em uma Conta da AWS sem afetar as outras. Pode haver necessidades de segurança diferentes devido a diferentes equipes ou perfis de segurança diferentes.
- **Muitas equipes**— Diferentes equipes têm suas diferentes responsabilidades e necessidades de recursos. Você pode evitar que as equipes interfiram entre si, movendo-as para separar Contas da AWS por times especificos.
- **Isolamento de dados**— Além de isolar as equipes, é importante isolar os armazenamentos de dados em uma conta. Isso pode ajudar a limitar o número de pessoas que podem acessar e gerenciar esse armazenamento de dados. Isso ajuda a conter a exposição a dados altamente privados e, portanto, pode ajudar em conformidade com a LGPD;
- **Processo de negócios**— Unidades de negócios ou produtos diferentes podem ter propósitos e processos completamente diferentes. Com várias Contas da AWS, você pode suportar as necessidades específicas várias unidade de negócios.
- **Faturamento**— Uma conta é a única maneira verdadeira de separar itens em um nível de faturamento. Várias contas ajudam a separar itens em um nível de faturamento em unidades de negócios, equipes funcionais ou usuários individuais. Você ainda pode consolidar todas as suas contas em um único pagador (usando AWS Organizations e o faturamento consolidado) enquanto tem itens de linha separados por Conta da AWS.



Boas práticas

A primeira dica ao criar uma conta AWS é, não utilize o Usuário root para operações do dia a dia. Crie uma senha forte, habilite o MFA, defina uma politica de senha forte para o gerenciamento IAM e em seguida guarde suas informações de acesso em uma cofre de senhas e esqueça que o usuário root existe. Tome suas ações do dia a dia com um usuário IAM e apenas utilize o usuário Root para raros casos em que as operações na AWS apenas sejam permitidas com este usuário.
Lembre-se sempre de definir as informações de contato da sua conta AWS, será através destas informações que será possível uma eventual recuperação em caso de problemas. Além das informações de contato da conta principal você também pode atualizar as seguintes informações de contato:

- Faturamento— O contato de faturamento alternativo receberá notificações relacionadas à cobrança, como notificações de disponibilidade de fatura.
- Operações— O contato de operações alternativas receberá notificações relacionadas às operações.
- Segurança— O contato de segurança alternativo receberá notificações relacionadas à segurança, incluindo notificações doAWSEquipe de abuso.

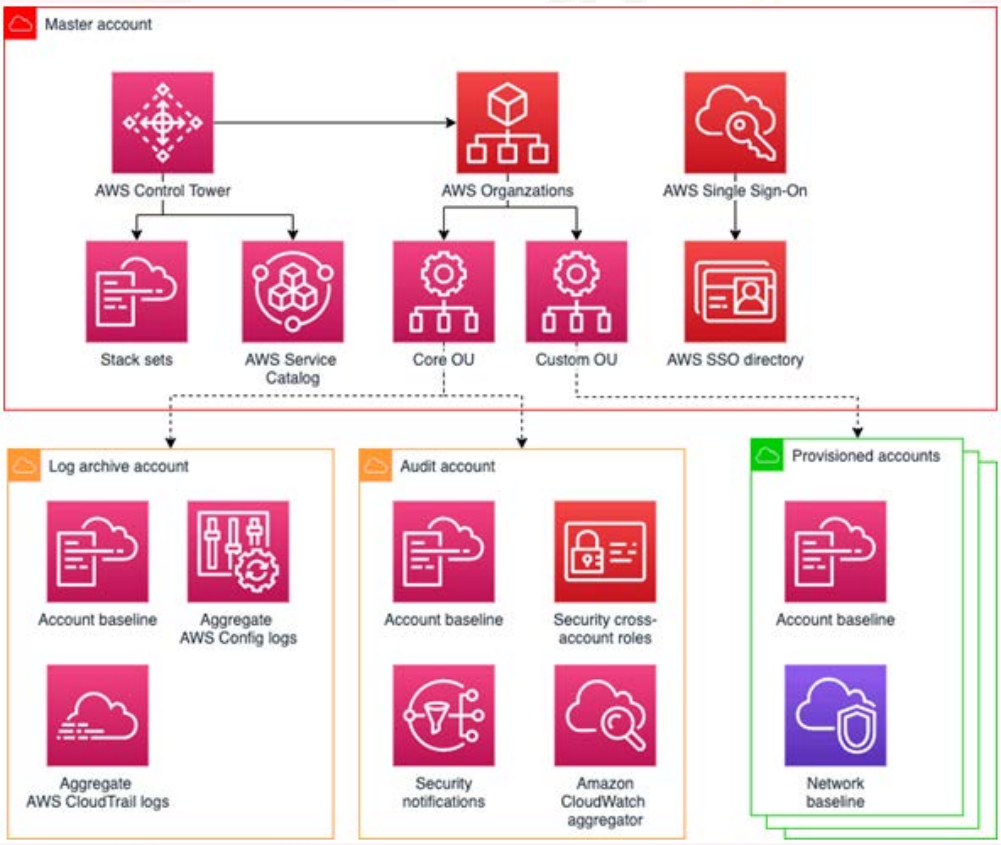
Após concluída a criação da primeira conta AWS (Chamada comumente de Master) podemos utilizar um recurso da AWS chamado de Organization, para criar as próximas contas e a gerenciar contas da AWS como um grupo. A partir do organizations suas contas membros, passaram a ter o billing direcionado para a conta Master, que é a Organization.

Você então terá uma fatura consolidada para todas as contas e poderá compartilhar créditos e benefícios entre as contas membros. Uma outra forma de gerenciar sua organização, de uma maneira ainda mais robusta e segura é com o AWS Control Tower.

AWS Control Tower

O **AWS Control Tower** oferece a maneira mais fácil de configurar e controlar um ambiente seguro com multicontas da AWS. Ele estabelece, cria e configura automaticamente uma série de recursos baseados em esquemas de práticas recomendadas, onde serão aplicadas algumas regras de segurança default e você também pode escolher e habilitar mais regras que já vem prontas e pré-definidas.

Dentre os recursos estabelecido, temos a criação de uma Landing Zone com esquemas de práticas recomendadas que configuram o AWS Organizations para uma estrutura de várias contas, fornecem gerenciamento de identidade usando o AWS SSO Directory, fornecem acesso federado usando o AWS Single Sign-On (AWS SSO), criam um arquivo de log central usando AWS CloudTrail e AWS Config, habilite auditorias de segurança em contas usando AWS SSO, implementa configurações de rede usando Amazon Virtual Private Cloud (Amazon VPC) e defina fluxos de trabalho para contas de provisionamento usando AWS Service Catalog e soluções de Control Tower associadas.



Algumas features:

- Conta log arquive possui um bucket para logs que irá receber todos os logs de cloudtrail e do aws config, de todas as contas que estão abaixo desta organization.
- Conta de auditoria recebe os serviços de segurança, como o aws config.
- Custom OU recebe contas novas provisionadas já com uma baseline de boas praticas de segurança;
- O Control Tower utiliza guardrails (proteções) que são regras pré configuradas para tender questões de boas práticas. São os preventivos e detectivos.e são aplicados a nível de OU.
- Preventivos utiliza o SCP com allow e deny a nivel do organization. Por exemplo, um guardrail preventivo que proibi qualquer usuario de desabilitar o cloudtrail é aplicado a nível de OU.
- Guard Rail detectivo, utiliza o AWS Config para estabelecer regras para monitorar os recursos que estão sendo implementados na sua conta a fim de garantir que as politicas da conta estão sendo atendidas. Por exemplo, nenhum bucket deve ter acesso publico de leitura. Se algum usuario colocar o bucket publico, sera disparado um alarme.

Alguns exemplos de Guardrails:

Objetivo/Catagoria	Exemplo de alarmes
Segurança IAM	Exigir MFA para usuário root
Segurança de dados	Não permitir acesso público de leitura aos buckets do Amazon S3
Segurança de rede	Não permitir conexão com a Internet via RDP (Remote Desktop Protocol)
Logs de auditoria	Habilite o AWS CloudTrail e o AWS Config
Monitoramento	Ative a integração do AWS CloudTrail com o Amazon CloudWatch
Criptografia	Garantir a criptografia de volumes do Amazon EBS anexados às instâncias do Amazon EC2
Drift	Não permitir alterações nas regras de configuração da AWS configuradas pela AWS Control Tower

O Control Tower usa o Account Factory em conjunto com Service Catalog.

Dentre os recursos estabelecidos, temos a criação de uma Landing Zone com esquemas de práticas recomendadas que configuram o AWS Organizations para uma estrutura de várias contas, fornecem gerenciamento de identidade usando o AWS SSO Directory, fornecem acesso federado usando o AWS Single Sign-On (AWS SSO), criam um arquivo de log central usando AWS CloudTrail e AWS Config, habilite auditorias de segurança em contas usando AWS SSO, implementa configurações de rede usando Amazon Virtual Private Cloud (Amazon VPC) e defina fluxos de trabalho para contas de provisionamento usando AWS Service Catalog e soluções de Control Tower associadas.

COMO MANTER SUAS APLICAÇÕES E CONTAS EXTERNAS PROTEGIDAS?

Uma vez com o processo de migração encaminhado, é importante levantar pontos de seguranças como exemplos para que possamos posteriormente pensar em como implementa-los na AWS e quais serviços da AWS irão atender nossa demanda, por exemplo:

Para atender ao gerenciamento de acesso e identidade, utilizamos o IAM sempre considerando a política do menor privilégio, uso forçado de MFA e a utilização de Funções para acesso à recursos. Também valide periodicamente suas políticas e garanta que as permissões são especificas e o menos permissíveis possível. Realize auditorias constantes nas alterações e atividades em sua conta AWS.

Para atender a detecção e prevenção de intrusão, podemos considerar diversas ferramentas, como o Amazon Detective, Amazon Inspector, Guard Duty, Amazon Macie e o Amazon Config para problemas relacionados a configuração de recursos. Porém há uma forma unificada para gerenciar estes alertas e recursos, através do Security Hub. O **AWS Security Hub** é um serviço de gerenciamento de postura de segurança na nuvem que realiza verificações de práticas recomendadas de segurança contínuas e automatizadas em relação aos seus recursos da AWS. O Security Hub agrega seus alertas de segurança (ou seja, descobertas) de vários serviços da AWS e produtos de parceiros em um formato padronizado para que você possa agir com mais facilidade. O Security Hub simplifica como você entende e melhora sua postura de segurança com verificações automatizadas de práticas recomendadas de segurança baseadas em regras do AWS Config e integrações automatizadas com dezenas de serviços da AWS e produtos de parceiros.

Você também pode gerenciar os serviços listados acima de forma individual, onde cada um cumpri um papel específico na proteção de seus recursos na AWS. Além dos serviços acima, existem outros serviços para manter a segurança da sua organização no que diz respeito a Proteção de Dados, Respostas a Incidentes e segurança da sua infraestrutura em geral:

Amazon Detective

Coleta automaticamente dados de log de seus recursos da AWS e usa machine learning, análise estatística e teoria dos gráficos para criar um conjunto de dados vinculados que permite realizar facilmente investigações de segurança mais rápidas e eficientes. Você pode agregar logs de vários serviços parceiros e da propria AWS e o Amazon Detective cuida de todo processo para identificar a causa raiz do problema, sem que você precise cruzar diversas informações e perder tempo realizando a investigação;

Amazon GuardDuty

O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos anômalos para proteger suas contas da AWS, workloads e dados armazenados no Amazon Simple Storage Service (Amazon S3).O GuardDuty é capaz de analisar dezenas de bilhões de eventos em várias fontes de dados da AWS, como logs de eventos do AWS CloudTrail, logs de fluxo da Amazon Virtual Private Cloud (VPC) e logs de consulta de DNS;

Amazon Inspector

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidade automatizado que verifica continuamente o Amazon Elastic Compute Cloud (EC2) e workloads de contêiner em busca de vulnerabilidades de software e exposição não intencional da rede;

Amazon Macie

O Amazon Macie avalia continuamente o seu ambiente do Amazon S3 e fornece um resumo dos recursos do S3 em todas as suas contas. Para todos os buckets não criptografados, acessíveis ao público ou compartilhados com as contas da AWS fora daquelas que você definiu no AWS Organizations, você pode ser alertado para tomar uma ação;

Amazon Config

O AWS Config é um serviço que permite acessar, auditar e avaliar as configurações dos recursos da AWS. O Config monitora e grava continuamente registros das configurações de recursos da AWS e lhe permite automatizar a avaliação das configurações registradas com base nas configurações desejadas;

Amazon CloudTrail

AWS CloudTrail é um serviço AWS que lhe permite administrar, manter-se compatível e realizar auditorias operacionais e de risco na sua conta AWS. As ações realizadas por um usuário, uma função ou um serviço da AWS são registradas como eventos no CloudTrail. Os eventos incluem ações realizadas em AWS Management Console, AWS Command Line Interface, e AWS SDKs e APIs;

Amazon KMS

O AWS Key Management Service (KMS) facilita a criação e o gerenciamento de chaves criptográficas e o controle do seu uso em uma ampla variedade de serviços da AWS e nas suas aplicações;

Flows Logs

O Flow Log é um recurso que permite capturar informações sobre o tráfego IP que vai de e para as interfaces de rede em sua VPC. Os dados dos logs de fluxo podem ser publicados no Amazon CloudWatch Logs ou no Amazon S3.

Demais serviços

Além dessas features, podemos considerar o uso do **AWS WAF** (Web Application Firewall) para proteger suas aplicações Web ou APIs contra bots e exploits comuns na Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos em excesso.

O uso do AWS Waf é recomendado em conjunto com o AWS Shield, um serviço gerenciado de proteção contra DDoS. O AWS Shield tem dois níveis, Standard e Advanced, onde por padrão todos os clientes da AWS se beneficiam gratuitamente com as proteções automáticas do AWS Shield Standard. O AWS Shield Standard protege contra os ataques de DDoS mais comuns, que ocorrem com frequência nas camadas de rede e transporte e visam sites ou aplicativos web.

Podemos também citar o uso do **AWS Backup** para centralizar e automatizar a proteção de dados em serviços da AWS e workloads híbridas. Ele oferece um serviço econômico, totalmente gerenciado e baseado em políticas que simplifica ainda mais a proteção de dados em grande escala.

O serviço também ajuda a garantir a conformidade regulatória ou as políticas de negócios para a proteção de dados. Com o AWS Organizations, o AWS Backup permite implantar políticas de proteção de dados de forma centralizada para configurar, gerenciar e controlar a atividade de backup em contas e recursos da AWS da sua organização, incluindo instâncias do Amazon Elastic Compute Cloud (Amazon EC2), volumes do Amazon Elastic Block Store (Amazon EBS), buckets do Amazon Simple Storage Service (Amazon S3), bancos de dados do Amazon Relational Database Service (Amazon RDS) (incluindo clusters do Amazon Aurora), tabelas do Amazon DynamoDB, bancos de dados do Amazon Neptune, bancos de dados do Amazon DocumentDB (compatível com MongoDB), sistemas de arquivos do Amazon Elastic File System (Amazon EFS), sistemas de arquivos do Amazon FSx for Lustre, sistemas de arquivos do Amazon FSx for Windows File Server e volumes do AWS Storage Gateway, além de workloads on-premises da VMware no VMware CloudTM on AWS.

Mesmo com todos esses recursos implantados e monitorados, é de suma importância que as contas com workload criticos possuam replicação para outras regiões AWS. Uma grande ferramenta para essa situação é o **Cloud Endure.**

Também existem diversas outras práticas como não expor acessos através da internet e utilizar sempre que possível o Systems Manager para gerenciar máquinas atavés da console, ou acessar instancias diretamente via Cloud Shell.

Por fim e não menos importante, utilize periodicamente o **AWS Well-Architected Tool** para revisar suas cargas de trabalho em relação às práticas recomendadas atuais da AWS e obter conselhos sobre como arquitetar suas cargas de trabalho para a nuvem.

Esta ferramenta faz parte do O AWS Well-Architected Framework e permite que você analise suas arquiteturas usando uma abordagem consistente e fornece orientações para melhorar projetos ao longo do tempo.

Os princípios gerais de design e as práticas recomendadas e orientações específicas da AWS estão organizadas em seis áreas conceituais. Essas áreas conceituais são os pilares do **AWS Well-Architected Framework**. Os seis pilares são: excelência operacional, segurança, confiabilidade, eficiência de performance, otimização de custos e sustentabilidade.

Conheça mais sobre a NPO Sistemas

As soluções da NPO são do tamanho da sua necessidade

Migrar o seu negócio para nuvem? Entender sobre como será essa jornada? Gerir ambientes 100% hospedados na nuvem? Ou em ambientes híbridos "on premise" com parte da sua "data-estrutura" local integrada à nuvem?

O céu é o limite!

QUER CONVERSAR COM O NOSSO TIME?

latam.sales@nposervices.com

REFERÊNCIAS

An Overview of the AWS Cloud Adoption Framework

Modelo de responsabilidade compartilhada

Pilar Segurança – AWS Well-Architected Framework

Segurança, identidade e conformidade na AWS

Práticas recomendadas para a conta de gerenciamento

Práticas recomendadas para contas membro

Amazon Detective

Amazon GuardDuty

Amazon Inspector

Amazon Macie

Amazon Config

Amazon CloudTrail

Amazon KMS

VPC Flow Logs

AWS Backup

AWS Well Architected

AWS WAF

Cloud Endure AWS