zappts

Treinamento AWS Cloud Practitioner - Domínio 2: Segurança e conformidade

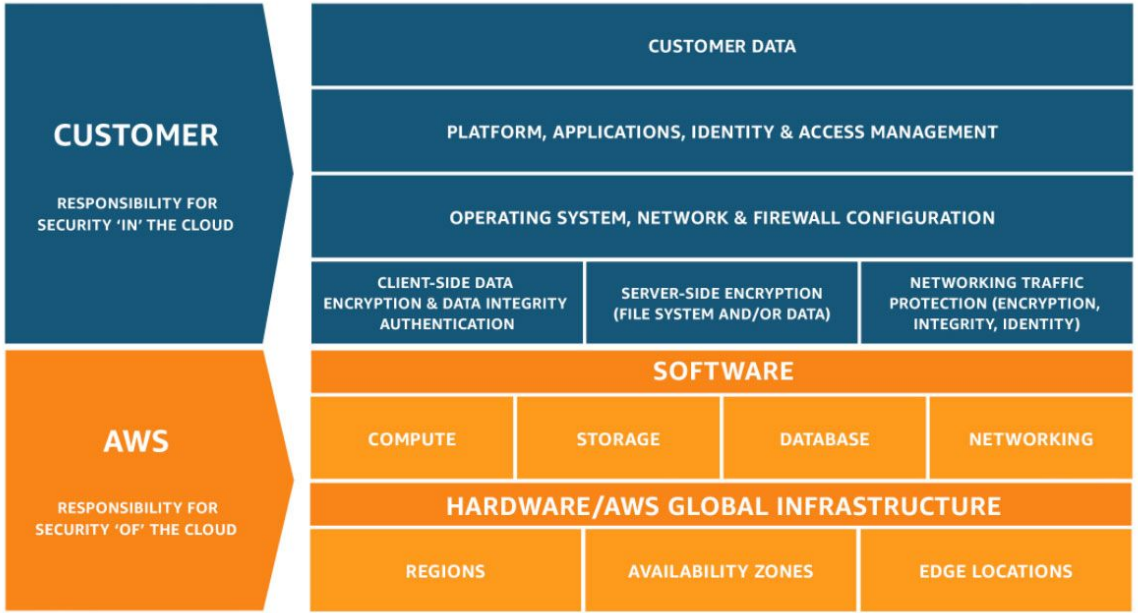
Agenda!

- Definição do modelo de responsabilidade compartilhada da AWS
- Definição dos conceitos de segurança e conformidade da nuvem AWS
- Identificação dos recursos de gerenciamento da AWS
- Identificação de recurso para suporte de segurança

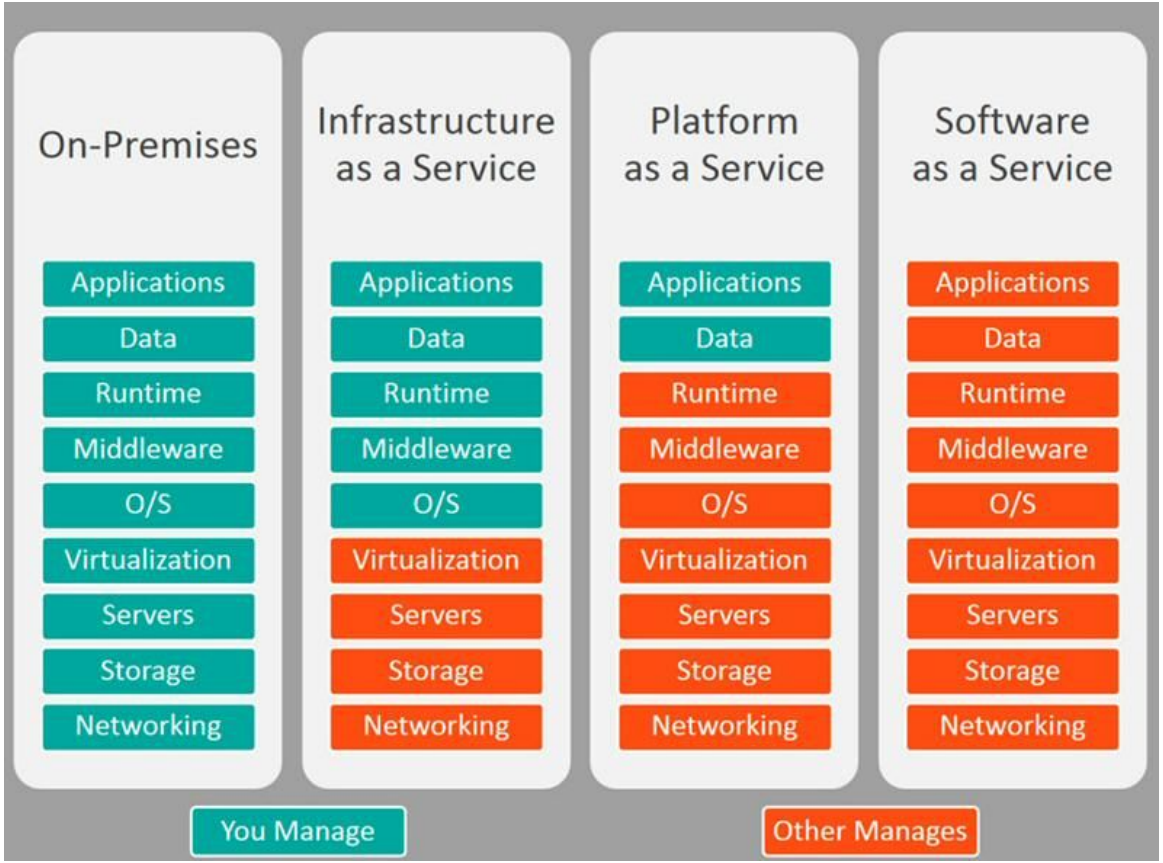
Definição modelo de responsabilidade compartilhada da AWS

Shared Responsibility Model

- AWS -> Segurança “da” nuvem (of the cloud)
- Cliente -> Segurança “na” nuvem (in the cloud)



Shared Responsibility Model



Shared Responsibility Model

Shared Responsibility Model

- As responsabilidades mudam de acordo com o serviço.
- EC2 -> Responsável por todas as configurações, manutenção, patches
- RDS -> Escolher o tamanho da máquina do banco, responsável por aumentar a máquina se necessário, quando o banco fica online ou não
- Aurora Serverless -> Você não se preocupa com infra e o tempo de utilização do banco é gerenciado por você

Responsabilidades da AWS

- Proteger a infraestrutura que executa todos os serviços da AWS
- Hardware, software, rede, instalações
- Saiba mais: https://aws.amazon.com/pt/compliance/shared-responsibility-model/

Conceitos de segurança e conformidade da nuvem AWS

O que é conformidade

- Compliance
- Estar de acordo com padrões de segurança do mercado
- https://aws.amazon.com/pt/compliance/

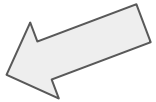
Padrões reconhecidos

- HIPAA/HITECH - https://aws.amazon.com/pt/compliance/hipaa-compliance/
- SOC - https://aws.amazon.com/pt/compliance/soc-faqs/
- PCI/DSS - https://aws.amazon.com/pt/compliance/pci-dss-level-1-faqs/
- LGPD - https://aws.amazon.com/pt/compliance/brazil-data-privacy/
- Serviços cobertos - https://aws.amazon.com/pt/compliance/services-in-scope/

Criptografia na AWS

- Opções de criptografia variam de acordo com cada serviço
- At rest, in transit
- Amazon KMS
  - https://aws.amazon.com/pt/kms/features/
- Cliente pode gerenciar as próprias chaves ou AWS se responsabiliza por elas

Auditoria e Relatórios



Muita atenção na diferença destes tipos de eventos!

- CloudTrail
  - Data Event e Management Events
  - https://aws.amazon.com/pt/cloudtrail/features/

- CloudWatch
  - Realização de coleta de logs e métricas
  - Métricas incorporadas e personalizadas
  - Visualização de métricas, criação de dashboards
  - Criação de alarmes
  - https://aws.amazon.com/pt/cloudwatch/features/

- AWS Config
  - Histórico de configurações
  - Detecção na mudança de configurações - https://aws.amazon.com/pt/config/features/

Identificação dos recursos de gerenciamento de acesso a AWS

Finalidade do gerenciamento de usuários

- Least Privilege Principle -> Regra dos menores privilégios
- Controle e auditoria
- IAM -> https://aws.amazon.com/pt/iam/features/

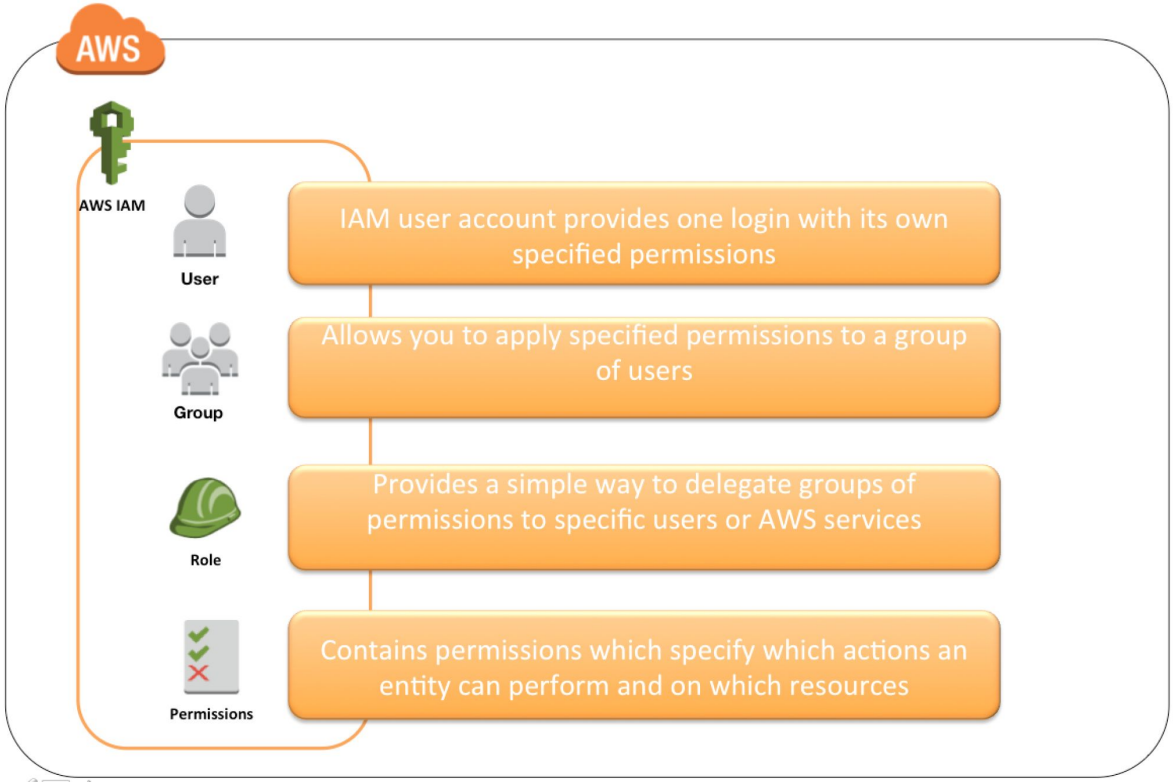
Funcionalidades do IAM

- Credenciais com senha para fazer login no console AWS
- Chaves de gerenciamento para fazer chamadas por meio da API AWS (AWS CLI, AWS SDK)
- Gerenciamento da complexidade / alternância de senha
- Controle de autenticação MFA

Alerta!

User, groups e roles

AWS IAM Identities



Conta Raiz da AWS

- Não deve ser utilizada para tarefas diárias / administrativas
- Boa prática usar MFA na conta raiz
- Utilizar conta raiz apenas em casos que se faz necessário: https://docs.aws.amazon.com/general/latest/gr/root-vs-iam.html#aws_tasks-that-require-root
- Melhor prática: criar um usuário IAM e fazer qualquer outra tarefa com este usuário

Identificação de Recursos para Suporte de Segurança

Segurança da rede

- Amazon WAF
  - https://aws.amazon.com/pt/waf/
- Network Access List
- Security Groups
- AWS Marketplace (para soluções de terceiros / parceiros)

Trusted Advisor

- Serviço que faz recomendações para seguir as melhores práticas da AWS
- Um dos pilares do serviço é **segurança**
- Verificações básicas de segurança fazem parte do Trusted Advisor

Exemplo de questões

Questão 1

What is a document that provides a formal statement of one or more permissions?

- ❑ Role
- ❑ Policy
- ❑ Permission
- ❑ Resource

Questão 1

What is a document that provides a formal statement of one or more permissions?

- ❑ Role
- ❑ Policy
- ❑ Permission
- ❑ Resource

Questão 2

Which of the following can be used as an additional layer of security to using a username and password when logging into AWS Console?

- ❑ Secondary Password
- ❑ Multi-Factor Authentication
- ❑ Secondary username
- ❑ Root access privileges

Questão 2

Which of the following can be used as an additional layer of security to using a username and password when logging into AWS Console?

- ❑ Secondary Password
- ❑ Multi-Factor Authentication
- ❑ Secondary username
- ❑ Root access privileges

Dúvidas?

OBRIGADO!

zappts

Conheça mais sobre a Zappts em

www.zappts.com