Semana 2 – Planejamento

- Conceitos importantes para revisar (15 min)

- Prática Parte 1: Lab (simulearn) para demonstração dos conceitos (15 min)

- Prática Parte 2: DIY -> Todos farão um lab (simulearn) para ver como funciona (10 min)

- Resolução de exercícios com conceitos chave (10 min)

- Dúvidas podem ser levantadas a qualquer momento

Semana 2 – Ponto de partida

Declaração de tarefa 1.1: Projetar acesso seguro aos recursos da AWS.

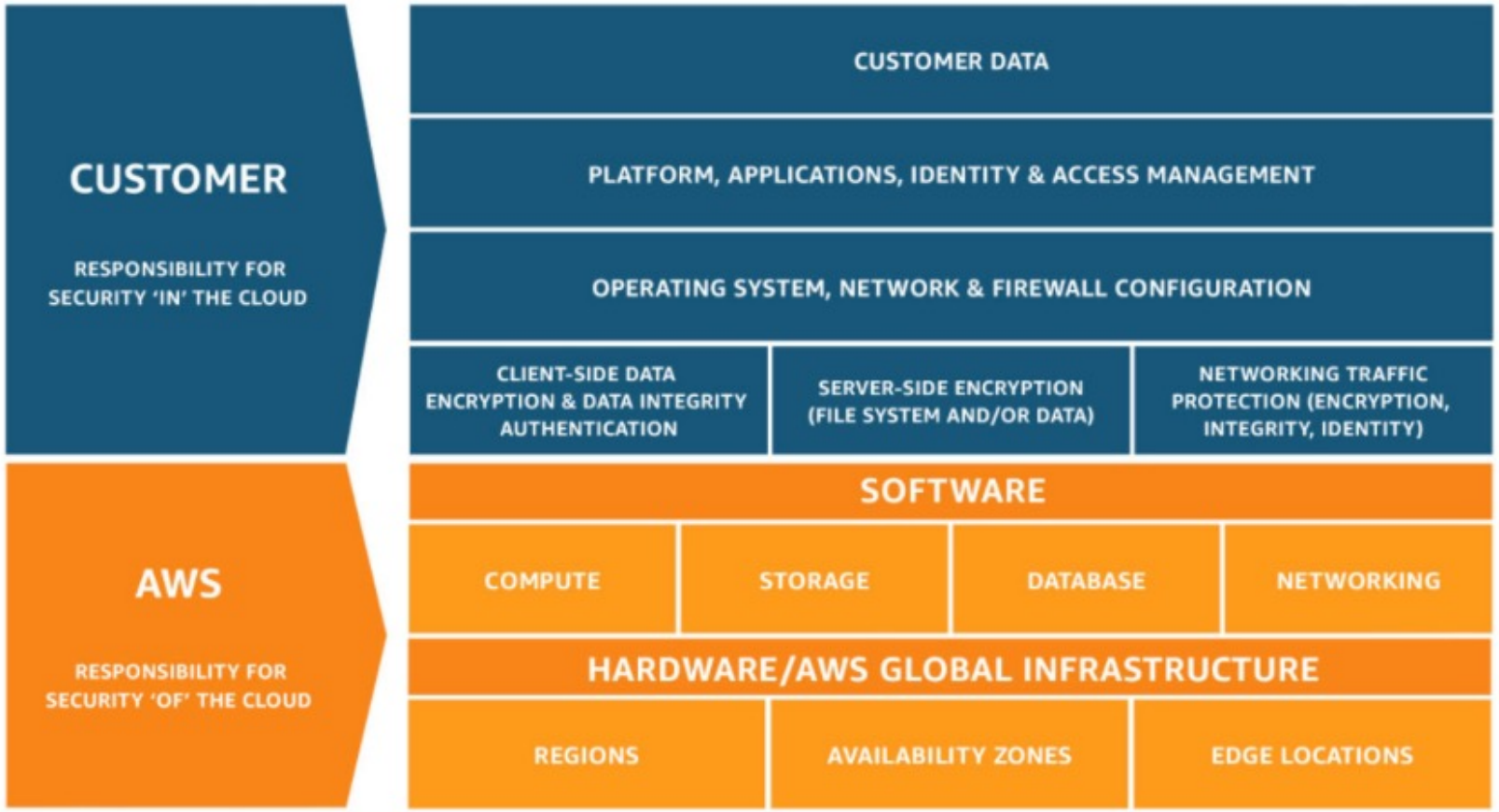
Conhecimento sobre:

- Controles de acesso e gerenciamento em várias contas.
- Serviços de identidade e acesso federado da AWS (por exemplo, AWS Identity and Access Management [IAM], AWS Identity Center [AWS Single Sign-On]).
- Infraestrutura global da AWS (por exemplo, Zonas de Disponibilidade, Regiões AWS).
- Práticas recomendadas de segurança da AWS (por exemplo, o princípio de menor privilégio).
- O modelo de responsabilidade compartilhada da AWS.

Habilidades em:

- Aplicar as práticas recomendadas de segurança da AWS a usuários do IAM e usuários-raiz (por exemplo, autenticação com multifator [MFA]).
- Projetar um modelo de autorização flexível que inclua usuários, grupos, funções e políticas do IAM.
- Projetar uma estratégia de controle de acesso baseada em função (por exemplo, AWS Security Token Service [AWS STS], mudança de função, acesso entre contas).
- Projetar uma estratégia de segurança para várias contas da AWS (por exemplo, AWS Control Tower, políticas de controle de serviço [SCPs]).
- Determinar o uso apropriado de políticas de recursos para os serviços da AWS.
- Determinar quando federar um serviço de diretório com funções do IAM.

Modelo de responsabilidade compartilhada da AWS



Modelo de responsabilidade compartilhada da AWS

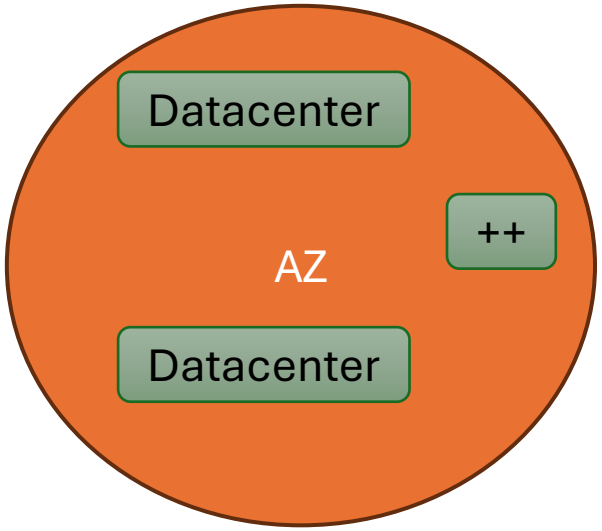
- Dica legal (referência CloudGuru): Quando estamos diante de uma pergunta se a responsabilidade é do cliente ou da AWS, vamos nos perguntar, consigo fazer tal ação no Console da AWS? Se a resposta for sim, provavelmente a responsabilidade é nossa. Exemplo, não podemos interferir no cabeamento dos datacenters, atualizar o sistema operacional do RDS, gerenciar os data centers etc.

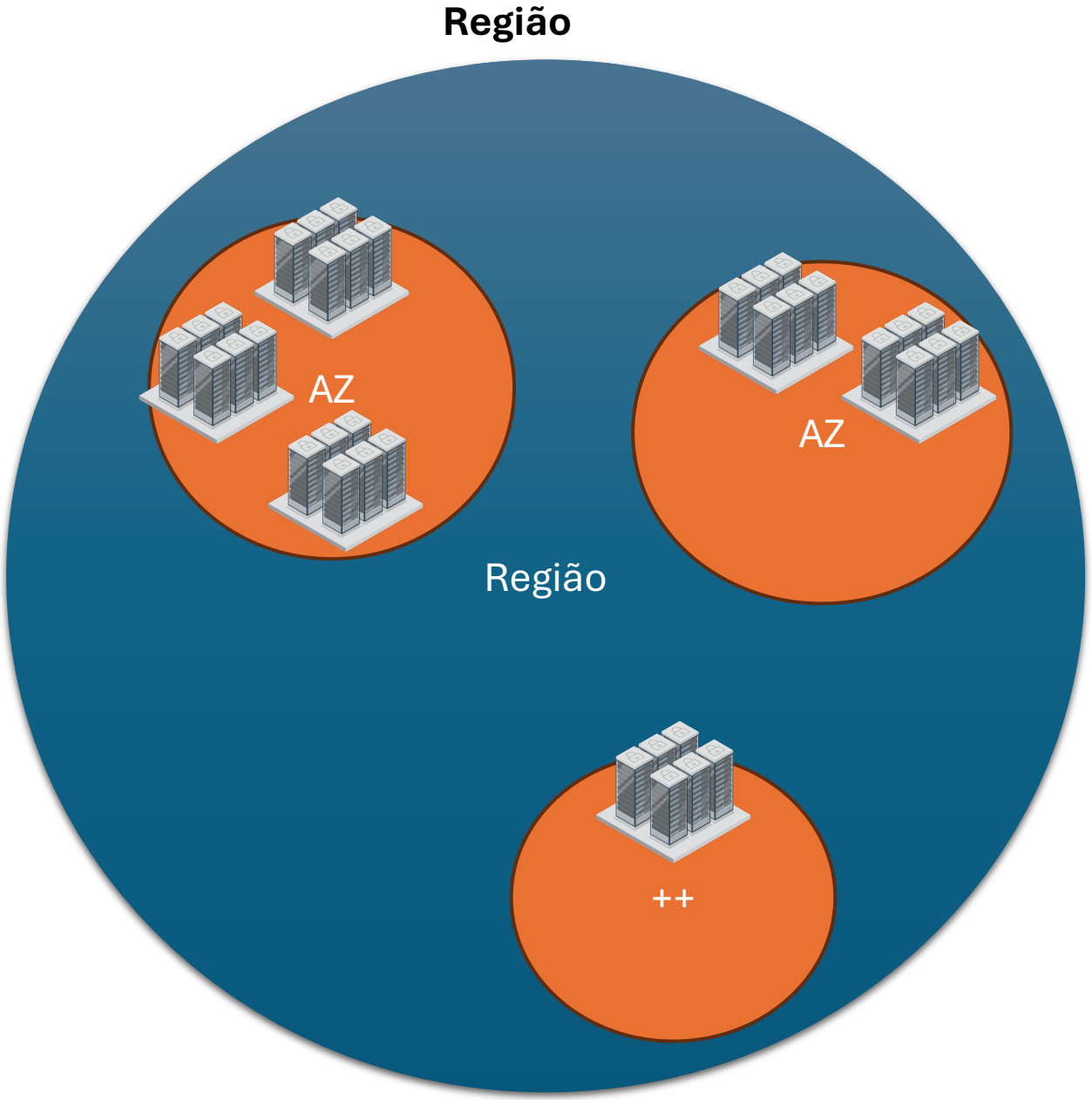
Infraestrutura Global da AWS

- 33 regiões lançadas
- 105 zonas de disponibilidade
- 600 + CloudFront Points of Presence
- https://aws.amazon.com/about-aws/global-infrastructure/

Infraestrutura Global da AWS

AZ: Availability Zone ->
Zona de Disponibilidade é representada pelo nome da região + símbolo alfanumérico. Ex.: us-east-1a





IAM é um serviço Global -> não está associado a uma região específica

Quando criamos um novo User, ele vem sem permissões

Access key ID e secret access keys (acesso programático) DIFERENTES DE username e password (console)

IAM: Identity Access Management

Aqui duas questões centrais estão em jogo, isto é, (a) quem é você? e (b) você é realmente quem diz ser? Palavra chave aqui é Identidade.

Acesso a recursos entre contas no IAM:
https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/access_policies-cross-account-resource-access.html

Quando criamos um novo User, ele vem sem permissões

Access key ID e secret access keys (acesso programático) DIFERENTES DE username e password (console)

IAM: Identity Access Management

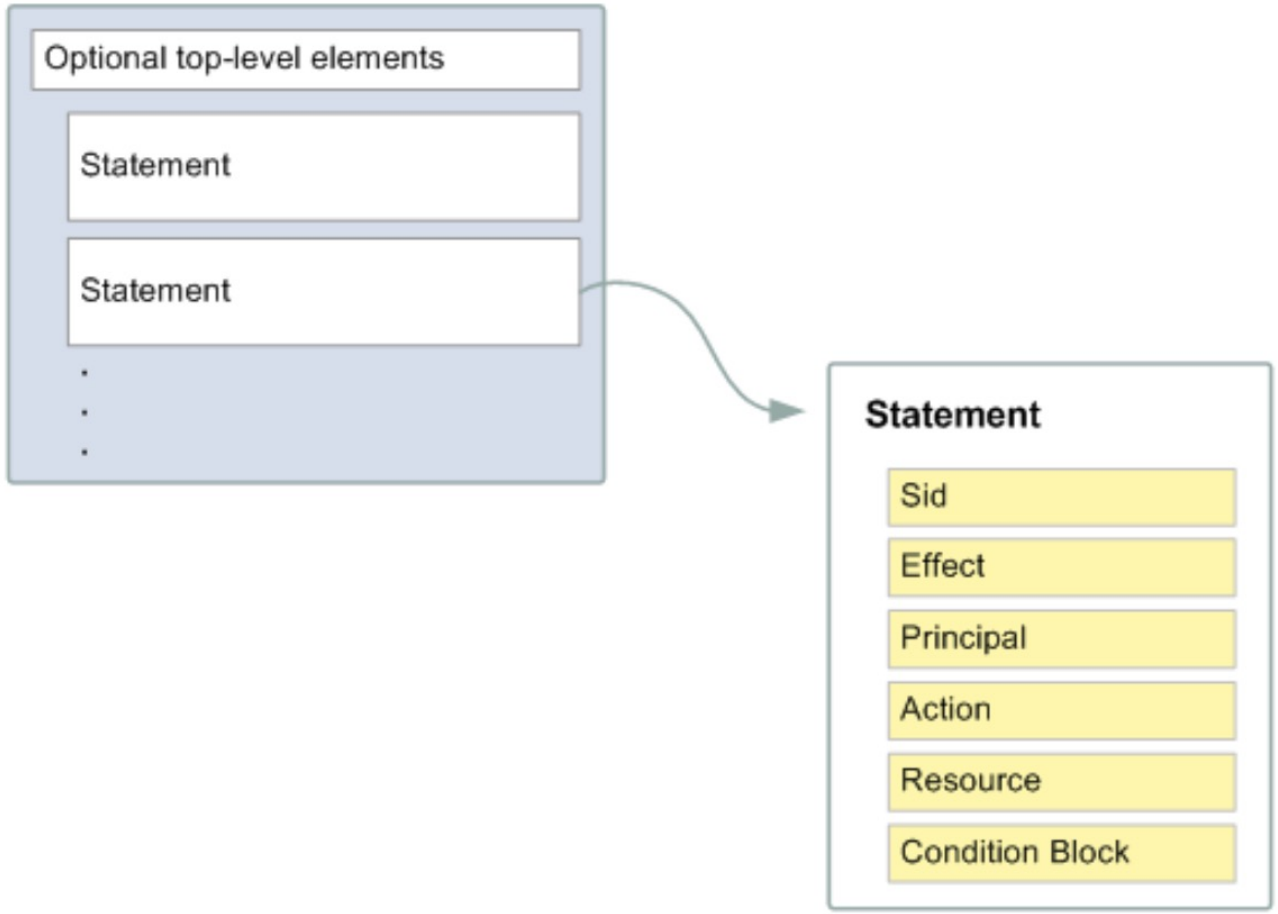
IAM: Identity Access Management
Policy Documents:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

- Estrututura básica de uma **política**: efeito, ação e recurso (mais itens no próximo slide)
- Uma política pode ser do tipo identity based, resource based entre outros

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

IAM: Identity Access Management

- Estrututura básica de uma **política**



IAM: Identity Access Management
Policy Documents:

Identity based:

Permissões de User ou Role (role pode ser resource based)

Resource based: associado a um recurso -> quem pode acessar e quais ações

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::exemplo-bucket/*",
                "arn:aws:s3:::exemplo-bucket"
            ]
        }
    ]
}
```

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExemploDeclaracao",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/ExemploUsuario"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::exemplo-bucket/*"
        }
    ]
}
```

Doc: https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/access_policies_identity-vs-resource.html

IAM: Identity Access Management
Policy Documents

- Algum principal com essa política, conseguirá listar objetos de um bucket S3 (Simple Storage Service)

a) Outro exemplo de política baseada em recurso
b) Por que é importante falarmos disso? Próximo slide

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "1",
    "Effect": "Allow",
    "Principal": {"AWS": ["arn:aws:iam::account-id:root"]},
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::mybucket",
      "arn:aws:s3:::mybucket/*"
    ]
  }]
}
```

E quando temos diversas políticas para um mesmo recurso, como a AWS vai escolher o resultado final?

https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

DENY explícito sempre prevalece sobre o ALLOW

SCP é uma forma organizacional (mais macro) de gerenciar permissões

Por padrão, os serviços vem com uma política de DENY implícito

IAM: Identity Access Management
Policy Documents:

> **Importante**
>
> Essa lógica só se aplica quando a solicitação é feita em uma única Conta da AWS. Para solicitações feitas de uma conta para outra, o solicitante em `Account A` deve ter uma política baseada em identidade que permita fazer uma solicitação para o recurso em `Account B`. Além disso, a política baseada em recurso no `Account B` deve permitir o solicitante em `Account A` para acessar o recurso. Deve haver políticas em ambas as contas que permitam a operação, caso contrário, a solicitação falhará. Para obter mais informações sobre políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM.

Destaque aqui para “Essa lógica só se aplica quando a solicitação é feita em uma única Conta da AWS”.

Referência: https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/access_policies_identity-vs-resource.html

IAM: Identity Access Management
Policy Documents:

- Política baseada em identidade

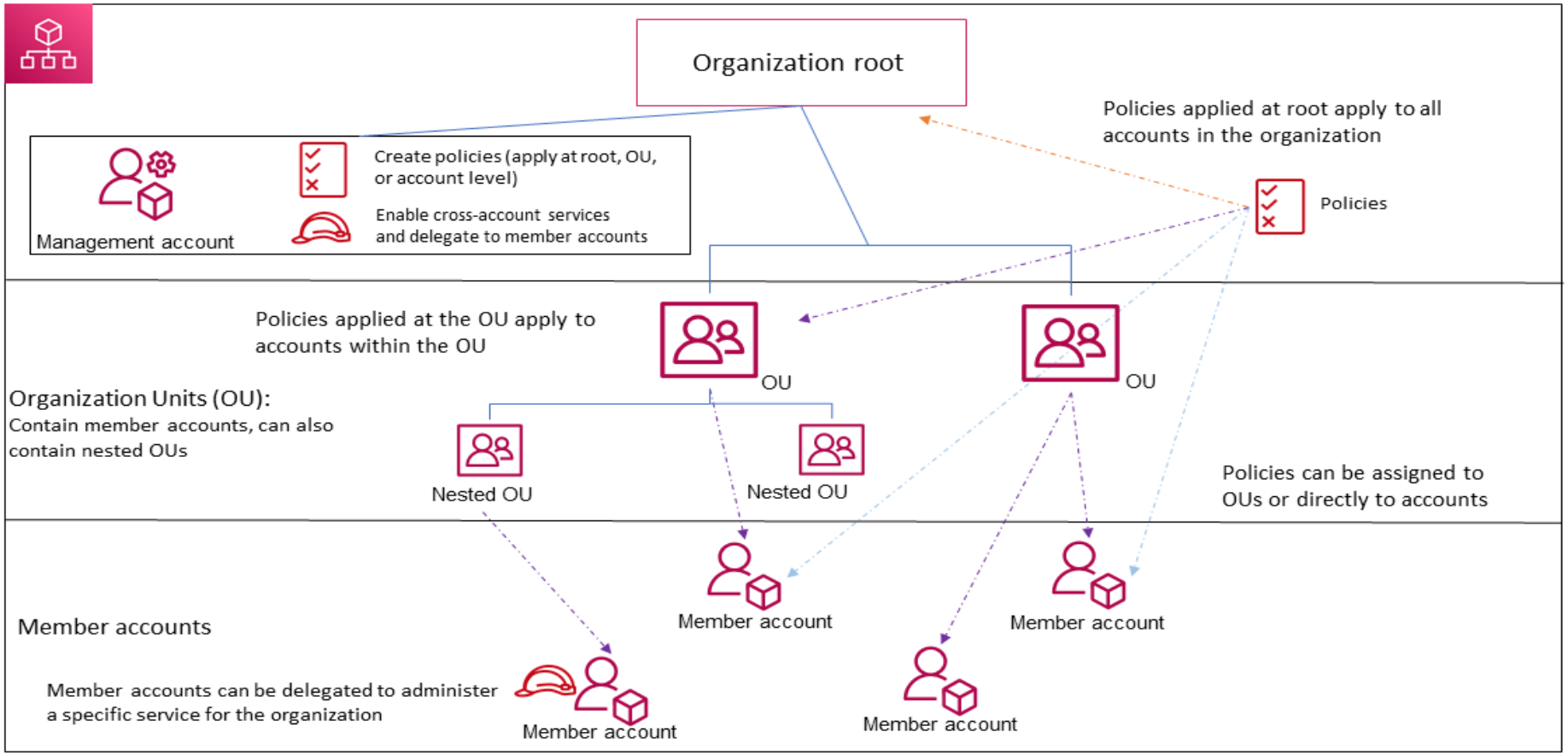
Conta A

Conta B

- Política baseada em recurso

Ambientes com múltiplas contas

AWS Organizations



Agrega vários serviços da AWS de gerenciamento de múltiplas contas (service catalog, aws organizations, aws iam etc)

AWS Control Tower

Quando criamos uma landing zone, a criação de uma conta de logs e outra de auditoria é automática (presentes na security OU)

Service Control Policy
(Políticas de controle de serviço)

Doc AWS.: “As políticas de controle de serviço (SCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões na sua organização. Os SCPs oferecem controle central sobre o máximo de permissões disponíveis para os usuários e funções do IAM na sua organização. As SCPs ajudam você a garantir que as suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização. ”

Importante

SCPs não afetam usuários ou funções na conta de gerenciamento. Elas afetam apenas as contas-membro de sua organização.

Service Control Policy (Políticas de controle de serviço)

Exemplo do elemento NotAction

O exemplo a seguir mostra como você pode usar um `NotAction` elemento para excluir AWS serviços do efeito da política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
      }
    }
  ]
}
```

Com essa declaração, as contas afetadas estão limitadas a realizar ações no especificado Região da AWS, exceto ao usar ações do IAM.

STS

Palavras-chave: credenciais temporárias, controle de acesso por tempo determinado aos recursos da AWS

Determinar quando federar um serviço de diretório com funções do IAM

Aqui estamos dizendo que vamos confiar em outra fonte de identificação (outro sistema de identidade)

Determinar quando federar um serviço de diretório com funções do IAM

AWS Managed Microsoft AD	Integração completa com aplicativos e serviços do Active Directory, ideal para grandes empresas.	Baseado em instâncias usadas, custos de armazenamento, e transferências de dados.	Totalmente compatível com serviços AD, integração com VPC, EC2, RDS.	Alta disponibilidade com várias Zonas de Disponibilidade, suporta confiança com AD on-premises.
AD Connector	Autenticação de usuários e autorização usando AD on-premises, sem necessidade de sincronização.	Paga-se por hora de uso, dependendo do número de conectores e domínios.	Integração com serviços que suportam IAM, como EC2, S3, RDS.	Funciona como um proxy, não armazena dados de diretório na AWS.
Simple AD	Diretório leve e gerenciado para pequenas e médias empresas, funcionalidades básicas de AD.	Preço baseado no tamanho do diretório (pequeno ou grande).	Compatível com EC2, RDS, Workspaces, e outras integrações básicas de AD.	Baseado em Samba 4, suporta funcionalidades básicas como grupos, usuários e GPOs.

Prática – Hands-on Labs

- LAB 1: https://explore.skillbuilder.aws/learn/course/20119/play/132191/start-aws-simulearn

- LAB 2: https://explore.skillbuilder.aws/learn/course/20135/play/132239/start-aws-simulearn;lp=2227

- https://explore.skillbuilder.aws/learn/learning_plan/view/2227/aws-simulearn-solutions-architect

Exercícios

Questão 1:

Qual das seguintes abordagens é mais apropriada para gerenciar o acesso a recursos em várias contas AWS em uma grande organização?

A) Configurar múltiplos usuários do IAM em cada conta individualmente sem nenhuma coordenação entre as contas.

B) Utilizar AWS Organizations para consolidar contas e aplicar políticas de controle de serviço (SCPs) para gerenciar permissões de maneira centralizada.

C) Criar uma política de bucket no Amazon S3 para cada recurso separado.

D) Utilizar grupos de segurança do EC2 para gerenciar o acesso a todas as contas.

Questão 2:

Qual serviço da AWS é mais adequado para oferecer uma experiência de login centralizada, permitindo que os usuários acessem várias contas AWS e aplicações empresariais com um único conjunto de credenciais?

A) Amazon Redshift

B) AWS Identity Center (AWS Single Sign-On), que integra com diretórios corporativos como Microsoft Active Directory e provedores SAML 2.0.

C) Amazon Cognito, que permite autenticação para aplicações móveis e web usando provedores de identidade social.

D) AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)

Questão 3:

Ao projetar uma estratégia de segurança para várias contas da AWS, qual combinação de serviços e práticas recomendadas pode oferecer o controle mais robusto e centralizado?

A) Utilizar apenas uma conta AWS e criar usuários do IAM para cada departamento da organização.

B) Implementar AWS Control Tower para configurar e governar um ambiente de várias contas, juntamente com SCPs para impor regras de segurança e conformidade.

C) Usar apenas grupos de segurança do EC2 para controlar o acesso.

D) Configurar permissões no nível do bucket S3 para cada usuário individualmente.

Questão 4:

Quais são as práticas recomendadas de segurança que devem ser aplicadas aos usuários do IAM e usuários-raiz na AWS para garantir a máxima proteção dos recursos?

A) Habilitar autenticação multifator (MFA) para todos os usuários, limitar permissões com base no princípio de menor privilégio, e revisar regularmente as políticas de acesso.

B) Conceder permissões de administrador a todos os usuários para simplificar o gerenciamento.

C) Usar apenas senhas de 4 dígitos para facilitar o acesso dos usuários e desativar a autenticação multifator (MFA).

D) Desativar logs de auditoria para melhorar o desempenho do sistema e conceder permissões de administrador a usuários raiz.

Em que cenário é mais apropriado federar um serviço de diretório com funções do IAM na AWS?

A) Quando há necessidade de fornecer acesso temporário a recursos da AWS para desenvolvedores externos.

B) Para permitir que funcionários de uma empresa utilizem suas credenciais corporativas existentes, como as do Active Directory, para acessar recursos da AWS, eliminando a necessidade de criar contas de usuário IAM adicionais.

C) Quando se deseja aumentar o número de usuários gerenciados diretamente no console da AWS.

D) Para migrar todos os usuários do Active Directory para um banco de dados relacional gerenciado no Amazon RDS.

Respostas:

B) Utilizar AWS Organizations para consolidar contas e aplicar políticas de controle de serviço (SCPs) para gerenciar permissões de maneira centralizada.

B) AWS Identity Center (AWS Single Sign-On), que integra com diretórios corporativos como Microsoft Active Directory e provedores SAML 2.0.

B) Implementar AWS Control Tower para configurar e governar um ambiente de várias contas, juntamente com SCPs para impor regras de segurança e conformidade.

A) Habilitar autenticação multifator (MFA) para todos os usuários, limitar permissões com base no princípio de menor privilégio, e revisar regularmente as políticas de acesso.

B) Para permitir que funcionários de uma empresa utilizem suas credenciais corporativas existentes, como as do Active Directory, para acessar recursos da AWS, eliminando a necessidade de criar contas de usuário IAM adicionais.