Criação de Papéis Personalizados no Google Cloud IAM

Criação de Papéis Personalizados no Google Cloud IAM

1. Como Criar um Papel Personalizado

No Google Cloud IAM (Identity and Access Management), os papéis personalizados permitem que você crie conjuntos de permissões específicos, ajustados às necessidades de sua organização. Isso é útil quando os papéis predefinidos não atendem exatamente aos requisitos do projeto.

Passos para Criar um Papel Personalizado no Google Cloud IAM:

1. Acessar o Console do Google Cloud:

- No Google Cloud Console, vá para a seção IAM & Admin e clique em Roles (Papéis).

2. Criar um Novo Papel:

- Clique em Create Role (Criar Papel).

- Defina os detalhes básicos:

Nome: Um nome descritivo e exclusivo para o papel.

ID do Papel: Um identificador exclusivo para o papel.

Descrição: Adicione uma descrição clara que ajude a entender a finalidade do papel.

3. Adicionar Permissões:

- Escolha as permissões que deseja atribuir ao papel. Você pode selecionar permissões de diferentes serviços, como Compute Engine, Storage, Kubernetes, etc.

- Exemplo: Se você está criando um papel para gerenciamento de VMs, selecione permissões como compute.instances.create e compute.instances.delete.

4. Salvar e Revisar o Papel:

- Após adicionar todas as permissões, clique em Create (Criar) para finalizar a criação do papel.

Se você tem uma equipe de desenvolvimento que só precisa gerenciar recursos no Compute Engine, você pode criar um papel personalizado que permita criar e deletar instâncias de máquinas virtuais, mas sem conceder permissões para acessar outros serviços, como o Cloud Storage.

2. Atribuição de Papéis a Usuários

Depois de criar um papel personalizado, você pode atribuí-lo a usuários, grupos ou identidades de serviço para garantir que eles tenham as permissões necessárias para acessar os recursos corretos.

Passos para Atribuir Papéis a Usuários:

1. Acessar a Seção IAM:

- No Google Cloud Console, vá para IAM & Admin e selecione IAM.

2. Selecionar o Projeto:

- Certifique-se de que você está no projeto correto para o qual deseja atribuir o papel.

3. Atribuir o Papel:

- Clique em Add (Adicionar) para incluir um novo membro.

- Digite o e-mail do usuário ou do grupo ao qual deseja atribuir o papel.

- Na lista de papéis, escolha o papel personalizado que você criou anteriormente.

4. Salvar a Atribuição:

- Após selecionar o papel e o usuário, clique em Save (Salvar).

Se você tem um grupo de administradores de rede que precisa de permissões específicas para configurar VPCs (Virtual Private Clouds), você pode criar um papel personalizado com permissões de rede e atribuí-lo a esse grupo, limitando o acesso apenas ao que for necessário para suas funções.

3. Verificação de Papéis

É importante revisar periodicamente os papéis atribuídos aos usuários para garantir que as permissões sejam apropriadas e não excessivas, evitando problemas de segurança.

Como Verificar os Papéis Atribuídos:

1. Acessar o Console IAM:

- No Google Cloud Console, vá para IAM & Admin e clique em IAM.

2. Verificar as Atribuições:

- A página de IAM lista todos os usuários, grupos e identidades de serviço com acesso ao projeto, além dos papéis atribuídos a cada um.

- Revise se os papéis concedidos ainda são adequados para as funções atuais de cada membro.

3. Ajustar ou Revogar Permissões:

- Se um papel atribuído for considerado excessivo, você pode modificá-lo diretamente ou remover o membro do projeto.

Se um funcionário mudou de departamento e não precisa mais de acesso a determinados recursos, você pode revisar seus papéis e ajustar as permissões para refletir sua nova função, garantindo que ele tenha apenas os acessos necessários.

4. Importância dos Papéis em um Projeto

A gestão adequada de papéis no Google Cloud é essencial para manter a segurança, a conformidade e o controle de acesso em um projeto. Papéis bem definidos garantem que os usuários e sistemas tenham acesso apenas ao que precisam, reduzindo o risco de violações de segurança ou acessos não autorizados.

Razões para Implementar Papéis Personalizados:

• **Princípio do Mínimo Privilégio**: Um dos princípios mais importantes de segurança é garantir que os usuários tenham o mínimo de permissões necessárias para realizar suas tarefas. Papéis personalizados ajudam a restringir permissões excessivas.

• **Segurança e Conformidade**: Papéis inadequadamente configurados podem expor recursos sensíveis a pessoas não autorizadas. Implementar papéis personalizados garante que as políticas de segurança da empresa sejam seguidas rigorosamente.

• **Facilita a Governança**: Definir papéis específicos para diferentes equipes ou funções facilita a governança e o gerenciamento de grandes projetos no Google Cloud. Isso também ajuda a auditar quem tem acesso a quais recursos.

Em um projeto que envolve várias equipes (desenvolvimento, segurança e operações), cada equipe pode ter papéis personalizados que limitam suas permissões a seus próprios domínios, como os desenvolvedores tendo acesso ao ambiente de desenvolvimento e a equipe de segurança apenas aos recursos de auditoria e monitoramento.

Conteúdo Bônus

Título: Papeis e permissões
Plataforma: Cloud.Google
Descrição: Nesta página, descrevemos os papeis do Identity and Access Management (IAM), que são coleções de permissões do IAM.

Referências Bibliográficas

BASSO, D. E. **Administração de Redes de Computadores**. Contentus, 2020.
KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 8. ed. Pearson, 2021.
MARINHO, A. L.; CRUZ, J. L. da. (Orgs.). **Desenvolvimento de Aplicações para Internet**. 2. ed. Pearson, 2020.

PUGA, S.; RISSETTI, G. **Lógica de Programação e Estruturas de Dados, com Aplicações em Java**. 3. ed. Pearson, 2016.

ROHLING, L. J. **Segurança de Redes de Computadores**. Contentus, 2020.

SILVA, C. F. da. **Projeto Estruturado e Gerência de Redes**. Contentus, 2020.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. **Redes de Computadores**. 6. ed. Pearson, 2021.

TOCCI, R. J.; WIDMER, N. S.; MOSS, G. L. **Sistemas Digitais: Princípios e Aplicações**. 12. ed. Pearson, 2018.

Ir para exercício