O acesso seguro e adequado às contas AWS é fundamental para garantir a operação eficiente dos clusters EKS (Amazon Elastic Kubernetes Service). Para obter acesso a essas contas, é necessário solicitar permissões por meio do portal OneID. É importante ressaltar que as permissões são concedidas com o objetivo de manter a segurança e o controle de acesso aos recursos da AWS.

No entanto, é importante notar que os nomes das permissões no OneID podem ser diferentes das "roles" que aparecem na AWS. Essas discrepâncias ocorrem devido à tradução e à adaptação das permissões específicas de cada ambiente.

No Portal OneID, existem dois tipos principais de permissões disponíveis: SRE e DEV. Cada uma dessas permissões é atribuída a usuários com necessidades diferentes, a fim de garantir que tenham acesso a recursos específicos no ambiente AWS.

As permissões SRE (Site Reliability Engineer) são destinadas aos engenheiros de confiabilidade de site. Esses profissionais têm como responsabilidade principal garantir a estabilidade e a confiabilidade dos sistemas. Com as permissões SRE, os usuários podem acessar e gerenciar os recursos relacionados aos clusters EKS, incluindo a capacidade de modificar configurações, solucionar problemas e executar ações que afetam o ambiente de produção.

Por outro lado, as permissões DEV (Desenvolvedor) são direcionadas aos desenvolvedores de aplicativos e equipes de engenharia. Essas permissões permitem que os usuários acessem e trabalhem com os recursos necessários para desenvolver e testar aplicativos no ambiente EKS, como criar e gerenciar pods, serviços e outros componentes do cluster.

É importante solicitar as permissões adequadas de acordo com o seu papel e as suas responsabilidades no ambiente EKS. Ao fazer isso, você terá acesso somente aos recursos e funcionalidades necessárias para desempenhar suas tarefas específicas, evitando acesso desnecessário a informações confidenciais e reduzindo riscos de segurança.

Em resumo, para garantir acesso aos clusters EKS na AWS, os usuários devem solicitar as permissões apropriadas no portal OneID. Lembre-se de que as permissões têm nomes diferentes no OneID em comparação com as "roles" exibidas na AWS. Escolha entre as permissões SRE e DEV, dependendo das suas necessidades e responsabilidades. Ao fazer isso, você poderá trabalhar de forma eficaz no ambiente EKS, mantendo a segurança e o controle adequados sobre os recursos da AWS.

Modelo 1:

Acesso às Contas AWS e Permissões no Portal OneID para Clusters EKS

É essencial que os usuários solicitem permissões para acessar as contas da AWS por meio do portal OneID, a fim de garantir um acesso seguro e controlado aos clusters EKS (Amazon Elastic Kubernetes Service). Essas permissões têm a finalidade de manter a integridade e a segurança dos recursos disponíveis na AWS.

É importante ressaltar que os nomes das permissões no OneID podem diferir das "roles" que aparecem na AWS. Essas discrepâncias são resultado da adaptação e tradução das permissões específicas em cada ambiente.

No portal OneID, são encontrados dois tipos principais de permissões: SRE e DEV. Cada uma dessas permissões é destinada a usuários com necessidades distintas, a fim de garantir que eles possuam acesso apenas aos recursos relevantes no ambiente AWS.

As permissões SRE (Site Reliability Engineer) são designadas aos engenheiros de confiabilidade de site. Esses profissionais têm a responsabilidade de manter a estabilidade e a confiabilidade dos sistemas. Com as permissões SRE, os usuários podem acessar e gerenciar recursos relacionados aos clusters EKS, o que inclui a possibilidade de modificar configurações, solucionar problemas e realizar ações que afetam o ambiente de produção.

Por outro lado, as permissões DEV (Desenvolvedor) são voltadas para desenvolvedores de aplicativos e equipes de engenharia. Essas permissões permitem que os usuários acessem e trabalhem com os recursos necessários para desenvolver e testar aplicativos no ambiente EKS. Por meio das permissões DEV, é possível criar e gerenciar pods, serviços e outros componentes do cluster.

É fundamental solicitar as permissões adequadas de acordo com o seu papel e suas responsabilidades no ambiente EKS. Ao fazer isso, você terá acesso somente aos recursos e funcionalidades necessárias para desempenhar suas tarefas específicas, evitando assim acessos desnecessários a informações confidenciais e reduzindo os riscos de segurança.

Em resumo, para garantir acesso aos clusters EKS na AWS, os usuários devem solicitar as permissões apropriadas no portal OneID. Lembre-se de que as permissões possuem nomes diferentes no OneID em comparação com as "roles" exibidas na AWS. Escolha entre as permissões SRE e DEV, de acordo com suas necessidades e responsabilidades. Dessa forma, você poderá trabalhar de maneira eficiente no ambiente EKS, mantendo a segurança e o controle adequados sobre os recursos da AWS.

Modelo 2:

Acesso às Contas AWS e Permissões no Portal OneID para Clusters EKS

No contexto dos clusters EKS (Amazon Elastic Kubernetes Service), é imprescindível que os usuários solicitem permissões para acessar as contas AWS por meio do portal OneID. Essas permissões têm um papel crucial na garantia de um acesso seguro e controlado aos recursos disponíveis na AWS.

É importante ressaltar que os nomes das permissões no OneID podem diferir das "roles" que aparecem na AWS. Essas diferenças ocorrem porque as permissões são adaptadas e traduzidas de acordo com