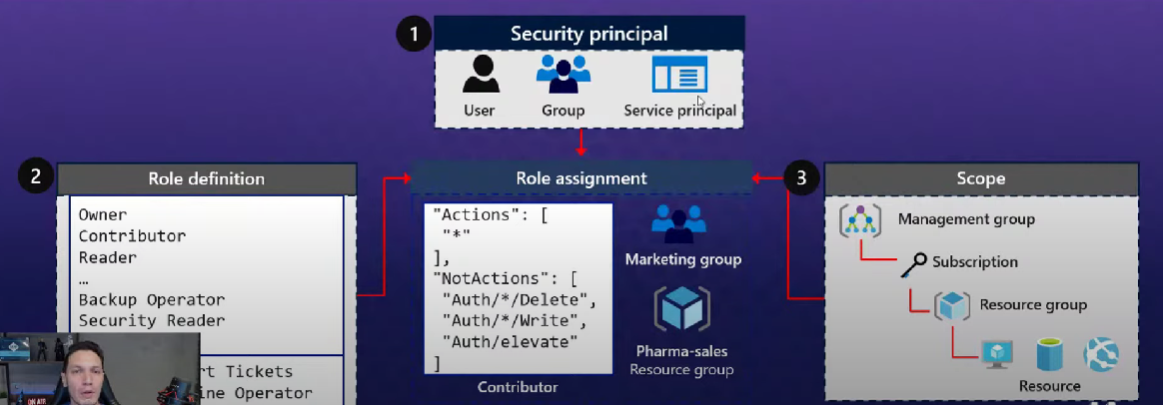
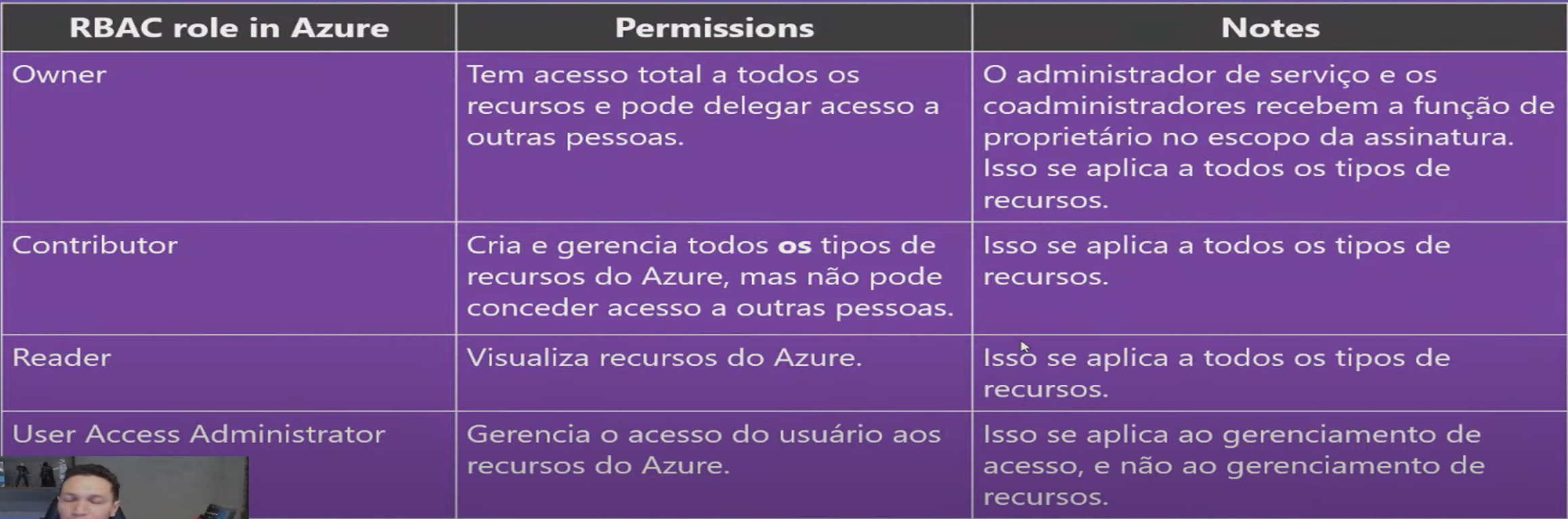
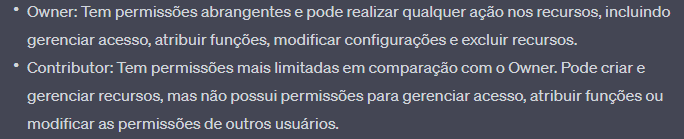
* Fornece gerenciamento de acesso refinado de recursos no Azure.
* Criado no Azure Resource Manager
* Separa tarefas dentro de uma equipe
* Concede apenas a quantidade de acesso aos usuários que eles precisam para executar suas tarefas
* Qualquer recurso dentro do Azure precisar passar pelo RBAC.
* RBAC x Azure Active Diretory
* O RBAC se concentra no controle de acesso a recursos específicos dentro do Azure, permitindo que você defina permissões granulares com base em funções.
* O Azure AD se concentra na autenticação e autorização de usuários para acessar aplicativos e serviços em nuvem, fornecendo recursos de gerenciamento de identidade.
* Conceitos
* Security principal (Quem vai receber a permissão)
* Objeto que representa algo que está solicitando acesso aos recursos.
* Role Definition
* Coleção de permissões que lista as operações que podem ser executadas.
* Ex: Reader, Owner, Contributor etc
* Scope
* Limite para o nível de acesso solicitado.
* Assigment
* Anexando uma definição de função a um objeto de segurança em um escopo específico.
* Os usuários podem conceder acesso descrito em uma definição de função, criando uma atribuição.



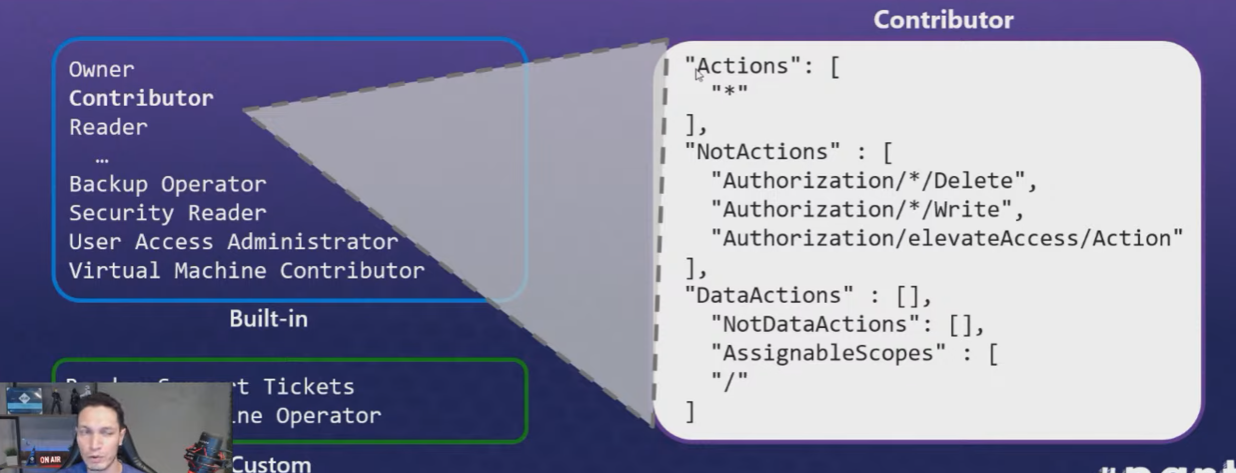
* Role Definition



* Owner
* **Atribuição**: A função de Owner é a de maior privilégio no Azure. Os proprietários têm acesso completo e controle sobre todos os recursos dentro de uma assinatura do Azure.
* **Permissões principais:** Pode gerenciar recursos, incluindo criar, modificar, excluir e gerenciar permissões. Pode criar, atribuir e gerenciar funções de RBAC. Pode visualizar e responder a alertas e notificações. Tem acesso a todas as informações e configurações dentro da assinatura, incluindo faturamento e suporte.
* Contributor
* **Atribuição:** A função de Contributor possui privilégios para realizar ações em recursos, mas não tem controle total sobre a assinatura.
* **Permissões principais:** Pode criar e gerenciar recursos, incluindo modificar e excluir recursos existentes. Pode atribuir e gerenciar permissões em recursos. Pode iniciar e parar máquinas virtuais e outros recursos computacionais. Pode criar e gerenciar redes virtuais e outros recursos de rede.
* A maior diferença entre as funções de Owner e Contributor no RBAC do Azure é que os Owners têm controle total sobre a assinatura ou grupo de recursos, enquanto os Contributors têm permissões para criar e gerenciar recursos, mas com restrições em relação ao gerenciamento de acesso e permissões de outros usuários.



* Reader
* Atribuição: A função de Reader tem permissões apenas de leitura, proporcionando uma visão somente leitura dos recursos na assinatura.
* Permissões principais: Pode visualizar recursos e suas propriedades. Pode visualizar configurações e metadados dos recursos. Não pode realizar alterações nos recursos. Pode visualizar logs e métricas.
* Da mesma forma que as policys são criadas via JSON, as definições de role dentro do RBAC também usa JSON.
* Nesse caso, é Contributor pois a única coisa que ele não pode é dar, remover ou elevar permissionamentos, tirando isso, o resto ele está livre para fazer.



* Azure RBAC Roles vs. Azure AD Roles

