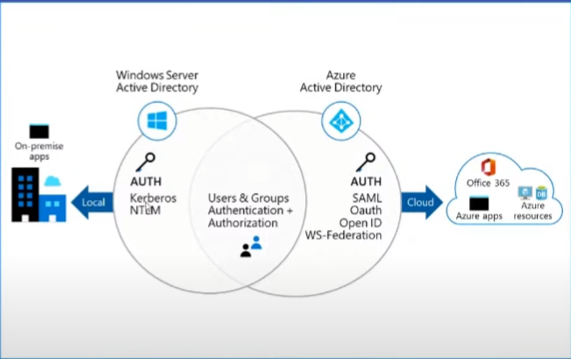
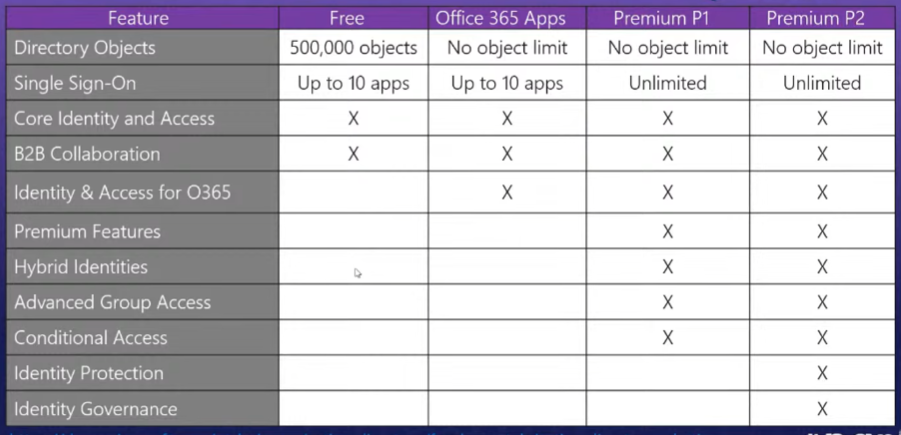
* Serviço de diretório
* Um serviço de diretório é um sistema de armazenamento e recuperação de informações relacionadas a usuários, recursos e serviços em uma rede. Ele fornece um mecanismo centralizado para gerenciar e organizar essas informações, permitindo o acesso e a localização eficiente de recursos dentro de uma rede.
* Um serviço de diretório é composto por um banco de dados especializado que armazena informações de identidade, como nomes de usuários, senhas, atributos de perfil, permissões de acesso e informações de configuração.
* Essas informações são organizadas em uma estrutura hierárquica, geralmente chamada de árvore de diretórios.
* Os serviços de diretório são usados para diversas finalidades, incluindo autenticação, autorização, gerenciamento de identidades, controle de acesso, descoberta de recursos, compartilhamento de informações e colaboração em uma rede.
* Eles facilitam a administração e o gerenciamento centralizado de usuários, grupos, dispositivos e outros objetos dentro de um ambiente de rede.
* Um exemplo bem conhecido de serviço de diretório é o Active Directory da Microsoft, que é usado em ambientes Windows para gerenciar identidades e recursos em uma rede local.
* Outros exemplos populares incluem o LDAP (Lightweight Directory Access Protocol), que é um padrão de serviço de diretório amplamente adotado, e o Azure Active Directory, que é um serviço de diretório baseado em nuvem fornecido pela Microsoft para gerenciar identidades e acesso em ambientes na nuvem.
* O Azure AD é um serviço de gerenciamento de identidade e acesso baseado em nuvem fornecido pela Microsoft como parte da plataforma Azure. Ele oferece recursos de autenticação e autorização para aplicativos e serviços na nuvem, permitindo que as organizações gerenciem o acesso de usuários e aplicativos aos recursos de maneira segura.
* Consiste no Identity Provider, ou seja, o gerador de autenticação, onde é armazenado todos os objetos (usuários, grupos, contas etc), a partir disso, é possível ter uma gestão centralizada de recursos.



* Conceitos
* Identity
* Um objeto que pode ser autenticado
* Account
* Uma identidade que possui dados associados.
* Azure AD Account
* Uma identidade criada pelo Azure AD ou outro serviço de nuvem da Microsoft.
* Azure tenant
* Uma instância dedicada e confiável do Azure AD, criada automaticamente quando sua organização se inscreve para uma assinatura do serviço de nuvem Microsoft.
* Azure AD directory
* Cada tenant do Azure tem um diretório dedicado e confiável do Azure AD.
* User subscription
* Usado para pagar pelos serviços em nuvem do Azure.
* AD DS (Active Diretory Domain Service) X Azure Active Diretory
* O Active Directory Domain Services (AD DS) e o Azure Active Directory (Azure AD) são dois serviços de diretório fornecidos pela Microsoft, mas eles têm finalidades diferentes e operam em ambientes distintos.
* O AD DS é um serviço de diretório local, tradicionalmente usado em ambientes de rede local baseados no Windows Server, enquanto o Azure AD é um serviço de diretório baseado em nuvem, projetado para autenticar e autorizar o acesso a aplicativos e serviços na nuvem.
* Cada um tem suas próprias funcionalidades e propósitos específicos, embora o Azure AD também possa ser integrado ao AD DS para fornecer recursos de identidade e acesso em ambientes híbridos (combinando recursos locais e na nuvem).
* Características Azure AD
* O Azure AD é principalmente uma solução de identidade projetada para comunicações HTTP e HTTPS.
* Os usuários e grupos do Azure AD são criados em uma estrutura plana e não existem Unidades Organizacionais (UOs) nem Objetos de Diretiva de Grupo (GPOs).
* Azure Active Directory Editions
* Cada subscription dará um nível de poder dentro do Azure AD.
* Ao adquirir uma conta trial, por exemplo, terá uma subscription free, nela terá seu respectivo licenciamento dentro o Azure AD.



* Azure AD Join
* Self-Service Password Reset
* Create Users Accounts
* Um usuário nativo é criado do Azure AD quando não há um ambiente híbrido
* Um ambiente híbrido, nesse contexto, se refere a replicação do AD local dentro do Azure AD. Desse modo, todas as identidades do local são replicadas para a nuvem.
* Caso crie um usuário na nuvem e ele já exista no local, eles não possuem sincronia.
* Para manter o sincronismo, é necessário criar o usuário local, instalar o Azure AD Connect, e replicar ele para nuvem.
* O sentido da replicação de criação de conta sempre é local🡪 nuvem.
* Ao criar um usuário, é possível colocá-lo como “cloud-only” (apenas nuvem), usuário que podem ser replicados (criou AD local, automaticamente é criado no AD Nuvem), e usuários convidados.
* Gerenciamento de conta de usuário
* Caso na empresa tenha algum fornecedor externo, é possível colocá-lo como usuário guest.
* Criar conta de usuário em massa
* Group Accounts
* Tipos de grupos
* Security Groups
* Office 365 Groups
* Tipos de associação
* Assigned
* Dynamic User
* Dynamic Device (Security groups only)
* Criar Administrative Units
* Managing Multiple Directories
* Dentro do Azure AD, cada tenant é um recurso totalmente independente.
* Não há relação pai-filho entre tenants.
* Essa independência entre tenants inclui recursos, administração e sincronização.