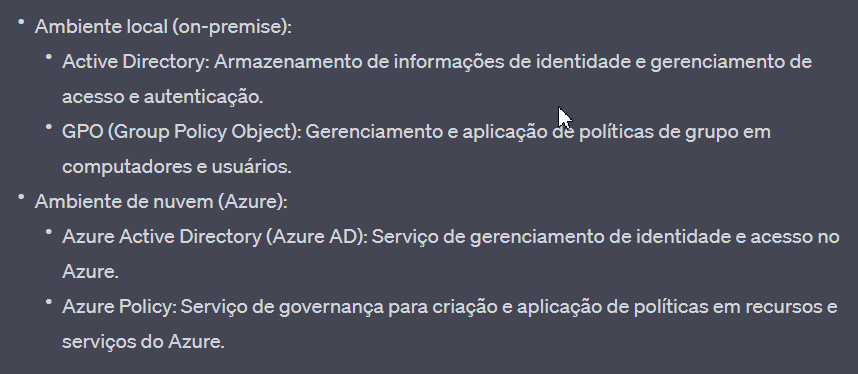
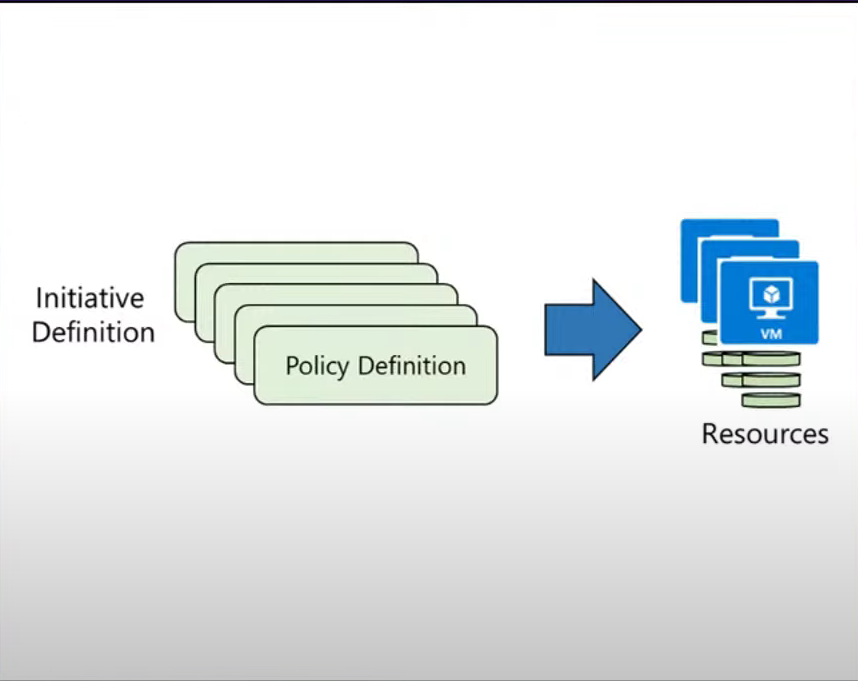
* O Azure Policy é uma ferramenta de governança que permite **impor regras** e **políticas específicas** em seu ambiente do Azure.
* Ele é usado para garantir que os recursos implantados no Azure estejam configurados corretamente e em conformidade com as políticas e requisitos específicos da organização.
* O Azure Policy pode ser usado para impor restrições de segurança, conformidade regulatória, boas práticas de governança e outros requisitos específicos.
* Embora o Azure AD tenha um foco mais direcionado ao gerenciamento de identidade e acesso, o Azure Policy é mais amplo e pode ser aplicado a várias áreas, como redes, armazenamento, máquinas virtuais, bancos de dados e assim por diante.
* Ele oferece flexibilidade para definir e impor políticas personalizadas para atender às necessidades específicas da sua organização.
* Portanto, enquanto o **Azure AD** é mais voltado para o **gerenciamento de identidade** e acesso de usuários, o **Azure Policy** é usado para definir e **aplicar políticas gerais** de governança em todo o ambiente do Azure.
* Azure Active Diretory X Azure Policy
* Azure Active Directory (Azure AD): Você pode usar o Azure AD para gerenciar o acesso de usuários e grupos aos recursos do Azure. Por exemplo, você pode criar usuários e grupos no Azure AD e atribuir permissões específicas a eles. Isso permite que você controle quem pode acessar determinados recursos e quais ações eles podem executar.
* Você também pode habilitar a autenticação multifator para aumentar a segurança e configurar o SSO para facilitar o acesso dos usuários aos aplicativos baseados na web.
* Azure Policy: Agora, suponha que você tenha uma política de segurança que exija que todas as máquinas virtuais em sua assinatura do Azure tenham o firewall do sistema operacional habilitado. Você pode criar uma política no Azure Policy para impor essa regra.
* A política pode ser definida para verificar e garantir que todas as máquinas virtuais estejam em conformidade com essa configuração específica. Se alguma máquina virtual não estiver em conformidade, o Azure Policy pode gerar um alerta ou até mesmo corrigir automaticamente a configuração.



* Casos de uso
* Tipos de recursos permitidos
* Especifique os tipos de recursos que sua organização pode implantar.
* SKUs de máquina virtual permitidos
* Especifique um conjunto de SKUs de máquina virtual que sua organização pode implantar.
* Ex: Tamanho de VM
* OBS: SKUs no contexto do Azure são identificadores usados para representar diferentes configurações, níveis de desempenho e opções de preços para os serviços do Azure.
* Locais permitidos
* Restringir os locais que sua organização pode especificar ao implantar recursos.
* Ex: Toda estrutura e recursos devem estar no Brasil.
* Exigir tag e seu valor
* Aplicar uma tag obrigatória e seu valor.
* Ex: Todos os recursos do Resource group X tenham a tag “Departamento Marketing”.
* Implementing Azure Policy
* Escolher a definição da política
* Criar definições da iniciativa
* Escopo de definição da iniciativa
* Iniciativa é um agrupamento de políticas



* Exibir resultados da avaliação da política
* Determine Compliance
* Compliance é o dashboard responsável por mostrar o quão próximo o sistema está das políticas definidas.
* O compliance mostra
* Iniciativas não conformes
* Políticas não compatíveis
* Recursos não compatíveis

