



AZ-104-Studies

- Created by Lucas B R Santos
- Fontes:

Exame AZ-104: Microsoft Azure Administrator - Certifications
Exame AZ-104: Microsoft Azure Administrator



<https://learn.microsoft.com/pt-br/certifications/exams/az-104/>

Login - TFTEC Prime



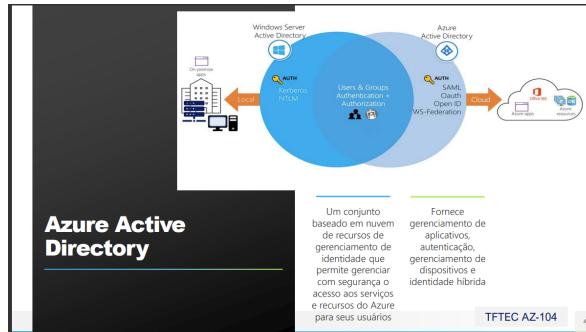
<https://www.tftecprime.com.br/ead/course/az-104/#section13>

▼ MD1 → Identity Solutions

▼ Azure Active Directory

▼ AzAD conceitos

- AD On-premises → utiliza windows server
 - Kerberos
 - NTLM
- Az AD → Utiliza os serviços da nuvem
 - SAML → Mais utilizado
 - Oauth
 - Open ID
 - WS-Federation
- É possível ter uma conexão híbrida através do azure ad conect entre o onpremises e a cloud



- Office 365 → é um serviço da nuvem, caso não haja esse ambiente híbrida, o user onpremises não irá conseguir se conectar
- Não se trata somente de contas de usuário, mas também de dispositivos e objetos que podem ser autenticados

CONCEPT	DESCRIPTION
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 da 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.

- Identidade → qualquer coisa logável nos serviços MS
- Account → Conta de usuário que tem dados associados
- AzAD connect → faz o sincronismo entre o ambiente onpremises e o ambiente cloud
- Tenant → uma instância no Azure AD, funciona como um diretório, quando criamos um az ad novo criamos um novo tenant
- Az AD Directory → Semelhante ao AD padrão, mas tem certas particularidades
- User Subscription → permite atribuir créditos diretamente a usuários, por ex créditos de teste gratuitos, porém é necessário ter uma sub atribuída

▼ AD DS vs AzAD

- Vantagens únicas do AzAD
 - Office365 → Só é possível através do AzAD connect quando é necessário integrar a identificação de usuários onpremises
 - Solução de identidade projetada para comunicação HTTP e HTTPS → Ex: Single Sign ON
 - AzAD permite consultar API REST sobre HTTP e HTTPS ao invés do LDAP
 - Protocolos HTTP e HTTPS, como SAML, WS-Federation e OpenID Connect para autenticação e OAuth para autorização em vez de Kerberos
 - Inclui serviços de federação e muitos serviços terceiros → Integrar uma conta do azad em outra nuvem, ou um site, utilizando o SAML
 - 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)

▼ AZ AD Directory Editions

Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

- AZAD possui Free → Permite SSO até 10 apps
 - É possível criar até 100 Users na modalidade try
- B2B → Trazer um outro usuario de outro dominio como convidado no tenant, sem criar outro user
- Advanced Group Acces → config de permissão de acesso a um dispositivo para um grupo de usuario
- Acesso condicional → Se o IP é de outra será necessário um 2FA, condições como está podem ser atribuídas
- Identity Protection → Monitora o comportamento das contas
- Identity Governance → Faz um controle de acesso nas contas de usuário, atribuir um tempo para um acesso mais administrativo e após o tempo remove automaticamente

▼ Az AD Join

- Colocar uma máquina no Az AD
- Pode usar o intune
- Mesmo se estiver fora da rede permite o acesso ao computador através do Az Ad Join
- Através da loja do windows pode colocar apps liberados para download
- Restrições de acessos a APPS
- Windows Hello para liberação de acesso a dispositivo
- É possível criar políticas de acesso
- É possível continuar acessar dispositivos locais

▼ Multi-Factor Authentication

- Duplo fator de autenticação → Senha + confirmação de dispositivo como token, sms, permissionamento
 - Condicionamento como → Se estiver fora da rede forçar o MFA
- Permite impor controles no acesso a aplicativos com base em condições específicas

▼ Self-Service Password Reset

- Permite que o próprio usuário faça o reset ou desbloqueio da senha
- Através de métodos personalizados para realizar procedimentos como esse
- Ex: Vai no app e faz a troca ou desbloqueio de conta
- Determinar grupos específicos ou usuários específicos para realizar o desbloqueio

▼ Users And Groups

▼ User Accounts

- Os usuários são as identidades no geral
- É semelhante ao AD normal
- Todos os usuários devem ter uma conta
- A conta é usada para autenticação e autorização
- Fonte de identidade : nuvem, sincronizado com diretório e convidado

	Name	User name	User type	Source
<input type="checkbox"/>	Ziaulla	ziaulla@mic...	Guest	External Azure Active Directory
<input type="checkbox"/>	Retail Crisis Notificati...	rscrisis@mic...	Member	Windows Server AD
<input type="checkbox"/>	"Planning & Launch Se...	plsoem@mi...		Windows Server AD
<input type="checkbox"/>	'amckenziec...	'amckenziec...	Guest	Invited user
<input type="checkbox"/>	"Evento FY20 Colombia	kickcolo@mi...	Member	Windows Server AD

▼ Managing User Accounts

- Necessário ter permissão global ou adm de usuários
- Os itens necessários para preencher é os mesmos do AD normal
- Usuários excluídos podem ser restaurados em até 30 dias
- As informações de logon e logs de auditoria estão disponíveis

▼ Bulk User Accounts

- É possível criar um arquivo CSV e repassar para o Azure AD, assim criar usuários em massa
- Assim é possível criar usuários em lote
- Atribuição a grupos, e remoção também é possível por este método
- Algumas colunas e linhas serão necessárias para o preenchimento correto do arquivo para que o Azure consiga puxar as informações

▼ Group Accounts

- Tipos de grupos → Security groups e Office 365
 - Office 365 → e-mail habilitado associado a um grupo, funciona como mailbox compartilhada para todo grupo
 - Grupos de segurança → Reservados para ter determinada autorização ou determinada role
- Tipos de associação → Assigned, dynamic user, dynamic device
 - Dynamic → usuários com determinado atributo serão inseridos em um determinado grupo, isso tanto para usuários quanto para devices

▼ Az AD Connect

- Integra seus diretórios locais ao Az AD
- Fornece uma identidade comum para seus usuários para apps do Office 365, Azure e SaaS integrados ao Az AD
- Existem várias opções de autenticação (hash synchronization and pass through authentication)
 - Password hash synchronization → guarda hash da senha do Azure no AD, sempre vai ser criptografado

- pass through authentication → Valida no ad on premises se a senha está correta, ao invés de validar na nuvem como o AzAD
 - Sem a conexão do ad local, não será possível autenticar

▼ Az AD Connect health

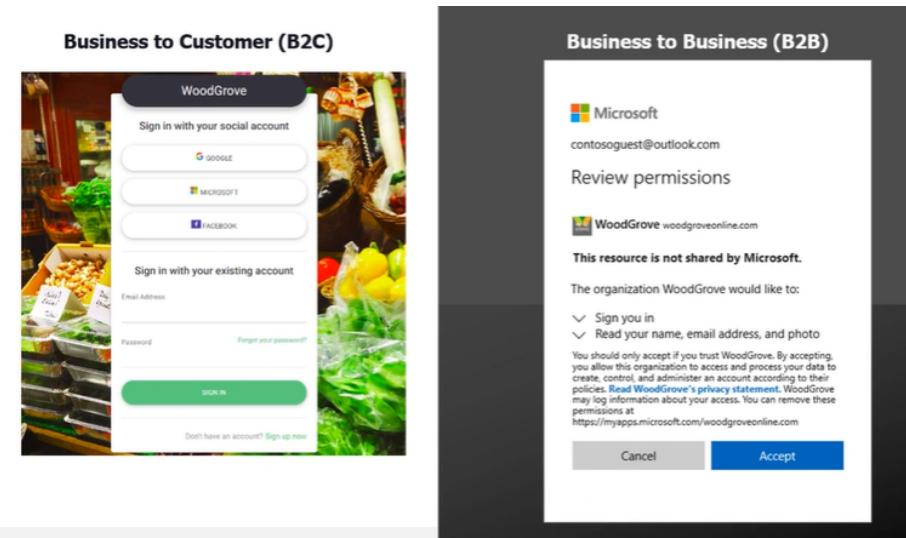
- Monitoramento do ambiente híbrido
- Monitora a saúde do ambiente, se os serviços, os recursos estão integros, em funcionamento
- Monitorar e obter informações referente aos servidores AD FS, AZ AD connect, e controladores de domínio do ad

▼ Managing Multiple Directories

- No Azure Active Directory (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

▼ Az AD B2B & B2C

- B2B
 - Convida usuários de outros tenants do azure ad para o tenant da org
 - O provisionamento do usuário é feita pela parte convidada (A origem)
- B2C
 - Convidar usuários de outras mídias sociais com tenant de identidade para o tenant da sua própria org
 - O provisionamento é feita da parte convidada



▼ MD2 → Governance and Compliance

▼ Subscriptions and Accounts

▼ Regions

- Conjuntos de datacenters do azure
- Cada país tem um par de região (exceto o Brasil)
- Cada região replica os dados com a outra
- Dentro de cada região há até 3 zonas
- zonas = datacenters
- A alta disponibilidade deve ser configurada quando trabalhamos com IaaS
- Zona de replicação do Brasil é em outro país devido haver apenas uma região
- Quanto mais distante a região for do usuário que está fazendo acesso, haverá mais latência
- Cada região possui seu valor estimado

Azure Speed Test 2.0

Azure Speed Test 2.0 - Measure the latency to your nearest Microsoft Azure Data Center

<https://azurespeedtest.azurewebsites.net/>

- Há serviços em que não é permitido selecionar a região
- Há serviços em que são bloqueadas ou não permitidos em determinadas regiões

▼ Az Subscription

- Assinatura associada a uma conta
- As subscription são idênticas, ou seja pode-se criar várias subscription
- Uma empresa pode ter várias subscription
- Com as subscription há limite de segurança e cobrança
- A subscription é associada a um diretório no tenant
- Para podermos criar recursos é necessário ter uma subscription

▼ Getting a Subscription

- Os clientes do **Enterprise Agreement (EA)** assumem um compromisso monetário inicial e consomem serviços ao longo do ano
 - Paga anualmente
 - Pode quebrar o pagamento
 - obter créditos e ir pagando de acordo com o contrato
- Os **revendedores** fornecem uma maneira simples e flexível de adquirir serviços em nuvem
 - Fazem o intermédio com a MS
- Os **parceiros** podem projetar e implementar sua solução de nuvem do Azure
 - Empresas terceiras
- Conta gratuita pessoal - comece imediatamente
 - A conta que qualquer usuário utiliza

▼ Subscription Usage

- Free → 200 U\$ em 30 dias, acesso ilimitado gratuito por 12 meses
- Pay-As-You-Go → Cobra você mensalmente
 - Pago pelo uso

- Necessario realizar o atualiza a conta para funcionar
- Enterprise → Um contrato, com descontos para novas licenças e software assurance - Direcionados a organizações de escala corporativa
 - EA → Melhor formato corporativo
 - Nível de parceria maior
 - Mais indicados para empresas
- Student → Inclui U\$ 100 por 12 meses - deve verificar o acesso do aluno
 - Instituições com parceria com a MS

▼ Cost Management



- Análise de custos
 - Não mostra a VM por exemplo, que está contribuindo com os 18K
 - Essa limitação acontece em diferentes clouds
- Criar um orçamento
- Revisar Recomendações
- Exportar os Dados
- É possível atribuir budgets → alertas, se atingir um determinado valor será encaminhado um aviso para um ou varios usuarios

▼ Resource Tags

- Etiqueta para cada recursos
- Cost management pode verificar tags e validar qual tag tá consumindo oq
- Essencial para billing por setor
- Tags são manuais
- Tags não são propagadas
- É possível forçar a obrigatoriedade de criação de tags

▼ Cost Savings

- Reservations do Azure → Ajuda a economizar dinheiro pagando antecipadamente pelos serviços

- Reservar uma vm, por exemplo, por 3 anos
- Se cancelar a multa
- Benefícios Híbridos do Azure → Use licenças locais do windows server e SQL server com software assurance
 - É necessário ter o assurance
- Créditos do Azure → benefício mensal de crédito que permite experimentar, desenvolver e testar novas soluções no azure
 - Licença Visual Studio
- Regiões → Escolha locais e regiões de baixo custo
 - Cada região tem um custo diferenciado

Azure VM Comparison

Select your cookie preferences We use cookies and similar tools to enhance your experience, provide our services, and make improvements. Approved third parties also use these tools to certain site features. More details available here Cookie Policy

<https://azureprice.net/>

VM Name	Cores	Memory (GB)	Local Price	Windows Price	Best Assurance (hrs)	Region	Buy in region (EUR)
Basic_A0	1	0.75	1.0007	1.0007	2nd hours	westeurope	€0.0001 / 0.0%
Basic_A1	1	1.75	2.0008	2.0008	2nd hours	westeurope	€0.0002 / 0.0%
Basic_A2	2	3.50	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Basic_A3	4	7.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Basic_A4	8	14.00	16.0009	16.0009	2nd hours	westeurope	€0.0016 / 0.0%
Standard_D1	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_D2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_D3	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_D4	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_D1_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_D2_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_D3_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_D4_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_G	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_G	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_G	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_G	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_G_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_G_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_G_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_G_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_H	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_H	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_H	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_H	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_H_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_H_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_H_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_H_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_I	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_I	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_I	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_I	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_I_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_I_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_I_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_I_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_M	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_M	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_M	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_M	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_M_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_M_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_M_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_M_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_H	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_H	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_H	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_H	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_H_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_H_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_H_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_H_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_M	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_M	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_M	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_M	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_M_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_M_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_M_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_M_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_H	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_H	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_H	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_H	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_H_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_H_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_H_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_H_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_M	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_M	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_M	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_M	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_M_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_M_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_M_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_M_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_EA	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_EA	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_EA	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_EA	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_EA_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_EA_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_EA_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_EA_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_EA_H	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_EA_H	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_EA_H	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_EA_H	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_EA_H_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_EA_H_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_EA_H_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_EA_H_V2	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_EA_M	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_EA_M	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_EA_M	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 / 0.0%
Standard_EA4_EA_EA_EA_M	8	6.00	8.0009	8.0009	2nd hours	westeurope	€0.0008 / 0.0%
Standard_EA1_EA_EA_EA_M_V2	1	0.75	1.0009	1.0009	2nd hours	westeurope	€0.0001 / 0.0%
Standard_EA2_EA_EA_EA_M_V2	2	1.50	2.0009	2.0009	2nd hours	westeurope	€0.0002 / 0.0%
Standard_EA3_EA_EA_EA_M_V2	4	3.00	4.0009	4.0009	2nd hours	westeurope	€0.0004 /

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.
Locais permitidos - restrinja os locais que sua organização pode especificar ao implantar recursos.
Exigir tag e seu valor - aplica uma tag obrigatória e seu valor.
O Backup do Azure deve estar habilitado para Máquinas Virtuais - Audite se o serviço de Backup do Azure estiver habilitado para todas as máquinas virtuais.

- É um serviço no azure que você usa para criar, atribuir e gerenciar políticas
- O az policy executa avaliações e verificações de recursos não compatíveis
- Vantagens:
 - Aplicação e conformidade
 - Aplicar políticas em escala
 - Remediação
- Lock → ou bloqueia a deleção, ou proíbe criação
- SKUs → Qual é o tam da maquina virtual

▼ Implementing Azure Policy

- Escolher a definição da politica
- Criar definições de iniciativa
 - Iniciativa de politica é diferente das definições de politica
- Escopo de definição da iniciativa
- Exibir resultados da avaliação da politica

▼ Policy Definitions

- Existem muitas definições de política disponíveis no azure
- Você pode importar políticas do github
 - É possível fazer instalações automatizadas
- As Definições de política têm um formato JSON específico
- Você pode criar definições de política personalizadas

Policy definition
New Policy definition

BASICS

Definition location *
Visual Studio Enterprise

Name * ⓘ
Github Sample Policy

Description
A sample policy from Github.

Category ⓘ
 Create new Use existing
Category

POLICY RULE

[Import sample policy definition from GitHub](#)

▼ Create Initiative Definitions

- Política - uma regra para determinado objeto ou recurso
- Definições de política de grupo incluir uma ou mais políticas, requer planejamento
- Em uma iniciativa pode ter n políticas ou seja um Compliance

The screenshot shows the Azure portal interface for managing initiative definitions. On the left, there's a sidebar with various icons and a main panel for 'Assign initiative' with fields for 'Scope' (set to 'ca-phschmitt-demo-test/TT-RG-Demo2b'), 'Exclusions' (empty), and 'Assignment name' (empty). On the right, under 'Available Definitions', it says 'Type: Built-in' and 'Search: Filter by name or id...'. Below this, it lists 'Initiative Definitions (36)'. There are four preview entries:

- [Preview]: Audit SWIFT CSP-CSCF v2020 controls and deploy specific VM Extensions to support audit requirements
- [Preview]: Audit VMs with insecure password security settings
- [Preview]: Audit PCI v3.2.1:2018 controls and deploy specific VM Extensions to support audit requirements
- [Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements

 Each preview entry includes a 'Built-in' link and a detailed description of the policy's purpose and scope.

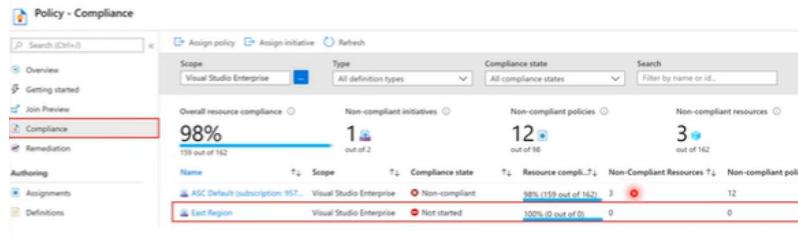
- Dependendo do ambiente a iniciativa é mais completa do que políticas isoladas

▼ Scope the Initiative definition

- Atribuir a definição a um escopo
- O escopo aplica a política
- Selecione a assinatura e, opcionalmente, o grupo de recursos

▼ Determine Compliance

- Quando criamos tanto as políticas quanto as iniciativas de definição, colocamos policy compliance
- O compliance vai indicar se está ou não de acordo
 - Iniciativas não conformes
 - Políticas não compatíveis
 - Recursos não compatíveis



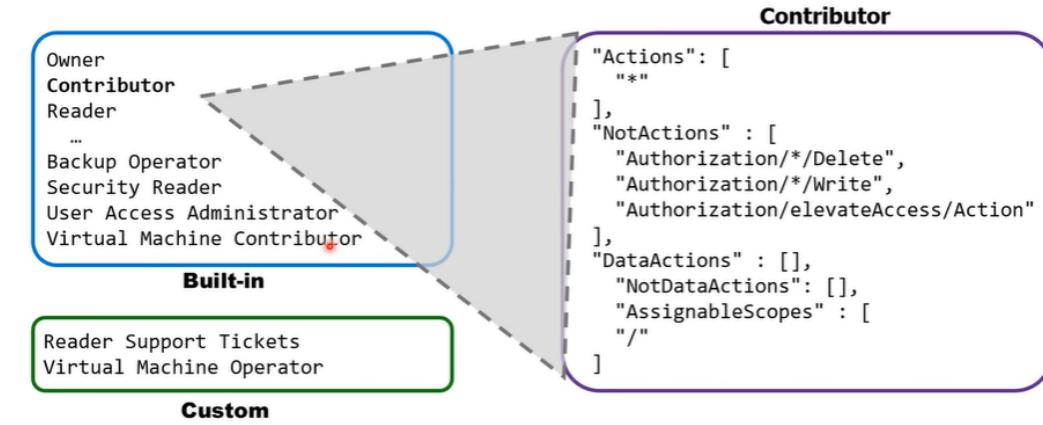
- Vai indicando oq está e o que não está compliance
- Quando o recurso não está compliance pode fazer uma remediação, para que de forma automática seja realizado um ajuste e o recurso ou objeto volte a se tornar compliance
- É possível fazer uma remediação manual
- Um bom exemplo seria remediação com tags
- not started → varredura da política não iniciada
- non-compliance → Indica que algo no ambiente não está compliance

▼ RBAC

- Role-Based Access Control
- Uma forma de gerenciamento para customizar para que cada usuário tenha determinado acesso para uma determinada atividade
 - Liberação de acesso granular / permissão granular
- Criado no Az Resource manager
- Separa tarefas dentro da sua equipe
- **Security principal** → objeto, usuário, etc.
- **Role Definition** → Definições de permissões que role irá possuir
- **Scope** → Limite que estará definido, para uma assinatura, para um RG, para um recurso
- **Assignment** → Anexando diretamente ao objeto/usuário
 - Negar atribuições atualmente são somente leitura e são definidas pelo Az Blueprint e pelos Az Managed apps

▼ Role Definition

- Temos roles já definidas como owner, contributor, reader (são os principais)
 - owner - dono, faz tudo, domain admin
 - contributor - igual ao owner, mas não pode atribuir permissão para outras pessoas
 - reader - consegue visualizar todo ambiente, mas não consegue ter uma atuação (criar, deletar, etc)
 - O template vem em Json



- No exemplo mostra uma role personalizada que pode ser usada para monitorar e reiniciar máquinas virtuais

JSON

```

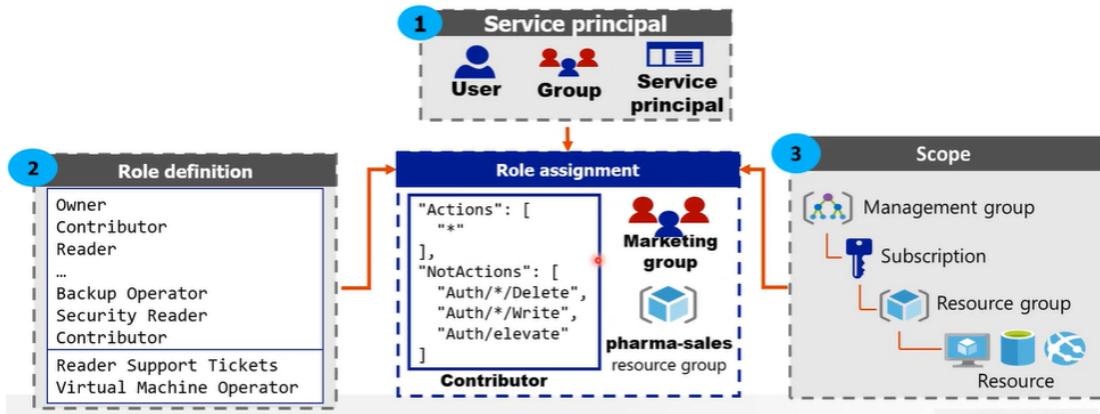
{
    "Name": "Virtual Machine Operator",
    "Id": "88888888-8888-8888-888888888888",
    "IsCustom": true,
    "Description": "Can monitor and restart virtual machines.",
    "Actions": [
        "Microsoft.Storage/*/read",
        "Microsoft.Network/*/read",
        "Microsoft.Compute/*/read",
        "Microsoft.Compute/virtualMachines/start/action",
        "Microsoft.Compute/virtualMachines/restart/action",
        "Microsoft.Authorization/*/read",
        "Microsoft.ResourceHealth/availabilityStatuses/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Insights/alertRules/*",
        "Microsoft.Insights/diagnosticSettings/*",
        "Microsoft.Support/*"
    ],
    "NotActions": [],
    "DataActions": [],
    "NotDataActions": [],
    "AssignableScopes": [
        "/subscriptions/{subscriptionId1}",
        "/subscriptions/{subscriptionId2}",
        "/providers/Microsoft.Management/managementGroups/{groupId1}"
    ]
}

```

- No caso pode aplicar somente para uma sub, rg, recurso em si.

▼ Role Assignment

1. Escolhemos o usuário, grupo ou service principal
2. Criamos ou escolhemos uma role
3. Associamos a role ao objeto e ao ambiente em si

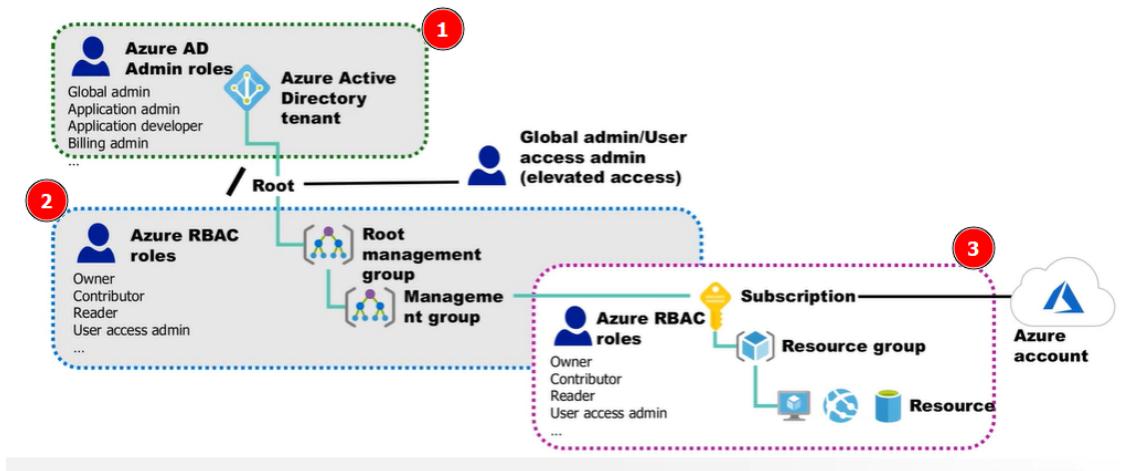


▼ Az RBAC Roles vs Azure AD Administrator roles

- Temos os RBAC que são específicas para os recursos
- E tem as roles do AAD que são voltadas para permissionamento licença, permissões voltadas ao AD, e etc.

Azure RBAC roles	Azure AD roles
Gerenciar o acesso aos recursos do Azure	Gerenciar o acesso aos objetos do Azure AD
O escopo pode ser especificado em vários níveis	O escopo está no nível do tenant
As informações de função podem ser acessadas no portal do Azure, CLI do Azure, Azure PowerShell, modelos do Azure Resource Manager, API REST	As informações de função podem ser acessadas no portal do Azure, portal de administração do Office 365, Microsoft Graph, Azure Active Directory PowerShell for Graph

▼ RBAC Authentication



1. Associamos as permissões de usuário → Roles do AD
2. Usuário com global admin consegue validar as permissões e ter atribuições para as roles, owner, contributor, reader. Podemos atribuir ao root management group ou a um management group específico → Roles RBAC de recursos
3. Está atrelado ao RBAC de subscription, RGs e Recursos → Roles RBAC de recursos

▼ Az RBAC Roles

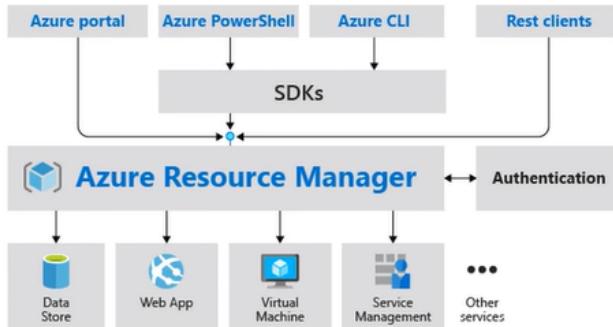
- Há 3 funções específicas do RBAC

RBAC ROLE IN AZURE	PERMISSIONS	NOTES
Owner	Tem acesso total a todos os recursos e pode delegar acesso a outras pessoas.	O administrador de serviço e os coadministradores recebem a função de proprietário no escopo da assinatura. Isso se aplica a todos os tipos de recursos.
Contributor	Cria e gerencia todos os tipos de recursos do Azure, mas não pode conceder acesso a outras pessoas.	Isso se aplica a todos os tipos de recursos.
Reader	Visualiza recursos do Azure.	Isso se aplica a todos os tipos de recursos.
User Access Administrator	Gerencia o acesso do usuário aos recursos do Azure.	Isso se aplica ao gerenciamento de acesso, e não ao gerenciamento de recursos.

▼ MD3 → Azure Administration

▼ Resource Manager

▼ Resource Manager



- Enviamos uma solicitação através do Azure portal, PowerShell, etc. O Resource Manager recebe e realiza a ação
- Implantação e orquestração dos recursos do Azure
- Toda a camada de gerenciamento e criação de recursos no Azure

▼ Terminology

- Resource → Recurso (vm, vnet, storage, etc.)
- Resource Group → Agrupamento dos recursos
- Az Resource manager Template (ARM Template) → Arquivo JSON no qual podemos declarar toda a nossa infraestrutura que será provisionada
- Sintaxe Declarativa → Permite que coloquemos sequências de comandos para criar a infraestrutura no Azure através do arquivo JSON

- Resource Provider → Responsável por fornecer todos os recursos que pode ser implantado através do resource manager

▼ Resource Group Deployments

- Precisamos ter uma subscription e um resource group para criar um recurso
- Podem existir apenas em um grupo de recurso
- Groups não podem ser renomeados
- Podem ter recursos de muitos tipos diferentes (serviços)
 - Criar RG de vm, ou de ambientes (dev, homol, prod)
- Grupos podem ter recursos de várias regiões diferentes
 - RG da south-east e os recursos de outras regiões
- As implantações são incrementais
 - Se criamos um recurso, ou uma nova infra, ele irá incrementar, sem excluir o existente

▼ Resource Manager Locks

- Lock → dois tipos:
 - Read only
 - Só vê
 - Delete
 - só não consegue deleta
- Lock pode ser add no nível mais alto ou até o nível baixo
- Lock é propagável, se colocarmos na sub, os rgs e os recursos receberam esse lock

▼ Moving Resources

- Os recursos podem ser movimentados para outros RGs e outras subs (outro RG que está em outra subscription)
- O RG de origem e destino são bloqueados durante a alteração
- Alguns recursos não podem ser movidos
 - Az AD
 - Express route
 - Site recovery

▼ Removing Resources and Resource Groups

- Recursos podem ser removidos normalmente
- Se deletarmos o RG, todos os resources serão excluídos



- Comando

- `Get-AzResourceGroup -Name 'az104-03' | Remove-AzResourceGroup -Force -AsJob`

- AsJob → Para rodar em background

▼ Resource Limits

- Alguns tipos de recurso possuem limites
 - Também conhecido como cota
- Por exemplo há limites de vCPU para os recursos de VM
- É possível solicitar através da ms para aumentar o limite de cotas
- É possível ter limite de storage, IPs, vCPU por região, etc.
- Só não é possível solicitar para contas de treinamento

▼ Az Portal and Cloud Shell

▼ Azure Portal

- Portal que utilizamos pelo navegador mesmo
- portal.azure.com
- Principal modo de acesso
- Permite
 - gerenciamento de recursos
 - criar painéis
 - Podemos usar o cloud shell através do portal
 - Pede uma storage account pois as sessões precisão de um /home

▼ Azure Mobile App

- Conectado à nuvem
- Utilização do cloudshell
- Utilizar para gerenciamento de recursos não é possível porém podemos controlar através do cloudshell no celular
- Podemos ver os recursos que usarmos ou criamos recentemente
- podemos listar os grupos de recursos
- Validar subscriptions
- Notificações e integridade de serviços
- Podemos iniciar vms pelo app e até mesmo acessar

▼ Azure Cloud shell & PowerShell

- Interativo pelo navegador
- Oferece bash ou powershell
- É temporário e é fornecido por sessão, por usuário, requer rg, storage account e compartilhamento de arquivos do azure
- Autentica automaticamente

▼ Az Powershell and CLI

▼ Azure PowerShell

- Podemos executar todas ações que realizamos no portal através do powershell

- Mais Agil que a interface grafica
- Modulo do azure → AZ
- Disponível para navegador, instalado nativo no windows, mas também tem o powershell core para linux e macos
- Tem um mode interativo e um de script
- Comando powershell :
 - `New-AzVM -ResourceGroupName "crmtestingResourceGroup" -Name "crmUnitTest" -Image "UbuntuLTS"`
 - Comando irá criar uma VM ubuntu no RG crmtestingResourceGroup
 - Podemos contatenar os comandos

▼ Powershell Cmdlets and modules

- Os cmdlets seguem uma convenção de nomenclatura verbo-substantativo. enviado em módulos
- cmdlets → Get, new, etc.
- Modulo → Az, msol, ms, exg
- Dependendo do tipo de modulo precisaremos importar
- Módulos são um arquivo DLL com o código para processar cada cmdlet
- Use Get-Modules para ver uma lista de módulos carregados

▼ Az CLI

- Começa com AZ + nome do recurso + Flags indicando RG + descrição do recurso
 - `az vm restart -g myresourcegroup -n myvm`
- Mais voltado para quem está acostumado a trabalhar com bash
- Programa de linha de comando de plataforma cross
- Executa no linux, macOS e windows
- Pode ser usado interativamente ou através de scripts
- Use Find para localizar comandos
- Use -help para informações mais detalhadas
- CLI → bash, começa com AZ
- Powershell → cmdlets + modulo

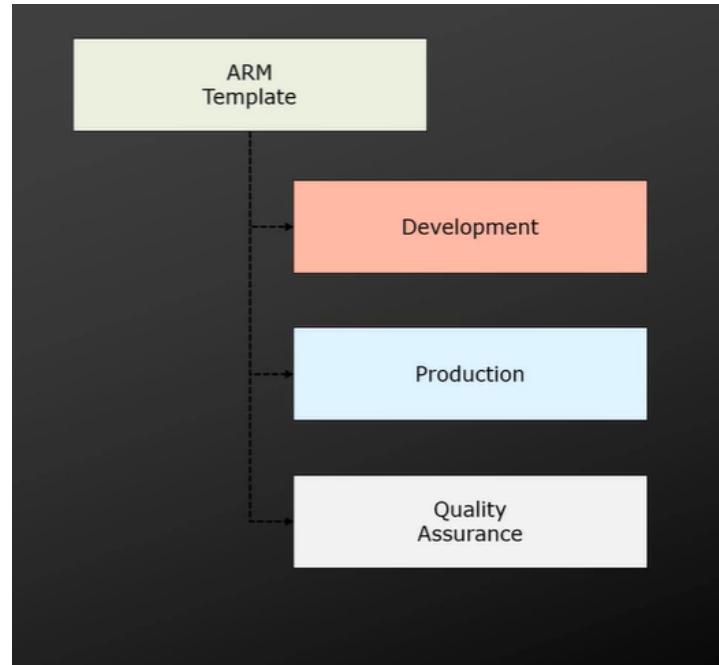
▼ ARM Templates

- IaC
- Trabalhar com códigos
- Podemos usar templates já prontos e modificar as partes que nos interessam

▼ Template Advantages (Vantagens)

- Melhora a consistência
- Expressa implantações complexas
- Reduz Tarefas manuais propensas a erros
- Expressar requisitos por meio de código
- Promove a reutilização
- Modular e pode ser vinculado

- Simplifica a orquestração



- Em vez de criar tudo via portal, com o script de automação, podemos definir uma criação complexa de uma infraestrutura para um determinado ambiente
- ARM → Linkado ao Resource Manager
- Podemos exportar as configurações
- automatização de CI/CD → Devops → ARM template auxilia
 - Terraform
 - VisualStudio Code
 - Ambiente de armazenamento de código como github, gitlabs, bitbucket

▼ Template Schema

- Define todos os recursos do Resource Manager em uma implantação
- Escrito em JSON
- Uma Coleção de pares de valores-chave
- Cada chave é uma string

```
{ Versão
  "$schema": "http://schema.management.
    azure.com/schemas/2019-04-
    01/deploymentTemplate.json#",
  "contentVersion": "",
  "parameters": {},
  "variables": {},
  "functions": [],
  "resources": [],
  "outputs": {}
}
```

O que iremos utilizar

- Schema → Declaração da forma que estaremos trabalhando com o nosso template
 - Primeiro item → Menção ao versionamento
- O resto serão estrutura de valores que iremos utilizar (recursos, funções, variáveis etc.)
- Nem todos os objetos são obrigatórios
- Recurso é obrigatório pois será com aquilo que estaremos trabalhando

```

"parameters": {
    "adminUsername": {
        "type": "string",
        "metadata": {
            "description": "Username for the VM."
        }
    },
    "adminPassword": {
        "type": "securestring",
        "metadata": {
            "description": "Password for the VM."
        }
    }
}

```



Definição de senha

- Parâmetros serão aquilo que iremos declarar para um determinado recurso, no exemplo acima se trata de uma VM que terá os parâmetros de usuário e senha

▼ Template Variables

- Definir valores usados em todo o modelo
- Facilita a manutenção de seus modelos

```

"variables": {
    "nicName": "VMNic01",
    "addressPrefix": "10.0.0.0/16",
    "subnetName": "Subnet01",
    "subnetPrefix": "10.0.0.0/24",
    "publicIPAddressName": "PublicIP01",
    "virtualNetworkName": "VNET-PRD"
}

```

- Este exemplo fornece variáveis que descrevem os recursos de rede para uma máquina virtual
- Variáveis são criadas
- No caso com esse template estamos declarando os valores necessários para a criação do recurso

▼ Template Functions

- Procedimentos reutilizáveis dentro do código

- Usada para não haver tanta repetição no código
 - Para que não precisemos escrever demais, utilizamos a function que será chamada quando requisitada em outras linhas
 - Facilita a manutenção do modelo

```
"functions": [
  {
    "namespace": "tftec",
    "members": {
      "uniqueName": {
        "parameters": [
          {
            "name": "namePrefix",
            "type": "string"
          }
        ],
        "output": {
          "type": "string",
          "value": "[concat(toLower(parameters('namePrefix')), uniqueString(resourceGroup().id))]"
        }
      }
    }
  }
]
```

- Esta função cria um nome exclusivo - use ao criar recursos que possuem requisitos de nomenclatura globalmente exclusivos
 - No caso (concat) está concatenando o código com o nameprefix, com o id do RG, e o name não irá se repetir

▼ Tamplate Resources

- Defina os recursos do azure que compõem sua implantação
 - Criando um IP publico, vnet, vm
 - Este exemplo que cria um recurso de endereço IP público
 - Nome é uma variável
 - Localização é um parâmetro

```
{
  "type": "Microsoft.Network/publicIPAddresses",
  "name": "[variables('publicIPAddressName')]",
  "location": "[parameters('location')]",
  "apiVersion": "2018-08-01",
  "properties": {
    "publicIPAllocationMethod": "Dynamic", config
    "dnsSettings": {
      "domainNameLabel": "[parameters('dnsLabelPrefix')]"
    }
  }
}
```

▼ Tamplate Outputs

- Defina qualquer informação que você gostaria de receber quando o modelo for executado
 - O que vai mostrar na tela

```
"outputs": {
  "hostname": {
    "type": "string",
    "value": "[reference(variables('publicIPAddressName')).dnsSettings.fqdn]"
  }
}
```

- Este exemplo recebe o endereço IP ou o FQDN de uma VM
- Nome do host é a saída
- O valor do FQDN é lido nas configurações de endereço IP public das vms

▼ Quickstart Tamplates

- ARM Templates fornecidos pela comunidade - Tamplates já prontos para a utilzação

Browse code samples

Get started with Microsoft developer tools and technologies. Explore our samples and discover the things you can build.

 <https://learn.microsoft.com/en-us/samples/browse/?expanded=azure&products=azure-resource-manager>



Deploy a simple Windows VM

Code Sample • 02/06/2023 • 6 contributors

[Browse code](#)

Validar o repositório

Azure Public Test Date 2023.02.02 Azure Public Test Result pass

Azure US Gov Test Date 2023.02.02 Azure US Gov Test Result pass

Best Practice Check pass CredScan Check Not Tested

Bicep Version 0.14.6

Deploy no ambiente

Visualizar o mapa (desenho do esquema)

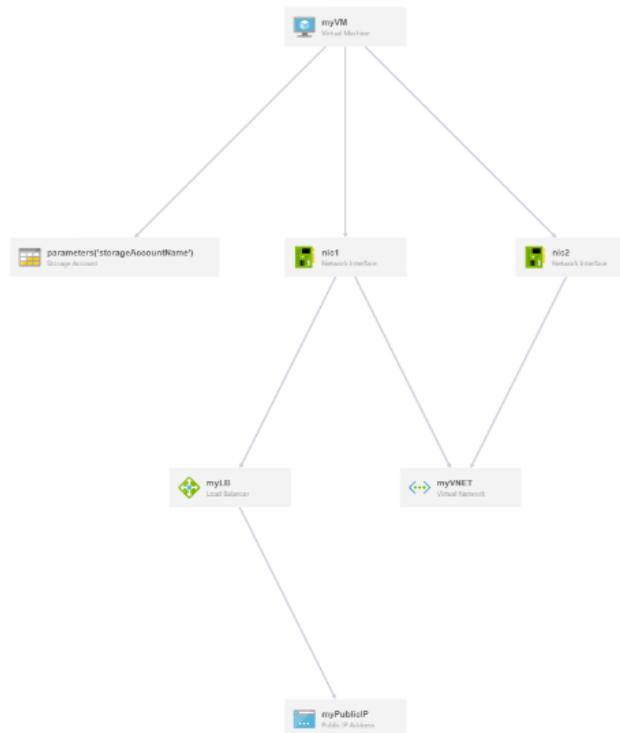
[Deploy to Azure](#)

[Deploy to Azure Gov](#)

[Visualize](#)

This template allows you to deploy a simple Windows Generation 2 VM using a few different options for the Windows version, using the latest patched version. This will deploy a D2s_v3 size VM in the resource group location and return the fully qualified domain name of the VM.

If you're new to Azure virtual machines, see:



```
{  
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "storageAccountName": {
```

```

    "type": "string",
    "metadata": {
        "description": "Name of storage account"
    }
},
"adminUsername": {
    "type": "string",
    "metadata": {
        "description": "Admin username"
    }
},
"adminPassword": {
    "type": "securestring",
    "metadata": {
        "description": "Admin password"
    }
},
"dnsNameforLBIP": {
    "type": "string",
    "metadata": {
        "description": "DNS for Load Balancer IP"
    }
},
"vmSize": {
    "type": "string",
    "defaultValue": "Standard_D2",
    "metadata": {
        "description": "Size of the VM"
    }
}
},
"variables": {
    "storageAccountType": "Standard_LRS",
    "addressPrefix": "10.0.0.0/16",
    "subnetName": "Subnet-1",
    "subnetPrefix": "10.0.0.0/24",
    "publicIPAddressType": "Dynamic",
    "nic1NamePrefix": "nic1",
    "nic2NamePrefix": "nic2",
    "imagePublisher": "MicrosoftWindowsServer",
    "imageOffer": "WindowsServer",
    "imageSKU": "2012-R2-Datacenter",
    "vnetName": "myVNET",
    "publicIPAddressName": "myPublicIP",
    "lbName": "myLB",
    "vmNamePrefix": "myVM",
    "vnetID": "[resourceId('Microsoft.Network/virtualNetworks',variables('vnetName'))]",
    "subnetRef": "[concat(variables('vnetID'), '/subnets/', variables('subnetName'))]",
    "publicIPAddressID": "[resourceId('Microsoft.Network/publicIPAddresses',variables('publicIPAddressName'))]",
    "lbID": "[resourceId('Microsoft.Network/loadBalancers',variables('lbName'))]",
    "frontEndIPConfigID": "[concat(variables('lbID'), '/frontendIPConfigurations/LoadBalancerFrontEnd')]",
    "lbPoolID": "[concat(variables('lbID'), '/backendAddressPools/BackendPool1')]"
},
"resources": [
{
    "type": "Microsoft.Storage/storageAccounts",
    "name": "[parameters('storageAccountName')]",
    "apiVersion": "2015-05-01-preview",
    "location": "[resourceGroup().location]",
    "properties": {
        "accountType": "[variables('storageAccountType')]"
    }
},
{
    "apiVersion": "2015-05-01-preview",
    "type": "Microsoft.Network/publicIPAddresses",
    "name": "[variables('publicIPAddressName')]",
    "location": "[resourceGroup().location]",
    "properties": {
        "publicIPAllocationMethod": "[variables('publicIPAddressType')]",
        "dnsSettings": {
            "domainNameLabel": "[parameters('dnsNameforLBIP')]"
        }
    }
},
{
    "apiVersion": "2015-05-01-preview",
    "type": "Microsoft.Network/virtualNetworks",
    "name": "[variables('vnetName')]"
}
]

```

```

"location": "[resourceGroup().location]",
"properties": {
    "addressSpace": {
        "addressPrefixes": [
            "[variables('addressPrefix')]"
        ]
    },
    "subnets": [
        {
            "name": "[variables('subnetName')]",
            "properties": {
                "addressPrefix": "[variables('subnetPrefix')]"
            }
        }
    ]
},
{
    "apiVersion": "2015-05-01-preview",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('nic1NamePrefix')]",
    "location": "[resourceGroup().location]",
    "dependsOn": [
        "[concat('Microsoft.Network/virtualNetworks/', variables('vnetName'))]",
        "[concat('Microsoft.Network/loadBalancers/', variables('lbName'))]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Dynamic",
                    "subnet": {
                        "id": "[variables('subnetRef')]"
                    },
                    "loadBalancerBackendAddressPools": [
                        {
                            "id": "[concat(variables('lbID'), '/backendAddressPools/BackendPool1')]"
                        }
                    ],
                    "loadBalancerInboundNatRules": [
                        {
                            "id": "[concat(variables('lbID'), '/inboundNatRules/RDP-VM0')]"
                        }
                    ]
                }
            }
        ]
    }
},
{
    "apiVersion": "2015-05-01-preview",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('nic2NamePrefix')]",
    "location": "[resourceGroup().location]",
    "dependsOn": [
        "[concat('Microsoft.Network/virtualNetworks/', variables('vnetName'))]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Dynamic",
                    "subnet": {
                        "id": "[variables('subnetRef')]"
                    }
                }
            }
        ]
    }
},
{
    "apiVersion": "2015-05-01-preview",
    "name": "[variables('lbName')]",
    "type": "Microsoft.Network/loadBalancers",
    "location": "[resourceGroup().location]",
    "dependsOn": [
        "[concat('Microsoft.Network/publicIPAddresses/', variables('publicIPAddressName'))]"
    ]
}

```

```

    ],
    "properties": {
        "frontendIPConfigurations": [
            {
                "name": "LoadBalancerFrontEnd",
                "properties": {
                    "publicIPAddress": {
                        "id": "[variables('publicIPAddressID')]"
                    }
                }
            }
        ],
        "backendAddressPools": [
            {
                "name": "BackendPool1"
            }
        ],
        "inboundNatRules": [
            {
                "name": "RDP-VM0",
                "properties": {
                    "frontendIPConfiguration": {
                        "id": "[variables('frontEndIPConfigID')]"
                    },
                    "protocol": "tcp",
                    "frontendPort": 50001,
                    "backendPort": 3389,
                    "enableFloatingIP": false
                }
            }
        ]
    }
},
{
    "apiVersion": "2015-06-15",
    "type": "Microsoft.Compute/virtualMachines",
    "name": "[variables('vmNamePrefix')]",
    "location": "[resourceGroup().location]",
    "dependsOn": [
        "[concat('Microsoft.Storage/storageAccounts/', parameters('storageAccountName'))]",
        "[concat('Microsoft.Network/networkInterfaces/', variables('nic1NamePrefix'))]",
        "[concat('Microsoft.Network/networkInterfaces/', variables('nic2NamePrefix'))]"
    ],
    "properties": {
        "hardwareProfile": {
            "vmSize": "[parameters('vmSize')]"
        },
        "osProfile": {
            "computerName": "[variables('vmNamePrefix')]",
            "adminUsername": "[parameters('adminUsername')]",
            "adminPassword": "[parameters('adminPassword')]"
        },
        "storageProfile": {
            "imageReference": {
                "publisher": "[variables('imagePublisher')]",
                "offer": "[variables('imageOffer')]",
                "sku": "[variables('imageSKU')]",
                "version": "latest"
            },
            "osDisk": {
                "name": "osdisk",
                "vhd": {
                    "uri": "[concat('http://', parameters('storageAccountName'), '.blob.core.windows.net/vhds/', 'osdisk', '.vhf')]"
                },
                "caching": "ReadWrite",
                "createOption": "FromImage"
            }
        },
        "networkProfile": {
            "networkInterfaces": [
                {
                    "properties": {
                        "primary": true
                    },
                    "id": "[resourceId('Microsoft.Network/networkInterfaces', variables('nic1NamePrefix'))]"
                },
                {
                    "properties": {
                        "primary": false
                    }
                }
            ]
        }
    }
}
]

```

```

        },
        "id": "[resourceId('Microsoft.Network/networkInterfaces', variables('nic2NamePrefix'))]"
    ],
},
"diagnosticsProfile": {
    "bootDiagnostics": {
        "enabled": "true",
        "storageUri": "[concat('http://', parameters('StorageAccountName'), '.blob.core.windows.net')]"
    }
}
}
]
}
}

```

▼ Regiões disponíveis para criar VMs B2S com conta trial

(Europe) - UK South(Europe) - UK West(Asian Pacific) - Australia East(Asian Pacific) - Australia Central(Asian Pacific) - Japan East(Asian Pacific) - Korea Central(Asian Pacific) - East Asian

Sintaxe para alterar nos scripts:

uksouth
ukwest
japaneast
australiaeast
koreacentral
australiacentral
eastasia

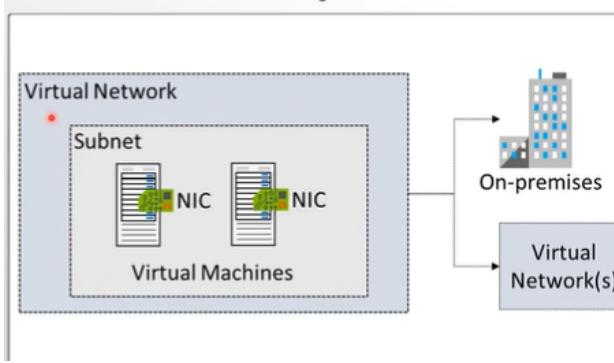
▼ MD4 → Virtual Networking

▼ Virtual Networks

▼ Azure Networking Components

- Adoção de soluções em nuvem pode economizar tempo e simplificar as operações
- O azure requer os mesmo tipos de funcionalidade que a infra local
- A rede do azure oferece diversos serviços
 - Traffic manager → controle de tráfego que está chegando
 - Virtual Network Gateway → base para conexão entre o ambiente onpremises com a nuvem
 - Virtual Wan → Link ponta a ponta entre redes
 - Virtual network → Estrutura de rede na nuvem para um determinado ambiente, não é possível criar vms sem uma estrutura de rede
 - Load Balancer → faz as distribuições de carga, trabalha somente com IP, e possui somente um pool
 - Application Gateway → Semelhante ao load balancer, mas com uma camada extra de proteção, trabalha na camada 7, faz direcionamento de urls para servidores

▼ Virtual Networks



- VNET → Representação da rede local.
 - vnet → /16
 - subnets → /24
- Cada subnet tem um tráfego exclusivo
- Estende seu datacenter com segurança com redes virtuais
- Por ela utilizasse para o formato híbrido
- Vnet → Enlace como um todo
- subnet → por onde as vms e os demais recursos irão se conectar

▼ Subnets

- A vnet pode ser segmentada em subnets
- As subnets fornecem divisões lógicas na sua rede
- GatewaySubnet → utilizado para saída e acesso a uma on premisses
 - A GatewaySubnet é uma subnet especial em uma rede virtual que é usada para hospedar o Gateway VPN, o Gateway de Aplicativo e outros tipos de gateways. É obrigatório criar uma GatewaySubnet para cada rede virtual que utiliza um gateway VPN ou de aplicativo. A subnet é configurada com o tipo de gateway apropriado durante a criação do Gateway VPN ou de Aplicativo.
- Cada subnet deve ter um intervalo de endereços exclusivos, não pode se sobrepor a outras sub-redes na rede virtual da assinatura
- É possível criar regras de redirecionamento

▼ Implementing Virtual Networks

Para criar uma rede virtual (VNet) no Azure, siga os seguintes passos:

1. Acesse o portal do Azure
2. Selecione "Criar um recurso"
3. Na barra de pesquisa, digite "Rede Virtual"
4. Selecione "Rede Virtual" nos resultados da pesquisa
5. Clique em "Criar"
6. Preencha as informações necessárias, como nome, região, espaço de endereços de rede e sub-redes
7. Clique em "Revisar e criar"
8. Verifique as informações e clique em "Criar"

Pronto! Sua rede virtual foi criada e agora você pode configurar suas sub-redes e outros recursos de rede.

- A vnet sempre deverá estar em um RG
- É preciso pensar em uma estrutura grande ao denominar os nomes
- /16 é o range de enderençamento ideal pois será onde se colocará as subnets
- É preciso se atentar com overlapping
 - Overlapping é quando dois ou mais intervalos de endereços IP se sobrepõem, o que pode causar problemas ao tentar rotear o tráfego de rede. É importante evitar o overlapping para garantir que a rede funcione corretamente.
- Por padrão o tráfego de padrão duas vnets em diferentes RGs ou no mesmo não se comunicam, para que ambas se comuniquem é necessário a utilização do peering
 - Peering é uma conexão direta entre duas redes virtuais no Azure que permite que o tráfego de rede fluia livremente entre elas. Isso é útil quando você deseja conectar redes virtuais em diferentes regiões ou assinaturas, ou se deseja conectar redes virtuais em diferentes modelos de implantação (clássico ou Resource Manager).
- Isolar tráfego, o ideal é criar diferentes vnets
 - Porém é possível isolar dentro das subnets, com a utilização dos NSGs

▼ IP Address

▼ IP Addressing



- Muitos recursos utilizam o IP
- Há dois tipos de endereçamento
 - Privado - dentro da rede, on-premises, vnet, vpn gateways, expressroute
 - Público - usado para comunicação com a internet incluindo serviços públicos do Azure, load balancer, para acessar VMs na conta gratuita temos que colocar ip público.

▼ Creating IP Address

Existem duas maneiras de criar endereços IP no Azure: público e privado.

Endereço IP público

Para criar um endereço IP público no Azure, siga os seguintes passos:

1. Acesse o portal do Azure
2. Selecione "Criar um recurso"
3. Na barra de pesquisa, digite "Endereço IP público"
4. Selecione "Endereço IP público" nos resultados da pesquisa
5. Clique em "Criar"
6. Preencha as informações necessárias, como nome e região
7. Clique em "Revisar e criar"
8. Verifique as informações e clique em "Criar"

Pronto! Seu endereço IP público foi criado e agora pode ser usado para se comunicar com a internet, bem como com outros recursos no Azure.

Endereço IP privado

Para criar um endereço IP privado no Azure, é necessário criar uma sub-rede dentro de uma rede virtual (VNet). Cada sub-rede tem um intervalo de endereços IP exclusivo que pode ser usado para atribuir endereços IP privados a recursos na sub-rede.

Para criar uma sub-rede com um intervalo de endereços IP privado, siga os seguintes passos:

1. Acesse o portal do Azure
2. Selecione "Criar um recurso"
3. Na barra de pesquisa, digite "Rede Virtual"
4. Selecione "Rede Virtual" nos resultados da pesquisa
5. Clique em "Criar"
6. Preencha as informações necessárias, como nome, região, espaço de endereços de rede e sub-redes
7. Clique em "Revisar e criar"
8. Verifique as informações e clique em "Criar"

Pronto! Sua sub-rede com um intervalo de endereços IP privado foi criada e agora pode ser usada para atribuir endereços IP privados a recursos na sub-rede.

- Criando IP publico
 - Podemos utilizar o IPv4 ou IPv6
 - SKU → Modelo do IP
 - Basic → Dinamico (pode mudar), ou estatico
 - Standard → Sempre estatico, não muda, mais caro, independente da zona, se migrar o IP não vai mudar
→ Redun

▼ Public IP Address

Um endereço IP público no Azure é um endereço IP que pode ser usado para se comunicar com a Internet e com outros recursos no Azure. Ele pode ser criado em SKU Basic (dinâmico ou estático) ou SKU Standard (sempre estático e independente da zona). O endereço IP público é necessário para acessar recursos na nuvem a partir da Internet, como máquinas virtuais ou serviços do Azure.

- Um Recurso de IP publico pode ser associado a interfaces de rede de vms, load balancer voltado para internet, gateway VPN e gateway de apps
- IP estatico é apropriado de usar quando
 - Precisa de regras de firewall para se comunicar com os recursos do azure
 - Resolução de nomes
 - Comunicação entre recursos com outros aplicativos ou serviços baseados em IP

▼ Private IP Address

O endereço IP privado no Azure é um endereço IP que é usado para se comunicar dentro da rede virtual ou entre redes virtuais. Cada sub-rede possui um intervalo de endereços IP privados exclusivo que pode ser usado para atribuir endereços IP privados a recursos na sub-rede.

- IP que não vai ser resolvido externamente, não é visível da rua, somente interno
- Podemos comunicar o IP privado com a rede on-premises através da vpn ou express route

- Não posso usar IP publico para acessar as vms, como acessar?
 - VPN → site-to-site → do datacenter com a nuvem
 - VPN → point-to-site → client no pc, para acessar a rede
 - Bastion → Gateway de conexão, acesso via porta 443, a partir dele o acesso é feito pelo browser
 - Custo alto
- IP privado possui o mesmo padrão
 - Dynamic → on premisses geralmente não é problema, exceto quando se trata de servidores de acesso
 - Static → podemos modificar o IP para estatica, mas não é pela maquina, realizamos através do portal do azure, pelo DNS podemos alterar também.

▼ Network Security Groups

NSG significa Grupo de Segurança de Rede. É um recurso do Azure que permite controlar o tráfego de entrada e saída em uma interface de rede, sub-rede ou máquina virtual. Os NSGs funcionam como um firewall, permitindo ou negando comunicações com base em regras e filtros. Eles podem ser usados para controlar o tráfego entre as camadas 3 e 4 do modelo OSI.

- Filtragem de pacotes, semelhante a um firewall
- Limitar o tráfego de rede aos recursos em uma rede virtual
- Possui uma lista de regras de entrada e saída
- Pode ser associado a uma sub-rede ou interface de rede (NIC)
 - Não é aplicado para a VNET

▼ NSG Rules

- As regras são inbound ou outbound
- Algumas regras são padrão no NSG e não são excluíveis
- As regras de segurança nos NSGs permitem filtrar o tráfego de rede que pode fluir dentro e fora das subnets e interface de rede virtuais

▼ NSG Effective Rules

- Os NSGs podem ser aplicados em até dois níveis, na subnet e na NIC da VM
- Deve haver regras de permissão nos dois níveis
- Use o link de regras efetivas se não tiver certeza de quais regras de segurança estão sendo aplicadas

▼ Creating NSG Rules

Para criar uma regra de NSG no azure, siga os seguintes passos:

1. Acesse o portal do Azure
2. Selecione o recurso de rede virtual ou interface de rede (NIC) ao qual deseja aplicar o NSG
3. No menu, clique em "Grupos de segurança de rede"
4. Clique em "Adicionar" para criar um novo NSG ou selecione um NSG existente
5. Para criar uma nova regra, clique em "Adicionar uma regra de entrada" ou "Adicionar uma regra de saída"
6. Preencha as informações necessárias:
 - Nome: nome da regra
 - Prioridade: número que define a ordem de processamento da regra, quanto menor o número, maior a prioridade

- Origem: origem do tráfego. Pode ser um endereço IP, um intervalo de endereços ou qualquer
 - Protocolo: protocolo de rede como TCP, UDP ou * para todos
 - Porta de origem: porta de origem do tráfego
 - Porta de destino: porta de destino do tráfego
 - Ação: permitir ou negar o tráfego
 - Descrição: descrição opcional da regra
7. Clique em "Adicionar" para salvar a regra
 8. As regras são processadas na ordem de prioridade, da maior para a menor. Certifique-se de que as regras mais restritivas tenham as prioridades maiores.

Pronto! Sua regra de NSG foi criada e agora o tráfego de rede será filtrado de acordo com as regras definidas.

- Service → O protocolo de destino e o intervalo de portas para esta regra
- Port Ranges → Porta única ou varias portas
- Priority → Quanto menor o número, maior a prioridade

▼ Application Security Groups

Application security groups (ASGs) são um recurso do Azure que permite agrupar recursos de computação como máquinas virtuais para aplicar regras de segurança de rede e controle de acesso comuns. As ASGs funcionam semelhante aos grupos de segurança de rede (NSGs), mas podem ser usadas para aplicar regras de segurança em recursos que estão em várias sub-redes.

- Permite reutilizar sua política de segurança em grande escala sem manutenção manual de endereços IP explícitos
- Lida com a complexidade de endereços IP explícitos e vários conjuntos de regras, permitindo que você se concentre na lógica de negócios

▼ Azure Firewall

O firewall do Azure funciona da seguinte forma:

1. Ele é implantado como um recurso de rede na sua assinatura do Azure. Você o implanta em uma sub-rede dentro de uma rede virtual do Azure.
2. O tráfego de entrada para a sua rede virtual é encaminhado automaticamente para o firewall do Azure para inspeção. O firewall aplica as regras e políticas de segurança definidas para determinar se o tráfego deve ser permitido ou negado.
3. O tráfego de saída da sua rede virtual também é encaminhado para o firewall do Azure. Ele aplica regras de controle de tráfego de saída para determinar se o tráfego deve ser permitido para a Internet.
4. O firewall do Azure também oferece monitoramento contínuo de tráfego e detecção de ameaças. Ele pode alertá-lo sobre atividades potencialmente mal-intencionadas e ajudá-lo a proteger seus recursos do Azure.
5. O firewall do Azure pode ser implantado em modo HA (alta disponibilidade) para alta resiliência. Ele também oferece logs de atividades de firewall detalhados que podem ser usados para monitoramento e auditoria.
 - Firewall stateful como um serviço - Validação do comportamento de pacote, faz análise de ponta a ponta, quem recebe e quem entrega. Se um app trabalha com a porta 443 e muda para a 3389, ele faz um bloqueio devido ao rastreamento de comportamento
 - Alta disponibilidade integrada com escalabilidade irrestrita na nuvem
 - Criar, importar e registrar políticas de conectividade de apps e rede
 - FireSwall é mais caro e seu nível de inteligência é maior do que o NSG que não é stateful
 - Integrado ao Azure monitor para log e análise

- Suporte para conectividade híbrida por meio de implantação atrás de VPN e ExpressRoute Gateway

▼ Implementing Firewalls

- Criar a infraestrutura de rede
- Implantar o firewall em uma subnet
- Criar as rotas padrões, para que passem pelo firewall
- Por fim criar as regras necessárias para cada aplicação

▼ Firewall Rules

- Regras NAT → Configurar regras DNAT para permitir conexões de entrada → Bate no firewall e faz a conversão de um IP externo para um IP interno
- Regras de rede → Configurar regras que contêm endereços de origem, protocolos, portas de destino e endereços de destino
- Regras de aplicação → Configurar nomes de domínio totalmente qualificados (FQDNs) que podem ser acessados a partir de uma sub-rede → Ao invés do IP, utiliza o nome de uma aplicação externa

▼ Azure DNS

▼ Domains and Custom Domains

- Por padrão sempre é criado um domínio no tenant domainname.onmicrosoft.com
- Porém podemos adicionar um domínio personalizado, quando vamos criar um custom domain o mesmo precisa ser verificado
- Assim quando o domínio customizado for adicionado e deixado como padrão, os usuários adicionados ao tenant terão o domínio na UPN

▼ Verifying Custom Domain Names

- Assim que o custom domain for adicionado o mesmo precisará ser verificado
- Os tipos de registros são MX ou TXT para validar a propriedade do domínio
- É necessário registrar no provedor do domínio (como hostgator)
- O tempo estimado pode ser de 5 minutos a 24h para validar

▼ Azure DNS Zones

- É um serviço de servidor de domínios onde hospeda os registro DNS de um domínio
- O Azure não é um registrador de nomes, para isso é necessário comprar o domínio em um registrador antes de adicioná-lo
- Caso não tenhamos, ainda sim podemos adicionar o domínio mas não irá resolver pois será necessário a verificação
- O nome da zona deve ser exclusivo dentro do RG
- Quando várias zonas compartilham o mesmo nome, cada instância recebe diferentes endereços de servidor DNS
- Somente um conjunto de endereços pode ser configurado com o registrador de nomes de domínio

▼ DNS Delegation

- Ao delegar um domínio ao DNS do Azure, você deve usar os nomes de servidor de nomes fornecidos pelo DNS do Azure - Use os quatro

- Depois que a zona DNS for criada atualize o registrador pai
- Para zonas filho , registre os registros NS no domínio pai

▼ DNS Record Sets

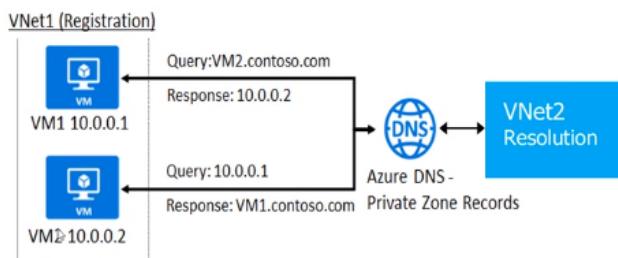
- Funciona como um loadbalancer de DNS
- Um conjunto de registros é uma coleção de registros em uma zona que tem o mesmo nome e é do mesmo tipo
- Você pode adicionar até 20 registros a qualquer conjunto de registros
- Um conjunto de registros não pode conter dois registros idênticos

▼ DNS for Private Domains

- Use seus próprios nomes de domínio personalizados
 - Dominios .local (Utilizada pela rede interna da empresa intranet)
- Fornece resolução de nomes para VMs dentro de uma VNet e entre VNets
 - Resolve internamente não externamente
- Gerenciamento automático de registros de nome de host
- Remove a necessidade de soluções DNS personalizadas
- Use todos os tipos comuns de registros DNS
- Disponível em todas as regiões do Azure

▼ Private Zones Scenarios

- A resolução de DNS na VNet1 é privada e não acessível pela internet



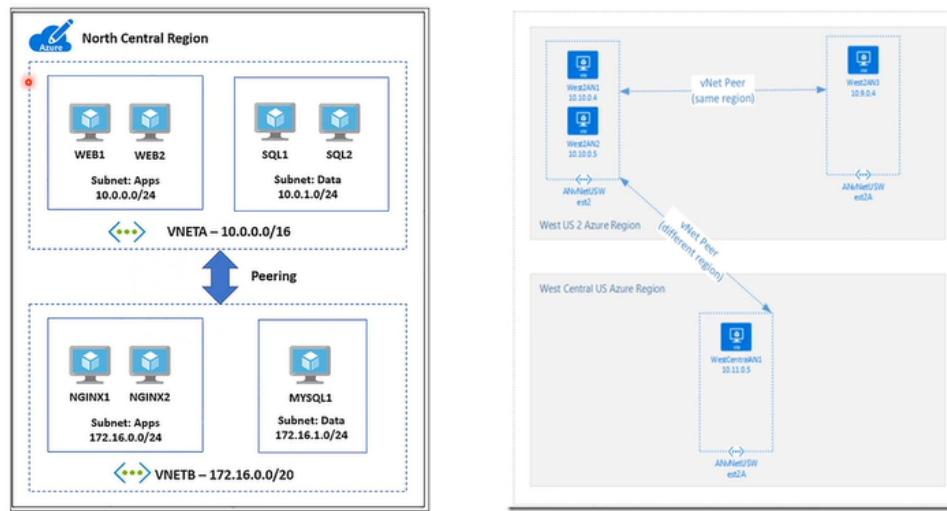
- As consultas DNS nas redes virtuais são resolvidas
- As consultas DNS reversas têm o escopo definido para a mesma rede virtual

▼ MD5 → Intersite Connectivity (Conexão entre VNETS)

- As VNETS não se comunicam por padrão
- A principal forma é habilitando uma configuração para que haja a comunicação

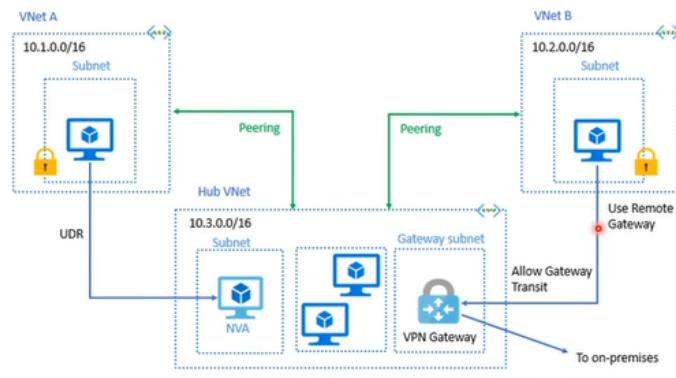
▼ VNet Peering

- O peering da VNet conecta duas VNets do Azure
- Dois tipos de peering
 - Regional → vnets na mesma regional
 - Global → Vnets em regiões diferentes
- Redes peering usam o backbone do azure para privacidade e isolamento
 - O tráfego é isolado dentro do ambiente MS
- Fácil de configurar, transferência contínua de dados e ótimo desempenho



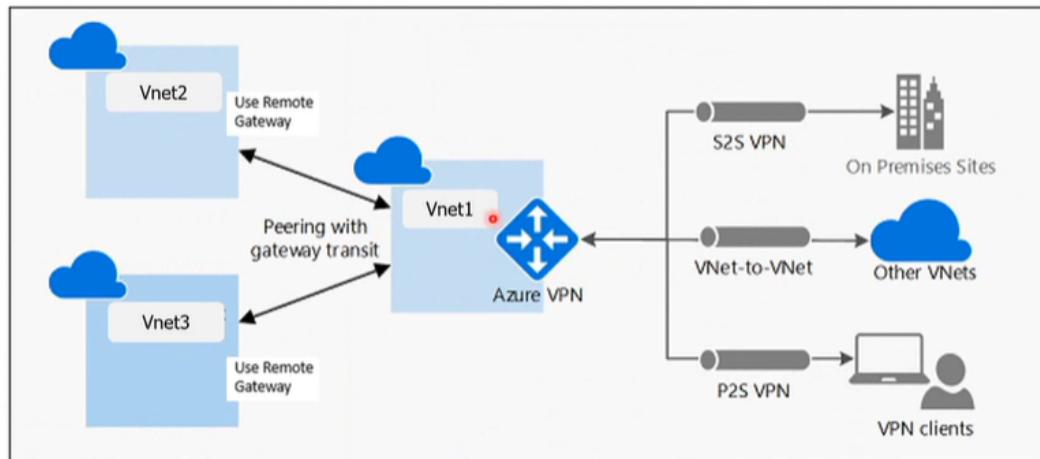
▼ Gateway Transit and Connectivity

- O transitividade de Gateway permite que Vnets com peering compartilhem o gateway e tenham acesso a recursos
 - Possibilitar que vnets utilizem o mesmo gateway
- Nenhum gateway VPN é necessário na rede virtual de peering
 - O VPN Gateway é apenas para realizar o segundo tráfego
- O endereçamento não pode se sobrepor, pois pode ocorrer overlapping
- O peering VNet padrão fornece conectividade total



▼ Configure VNet Peering

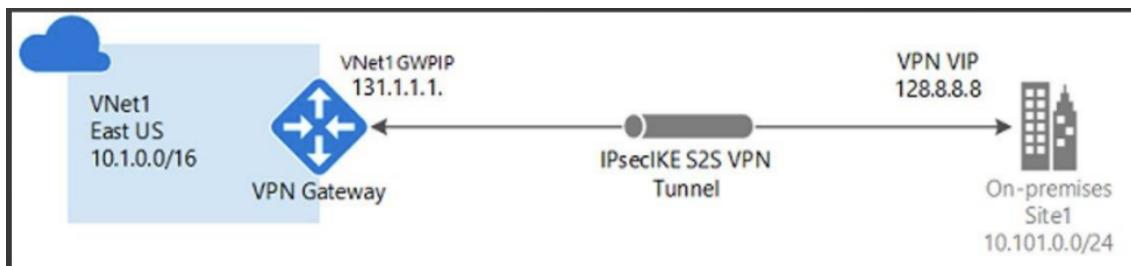
- Allow Forwarded traffic → de dentro da VNET com peering para sua VNET
- Allow gateway transit → Permite que a VNET com peering use seu virtual network gateway
- Use remote gateways → Uma VNET só pode ter um gateway, local ou remoto
- Se vc selecionar "Allow gateway transit" deve selecionar "use remote gateways" na outra vnet



▼ VPN Gateway Connections

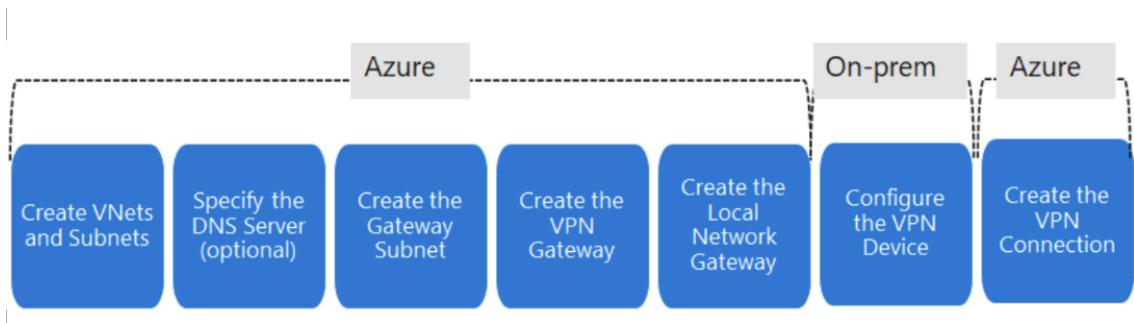
▼ VPN Gateways

- As conexões site-to-site conectam redes locais a redes do azure
- As conexões network-to-network conectam redes virtuais do azure
- As conexões point-to-site (VPN do usuario) conectam dispositivos individuais ás redes virtuais do azure



▼ Implement Site-to-Site VPN Connections

- Necessario planejamento para sua implantação
- A parte on premises só é necessaria em configurações site-to-site
- Verificar e testar conexões sempre que necessário



▼ Gateway Subnet

- O gateway de subnet contém os address IP ; se possível, use um bloco cidr de /28 ou /27
- Quando você cria uma subnet de gateway, o gateway das VMs são implantados na subnet de gateway e configuradas com as configurações de gateway de VPN necessárias.
- Nunca implante outros recursos (por exemplo, VMs adicionais) na subnet de gateway.
- Evite associar um NSG à subnet de gateway.

vnet01 - Subnets

Search (Ctrl+ /) <> + Subnet **+ Gateway subnet** Refresh

Add subnet

Name: GatewaySubnet

Address range (CIDR block) * ⓘ
10.1.255.0/27
10.1.255.0 - 10.1.255.31 (27 + 5 Azure reserved addresses)

NAT gateway ⓘ None

Network security group ⓘ None

Route table ⓘ None

Service endpoints

Services ⓘ 0 selected

Subnet delegation

Delegate subnet to a service ⓘ None

▼ VPN Gateway Configuration

- A maioria dos tipos de VPN são Route-based

- O SKU do gateway afeta o numero de conexões que podem haver e a taxa de transferencia agregada
- Associar uma VNet que inclui a subnet de gateway
- O gateway precisa de um public IP Address
- Pode demorar até 45 minutos para provisionar um gateway VPN

▼ VPN Gateway Types

- Route-based VPNs → rota da tabela de encaminhamento ou roteamento de IP para direcionar os pacotes
 - Suporta IKEv2
 - Pode usar protocolos dynamics
- Policy-based VPNs → criptografar e direcionar os pacotes através de tuneis ipsec com base nas diretivas ipsec
 - Dispositivos de vpn on premises legados
 - IKEv1

Create virtual network gateway

VPN type 
 Route-based Policy-based

A maioria das configurações do Gateway VPN requer Route-based

▼ VPN Gateway SKU and Generation

- SKU afeta as conexões e a taxa de transferencia
- Redimensionamento permitido dentro da geração
- SKU Básico é legado e não deve ser usado

Sampling of available SKUs

Gen	SKU	S2S/VNet-to-VNet Tunnels	P2S IKEv2 Connections	Throughput Benchmark
1	VpnGw1/Az	Max. 30	Max. 250	650 Mbps
1	VpnGw2/Az	Max. 30	Max. 500	1.0 Gbps
2	VpnGw2/Az	Max. 30	Max. 500	1.25 Gbps
1	VpnGw3/Az	Max. 30	Max. 1000	1.25 Gbps
2	VpnGw3/Az	Max. 30	Max. 1000	2.5 Gbps
2	VpnGw4/Az	Max. 30	Max. 5000	5.0 Gbps

▼ Local Network Gateway

- Define a configuração de rede local
- De ao site o nome pelo qual o azure possa referirse

- O gateway local precisa de public ip
- Especificar os prefixo de IP address que serão roteados através do gateway para o dispositivo VPN

Create local network gateway

Name *

 ✓

IP address * ⓘ

 ✓

Address space ⓘ

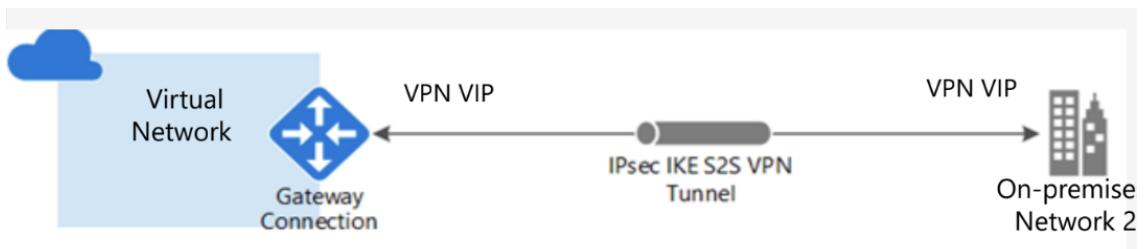
192.168.3.0/24 ***

Add additional address range ***

Configure BGP settings

▼ On-Premises VPN Devices

- Lista de dispositivos VPN suportados → redes cisco, juniper, barracuda
- Lembre-se da chave compartilhada da conexão do azure (próxima etapa)
- Especifique o endereço public ip (etapa anterior)



▼ VPN Connection

- Após a criação do gateway e os dispositivos configurados, será necessário criar um objeto de conexão
- Configure um nome para a conexão e especifique o tipo como site-to-site (IPsec)
- Selecione o VPN gateway e o local network gateway
- Digite a chave compartilhada para a conexão

The screenshot shows the 'Add connection' blade and the 'Choose local network gateway' blade side-by-side.

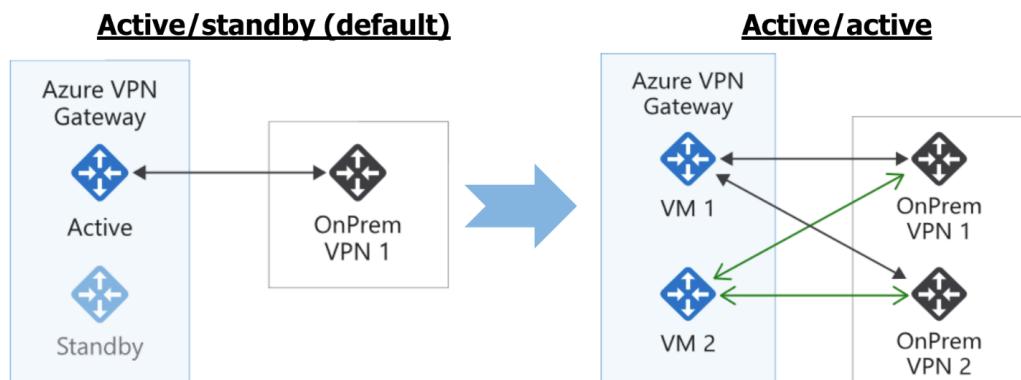
Add connection (Left):

- Name:** Azure-to-OnPrem
- Connection type:** Site-to-site (IPsec)
- *Virtual network gateway:** vng01
- *Local network gateway:** Azure-to-OnPrem
- Shared key (PSK):** abc123

Choose local network gateway (Right):

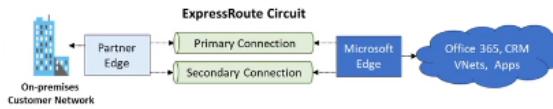
- Create new
- Azure-to-OnPrem NetworkRG

▼ High Availability Scenarios



- VPN gateways são implementados com 2 vms
- habilite active/active mode para alta disponibilidade (necessário ativar o BGP)
- Para uma manutenção planejada a conectividade deve ser restaurada dentro de 10 a 15s. Para os problemas não planejados, a recuperação da conexão será mais longa, aproximadamente de 1 minuto a 1 e meio

▼ ExpressRoute and Virtual WAN



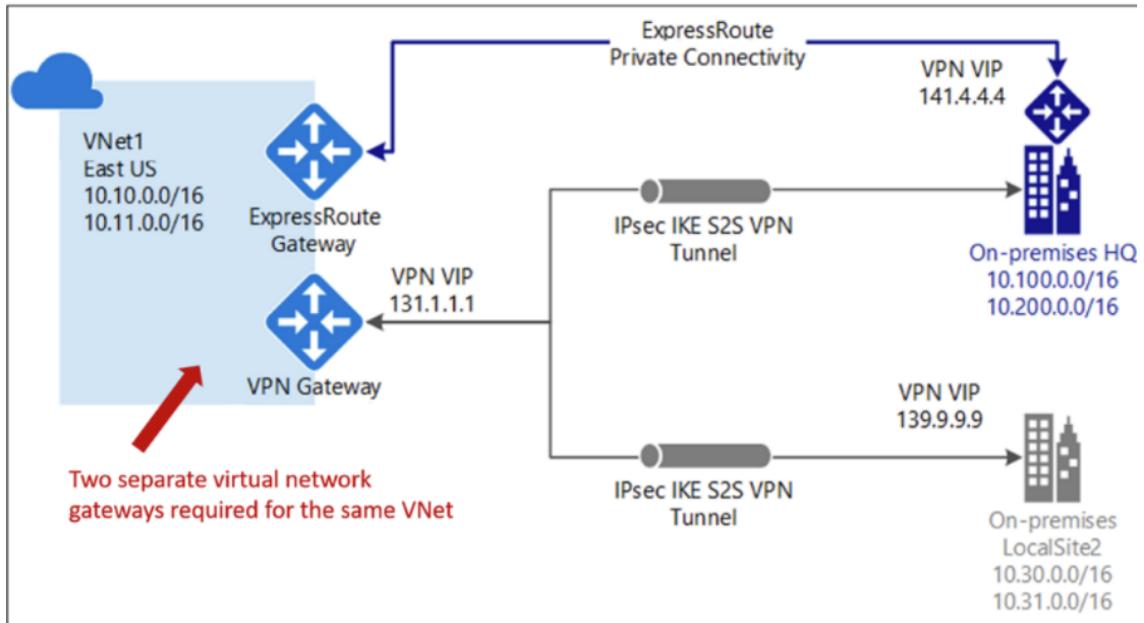
- Conexões privadas entre rede local e datacenters MS
 - Mais performático de todos
- Não passam pela internet publica - e sim rede de parceiros
 - Rota totalmente privada
- Seguro, confiável, de baixa latência e alta velocidade

▼ ExpressRoute Capabilities



- Conectividade de layer 3 com redundância
- Conectividade com todas as regiões dentro de uma região geográfica
- Conectividade global com o complemento premium ExpressRoute
- Opções de largura de banda 50Mbps a 100Gbps
- Modelos de faturamento - ilimitado, medido e premium
 - Ilimitado → Trafego ilimitado
 - Medido → Custo encima do que está trafegando
 - Premium → permite conexões com todas as regiões

▼ Coexisting Site-to-Site and Express Route



- Podemos ter conexão expressRoute e VPN S2S
 - Porém precisamos ter dois Virtual Network gateway (um pra vpn e outro pro expressRoute) na mesma VNet
 - Boa prática de contingência
- Use S2S VPN como um caminho de failover seguro para o expressroute
- Use s2s VPNs conectar-se a sites que não estão conectados a um expressroute

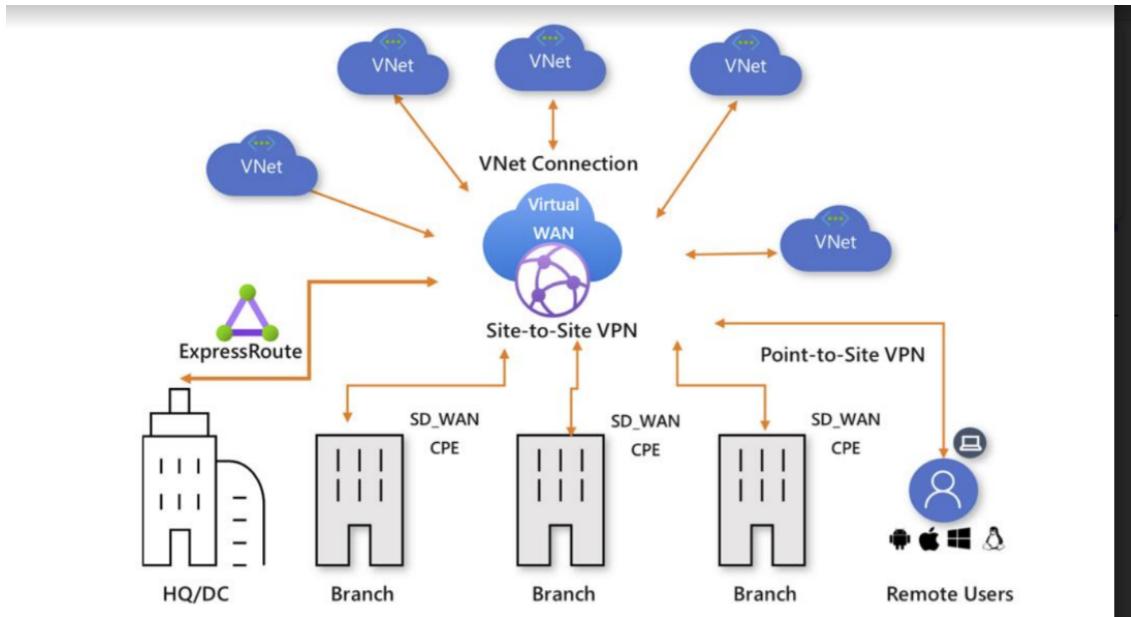
▼ Intersite Connection Comparisons

Connection	Azure services supported	Bandwidth	Protocols	Typical use case
Virtual network, point-to-site	Azure IaaS services, Azure Virtual Machines	Based on the gateway SKU	Active/passive	Ambientes de dev, teste e laboratório para serviços em nuvem e máquinas virtuais.
Virtual network, site-to-site	Azure IaaS services, Azure Virtual Machines	Typically < 1 Gbps aggregate	Active/passive Active/active	Ambientes de dev, teste e laboratório. Cargas de trabalho de produção em pequena escala e máquinas virtuais.
ExpressRoute	Azure IaaS and PaaS services, Microsoft Office 365 services	50 Mbps up to 100 Gbps	Active/active	Cargas de trabalho empresarial e de missão crítica. Soluções de big data.

- point-to-site → Azure IaaS e vms, baseado no sky do networking gateway, ativo passivo, ambientes de dev, testes, hml etc.
- site-to-site → IaaS e vms tbm, Geralmente abaixo de 1 Gps, ativo passivo ou ativo/ativo, para ambientes de dev, teste, hml, ou cargas de prd em escala
- expressRoute → IaaS Paas MS365, 50 Mbps para 100Gbps, ativo/ativo, cargas de trabalho empresarial e de missão crítica. Soluções de big data.

▼ Virtual WANs

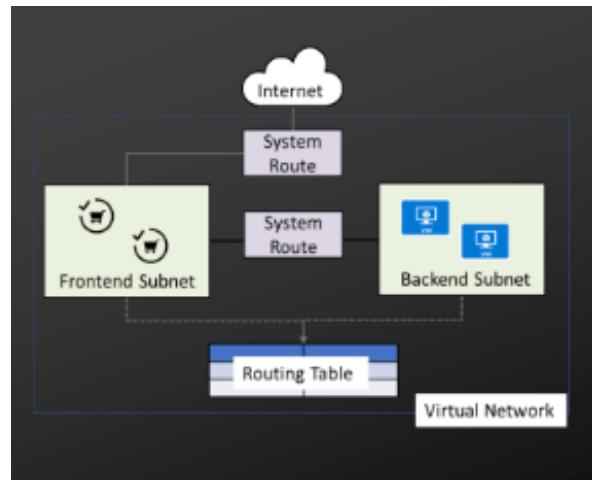
- Reúne S2S, P2S e express route
 - Atua como um gateway, todas as conexões chegam nele, um centralizador de conexões
- Conectividade integrada usando um modelo de conectividade hub-and-spoke
- Conecte redes virtuais e cargas de trabalho ao hub do azure automaticamente
- Visualize o fluxo de ponta a ponta no azure
- Dois tipos
 - Basic
 - Standard



▼ MD6 → Network Traffic Management

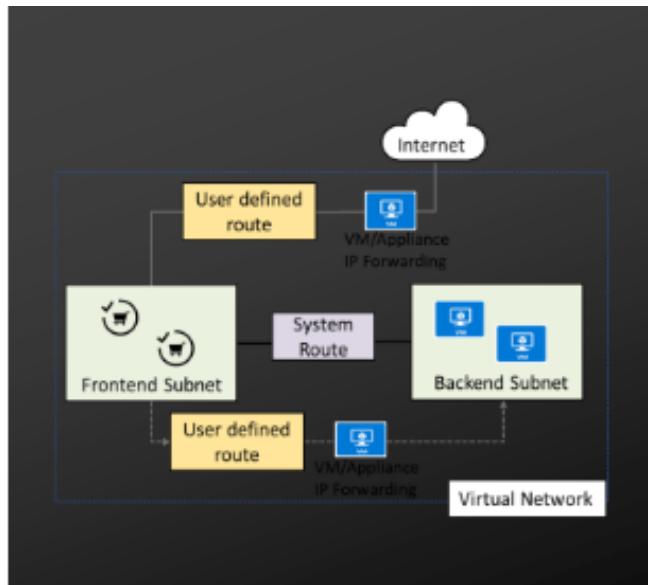
▼ Network Routing and Endpoints

▼ System Routes



- Roteia o tráfego de rede direto entre VMs, redes locais e a internet
 - Config padrão
 - Não definimos uma rota, elas vêm como padrão de forma automática
 - Rotas do sistema criada de forma automática
- Tráfego entre VMs na mesma subnet
- Entre VMs em diferentes subnets na mesma rede virtual
- Fluxo de dados das VMs para a Internet
 - Rota criada de forma automática
- Comunicação entre VMs usando uma VPN, VNet para VNet
- Comunicação Site-to-site e expressRoute através do gateway VPN
- Caso precisemos customizar rotas podemos realizar
- Rotas default, state active, endereçamento, e salto para um determinado lugar são as rotas criadas pelo próprio Azure
- Não é possível realizar alteração nas regras default mas podemos substituir

▼ User Defined Routes



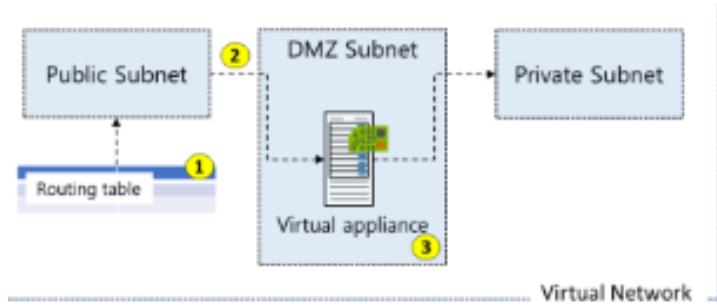
- Rotas criadas e regras de redirecionamento criadas de forma personalizada
- No exemplo acima temos rotas definidas, firewall na saída/entrada pra internet.
- O firewall possui um user defined route que manda para o frontend, que joga para outro user defined route, que passa pelo firewall e joga no backend subnet
- **Uma tabela de roteamento contém um conjunto de regras, chamadas rotas, que especifica como os pacotes devem ser roteados em uma rede virtual**
- **As User-defined routes são rotas personalizadas que controlam o tráfego de rede, definindo rotas que**

especificam o próximo salto do fluxo de tráfego

- O próximo salto pode ser um gateway de rede virtual, rede virtual, Internet ou dispositivo virtual
- UDR → podemos colocar o salto na tabela para jogar em um virtual appliance
 - UDR tem prioridade sobre a default

▼ Routing Example

- Todo o tráfego que entra na subnet public e dirigido para a subnet private deve passar pelo virtual appliance

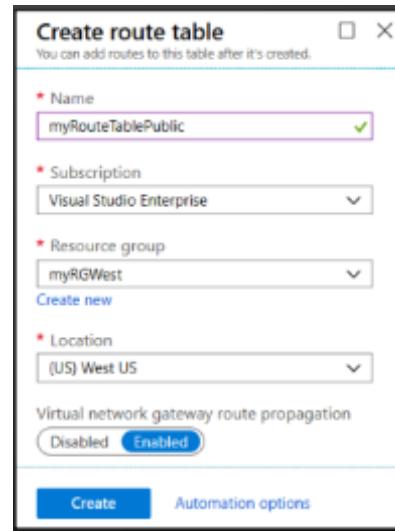


1. Crie uma tabela de roteamento
2. Adicione uma rota personalizada que exija que todo o tráfego de subnet private seja direcionado para um virtual appliance
3. Associe a nova rota à subnet public

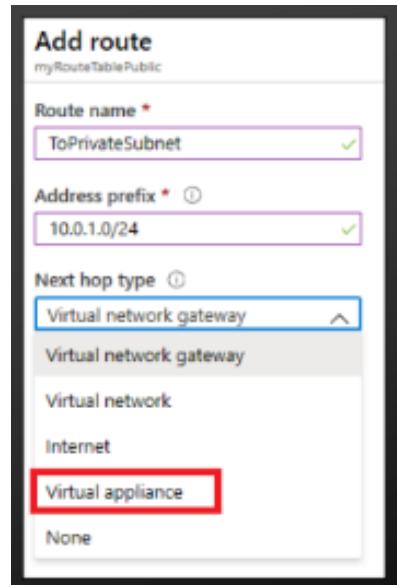
- No exemplo o que está ocorrendo é que há uma public subnet (frontend) e uma private subnet (backend), entre eles há um DMZ (virtual appliance) que seria um barramento para impedir acessos irrestritos a subnet privada
- A UDR faz com que o tráfego do frontend passe primeiro pelo virtual appliance antes de chegar no backend

▼ Create a Routing Table

- Um protocolo de roteamento padrão é usado para trocar informações de roteamento e acessibilidade entre duas ou mais redes
- As rotas são adicionadas automaticamente à tabela de rotas de todas as subnets com a propagação da rota do gateway de rede virtual habilitada



▼ Create a Custom Route



- Quando você cria uma rota, existem vários tipos de próximo salto
- Neste exemplo, qualquer endereço IP da subnet privada será enviado ao dispositivo virtual
- Outras opções são virtual network gateway, virtual network, Internet e nenhuma

▼ Associate the Route Table

Add subnet

VNet1

Name *
Public

Address range (CIDR block) *
10.0.1.0/24
10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

NAT gateway
None

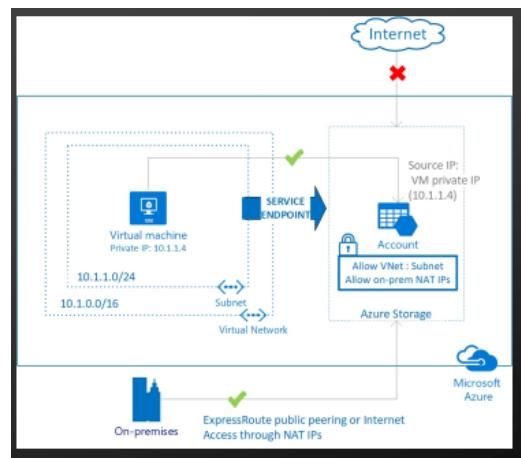
Add IPv6 address space

Network security group
None

Route table
myRouteTablePublic

- Cada subnet pode ter zero ou uma tabela de rota associada a ela
- No nosso exemplo, a subnet pública será associada à tabela de roteamento

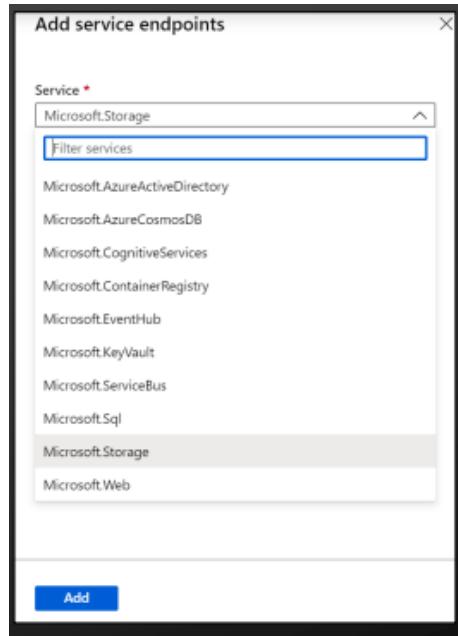
▼ Service Endpoints



- **Endpoints limitam o acesso da rede a subnets e endereços IP específicos**
 - Todo tráfego passe pelo datacenter para chegar em um determinado serviço sem precisar passar pela internet
 - O recurso ainda terá um IP Público
- **Segurança aprimorada para seus recursos de serviço do Azure**
- **Roteamento ideal para o tráfego de serviço do Azure da sua virtual network**
- **Os Endpoints usam a rede de backbone do Microsoft Azure**
- **Simples de configurar com menos sobrecarga de gerenciamento**
- É apenas autorizado, o endpoint já é criado por padrão, só é necessário habilitar

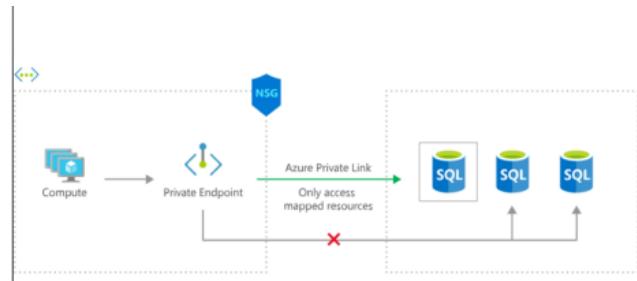
▼ Service Endpoint Services

- A adição de um service Endpoint pode levar até 15 minutos para ser concluída



▼ Private Link

- Tem o mesmo objetivo do service endpoint
 - Mas a diferença é que não haverá o private link
 - O tráfego será 100% interno
 - Suporta acesso VPN
 - Precisará de uma zona de DNS
- Conectividade privada a serviços no Azure. O tráfego permanece na rede da Microsoft, sem acesso à internet pública
- Integração com redes locais e peering
- No caso de um incidente de segurança na sua rede, apenas o recurso mapeado estaria acessível

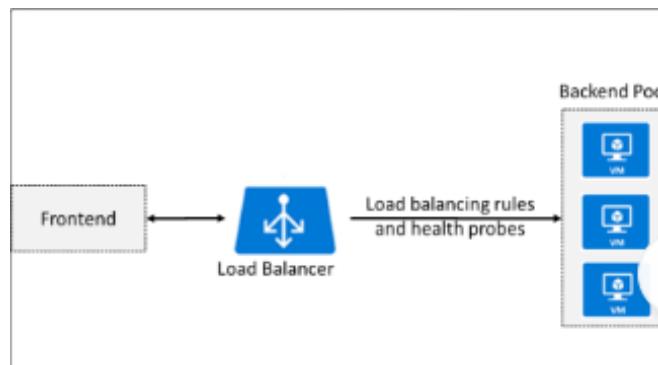


▼ Private Link vs Service Endpoint

- Private Link
 - Controle o acesso aos serviços PaaS pela rede privada

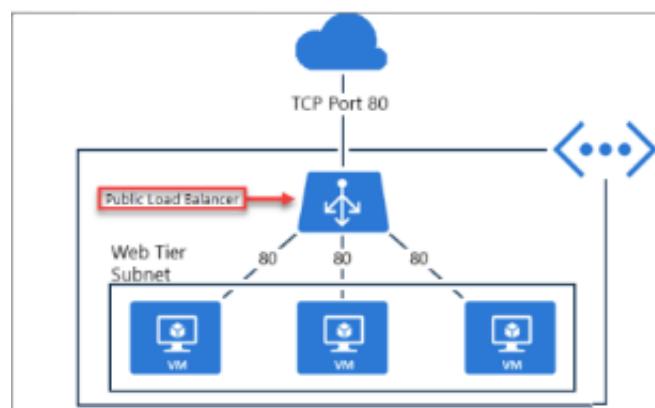
- VNET para instancia PaaS via backbone da MS
- Recurso PaaS mapeado para um endereço IP privado. NSGs são restritos ao espaço VNET
- Proteção embutida de exfiltração de dados
- Facilmente extensível para tráfego de rede local via expressroute ou VPN
- Service Endpoint
 - Controlo o acesso aos serviços PaaS pela internet pública
 - Vnet para serviço PaaS através do backbone da MS
 - O destino ainda é um endereço IP Público, NSG precisa ser aberto
 - O tráfego precisará ser passado por um NVA/fw para proteção de exfiltração
 - A restrição do tráfego local não é direta

▼ Azure Load Balancer



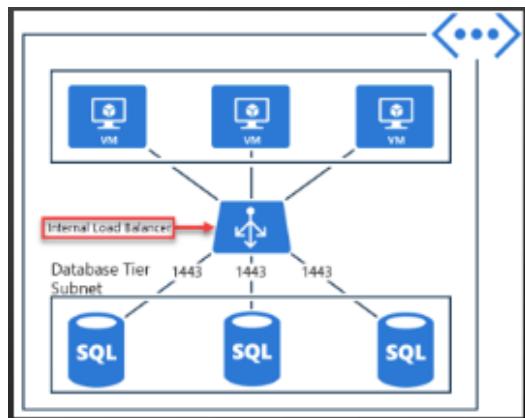
- Distribui o tráfego de entrada para recursos de back-end usando regras de balanceamento de carga e análises de integridade
- Dois tipos: Público e Interno
- Todo o tráfego pode ser centralizado nele
- Recebe a solicitação avalia o backend pool (vms) e ve qual está mais disponível
- Opera na camada 4 (transporte) no modelo OSI
 - Trabalha sempre com IP e porta

▼ Public Load Balancer



- Mapeia os endereços IP públicos e o número da porta do tráfego de entrada para o endereço IP privado e o número da porta da VM e vice-versa.
 - Fica na vnet, expõe o IP publico pelo load balancer, recebe o trafego e direciona para as vms que estão na subnet
- Aplique regras de balanceamento de carga para distribuir o tráfego entre VMs ou serviços.

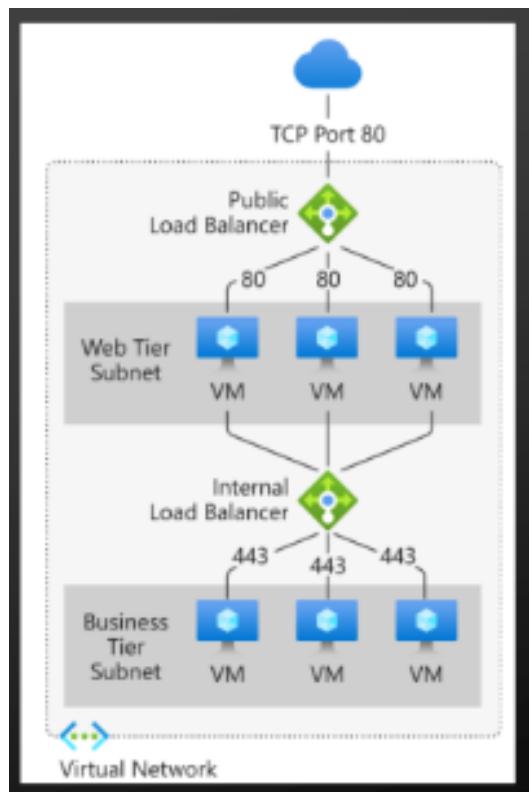
▼ Internal Load Balancer



- Mesma função mas não estará exposto para a rua.
- No exemplo as vms da rua mandam os dados para LB interno que redireciona para os databases
- Direciona o tráfego apenas para recursos dentro de uma rede virtual ou que usam uma VPN para acessar a infraestrutura do Azure.
- Os endereços IP de frontend e as redes virtuais nunca são diretamente expostos a um endpoint da Internet.
- Permite o balanceamento de carga em uma rede virtual, para redes virtuais entre instalações, para aplicativos de várias camadas e para aplicativos de linha de negócios.

▼ Load Balancer Public + Internal

- É possível na mesma estrutura de aplicação termos uma camada de load balancer público e outra camada interna.
 - VM recebem o trafego do public load balancer através da porta 80
 - E envia para o LB interno que vai mandar para as vms de banco de dados
 - Pratica segura pois os dados não estarão expostos



▼ Load Balancer SKUs

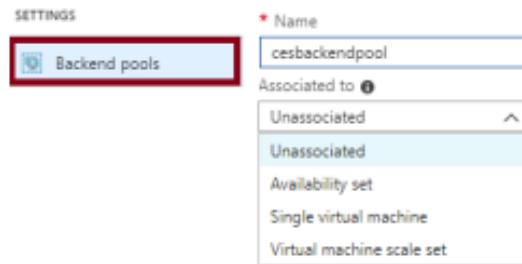
Instance details	
Name *	lb01
Region *	(US) East US
Type *	<input checked="" type="radio"/> Internal <input type="radio"/> Public
SKU *	<input checked="" type="radio"/> Basic <input type="radio"/> Standard
Configure virtual network.	
Virtual network *	vnet01
Subnet *	subnet01 (10.1.0.0/24) Manage subnet configuration
IP address assignment *	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic

- O balanceador de carga suporta SKUs Basic e Standard (mais recentes)
- Sem custo para o SKU do Basic Load Balancer
 - Limitação de até 300 máquinas para o basic e 1000 para o standard
 - No basic testa a porta TCP e HTTP, e o standard faz teste TCP, HTTP e HTTPS

- Essa é a principal limitação do basic
 - Standard tem redundância de zona
 - Basic não tem
- SKUs não são mutáveis
 - Ha não ser que exclua
- A regra do Load Balancer não pode abranger duas redes virtuais

▼ Backend Pools

- Para distribuir tráfego, um pool de endereços back-end contém os endereços IP das NICs virtuais conectadas ao平衡ador de carga

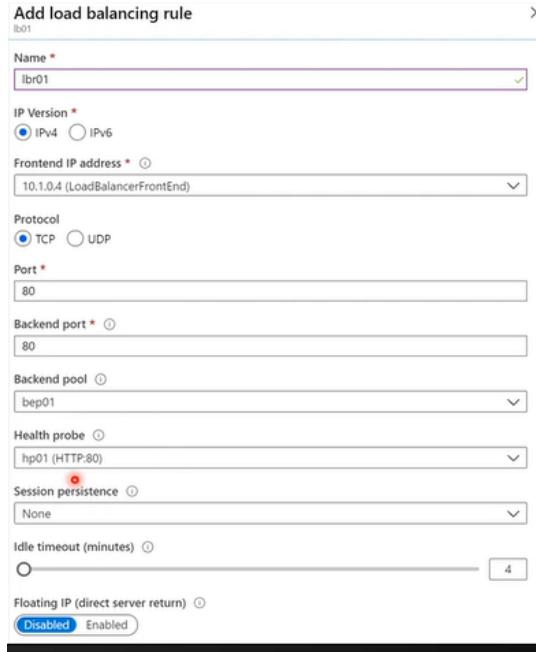


- Podemos posteriormente adicionar posteriormente após a criação
- Podemos escolher qualquer um desses backend porém temos limitações dependendo do SKU

SKU	Backend pool endpoints
Basic SKU	VMs em um único scale set ou VM de um availability set.
Standard SKU	Qualquer VM em uma única rede virtual, incluindo uma mistura de VMs, scale set e availability set.

▼ Load Balancer Rules

- Mapeia uma combinação de IP e porta de front-end para um conjunto de endereços IP de back-end e combinação de porta
- Regras podem ser usadas em combinação com regras NAT
- Uma regra NAT é explicitamente anexada a uma VM (ou interface de rede) para concluir o caminho para o destino
 - Pq ira receber através de um IP e ira converter para o IP da VM



▼ Session Persistence

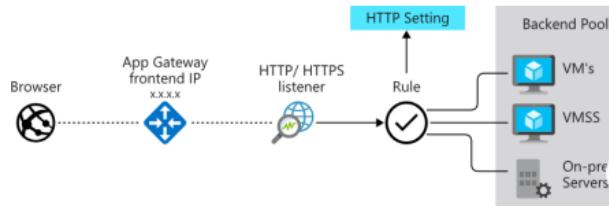
- A persistência da sessão especifica como o tráfego do cliente é tratado
- Se isso não é configurado as requisição pode ir para vms diferentes do backend ocasionando erros no ambiente
- Para isso temos as seguintes opção para tratar este tipo de configuração
 - **None (default)** as solicitações podem ser tratadas por qualquer máquina virtual
 - **Client IP** as solicitações serão tratadas pela mesma máquina virtual
 - Requisição irá manter em uma vm com o mesmo IP
 - **Client IP and protocol** especifica que solicitações sucessivas do mesmo endereço e protocolo serão tratadas pela mesma máquina virtual
 - Além de validar o IP irá validar o protocolo também

▼ Health Probes

- Faz o monitoramento, através dela que vê se a máquina pode receber a requisição
 - Permite que o balanceador de carga monitore o status de um aplicativo
 - Adiciona ou remove VMs dinamicamente do balanceador de carga com base em sua resposta às verificações de integridade
 - Teste personalizado HTTP (preferencial) e pings a cada 15 segundos
 - O probe personalizado TCP tenta estabelecer uma sessão TCP com sucesso
 - Da para limitar a tentativa de validação

▼ Azure Application Gateway

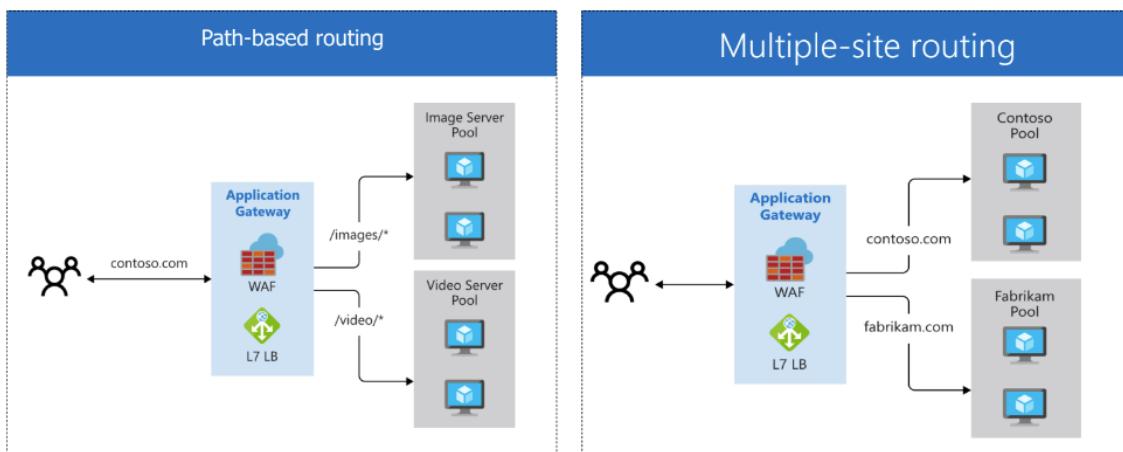
- Função semelhante ao LB, porém ele atua na camada 7
 - Isso permite o redirecionamento de domínio via path, aceitando FQDNs para a resolução, não apenas IPs



- Gerencia solicitações de aplicativos da web
 - Encaminhamento para backend pool
- Encaminha o tráfego para um pool de servidores da web com base na URL de uma solicitação
 - Através do listener
- Os servidores web podem ser máquinas virtuais do Azure, scale sets de máquina virtual do Azure, Serviço de Apps do Azure e até mesmo servidores locais

▼ Application Gateway Routing

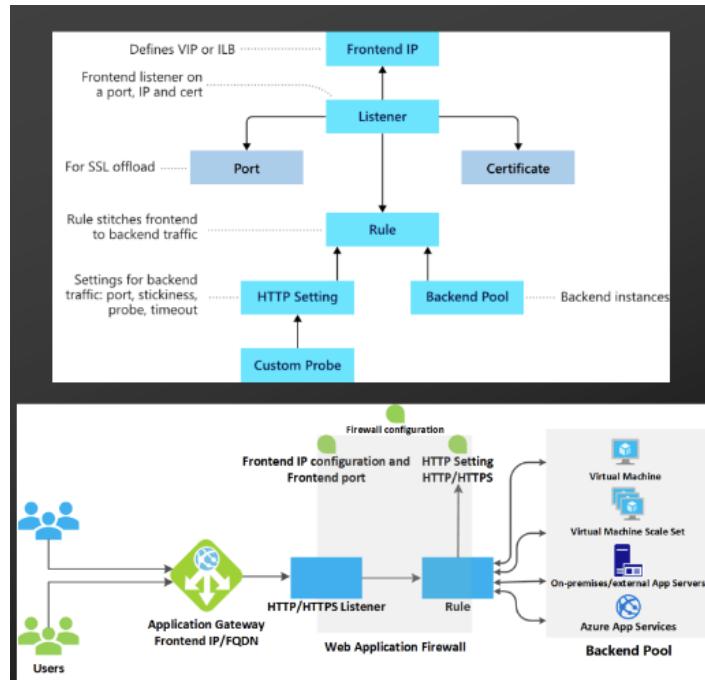
- Path Based Routing
 - Quando bate no App Gateway o mesmo vai direcionar o pool de acordo com o nome
 - Dependendo do que se acessa, o pool será diferente
 - Rota baseada no caminho
- Multiple-site Routing
 - Encaminhamento de backend pool, de acordo com o domínio
 - contoso.com → encaminha para um domínio
 - teste.com → encaminha para outro
 - Ambos no mesmo app gateway



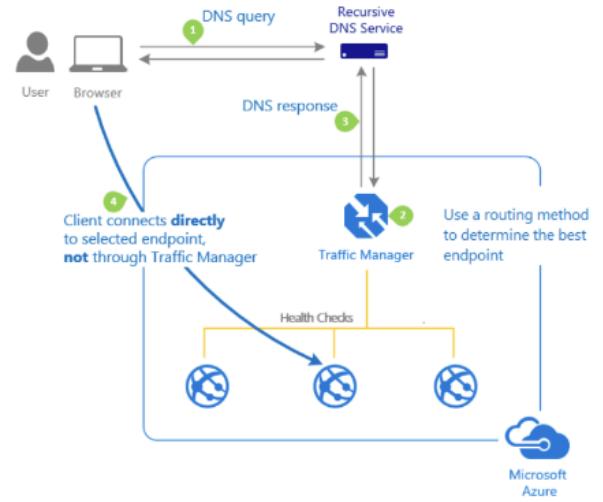
▼ Application Gateway Configuration

- Frontend IP
 - Recebe, onde chega, semelhante ao LB
- Listeners

- Componente logico que determina o tipo de direcionamento Multiple-site Routing ou based
 - SSL ofload → Faz o processo de descriptografar requisições https, o processo diminui a carga do servidor
- **Routing rules**
 - vai processar o tipo de protocolo e configura o tipo de encaminhamento, se será apenas para uma vm, scale set, on-premises, app services
- **Backend pools**
 - As vms, no geral
- **Web application firewall (optional)**
 - WAF → Como se fosse um firewall mas trabalha na camada de aplicação, e analise o comportamento de app
 - Avalia possibilidades de segurança através do comportamento da aplicação como SQL injection, DDoS, etc.
- **Health probes**
 - Semelhante ao LB, detecta se uma vm estará ou não apta a responder



▼ Azure Traffic Manager



- Entregar o conteúdo de forma mais proxima do usuário
 - Ex → Netflix br tem um server de streaming que entrega o serviço de forma mais rápida para brasileiros, nos EUA tem outro e por ai vai
 - Permite que você controle a distribuição do tráfego do usuário para terminais de serviço em todo o mundo
 - Baseado em métodos e regras para a entrega
 - Usa DNS para direcionar as solicitações do usuário final para o endpoint mais apropriado
 - Ele não vai guardar em cache do conteúdo
 - Ele gerencia por qual servidor o usuário irá acessar
 - E não no meio entre a conexão do usuário com o servidor
 - Seleciona um ponto de extremidade com base na configuração do método de roteamento de tráfego
 - Fornece verificações de integridade de endpoint e failover automático de endpoint
 - O ponto mais importante para entender é que o Traffic Manager funciona no nível de DNS.
 - Faz a consulta através de CNames que faz o direcionamento
 - Determina com base na lista, e entrega o servidor mais próximo e mais rápido do usuário
 - O Traffic Manager usa o DNS para direcionar clientes para endpoints de serviço específicos com base nas regras do método de roteamento de tráfego.
 - Os clientes se conectam diretamente ao ponto de extremidade selecionado.
 - O Traffic Manager não é um proxy nem um gateway. O Traffic Manager não vê o tráfego que passa entre o cliente e o serviço.
 - Ele não se encontra no meio da conexão
- ▼ Traffic Manager Routing Methods
- Validação que o TMR irá usar para fazer os encaminhamentos de acessos:
- **Priority** o roteamento encaminha o tráfego para uma lista priorizada de pontos de endpoints de serviço
 - Tem o servidor A, B e C, ele vai checar o acesso e o tempo, latência, e irá julgar o mais apropriado, mas já irá vir determinado o servidor prioritário
 - **Performance** roteamento encaminha o tráfego para o local mais próximo do usuário

- O TMR irá determinar o server mais adequado
 - **Geographic** o roteamento encaminha o tráfego para um conjunto de localizações geográficas
 - Entrega o mais proximo de acordo com a região
 - **Weighted** o roteamento distribui o tráfego de maneira uniforme usando uma ponderação predefinida
 - Preferência de acesso, acesso com o server com maior peso
 - **MultiValue** o roteamento distribui o tráfego apenas para terminais IPv4 e IPv6
 - **Subnet** o roteamento distribui o tráfego com base nos intervalos de IP de origem
-
- Os mais utilizados são Prioridade, Peso, desempenho (Tomar cuidado com o gerenciamento), geografico

▼ Distributing Network Traffic

- Azure tem várias opções para distribuir o tráfego de rede
 - É possível combinar os 3 tipos de entrega LB, App Gateway e Traffic manager
- Eles podem ser usados isoladamente ou em combinação
 - Traffic manager é 100% externo

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport Layer (level 4)	Application Layer (level 7)	DNS Resolver
Protocols	Any TCP or UDP Protocol	HTTP, HTTPS, HTTP/2, & WebSockets	DNS Resolution
Backends or Endpoints	Azure Virtual Machines, and Azure Virtual Machine Scale Sets	Azure Virtual Machines, Azure Virtual Machine Scale Sets, Azure App Services, IP Addresses, and Hostnames	Azure Cloud Services, Azure App Services, Azure App Service Slots, and Public IP Addresses
Network Connectivity	External and Internal	External and Internal	External

▼ MD7 → Azure Storage

▼ Storage Accounts

▼ Azure Storage

- Um serviço que você pode usar para armazenar arquivos, mensagens, tabelas e outros tipos de informações
 - Parecido um storage on-prem, porém ele trabalha com N formatos de storage
- Durável, seguro, escalonável, gerenciado, acessível
- Gerenciar dados com várias contas de armazenamento
- Três categorias de armazenamento Azure:
 - Storage for virtual machines – Disks and File Shares → VMs ou file share
 - Unstructured data – Blobs and Data Lake Store
 - Structured data – Tables and Azure SQL DB
- Standard storage utiliza magnetic drives (HDD) is lowest cost → Performance menor, e custo reduzido

- Premium storage utiliza solid state drives (SSD) → Maior performance, mais caro

▼ Azure Storage Services

- Podemos adicionar formatos de “discos” no storage
 - Azure Containers: Um armazenamento de objetos altamente escalonável para texto e dados binários → Blobs
 - Azure Files: Compartilhamento de arquivos gerenciados para implantações em nuvem ou on premises → //, smb
 - Azure Tables: Um NoSQL armazenamento sem esquema de dados estruturados
 - Azure Queues: Um armazenamento de mensagens confiáveis entre os componentes do aplicativo → Os apps disparam e aguardam um proximo passo.

▼ Storage Account Kinds

Storage account type	Supported services	Supported tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
Storage (general purpose v1)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
StorageV2 (general purpose v2)	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
File Storage	Files only	Premium	LRS, ZRS (limited regions)

- Todas as contas de armazenamento são criptografadas usando o Storage Service Encryption (SSE) para dados em repouso
 - Enquanto o dado estiver em repouso
- Standard → Barato, performance menor
- Premium tem opções de serviço
 - block blob → arquivos pequenos
 - Page Blobs → arquivos grandes, vhds
- Temos mais opções de replicação no tier standard pois na tier premium temos mais performance e é mais exigido do poder computacional regional

▼ Replication Strategies

- Temos 6 formatos de replicação

Data Replication Options
Locally redundant storage (LRS)
Zone-redundant storage (ZRS)
Geo-redundant storage (GRS)
Read access geo-redundant storage (RA-GRS)
Geo-zone-redundant storage (GZRS)
Read-access Geo-zone-redundant storage (RA-GZRS)

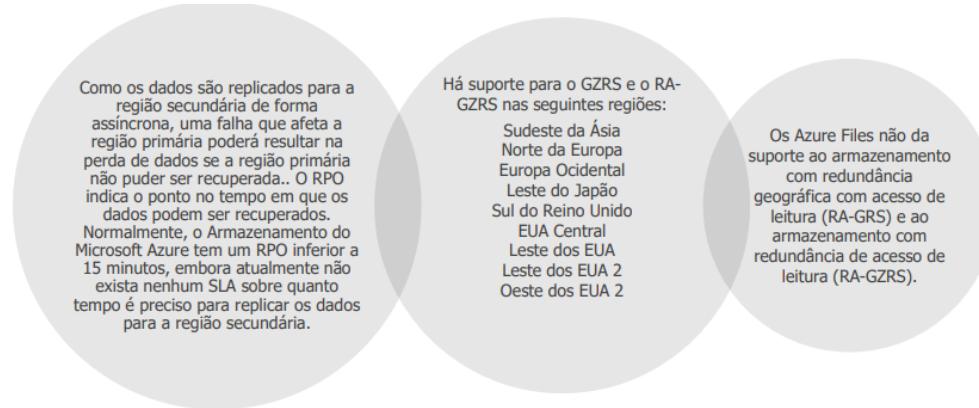
- **Mesma região**

- LRS - Local (ou em um unico datacenter)
 - Copia seus dados de forma síncrona três vezes em um único local físico na região primária usando o LRS. Em seguida, ele copia os dados de forma assíncrona para um único local físico na região secundária.
 - 3 cópias de um mesmo datacenter
 - Recomendado para app não críticos
- ZRS - Zonas de disponibilidade
 - Copia seus dados de forma síncrona três vezes em um único local físico na região primária usando o LRS. Em seguida, ele copia os dados de forma assíncrona para um único local físico na região secundária – com acesso de leitura.
 - Se falha um datacenter inteiro, outro na mesma região irá manter a replicação
 - Assíncrona não irá replicar no mesmo tempo, será replicação em tempos diferentes

- **Regionais/Globais**

- GRS
 - Copia seus dados de forma síncrona em três zonas de disponibilidade do Azure na região primária usando o ZRS. Em seguida, ele copia os dados de forma assíncrona para um único local físico na região secundária.
- RA-GRS
 - Copia seus dados de forma síncrona três vezes em um único local físico na região primária usando o LRS. Em seguida, ele copia os dados de forma assíncrona para um único local físico na região secundária – com acesso de leitura.
 - Faz a cópia de leitura, que pode ser verificada
- GZRS
 - Copia seus dados de forma síncrona em três zonas de disponibilidade do Azure na região primária usando o ZRS. Em seguida, ele copia os dados de forma assíncrona para um único local físico na região secundária.

- Em 3 zonas de disponibilidade na região primária, em seguida copia assíncrona para um datacenter na região secundária
- RA-GZRS
 - Copia seus dados de forma síncrona em três zonas de disponibilidade do Azure na região primária usando o ZRS. Em seguida, ele copia os dados de forma assíncrona para um único local físico na região secundária – com acesso de leitura.
 - Faz a cópia, e coloca na região secundaria na qual pode ser usada para somente leitura



- RPO de 15m, porém não há SLA a respeito
- GZRS é restrito para certas regiões
- Az Files sem acesso RA-GRS e RA-GZRS
- SLA's - Storages

Parâmetro	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
SLA anual	no mínimo 99,99999999% (11 9's)	no mínimo 99,9999999999% (12 9's)	no mínimo 99,99999999999999% (16 9's)	no mínimo 99,99999999999999% (16 9's)

Cenário de interrupção	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
Um nó dentro de um data center, fica disponível?	Sim	Sim	Sim	Sim
Um data center inteiro, fica disponível?	Não	Sim	Sim	Sim
Uma interrupção ocorre em toda a região primária, fica disponível?	Não	Não	Sim	Sim
O acesso de leitura na região secundária estará disponível se a região primária ficar indisponível?	Não	Não	Sim (com RA-GRS)	Sim (com RA-GZRS)

▼ Accessing Storage

- Cada objeto tem um endereço URL exclusivo
- O nome da conta de armazenamento forma o subdomínio desse endereço
- O subdomínio e o nome de domínio formam um ponto de Endpoint
 - Container service:
<http://mystorageaccount.blob.core.windows.net>

- Table service:
<http://mystorageaccount.table.core.windows.net>
- Queue service:
<http://mystorageaccount.queue.core.windows.net>
- File service:
<http://mystorageaccount.file.core.windows.net>
- Se preferir, você pode configurar um nome de domínio personalizado

▼ Securing Storage Endpoints

- Firewalls and virtual networks permitem restringir o acesso à conta de armazenamento de subnets específicas em redes virtuais
- Devem existir subnets e redes virtuais na mesma região do Azure ou par de regiões que a conta de armazenamento

▼ Blob Storage

▼ Blob Storage

- **Armazena dados não estruturados na nuvem**
 - Aceita qualquer tipo de arquivo, vídeo, imagem, etc
- **Pode armazenar qualquer tipo de texto ou dados binários**
- Conectado através da web, api rest, chamada da aplicação
 - Não por meio // ou smb
- **Usos comuns:**
 - Servir imagens ou documentos diretamente para um navegador
 - Armazenamento de arquivos para acesso distribuído
 - Streaming de vídeo e áudio o Armazenamento de dados para backup e restauração, recuperação de desastres, arquivamento
 - Armazenamento de dados para análise por um serviço local ou hospedado pelo Azure
 - Utilizado para armazenar VHDS
 - Podemos subir imagens personalizadas

▼ Blob Containers

- **Todos os blobs devem estar em um contêiner**
- **As contas têm contêineres ilimitados**
- **Os contêineres podem ter blobs ilimitados**
- Formas de conexão
 - **Private blobs - sem acesso anônimo**
 - **Blob access - acesso de leitura público anônimo apenas para blobs**
 - **Container access - acesso público anônimo de leitura e lista a todo o contêiner, incluindo os blobs**

▼ Blob Access Tiers

- **Hot tier** - Otimizado para acesso frequente de objetos na conta de armazenamento
 - Acesso constante

- Acesso - Mais caro
 - Armazenamento - mais barato
- **Cool tier** - Otimizado para armazenar grandes quantidades de dados que raramente são acessados e armazenados por pelo menos 30 dias
 - Acesso ocasional
 - Acesso - Menos caro
 - Armazenamento - Mais caro
- **Archive** - Otimizado para dados que podem tolerar várias horas de latência de recuperação e permanecerão na camada Arquivo por pelo menos 180 dias
 - Acesso historico
 - Reidratação do dado tempo padrão de 15 horas
 - Acesso - Mais barato de todos
 - Armazenamento - Mais Caro de todos
- Podemos alterar a tier a qualquer momento

Tier Cool Tier Hot Archive

<ul style="list-style-type: none"> ◦ Menor custo de armazenamento ◦ Maior custo de acesso 	<ul style="list-style-type: none"> ◦ Maior custo de armazenamento ◦ Menor custo de acesso 	<ul style="list-style-type: none"> ◦ Menor custo de armazenamento de todos ◦ Maior custo de acesso de todos ◦ Necessita reidratação de dados (tempo padrão até 15 horas)
---	---	---

•

▼ Blob Lifecycle Management

- O **Blob Lifecycle Management** permite:
 - **Transição de blobs para uma camada de armazenamento mais fria para otimizar desempenho e custo**
 - **Exclua blobs no final de seu ciclo de vida**
- Podemos criar regras para mudar a tier de um blob após um periodo de tempo

▼ Uploading Blobs

Quando queremos fazer algum upload no blob temos as opções :

- **Block blobs (default)** - útil para armazenar arquivos de texto ou binários
- **Page blobs** - Mais eficiente para operações frequentes de leitura / gravação
- **Append blobs** - útil para cenários de registro
- **Access tier** – selecione entre Hot, Cool, or Archive

Você não pode alterar um tipo de blob, uma vez que ele foi criado

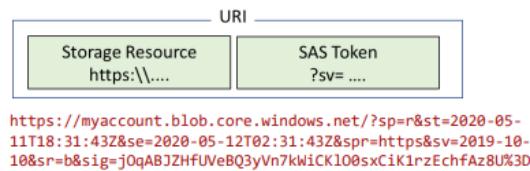
▼ Storage Pricing

- **Custos de armazenamento**
 - Custo mensal por GB
- **Armazenamento de blob**
 - Padrão
- **Custos de acesso a dados**
- **Custos de transação**
 - Movimentação do dado
- **Custos de transferência de dados de replicação geográfica**
- **Custos de transferência de dados de saída**
 - Upload não é cobrado
 - Download é cobrado

▼ Storage Security

- **Storage Encryption Services**
 - MS faz a criptografia dos Dados, quando acessamos é efetuado a descriptografia
 - **Authentication with Azure AD and RBAC**
 - Acesso através do AzAD ou RBAC
 - **Client-side encryption, HTTPS, and SMB 3.0 for data in transit**
 - Trabalhar sempre com HTTPS e não HTTP
 - **Azure disk encryption**
 - MS encripta os dados de disco
 - **Shared Access Signatures – delegated access**
 - SAS → Acesso de forma segura através de assinatura, fornece a um recurso específico, segmentar
 - **Shared Key – encrypted signature string**
 - SAS > SK
 - SK a todos os recursos do container
 - **Anonymous access to containers and blobs**
 - Anônimo é um formato de acesso
 - Não é ideal
- ▼ Shared Access Signatures
- Fornece acesso delegado a recursos
 - Qual tipo de acesso a pessoa irá ter?
 - Podemos atribuir permissões específicas na chave que será compartilhada
 - Podemos colocar tempo de vida para o SAS
 - Concede acesso a clientes sem compartilhar suas chaves de conta de armazenamento
 - A conta SAS delega acesso a recursos em um ou mais dos serviços de armazenamento
 - O serviço SAS delega acesso a um recurso em apenas um dos serviços de armazenamento
- ▼ URI and SAS Parameters

- Um SAS é um URI assinado que aponta para um ou mais recursos de armazenamento
 - URI → O que identificar o recurso
- Consiste em um URI de recurso de armazenamento e o token SAS]



Inclui parâmetros para URI de recurso, versão de serviços de armazenamento, serviços, tipos de recursos, hora de início, tempo de expiração, recurso, permissões, intervalo de IP, protocolo, assinatura

The screenshot shows the Azure Storage blade with the 'Shared access signature' section selected. On the left, there's a sidebar with various storage-related options like Access keys, Geo-replication, CORS, Configuration, Encryption, Shared access signature (which is highlighted), Firewalls and virtual networks, Advanced Threat Protection, Static website, and Properties.

The main area displays the configuration for generating a SAS token. It includes a 'Signing key' dropdown set to 'key1', a 'Generate SAS and connection string' button, and three text input fields:

- Connection string:** BlobEndpoint=https://azstoragedemo12.blob.core.windows.net/QueueEndpoint=https://azstoragedemo12.queue.core.windows.net/FileEndpoint=https://azstoragedemo12.file.core.windows.net/
- SAS token:** ?sv=2018-03-28&ss=b&srt=co&sp=r&se=2019-03-25T03:50:07Z&st=2019-03-24T19:50:07Z&spr=https&sig=HnbC4lbcjk5R%2FttwzXAxMz...
- Blob service SAS URL:** https://azstoragedemo12.blob.core.windows.net/?sv=2018-03-28&ss=b&srt=co&sp=r&se=2019-03-25T03:50:07Z&st=2019-03-24T19:50:07Z...

- A URI é junção com o TOKEN SAS, permitindo um acesso específico
- Quem tiver o SK → Terá acesso ao dado
- O ideal é usar o SAS Token

▼ Storage Service Encryption

- Protege seus dados com segurança e conformidade
 - Criptografia é uma camada a mais de segurança
- Criptografa e descriptografa automaticamente seus dados
- Criptografado por meio de criptografia AES de 256 bits
 - Segura mas não impossível de ser quebrada
- Está habilitado para todas as contas de armazenamento novas e existentes e não pode ser desabilitado
- É transparente para os usuários
- Pode usar a própria chave

▼ Customer Managed Keys

- Usamos nossa própria chave de criptografia
- Use o Azure Key Vault para gerenciar suas chaves de criptografia
- Crie suas próprias chaves de criptografia e armazene-as em um cofre de chaves
- Use APIs do Azure Key Vault para gerar chaves de criptografia

▼ Storage Security Best Practices

- Sempre use HTTPS para criar ou distribuir um SAS

- Não compartilhar sem o HTTPS
- Consulte as políticas de acesso armazenadas sempre que possível
 - Valide os acessos indevidos
- Faça com que os clientes renovem automaticamente o SAS, se necessário
 - Token SAS pode ter um tempo de vida
- Tenha cuidado com a hora de início do SAS
 - Período de tempo a ser liberado
- Seja específico com o recurso a ser acessado
 - Segmentar e granularizar os acessos
- Entenda que sua conta será cobrada por qualquer uso
 - Custo armazenamento e custo por transação e acesso
 - Standard se compartilhar o acesso, e quanto mais a pessoa estiver acessando e validando, haverá custo
- Validar dados gravados usando SAS
 - Quais dados estão sendo compartilhados
- Use o Storage Analytics para monitorar seu aplicativo
 - Valida saúde infraestrutura, etc.

▼ Azure Files and File Sync

▼ Files vs Blobs

- Blob → Arquivo não estruturado
 - Acesso Portal ou resto
 - Suporta volumes sem estrutura, acessos de diferentes formas
 - Não tem o acesso SMB
 - Local indicado para salvar VHDS (imagens)
- Files → Possui estrutura de arquivo
 - Acesso Podemos usar o SMB (445) ou REST
 - File server, na nuvem, unidade de rede, usar o mapeamento '//'

Feature	Description	When to use
Azure Files	Interface SMB, bibliotecas de cliente e uma interface REST que permite o acesso de qualquer lugar aos arquivos armazenados.	<ul style="list-style-type: none"> • Funciona como File Server. • Possui acesso SMB. • Pode ser mapeado como unidade de rede em máquinas Windows, Linux e MacOs.
Azure Blobs	Bibliotecas cliente e uma interface REST que permite que dados não estruturados (namespace simples) sejam armazenados e acessados em grande escala em blobs de blocos.	<ul style="list-style-type: none"> • Suporte a cenários de streaming e acesso aleatório. • Acesse os dados do aplicativo de qualquer lugar. • Não possui acesso SMB.

▼ Managing File Shares

- Cotas de file share

- Especificar o tamanho dele
- Custo irá depender da tier do storage
- Standard pago pelo uso
- Premium, as transações não serão provisionado
- Podemos mapear direto na máquina, com letra e tudo mais
 - Windows - verifique se a porta 445 está aberta
 - SMB liberado
 - Linux - monte a unidade
 - MacOS - monte a unidade
- É necessária uma transferência segura - criptografia SMB 3.0

▼ File Share Snapshots

- Snapshot incremental que captura o estado de compartilhamento em um determinado momento
 - Podemos adicionar um snapshot
 - Uma foto de um momento em que os dados estavam
 - Snapshot não é backup
- É uma cópia somente leitura de seus dados
 - Usamos para restaurar os arquivos
 - Contingência de recuperação de dados
- Snapshot no nível de compartilhamento de arquivo e restauração no nível de arquivo
 - Usos:
 - Proteção contra erro de aplicativo e corrupção de dados.
 - Proteção contra exclusões acidentais ou alterações não intencionais.
 - Finalidades gerais de backup.
 - Usar o snapshot entre os backups

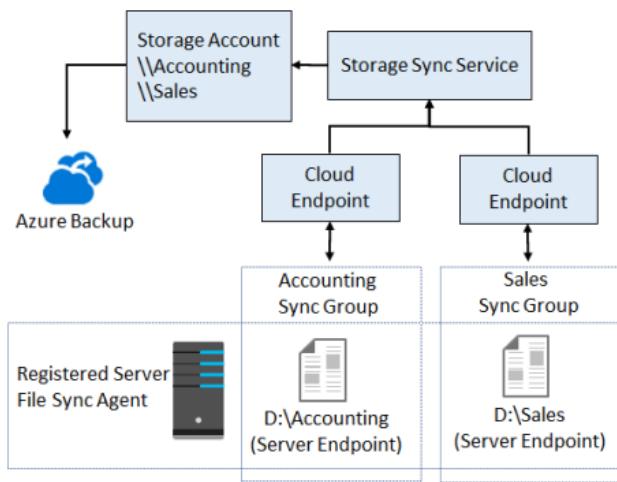
▼ Azure File Sync

- Replicar o fileserver local com a nuvem
- Sincroniza o dado para nuvem, e a nuvem se torna o principal ponto de armazenamento
 - Centralize file shares in Azure Files
 - Lift and shift
 - Migra sem fazer alteração
 - Nem sempre funciona
 - Backup de filiais
 - Replicar para um local centralizado
 - Backup and Disaster Recovery
 - Mesmo que vá pra nuvem é necessário ter um bkp
 - Subir tudo pra nuvem e deixar no local o que é acessado constantemente
 - File Archiving

- Podemos alterar o tier, e mandar os dados sincronizados para o arquivamento

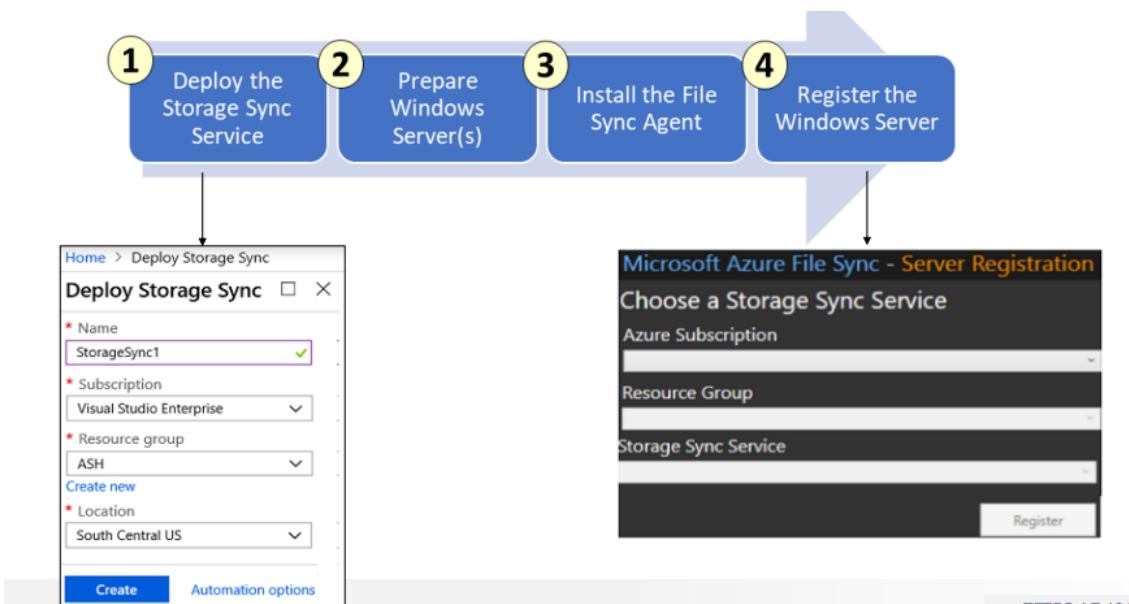
▼ Azure File Sync Components

- **Storage Sync Service** é o recurso de nível superior.
 - Criou o storage, add o componente de storage
- O **registered server** objeto representa uma relação de confiança entre o seu servidor (ou cluster) e o Storage Sync Service
- O **Azure File Sync agent** é um pacote para download que permite que o Windows Server seja sincronizado com um Azure file share
 - Instalamos o cliente nas maquinas que irá realizar a replicação no servidor que desejamos realizar a sincronização
 - VPN não é necessaria
- O **server endpoint** representa um local específico em um servidor registrado, como uma pasta
- O **cloud endpoint** é um Azure file share
- O **sync group** define quais arquivos são mantidos em sincronia
 - Alterar um arquivo no ambiente onprem, o arquivo na nuvem será replicado com base no onprem
 - Verificação de 24/7



▼ File Sync Steps

- 1 - Ter um storage account
- 2 - Prepara o servidor windows
- 3 - Instalar o file sync agent
- 4 - Registrar o servidor para que haja relação de confiança
 - Podemos ter um failover



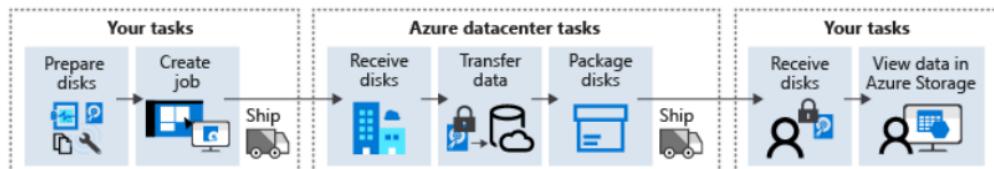
▼ Managing Storage

▼ Storage Explorer

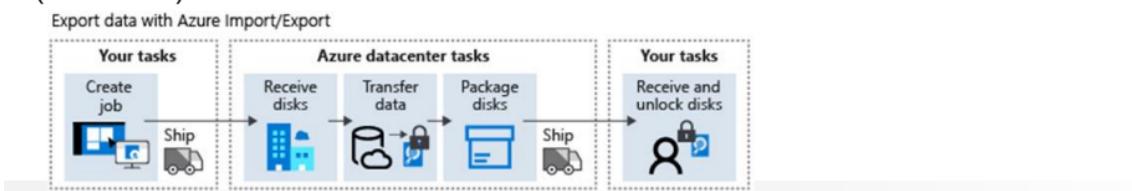
- Programa que permite visualizar todos os storages das assinaturas
- Acesse várias contas e assinaturas
- Criar, excluir, visualizar e editar recursos de armazenamento
- Visualize e edite Blob, Fila, Tabela, Arquivo, armazenamento Cosmos DB e Data Lake Storage

▼ Import and Export Service

- Import jobs move grandes quantidades de dados para o Azure blob storage ou files

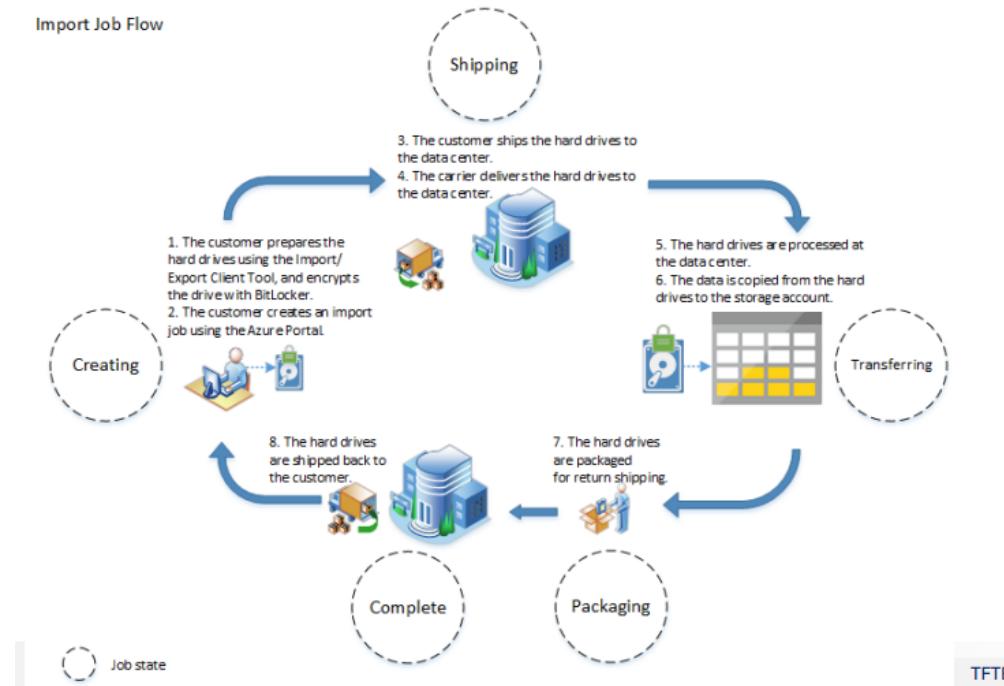


- Export jobs move grandes quantidades de dados do blob do Azure (não files)

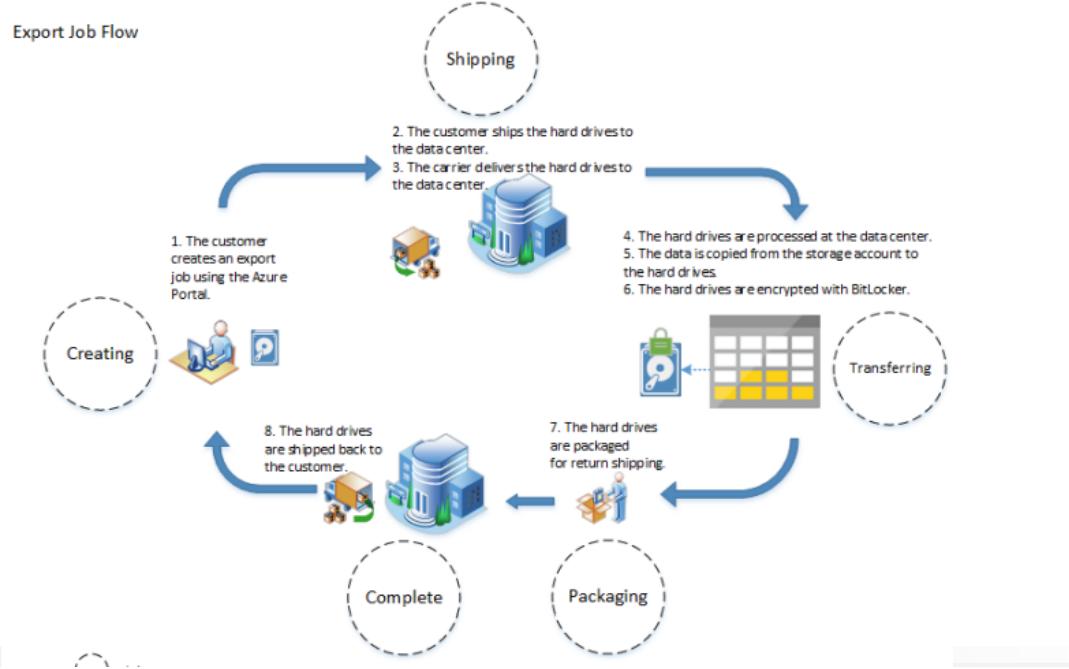


- Import Service
 - Trabalhar jogando os discos e colocar dentro de um blob ou files
 - HD empacotado com todos os dados, criamos um job de import

- Empresas parceira irão coletar o HD e enviar para um datacenter ms
- Os dados vão para um blob ou files
- E o HD irá retornar através da empresa parceira



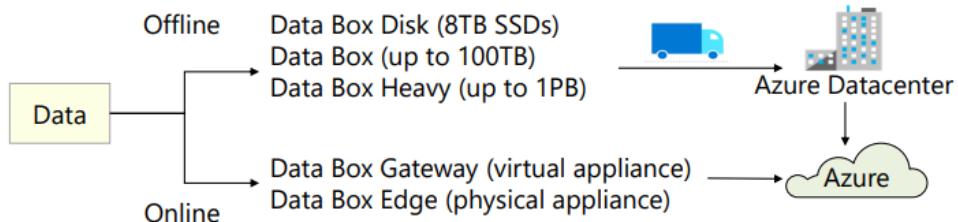
- Export Service
 - Exporto somente de files
 - Preparo disco sem dados
 - Empresa vai pegar o disco, enviar ao datacenter ms, transferir os dados pro disco
 - E encaminhar novamente o disco para o remetente



- O serviço de importação/exportação usa os seguintes componentes:
 - Serviço de Importação/Exportação: esse serviço disponível no portal do Azure ajuda o usuário a criar e acompanhar trabalhos de importação (upload) e exportação (download) de dados.
 - Ferramenta WAImpExp: esta é uma ferramenta de linha de comando que faz o seguinte:
 - Prepara as unidades de disco que são enviadas para importação.
 - Facilita a cópia de seus dados para a unidade.
 - Criptografa os dados na unidade com o BitLocker de 256 bits do AES. Você pode usar um protetor de chave externa para proteger sua chave do BitLocker.
 - Ajuda a identificar os números de unidades necessárias para trabalhos de exportação

▼ Data Box

- Utilizamos um equipamento para o import/export



- Transferência de dados de grande volume fácil, segura e rápida
- Uso offline - migração única, transferência incremental, atualizações periódicas

- Uso online - arquivamento em nuvem, integração com cargas de trabalho locais, dados pré-processados (Edge), inferência Azure Machine Learning (Edge)
 - Quando precisamos enviar dados continuamente
 - Usamos o data box gateway

Data Box



Data Box



Data Box Heavy



Data Box Edge

▼ AzCopy

- Utilitário de linha de comando
 - Trafegar quantidade pequena de dados
- Disponível em Windows, Linux e MacOS
- Projetado para copiar dados de e para o storage Blob, Files e Tables do Azure
- As opções de autenticação incluem **Active Directory** ou **token SAS**
 - `azcopy copy /Source: /Dest: [Options]`

▼ Data Transfer Tool Selection

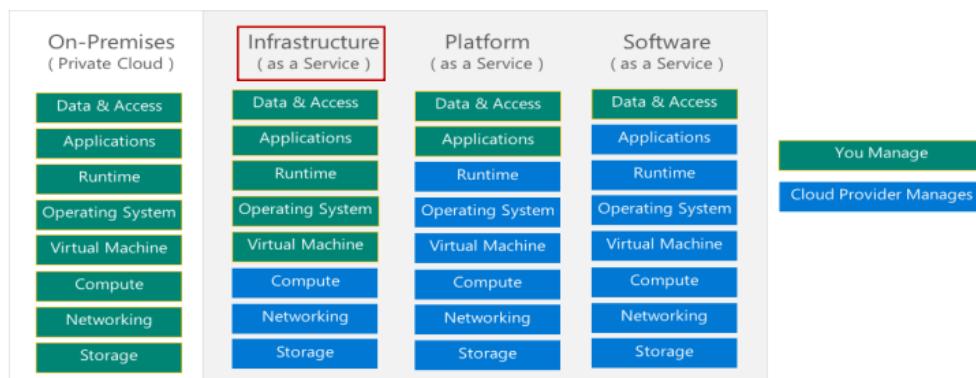
- A ferramenta depende da necessidade
- Conexão lenta alto volume de transferencia → import/export ou databox
- Conexão rápida 1Gbps → Azcopy online, import com az data box edge ou gateway
- Conexão moderada 100 Mb/s → Import / export ou az data box
- Conexão moderada e baixa → alguns arquivos, az storage explorer, portal, az copy, cli

Largura de banda da rede	Solução para usar
Rede de baixa largura de banda menos de 100 megabits	Importação / Exportação do Azure para exportação ou Azure Databox
Rede de alta largura de banda: 1 gigabit por segundo (Gbps) - 100 Gbps	AzCopy para transferências online; ou para importar dados, Azure Data Box Edge ou Azure Data Box Gateway
Rede de largura de banda moderada: 100 megabits por segundo (Mbps) - 1 Gbps	Importação / Exportação do Azure para exportação ou família do Azure Data Box para importação onde houver suporte
Rede de largura de banda baixa a moderada: até 1 Gbps	Se estiver transferindo apenas alguns arquivos, use o Azure Storage Explorer, o portal do Azure, AzCopy ou AZ CLI

▼ MD8 → Azure Virtual Machines

▼ Virtual Machine Planning

▼ IaaS Cloud Services



- IAAS → primeiro pilar de cloud
 - Se trata da infraestrutura na nuvem
 - É a camada com maior gerenciamento

▼ Planning Checklist

- Plano de migração ou criação de infraestrutura
 1. Comece com a rede
 2. Nomeie a VM
 3. Decida a localização da VM → O custo pode variar de acordo com a região
 4. Determine o tamanho da VM → Tamanho é diretamente proporcional ao custo
 5. Compreenda o modelo de preços
 6. Considere o armazenamento para a VM → SSD ou HDD
 7. Selecione um sistema operacional

▼ Location and Pricing

Nem todas as regiões possuem todos os serviços ou tamanhos de máquina.

- Localização
 - Cada região tem diferentes recursos de hardware e serviço
 - Localize máquinas virtuais o mais próximo possível de seus usuários
 - Localize máquinas virtuais para garantir conformidade e obrigações legais
- Preço
 - Custos de computação → Pode ser pausado
 - Custos de armazenamento (com base no consumo e instâncias reservadas) → Continua mesmo se a VM for desligada

▼ Virtual Machine Sizing

VM Type	Sizes	Purpose
General Purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	Proporção balanceada de CPU para memória. Ideal para teste e desenvolvimento, bancos de dados de pequeno a médio porte e servidores da web de baixo a médio tráfego.
Compute Optimized	Fsv2	Alta proporção de CPU para memória. Bom para servidores web de tráfego médio, dispositivos de rede, processos em lote e servidores de aplicativos.
Memory Optimized	Esv3, Ev3, Easv4, Eav4, Mv2, M, DSv2, Dv2	Alta proporção de memória para CPU. Ótimo para servidores de banco de dados relacionais, caches de médio a grande porte e análises em memória.
Storage Optimized	Lsv2	Alta taxa de transferência de disco e IO ideal para Big Data, SQL, bancos de dados NoSQL, data warehousing e grandes bancos de dados transacionais.
GPU	NC, NCv2, NCv3, ND, NDv2 (Preview), NV, NVv3, NVv4 (Preview)	Máquinas virtuais especializadas voltadas para renderização gráfica pesada e edição de vídeo, bem como treinamento e inferência de modelos (ND) com aprendizado profundo. Disponível com uma ou várias GPUs.
High Performance Compute	HB, HC, H	Nossas máquinas virtuais de CPU mais rápidas e poderosas com interfaces de rede de alto rendimento (RDMA) opcionais.

▼ Virtual Machine Disks

- Os discos do sistema operacional são unidades rotuladas como C:
- Os discos temporários fornecem armazenamento de curto prazo
- Os discos de dados são unidades de armazenamento e dependem do seu tipo de máquina virtual

▼ Storage Options

- Armazenamento premium oferece suporte a disco SSD de alto desempenho e baixa latência
- Use armazenamento premium para máquinas virtuais com cargas de trabalho intensivas de entrada / saída (E / S)
- Dois tipos de discos: não gerenciados e gerenciados
- Os discos não gerenciados exigem que você gerencie as contas de armazenamento e VHDS
 - Os discos gerenciados são mantidos pelo Azure (recomendado)

▼ Supported Operating Systems

- Windows Server inclui muitos produtos comuns, requer uma licença, não oferece suporte a atualizações de sistema operacional
- Distribuições Linux são suportadas, atualização do sistema operacional é suportada

▼ Virtual Machine Connection

- Protocolo de Área de Trabalho Remota para máquinas virtuais baseadas em Windows - RDP
- Protocolo Secure Shell para máquinas virtuais baseadas em Linux - SSH
- Subnet Bastion para RDP / SSH por meio do Portal sobre SSL

▼ Creating Virtual Machines

▼ Creating Virtual Machines in the Portal

- **Basic (required)** - , Administrator account, Inbound port rules, Size VM
- **Disks** - OS disk type, data disks
- **Networking** - Virtual networks, load balancing
- **Management** - Monitoring, Auto-shutdown, Backup
- **Advanced** - Add additional configuration, agents, scripts or applications

▼ Windows Virtual Machines

- Capacidades híbridas exclusivas
 - Usar instâncias reservadas
 - Usar licença assurance
- Segurança multcamada avançada
- Inovação mais rápida para aplicativos
 - No marketplace a imagens win com apps já instalados, ou configurações de features já realizadas
- Infraestrutura hiperconvergente sem precedentes
 - Todas as camadas de infraestrutura são conectadas não tendo problemas de criação

▼ Windows VM Connections

- O protocolo RDP (Remote Desktop Protocol) cria uma sessão GUI e aceita o tráfego de entrada na porta TCP 3389
- **WinRM** cria uma sessão de linha de comando para executar scripts
- Bastion → Acesso http via SSL

▼ Linux Virtual Machines

- Centenas de imagens criadas pela comunidade no Azure Marketplace
 - Possibilidade de rodar vms gratuitas (custo de 0,00...)
- O Linux tem as mesmas opções de implantação que as VMs do Windows
- Gerenciar VMs Linux com muitas ferramentas DevOps de código aberto populares

▼ Linux VM Connections

- Autenticar com uma chave pública SSH ou senha
- SSH é um protocolo de conexão criptografado que permite logins seguros em conexões não seguras
- Existem chaves públicas e privadas
- Conexão via bastion também é uma possibilidade

▼ Virtual Machine Availability

▼ Maintenance VS Downtime

VM na nuvem não garante 100% de disponibilidade.

- Manutenção - Programada
- Downtime - Atividade inesperada
- Quando a plataforma prevê uma falha, ela emitirá um **unplanned hardware maintenance** evento. Ação: Live migration.
 - Desligar o rack, e ocorre uma migração no Datacenter da MS, migrando a VM
- **Unexpected Downtime** é quando uma máquina virtual falha inesperadamente. Ação: migra automaticamente.

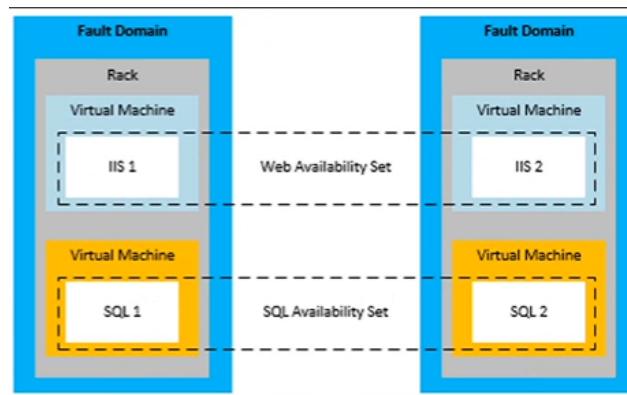
- **Planned Maintenance** eventos são atualizações periódicas feitas na plataforma Azure. Ação: nenhuma ação
 - Rotinas de manutenção planejada

▼ Availability Sets → Rack

- No mesmo datacenter
- Uma VM comum tem 99,9% de SLA , já com o Availability sets temos um SLA de 99,95%
- Configure várias máquinas virtuais em um conjunto de disponibilidade
 - Conjunto é feito manualmente e não são replicas
 - O que ocorre é uma distribuição de máquinas
- Configure cada camada de aplicativo em conjuntos de disponibilidade separados
- Combine um平衡ador de carga com conjuntos de disponibilidade
- Use discos gerenciados com as máquinas virtuais

▼ Update and Fault Domains

- **Update domains** permite que o Azure execute atualizações incrementais ou sem interrupção em uma implantação. Durante a manutenção planejada, apenas um domínio de atualização é reinicializado por vez.
- **Fault Domains** são um grupo de máquinas virtuais que compartilham um conjunto comum de hardware, switches, que compartilham um único ponto de falha. As VMs em um conjunto de disponibilidade são colocadas em pelo menos dois domínios de falha.



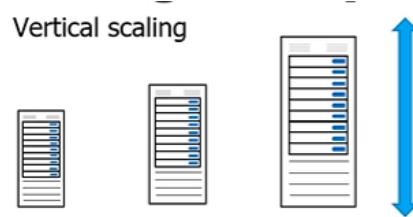
- Update domain é na horizontal

▼ Availability Zones

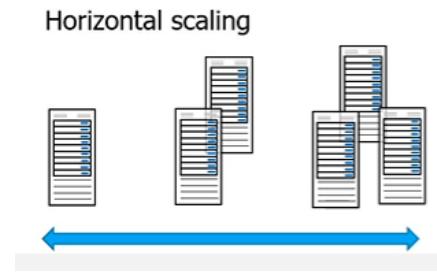
- VM com 99,99% de disponibilidade
- Locais físicos únicos em uma região
 - 3 Zonas em cada região
 - Inclui datacenters com alimentação
 - Independente, refrigeração e rede
 - Protege contra falhas do datacenter
 - Combina domínios de atualização e falha
 - Fornece SLA de 99,99%

▼ Scaling Concepts

- Vertical scaling (scale up and scale down) é o processo de aumentar ou diminuir o poder para uma única instância de uma carga de trabalho; geralmente manual



- Horizontal scaling (scale out and scale in) é o processo de aumentar ou diminuir o número de instâncias de uma carga de trabalho; frequentemente automatizado



▼ Scale Sets

Como deveriamos escalar o ambiente na black friday ?

- Scale sets deploy um conjunto de VMs idênticas
- Nenhum pré-provisionamento de VMs é necessário
- Conforme a demanda aumenta, as VMs são adicionadas
- Conforme a demanda diminui, as VMs são removidas
- O processo pode ser manual, automatizado ou uma combinação de ambos

▼ Implementing Scale Sets

- Instance count.** Número de VMs no conjunto de escala (0 a 1000)
- Instance size.** O tamanho de cada máquina virtual no scale set
- Azure Spot Instance.** Capacidade não utilizada com desconto
- Use managed disks
- Enable scaling beyond 100 instances

▼ Autoscale

- Defina regras para ajustar automaticamente a capacidade
 - Manual também é possível
- Dimensione (aumente) o número de VMs no conjunto
- Dimensione (reduza) o número de VMs no conjunto
- Programe eventos para aumentar ou diminuir em um horário fixo
- Reduz o monitoramento e otimiza o desempenho

▼ Implementing Autoscale

The screenshot shows the configuration interface for a VM Scale Set. It includes sections for 'Instance' (Initial instance count: 2), 'Scaling' (Scaling policy: Custom selected), 'Scale out' (CPU threshold: 75%, Duration in minutes: 10, Number of VMs to increase by: 1), and 'Scale in' (CPU threshold: 25, Number of VMs to decrease by: 1).

- Defina um número mínimo, máximo e padrão de instâncias de VM
- Crie conjuntos de escala mais avançados com escala e parâmetros de escala
 - Scale out → Cresce
 - Scale in → Diminui
 - Scaling policy → Pode ser custom ou manual

▼ Virtual Machine Extensions

▼ Virtual Machine Extensions

- Extensões são pequenos aplicativos/scripts que fornecem configuração de VM pós-implantação e tarefas de automação
- Gerenciado com CLI do Azure, PowerShell, modelos do Azure, Resource Manager e portal do Azure
- Empacotado com uma nova implantação de VM ou executado em qualquer sistema existente
- Diferente para máquinas Windows e Linux

▼ Custom Script Extensions

- Os scripts de extensão podem ser simples ou complexos
- As extensões têm 90 minutos para funcionar
- Verifique as dependências para garantir a disponibilidade
- Considere quaisquer erros que possam ocorrer
- Proteger / criptografar informações confidenciais
- Para PowerShell, use o comando Set-AzVmCustomScriptExtension

▼ Desired State Configuration

- Os blocos de configuração têm um nome
- Os blocos de nós definem os computadores ou VMs que você está configurando
- Os blocos de recursos configuram o recurso e suas propriedades
- Existem muitos recursos de configuração integrados

```
configuration IISInstall
{
    Node "localhost"
    {
        WindowsFeature IIS
```

```
{  
    Ensure = "Present"  
    Name = "Web-Server"  
}  
}  
}
```

▼ MD9 → Serverless Computing

▼ Azure App Service Plans

▼ Azure App Service Plans

- Web App
 - Aplicação PaaS
 - App service plan → O plano para colocar o web app
- Defina um conjunto de recursos de computação para um web app executar
 - Qnt de memoria, disco, scalling, etc.
- Determina o desempenho, preço e recursos
 - Maior poder computacional, maior o preço
 - Poder computacional pode ser compartilhado
- Um ou mais aplicativos podem ser configurados para serem executados no mesmo App Service plans, defina:
 - Região onde os recursos de computação serão criados
 - Número de instâncias de máquina virtual
 - Tamanho das instâncias de máquina virtual (pequeno, médio, grande)
 - Camada de preços (próximo slide)

▼ App Service Plan Pricing Tiers

- **Shared compute (Free and Shared).** Execute aplicativos na mesma VM do Azure que outros Apps Service Apps, e os recursos não podem ser dimensionados
- **Dedicated compute (Basic, Standard, Premium).** Execute apps no mesmo plano em Azure VMs dedicadas
 - Para de concorrer as vms
- **Isolated.** Execute apps em Azure VMs e Azure virtual networks dedicados
 - Para de concorrer a rede

▼ App Service Plan Scaling

- Scale up (mudança no App Service plan)
 - Mais hardware (CPU, memory, disk)
 - Mais features (dedicated virtual machines, staging slots, autoscaling)
- Scale out (aumento no número de VM instances)
 - Manual (número fixo de instances)
 - Autoscale (baseado em regras e agendamentos pré definidos)

▼ App Service Plan Scale Out

- Ajuste os recursos disponíveis com base na demanda atual
- Melhora a disponibilidade e tolerância a falhas

- Escala com base em uma métrica (porcentagem de CPU, porcentagem de memória, solicitações HTTP)
- Escala de acordo com um agendamento (dias de semana, fins de semana, horários, feriados)
- Pode implementar várias regras - combinar métricas e cronogramas
- Não se esqueça de reduzir

▼ Azure App Services

▼ Azure App Service

- Inclui web app APIs, aplicativos móveis e aplicativos de funções
- Ambiente totalmente gerenciado permitindo o desenvolvimento de alta produtividade
- Oferta de plataforma como serviço (PaaS) para construir e implantar aplicativos em nuvem altamente disponíveis para web e dispositivos móveis
- A plataforma gerencia a infraestrutura para que os desenvolvedores se concentrem nos principais aplicativos e serviços da web
- Produtividade do desenvolvedor usando .NET, .NET Core, Java, Python e uma série de outros
- Oferece segurança e conformidade de nível empresarial

▼ Creating an App Service

- O nome deve ser único
- Acesso usando [azurewebsites.net](#) - pode mapear para um domínio personalizado
- Publicar código (Runtime Stack)
- Publicar contêiner Docker
- Linux ou Windows
- Região mais próxima de seus usuários
- Plano de serviço de aplicativo

▼ Continuous Deployment

- Trabalhe em um único source control
- Sempre que as atualizações de código são enviadas para o source control, o site ou web app seleciona automaticamente as atualizações
- Um fluxo de trabalho de implantação contínua publica as atualizações mais recentes de um projeto
- Use o portal para implantações contínuas de GitHub, Bitbucket ou Azure DevOps

▼ Deployment Slots

- Implante em um slot de implantação diferente (depende do plano de serviço)
- Valide as alterações antes de enviar para a produção
- Slots de implantação são aplicativos ativos com seus próprios nomes de host
- Elimina o tempo de inatividade
- Fallback para um último site estável conhecido
- Troca automática quando a validação pré-troca não é necessária

▼ Creating Deployment Slots

- Um novo slot pode estar vazio ou clonado
- Ao clonar, preste atenção às configurações: o Configurações de aplicativo específicas de slot e strings de conexão
 - Configurações de implantação contínua
 - Configurações de autenticação do service app
- Nem todas as configurações são fixas (endpoints, nomes de domínio personalizados, certificados SSL, dimensionamento)
- Revise e edite suas configurações antes de trocar

▼ Securing an App Service

- Autenticação
 - Habilitar autenticação anônimo padrão
 - Faça login com um provedor de identidade de terceiros
- Segurança
 - Solucionar problemas com logs de diagnóstico - solicitações com falha, registro de aplicativo
 - Adicionar um certificado SSL - HTTPS
 - Defina uma lista de permissões / negações ordenada por prioridade para controlar o acesso à rede para o aplicativo
 - Armazenar secrets no Azure Key Vault

▼ Custom Domain Names

- Redirecionar o URL padrão do aplicativo da web
- Valide o domínio personalizado no Azure
- Use o registro DNS para seu provedor de domínio - crie um registro CNAME ou A com o mapeamento
- Certifique-se de que o plano de serviço de aplicativo oferece suporte a domínios personalizados

▼ Backup an App Service

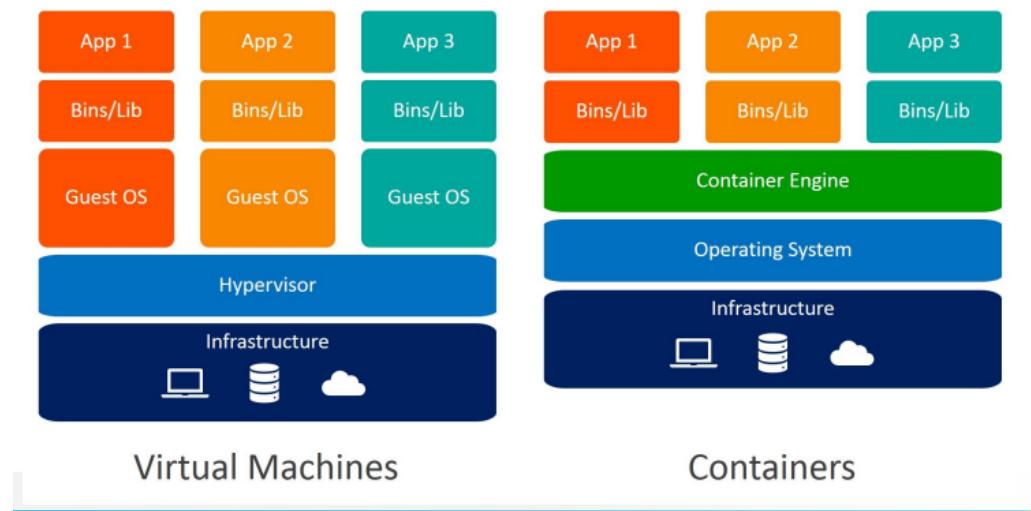
- Crie backups de aplicativos manualmente ou em uma programação
- Faça backup da configuração, do conteúdo do arquivo e do banco de dados conectado ao app
- Requer plano Standard ou Premium
- Os backups podem ter até 10 GB de conteúdo de aplicativo e banco de dados
- Restaure seu app sob demanda para um estado anterior ou crie um novo aplicativo

▼ Application Insights

- Taxas de solicitação, tempos de resposta e taxas de falha
- Taxas de dependência, tempos de resposta e taxas de falha
- Visualizações de página e desempenho de carregamento
- Contagens de usuários e sessões
- Contadores de desempenho
- Diagnósticos e exceções

▼ Container Services

▼ Containers vs. Virtual Machines



Feature Containers Virtual Machines

- Isolation
 - Normalmente fornece isolamento leve do host e de outros contêineres, mas não fornece um limite de segurança tão forte quanto uma máquina virtual.

- Fornece isolamento completo do sistema operacional host e outras VMs.
Isso é útil quando um limite de segurança forte é crítico, como hospedar aplicativos de empresas concorrentes no mesmo servidor ou cluster.
- Operating system
 - Executa a parte do modo de usuário de um sistema operacional e pode ser adaptado para conter apenas os serviços necessários para seu aplicativo, usando menos recursos do sistema.
 - Executa um sistema operacional completo incluindo o kernel, exigindo mais recursos do sistema (CPU, memória e armazenamento).
- Deployment
 - Implante contêineres individuais usando Docker via linha de comando; implantar vários contêineres usando um orquestrador, como o Azure Kubernetes Service.
 - Implante VMs individuais usando o Windows Admin Center ou o Gerenciador Hyper-V; implantar várias VMs usando PowerShell ou System Center Virtual Machine Manager.
- Persistent storage
 - Use discos do Azure para armazenamento local para um único nó ou arquivos do Azure (compartilhamentos SMB) para armazenamento compartilhado por vários nós ou servidores.
 - Use um disco rígido virtual (VHD) para armazenamento local para uma única VM ou um compartilhamento de arquivo SMB para armazenamento compartilhado por vários servidores.
- Fault tolerance
 - Se um nó do cluster falhar, todos os contêineres em execução nele serão recriados rapidamente pelo orquestrador em outro nó do cluster
 - As VMs podem fazer failover para outro servidor em um cluster, com o sistema operacional da VM reiniciando no novo servidor.

▼ Azure Container Instances

- Serviço PaaS
- Tempos de inicialização rápidos
- Conectividade de IP público e nome DNS
- Segurança de nível de hipervisor
- Recursos de isolamento
- Tamanhos personalizados
- Armazenamento persistente
- Contêineres Linux e Windows
- Implantação de rede virtual

▼ Container Groups

- Recurso de nível superior em instâncias de contêiner do Azure

- Uma coleção de contêineres que são programados no mesmo host
- Os contêineres groups compartilham um ciclo de vida, recursos, rede local e volumes de armazenamento

▼ Docker

- Permite que os desenvolvedores hospedem aplicativos em um contêiner
- Um contêiner é uma "unidade de software" padronizada que contém tudo o que é necessário para a execução de um app
- Disponível em Linux e Windows e pode ser hospedado no Azure

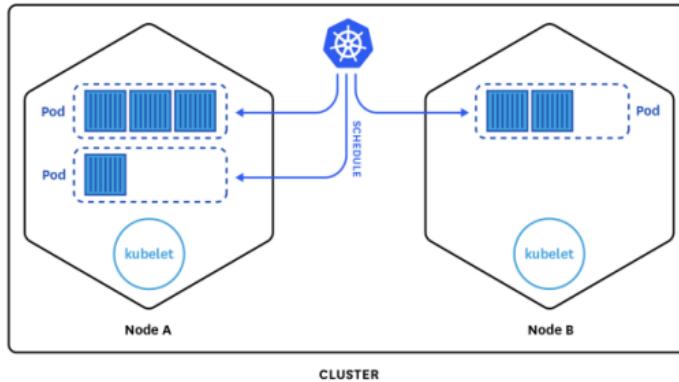
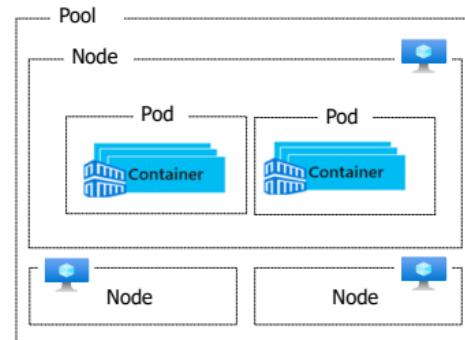
▼ Azure Kubernetes Service

▼ Azure Kubernetes Services (AKS)

- Gerencia o monitoramento de integridade e manutenção
- Executa escalonamento de cluster simples
- Permite que os nós masters sejam totalmente gerenciados pela Microsoft
- Você é responsável apenas por gerenciar os nós do agente
- Nós masters são gratuitos e você paga apenas para executar nós de agente

▼ AKS Terminology

Term	Description
Pools	Grupos de nós com configurações idênticas.
Nodes	VM individual executando aplicativos em contêineres.
Pods	Única instância de um aplicativo. Um pod pode conter vários contêineres



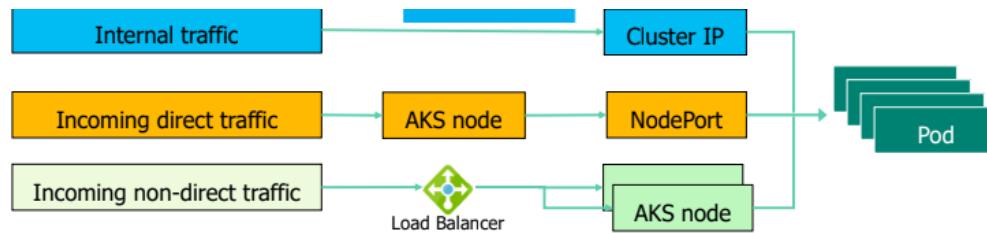
▼ AKS Clusters and Nodes

- O cluster master fornece serviços e orquestração centrais do Kubernetes

- Os nós executam aplicativos e serviços de suporte
- Cada nó individual é uma máquina virtual do Azure

▼ AKS Networking

- Pods executam uma instância do seu aplicativo
- Os serviços agrupam pods para fornecer conectividade de rede
- O IP do cluster fornece acesso ao tráfego interno
- NodePort fornece mapeamento para tráfego direto de entrada
- O平衡ador de carga tem endereço IP externo



▼ AKS Storage

- O armazenamento local no nó é rápido e simples de usar
- O armazenamento local pode não estar disponível após a exclusão do pod
- Vários pods podem compartilhar volumes de dados
- O armazenamento pode ser reanexado a outro pod

▼ AKS Security

- Cluster AKS - Orquestração de upgrade
- Cluster Master - totalmente gerenciado
- Node - patches automáticos de segurança do sistema operacional
- Networks - redes virtuais privadas e grupos de segurança de rede
- Data - secrets do Kubernetes para credenciais e keys

▼ AKS and Azure Active Directory

- Use o Azure AD como uma solução de identidade integrada
- Use contas de serviço, contas de usuário e controle de acesso baseado em função

▼ AKS Scaling

- Os aplicativos podem crescer além da capacidade de um único pod
- O Kubernetes tem autoescaladores integrados
- O Cluster autoscaler é escalonado com base em recursos de computação
- Horizontal Pod Autoscaler com base em métricas de recursos para o aplicativo

▼ Virtual Kubelet

- O virtual Kubelet é uma implementação open source do Kubernetes kubelet

- O virtual kubelet se registra como um nó e permite que os desenvolvedores implantem pods e contêineres com suas próprias APIs

▼ MD10 → Data Protection

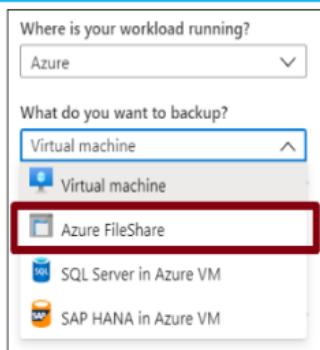
▼ File and Folder Backups

▼ Azure Backup

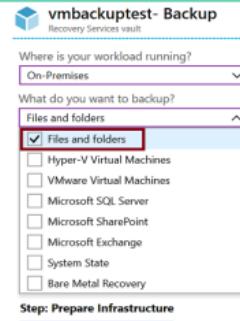
- Serviço baseado em Azure usado para fazer backup e restaurar dados na nuvem da Microsoft
- Gerenciamento Automático de Armazenamento
- Várias opções de armazenamento
 - blob, azure files, etc
- Transferência de dados ilimitada
 - Pagando apenas pelo armazenamento e pelo client
- Criptografia de dados
 - Chave de restore
- Retenção de longo prazo
 - Quanto tempo o dado precisa ser reservado
 - Ciclos etc.

▼ Recovery Service Vault Backup Options

Azure Workloads



On-Premises workloads



- Na nuvem é um pouco mais limitado
- Porém as maiores ferramentas de backups são do ambiente on premises

▼ Implementing On-Premises File and Folder Backups

1. Crie um recovery services vault
 - a. Onde os dados ficaram armazenados
2. Baixe o agente e o arquivo de credencial
 - a. Através do portal, sem isso não é possível fazer o registro da máquina
3. Instalar e registrar agente
4. Configure o backup

▼ Microsoft Azure Recovery Services Agent

- MARSA → ideal para notebooks empresariais da diretoria por exemplo
- Faça backup ou recupere arquivos e pastas no sistema operacional Windows físico ou virtual (as VMs podem ser locais ou no Azure)
- Nenhum servidor de backup separado necessário
- Sem suporte para Linux

▼ Virtual Machine Backups

▼ Virtual Machine - Data Protection

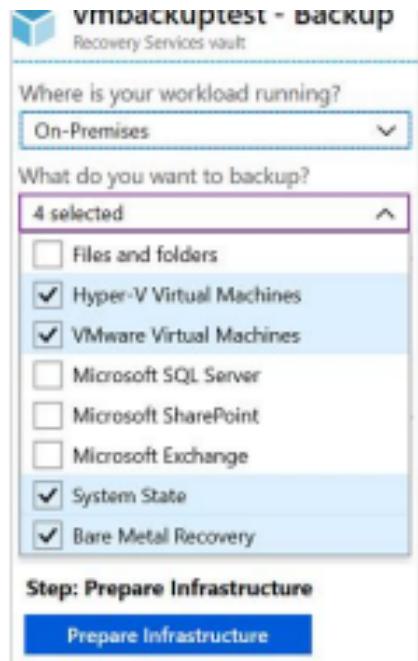
- Snapshots gerenciados fornecem uma opção rápida e simples para fazer backup de VMs que usam discos gerenciados
 - Rapido
 - Parte de solução de bkp
- O Backup do Azure dá suporte a backups consistentes com aplicativos para VMs do Windows e Linux
 - Diferente do MARS que só tem para o windows
 - Gerenciamento centralizado, suporte de granularidade
- O Azure Site Recovery (ASR) protege suas VMs de um cenário de grande desastre quando uma região inteira sofre uma interrupção
 - Replicar máquinas para uma segunda região
 - Protege tanto da parte de replicação
 - Replica do on-prem para o azure, ou de outras clouds para o azure
- **Workload Protection Needs**
 - Muitas opções de backup estão disponíveis no marketplace
 - VEEAM
 - Acronis
 - Quickbooks
 - Como a carga de trabalho está sendo protegida hoje?
 - Com que frequência é feito backup da carga de trabalho?
 - Que tipos de backups estão sendo feitos?
A proteção de recuperação de desastres está em vigor?

▼ Virtual Machine - Snapshots

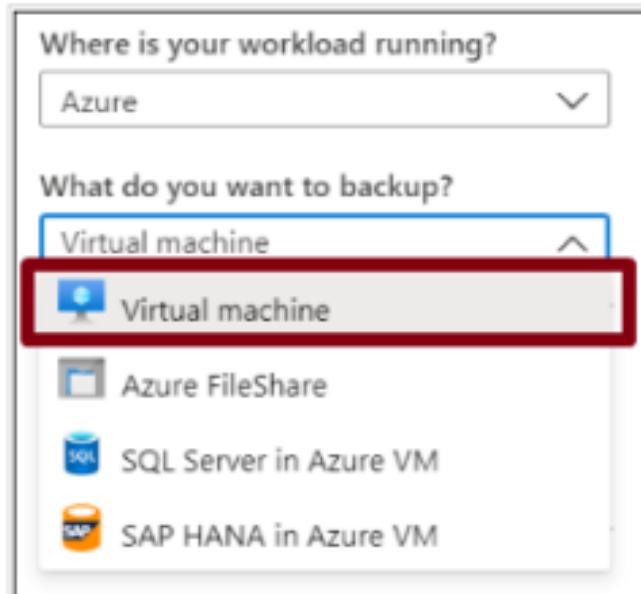
- Parte de uma solução mas não é solução, pois não tem retenção, ou granularidade na hora de voltar um bkp, como data e hora etc.
- Use snapshots tirados como parte de um trabalho de backup
- Reduz os tempos de espera de recuperação - não espere que a transferência de dados para o cofre termine
- Configure a retenção da Restauração Instantânea (1 a 5 dias)
 - Podemos fazer e restaurar um snap em segundos
 - No az bkp podemos agendar snaps

▼ Recovery Services Vault VM Backup Options

- On-Premises Workloads



- Azure Workloads



- Vários servidores podem ser protegidos usando o mesmo recovery service vault
- Podemos ter diversos servidores no mesmo vault de bkp

▼ Implementing VM Backups

1. Use um Recover Service Vault na região onde você está executando seus backups de máquina virtual e escolha uma estratégia de replicação para o Vault.

2. Faça snapshot (pontos de recuperação) de seus dados em intervalos definidos. Esses snapshot são armazenados em recovery service vaults.
 - a. Recomendado a fazer 1 ou 2 vezes por dia
 - b. Pois o snapshot é rápido
3. Para que a extensão de backup funcione, o VM Agent do Azure deve ser instalado na máquina virtual do Azure.

▼ Implementing VM Restore

- Depois de acionar a operação de restauração, o serviço de backup cria uma tarefa para rastrear a operação
- O serviço de backup também cria e exibe temporariamente notificações, para que você monitore como o backup está ocorrendo

▼ Azure Backup - Server

- Backups compatíveis com aplicativos, backups de arquivos / pastas / volumes e backups de estado da máquina (bare-metal, estado do sistema)
- Cada máquina executa o agente de proteção DPM / MABS e o agente MARS é executado no MABS / DPM
 - Cada vm terá o mabs
- Flexibilidade e opções de programação granular
- Gerenciar backups para várias máquinas em um grupo de proteção

▼ Backup - Component Comparison

Component	Benefits	Limits	Protects	Backup Storage
Azure Backup (MARS) agent	<ul style="list-style-type: none"> • Faça backup de arquivos e pastas no sistema operacional Windows físico ou virtual • Nenhum servidor de backup separado necessário. 	<ul style="list-style-type: none"> • Backup 3x por dia • Somente restauração em nível de arquivo, pasta e volume • Sem suporte para Linux 	<ul style="list-style-type: none"> • Arquivos • Pastas 	<ul style="list-style-type: none"> • Recovery services vault
Azure Backup Server	<ul style="list-style-type: none"> • Flexibilidade total para quando fazer backups • Granularidade de recuperação • Suporte Linux em VMs Hyper-V e VMware • Backup e restauração de VMs VMware 	<ul style="list-style-type: none"> • Não é possível fazer backup de cargas de trabalho Oracle • Sempre requer assinatura ativa do Azure • Sem suporte para backup em fita 	<ul style="list-style-type: none"> • Arquivos • Pastas, • Volumes • VMs • Aplicações • Workloads 	<ul style="list-style-type: none"> • Recovery services vault • Disco conectado localmente

▼ Soft Delete Azure Site Recovery

- Os dados de backup são retidos por mais 14 dias
- Recupere itens de backup excluídos de forma reversível usando uma operação "Desfazer exclusão"
- Integrado nativamente para todos os recovery service vault

▼ Azure site recovery

- Principal ferramenta de migração para a nuvem
- Replicar VMs do Azure de uma região do Azure para outra
- Replicar VMs VMware locais, VMs Hyper-V, servidores físicos (Windows e Linux) para o Azure
- Replicar instâncias do Windows AWS para o Azure
- Replique VMs VMware locais, VMs Hyper-V gerenciadas pelo System Center VMM e servidores físicos em um site secundário

- Ideal para Failover e fail back

▼ Azure to Azure Architecture

1. A VM está registrada no Azure Site Recovery
 2. Os dados são continuamente replicados para o cache
 3. O cache é replicado para storage account de destino
 4. Durante o failover, a máquina virtual é adicionada ao ambiente de destino
- Pode usar para replicar o ambiente on-prem para a nuvem

▼ Lab - Task01 - Criar um Recovery Services vault

▼ Lab - Task02 - Implementar backup em nível de máquina virtual do Azure

▼ Lab - Task03 - Implementar backup de arquivos e pastas em máquina on-premises com cliente MARS

▼ Lab - Task04 - Execute a recuperação da VM

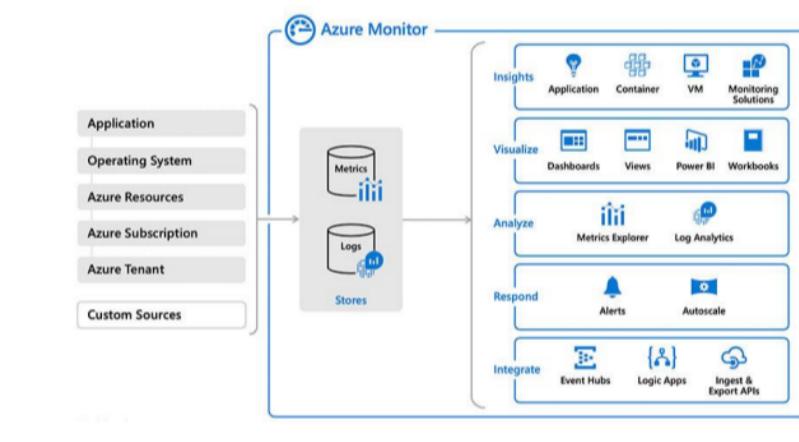
▼ Lab - Task05 - Execute a recuperação de arquivos da máquina on premises

▼ Lab - Task06 - Revise a funcionalidade do softdelete do Azure Recovery Services

▼ MD11 → Monitoring

▼ Azure Monitor

▼ Azure Monitor Service



- Key Capabilities
 - Monitoramento principal para serviços do Azure
 - Coleta métricas, registros de atividades e registros de diagnóstico
 - Use para alertas e notificações urgentes

▼ Monitoring Data Platform

- As métricas são valores numéricos que descrevem algum aspecto de um sistema em um determinado momento. Eles são leves e capazes de suportar cenários quase em tempo real.
 - Metric ou threshold

▼ Log Data

- Os logs contêm diferentes tipos de dados organizados em registros com diferentes conjuntos de propriedades para cada tipo. A telemetria, como eventos e

rastreamentos, são armazenados como registros, além dos dados de desempenho, para que todos possam ser combinados para análise.

- Os dados de log são armazenados no Log Analytics, que inclui uma linguagem de consulta rica para recuperar, consolidar e analisar rapidamente os dados coletados
- A linguagem de consulta do Data Explorer que é adequada para consultas de log simples, mas também inclui funcionalidades avançadas, como agregações, junções e análises inteligentes

▼ Data Types

- Application monitoring data - Desempenho e funcionalidade do código que você escreveu, independentemente de sua plataforma
- Guest OS monitoring - Azure, outra nuvem ou local
- Azure resource monitoring
- Azure subscription monitoring - Operação e gerenciamento de uma assinatura do Azure, bem como dados sobre a integridade e operação do próprio Azure
- Azure tenant monitoring – Operação de serviços do Azure de nível de tenant, como o Azure Active Directory
- O armazenamento dos logs serão cobrados

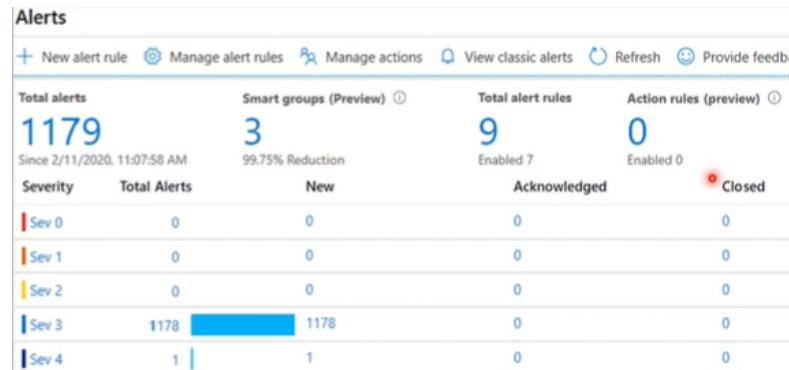
▼ Azure Advisor

- Consultor de nuvem personalizado
- Analisa sua configuração e recomenda soluções
- Alta disponibilidade, segurança, desempenho, excelência operacional e custo

▼ Azure Alerts

▼ Azure Monitor Alerts

- Experiência de autoria unificada
- Exibido por severidade
- Categorizado por Novo, Reconhecido e Fechado



- Nível 0 é o pior

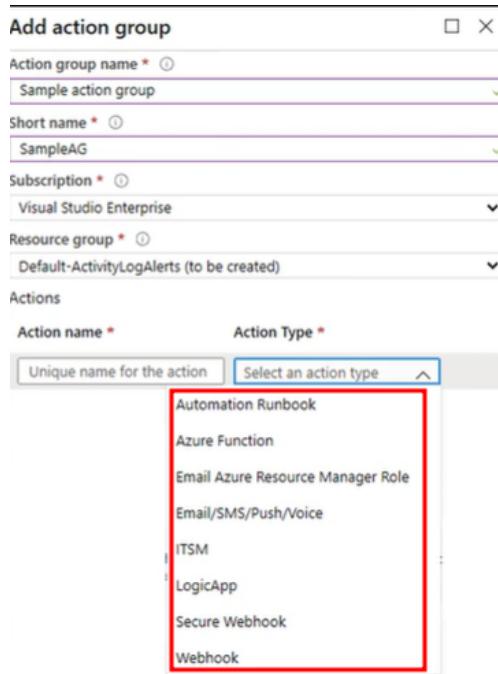
▼ Creating Alert Rules

- Resource: Seleção de alvo, critérios de alerta e lógica de alerta
 - Qual recurso ? Qual o criterio ?
- Condition: Nome, descrição e gravidade da regra de alerta (0 to 4)
 - 4 leve, e 0 critico

- Action group: notifique sua equipe por e-mail e mensagens de texto ou automatize ações usando webhooks e runbooks

▼ Action Groups

- Notifica um grupo de usuários que um alerta foi acionado
 - Através de uma função, podemos disparar para uma aplicação



- É uma coleção de preferências de notificação

▼ Log Analytics

▼ Log Analytics

- Um serviço que ajuda você a coletar e analisar dados gerados por recursos em seus ambientes de nuvem e locais
- Escreva consultas de registro e analise interativamente seus resultados
- Os exemplos incluem a avaliação de atualizações do sistema e solução de problemas de incidentes operacionais

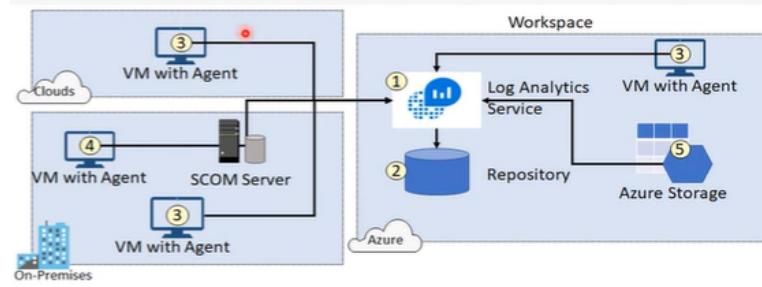
▼ Create a Workspace

- A workspace é um recurso do Azure e é um contêiner onde os dados são coletados, agregados, analisados e apresentados
 - Dentro do workspace haverá o custo
 - Local onde o dado estará centralizado, ou seja o local final
- Você pode ter vários workspaces por assinatura do Azure e pode ter acesso a mais de um espaço de trabalho
- Um workspace fornece uma localização geográfica, isolamento de dados e escopo

▼ Connected Sources

- Fontes conectadas geram dados
 - Pode coletar logs do ambiente on-prem

- Os dados podem ser coletados do Windows, Linux, SCOM e Azure Storage



▼ Data Sources

- As fontes de dados incluem: Logs de eventos do Windows, Windows performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs e Syslog.
- Cada fonte de dados possui opções de configuração adicionais

▼ Log Analytics Querying

- O Log Analytics fornece uma sintaxe de consulta
- Recupere e consolide dados rapidamente no repositório
- Salve ou faça com que as pesquisas de registro sejam executadas automaticamente para criar um alerta
- Exporte os dados para Power BI ou Excel

▼ Query Language Syntax

```

Event
| where (EventLevelName == "Error") --> Erro
| where (TimeGenerated > ago(1days)) --> DATA
| summarize ErrorCount = count() by Computer --> formato - contar quantos erros os computadores teve
Computer
| top 10 by ErrorCount desc --> Os 10 computadore que tiveram tal erro

```

▼ Network Watcher

▼ Network Watcher

- É um serviço regional
 - Deploy automatico, cria um RG com os recursos
- Fornece ferramentas para monitorar, diagnosticar, visualizar métricas e habilitar ou desabilitar registros
- Fornece monitoramento em nível de cenário para que você possa diagnosticar problemas em uma visão de nível de rede de ponta a ponta
- Fornece uma representação visual de seus elementos de rede

▼ Network Watcher Diagnostics

- IP Flow Verify diagnostica problemas de conectividade
- Next Hop determina se o tráfego está sendo roteado corretamente
- VPN Diagnostics soluciona problemas de gateways e conexões
- NSG Flow Logs mapeia o tráfego IP através de um grupo de segurança de rede
- Connection troubleshoot mostra a conectividade entre a VM de origem e o destino
- Topology gera um diagrama visual de recursos

- **Diagnostics - IP Flow Verify**
 - Diagnosticar problemas de conectividade de ou para a Internet e de ou para o ambiente local. Ideal para garantir que as regras de segurança sejam aplicadas corretamente.
- **Diagnostics - Next Hop**
 - Ajuda a determinar se o tráfego está sendo direcionado ao destino pretendido, mostrando o próximo salto
- **Diagnostics - Effective Security Rules**
 - Ajuda a solucionar problemas de gateways e conexões
 - Fornece informações resumidas e informações detalhadas
 - Pode solucionar problemas de vários gateways ou conexões simultaneamente
- **Diagnostics - VPN Troubleshoot**
 - Ajuda a solucionar problemas de gateways e conexões
 - Fornece informações resumidas e informações detalhadas
 - Pode solucionar problemas de vários gateways ou conexões simultaneamente
- **Diagnostics - Packet Capture**
 - Captura o tráfego de entrada e saída de uma máquina virtual
 - Salva dados em uma conta de armazenamento, um arquivo local ou ambos.
 - Como se fosse um wireshark
- **Diagnostics - Connection Troubleshoot**
 - Verifique a conectividade entre a VM de origem e o destino
 - Identifique os problemas de configuração que estão afetando a acessibilidade
 - Fornece todos os caminhos de salto a salto possíveis da origem ao destino
 - Analise a latência de salto a salto - mínimo, máximo e média entre a origem e o destino
 - Visualize uma topologia gráfica da sua origem ao destino

▼ Logs - NSG Flow Logs

- Visualize informações sobre o tráfego IP de entrada e saída por meio de um NSG
- Os registros de fluxo são gravados no formato JSON e mostram fluxos de entrada e saída de acordo com a regra
- O formato JSON pode ser exibido visualmente no Power BI ou em ferramentas de terceiros como Kibana
- Monitoring - Topology
 - Fornece uma representação visual de seus elementos de rede
 - Visualize todos os recursos em uma rede virtual, associações de recursos para recursos e relacionamentos entre os recursos
 - A instância do Network Watcher na mesma região da rede virtual

▼ Simulados de Revisão

AZ-Rv-ID Azure AD and Azure policies & Compliance  https://docs.google.com/forms/d/1yT2Vyx1dTp6TBVIJrVey_jhhim0BZT0ZEJ3ujzWQDgo/edit?usp=for ms_home&hs=true	<p>Nome de usuário de teste para diretório contábil. Controle quais que têm os seguintes atributos:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>User1</td> <td>Cloud User</td> </tr> <tr> <td>User2</td> <td>Administrador</td> </tr> </tbody> </table> <p>Centro com base no seguinte dispositivo Windows 10:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Join type</th> </tr> </thead> <tbody> <tr> <td>Device1</td> <td>Assigned</td> </tr> <tr> <td>Device2</td> <td>Azure AD joined</td> </tr> </tbody> </table> <p>Selecione quais grupos de segurança o dispositivo pertence:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Membership Type</th> <th>Owner</th> </tr> </thead> <tbody> <tr> <td>Group1</td> <td>Assigned</td> <td>User1</td> </tr> <tr> <td>Group2</td> <td>Dynamic Device</td> <td>User2</td> </tr> </tbody> </table> <p><input type="checkbox"/> User1 pode editar Device2 para o Group1</p> <p><input type="checkbox"/> User2 pode editar Device2 para o Group1</p> <p><input type="checkbox"/> User2 pode editar Device2 para o Group2</p>	Name	Role	User1	Cloud User	User2	Administrador	Name	Join type	Device1	Assigned	Device2	Azure AD joined	Name	Membership Type	Owner	Group1	Assigned	User1	Group2	Dynamic Device	User2
Name	Role																					
User1	Cloud User																					
User2	Administrador																					
Name	Join type																					
Device1	Assigned																					
Device2	Azure AD joined																					
Name	Membership Type	Owner																				
Group1	Assigned	User1																				
Group2	Dynamic Device	User2																				

AZ104-Rv-AzAdmin	<p>RBAC + ARM +CLI+Powershell</p> <p>https://docs.google.com/forms/d/1sYCJlWhQoexWchkn5lmTqJUF6TXAmyWUv-HiRro3o-Q/edit</p>
AZ104-Rv-NETWORK	<p>Az104 network revion questions</p> <p>https://docs.google.com/forms/d/1fX_EggTTTKmqBSmdV4xQWgr94oh96LgErvvhUciZE6g/edit</p>
AZ104-Rv-STO&DataProtecion	<p>Questions about storage, and data protecion services (bkp)</p> <p>https://docs.google.com/forms/d/1oDcz8VConCP0_D1-JLQP6-uEfATnk9V09cMuWAjcl8/edit</p>
AZ104-Rv-VMs&Severless	<p>Questions about vms and serverless</p> <p>https://docs.google.com/forms/d/1vQCXvxLlqvqO59EU5peAzZJFW0jDwVcYmOw2D9K0lhg/edit</p>
AZ104-Rv-Monitoring	<p>Questions about monitoring</p> <p>https://docs.google.com/forms/d/1smMCsaOGUsnnLBa3_Rl5otAoGMc0hAyZDqcm00G4o3c/edit</p>