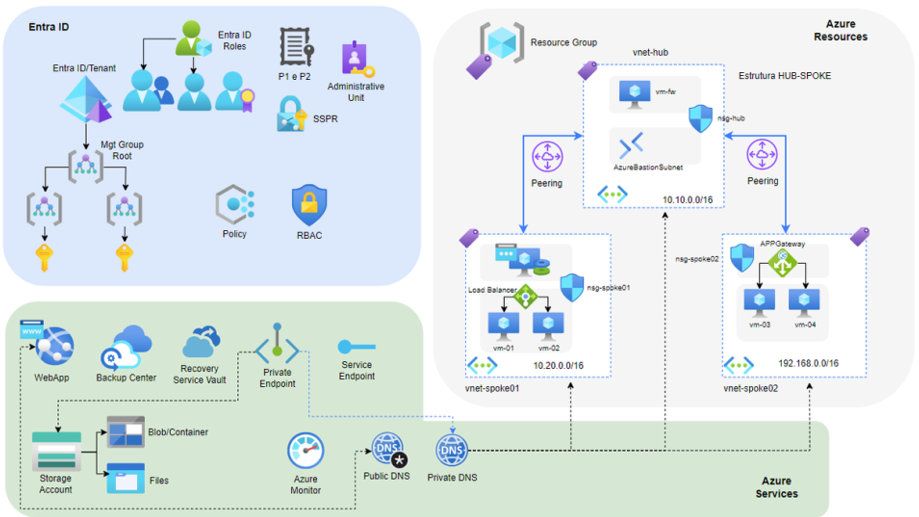
Rovati Tech Cloud

Laboratórios práticos com foco no AZ-104



Laboratórios práticos com foco no AZ-104

**1. Criar usuário**

- Criar 3 usuários nativos do tenant

- usuário 01 - global administrator

- usuário 02 - global administrator

- usuário 03 - nenhuma role do azure ad

- ajustar a senha para os 3 usuários

**2. RBAC**

- Add permissão de contributor para o usuário 03 no nível da Subscription

- Realizar teste criando um recurso Rg-Prod

**3. Criar Grupos**

- Grp TI e MKT

- Associar usuário de forma manual

- Associar usuário de forma automática

**4. Criar um novo Tenant**

- Criar um novo tenant e validar usuários e permissão

**5. Criar Policies**

- Add a tag to resources

- Allowed locations

**6. Criar o Resource Group PRD**

- Criar o Rg-Prod

**7. Virtual Network**

- Criar Vnet-Hub - 10.1.0.0/16 – UK South

- Criar Sub-Hub - 10.1.1.0/24

- Criar AzureBastionSubnet - 10.1.250.0/26

- Criar Vnet-Spk01 - 10.2.0.0/16 – UK South

- Criar Sub-Web - 10.2.1.0/24

- Criar Sub-AppGw - 10.2.250.0/24

- Criar Vnet-Spk02 - 10.3.0.0/16 – Australia East

- Criar Sub-Intra - 10.3.1.0/24

- Ajustar peering entre hub e spokes e testar as conexões entre as Vms

- Criar bastion (Bst-Prod)

**8. NSG**

- Criar e associar os NSGs - um para cada vnet

- Liberar acesso via RDP

- Fazer teste no NSG

- Criar ASG para liberar acesso RDP para servidores Web01 e Web02

**9. Virtual Machines**

- Criar Vm-Fw (Vnet-Hub) - UK South - B2S

* Sem redundância de zona
* Habilitar o IP forwarding

- Criar Vm-Web01 (Vnet-Spk01) - UK South - DS1\_V2

* Redundância zona 1

- Criar Vm-Web02 (Vnet-Spk01) - UK South - DS1\_V2

* Redundância zona 2

- Criar Vm-Intra01 (Vnet-Spk02) – Australia East - B2S

- Criar Vm-Intra02 (Vnet-Spk02) - Australia East - B2S

- Desabilitar o Firewall de todas as Vms

- Realizar teste de ping entre as Vms

- Validar ips estáticos e privados/públicos

- Realizar teste de conectividade com internet (site IIS) – liberar regra no NSG

- Deletar os ips públicos

**10. Configurar IIS Site (Vm-Web01 e Vm-Web02)**

*# Install IIS*

*Install-WindowsFeature -name Web-Server -IncludeManagementTools*

*# Remove default htm file*

*remove-item C:\inetpub\wwwroot\iisstart.htm*

*#Add custom htm file*

*Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Rovati Tech - Site Externo -" + $env:computername)*

**11. Configurar IIS Intranet (Vm-Intra01 e Vm-Intra02)**

*# Install IIS*

*Install-WindowsFeature -name Web-Server -IncludeManagementTools*

*# Remove default htm file*

*remove-item C:\inetpub\wwwroot\iisstart.htm*

*#Add custom htm file*

*Add-Content -Path "C:\inetpub\wwwroot\iisstart.htm" -Value $("Rovati Tech - Intranet -" + $env:computername)*

**12. Configurar Firewall**

- Habilitar IP forwarding na NIC

*Install-WindowsFeature RemoteAccess -IncludeManagementTools*

*Install-WindowsFeature -Name Routing -IncludeManagementTools -IncludeAllSubFeature*

*Install-WindowsFeature -Name "RSAT-RemoteAccess-Powershell"*

*Install-RemoteAccess -VpnType RoutingOnly*

*Get-NetAdapter | Set-NetIPInterface -Forwarding Enabled*

**13. Route Table**

- Criar as tabelas de roteamentos

- Não propagar rotas de Gateway

- Adiconar route table na Sub-Spk01

\* Route-Spk02

- Adiconar route table na Sub-Spk02

\* Route-Spk01

- Associar as rotas nas Subnets

**14. Criar zona de DNS Privada**

- Vnet-Hub - auto registration

- Vnet-Spk01 - auto registration

- Vnet-Spk02 - manual registration

- Criar o Virtual Network Link para cada Vnet para ser utilizado o nome do domínio interno (rovatitech.cloud), nas pesquisas

**15. Criar Storage Account**

- Criar um blob testar acesso anonimo

- Configurar azure files

- Restringir acesso via service endpoint

- Instalar Storage Explorer em um dos servers

- Testar acesso via SAS

- Configurar private endpoint para blob

- Configurar private endpoint para files

- Configurar virtual network link para as vnets no private dns

- Testar acesso de forma privada

**16. Configurar Load Balancer Interno**

- Configurar load balancer (standard, interno e regional)

- Adicionar o frontend IP (IP Vip = VipLbintra)

- Criar o backend pool para as Vms Intranet (Bkpool-Intra) e configurar na Nic

- Adicionar as duas Vms no backend pool

- Adicionar regras para o load balancer (Rule-Intra)

- Adicionar o Health Probe (Probe-Intra), protocolo HTTP

- Habilitar o TCP Reset

- Realizar o Create

- Fazer o teste de balanceamento entre as Vms Intra (parar o IIS de uma delas para testar (iisreset /stop)

**17. Configurar o Application Gateway**

- Configurar application gateway (standard V2) 2add as duas vms web no backend

- Habilitar o autoscalinge (mínimo: 1 e máximo: 2

- Adicionar o frontend IP (IP Público = Pip-AppGw01)

- Criar o backend pool para as Vms Web (Bkpool-Web) e configurar o tipo de target como Vms

- Configurar as regras de roteamento para o Aplication Gateway (Rule-Web) e colocar como prioridade 10

- Criar o Listener (Lst-Web) com frontend IP público na porta 80 e tipo como basic (caso tivesse 2 sites, o tipo seria o Multi site)

- Adicionar o backend targets e escolher o backend já configurado. Adicionar o backend settings (Stg-Web) na porta 80 (pois não temos um certificado para usar na porta 443), e manter o padrão para o restante da configuração.

- Adicionar o Health Probe (Probe-Intra), protocolo HTTP

- Realizar o Create

- Fazer o teste de balanceamento entre as Vms Web (parar o IIS de uma delas para testar (iisreset /stop)

**18. Estrutura de DR**

- Criar Rg-Dsr na região Brazil South

- Criar Vnet-Dsr – 192.168.0.0 /16 – Brazil South

- Criar Sub-Dsr - 192.168.1.0 /24 – Brazil South

- Criar uma Subnet para o Aplication Gateway (192.168.250.0 /24) – Brazil South

- Criar um Aplication Gateway (seguir as mesmas configurações da região principal, exceto ao backendpool, pois as Vms ainda não foram migradas da região principal para inserí-las nele)

- Desabilitar o “Soft Delete” no “Data Protection” do “Storage Account” de de origem (Rg-Prod), para realizar a replicação das Vms para essa região (Rg-Dsr).

- Criar um Recovery Service Vault, habilitar o Azure Site Recovery e habilitar a replicação das Vms do Azure

- Realizar o teste de failover com apenas uma Vm antes de fazer o failover definitivo

- Criar um plano de recovery para replicar todas as Vms de uma vez (essa opção encontra-se dentro do vault-dsr

- Desligar as Vms da origem para simular que a região está fora

- Testar virada para região de Dsr

- Commit para finalizar e Re-protect para replicar para a outra região quando for fazer o processo inverso.