



## **Módulo 2 – Soluções de Infraestrutura Básica**

**Bootcamp: Arquiteto Cloud Computing**

Osanam Giordane da Costa Junior

2020

## **Soluções de Infraestrutura Básica**

Bootcamp: Arquiteto Cloud Computing

Osanam Giordane da Costa Junior

© Copyright do Instituto de Gestão e Tecnologia da Informação.

Todos os direitos reservados.

## Sumário

---

Capítulo 1. Serviços de conectividade e rede da Azure, AWS e GCP .....	5
Introdução .....	5
Principais serviços de rede e comparativo de nomenclaturas .....	5
Azure Virtual Network (Vnet).....	9
Azure Express Route .....	11
Azure Virtual Network Gateway e VPN.....	13
Azure Virtual WAN .....	13
Azure Peering VNet .....	14
Azure Route Table .....	15
Azure DNS .....	16
Azure NAT Gateway .....	17
Virtual Machines e integração com Vnet na Azure .....	18
AWS Virtual Private Cloud (VPC) .....	18
AWS Route 53 .....	19
Virtual Machines e integração com VPC na AWS.....	20
Google Cloud Private Cloud (VPC).....	20
Virtual Machines e integração com VPC na GCP .....	20
Capítulo 2. Segurança e Governança no Microsoft Azure.....	21
Azure Network Security Group.....	21
Azure Policy .....	22
Azure Security Center .....	22
Capítulo 3. Virtualização e Containers na Azure .....	23
Azure Container Instance .....	23
Azure Container Registry .....	23

Capítulo 4. Armazenamento na Azure.....	25
Azure Storage account .....	25
Discos gerenciáveis .....	25
Capítulo 5. Escalabilidade, elasticidade e alta disponibilidade na Azure.....	27
Azure Virtual Machines Scale Set (VMSS) .....	27
Load balance de máquinas virtuais.....	29
Capítulo 6. Backup, monitoração e automação .....	30
Azure Backup.....	30
Azure Monitor.....	31
Azure Automation .....	32
Referências.....	34

## Capítulo 1. Serviços de conectividade e rede da Azure, AWS e GCP

---

### Introdução

---

O propósito deste material é que você tenha em mãos um apoio onde possa consultar, entender e aplicar no seu dia a dia ou no seu estudo os conceitos das ferramentas abordadas em cloud em nosso bootcamp.

Temos aqui tudo que foi abordado em nosso bootcamp, onde poderemos exemplificar na prática formas de implantação dos serviços hoje utilizado no Microsoft Azure, Amazon Webservices e Google Cloud Provider, abordando cada ponto dos serviços ensinados.

Espero que seja de ótimo proveito este material e que possa lhe auxiliar seja para você em sua nova caminhada de arquiteto de cloud, ou para você que já tenha experiência e busca sempre o aprendizado contínuo de novas tecnologias, que a todo momento são apresentadas a todos nós no que diz respeito a tecnologias voltadas ao mundo da computação em nuvem.

### Principais serviços de rede e comparativo de nomenclaturas

---

Hoje, nos três principais providers existentes, temos alguns serviços que são a base da estrutura de cloud no que dizem respeito a serviços de cloud básica, sendo elas:

- Redes virtuais ou VPCs:
  - A rede virtual ou VPC é uma seção logicamente isolada, onde você pode executar recursos da cloud em uma rede virtual definida por você.

Esta rede virtual é muito semelhante a rede tradicional que operamos em um datacenter, onde hoje deixamos de operar o ambiente físico para efetuar operações na modalidade SDN (Software-defined networking).




A tecnologia de rede definida por software é uma abordagem ao gerenciamento de rede, que permite uma configuração de rede dinâmica e

programaticamente eficiente para melhorar o desempenho e o monitoramento da rede, tornando-a mais parecida com a computação em nuvem do que com o gerenciamento de rede tradicional.

Desta forma, temos a possibilidade de configurar todo o ambiente de conectividade e rede sem a necessidade de uma configuração ou preocupação com appliances de rede como switches, roteadores, dentre outros.




Assim, as redes virtuais que trabalham como uma espécie de switch virtual nos auxiliam a segregar nosso ambiente em nuvem, a fim de manter ambientes isolados dos demais ambientes a serem criados em nossa cloud. Como temos hoje diversos serviços em nuvem, também temos uma diversidade de nomenclaturas de serviços em cada provider (provedor), que pode ter a mesma utilização, mas com nomes diferentes. Segue abaixo uma lista de nomenclaturas comparadas entre os três principais players de nuvem hoje do mercado:

### Computação:




Serviços	 <b>Amazon Web Services</b>	 <b>Google Cloud Platform</b>	 <b>Microsoft Azure</b>
Deploy, manage, and maintain virtual servers	<a href="#">Elastic Compute Cloud (EC2)</a>	<a href="#">Compute Engine</a>	<a href="#">Virtual Machines</a> <a href="#">Virtual Machine Scale Sets</a>
Management support for Docker/Kubernetes containers	<a href="#">EC2 Container Service (ECS)</a> <a href="#">Kubernetes (EKS)</a>	<a href="#">Kubernetes Engine</a> <a href="#">Container Engine</a>	<a href="#">Container Service</a> <a href="#">Container Service (AKS)</a>
Docker container registry	<a href="#">EC2 Container Registry (ECR)</a>	<a href="#">Container Registry</a>	<a href="#">Container Registry</a>
Integrate systems and run backend logic processes	<a href="#">Lambda</a>	<a href="#">Cloud Functions (Beta)</a>	<a href="#">Functions</a> <a href="#">Event Grid</a> <a href="#">Web Jobs</a>

Automatically scale instances	<a href="#">Auto Scaling</a>	<a href="#">Instance Groups</a>	<a href="#">Virtual Machine Scale Sets</a>  <a href="#">App Service Scale Capability (PAAS)</a>  <a href="#">Autoscaling</a>
-------------------------------	------------------------------	---------------------------------	--

### Armazenamento:




Serviços	 <b>Amazon Web Services</b>	 <b>Google Cloud Platform</b>	 <b>Microsoft Azure</b>
Object storage service for use cases	<a href="#">Simple Storage Services (S3)</a>	<a href="#">Google Cloud Storage</a>	<a href="#">Storage (Block Blob)</a>
Virtual server disk infrastructure	<a href="#">Elastic Block Store (EBS)</a>	<a href="#">Compute Engine Persistent Disks</a>	<a href="#">Storage (Page Blobs)</a>
Archive storage	<a href="#">S3 Infrequent Access (IA)</a> <a href="#">Glacier</a> <a href="#">Data Archive</a>	<a href="#">Nearline</a> <a href="#">Coldline</a>	<a href="#">Storage (Cool)</a> <a href="#">Storage (Archive)</a>
Create and configure shared file systems	<a href="#">Elastic File System (EFS)</a>	<a href="#">ZFS / Avere</a>	<a href="#">Files</a>
Backup	<a href="#">Object Storage</a> <a href="#">Cold Archive Storage</a> <a href="#">Storage Gateway</a>		<a href="#">Backup</a>
Automatic protection and disaster recovery	<a href="#">Disaster Recovery</a>	<a href="#">Disaster Recovery Cookbook</a>	<a href="#">Site Recovery</a>

## Redes e CDN:

Serviços	 <b>Amazon Web Services</b>	 <b>Google Cloud Platform</b>	 <b>Microsoft Azure</b>
Isolated, private cloud private networking	<a href="#">Virtual Private Cloud</a>	<a href="#">Virtual Private Cloud</a>	<a href="#">Virtual Network</a>
Cross-premises connectivity	<a href="#">API Gateway</a>	<a href="#">Cloud VPN</a>	<a href="#">VPN Gateway</a>
Manage DNS names and records	<a href="#">Route 53</a>	<a href="#">Google Cloud DNS</a>	<a href="#">Azure DNS Traffic Manager</a>
Dedicated, private network connection	<a href="#">Direct Connect</a>	<a href="#">Cloud Interconnect</a>	<a href="#">ExpressRoute</a>
Load balancing configuration	<a href="#">Elastic Load Balancing</a>	<a href="#">Cloud Load Balancing</a>	<a href="#">Load Balancer Application Gateway</a>



## Segurança:

Serviços	 <b>Amazon Web Services</b>	 <b>Google Cloud Platform</b>	 <b>Microsoft Azure</b>
Authentication and authorization	<a href="#">Identity and Access Management (IAM)</a> <a href="#">Organizations</a>	<a href="#">Cloud IAM</a> <a href="#">Cloud Identity-Aware Proxy</a>	<a href="#">Active Directory</a> <a href="#">Active Directory Premium</a>
Protect and safeguard with data encryption	<a href="#">Key Management Service</a>		<a href="#">Storage Service Encryption</a>
Hardware-based security modules	<a href="#">CloudHSM</a>	<a href="#">Cloud Key Management Service</a>	<a href="#">Key Vault</a>
Firewall	<a href="#">Web Application Firewall</a>		<a href="#">Application Gateway</a>
Cloud security assessment and certification services	<a href="#">Inspector</a> <a href="#">Certificate Manager</a>		<a href="#">Security Center</a> <a href="#">App Service Certificates</a>
Identity management	<a href="#">Cognito</a>		<a href="#">Active Directory B2C</a>

## Azure Virtual Network (Vnet)

A Rede Virtual do Azure (VNet) é o ponto principal na construção de seu ambiente de rede privada na Azure. A Vnet garante uma comunicação segura com a internet de suas Máquinas Virtuais e demais serviços ofertados que necessitem de uma comunicação interna ou externa. Além dos benefícios tradicionais de um datacenter, ela traz também benefícios voltados a escalabilidade, disponibilidade e isolamento.

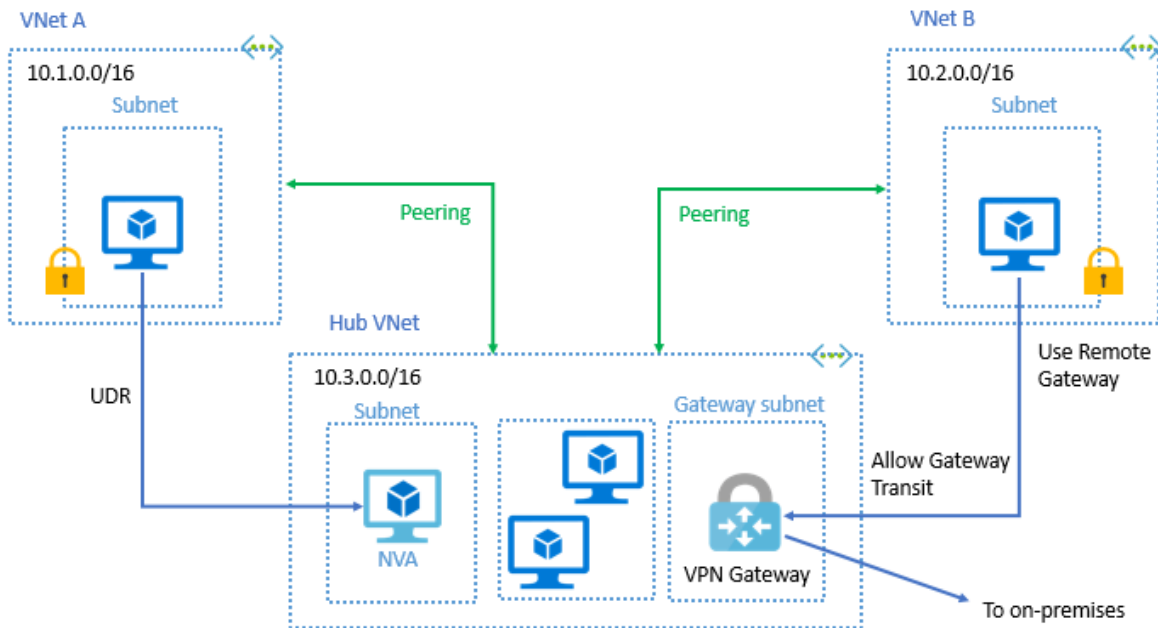
**Conceitos de VNet:**

- **Espaço de endereço:** na criação de sua VNet lhe é solicitada a deste address space para definição de seus IP Privado.
- **Sub-redes:** a sub-rede permite que você segmente a rede virtual em uma ou mais sub-redes, alocando uma parta do address space da sua VNet.
- **Regiões:** aqui você informa a região onde quer que a sua VNet seja criada, conforme região/localização, onde é possível a conexão de várias redes virtuais de regiões diferentes, efetuando o Peering das redes virtuais.

**Práticas recomendadas:**

- Cuidado para não sobrepor espaços de endereço.
- Suas sub-redes não devem abranger todo o espaço de endereço da VNet. Planeje com antecedência e reserve algum espaço de endereço para o futuro.
- Recomendamos que você tenha menos VNets maiores do que várias VNets pequenas. Isso evitará a sobrecarga no gerenciamento.
- Projeta suas VNets atribuindo NSGs (Grupos de Segurança de Rede) às sub-redes abaixo deles.

Segue topologia exemplo de uma VNet:



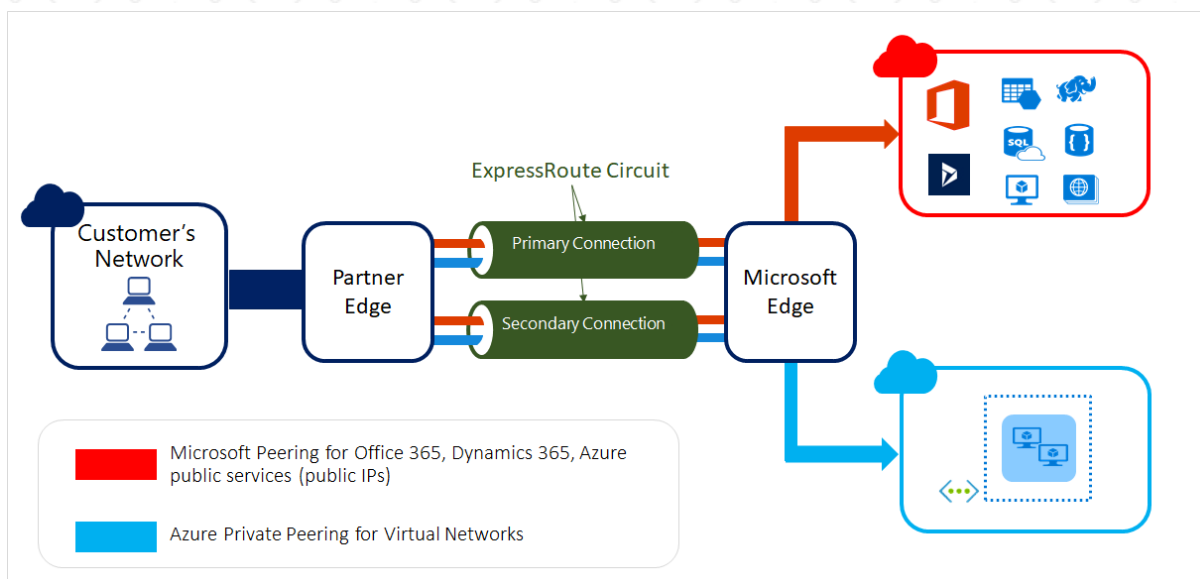
**Fonte:** [docs.microsoft.com](https://docs.microsoft.com/pt-br/office/onenote/onenote-features).

## Azure Express Route

O Express Route possibilita criar uma estrutura híbrida de comunicação utilizando um parceiro Microsoft, fechando conexão direta com o Microsoft Azure.

Com esta possibilidade você terá uma menor latência na comunicação com a nuvem Azure e possibilidade de uma comunicação dedicada, de alta performance e com maior segurança.

Para criação do Express Route, você terá que efetuar contato diretamente com a Microsoft, que fará os tramites e indicará os parceiros para que possa efetuar a aquisição dos circuitos de dados e assim poderá fechar a comunicação configurando todo ambiente.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

Home > ExpressRoute circuits >

**CMS-SPBR-PRD-XR**  
ExpressRoute circuit

Search (Ctrl+/) Delete Refresh

**Overview**

Resource group (change)  
NET-SPBRVNET-RG

Circuit status  
Enabled

Location  
Brazil South

Subscription (change)

Subscription ID  
[REDACTED]

Tags (change)

Provider  
Equinix

Provider status  
Provisioned

Peering location  
Sao Paulo

Bandwidth  
1000 Mbps

Service key  
[REDACTED]

**Peerings**

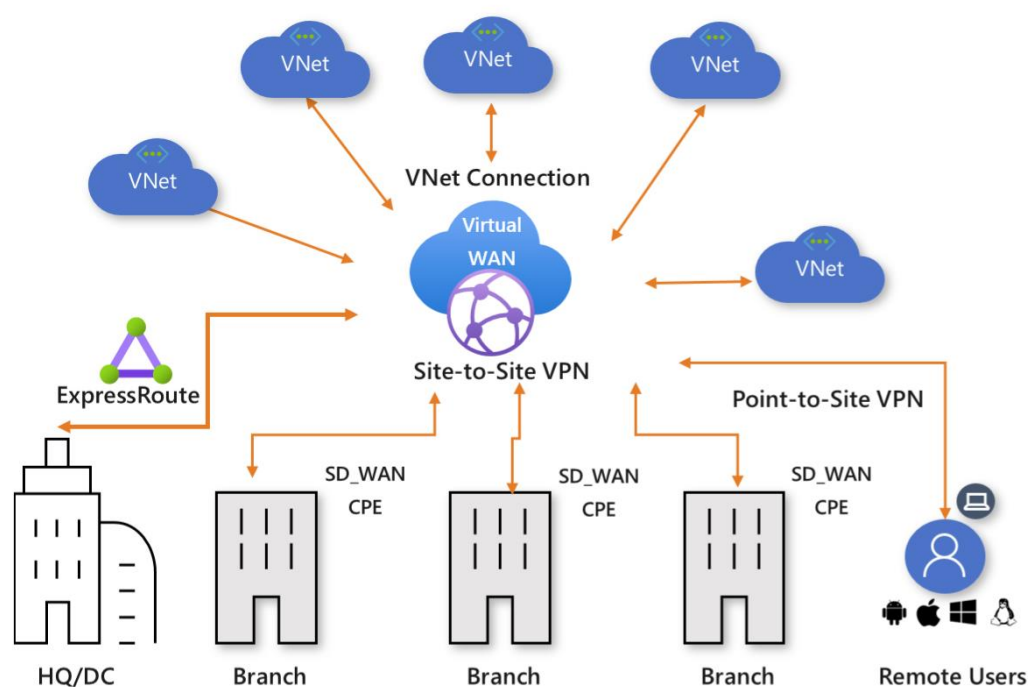
Type	Status	Primary subnet	Secondary subnet	Last modified by
Azure private	Provisioned	[REDACTED]	[REDACTED]	Customer
Azure public	Not provisioned	-	-	-
Microsoft	Not provisioned	-	-	-

## Azure Virtual Network Gateway e VPN

Um gateway de VPN é um tipo específico de gateway de rede virtual, usado para enviar tráfego criptografado entre uma rede virtual do Azure e um local pela internet pública. Você também pode usar um gateway VPN para enviar tráfego criptografado entre redes virtuais do Azure pela rede da Microsoft.

## Azure Virtual WAN

Azure virtual WAN é um serviço da Azure onde há a possibilidade de se criar Hubs de comunicação e integrar VNet, VPN Site-to-Site, Express Route, filiais e VPN Point-to-Site, a fim de se ter um único ambiente de gerenciamento de conectividade entre estes ambientes.

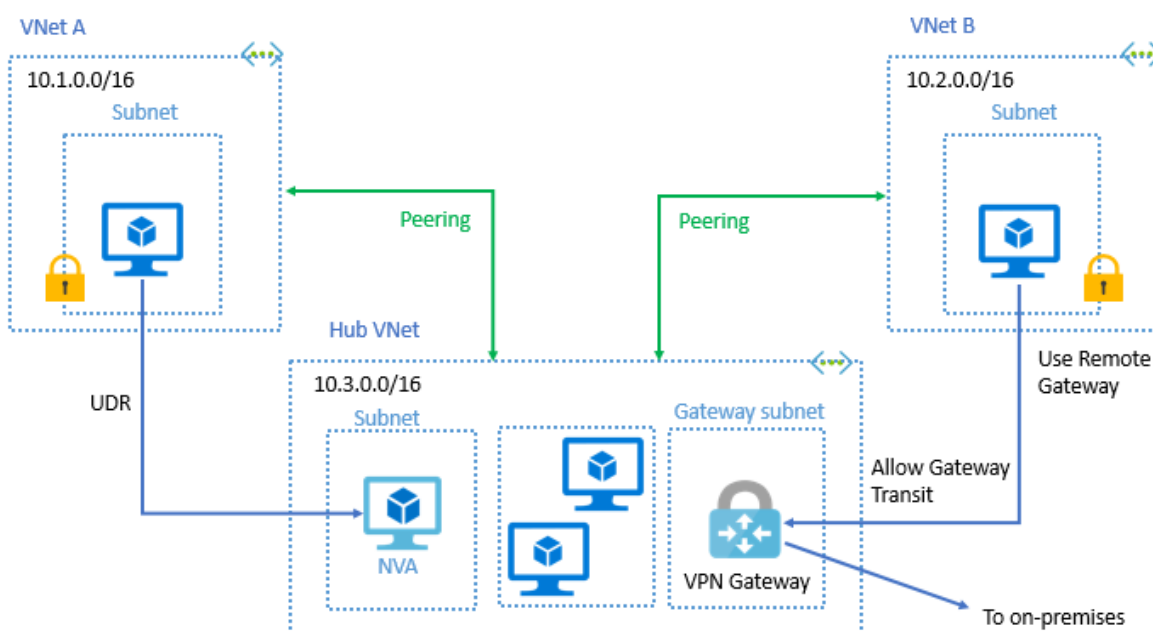


Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Azure Peering VNet

Com o Peering você tem a possibilidade de integrar VNet umas as outras, sem a necessidade de criação de VPNs para comunicação entre essas VNets.

As VNets podem estar contidas em uma mesma subscription ou em subscriptions diferentes, e você conseguirá comunicação com menor latência e performance que a utilização de uma VPN.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

### Restrições para Peering em VNets:

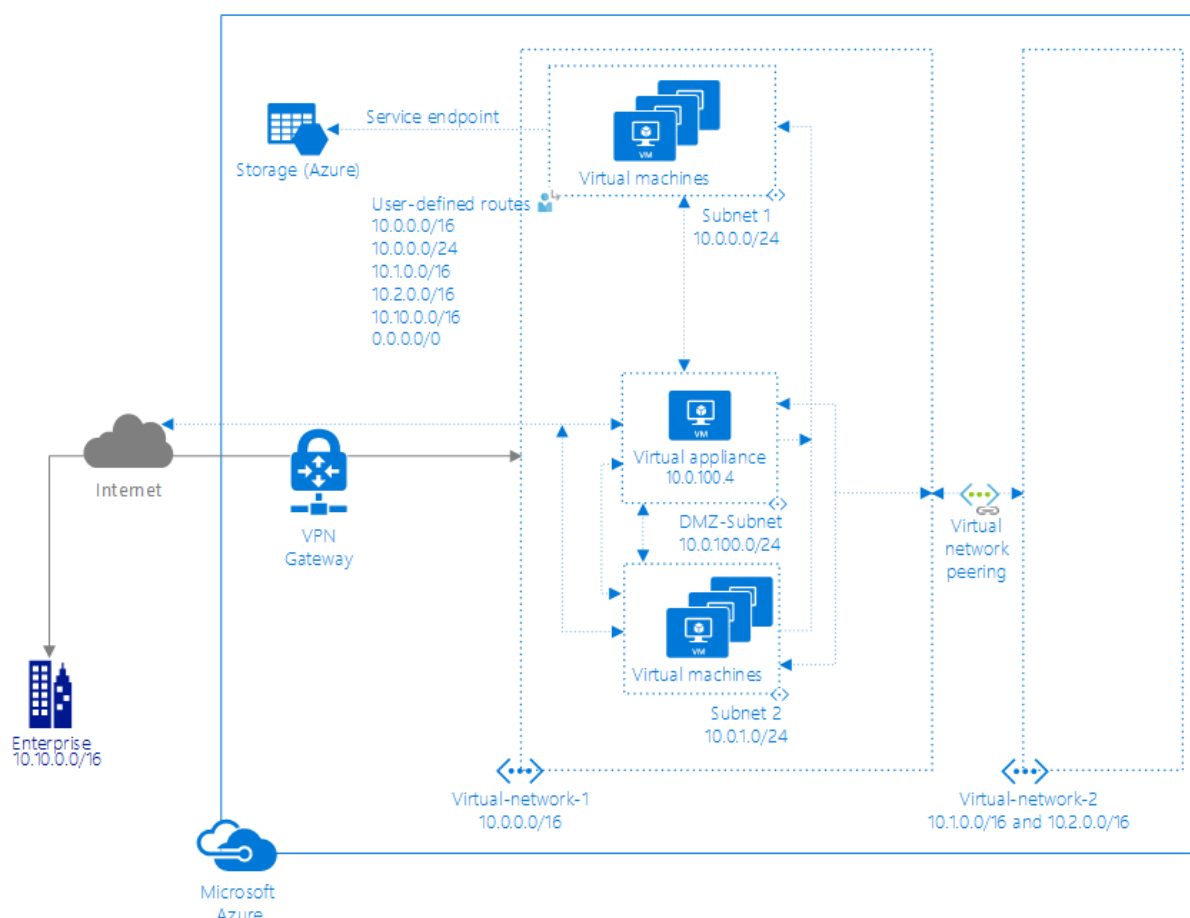
As seguintes restrições se aplicam somente quando as redes virtuais são emparelhadas globalmente:

- Os recursos em uma rede virtual não podem se comunicar com o endereço IP de front-end de um Load Balancer interno básico (ILB), em uma rede virtual emparelhada globalmente.
- Alguns serviços que usam um balanceador de carga básica não funcionam em emparelhamento de rede virtual global.

## Azure Route Table

As Route Tables são utilizadas nos casos de necessidade de se criar rotas específicas dentro de sua VNet ou até mesmo de máquinas virtuais, pois há a possibilidade de segregar a sua rede e manter rotas estáticas necessárias a comunicação de seu ambiente híbrido.

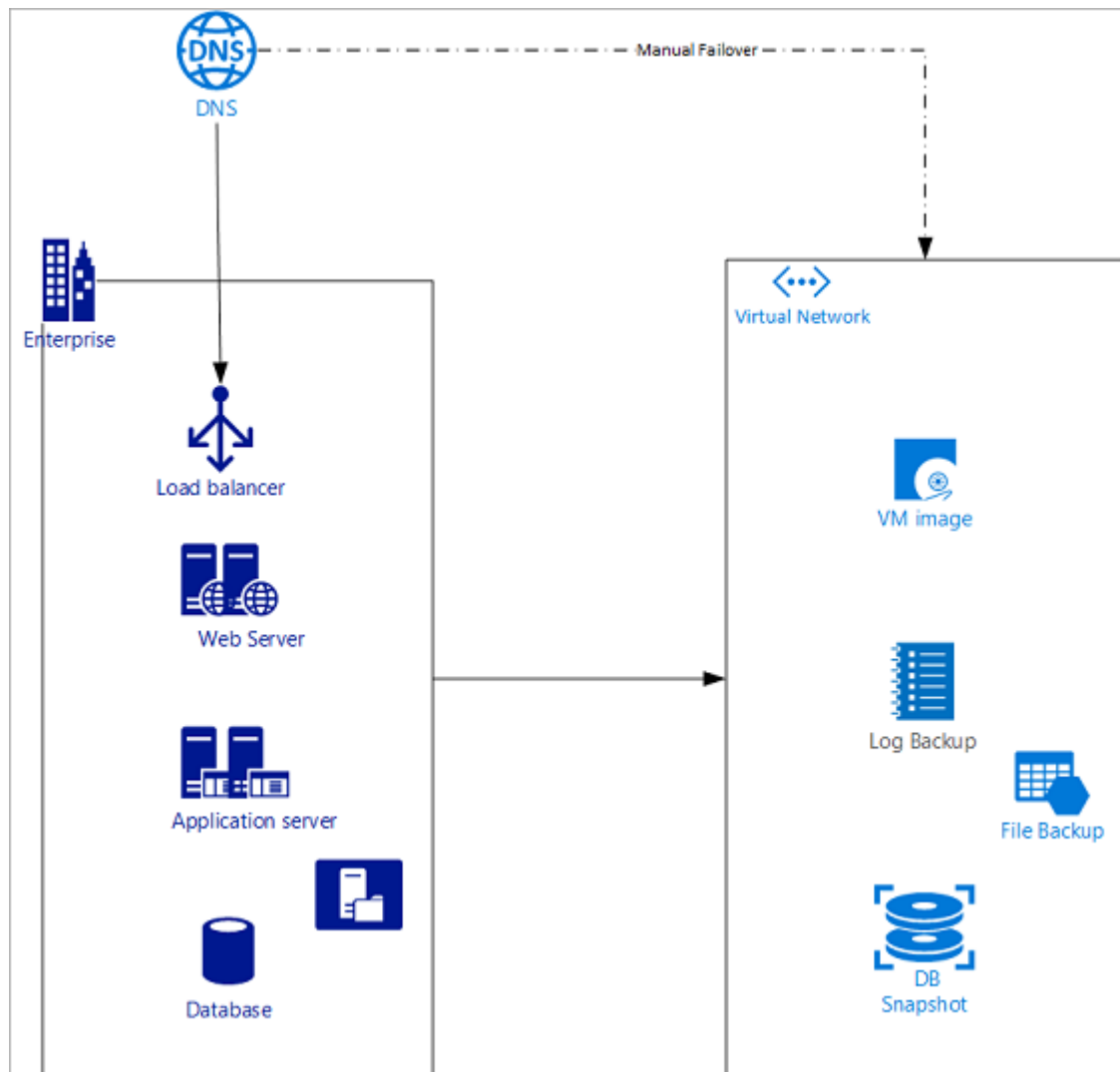
As rotas podem ser criadas diretamente pelo serviço de Route Table e atachadas conforme necessidade



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Azure DNS

Azure DNS e DNS Private provê a possibilidade de utilizar os serviços PaaS de resolução de nomes, seja ele interno ou externo, sem a necessidade de criação de um ambiente DNS em servidores ou serviços internos de resolução de nomes, como BIND (Linux) ou Microsoft Windows Server DNS service.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).



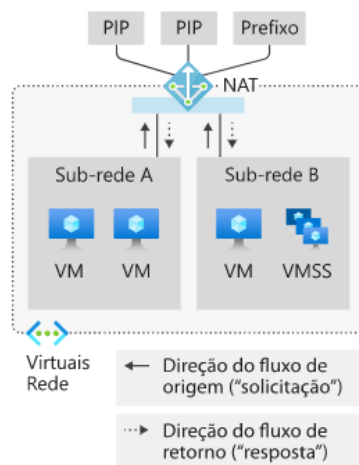
## Azure NAT Gateway

Recursos de gateway da NAT são parte da NAT de Rede Virtual e fornecem conectividade com a Internet de saída para uma ou mais sub-redes de uma rede virtual.

A sub-rede da rede virtual declara qual gateway da NAT será usado. A NAT fornece a SNAT (conversão de endereços de rede de origem) para uma sub-rede. Os recursos do gateway da NAT especificam quais máquinas virtuais de endereço IP estático usar ao criar fluxos de saída.

Endereços IP estáticos vêm de recursos de endereço IP público, recursos de prefixo IP público ou de ambos. Se um recurso de prefixo de IP público for usado, todos os endereços IP de todo o recurso de prefixo de IP público serão consumidos por um recurso de gateway da NAT.

Este recurso é muito utilizado no momento em que temos um Load Balancer em nosso ambiente, onde mantemos o tráfego de entrada no load balance e o tráfego de saída via NAT das aplicações sobre o serviço de NAT de portas.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Virtual Machines e integração com Vnet na Azure

---

As VMs do Azure são um dos vários tipos de recursos de computação escalonáveis sob demanda oferecidos pelo Azure. Com as VMs, você tem controle total sobre a configuração e pode instalar qualquer coisa que precisar para realizar o trabalho. Você não precisa comprar o hardware físico quando precisar dimensionar ou estender o datacenter.

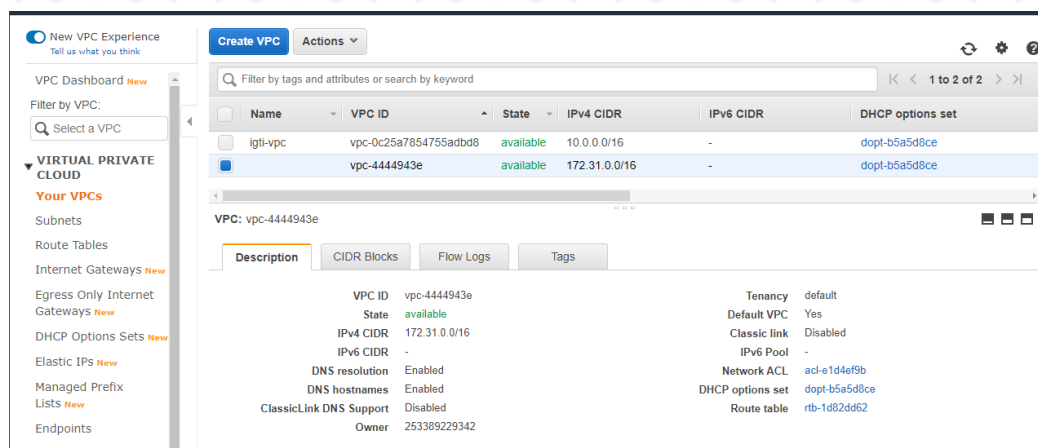
Para criação de uma Máquina virtual, devemos criar um ambiente de rede via VNet, ou gerar a nova VNet no momento de seu provisionamento, ou utilizar uma já existente. Desta forma, o ambiente já nascerá dentro da estrutura arquitetada para cloud Azure.

## AWS Virtual Private Cloud (VPC)

---

Uma VPC tem o mesmo conceito de uma VNet Microsoft, com algumas diferenças em sua arquitetura, como é o caso de uma necessidade de acesso a internet de sua VM ou VPC, uma vez que há a necessidade de se criar uma Gateways da internet e assim atachar a sua VPC, para que suas VM ou serviço tenha acessos direto para a internet. Caso contrário, a mesma não terá a conectividade necessária para a internet.

As demais funcionalidades de uma VPC são bem parecidas aos da VNet Azure, onde no mesmo formato um ambiente cloud não poderá nascer sem uma VPC criada e estruturada.



The screenshot shows the AWS VPC console. On the left, there's a sidebar with navigation options like 'Subnets', 'Route Tables', 'Internet Gateways', etc. The main area displays a table of VPCs. Below the table, the details for VPC 'vpc-4444943e' are shown, including its CIDR blocks, DNS settings, and DHCP options set.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
igti-vpc	vpc-0c25a7854755adb8	available	10.0.0.0/16	-	dopt-b5a5d8ce
vpc-4444943e	vpc-4444943e	available	172.31.0.0/16	-	dopt-b5a5d8ce

**VPC: vpc-4444943e**

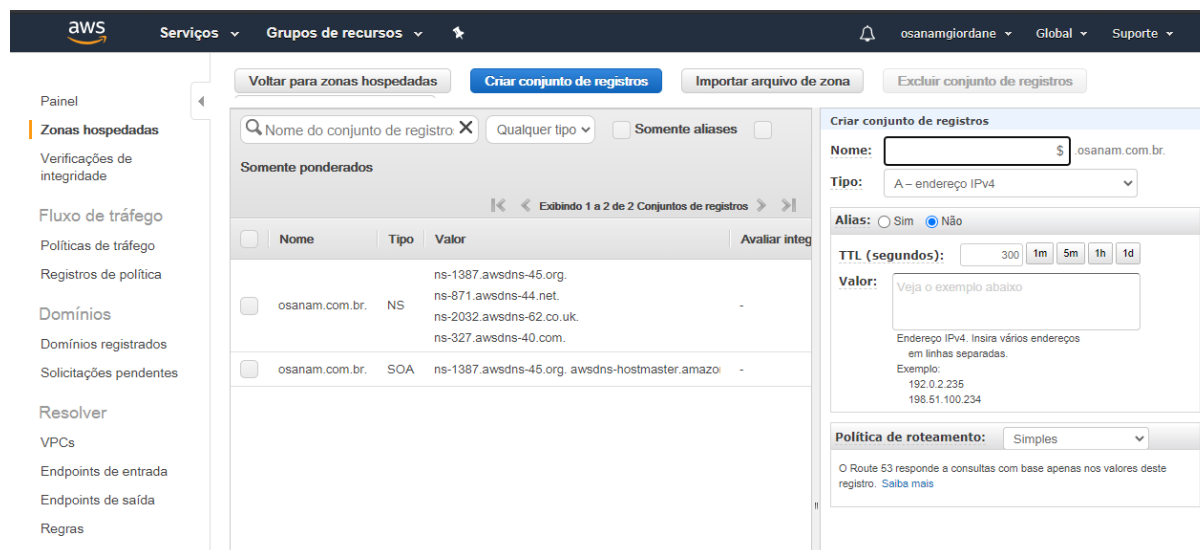
Description	CIDR Blocks	Flow Logs	Tags
VPC ID	vpc-4444943e		
State	available		
IPv4 CIDR	172.31.0.0/16		
IPv6 CIDR	-		
DNS resolution	Enabled		
DNS hostnames	Enabled		
ClassicLink DNS Support	Disabled		
Owner	253389229342		

Tenancy	default
Default VPC	Yes
Classic link	Disabled
IPv6 Pool	-
Network ACL	acl-e1d4ef9b
DHCP options set	dopt-b5a5d8ce
Route table	rtb-1d82dd62

## AWS Route 53

O Route 53 é o serviço da AWS, encarregado de prover serviços de resolução de nomes, seja sua necessidade de uma resolução de nomes externas para suas aplicações, seja para resolução de nomes em sua rede privada AWS e híbrida.

Desta forma, você terá um serviço PaaS, não necessitando de servidores com serviços de DNS ativados, facilitando ainda mais a gestão do ambiente DNS.



The screenshot shows the AWS Route 53 console. The left sidebar contains navigation options like 'Zonas hospedadas', 'Fluxo de tráfego', 'Domínios', etc. The main area displays the 'Criar conjunto de registros' (Create record set) page. It includes a search bar for the record set name, a table of existing record sets, and a form to create a new record set.

**Criar conjunto de registros**

Nome:  Tipo:

Alias: ☐ Sim ☒ Não

TTL (segundos):  1m 5m 1h 1d

Valor:

Endereço IPv4. Insira vários endereços em linhas separadas.  
Exemplo:  
192.0.2.235  
198.51.100.234

Política de roteamento:

O Route 53 responde a consultas com base apenas nos valores deste registro. [Saiba mais](#)

## Virtual Machines e integração com VPC na AWS

---

Da mesma forma que vimos que ao criar uma VM na Azure há a necessidade de sua VNet ou criação, na AWS não há diferenças. A forma de criação é similar, onde serão necessários os dados relacionados a nova VM, como size da VM, disco e VPC a ser integrada.

## Google Cloud Private Cloud (VPC)

---

A VPC em um ambiente de cloud da GCP se iguala as configurações de uma VPC AWS, possibilidade conectividade tanto internamente quanto externamente e de modo híbrido em seu ambiente de cloud.

Para conexão a internet, ele não se iguala a AWS, mas sim a Azure, onde assim que se cria a conexão, ao criar uma VM, a conexão à internet já é criada ao atachar um IP Público.

## Virtual Machines e integração com VPC na GCP

---

O formato é o mesmo para a criação de uma VM na GCP e integração com sua VPC. A forma de criação é similar, onde serão necessários os dados relacionados a nova VM, como size da VM, disco, VPC a ser integrada e também a criação de chaves de acesso após geração da VM, como na AWS.

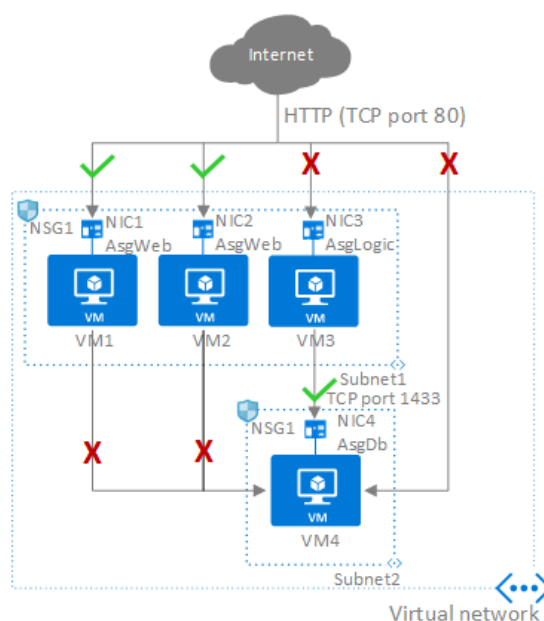
## Capítulo 2. Segurança e Governança no Microsoft Azure

### Azure Network Security Group

Você pode usar o Network Security Group do Azure para filtrar o tráfego de rede de e para recursos do Azure em uma rede virtual do Azure.

Um Network Security Group contém regras de segurança que permitem ou negam o tráfego de rede de entrada ou de saída em relação a vários tipos de recursos do Azure. Para cada regra, você pode especificar origem e destino, porta e protocolo.

O Network Security Group não é um firewall, ele somente te dá a possibilidade de criar ACL de inbound e outbound. Para a necessidade de filtragem de websites e protocolos específicos há a necessidade de se ter implantado um firewall, como exemplo o serviço Azure Firewall mostrado em nosso módulo.



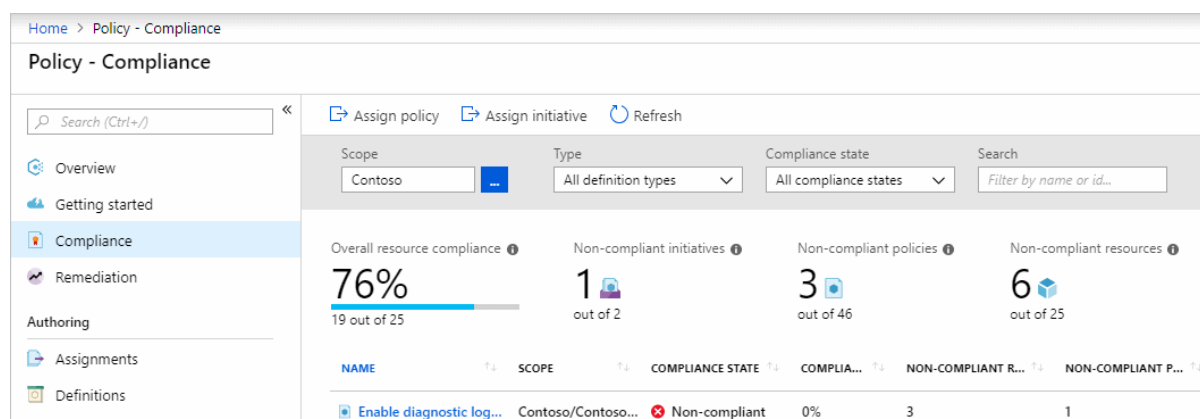
Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Azure Policy

As políticas do Azure te darão a possibilidade de efetuar uma governança de seu ambiente cloud de forma automatizada e com maior controle, uma vez que poderá criar políticas ou grupo de políticas personalizadas em seu ambiente cloud.

Caso seja necessário gerenciar seu ambiente e efetuar bloqueios para evitar custos desnecessários, como a possibilidade de bloqueio de criação de serviços em regiões que não há o interesse e de custos maior, você poderá criar políticas ou usar as políticas exemplo para o mesmo.

Sua edição pode ser feita diretamente em seu arquivo JSON, o que neste caso, como pré-requisito, seria necessário conhecer o formato para edição.



## Azure Security Center

O Security Center é uma suíte que engloba ferramentas utilizando a inteligência artificial Azure, com o Azure advisor para lhe auxiliar no gerenciamento de vulnerabilidades, falhas ou melhores práticas de seu ambiente, seja ele cloud, on-premises, outras nuvens ou híbrido.

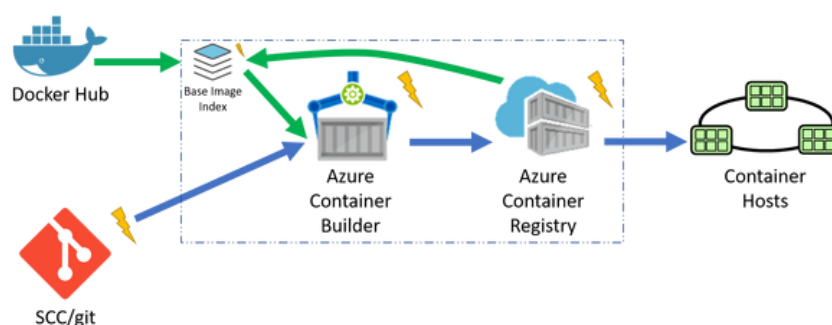
Com ele você terá a oportunidade de automatizar processos e ter uma maior governança.

## Capítulo 3. Virtualização e Containers na Azure

### Azure Container Instance

O ACI trabalha em um formato novo chamado Serverless (sem servidor), onde o conceito é ter um servidor que é transparente para o arquiteto cloud, e o arquiteto pode se preocupar somente com suas containers criadas no ambiente, e não há a necessidade de se preocupar com a engine e container (Docker) que roda no mesmo. Assim, terá a possibilidade de hospedar seus containers, rodar diretamente do Azure e criar grupos de containers para prover Alta Disponibilidade.

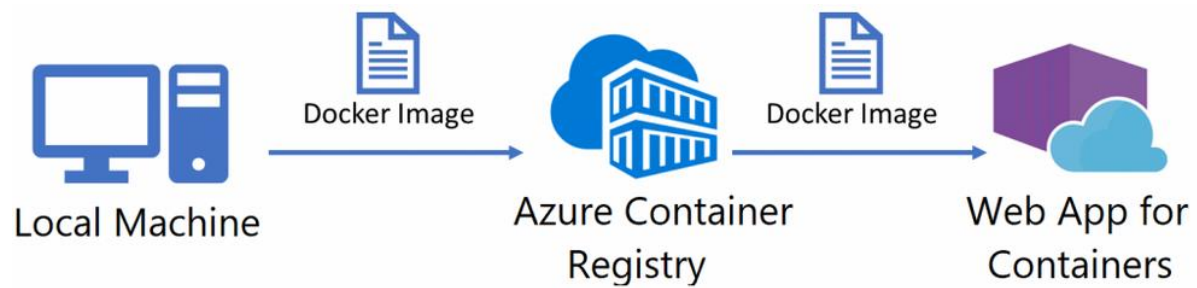
Há ainda a possibilidade de utilização de suas imagens públicas ou imagens privadas, sejam elas armazenadas em seu Azure Container Registry ou outro registry privado.



Fonte: <https://khanasif1.wordpress.com/category/azure-container-registry/>.

### Azure Container Registry

Já o ACR é o repositório de armazenamento de suas imagens de container geradas e provisionadas conforme sua necessidade, onde pode ser utilizado como registry externo de outros ambientes, interno do Azure ou até mesmo integrada a suas aplicações web na Azure. Há funcionalidades para expurgo de imagens não utilizadas, segurança e avaliação de vulnerabilidades integrada ao Azure Security Center e gerenciamento via APIs de comunicação.



**Fonte:** <https://techcommunity.microsoft.com/t5/wiki-ninjas-blog/ms-wiki-article-spotlight-azure-custom-docker-container-in/ba-p/1359465>.



## Capítulo 4. Armazenamento na Azure

---

### Azure Storage account

---

Uma conta de armazenamento do Azure contém todos os seus objetos de dados do Armazenamento do Azure: blobs, arquivos, filas, tabelas e discos.

A conta de armazenamento fornece um namespace exclusivo para os dados do armazenamento do Azure, que podem ser acessados de qualquer lugar do mundo por HTTP ou HTTPS.

Os dados em sua conta de armazenamento do Azure são duráveis e altamente disponíveis, seguros e amplamente escalonáveis.

- Tipos de contas de armazenamento:
  - **Contas de uso geral v2:** tipo de conta de armazenamento básico. Recomendado para a maioria dos cenários que usam o Armazenamento do Azure.
  - **Contas de uso geral v1:** tipo de conta herdada para BLOBs, arquivos, filas e tabelas. Use contas de uso geral v2 em vez desta opção, quando possível.
  - **Contas BlobStorage:** contas de armazenamento somente blob herdadas. Use contas de uso geral v2 em vez desta opção, quando possível.

As contas de armazenamento podem ser utilizadas como discos atachado em suas VMs, mas não é recomendável por não ter uma alta performance para discos de servidores.

### Discos gerenciáveis

---

Os Azure Managed Disks são volumes de armazenamento em nível de bloco, que são gerenciados pelo Azure e usados com Máquinas Virtuais do Azure.

Os discos gerenciados são como um disco físico em um servidor local, mas virtualizado. Com os discos gerenciados, basta especificar o tamanho e o tipo de disco e provisioná-lo.

Os tipos disponíveis de discos são: Discos Ultra, SSD (unidades de estado sólido) Premium, SSDs Standard e HD (unidades de disco rígido) Standard. Os discos SSDs possuem um desempenho maior que os discos HDD, por se tratarem de discos lógicos, diferente do discos HDD que são mecânicos.

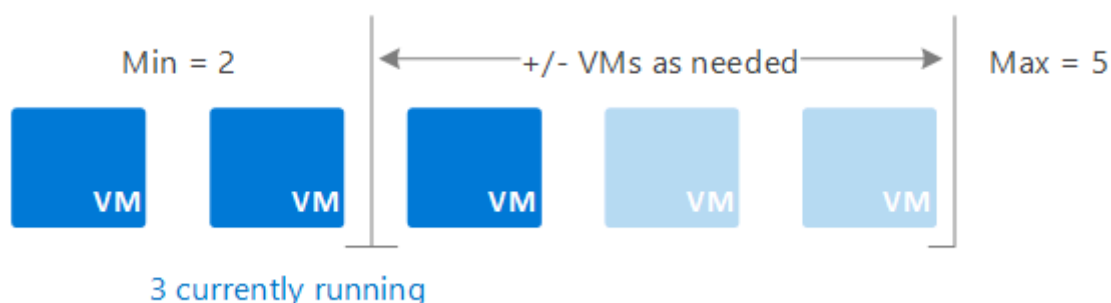
## Capítulo 5. Escalabilidade, elasticidade e alta disponibilidade na Azure

### Azure Virtual Machines Scale Set (VMSS)

O VMSS é utilizado para que possamos escalar nossas máquinas virtuais de forma horizontal, a fim de que se houver a necessidade no momento de mais servidores idênticos, o VMSS cria novas instâncias do workload principal para suprir a necessidade de recursos (vCPU, Memória RAM e Disco), e assim mantém seu ambiente em pleno funcionamento, evitando que o negócio sofra com a falta de recursos e pare.

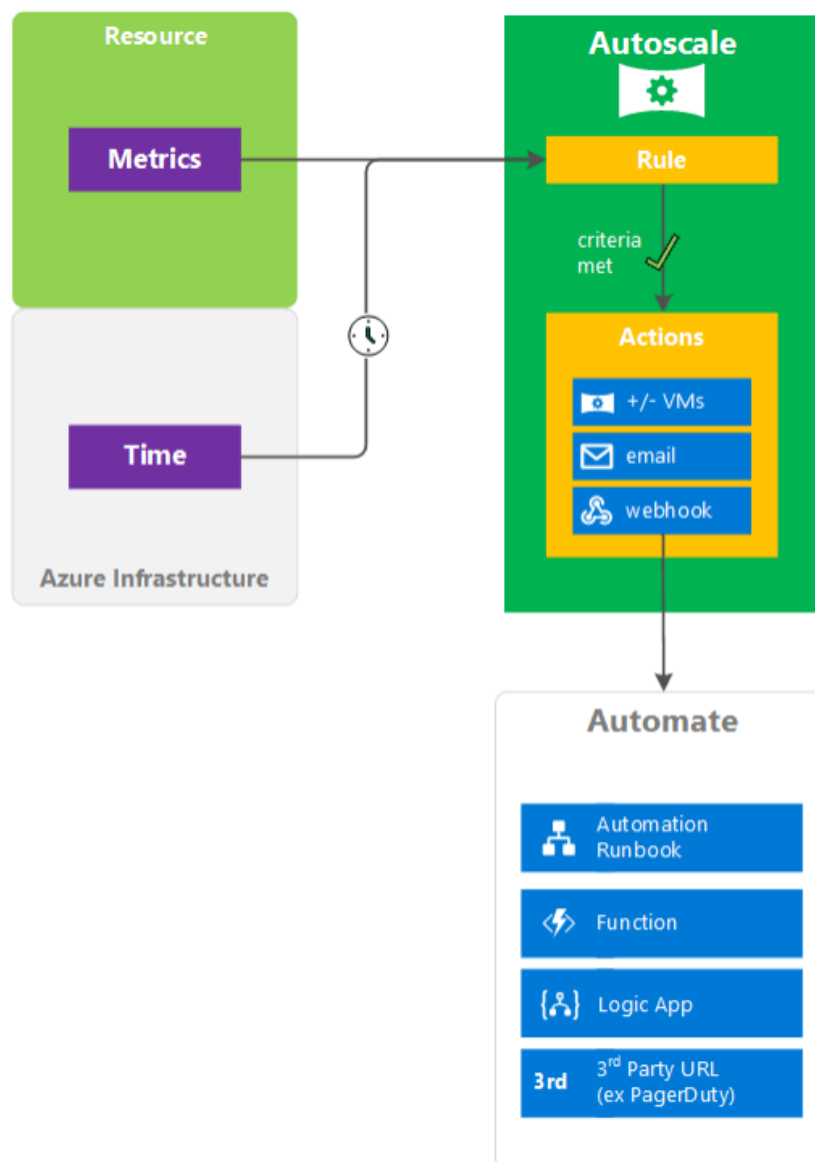
Este é um dos benefícios chave da cloud, pois você tem a possibilidade de uso momentâneo de novos recursos, sem que seja necessário manter após o ambiente, por não necessitar mais dessas “cópias” provisionadas.

Com o VMSS você também tem um ambiente automatizado de balanceamento de cargas, sem necessidade de criação de novos workloads e configuração como é feito hoje em ambientes de Datacenter ou on-premises.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

**Figura – Forma de atuação do autoscale integrado ao VMSS.**



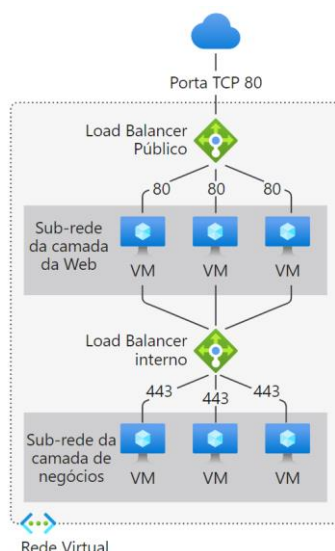
Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Load balance de máquinas virtuais

O Load Balance é o ponto de contato único para clientes. Ele distribui fluxos de entrada, que chegam nas instâncias de pool de front-end a back-end do balanceador de carga. Esses fluxos ocorrem de acordo com as investigações de integridade e regras de balanceamento de carga especificadas. As instâncias do pool de back-end podem ser Máquinas Virtuais ou instâncias do Azure em um conjunto de dimensionamento de máquinas virtuais.

Um balanceador público de carga pode fornecer conexões de saída para VMs (máquinas virtuais) dentro de sua rede virtual. Essas conexões são realizadas por meio da tradução dos endereços IP privados para endereços IP públicos. Os balanceadores de carga públicos são usados para balancear a carga do tráfego de Internet para suas VMs.

Um balanceador de carga interno (ou privado) é usado quando IPs privados são necessários apenas no front-end. Os balanceadores de carga internos são usados para balancear a carga do tráfego dentro de uma rede virtual. Um front-end do balanceador de carga pode ser acessado de uma rede local em um cenário híbrido, de forma a manter o seus serviços com Alta disponibilidade.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

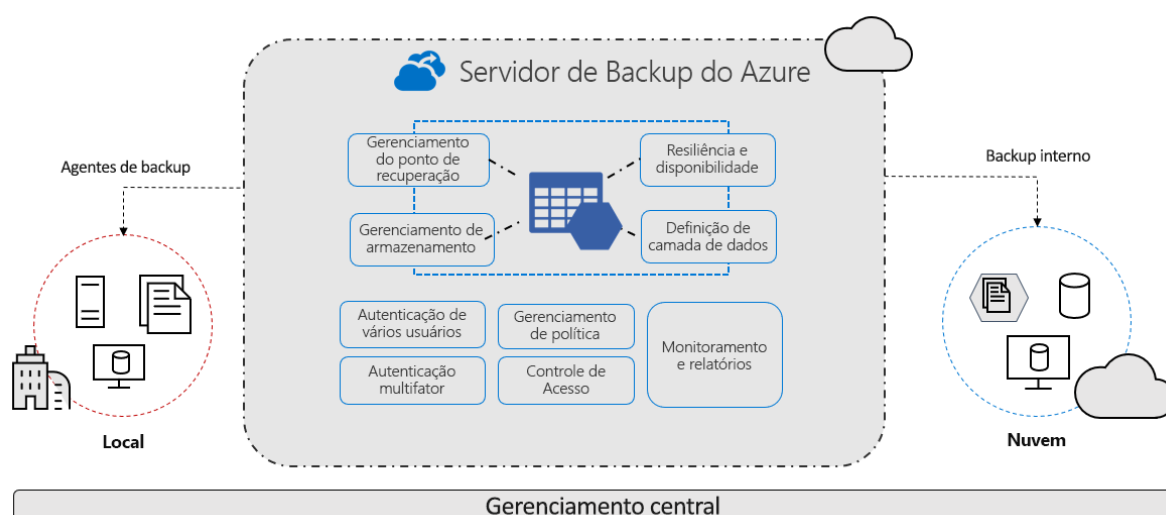
## Capítulo 6. Backup, monitoração e automação

### Azure Backup

Azure Backup é a ferramenta nativa da Azure, que pode ser utilizado para backup de workload e serviços Azure, assim como para ambientes que não estejam na cloud Azure ou também para ambiente on-premises.

Com ele você deixa de manter o backup local para não se preocupar com a segurança de se ter backups íntegros e livres de ataques, como Ransomware.

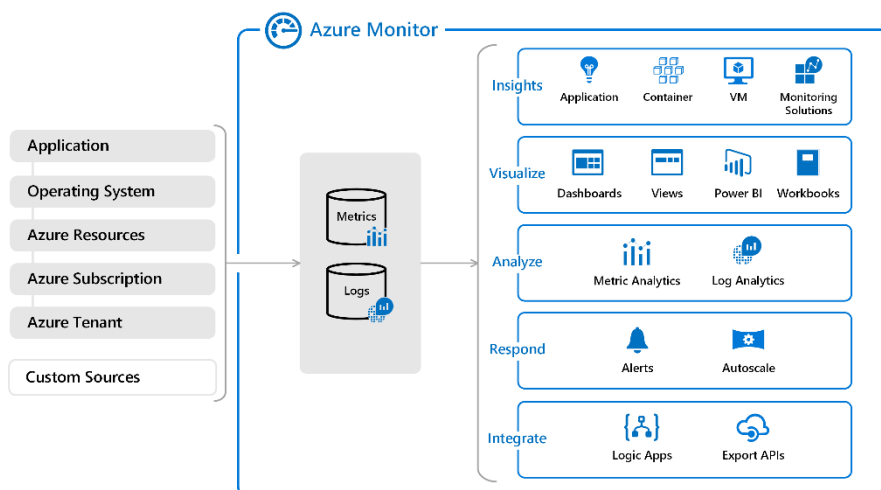
Facilidade de dimensionamento e seguro, o Azure Backup mantém seus dados seguros conforme o tempo que você configurar e ainda com opção de redundância em datacenter Microsoft.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Azure Monitor

Azure Monitor é a suíte de serviços de monitoramento de recursos Azure, onde há a possibilidade de se ter um monitoramento completo, seja de seus workloads VMs, aplicação web (App Services), functions, containers ou até mesmo seus databases PaaS Azure.



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

- Quais dados são coletados pelo Azure Monitor?
  - **Dados de monitoramento de aplicativo:** os dados sobre o desempenho e a funcionalidade do código que você gravou, independentemente da plataforma.
  - **Dados de monitoramento de SO Convidado:** dados sobre o sistema operacional no qual seu aplicativo está em execução. Ele pode estar em execução no Azure, em outra nuvem ou localmente.
  - **Dados de monitoramento de recursos do Azure:** dados sobre a operação de um recurso do Azure.
  - **Dados de monitoramento de assinatura do Azure:** dados sobre a operação e o gerenciamento de uma assinatura do Azure, bem como dados sobre a integridade e a operação do próprio Azure.

- **Dados de monitoramento do locatário (subscription) do Azure:** dados sobre a operação de serviços do Azure no nível de locatário, como Azure Active Directory.

## Azure Automation

---

O Azure Automation provê a automação de seus serviços de cloud no que diz respeito a automação de processos e tarefas frequentes, demoradas e propensas a erros. Podemos utilizar para controle de alterações e inventário, gerenciamento de configuração e até mesmo gerenciamento de atualizações.

Utiliza-se de recursos compartilhados para que a automação aconteça como os seguintes:

- **Agendas** – Disparo em horários predefinidos.
- **Módulos** – Possibilidade de importação de módulos Microsoft e terceiros para atuação.
- **Galeria de módulos** – Possui uma infinidade de módulos nativos que auxiliará na execução e criação das automações.
- **Pacotes do Python 2** – Suporte a runbooks do Python 2 para automação.
- **Credenciais** – Armazenamento seguro de credenciais que podem ser utilizadas pelo runbook e configurações de automação.

A automação poder ser efetuada tanto em workloads Windows quanto Linux.

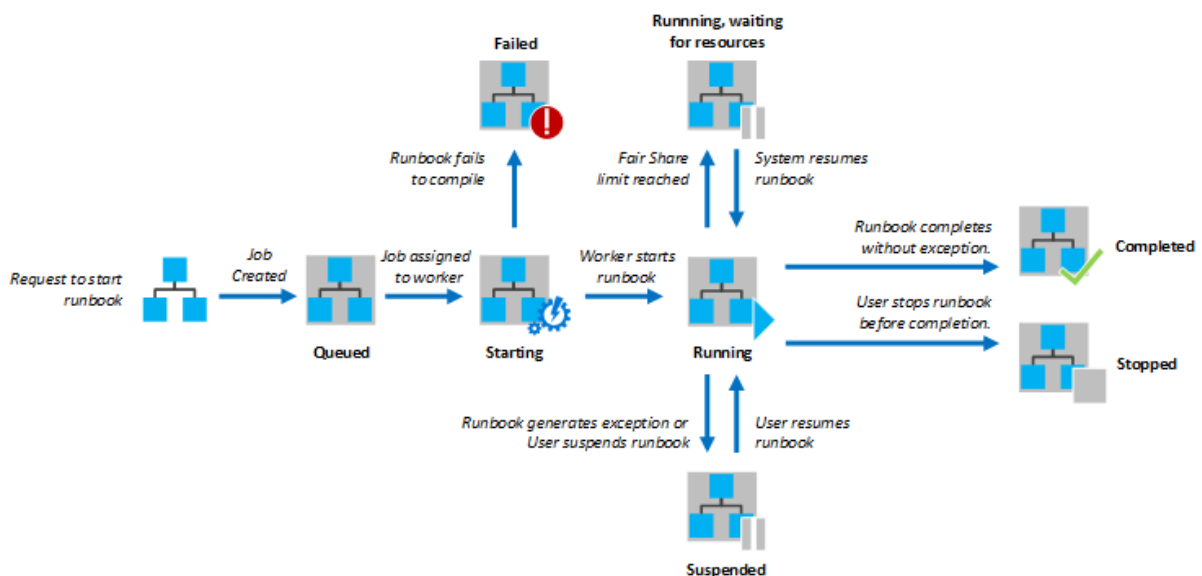
Cenários de automação:

- **Runbooks** – Escrita de runbooks de automação em PowerShell, Fluxo de Trabalho do Powershell, gráficos, Python 2, e DSC em linguagens comuns.
- **Criação e implantação de recursos.**



- Configurar VMs.
- Compartilhar conhecimento ao sistema.
- Recuperação de inventario de recursos.
- Localização de alterações.
- Monitoramento de alterações com problema.
- Proteção de workloads.
- Administração de RBAC para equipes.

**Figura – Fluxo de automação em ação.**



Fonte: [docs.microsoft.com](https://docs.microsoft.com).

## Referências

---

AWS – AMAZON WEB SERVICES. *Documentação da AWS*. 2020. Disponível em: <[https://docs.aws.amazon.com/pt\\_br](https://docs.aws.amazon.com/pt_br)>. Acesso em: 23 jul. 2020.

GOOGLE CLOUD. Disponível em <<https://cloud.google.com/docs>>. Acesso em 23 jul. 2020.

MICROSOFT. *Microsoft Docs*. 2020. Disponível em: <<https://docs.microsoft.com/pt-br/>>. Acesso em: 23 jul. 2020.