AZ-900

CAPEX (Capital Expenditure) – on-premise data centers. Muito dinheiro é gasto em primeiro momento, pois tudo na infraestrutura é construído logo de cara.

OPEX (Operational Expenditure) – cloud. Os custos relacionados às despesas físicas dos on-premise são eliminados, e aqui temos os custos de capacitação dos profissionais de T.I que trabalharão na nuvem.

Em Máquinas Virtuais o hardware é virtualizado, em contêiners o SO é virtualizado.

Azure Global Infrastructure

Geografia = Grupo de regiões.

Região = Grupo de Zonas de Disponibilidade

Azure tem 58 regiões em 140 países.

Azure Geography – regiões onde temos residencia de dados e fronteiras de compliance, ou seja, nestes locais, você pode garantir que seus dados e informações não sejam levados para outra região. São as seguintes localidades: EUA, EUA Gov, Canada, Brasil e México.

Paired Region – são localidades da Azure em que temos Regiões com no mínimo 300 milhas de distância conectadas entre si. Alguns serviços utilizam esta arquitetura para criação de Disaster Recovery. O **Azure Geo-redundant Storage (GRS)** replica os dados para uma segunda região automaticamente, para ter certeza de que as informações estarão disponíveis mesmo em cenários de problemas.

Regiões Recomendadas – regiões que oferecem uma extensa gama de recursos para os usuários e são arquitetadas para suportar Zonas de Disponibilidade.

Regiões Alternativas – no portal Azure são entituladas como *outras*. Não suportam zonas de disponibilidade.

Zona de Disponibilidade = Fault Domain + Update Domain

Fault Domain: é um grupo lógico de hardwares criado para evitar uma possível falha. É um grupo de máquinas virtuais que compartilham da mesma fonte de energia e de switch de rede. É uma proposta muito parecida com os modos de agrupamentos de instâncias da AWS, onde escolhe-se se as máquinas devem ser colocadas em racks diferentes, mesmos racks, ...

Update Domain: garante que os recursos não sejam desligados quando for necessário realizar manutenção em algum equipamento no servidor.

Availability Set: agrupamento lógico de VMs para ter certeza de que elas estarão em diferentes Fault/Update Domain, garantindo assim maior disponibilidade do recurso.

Compute Services

Azure Virtual Machines – máquinas virtuais linux ou windows.

Azure Dedicated Host – são servidores de VMs dedicados que ficam no datacenter da microsoft. O pagamento é pelo número de hosts criados (quantidade de máquinas e as especificações de cada uma delas).

Azure Virtual Machine Scale Sets – adiciona elasticidade no serviço de máquinas virtuais. Permite que VMs identicas sejam escaladas horizontalmente de acordo com alguma métrica que você definir. As métricas

podem ser por uso de CPU, memória, armazenamento ou de performance de rede; também pode agendar um horário para que novas máquinas sejam criadas ou desligadas.

Azure Kubernetes Service – gerenciamento de containers. Usa o software open source K8.

Azure Container Instances – execução de contêiners de forma serverless, ou seja, sem a necessidade de se criar um servidor ou uma VM.

Azure Service Fabric – serviço de containers construído para ser usado em sistemas distribuídos. Pode ser executada na nuvem ou on-premise.

Azure Batch – execução de trabalhos em lotes (100+) em paralelo. Possível usar Spot VMs (mesma coisa das EC2 Spot Instances, você utiliza hardware que não está sendo utilizado no momento por um preço menor).

Storage Services

Antes de poder utilizar os serviços de storage, é necessário a criação de um ***Storage Account***. Todos os dados que forem armazenados em serviços de storage ficarão atrelados à *storage account.* Uma storage account é única no mundo todo e é utilizada para acessar os dados via HTTP e HTTPS.

Azure Blob Storage – object serverless storage. Arquivos muito grandes e em grandes quantidades. Pay-as-you-use. Não é necessário configurar um volume antes de começar a usar. Os blobs serão armazenados em uma espécie de contêiners, para facilitar a organização de acordo com o caso de uso.

Podemos definir ***Access Tiers*** para os arquivos blob:

- Hot access tier: arquivos que são acessados frequentemente.

- Cool access tier: arquivos que não são frequentemente acessados e que serão armazenados por no mínimo 30 dias.

- Archive access tier: arquivos que são raramente acessados e armazenados por no mínimo 180 dias. Neste nível os dados são armazenados de forma offline, ou seja, terão o menor custo de armazenamento, porém terão o custo mais alto para serem recuperados.

Os tiers *Hot* e *Cool* podem ser configurados no nível da conta, o *Archive* não.

Azure Disk Storage – volume conectado nas VMs. Criptografado por padrão. SSD ou HD.

Azure File Storage – volume compartilhado que pode ser acessado por mais de uma pessoa no momento. Os arquivos armazenados neste serviço podem ser acessados por URLs únicas no mundo inteiro. É possível também utilizar *Shared Access Signature tokens* para permitir o acesso à uma quantia restrita de arquivos dentro do file system.

Azure Data Box/Azure Databox Heavy – dispositivo físico para transporte de dados. Semelhante ao AWS Snow. Terabytes and Petabytes.

Azure Archive Storage – serviço para criação de arquivos de dados. Dados quase nunca acessados mas que há a necessidade de mantê-los.

Azure Data Lake Storage – repositório de dados centralizado, que permite o armazenamento de dados estruturados e não estruturados em qualquer escala. Usado para armazenar dados que passaram por workloads de análise.

Database Services

Azure Cosmos DB – NoSQL database completamente gerenciado. Criado para escalar com uma garantia de 99,999% de disponibilidade. Aceita múltiplos tipos de bancos NoSQL. Suporta uma variedade extensa de APIs para queries: SQL, MongoDB, Cassandra, Tables e Gremlin.

Azure Table Storage – NoSQL que armazena dados NÃO estruturados e independentes de qualquer tipo de schema.

Azure SQL Database – criado para usar a engine Microsoft SQL Server. Completamente gerenciado, com escala automática e segurança robusta.

Azure Database for MySQL – banco de dados relacional construído baseado no MySQL Community Edition. Provê 99.99% de disponibilidade. É possível restaurar informações de até 35 dias anteriores com o *point-in-time restore*. Modo de cobrança: *pay-as-you-go*.

Azure Database for PostgreSQL – baseado na engine open source PostgreSQL. Tem diversos níveis de pricing, com a performance variando de acordo com o nível escolhido. É possível restaurar informações de até 35 dias anteriores com o *point-in-time restore*. Disponível em duas formas de deploy:

- ***Single Server***: alta disponibilidade, *pay-as-you-go* pricing, é possível proteger os dados *in-motion* e *at-rest*.

- ***Hyperscale***: modo de deploy utilizado para workloads e aplicações que ou estão chegando ou já passaram de 100 GB de dados.

SQL Managed Instance – fornece grande parte das features que o *Azure SQL Database*, porém permite que algumas configurações sejam modificadas para acomodar um banco personalizado.

SQL Servers on VMs – implantação de bases de dados MS SQL em VMs. É o serviço utilizado quando se tem bases de dados on-premise MS SQL sendo executadas e se deseja colocá-las na nuvem.

Azure Synapse Analytics – data warehouse.

Azure Database Migration Service – migração de bases de dados sem ter que alterar nenhuma linha de código.

Azure Cache for Redis – caches para diminuir o tempo de resposta para dados e informações acessados frequentemente.

Application Integration Services

Azure Notifications Hub – PUB/SUB.

Azure API Apps – API gateway para criação e consumo de APIs na nuvem.

Azure Service Bus – serviço de MaaS (Message as a Service). Permite a distribuição de mensagens para back-ends em escala.

Azure Stream Analytics – serverless real-time analytics, da nuvem para a borda.

Azure Logic Apps – cria, automatiza e orquestra tarefas e workflows. Tem integração com serviços utilizados por empresas.

Azure API Managment – funciona como se fosse um proxy para APIs. Conecta-se à API existente e permite que se adicione novas funcionalidades nela.

Azure Queue Storage – serviço de filas para aplicativos.

Developer and Mobile Tools

Azure SignalR Service – criação de serviços que fornecem informações em tempo real para apps Web e Mobile. Não há a necessidade de se manter um back-end, então o usuário pode focar 100% no negócio. Notificações em tempo real, mensagens, dashboards que tem seus valores alterados de forma momentânea, e muito mais.

Azure App Service – deploy e escala de apps. Parecido como heroku, porém para o azure. Pode ser utilizado para *Web Apps, WebJobs, Mobile Apps* e *API Apps*. Recomendado para quem quer focar somente no desenvolvimento da aplicação.

Visual Studio – editor de código.

Xamarin – criação de apps mobile nativos em .NET.

DevOps Services

Azure DevOps – é um serviço que contém vários outros serviços que serão descritos abaixo:

Azure Boards – kanban.

Azure Pipelines – CI/CD para construir, testar e dar deploy em apps em qualquer linguagem.

Azure Repos – repositórios de código privados na nuvem. É exatamente a mesma coisa que os repositórios do github, porém na cloud.

Azure Test Plans – testar aplicações com ferramentas de teste pré-existentes.

Azure Artifacts – um armazenamento para pacotes que devem ser compartilhados com os times de desenvolvimento para uso no Azure Pipelines, por exemplo.

Azure DevTest Labs – dev-test environments.

Azure Test Plans – ferramenta de teste automatizado que pode ser usada com o Azure Pipelines, para antecipar a etapa de qualificação do software antes do lançamento.

Resource Manager

Este serviço é a porta de entrada para criação de recursos dentro do Azure. Ele recebe os comandos por meio de conexões seguras com as ferramentas disponíveis no Azure – Azure Portal, Azure PowerShell, Azure CLI, REST Clients – autêntica os usuários que os estão realizando e por fim cria os recursos da forma solicitada.

Quickstart Templates

São uma lista de templates já criados pela comunidade, que permitem que você execute serviços sem ter conhecimento profundo. É uma boa maneira de se começar a mexer com o Azure.

vNets e Subnets

Virtual Network – área isolada logicamente para você lançar seus recursos. Escolhe-se um range de IPs usando CIDR range. Dentro de uma Virtual Network (vNet) cria-se subnets, que podem ser públicas ou privadas.

Network Security Groups – são uma série de regras de *inbound* e *outbound traffic* que permitem ou restringem o acesso a determinados recursos a partir de endereços IP de origem e destino, porta e protocolo.

Network Virtual Appliance – é uma VM encarregada de executar algumas funções na rede, como executar um firewall ou performar uma otimização da WAN.

Virtual Network Peering – modo de conectar vNets diferentes. Este recurso permite que vNets em diferentes localidades, sejam zonas de disponibilidade ou regiões, comuniquem-se entre si, dando a possibilidade de se criar uma rede global de recursos.

Na criação de uma subnet os seguintes passos são seguidos:

Nome da Rede -> Range de Endereços -> Subscription -> Resource Group -> Location -> Subnet -> DDoS Protection (é possível escolher entre o plano básico e o standard) -> Service Endpoints (escolhe-se os endpoints dos serviços que serão utilizados dentro da vNet, como por exemplo endpoints de bancos de dados).

Cloud-Native Networking Services

Azure DNS – serviço de DNS da azure. Permite hospedar os domínios já comprados no Azure. O azure NÃO fornece a opção de comprar domínios dentro da plataforma, diferente do Route53 da AWS que permite que se faça isso.

Azure Load Balancer – balanceador de carga da CAMADA 4 DO MODELO OSI. Trabalha somente com os protocolos TCP/IP. Public load balancers ou load balancers internos (privados; funcionam para distribuir carga em workloads que não utilizam a internet).

Azure Application Gateway – balanceador de carga da CAMADA 7 DO MODELO OSI. Aqui sim, trabalhamos com o protocolo HTTP/HTTPS. Pode ter anexado um web application firewall, para camada extra de segurança.

Azure Network Watcher – monitora e diagnóstica problemas relacionados a serviços de infraestrutura (IaaS).

Enterprise/Hybrid Networking Services

Azure Front Door – serviço de CDN legado do Azure. Porta de entrada escalável e segura para aplicações à nível global. Melhor utilizado quando se há a necessidade de entregar sites, serviços e APIs de forma global.

Azure CDN – diferente do Front Door (legado), o Azure CDN conta com melhor capacidade para transmissão de conteúdo estático, como vídeos, imagens e PDFs.

Azure ExpressRoute – conexão dedicada do on-premise para a cloud de 50Mbps até 10 Gbps. O *ExpressRoute* fornece 3 tipos de conexão diferentes:

- CloudExchange colocation: quando se há a instalação de um provedor de serviços no local, é possível solicitar uma conexão cruzada entre o provedor de internet e a cloud da microsoft.

- Point-to-Point ethernet connection: realiza conexão nas camadas 2 e 3 do OSI. Fornece um link ethernet para que se realize uma conexão point-to-point.

- Any-to-Any connection: conexão somente na camada 3. Fornece conexão para WAN.

Virtual WAN – cria uma WAN (Wide Area Network) que permite a conexão local e de lugares remotos.

Azure Connection – conexão segura com a VPN da Azure utilizando IPsec.

VPN Gateway – são criadas dentro de cada vNet e permitem realizar as seguintes conexões:

- *Site-to-Site*: conexão com datacenter on-premise;

- *Point-to-Site*: conexão com dispositivos individuais;

- *Network-to-Network*: conecta redes virtuais com outras redes virtuais;

Só é possível instanciar 1 *VPN Gateway* em cada vNet, porém cada gateway pode ser conectado com diversos pontos diferentes. As VPNs podem ser *policy-based* ou *route-based*.

Para ativar a tolerância a falhas no VPN Gateway, dois modos de deploy foram criados:

- active/standby: este modo cria duas instâncias que serão os gateways, uma instância ficará ativa e operando até que se tenha alguma manutenção ou problema, quando acaba sendo desativada e a que estava em standby entra em ação.

- active/active: é determinado 1 IP público para cada instância e ambas ficam operando ao mesmo tempo. Deve ser criado um túnel diferente para cada comunicação com cada uma das instâncias.

Azure Traffic Manager – opera na camada de DNS. Roteia os requests de acordo com as regras cadastradas (por exemplo, geograficamente, subnet, porcentagem de requests [para direcionar mais requests para uma máquina], ...).

IoT Services

IoT Hub – comunicação altamente segura entre os dispositivos IoT e as aplicações que os monitoram. Fornece 2 tipos de comunicação – *device-to-cloud* (recebimento de dados e arquivos dos dispositivos IoT e possbilidade de roteamento de mensagens para outros dispositivos) e *cloud-to-device* (permite controlar os dispositivos IoT a partir da nuvem, ou seja, temos a possibilidade de recalibrá-los e ajustá-los a partir da nuvem).

IoT Central – fornece uma UI completa para monitoramento dos dispositivos de IoT. Com este serviço é possível monitorar e controlar os dispositivos tudo a partir de uma dashboard.

Azure Sphere – permite a criação de uma solução *end-to-end* dentro do Azure. É dividido em 3 partes:

- Azure sphere Micro Controller Unit (MCU): é um dispositivo de hardware responsável por processar o sistema operacional e controlar os sensores conectados.

- Linux SO totalmente customizado.

- Azure Sphere Security Service: conhecido também como AS3, a função deste serviço é certificar de que o dispositivo não foi comprometido por um vírus ou algo do tipo. Quando o dispositivo tenta se conectar no Azure, é realizada uma autenticação feita por certificados. Após a autenticação, é feita uma verificação para saber se o dispositivo não foi comprometido de alguma forma. Após isso a conexão é realizada e as tarefas determinadas são iniciadas.

IoT Edge – uso de equipamentos que ficam mais próximos dos dispositivos de IoT.

Windows 10 IoT Core Services – uma subscrição de longo prazo do windows 10 para dispositivos de IoT.

Big Data and Analytics Services

Azure Synapse Analytics – data warehouse para uso de SQL. Permite a execução de queries SQL em quantidades massivas de dados.

HDInsight – softwares de analytics open source, como Hadoop, Kafka e Spark.

Azure Databricks – plataforma de analytics otimizada para o Azure construída baseada no Spark.

Data Lake Analytics – serviço de analytics para Data Lakes (armazenamento de quantidades massivas de dados que são armazenados em seu formato cru, sem sofrer transformações até ser necessário).

AI/ML Services

AI > ML > Deep Learning

Azure Machine Learning Service – fornece total controle sobre modelos de machine learning para os desenvolvedores e cientistas de dados. Permite treinar e modelar algoritmos utilizando dados próprios.

*Azure Machine Learning Studio – serviço legado para administração de workloads de ML. A transição de workloads deste serviço para o Azure Machine Learning Service não é simples. É um plataforma visual e colaborativa que permite utilizar modelos pré-construídos de machine learning.

Personalizer – entrega de experiências personalizadas para cada usuário.

Translator – tradução de múltiplas linguagens em tempo real para apps, websites e ferramentas.

Anomaly Detector – detecta anomalias em dados para identificar rapidamente problemas que podem ser causados.

Azure Bot Service – criação e desenvolvimento de bots de conversação.

Form Recognizer – automatiza a extração de textos, chave/valor e tabelas dos documentos.

Computer Vision – permite analisar o conteúdo contido em imagens e vídeos.

Language Understanding – entendimento de linguagem natural para apps, bots e dispositivos de IoT.

Speech – conversão de audio falado em texto.

QnA Maker – criação de bots de conversação, que perguntam e respondem de acordo com o contexto.

Text Analytics – extrai informações de textos como frases, nomes e linguagens.

Content Moderator – moderação de conteúdo para provisionar uma experiência segura para o usuário.

Face – detecta e identifica pessoas e emoções nas imagens.

Ink Recognizer – identifica tinta, como escritas à mão, formas e layout de documentos.

Azure Cognitive Search – este serviço permite que o usuário realize pesquisas na internet e obtenha os resultados que melhor se encaixam na procura. É como se fosse o sistema de pesquisa do google.

Knowledge Mapping – mapeia recomendações para oferecer recomendações inteligentes e pesquisa semântica.

Bing Search – permite adicionar os recursos da pesquisa bing na sua aplicação.

Serverless Services

Para criar uma Azure Function é necessário criar um *Function App* e é dentro deste recurso criado que iremos criar nossas functions.

Azure Functions – funçoes serverless para execução de pequenas quantidades de código nas linguagens: C#, Java, JavaScript, Python e Powershell. Por padrão são *stateless*, ou seja, toda vez que forem executadas, agirão como se estivessem sendo executadas pela primeira vez. É possível configurá-las para serem *stateful*, então ao serem chamadas, um contexto será passado para elas para que seja possível mapear os passos anteriores. Usado frequentemente para REST requests (eventos de APIs).

Blob Storage – armazenamento serverless, ou seja, não é necessário se preocupar com o provisionamento de espaço e de processamento, basta subir os arquivos e ir utilizando.

Logic Apps – plataforma no-code/low-code para construção de workloads composto de diversas Azure Functions. Da mesma forma que as functions, os *Logic Apps* são ativados por gatilhos, que ocorrem quando um evento X é realizado, porém neste serviço é possível construír uma lógica total para ser executada quando o gatilho for ativado. Os workflows são construídos em uma GUI, para que fique mais fácil de visualizar todas as tarefas que serão feitas.

Event Grid – usa pub/sub messaging para reagir a eventos e ativar outros serviços, como por exemplo Azure Functions.

Azure Virtual Desktop

Este serviço permite que "computadores virtuais" sejam criados de forma personalizada de acordo com o desejo do usuário. Ex: ao invés de ter que configurar um SO e os Apps personalizados para cada máquina, para cada departamento diferente, a empresa pode optar por utilizar este serviço, que roda em qualquer SO, e que retira a necessidade de se comprar e configurar de forma personalizadas as máquinas para os funcionários.

Caso a empresa tenha licenças do windows ou do Microsoft 365, elas podem ser importadas para o *Azure Virtual Desktop* e isentam o cliente de ter que pagar por elas, tendo que se preocupar somente com os custos dos recursos que foram utilizados por baixo dos panos.

Azure Portal

É a plataforma web onde acessamos e controlamos todos os serviços.

Azure PowerShell

É um framework construído em cima do .NET para automação de tarefas e configurações.

O Azure PowerShell é uma série de comandos para gerenciamento de recursos no Azure diretamente do PowerShell CLI.

Azure CloudShell

É um terminal que fica no Azure Portal e pode ser usando tanto com Bash quanto com PowerShell.

Azure CLI

Pode ser instalada no Windows, Mac e Linux para utilizar o Azure na CLI diretamente no computador.

ARM Templates

São templates de *infrastructure-as-code* para rápido provisionamento de recursos.

Azure Trust Center

É um site público que contém informações de segurança e compliance sobre o microsoft azure.

Azure Security – Compliance Programs

É uma lista de programas de compliance que a Azure segue.

Azure Active Directory

Azure Active Directory != Active Directory

A microsoft lançou o *Active Directory* nos anos 2000, como um software de gerenciamento de identidade e componentes da infraestrutura local da empresa. Em ambientes locais o *AD* deverá ser gerenciado pela própria organização, nos windows servers. O *Azure Active Directory* é o sistema de gerenciamento baseado na nuvem, ou seja, a microsoft garante sua disponibilidade e acesso em qualquer lugar do planeta.

IAM no Azure. Permite que funcionários acessem o azure e consigam criar e lançar recursos.

Fornce e acesso a recursos privados (apps que estão na rede privada) e públicos (Office 365, Azure Portal e SaaS Applications).

***SSO (Single Sign-On)*:** o usuário utilizará somente uma combinação de um ID e de uma senha para acessar os aplicativos e recursos determinados.

***Azure AD Connect*:** permite conectar o Azure AD com o AD local da empresa, realizando assim sincronizações entre os dois e permite que recursos como SSO, Autenticação Multi-fator e redefinição de senha sejam utilizados tanto na nuvem quanto no datacenter on-premise.

***Acesso Condiconal*:** permite ou nega o acesso de um usuário de acordo com outros fatores de sua conexão, como por exemplo a localização do mesmo – pode ser solicitado ao usuário que forneça acesso à sua localização, para permitir ou não seu acesso.

Disponível em 4 formatos:

- Free: MFA, SSO, Segurança Básica e relatórios de uso, Gerenciamento de Usuários.

- Office 365 Apps: para empresas, SLA, sincronização entre on-premise e cloud.

- Premium 1: arquitetura híbrida, grupos de acesso avançados e acesso condicional.

- Premium 2: proteção de identidade e governança de identidade.

Azure Security Center

É um serviço que fornece uma visão unificada da sua infraestrutura (na nuvem e on-premise) para controle de segurança e gerenciamento dos sistemas. Fornece proteção avançada contra ameaças aos workloads.

As informações visualizadas neste painel são relacionadas com a segurança dos recursos.

Fornece recomendações de como melhorar a segurança dos recursos de acordo com os recursos da conta e com as configurações de rede.

Security Points: fornecem uma visão avaliativa de o quão segura está a sua infraestrutura.

Segurança em VMs, rede e integridade de arquivo:

- Acesso *Just-In-Time* nas VMs: portas especificas são bloqueadas nas VMs e tem seu acesso liberado quando o administrador liberar.

- Controles de Aplicativos Adaptáveis: é possível determinar quais aplicativos podem ser executados nas VMs.

- Proteção de Rede Adaptável: o tráfego da rede pode ser monitorado e ser comparado com os grupos de segurança definidos para sugerir alterações de segurança.

- Monitoramento de integridade de arquivo: arquivos nas VMs podem ser monitorados contra mudanças e deleções.

Azure Sentinel

Permite a coleta de dados de todas as fontes conectadas à nuvem, detecção de ameaças com IA e rápida resposta a incidentes.

É o primeiro sistema SIEM nativo de nuvem.

Key Vault

Auxilia no armazenamento e na segurança de chaves e segredos utilizados em outros serviços.

Secrets Mangement – armazena e monitora senhas, tokens, chaves de APIs, entre outras coisas.

Key Management – permite criar e controlar as chaves utilizadas para criptografar seus dados.

Certificate Management – certificados SSL para uso dentro do Azure.

Hardware Security Module – nível de proteção na hierarquia do hardware. Segredos e chaves podem ser protegidos por software ou por validações ***FIPS 140-2 Level 2*** (certificação de segurança). O Azure utiliza um hardware específico que guarda os segredos escolhidos pelos usuários. Este hardware não armazena os segredos em disco, eles ficam na memória, então se este equipamento for desligado, ele não terá nada salvo dentro dele ao ser religado.

Defesa em Profundidade

Segurança Física > Identidade e Acesso > Perímetro > Rede > Computação > Aplicativo > Dados

Segurança Física – proteger fisicamente o acesso aos datacenters.

Identidade e Acesso – controle de acesso à infraestrutura, SSO e autenticação multi-fator.

Perímetro – uso de firewalls e proteção contra DDoS.

Rede – restringir acesso à internet, por padrão NEGAR os acessos, limite de comunicação entre recursos.

Computação – proteção às VMs e *Endpoint Protection*.

Aplicativo – segurança no nível do software.

Dados – centro da proteção.

Postura de segurança – 3 princípios que devem ser atendidos para garantir a segurança da aplicação:

- Confidencialidade: princípio do privilégio mínimo, ou seja, garantir somente o acesso imprecindível.

- Integridade: impedir a alteração não autorizada de informações.

- Disponibilidade: garantir que os dados estarão disponíveis quando o usuário precisar acessá-los.

Azure DDoS Protection

2 Níveis de proteção contra DDoS:

- Basic: gratuito e ativo automaticamente para todas as contas criadas.

- Standard: 2.994 dólares por mês. Ao assinar este plano um especialista DDoS dedicado para sua conta é contratado, você tem acesso à métricas, alertas e relatórios sobre os ataques.

Azure Firewall

Protege as vNets. O firewall é exposto à internet e protegerá o tráfego para as vNets que estão conectadas a ele.

Utiliza um IP estático público para que aplicações externas reconheçam as requisições que estão vindo daquele firewall.

Há um custo adicional para tráfego de dados entre Azs.

Azure Information Protection

Protege informações sensíveis como emails e documentos com criptografia. É um serviço integrados nos aplicativos e até no pacote office (grandes corporações querem monitorar o que entra e o que sai dos aplicativos, para isso podem utilizar o AIP).

Advanced Threat Protection

Monitora o Azure Active Directory de uma conta para identificar e proteger contra ameaças.

Microsoft Security Development Lifecycle

É um processo de implementação de segurança para software utilizado por grandes empresas no mercado. O processo é o seguinte:

Treinamento -> Requerimentos -> Design -> Implementação -> Verificação -> Liberação (do software) -> Resposta

Azure Policies

É um documento JSON que permite controlar o acesso e a criação de recursos. Mesma coisa do IAM Policies.

Role-Based Access Control

Não é um serviço, é um conceito.

Auxilia a controlar os recursos, o acesso a eles e quem pode acessar o que.

Lock Resources

Evita que usuários modifiquem e mexam em recursos acidentalmente e que realizem ações que não deveriam.

Se por exemplo um *bloqueio de recurso* for definido para impedir a deleção de um resource group, quando o usuário realizar uma ação que gere a deleção do resource group, ela será interrompida e o usuário informado de que não é possível realizar este tipo de operação.

Podem ser definidos nos seguintes níveis:

CanNotDelete: usuários autorizados podem ver e modificar um recurso porém não podem deletá-lo.

ReadOnly: usuários podem visualizar um recurso, porém não podem deletar o modificá-lo.

Azure Tags

Tags podem ser adicionadas aos recursos para facilitar a identificação dos mesmos e para prover uma camada extra de informações.

Azure Policy

Permite a criação e a definição de políticas para garantir a conformidade dos padrões aplicados nos recursos que são criados e executados no azure. A política do azure avalia e destaca os recursos que não

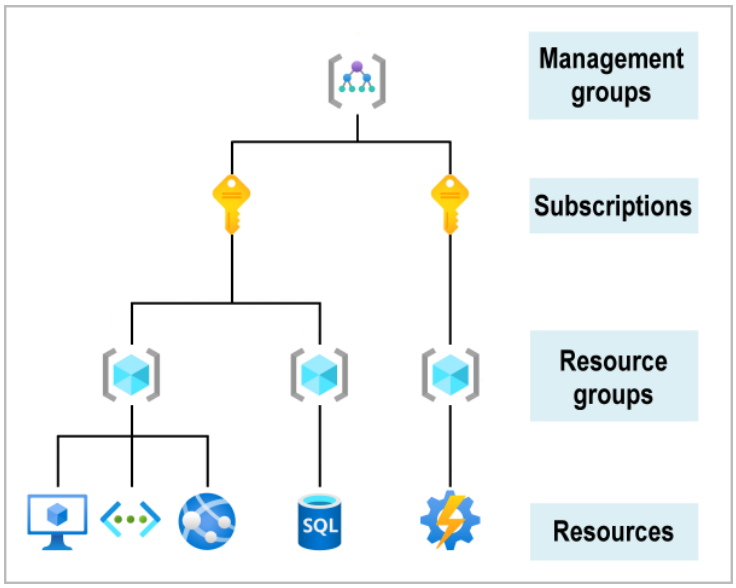
estão em conformidade com as políticas definidas, podendo também corrigí-las para que tudo fique em conformidade. Uma política pode ser criada por exemplo para não permitir a criação de uma VM em uma determinada região do Azure.

Iniciativa de Política: é uma maneira de agrupar políticas do azure.

Azure BluePrints

Podemos criar moldes com diversas configurações de compliance que podem ser repetidas diversas vezes e implementadas em dificuldade e sem a necessidade de se criar novas configurações todas as vezes.

Dentro das *plantas (blueprints)* são inseridos ***Artefatos***, que são as especificações relacionadas a recursos e que serão inseridas nas plantas. Ex: **Implementar detecção de ameaças contra servidores SQL**.



Management Groups

É uma maneira de controlar **subscriptions** (que podem ser chamadas somente de contas) dentro de um sistema hierárquico.

Cada grupo tem um grupo que é chamado de root.

As **subscriptions** herdam as políticas de acesso e de controle do grupo que estão presentes.

Azure Subscriptions

Uma conta do Azure pode ter diversas ***Subscriptions***, como por exemplo uma para cada departamento: desenvolvimento, marketing, finanças, ... Cada *subscription* pode ter uma forma de cobrança diferente.

Na parte mais alta da hierarquia, está a **Conta do Azure**, seguido das **Subscriptions**, seguido de **Resource Groups** e então de recursos própriamente ditos.

Existem 4 tipos de *Subscription*:

Free – necessário cartão de crédito, 200 dólares em créditos para serem usados em 30 dias, alguns serviços são gratuitos por 12 meses.

Pay-As-You-Go (PAYG) – necessário cartão de crédito, cobrado no final do mês de acordo com o consumo dos recursos.

Enterprise Agreement – uma empresa tem contrato com o Azure e recebe descontos e ofertas exclusivas para licensas e serviços do Azure.

Student Subscription – não há a necessidade de cartão de crédito, 100 dólares em créditos para serem usados por 12 meses, necessita um email estudantil válido.

Resource Groups

São grupos lógicos onde os recursos do Azure deverão ser alocados.

Não é possível criar um recurso sem antes ter um resource group para colocá-lo.

Um recurso NÃO pode ser colocado dentro de mais de 1 resource group.

Resources groups NÃO podem ser colocados uns dentro dos outros.

Azure Monitor

Serve como uma dashboard centralizada para visualizar informações sobre os recursos da conta.

Azure Service Health

Fornece informações sobre ocorrências atuais e futuras nos serviços do Azure como eventos que podem impactar os serviços, manutenção planejada e outras mudanças que podem afetar a disponibilidade.

Azure Status – informa sobre serviços que estão fora do ar.

Azure Service Health – informações personalizadas dos serviços e das regiões do Azure que você está utilizando.

Azure Resource Health – informação sobre a disponibilidade de serviços individuais do Azure.

Azure Advisor

Fornece algumas sugestões para otimizar seu uso do Azure em 5 categorias:

Reliability

Security

Performance

Cost

Operational Excellence

Service Level Agreements – SLAs

Comprometimento do Azure com *uptime* e *connectivity*.

São individualizados por serviço.

São descritos como ***Performance Targets***. Os *Performance Targets* são representados como porcentagem.

Percentual de SLA	Tempo de inatividade por semana	Tempo de inatividade por mês	Tempo de inatividade por ano
99	1,68 hora	7,2 horas	3,65 dias
99,9	10,1 minutos	43,2 minutos	8,76 horas
99,95	5 minutos	21,6 minutos	4,38 horas
99,99	1,01 minuto	4,32 minutos	52,56 minutos
99,999	6 segundos	25,9 segundos	5,26 minutos

Pricing and Support – Service Credits

Os usuários do Azure podem ter descontos nos serviços por baixa performance dos mesmos. Vamos dizer que por exemplo um serviço teve sua média mensal de *uptime* em 98%, o usuário receberá na sua conta mensal do Azure um desconto de X% sobre o valor por conta do *downtime* do serviço que ele estava utilizando.

Composite SLAs

É uma maneira de "somar" os ***Performance Targets*** dos serviços que estão sendo utilizados.

No Azure cada serviço tem ***Performance Target*** diferente, para ter uma ideia do valor total de uma arquitetura, o que deveria ser feito é multiplicar todos os valores entre si, para assim obter uma **%** total da disponibilidade da arquitetura.

Uma forma de aumentar a disponibilidade da arquitetura é a adição de sistemas de failover, que serão ativados quando os serviços principais caírem. Isso aumenta ainda mais o valor total do ***Performance Target*** da arquitetura.

TCO Calculator

TCO = Total Cost of Ownership

Estima os custos que podem ser reduzidos se for realizado uma migração para o Azure.

Permite gerar um relatório bem detalhado e exportá-lo como PDF para demosntrações.

Utiliza de 4 categorias para avaliar os valores:

- Servidores: tudo relacionado aos servidores que serão migrados (CPU, RAM, SOs, ...).

- Banco de Dados: hardware, tipo de database e o serviço do azure que será utilizado.

- Storage: tipo de armazenamento e capacidade total.

- Rede: quantidade de bandwidth que é consumida no datacenter local.

Azure Marketplace

É uma grande lojinha de softwares para seus serviços no Azure.

Os softwares podem ser pagos ou gratuitos.

Azure Support Plans

<table>
<tr><th>BASIC</th><th>DEVELOPER</th><th>STANDARD</th><th>PROFESSIONAL DIRECT</th></tr>
<tr><td rowspan="6">Suporte por email somente por problemas na conta de pagamento e na conta do Azure.</td><td colspan="3">Suporte técnico por email em horário comercial.</td></tr>
<tr><td></td><td colspan="2">Suporte por telefone 24/7</td></tr>
<tr><td colspan="3">Suporte para softwares de terceiro (mesmo que isso não seja problema com serviços do Azure, o suporte fará de tudo para auxiliar na solução do problema).</td></tr>
<tr><td colspan="2">Problemas com serviços que não impactarão o negócio gravemente (Gravidade C). Tempo de resposta < 8 horas.</td><td>Problemas com serviços que não impactarão o negócio gravemente (Gravidade C). Tempo de resposta < 4 horas.</td></tr>
<tr><td></td><td>Problemas com serviços que terão um impacto moderado nos negócios (Gravidade B). Tempo de resposta < 4 horas.</td><td>Problemas com serviços que terão um impacto moderado nos negócios (Gravidade B). Tempo de resposta < 2 horas.</td></tr>
<tr><td></td><td colspan="2">Impacto severo nos negócios (Gravidade A). Tempo de resposta < 1 hora.</td></tr>
<tr><td colspan="4">Azure Advisor, Azure Health Status, Community Support, Azure Documentation.</td></tr>
<tr><td></td><td colspan="2">Architecture General Guidance.</td><td>Architecture, Operational Support and Proactive Guidance by pool ProDirect delivery managers. Webinar ensinados por arquitetos do Azure.</td></tr>
<tr><td>0 USD/Mês</td><td>29 USD/Mês</td><td>100 USD/Mês</td><td>1000 USD/Mês</td></tr>
</table>

Azure Lincesing

Clientes que investiram em licenças pagas do windows server, podem reutilizar este investimento no Azure.

Azure **Hybrid Use Benefit (HUB)** – dá o direito para que os clientes utilizem licenças do Windows Server e do SQL Server no Azure. Pode ser ligado e desligado em qualquer momento nas VMs e pode ser aplicado no momento de deploy das VMs.

BYOL = Bring Your Own License.

Pricing Calculator

Estima os custos para produtos do Azure.

Basta baixar uma planilha do excel e utilizá-la para calcular os custos.

Azure Cost Management

Permite realizar análises sobre os custos dos serviços utilizados.

Crie orçamentos de uso, para ser alertado quando o valor da conta estiver próximo de certa porcentagem do valor do orçamento e quando o valor ultrapassar o orçamento determinado.

Cloud Adoption Framework

É um conjunto de ferramentas, documentação e boas práticas para migração e adoção da infraestrutura na nuvem.

Definir a Estratégia -> Criar um plano -> Preparar a organização -> Adotar a nuvem -> Controlar e gerenciar os ambientes.

RBAC – Controle de Acesso Baseado em Função. Permite atribuir a usuários permissões diferentes de acordo com os acessos necessários.

Certificações de Conformidade

CJIS (Serviços de Informações de Justiça Criminal) – qualquer agência estadual ou local dos Estados Unidos que quiser acessar o banco de dados do CJIS do FBI, precisa aderir a política de segurança determinada pelo CJIS.

STAR – certicicação da Cloud Security Alliance. Baseia-se na obtenção da certificação ISSO 27001.

Clausulas da União Europeia – exigem garantias com relação às transferências de dados pessoais para fora da EU.

Lei Health Insurance Portability and Accountability – é uma lei que regula informações médicas de pacientes nos EUA.

DPA – Adendo de Proteção de Dados

Define com profundiadde os termos de segurança e processamento dos dados dos serviços online.