Módulo 1

1-) Definir computação em nuvem.

ENTREGA DE SERVIÇOS DE COMPUTAÇÃO PELA INTERNET.

2-) Descrever o modelo de responsabilidade compartilhada.

ORGANIZAÇÃO E PROVEDOR DIVIDEM RESPONSABILIDADE NA COMPUTAÇÃO EM NUVEM.

3-) Definir modelos de nuvem público, privado e híbrido.

PÚBLICO - PROVEDORES OFERECEM O SERVIÇO AO PÚBLICO E EMPRESAS.
PRIVADA - EMPRESA MONTA UMA ESTRUTURA DE NUVEM PARA ELA.
HÍBRIDA - MISTURA DOS SERVIÇOS ANTERIORES.

4-) Identificar os casos de uso apropriados para cada modelo de nuvem.

PÚBLICO - ACESSÍVEL PARA PESSOAS, PEQUENAS EMPRESAS.
PRIVADA - PARA EMPRESAS GRANDES QUE JÁ TEM MONTADA SUA ESTRUTURA DE NUVEM.
HÍBRIDA - MAIOR FLEXIBILIDADE PARA AS EMPRESAS GRANDES E SE TORNA ACESSÍVEL PARA AS PEQUENAS EMPRESAS NA MEDIDA QUE CRESCEM.

5-) Descrever o modelo baseado no consumo.

USUÁRIO OU EMPRESA SÓ PAGA PELO QUE USA, O QUE GERA ECONOMIA, MENOS TRABALHO E FACILIDADE NO GERENCIAMENTO DO SERVIÇO.

6-) Comparar os modelos de preços de nuvem.

CapEx - DESPESAS DE CAPITAL SÃO GASTOS INICIAIS PARA MONTAGEM DE UMA ESTRUTURA.
OpEx - DESPESAS OPERACIONAIS SÃO GASTOS AO LONGO DO TEMPO, PARA MANUTENÇÃO DO SERVIÇO CONTRATADO.

Módulo 2

1-)Descrever os benefícios da alta disponibilidade e da escalabilidade na nuvem.

DISPONIBILIDADE - GARANTIA DO SERVIÇO ESTAR DISPONÍVEL POR 99% DO TEMPO DE CONTRATAÇÃO, REDUZINDO PROBLEMAS OPERACIONAIS.
ESCALABILIDADE - POSSIBILIDADE DE ALTERAR RECURSOS PARA ATENDER UMA DEMANDA COMPUTACIONAL.

2-)Descrever os benefícios da confiabilidade e da previsibilidade na nuvem.

CONFIABILIDADE - EM CASO DE PROBLEMA NO FUNCIONAMENTO DO SERVIÇO DA NUVEM EM ALGUMA ÁREA, OUTRO DATACENTER ASSUME O TRABALHO E GARANTE SEU FUNCIONAMENTO, SEM PREJUDICAR O USUÁRIO.
PREVISIBILIDADE - PREVER OS MELHORES RECURSOS E SUA CAPACIDADE, ASSIM COMO ESTIMAR OS CUSTOS.

3-)Descrever os benefícios da segurança e da governança na nuvem.

SEGURANÇA - USUÁRIO PODE CONTAR COM SERVIÇOS PRESTADOS PELO PROVEDOR, COMO CRIPTOGRAFIA DE DADOS.
GOVERNANÇA - FACILITA O GERENCIAMENTO E A CRIAÇÃO DE UM CONJUNTO DE REGRAS PARA O USO DOS SERVIÇOS CONTRATADOS.

4-) Descrever os benefícios da capacidade de gerenciamento na nuvem.

É FÁCIL ACESSAR, USAR E GERENCIAR OS RECURSOS DISPONÍVEIS PARA CONTRATAÇÃO, ASSIM COMO GERENCIAR OS RECURSOS CONTRATADOS EM SEU AMBIENTE DE NUVEM.

Módulo 3

1-) Descrever o IaaS (infraestrutura como serviço).

MAIOR RESPONSABILIDADE PARA O CONTRATANTE. ELE ALUGA O RECURSO COMPUTACIONAL NA NUVEM (TAL QUAL SERIA COM UM HARDWARE FÍSICO) E CUIDA DE TODO O RESTANTE DO TRABALHO.

2-) Descrever a PaaS (plataforma como serviço).

RESPONSABILIDADE DIVIDIDA ENTRE PROVEDOR E CONTRATANTE. NESSE TIPO DE SERVIÇO, A PESSOA USA OS SERVIÇOS DA PLATAFORMA PARA CONFIGURAR SUA APLICAÇÃO.

3-) Descrever Software como Serviço (SaaS).

RESPONSABILIDADE MAIOR PARA O PROVEDOR. CABE AO CONTRATANTE USAR AS FERRAMENTAS PARA TRABALHAR EM SUA APLICAÇÃO.

4-) Identificar os casos de uso apropriados para cada serviço de nuvem (IaaS, PaaS e SaaS).

Iaas - migração "Lift And Shift", ou seja, migração de aplicativos e dados associados para a nuvem com o mínimo ou nenhuma alteração; fazer testes.

PaaS - desenvolvedores podem usar como base para desenvolver ou personalizar aplicativos baseados em nuvem, reduzindo a quantidade de codificação que os desenvolvedores precisam realizar; análise ou business intelligence, ou seja, as ferramentas fornecidas como serviço com o PaaS permitem que as organizações analisem e minerem dados.

Saas - contratante quer serviço de Email e mensagens, aplicativos de produtividade empresarial, controle de finanças e despesas.

Módulo 4

1-) Descrever regiões do Azure, pares de regiões e regiões soberanas.

Regiões - reúne 3 datacenters.
Par de região - caso uma região apresente falha, os dados podem ser direcionados para outra região para manter o serviço funcionando.
Região soberana - regiões controladas por governos em parceria com a Microsoft.

2-) Descrever Zonas de Disponibilidade.

Em cada região, os 3 datacenters são interligados, para, em caso de falha em um ou dois, o outro mantenha o serviço funcionando.

3-) Descrever datacenters do Azure.

São instalações com recursos, organizados em racks com energia, refrigeração e infraestrutura de rede dedicadas.

4-) Descrever recursos e grupos de recursos do Azure.

Recurso: são componentes, como máquinas virtuais, armazenamento e redes, para criar soluções na nuvem.
Grupo de recurso: relação de recursos para uma aplicação. Pode ter recursos de regiões diferentes. Grupo de recursos pode ter mais que um recurso, mas recurso só pode pertencer a um grupo de cada vez. O Grupo de Recursos fornece uma maneira de monitorar, controlar acesso, provisionar e gerenciar os custos das aplicações.

5-) Descrever assinaturas.

Assinatura: unidade de gerenciamento, cobrança e escala. Por meio dela, pode facilitar o gerenciamento dos recursos e cobrança. Uma conta pode estar vinculada a várias assinaturas.
Existem dois tipos de limites de assinaturas:

- **Limite de cobrança: gerar faturas e relatórios de cobrança separados para cada assinatura.**
- **Limite de controle de acesso: gerenciar e controlar o acesso aos recursos que os usuários provisionam com assinaturas específicas.**

6-) Descrever grupos de gerenciamento.

Nível acima das assinaturas. Nele, reúne as assinaturas, aplica as condições de governança tal qual os grupos de recursos.

7-) Descrever a hierarquia de grupos de recursos, assinaturas e grupos de gerenciamento.

O grupo de gerenciamento reúne os grupos de recursos. O recurso, para ser utilizado, precisa estar ligado a uma assinatura.

Módulo 5

1-) Comparar tipos de computação, incluindo instâncias de contêiner, máquinas virtuais e funções

MÁQUINAS VIRTUAIS (VM) - OFERTA DE IaaS - EMULAÇÃO DE SOFTWARE DE COMPUTADOR FÍSICO. INCLUI PROCESSADOR VIRTUAL, MEMÓRIA, ARMAZENAMENTO E REDE. É UM COMPUTADOR, PORÉM NA NUVEM.

CONTÊINER - OFERTA DE PaaS - AMBIENTE ISOLADO ONDE HÁ TODAS AS CONFIGURAÇÕES E COMPARTIMENTOS NECESSÁRIOS PARA EXECUTAR APLICAÇÕES. ENQUANTO A VM TORNA VIRTUAL TODO O SISTEMA OPERACIONAL, O CONTÊINER SERÁ APENAS A APLICAÇÃO. POR ISSO, É MAIS LEVE, PARA SER CRIADO, DIMENSIONADO E INTERROMPIDOS DINAMICAMENTE.

FUNÇÕES - O Azure Functions é um serviço de computação serverless (sem servidor) que permite a execução de pequenas porções de códigos – também conhecidas como funções no vocabulário de desenvolvimento – disparadas a partir de eventos específicos. Esses gatilhos podem ser respostas a mudanças em dados, respostas a mensagens, além de solicitações HTTP.

2-) Descrever opções de VM (máquina virtual), incluindo VMs, conjuntos de dimensionamento de máquinas virtuais, conjuntos de disponibilidade, Área de Trabalho Virtual do Azure

CONJUNTO DE DIMENSIONAMENTO -
CONJUNTO DE DISPONIBILIDADE -
ÁREA DE TRABALHO VIRTUAL -

3-) Descrever os recursos necessários para máquinas virtuais

- **Tamanho (finalidade, número de núcleos de processador,quantidade de RAM)**
- **Discos de armazenamento (unidades de disco rígido, unidades de estado sólido etc.)**
- **Rede (rede virtual, endereço IP público e configuração de porta)**

4-) Descrever opções de hospedagem de aplicativos, incluindo Aplicativos Web do Azure, contêineres e máquinas virtuais.

5-) Descrever a rede virtual, incluindo a finalidade das Redes Virtuais do Azure, sub-redes virtuais do Azure, emparelhamento, DNS do Azure, Gateway de VPN e ExpressRoute.

Redes Virtuais do Azure – permitem que recursos do Azure, como VMs, aplicativos Web e bancos de dados, comuniquem-se uns com os outros, com usuários na Internet e com computadores cliente locais. Você pode pensar em uma rede do Azure como uma extensão de sua rede local com recursos que vinculam outros recursos do Azure.

As redes virtuais do Azure oferecem as seguintes funcionalidades de rede essenciais:

- Isolamento e segmentação
- Comunicação pela Internet
- Comunicação entre recursos do Azure
- Comunicação com os recursos locais
- Rotear tráfego de rede
- Filtrar tráfego de rede
- Conectar redes virtuais

sub-redes virtuais do Azure – A rede virtual do Azure permite criar várias redes virtuais isoladas. Quando você configura uma rede virtual, define um espaço de endereço IP privado usando intervalos de endereços IP públicos ou privados. O intervalo de IP existe somente na rede virtual e não é roteável pela Internet. Você pode dividir esse espaço de endereços IP em sub-redes e alocar parte do espaço de endereço definido para cada sub-rede nomeada.

emparelhamento – O emparelhamento de rede virtual permite que você conecte duas ou mais redes virtuais no Azure sem interrupção. As redes virtuais aparecerão como uma só para fins de conectividade. O tráfego entre máquinas virtuais em uma rede virtual emparelhada usa infraestrutura de backbone da Microsoft. Assim como o tráfego entre máquinas virtuais na mesma rede, o tráfego é roteado somente pela rede *privada* da Microsoft.

O Azure é compatível com os seguintes tipos de emparelhamento:

- **Emparelhamento de rede virtual:** conexão de redes virtuais na mesma região do Azure.
- **Emparelhamento de rede virtual global**: conecte redes virtuais em diferentes regões do Azure.

Os benefícios do uso do emparelhamento de rede virtual, seja local ou global, incluem:

- Baixa latência, conexão com largura de banda alta entre os recursos em redes virtuais diferentes.
- A capacidade de recursos em uma rede virtual para se comunicar com recursos em uma rede virtual diferente.
- A capacidade de transferir dados entre redes virtuais entre as assinatura do Azure, Azure Active Directory locatários, modelos de implantação e regiões do Azure.
- A capacidade de emparelhar redes virtuais criadas por meio do Azure Resource Manager.

DNS do Azure – serviço de hospedagem para domínios DNS que fornece a resolução de nomes usando a infraestrutura do Microsoft Azure. Ao hospedar seus domínios no Azure, você pode gerenciar seus registros DNS usando as mesmas credenciais, APIs, ferramentas e cobrança que seus outros serviços do Azure.

O DNS do Azure aproveita o escopo e a escala do Microsoft Azure para proporcionar inúmeros benefícios, incluindo:

- Confiabilidade e desempenho
- Segurança
- Facilidade de uso
- Personalizar redes virtuais
- Registros de alias

O DNS do Azure baseia-se no Azure Resource Manager, que fornece recursos como:

- Azure RBAC (controle de acesso baseado em função do Azure) para controlar quem tem acesso a ações específicas da sua organização.
- Log de atividades para monitorar como um usuário em sua organização modificou um recurso ou para encontrar um erro ao solucionar problemas.
- Bloqueio de recursos para bloquear uma assinatura, um grupo de recursos ou um recurso. O bloqueio impede que os usuários em sua organização acidentalmente excluam ou modifiquem recursos essenciais.

Gateway de VPN – Um gateway de VPN é um tipo de gateway de rede virtual. As instâncias do Gateway de VPN do Azure são implantadas em uma subrede dedicada da rede virtual e permitem a seguinte conectividade:

- Conecte datacenters locais a redes virtuais por meio de uma conexão site a site.
- Conecte dispositivos individuais a redes virtuais por meio de uma conexão ponto a site.
- Conecte redes virtuais a outras redes virtuais por meio de uma conexão rede a rede.

Todas as transferências de dados são criptografadas em um túnel privado à medida que atravessam a Internet. Você pode implantar apenas um gateway de VPN em cada rede virtual. Porém, você pode usar um gateway para se conectar a vários locais, incluindo outras redes virtuais ou datacenters locais.

Ao implantar um gateway de VPN, você especifica o tipo de VPN, que pode ser baseada em política ou em rota. A principal diferença entre esses dois tipos de VPN é como o tráfego a ser criptografado é especificado. No Azure, ambos os tipos de gateways de VPN usam uma chave pré-compartilhada como o único método de autenticação.

- Gateways de VPN baseados em política especificam estaticamente o endereço IP dos pacotes que devem ser criptografados por meio de cada túnel. Esse tipo de dispositivo avalia cada pacote de dados em relação a esses conjuntos de endereços IP para escolher o túnel para o qual o pacote será enviado.
- Em gateways baseados em rota, os túneis IPSec são modelados como um adaptador de rede ou uma interface de túnel virtual. O roteamento de IP (protocolos de roteamento dinâmico ou rotas estáticas) decide qual dessas interfaces de túnel usar ao enviar cada pacote. VPNs baseadas em rota são o método preferido para conectar dispositivos locais. Elas são mais resilientes a alterações de topologia, como a criação de novas sub-redes.

Use um gateway de VPN baseado em rota se precisar de qualquer um dos seguintes tipos de conectividade:

- Conexões entre redes virtuais
- Conexões ponto a site
- Conexões multissite

- Coexistência com um gateway do Azure ExpressRoute

ExpressRoute – permite que você estenda suas redes locais para a nuvem da Microsoft em uma conexão privada com a ajuda de um provedor de conectividade. Essa conexão é chamada de Circuito do ExpressRoute.

É possível estabelecer conexões com os serviços em nuvem da Microsoft, como o Microsoft Azure e o Microsoft 365. Ela permite que você conecte escritórios, datacenters ou outras instalações à Microsoft Cloud. Cada local teria o próprio circuito do ExpressRoute.

Há vários benefícios de usar o ExpressRoute como o serviço de conexão entre o Azure e as redes locais.

- Conectividade com os serviços de nuvem da Microsoft em todas as regiões da região geopolítica.
- Conectividade global com os serviços da Microsoft em todas as regiões com o Alcance Global do ExpressRoute.
- Roteamento dinâmico entre sua rede e a Microsoft por meio do BGP (Border Gateway Protocol).
- Redundância interna em cada local de emparelhamento para proporcionar maior confiabilidade.

Você pode habilitar o Alcance Global do ExpressRoute para trocar dados entre sites locais conectando seus circuitos do ExpressRoute. Por exemplo, escritório na Ásia e um datacenter na Europa, ambos com circuitos do ExpressRoute os conectando à rede da Microsoft. Você pode usar o Alcance Global do ExpressRoute para conectar essas duas instalações, permitindo que elas se comuniquem sem transferir dados pela Internet pública.

Os seus dados não passam pela Internet pública e, portanto, não são expostos aos riscos potenciais associados às comunicações da Internet.

6-) Definir pontos de extremidade públicos e privados.

A rede virtual do Azure dá suporte a pontos de extremidade públicos e privados para habilitar a comunicação entre recursos externos ou internos com outros recursos internos.

- **Pontos de extremidade públicos** têm um endereço IP público e podem ser acessados de qualquer lugar do mundo.
- **Pontos de extremidade privados** existem em uma rede virtual e têm um endereço IP privado dentro do espaço de endereço dessa rede virtual.

Módulo 6

1-) Descrever as camadas de armazenamento.

- **Camada de acesso quente:** dados que são acessados com frequência (por exemplo, imagens de seu site).
- **Camada de acesso frio:** dados acessados com menos frequência e armazenados por pelo menos 30 dias (por exemplo, faturas de seus clientes).

- **Camada de acesso aos arquivos:** dados acessados raramente e armazenados por pelo menos 180 dias, com requisitos de latência flexíveis (por exemplo, backups de longo prazo).

2-) Descrever as opções de redundância.

- **LRS** (armazenamento com redundância local) - Protege nos casos de… um nó dentro de um data center se torna indisponível.
- **ZRS** (armazenamento com redundância de zona) - Protege nos casos de… um data center (zona) inteiro fica indisponível.
- **GRS** (Armazenamento com redundância geográfica) - Protege nos casos de…uma interrupção ocorrer em toda a região primária.
- **RA-GRS** (armazenamento com redundância geográfica com acesso de leitura) - Igual ao GRS, pórem a cópia feita para região secundária, é com acesso apenas de leitura.
- **GZRS** (Armazenamento com redundância de zona geográfica) - Protege nos casos de…uma interrupção ocorrer em toda a região primária.
- **RA-GZRS** (armazenamento com redundância de zona geográfica com acesso de leitura) - Igual ao GZRS, pórem a cópia feita para região secundária, é com acesso apenas de leitura.

3-) Descrever as opções de conta de armazenamento e os tipos de armazenamento.

- **Blobs do Azure:** um repositório de objetos altamente escalonável para texto e dados binários. Ela também inclui suporte para análise de Big Data por meio do Data Lake Storage Gen2.
- **Arquivos do Azure:** compartilhamentos de arquivos gerenciados para implantações locais e em nuvem.
- **Filas do Azure:** um armazenamento de mensagens para um sistema de mensagens confiável entre componentes do aplicativo.
- **Azure Disks:** volumes de armazenamento em nível de bloco para VMs do Azure.

4-) Identificar opções para mover arquivos, incluindo o AzCopy, o Gerenciador de Armazenamento do Azure e a Sincronização de Arquivos do Azure.

- AzCopy - utilitário de linha de comando que você pode usar para copiar blobs ou arquivos de/para uma conta de armazenamento. Com o AzCopy, você pode carregar arquivos, baixar arquivos, copiar arquivos entre contas de armazenamento e até mesmo sincronizar arquivos. O AzCopy pode até mesmo ser configurado para trabalhar com outros provedores de nuvem para ajudar a mover arquivos entre nuvens.

- Gerenciador de Armazenamento do Azure - aplicativo autônomo que fornece uma interface gráfica para gerenciar arquivos e blobs em sua Conta do Armazenamento do Azure. Você pode carregar no Azure, baixar do Azure ou mover entre contas de armazenamento.

- Sincronização de Arquivos do Azure - ferramenta que permite centralizar seus compartilhamentos de arquivos no serviço Arquivos do Azure e manter a flexibilidade, o desempenho e a compatibilidade de um servidor de arquivos do Windows.

5-) Descrever as opções de migração, incluindo as Migrações para Azure e o Azure Data Box.

Migrações para Azure - serviço que ajuda você a migrar de um ambiente local para a nuvem. O Migrações para Azure funciona como um hub para ajudar você a gerenciar a avaliação e a migração do datacenter local para o Azure. Elas fornecem um único portal para iniciar, executar e acompanhar sua migração para o Azure, uma variedade de ferramentas para avaliação e migração.

Azure Data Box - serviço de migração física que ajuda a transferir grandes quantidades de dados de maneira rápida, barata e confiável, ideal para transferir os tamanhos de dados maiores do que 40 TB em cenários com conectividade de rede limitada a inexistente. A movimentação de dados pode ser única, periódica ou uma transferência de dados em massa inicial seguida por transferências periódicas.

Módulo 7

1-) Descrever os serviços de diretório no Azure, incluindo o AD (Azure Active Directory) e o Azure AD DS.

O **Azure AD (Azure Active Directory)** é um serviço de diretório que permite que você entre e acesse aplicativos de nuvem da Microsoft e aplicativos de nuvem que você desenvolve. O Azure AD também pode ajudar você a manter sua implantação do Active Directory local.

O Azure AD é o serviço de gerenciamento de acesso e identidade baseado em nuvem da Microsoft. Com o Azure AD, você controla as contas de identidade, mas a Microsoft garante que o serviço esteja disponível globalmente.

O **Azure AD DS (Azure Active Directory Domain Services)** é um serviço que fornece serviços de domínio gerenciado. Com Azure AD DS você obtém o benefício dos serviços de domínio sem a necessidade de implantar, gerenciar e corrigir DCs (controladores de domínio) na nuvem.

2-) Descrever os métodos de autenticação no Azure, incluindo SSO (logon único), MFA (autenticação multifator) e acesso sem senha.

SSO (logon único) - permite que um usuário entre uma vez e use essa credencial para acessar vários recursos e aplicativos de provedores diferentes. Quanto mais senhas um usuário precisa gerenciar, maior o risco de um incidente de segurança relacionado às credenciais.

Autenticação multifator - processo de solicitar a um usuário uma forma (ou um fator) adicional de identificação durante o processo de entrada. A MFA ajuda a proteger contra uma exposição de senha em situações em que a senha tenha sido comprometida, mas o segundo fator não.

A autenticação multifator fornece segurança adicional para as identidades, exigindo dois ou mais elementos para a autenticação completa. Esses elementos se enquadram em três categorias:

· Algo que o usuário saiba– essa pode ser uma pergunta de desafio.

· Algo que o usuário tenha – pode ser um código enviado para o telefone celular do usuário.

· Algo que o usuário seja – normalmente é algum tipo de propriedade biométrica, como a leitura de impressão digital ou reconhecimento facial.

A Autenticação Multifator do Azure AD permite que os usuários escolham uma forma adicional de autenticação durante a conexão, como uma chamada telefônica ou uma notificação no aplicativo móvel.

Autenticação sem senha - Os métodos de autenticação sem senha são mais convenientes porque a senha é removida e substituída por algo que você tenha, além de algo que você seja ou saiba.

A autenticação sem senha precisa ser configurada em um dispositivo para poder funcionar. Por exemplo, seu computador é algo que você tem. Depois de registrado ou inscrito, o Azure agora sabe que ele está associado a você. Agora que o computador é conhecido, uma vez que você forneça algo que você saiba ou seja (como um PIN ou uma impressão digital), você poderá ser autenticado sem usar uma senha.

O Azure e Azure Governamental da Microsoft global oferece estas três opções de autenticação sem senha que se integram ao Azure Active Directory (Azure AD):

· Windows Hello para Empresas
· Aplicativo Microsoft Authenticator
· Chaves de segurança FIDO2

3-) Descrever as identidades externas e o acesso de convidado no Azure

Uma identidade externa é uma pessoa, um dispositivo, um serviço etc. que está fora da sua organização. O recurso Identidades Externas do Azure AD refere-se a todas as maneiras pelas quais você pode interagir com usuários fora da organização com segurança.

4-) Descrever o acesso condicional do Azure AD

O Acesso Condicional é uma ferramenta que o Azure Active Directory usa para permitir (ou negar) o acesso a recursos com base em sinais de identidade. Esses sinais incluem quem é o usuário, onde ele está e de qual dispositivo está solicitando acesso.

Ele não exigirá um segundo fator de autenticação se o usuário estiver em uma localização conhecida, ou exigir se os sinais de conexão do usuário forem incomuns ou se o usuário estiver em uma localização inesperada.
Ou seja, é analisado a localização do usuário, o dispositivo do usuário ou o aplicativo que o usuário está tentando acessar.

Com base nesses sinais, a decisão poderá ser permitir acesso completo se o usuário estiver entrando de seu local usual. Se o usuário estiver entrando de uma localização incomum ou que esteja marcada como de alto risco, o acesso poderá ser totalmente bloqueado ou possivelmente concedido depois que o usuário fornecer uma segunda forma de autenticação.

5-) Descrever o RBAC (controle de acesso baseado em função) do Azure

O princípio de privilégios mínimos diz que você só deve conceder acesso até o nível necessário para concluir uma tarefa. Apesar de ser uma boa prática de segurança para seguir, o gerenciamento desse nível de permissões para uma equipe inteira se tornaria tedioso.

Com o RBAC do Azure (controle de acesso baseado em função do Azure), é possível fornecer funções internas que descrevem regras de acesso comuns para os recursos de nuvem. Você também pode definir suas funções. Cada função tem um conjunto associado de permissões de acesso relacionadas a

essa função. Quando você atribui indivíduos ou grupos a uma ou mais funções, eles recebem todas as permissões de acesso relacionadas.

6-) Descrever o conceito de Confiança Zero.

A Confiança Zero é um modelo de segurança que pressupõe o pior cenário e protege os recursos com essa expectativa. A Confiança Zero pressupõe uma violação desde o início e verifica cada solicitação como se ela tivesse sido originada em uma rede não controlada.

7-) Descrever a finalidade do modelo de defesa em profundidade.

O objetivo da defesa em profundidade é proteger as informações e impedir que elas sejam roubadas por pessoas que não estejam autorizadas a acessá-las.

Uma estratégia de defesa em profundidade usa uma série de mecanismos para reduzir o avanço de um ataque que busca obter acesso não autorizado aos dados. Você pode visualizar a defesa em profundidade como um conjunto de camadas, com os dados a serem protegidos no centro e todas as outras camadas funcionando para proteger essa camada de dados central.

Cada camada fornece proteção, de modo que se uma camada for violada, uma camada seguinte já estará em vigor para impedir a exposição adicional. Essa abordagem elimina a dependência de qualquer camada única de proteção. Ela desacelera um ataque e fornece informações de alerta sobre as quais as equipes de segurança podem agir, automática ou manualmente.

8-) Descrever a finalidade do Microsoft Defender para Nuvem.

O Defender para Nuvem é uma ferramenta de monitoramento para gerenciamento da postura de segurança e proteção contra ameaças. Ele monitora ambientes de nuvem, locais, híbridos e de multinuvem para fornecer diretrizes e notificações com o objetivo de fortalecer sua postura de segurança.

O Defender para Nuvem fornece as ferramentas necessárias para proteger seus recursos, acompanhar sua postura de segurança, proteger contra ataques cibernéticos e simplificar o gerenciamento de segurança. A implantação do Defender para Nuvem é fácil e já está integrada nativamente ao Azure.

Módulo 8

1-) Descrever fatores que podem afetar os custos no Azure.

- **Tipo de recurso -** qual recurso contratado, sua configuração e região.
- **Consumo** - paga pelo que usa.
- **Manutenção** - Os custos de energia, mão de obra, impostos e taxas pela Azure variam dependendo do local.
- **Tráfego de rede** - custo pago pela transferências de dados de saída (dados que saem de data centers do Azure) é baseado em zonas.
- **Tipo de assinatura -** se junto ao recurso, foi contratado outro serviço ou app.
- **Azure Marketplace -** contratação de app na loja do Azure.

2-) Comparar a calculadora de preços e a calculadora de TCO (Custo Total de Propriedade).

Calculadora de preço - projetada para fornecer um custo estimado para provisionar recursos no Azure. Você pode obter uma estimativa para recursos individuais, criar uma solução ou usar um cenário de exemplo para ver uma estimativa dos gastos do Azure. O foco da calculadora de preços está no custo dos recursos provisionados no Azure.

Calculadora de TCO - projetada para ajudá-lo a comparar os custos para executar uma infraestrutura local versus uma infraestrutura de nuvem do Azure. Com a calculadora de TCO, você insere sua configuração de infraestrutura atual, e pode comparar o custo de um ambiente do Azure que dá suporte aos mesmos requisitos de infraestrutura.

3-) Descrever a ferramenta Gerenciamento de Custos do Azure.

O Gerenciamento de Custos permite verificar rapidamente os custos de recursos do Azure, criar alertas com base nos gastos com recursos e criar orçamentos que podem ser usados para automatizar o gerenciamento de recursos.

O objetivo com ele é visualizar rapidamente o custo total de várias maneiras, inclusive por ciclo de cobrança, região, recurso etc.

4-) Descrever a finalidade das marcas (TAGS).

As marcas (TAGS) fornecem informações extras ou metadados sobre os recursos.

As tags são marcações que podem ser aplicadas nos recursos do Azure e assinaturas para organizá-los logicamente por categorias. Cada tag consiste em um nome e um valor, por exemplo Centro de Custo/TI, ou Ambiente/Produção. Depois de criar suas tags você pode associá-las aos recursos apropriados.

Módulo 9

1-) Descrever a finalidade do Azure Blueprints.

Permite padronizar as implantações de ambiente ou de assinatura de nuvem. Em vez de precisar configurar recursos como o Azure Policy para cada nova assinatura, com o Azure Blueprints você pode definir configurações e políticas repetíveis que são aplicadas à medida que as assinaturas são criadas.

O Azure Blueprints permite implantar um novo ambiente de Teste/Desenvolvimento com configurações de segurança e conformidade já definidas. Dessa forma, as equipes de desenvolvimento podem criar e implantar rapidamente novos ambientes com a certeza de que estão cumprindo os requisitos organizacionais.

2-) Descrever a finalidade do Azure Policy.

serviço do Azure que permite criar, atribuir e gerenciar políticas que controlam ou auditam os recursos. Essas políticas impõem regras diferentes sobre as configurações dos recursos, de modo que essas configurações permaneçam em conformidade com os padrões corporativos.

3-) Descrever a finalidade dos bloqueios de recurso.

Um bloqueio de recurso impede que os recursos sejam excluídos ou alterados acidentalmente. Os bloqueios de recursos impedem que recursos sejam excluídos ou atualizados, dependendo do tipo de bloqueio. Os bloqueios de recursos podem ser aplicados a recursos individuais, grupos de recursos ou até mesmo a toda uma assinatura. Os bloqueios de recursos são herdados, o que significa que, se você colocar um bloqueio de recurso em um grupo de recursos, todos os recursos do grupo de recursos também terão o bloqueio de recurso aplicado.

4-) Descrever a finalidade do Portal de Confiança do Serviço.

Oferece acesso a vários conteúdos, ferramentas e outros recursos sobre práticas de segurança, privacidade e conformidade da Microsoft.
O Portal de Confiança do Serviço contém detalhes sobre a implementação de controles e processos da Microsoft que protegem nossos serviços na nuvem e os dados do cliente encontrados neles.

Módulo 10

1-) Descrever o portal do Azure.

O portal do Azure é um console unificado baseado na Web que fornece uma alternativa para as ferramentas de linha de comando. Com o portal do Azure, você pode gerenciar a assinatura do Azure usando uma interface gráfica do usuário.

2-) Descrever o Azure Cloud Shell, incluindo a CLI do Azure e o Azure PowerShell.

Ferramenta de shell baseada em navegador que permite criar, configurar e gerenciar recursos do Azure usando um shell. O Azure Cloud Shell dá suporte ao Azure PowerShell e à CLI (Interface de Linha de Comando) do Azure, que é um shell bash.
Azure PowerShell é um shell com o qual desenvolvedores, DevOps e profissionais de TI podem executar comandos chamados de command-lets (cmdlets).
Equivalente ao Azure PowerShell, sendo a principal diferença a sintaxe dos comandos. Enquanto o Azure PowerShell usa comandos do PowerShell, a CLI do Azure usa comandos Bash.

3-) Descrever a finalidade do Azure Arc.

Permite estender a conformidade e o monitoramento do Azure para suas configurações híbridas e multinuvem.

4-) Descrever o ARM (Azure Resource Manager) e modelos do ARM do Azure.

O ARM (Azure Resource Manager) é o serviço de implantação e gerenciamento do Azure. Ele fornece uma camada de gerenciamento que lhe permite criar, atualizar e excluir recursos em sua conta do Azure. Sempre que você faz qualquer coisa com seus recursos do Azure, o ARM está envolvido.

Módulo 11

1-) Descrever a finalidade do Assistente do Azure.

Avalia seus recursos do Azure e faz recomendações para ajudar a melhorar a confiabilidade, a segurança e o desempenho, alcançar a excelência operacional e reduzir os custos.

2-) Descrever a Integridade do Serviço do Azure.

Ajuda a manter o controle do recurso do Azure, tanto os recursos especificamente implantados quando o status geral do Azure. A integridade do serviço do Azure faz isso combinando três serviços diferentes do Azure:

- **Status do Azure -** informa sobre interrupções de serviço no Azure.
- **Integridade do Serviço -** se concentra nos serviços e regiões do Azure que você está usando.
- **Resource Health -** fornece informações sobre a integridade de cada um de seus recursos de nuvem, como uma instância de máquina virtual específica.

3-) Descrever o Azure Monitor, incluindo o Azure Log Analytics, os alertas do Azure Monitor e o Application Insights.

Plataforma para coletar dados sobre seus recursos, analisar esses dados, visualizar as informações e até mesmo agir com base nos resultados. O Azure Monitor pode monitorar recursos do Azure, seus recursos locais e até mesmo recursos de várias nuvens, como máquinas virtuais hospedadas com um provedor de nuvem diferente.

Além disso, os dados podem ser usados para ajudar você a reagir a eventos críticos em tempo real, por meio de alertas.

Azure Log Analytics é uma ferramenta robusta que dá suporte a consultas simples e complexas e à análise de dados.

Os **Alertas do Azure Monitor** são formas automatizadas de se manter informado caso o Azure Monitor detecte um limite sendo ultrapassado.

Application Insights é um recurso do Azure Monitor que monitora seus aplicativos Web. O Application Insights consegue monitorar aplicativos que esteja em execução no Azure, localmente ou em outro ambiente de nuvem.

Termos importantes

Colocalização em uma troca de nuvem

A colocalização se refere ao datacenter, ao escritório ou a outras instalações fisicamente localizadas em uma troca de nuvem, como um ISP. Se a sua instalação estiver colocalizada em uma troca de nuvem, você poderá solicitar uma conexão cruzada virtual com a Microsoft Cloud.

Conexão Ethernet ponto a ponto

A conexão de Ethernet ponto a ponto se refere ao uso de uma conexão ponto a ponto para conectar sua instalação à Microsoft Cloud.

Any-to-any (Redes qualquer para qualquer)

Com a conectividade any-to-any, você pode integrar sua WAN (rede de longa distância) ao Azure fornecendo conexões aos seus escritórios e datacenters. O Azure é integrado à sua conexão WAN para fornecer uma conexão, da mesma forma que você teria entre o datacenter e as filiais.