O que é a computação em nuvem?
É a entrega de serviços de computação pela Internet, que também é conhecida como nuvem. A computação em nuvem oferece inovação mais rápida, recursos flexíveis e economias de escala.

O portal do Azure foi projetado para ter resiliência e disponibilidade contínua. Ele mantém uma presença em todos os datacenters do Azure. Essa configuração torna o portal do Azure resiliente a falhas de datacenters individuais e evita a lentidão da rede ao se manter perto dos usuários.

O Azure Marketplace ajuda a conectar usuários a parceiros da Microsoft, fornecedores independentes de software e startups que estão oferecendo soluções e serviços otimizados para execução no Azure. Todas as soluções e serviços são certificados para execução no Azure.

Computação

Serviços de computação são muitas vezes um dos principais motivos pelos quais as empresas mudam para a plataforma do Azure. O Azure fornece uma variedade de opções para hospedar aplicativos e serviços. Aqui estão alguns exemplos d serviços de computação no Azure.

Nome do serviço	Função do serviço
Máquinas Virtuais do Azure	VMs (máquinas virtuais) do Windows ou do Linux hospedadas no Azure.
Conjuntos de Dimensionamento de Máquinas Virtuais do Azure	Escala para VMs do Windows ou do Linux hospedadas no Azure.
Serviço de Kubernetes do Azure	Gerenciamento de clusters para VMs que executam serviço em contêineres.
Azure Service Fabric	Plataforma de sistemas distribuídos executada no Azure ou localmente.
Lote do Azure	Serviço gerenciado para aplicativos de computação paralelos e de alto desempenho.
Instâncias de Contêiner do Azure	Aplicativos em contêineres executados no Azure sem o provisionamento de servidores ou de VMs.
Funções do Azure	Um serviço de computação sem servidor controlado por eventos.

Rede

Vincular recursos de computação e fornecer acesso a aplicativos são as principais funções da rede do Azure. A funcionalidade de rede do Azure inclui uma série de opções para conectar o mundo exterior aos serviços e recursos dos datacenters globais do Azure.

Rede Virtual do Azure: Conecta VMs a conexões VPN (rede virtual privada) de entrada.

Azure Load Balancer: Equilibra as conexões de entrada e saída para pontos de extremidade de serviço ou aplicativos.

Gateway de Aplicativo do Azure: Otimiza a entrega de farm de servidores de aplicativo, aumentando simultaneamente a segurança do aplicativo.

Gateway de VPN do Azure: Acessa as Redes Virtuais do Azure por meio de gateways de VPN de alto desempenho.

DNS do Azure: Fornece respostas DNS extremamente rápidas e disponibilidade de domínio extremamente alta.

Rede de Distribuição de Conteúdo do Azure: Distribui o conteúdo de alta largura de banda para clientes no mundo todo.

Proteção contra DDoS do Azure: Protege os aplicativos hospedados no Azure contra ataques de DDoS (negação de serviço distribuído).

Gerenciador de Tráfego do Azure: Distribui o tráfego de rede entre as regiões do Azure no mundo todo.

Azure ExpressRoute: Conecta-se ao Azure por meio de conexões seguras dedicadas de alta largura de banda.

Observador de Rede do Azure: Monitora e diagnostica problemas de rede usando a análise baseada em cenário.

Firewall do Azure: Implementa um firewall de alta segurança e alta disponibilidade com escalabilidade ilimitada.

WAN Virtual do Azure: Cria uma WAN (rede de longa distância) unificada que conecta sites remotos e locais.

Armazenamento

O Azure fornece quatro tipos principais de serviços de armazenamento.

Nome do serviço	Função do serviço
Armazenamento de Blobs do Azure	Serviço de armazenamento para objetos muito grandes, como arquivos de vídeo ou bitmaps.
Armazenamento de arquivos do Azure	Compartilhamentos de arquivos que podem ser acessados e gerenciados como um servidor de arquivos.
Armazenamento de Filas do Azure	Um armazenamento de dados para o enfileiramento de mensagens e a entrega confiável delas entre aplicativos.
Armazenamento da tabela do Azure	O armazenamento de tabela é um serviço que armazena dados estruturados não relacionais (também conhecidos como dados NoSQL estruturados) na nuvem, fornecendo um repositório de chave/atributo com um design sem esquema.

Bancos de dados

O Azure fornece vários serviços de banco de dados para armazenar uma ampla variedade de volumes e tipos de dados. E com a conectividade global, esses dados ficam disponíveis para os usuários instantaneamente.

Nome do serviço	Função do serviço
Azure Cosmos DB	Banco de dados distribuído globalmente que dá suporte a opções de NoSQL.
Banco de Dados SQL do Azure	Banco de dados relacional totalmente gerenciado com dimensionamento automático, inteligência integral e segurança robusta.
Banco de Dados do Azure para MySQL	Banco de dados relacional MySQL totalmente gerenciado e escalonável, com alta disponibilidade e segurança.
Banco de Dados do Azure para PostgreSQL	Banco de dados relacional PostgreSQL totalmente gerenciado e escalonável, com alta disponibilidade e segurança.
SQL Server nas Máquinas Virtuais do Azure	Serviço que hospeda aplicativos empresariais do SQL Server na nuvem.
Azure Synapse Analytics	Data warehouse totalmente gerenciado com segurança integral em todos os níveis de escala sem custo adicional.
Serviço de Migração de Banco de Dados do Azure	Serviço que migra bancos de dados para a nuvem sem alterações no código do aplicativo.

Cache Redis do Azure	Caches de serviço totalmente gerenciados usados com frequência e dados estáticos para reduzir a latência de dados e de aplicativos.
Banco de Dados do Azure para MariaDB	Banco de dados relacional MariaDB totalmente gerenciado e escalonável, com alta disponibilidade e segurança.

Web

No mundo dos negócios atual, é essencial ter uma experiência de sucesso da Web. O Azure inclui suporte de primeira classe para criar e hospedar aplicativos Web e serviços Web baseados em HTTP. Os serviços do Azure a seguir são voltados para a hospedagem na Web.

Nome do serviço	Descrição
Serviço de Aplicativo do Azure	Crie rapidamente poderosos aplicativos de nuvem baseados na Web.
Hubs de Notificação do Azure	Envie notificações por push para qualquer plataforma de qualquer back-end.
Gerenciamento de API do Azure	Publique APIs para desenvolvedores, parceiros e funcionários de maneira segura e em escala.
Azure Cognitive Search	Implante esta pesquisa totalmente gerenciada como serviço.
Recurso de Aplicativos Web do Serviço de Aplicativo do Azure	Crie e implante aplicativos Web críticos em escala.
Serviço Azure SignalR	Adicione funcionalidades da Web em tempo real com facilidade.

IoT

As pessoas são capazes de acessar mais informações do que em qualquer momento da história anterior. Os assistentes digitais pessoais levaram aos smartphones e agora existem relógios inteligentes, termostatos inteligentes e até mesmo refrigeradores inteligentes. Computadores pessoais costumavam ser a regra. Agora, a Internet permite que qualquer item que tenha funcionalidade online acesse informações valiosas. Essa capacidade dos dispositivos de coletar e depois retransmitir informações para análise de dados é conhecida como IoT.

Muitos serviços podem ajudar a criar e impulsionar soluções de ponta a ponta para a IoT no Azure.

Nome do serviço	Descrição
IoT Central	Solução SaaS (software como serviço) de IoT global totalmente gerenciada que torna fácil conectar, monitorar e gerenciar os ativos de IoT em escala.
Hub IoT do Azure	Hub de mensagens que fornece comunicações seguras e monitoramento entre milhões de dispositivos IoT.
IoT Edge	Serviço totalmente gerenciado que permite que os modelos de análise de dados sejam enviados por push diretamente aos dispositivos de IoT, possibilitando que esses dispositivos reajam rapidamente a alterações de estado sem a necessidade de consultar modelos de IA baseados em nuvem.

Big Data

Os dados vêm em todos os formatos e tamanhos. Quando falamos em Big Data, estamos nos referindo a *grandes* volumes de dados. Dados de sistemas de clima, sistemas de comunicação, pesquisa genômica, plataformas de geração de imagens e muitos outros cenários produzem centenas de gigabytes de dados. Essa quantidade de dados torna difícil analisar e tomar decisões. O volume geralmente é tão grande que formas tradicionais de processamento e análise não são mais apropriadas.

Tecnologias de cluster de software livre foram desenvolvidas para lidar com esses grandes conjuntos de dados. O Azure é compatível com uma ampla variedade de tecnologias e serviços para fornecer soluções de análises e Big Data.

Nome do serviço	Descrição
Azure Synapse Analytics	Execute a análise em grande escala usando um data warehouse empresarial baseado em nuvem que aproveita c processamento paralelo massivo para executar consultas complexas rapidamente sobre petabytes de dados.
Azure HDInsight	Processe grandes quantidades de dados com clusters gerenciados de clusters Hadoop na nuvem.
Azure Databricks	Integre esse serviço de análise colaborativa com base no Apache Spark com outros serviços de Big Data do Azure.

DevOps

O DevOps reúne pessoas, processos e tecnologias, automatizando a entrega de software para fornecer valor contínuo aos usuários. Com o Azure DevOps você pode criar, *compilar* e *lançar* pipelines que fornecem integração, entrega e implantação contínuas para seus aplicativos. Você pode integrar repositórios e testes de aplicativos, executar o monitoramento de aplicativo e trabalhar com artefatos de compilação. Você também pode trabalhar os itens e inseri-los em uma lista de pendências do produto para acompanhar, automatizar a implantação de infraestrutura e integrar uma série de ferramentas e serviços de terceiros, como Jenkins e Chef. Todas essas funções e muitas outras estão totalmente integradas ao Azure a fim de permitir implantações consistentes e repetíveis para seus aplicativos, visando fornecer processos de build e versão simplificados.

Nome do serviço	Descrição
Azure DevOps	Use ferramentas de colaboração de desenvolvimento, tais como pipelines de alto desempenho, repositórios Git privados gratuitos, quadros Kanban configuráveis e amplos testes de carga baseados em nuvem automatizados. Anteriormente conhecido como Visual Studio Team Services.
Azure DevTest Labs	Crie rapidamente ambientes Windows e Linux sob demanda para testar ou demonstrar aplicativos diretamente dos pipelines de implantação.

Exercicio

1. Verdadeiro ou falso: Compre uma conta do Azure para usar os recursos do Azure.

- ○ Falso
  - ✔ **A resposta está correta. Você pode usar uma conta gratuita do Azure ou uma área restrita do Microsoft Learn para criar recursos.**
- ◉ True
  - ✘ **A resposta está incorreta. Você pode usar uma conta gratuita do Azure ou uma área restrita do Microsoft Learn para criar recursos.**

2. O que significa computação em nuvem?

- ◉ Entrega de serviços de computação pela Internet.
  - ✔ **A resposta está correta. A computação em nuvem é a entrega de serviços de computação pela Internet, que também é conhecida como nuvem**
- ○ Configuração do seu próprio data center.
- ○ Uso da Internet

3. Qual das opções a seguir *não* é um recurso da Computação em nuvem?

- ○ Inovação mais rápida
- ◉ Um pool limitado de serviços
  - ✔ **A resposta está correta. A nuvem oferece um pool quase ilimitado de componentes brutos de computação, armazenamento e rede para ajudar você a proporcionar experiências inovadoras ao usuário rapidamente.**
- ○ Reconhecimento de fala e outros serviços cognitivos

O que são nuvens públicas, privadas e híbridas?

Nuvem pública

Os serviços são oferecidos pela Internet pública e ficam disponíveis para qualquer pessoa que deseje comprá-los. Os recursos de nuvem, como servidores e armazenamento, são de propriedade e operados por um provedor de serviços de nuvem de terceiros e entregues pela Internet.

Nenhuma despesa de capital para escalar verticalmente.

Os aplicativos podem ser provisionados e desprovisionados rapidamente.

As organizações pagam apenas pelo que utilizam.

Tem fins lucrativo

Nuvem privada

Uma nuvem privada consiste em recursos de computação usados exclusivamente por usuários de uma empresa ou organização. Uma nuvem privada pode estar localizada fisicamente no datacenter (local) da organização ou ser hospedada por um provedor de serviços de terceiros.

O hardware deve ser comprado para inicialização e manutenção.

As organizações têm controle total sobre os recursos e a segurança.

As organizações são responsáveis pela manutenção e pelas atualizações de hardware.

Nuvem híbrida

Uma nuvem híbrida é um ambiente de computação que combina uma nuvem pública e uma nuvem privada, permitindo que dados e aplicativos sejam compartilhados entre elas.

Fornece a maior flexibilidade.

As organizações determinam onde executar seus aplicativos.

As organizações controlam a segurança, a conformidade ou os requisitos legais.

Os dez benefícios da Azure

1. High Availabitity -= Alta disponibilidade colocando um load balacer, tem SLA (medir)
2. Scalability = Escabilidade, mais equipamentos no Azure
3. Global reach = Alcance Global (crescer em outro pais) sem deslocamento
4. Agility = Agilidade (pegar tudo pronto no Azure)
5. Disaster Recovery = Recuperação de desastre
6. Fault Tolerance = Tolerância a falha (site recovery)
7. Elasticity = Elasticidade, aumentar ou diminuir os equipamentos (custo)
8. Custome latency capabilities = Latência do cliente (internet ruim, lentidão)

9. Predictive cost considerations = Custos previsíveis (roull back), CTO, calculadora
10. Security = Segurança

- **Alta disponibilidade**: dependendo do SLA (Contrato de Nível de Serviço) que você escolher, seus aplicativos baseados em nuvem poderão oferecer uma experiência de usuário contínua, sem tempo de inatividade aparente, mesmo quando as coisas derem errado.
- **Escalabilidade**: os aplicativos na nuvem podem ser dimensionados *verticalmente* e *horizontalmente*:
  - Dimensione verticalmente para aumentar a capacidade de computação adicionando RAM ou CPUs a uma máquina virtual.
  - Dimensionar horizontalmente aumenta a capacidade de computação adicionando instâncias de recursos, por exemplo, adicionando VMs à configuração.
- **Elasticidade**: você pode configurar aplicativos baseados em nuvem para aproveitar o dimensionamento automático, de modo que os aplicativos sempre tenham os recursos de que precisam.
- **Agilidade**: implante e configure rapidamente os recursos baseados em nuvem à medida que os requisitos de aplicativo mudarem.
- **Distribuição geográfica**: você pode implantar aplicativos e dados em data centers regionais em todo o mundo, garantindo assim que os clientes sempre tenham o melhor desempenho em sua região.
- **Recuperação de desastre**: ao aproveitar os serviços de backup baseados em nuvem, a replicação de dados e a distribuição geográfica, você pode implantar os aplicativos com a confiança de saber que seus dados estarão seguros em caso de desastre.

Despesas de capital versus despesas operacionais. Há dois tipos diferentes de despesas que você deve considerar:

CapEx (despesas de capital) = dinheiro para comprar, pode ser rodizio ao longo do tempo, gera ativo imobilizado.

OpEx (despesas operacionais = Prestando um serviço, operação, só paga pela utilização

Azure é 100% OPEx

IaaS - *Infraestrutura como Serviço*

Esse modelo de serviço de nuvem é o mais próximo do gerenciamento de servidores físicos; um provedor de nuvem manterá o hardware atualizado, mas a manutenção do sistema operacional e a configuração da rede ficam a cargo do locatário da nuvem.

PaaS - *Plataforma como serviço*

Esse modelo de serviço de nuvem é um ambiente de hospedagem gerenciado. O provedor de nuvem gerencia as máquinas virtuais e os recursos de rede e o locatário de nuvem implanta seus aplicativos no ambiente de hospedagem gerenciado.

SaaS - *Software como serviço*

Nesse modelo de serviço de nuvem, o provedor de nuvem gerencia todos os aspectos do ambiente de aplicativo, como as máquinas virtuais, os recursos de rede, o armazenamento de dados e os aplicativos. O locatário de nuvem só precisa fornecer seus dados para o aplicativo gerenciado pelo provedor de nuvem.

Comparação de modelos de serviço de nuvem

IaaS	PaaS	SaaS
O serviço de nuvem mais flexível.	Focado no desenvolvimento de aplicativos.	Modelo de preço pago conforme o uso.
Você configura e gerencia o hardware para seu aplicativo.	O gerenciamento de plataforma é realizado pelo provedor de nuvem.	Os usuários pagam pelo software que utilizam em um modelo de assinatura.

Computação sem servidor – Serverles Computing

Assim como a PaaS, ***a computação sem servidor*** permite que os desenvolvedores criem aplicativos mais rapidamente, eliminando a necessidade de gerenciar a infraestrutura. Com aplicativos sem servidor, o provedor de serviços de nuvem provisiona, escala e gerencia automaticamente a infraestrutura necessária para executar o código.

É cobrado pela execução, é muito barato

Azure Functions: faz o código, ou seja, faz tudo automático

Azure Logic Apps: código pronto, através de terceiro, usando telas com baixo codigo.

Não grande conhecimento de programação

Exercício

Escolha a melhor resposta para cada pergunta. Em seguida, selecione **Verificar suas respostas.**

1. Qual das opções a seguir não é uma categoria de computação em nuvem?

- (●) NaaS (Rede como Serviço)
  - ✔ **A resposta está correta. NaaS não é uma categoria de computação em nuvem.**
- ( ) PaaS (Plataforma como Serviço)
- ( ) IaaS (Infraestrutura como Serviço)
- ( ) SaaS (Software como Serviço)

2. Qual das afirmações a seguir é verdadeira?

- ( ) Com as OpEx (despesas operacionais), você é responsável por comprar e manter seus recursos de computação.
- ( ) Com as OpEx (despesas operacionais), você é responsável somente pelos recursos de computação que usa.
  - ✔ **A resposta está correta. Com as OpEx (despesas operacionais), você é responsável somente pelos recursos de computação que usa.**
- (●) Com as CapEx (despesas de capital), você é responsável somente pelos recursos de computação que usa.
  - ✘ **A resposta está incorreta. Com CapEx (despesas de capital), você é responsável pelos recursos de computação que usa E pela compra e pela manutenção de seus recursos de computação.**

3. Qual das opções a seguir não é um tipo de computação em nuvem?

- (●) Nuvem distribuída
  - ✔ **A resposta está correta. Uma nuvem distribuída não é um tipo válido de computação em nuvem.**
- ( ) Nuvem híbrida
- ( ) Nuvem privada
- ( ) Nuvem pública

4. Qual das opções a seguir não é um benefício de usar serviços de nuvem?

- ( ) Escalabilidade
- ( ) Recuperação de desastre
- ( ) Alta disponibilidade
- (●) Isolamento geográfico
  - ✔ **A resposta está correta. Você pode optar por criar recursos em uma única região; no entanto, uma das principais vantagens da computação em nuvem é a distribuição geográfica.**

Visão geral de assinaturas, grupos de gerenciamento e recursos do Azure

1. **Grupos de gerenciamento**: esses grupos ajudam a gerenciar o acesso, a política e a conformidade para várias assinaturas. Todas as assinaturas em um grupo de gerenciamento herdam automaticamente as condições aplicadas ao grupo de gerenciamento.

2. **Assinaturas**: uma assinatura agrupa contas de usuário e os recursos que foram criados por elas. Para cada assinatura, há limites ou cotas na quantidade de recursos que você pode criar e usar. As organizações podem usar assinaturas para gerenciar os custos e os recursos criados por usuários, equipes ou projetos.

3. **Grupos de recursos**: os recursos são combinados em grupos de recursos, que atuam como um contêiner lógico no qual os recursos do Azure, como aplicativos Web, bancos de dados e contas de armazenamento, são implantados e gerenciados.

4. **Recursos**: recursos são instâncias de serviços que você cria, como máquinas virtuais, armazenamento ou bancos de dados SQL.

Regiões do Azure

Uma *região* é uma área geográfica do planeta que contém pelo menos um, mas possivelmente vários data centers próximos e conectados a uma rede de baixa latência. O Azure atribui e controla os recursos de modo inteligente dentro de cada região para garantir que as cargas de trabalho sejam balanceadas corretamente.

As regiões globais proporcionam maior escalabilidade e redundância. Elas também preservam a residência de dados de seus serviços.

Importante: Alguns serviços ou recursos de VM estão disponíveis somente em determinadas regiões, como tamanhos específicos de VMs ou tipos de armazenamento. Também há alguns serviços globais do Azure que não

exigem que você selecione uma região específica, como o Azure Active Directory, o Gerenciador de Tráfego do Azure e o DNS do Azure.

Zonas de disponibilidade do Azure

É importante verificar se seus serviços e dados são redundantes para que você possa proteger suas informações em caso de falha. Ao hospedar sua infraestrutura, a configuração de sua **redundância** exigirá a criação de ambientes de hardware duplicados. O Azure pode ajudar a tornar seu aplicativo altamente disponível por meio das zonas de disponibilidade. São datacenters separados fisicamente dentro de uma região do Azure. Cada zona de disponibilidade é composta de um ou mais datacenters equipados com energia, resfriamento e rede independentes. Uma zona de disponibilidade é configurada para ser um *limite de isolamento*. Se uma zona ficar inativa, as outras continuarão funcionando. Zonas de disponibilidade são conectadas por meio de redes de fibra óptica privadas de alta velocidade.

Pares de regiões do Azure

As zonas de disponibilidade são criadas usando um ou mais data centers. Há um mínimo de três zonas em uma região. É possível que um desastre de maiores proporções cause uma interrupção grande o suficiente para afetar até mesmo dois datacenters. Por isso, o Azure também cria *pares de regiões*.

Como o par de regiões está diretamente conectado e suficientemente afastado para ser isolado contra desastres regionais, você pode usá-lo para fornecer redundância de dados e serviços confiáveis. Alguns serviços oferecem armazenamento com redundância geográfica automática usando pares de regiões.

Vantagens adicionais dos pares de regiões:

Se ocorrer uma interrupção ampla do Azure, uma região de cada par será priorizada para que pelo menos uma seja restaurada o quanto antes para os aplicativos hospedados nesse par de regiões.

As atualizações planejadas do Azure são distribuídas para regiões emparelhadas uma por vez, de modo a minimizar o tempo de inatividade e o risco de interrupção dos aplicativos.

Os dados continuam residindo na mesma geografia que seu par (com exceção do Sul do Brasil) para fins de jurisdição do imposto e aplicação da lei.

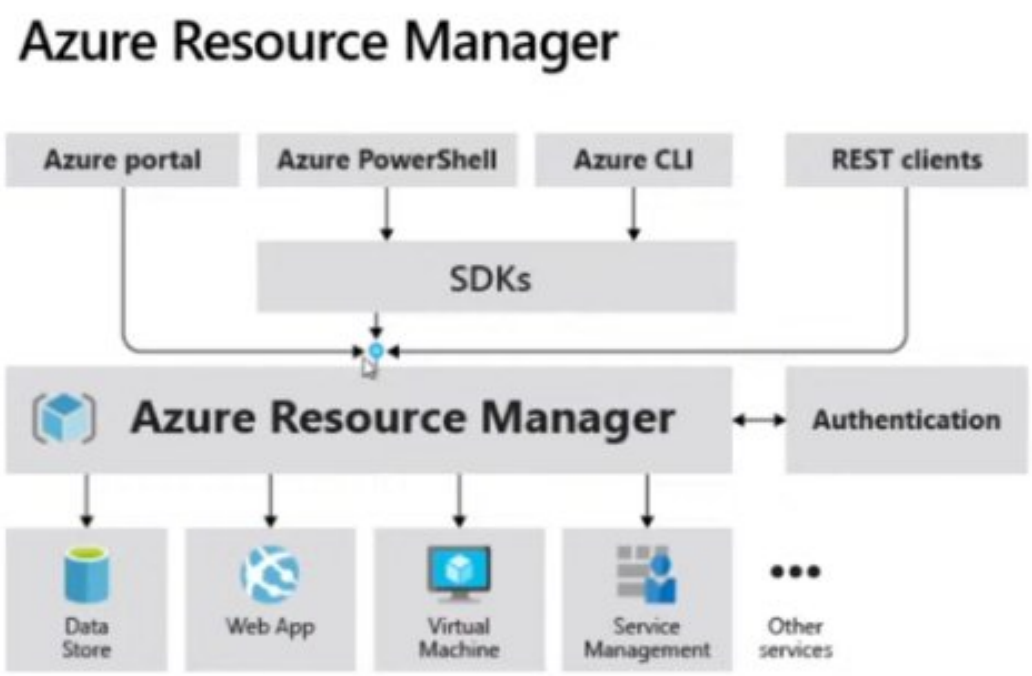
Ter um conjunto de datacenters distribuído em larga escala permite que o Azure forneça uma garantia de alta disponibilidade.

Recursos do Azure e Azure Resource Manager

Recurso: um item gerenciável disponibilizado por meio do Azure. VMs (máquinas virtuais), contas de armazenamento, aplicativos Web, bancos de dados e redes virtuais são exemplos de recursos.

Grupo de recursos: um contêiner que armazena os recursos relacionados de uma solução do Azure . O grupo de recursos inclui os recursos que você deseja gerenciar como um grupo**. Você decide quais recursos pertencem a um grupo de recursos com base no que faz mais sentido para sua organização (Permissão).**

Ele é obrigatório, são divido em 7 itens = 01 VM, por exemplo.



Azure Resource Manager é um 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. Você usa recursos de gerenciamento como controle de acesso, bloqueios e marcas para proteger e organizar seus recursos após a implantação.

Assinaturas do Azure

A utilização do Azure exige uma Assinatura do Azure. Uma assinatura fornece a você acesso autenticado e autorizado a serviços e produtos do Azure. Ela também permite que você provisione recursos. Uma assinatura do Azure é uma unidade lógica de serviços do Azure que se vincula a uma conta do Azure, que é uma identidade no Azure AD (Azure Active Directory) ou em um diretório no qual o Azure AD confia.

Com o Resource Manager, você pode:

Gerenciar sua infraestrutura por meio de modelos declarativos em vez de scripts. Um modelo do Resource Manager é um arquivo JSON que define o que você deseja implantar no Azure.

Implantar, gerenciar e monitorar todos os recursos da sua solução como um grupo em vez de tratá-los individualmente.

Reimplantar a solução durante o ciclo de vida de desenvolvimento e ter confiança de que os recursos serão implantados em um estado consistente.

Definir as dependências entre os recursos para que eles sejam implantados na ordem correta.

Aplicar o controle de acesso a todos os serviços porque o RBAC é integrado nativamente à plataforma de gerenciamento.

Aplicar marcas aos recursos para organizar de modo lógico todos os recursos em sua assinatura.

Esclarecer a cobrança da organização exibindo os custos de um grupo de recursos que compartilham a mesma marca.

Assinaturas (Subscriptions) do Azure

A utilização do Azure exige uma Assinatura do Azure. **Uma assinatura** fornece a você acesso autenticado e autorizado a serviços e produtos do Azure. Ela também permite que você provisione recursos. Uma assinatura do Azure é uma unidade lógica de serviços do Azure que se vincula a uma conta do Azure, que é uma identidade no Azure AD (Azure Active Directory) ou em um diretório no qual o Azure AD confia.

Tenant = inquilino

Exercício

1. Quais das alternativas a seguir podem ser usadas para gerenciar a governança entre várias assinaturas do Azure?

- ○ Iniciativas do Azure
- ◉ Grupos de gerenciamento

✔ **A resposta está correta. Os grupos de gerenciamento facilitam a ordenação hierárquica de recursos do Azure em coleções em um nível de escopo acima das assinaturas. Condições de governança distintas podem ser aplicadas a cada grupo de gerenciamento, juntamente com o Azure Policy e os controles de acesso baseado em função do Azure, para gerenciar assinaturas do Azure com eficiência. Os recursos e as assinaturas atribuídos a um grupo de gerenciamento herdam automaticamente as condições aplicadas ao grupo de gerenciamento.**

- ○ Grupos de recursos

2. Quais das alternativas a seguir é uma unidade lógica dos serviços do Azure vinculadas a uma conta do Azure?

- ◉ Assinatura do Azure

✔ **A resposta está correta. Uma assinatura do Azure é uma unidade lógica de serviços do Azure vinculada a uma conta do Azure. Uma assinatura do Azure é um objeto que representa um contêiner em que você pode inserir recursos. As assinaturas estão vinculadas aos locatários, portanto, cada locatário pode ter várias assinaturas, mas não o contrário.**

- ○ Grupo de gerenciamento
- ○ Resource group
- ○ Nuvem pública

3. Qual dos recursos a seguir *não* se aplica aos grupos de recursos?

- ○ Os recursos podem estar em apenas um grupo de recursos.
- ○ O controle de acesso baseado em função pode ser aplicado ao grupo de recursos.
- ◉ Os grupos de recursos podem ser aninhados.

✔ **A resposta está correta. Os grupos de recursos não podem ser aninhados.**

4. Quais das afirmativas a seguir é verdadeira sobre uma assinatura do Azure?

- ○ O uso do Azure não requer uma assinatura.
- ◉ Uma assinatura do Azure é uma unidade lógica de serviços do Azure.

✔ **A resposta está correta. Uma assinatura é um conjunto de serviços do Azure agrupados para acompanhamento e cobrança. O controle de acesso a recursos ocorre no nível da assinatura. As organizações usam as assinaturas do Azure para gerenciar e controlar os recursos do Azure delas.**

Parte 2: descrever os principais serviços do Azure

Máquinas virtuais - IAAS

Máquinas virtuais são emulações de software de computadores físicos. Elas incluem um processador virtual, memória, armazenamento e recursos de rede. As VMs hospedam um sistema operacional, e você pode instalar e executar o software como se fosse um computador físico. Utilize um cliente da Área de Trabalho Remota para usar e controlar a VM como se estivesse na frente dela.

Serviço de Aplicativo

Com o Serviço de Aplicativo do Azure, você pode criar, implantar e dimensionar rapidamente **aplicativos Web, móveis e de API de nível empresarial executados em qualquer plataforma.** Você pode atender a requisitos rigorosos de desempenho, escalabilidade, segurança e conformidade ao usar uma plataforma totalmente gerenciada para executar a manutenção de infraestrutura. **O Serviço de Aplicativo é uma oferta de PaaS (plataforma como serviço).**

Deployment Center, dentro dele têm

CI - Continuous integration

CD - Continuous Deployment

Contêineres - PaaS e Kubernetes

Contêineres são ambientes de aplicativos leves e virtualizados. Eles foram projetados para serem criados rapidamente, escalados horizontalmente e interrompidos dinamicamente. Você pode executar várias instâncias de um aplicativo em contêineres em um **computador host.**

Azure Functions Funções

As funções são ideais quando você está preocupado apenas com o código que executa o serviço, e não com a plataforma ou a infraestrutura subjacente. Elas costumam ser usadas quando você precisa executar um trabalho em resposta a um evento (geralmente por meio de uma solicitação REST), um temporizador ou uma mensagem de outro serviço do Azure, e quando esse trabalho pode ser concluído dentro de segundos.

Aplicativos Lógicos do Azure

Os aplicativos lógicos são semelhantes às funções. Ambos permitem que você dispare lógica com base em um evento. Enquanto as funções executam código, os aplicativos lógicos executam *fluxos de trabalho* criados para automatizar cenários de negócios com base em blocos de lógica predefinida.

Functions vs. Aplicativos Lógicos

O Functions e os Aplicativos Lógicos podem criar orquestrações complexas. Uma orquestração é uma coleção de funções ou etapas que são executadas para realizar uma tarefa complexa.

Com o Functions, você escreve código para concluir cada etapa.

Com os Aplicativos Lógicos, você usa uma GUI para definir as ações e como elas se relacionam entre si.

Você pode combinar serviços ao compilar uma orquestração, chamando funções de aplicativos lógicos e chamando aplicativos lógicos de funções. No entanto, há algumas diferenças entre essas implementações.

O **Lote do Azure** trabalhos em lotes paralelos e de HPC (computação de alto desempenho) de grande escala com a capacidade de dimensionar dezenas, centenas ou milhares de VMs.

Pode haver situações em que você precise de potência de computação bruta ou de potência de computação no nível de supercomputador.

Tipos de serviços de aplicativos

Com o Serviço de Aplicativo, você pode hospedar os estilos mais comuns de serviço de aplicativos, como:

Aplicativos Web

O Serviço de Aplicativo inclui suporte completo para a hospedagem de aplicativos Web usando ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP ou Python. Você pode escolher Windows ou Linux como sistema operacional do host.

Aplicativos de API

Da mesma forma como se hospeda um site, você pode criar APIs Web baseadas em REST usando a linguagem e a estrutura que você quiser. Receba o suporte completo do Swagger e a capacidade de empacotar e publicar sua API no Azure Marketplace. Os aplicativos produzidos podem ser consumidos por qualquer cliente baseado em HTTP ou em HTTPS.

WebJobs

Você pode usar o recurso do WebJobs para executar um script (.cmd, .bat, PowerShell ou Bash) ou um programa (.exe, Java, PHP, Python ou Node.js) no mesmo contexto de um aplicativo Web, aplicativo de API ou aplicativo móvel. Eles também podem ser agendados ou executados por um gatilho. O WebJobs geralmente é usado para executar tarefas em segundo plano como parte da lógica do aplicativo.

Aplicativos móveis

Use o recurso Aplicativos Móveis do Serviço de Aplicativo para criar rapidamente um back-end para aplicativos iOS e Android.

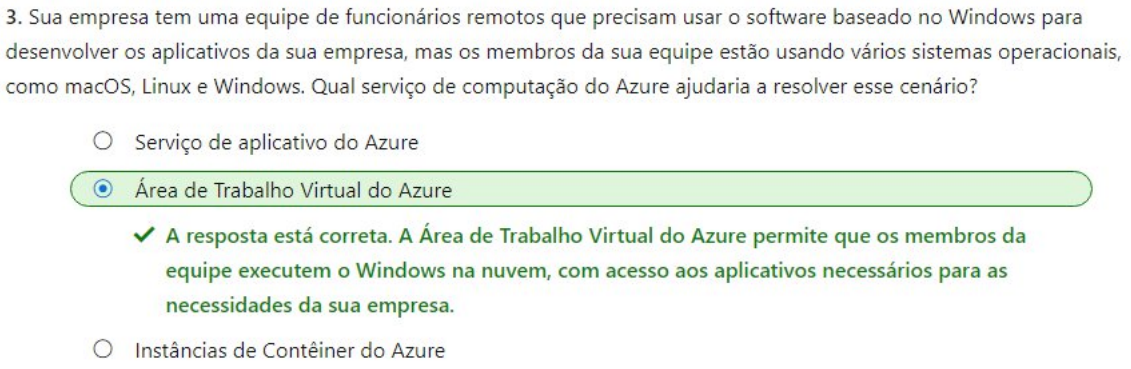
Exercício

1. Qual recurso de Computação do Azure pode ser implantado para gerenciar um conjunto de máquinas virtuais idênticas?

- (●) conjuntos de escala de máquina virtual
  - ✔ **A resposta está correta. Com os conjuntos de dimensionamento de máquinas virtuais, você pode implantar e gerenciar um conjunto de máquinas virtuais idênticas.**
- ( ) Conjuntos de disponibilidade da máquina virtual
- ( ) Zonas de disponibilidade da máquina virtual

2. Quais dos seguintes serviços devem ser usados quando a principal preocupação é executar o trabalho em resposta a um evento (geralmente por meio de um comando REST) que precisa de uma resposta em alguns segundos?

- (●) Azure Functions
  - ✔ **A resposta está correta. O Azure Functions é usado quando você precisa executar um trabalho em resposta a um evento (geralmente por meio de uma solicitação REST), um temporizador ou uma mensagem de outro serviço do Azure, e quando esse trabalho pode ser concluído dentro de segundos.**
- ( ) Serviço de aplicativo do Azure
- ( ) Instâncias de Contêiner do Azure



Rede virtual : A Rede Virtual do Azure (VNet) é o bloco de construção fundamental de sua rede privada no Azure.

ExpressRoute: O ExpressRoute permite que você estenda as redes locais para a nuvem da Microsoft por meio de uma conexão privada, facilitada por um provedor de conectividade. Essa conexão é privada.

Gateway de VPN: O Gateway de VPN ajuda você a criar conexões criptografadas entre locais para sua rede virtual pelos locais ou criar conexões criptografadas entre as VNets. Há diferentes configurações disponíveis para conexões de Gateway de VPN, como site a site, ponto a site e VNet a VNet.

Exercício

1. A Tailwind Traders quer criar um túnel de comunicação seguro entre as filiais. Quais das tecnologias a seguir não podem ser usadas?

- ○ Rede virtual privada ponto a site
- ○ FTP sobre SSL implícito

✔ A resposta está correta. O FTP sobre SSL não pode ser usado para criar um túnel de comunicação seguro.

- ◉ Azure ExpressRoute

✘ A resposta está incorreta. O Azure ExpressRoute pode ser usado para criar um túnel de comunicação seguro entre as localizações.

- ○ Rede virtual privada site a site

2. A Tailwind Traders quer usar o Azure ExpressRoute para conectar a rede local à nuvem da Microsoft. Quais das opções a seguir não é um modelo de ExpressRoute que a Tailwind Traders pode usar?

- ○ Conexão qualquer para qualquer
- ○ Rede virtual privada site a site

✔ A resposta está correta. Uma rede virtual privada site a site não é um modelo do ExpressRoute.

- ◉ Conexão Ethernet ponto a ponto

✘ A resposta está incorreta. A conexão Ethernet ponto a ponto é um modelo do ExpressRoute.

- ○ Colocação do CloudExchange

3. Quais das opções a seguir você pode usar para vincular redes virtuais?

- ○ Conversão de endereços de rede
- ○ Agregação de link de vários chassis
- ○ Protocolo DHCP
- ◉ Emparelhamento de rede virtual

✔ A resposta está correta. O emparelhamento de rede virtual pode ser usado para vincular redes virtuais.

4. Qual das opções a seguir não é um benefício do ExpressRoute?

- ◉ Conectividade redundante

✘ Esta opção é um benefício de escolher conectar sua rede à Microsoft usando o ExpressRoute.

- ○ Taxa de transferência de rede consistente
- ○ Comunicação de rede criptografada

✔ A resposta está correta. O ExpressRoute fornece conectividade privada, mas não é criptografado.

- ○ Acesso aos serviços em nuvem da Microsoft

O Armazenamento de Blobs do Azure é uma solução de armazenamento de objetos para a nuvem. Ele pode armazenar grandes quantidades de dados, como texto ou dados binários. Não é estruturado, o que significa que não há nenhuma restrição quanto aos tipos de dados que ele pode armazenar. Pode

gerenciar milhares de carregamentos simultâneos, grandes quantidades de dados de vídeo, arquivos de log em constante crescimento e pode ser acessado de qualquer lugar com uma conexão com a Internet.

O Armazenamento do Azure oferece diferentes camadas de acesso para seu armazenamento de blobs, ajudando você a armazenar dados de objeto da maneira mais econômica. As camadas de acesso disponíveis incluem:

Camada de acesso quente: otimizada para armazenar dados que são acessados com frequência (por exemplo, imagens de seu site).

Camada de acesso frio: otimizada para dados acessados com menos frequência e armazenados por pelo menos 30 dias (por exemplo, faturas de seus clientes).

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

Os Arquivos do Azure: oferecem compartilhamentos de arquivo totalmente gerenciados na nuvem que são acessíveis por meio dos protocolos SMB e Network File System (versão prévia) padrão do setor. Os compartilhamentos de arquivos do Azure podem ser montados de maneira simultânea por implantações locais ou na nuvem do Windows, do Linux e do MacOS.

Firewall do Azure: é um serviço de segurança de rede gerenciado e baseado em nuvem que protege seus recursos de Rede Virtual do Azure. Usando o Firewall do Azure, é possível criar, impor e registrar centralmente políticas de conectividade de rede e de aplicativo em assinaturas e redes virtuais. O Firewall do Azure usa um endereço IP público estático para seus recursos de rede virtual, permitindo que firewalls externos identifiquem o tráfego originário de sua rede virtual.

Serviços de monitoramento de rede

Esta seção descreve os serviços de rede no Azure que ajudam a monitorar os recursos de rede: Observador de Rede, Insights de Rede do Azure Monitor, Azure Monitor, Monitor do ExpressRoute e TAP de Rede Virtual.

Observador de Rede

Observador de Rede do Azure fornece ferramentas para monitorar, diagnosticar, exibir métricas e ativar ou desativar os logs de recursos em uma rede virtual do Azure. Para obter mais informações, confira O que é o Observador de Rede?.

Insights de Rede do Azure Monitor

O Azure Monitor para Redes: fornece uma visão abrangente da integridade e das métricas para todos os recursos de rede implementados, sem exigir nenhuma configuração. Ele também fornece acesso a recursos de monitoramento de rede, como o Monitor da Conexão, o log de fluxo para grupos de segurança de rede e Análise de Tráfego. Para saber mais, confira Insights de Rede do Azure Monitor.

ExpressRoute Monitor: Para saber mais sobre como exibir métricas de circuito, logs de recursos e alertas do ExpressRoute, confira Monitoramento, métricas e alertas do ExpressRoute.

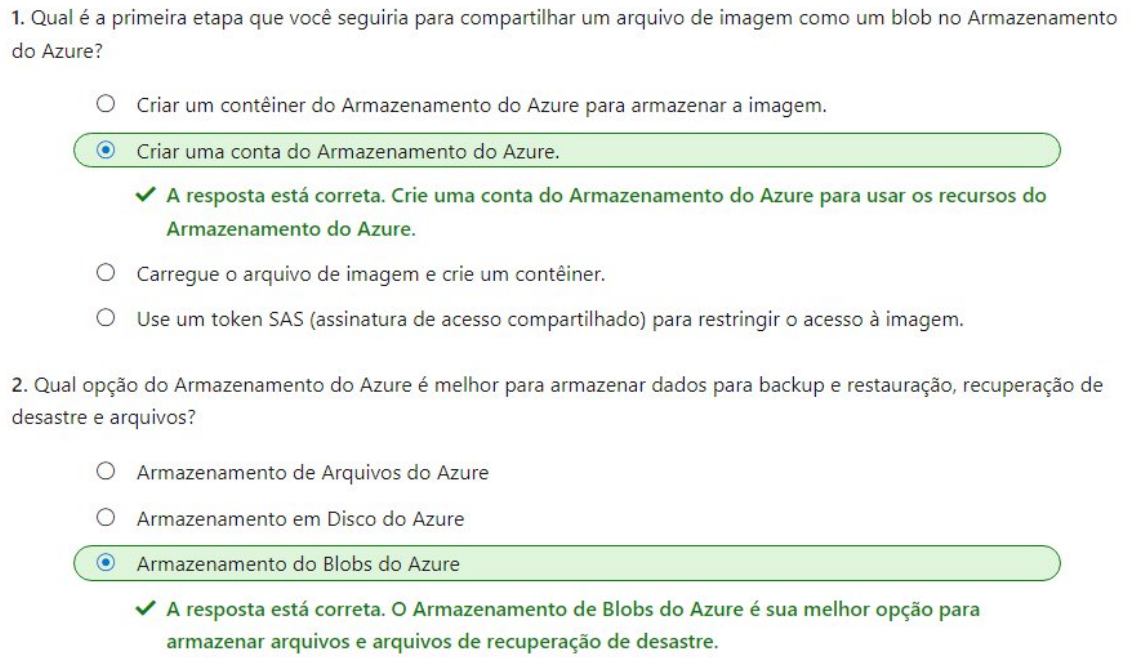
Azure Monitor: O Azure Monitor maximiza a disponibilidade e o desempenho de seus aplicativos fornecendo uma solução abrangente para coletar, analisar e agir em relação a dados telemétricos de seus ambientes locais e de nuvem. Ele ajuda a entender o desempenho de seus aplicativos, além de identificar de maneira proativa os problemas que os estão afetando e os recursos dos quais eles dependem.

O DNS do Azure: é um 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 faturamento que os outros serviços do Azure. Para obter mais informações, confira O que é DNS do Azure?.

O serviço do Azure Bastion: é um serviço PaaS totalmente gerenciado por plataforma que pode ser provisionado dentro de sua rede virtual. Ele fornece conectividade de RDP/SSH contínua e segura às suas máquinas virtuais, diretamente no portal do Azure, via TLS. Quando você se conecta

usando o Azure Bastion, suas máquinas virtuais não precisam de um endereço IP público. Para obter mais informações.

Exercício



O Armazenamento de Blobs do Azure é uma solução de armazenamento de objetos para a nuvem. Ele pode armazenar grandes quantidades de dados, como texto ou dados binários. Ele não é estruturado, o que significa que não há nenhuma restrição quanto aos tipos de dados que ele pode armazenar. Faz o conceito de RAID. Velocidade de acesso ao dados, por ser randômico (pedaço pequenos de dados em vários lugares)

Camada de acesso quente: otimizada para armazenar dados que **são acessados com frequência** (por exemplo, imagens de seu site).

Camada de acesso frio: otimizada para dados acessados com menos frequência e armazenados por pelo menos **30 dias**.

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

O Azure Cosmos DB é um serviço de multi modelo de banco de dados distribuído globalmente (plataforma de Dados). Você pode escalar de modo elástico e independente a taxa de transferência e o armazenamento em qualquer número de regiões do Azure em todo o mundo. Você pode aproveitar o acesso a dados rápido e em poucos milissegundos usando uma das várias APIs populares. O **Azure Cosmos DB** fornece contratos de nível de serviço abrangentes para taxa de transferência, latência, disponibilidade e garantias de consistência.

O Azure Cosmos DB é flexível. No nível mais baixo, o Azure Cosmos DB armazena dados no formato ARS (atom-record-sequence). Os dados são então abstraídos e projetados como uma API, que você especifica ao criar o seu banco de dados. Suas opções incluem SQL, MongoDB, Cassandra, Tables e Gremlin. Esse nível de flexibilidade significa que, conforme você migra os bancos de dados da empresa para o Azure Cosmos DB, os desenvolvedores podem continuar usando as APIs com as quais se sentem mais confortáveis.

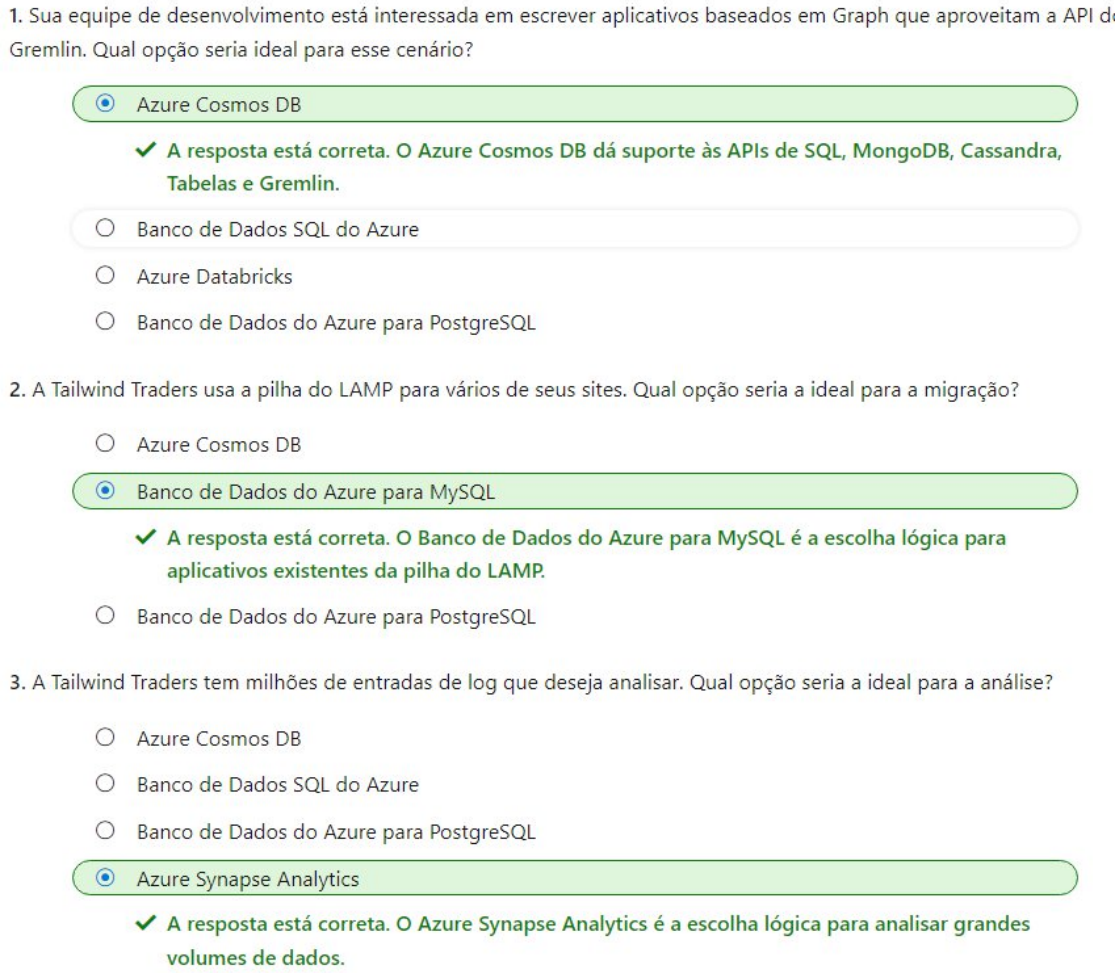
O Banco de Dados SQL do Azure é um mecanismo de banco de dados de PaaS (plataforma como serviço). Ele lida com a maioria das funções de gerenciamento de banco de dados, como atualização, aplicação de patches, backups e monitoramento, sem envolvimento do usuário. O Banco de Dados SQL fornece 99,99% de disponibilidade.

O Banco de Dados do Azure para MySQL é um serviço de banco de dados relacional na nuvem que se baseia no mecanismo de banco de dados MySQL Community Edition, nas versões 5.6, 5.7 e 8.0. Com ele, você tem um SLA de disponibilidade de 99,99% no Azure, desenvolvido por uma rede global de datacenters gerenciados pela Microsoft.

O Banco de Dados do Azure para PostgreSQL é um serviço de banco de dados relacional na nuvem. O software para servidores se baseia na versão da comunidade do mecanismo de banco de dados PostgreSQL de software livre. A sua familiaridade com as ferramentas e conhecimento sobre o PostgreSQL são aplicáveis ao usar o Banco de Dados do Azure para PostgreSQL.

O Azure HDInsight é um serviço de análise de software livre totalmente gerenciado para empresas. Trata-se de um serviço de nuvem que torna mais fácil, mais rápido e mais econômico o processamento de grandes quantidades de dados.
O Azure Databricks ajuda a descobrir insights dos seus dados e a criar soluções de inteligência artificial.

O Azure Data Lake Analytics é um serviço de trabalho de análise sob demanda que simplifica Big Data. Em vez de implantar, configurar e ajustar o hardware, você escreve consultas para transformar seus dados e extrair informações importantes. O serviço de análise pode manipular trabalhos de qualquer escala de maneira instantânea, simplesmente configurando o controle para a quantidade de potência necessária.
Exercício



Modulo 04 – descrever os recursos gerais de segurança de rede e segurança

O que é a Central de Segurança do Azure?

A Central de Segurança do Azure é um serviço de monitoramento que fornece visibilidade da postura de segurança em todos os serviços, tanto no Azure quanto localmente. O termo *postura de segurança* se refere a políticas e controles de segurança cibernética, bem como à sua capacidade de prever, impedir e responder com sucesso às ameaças de segurança.

A Central de Segurança pode:

- Monitorar as configurações de segurança das cargas de trabalho locais e na nuvem.
- Aplicar automaticamente as configurações de segurança obrigatórias aos novos recursos à medida que ficarem online.
- Fornecer recomendações de segurança baseadas nas configurações, nos recursos e nas redes atuais.
- Monitorar continuamente os recursos e realizar avaliações de segurança automáticas para identificar possíveis vulnerabilidades antes que elas possam ser exploradas.
- Usar machine learning para detectar e bloquear a instalação de malwares em VMs (máquinas virtuais) e em outros recursos. Você também pode usar os *controles de aplicativo adaptáveis* para definir regras que listam os aplicativos permitidos a fim de verificar se somente os aplicativos que você permitir serão executados.
- Detectar e analisar possíveis ataques de entrada e investigar ameaças e qualquer atividade pós-violação que possa ter ocorrido.
- Fornecer controle de acesso just-in-time para as portas de rede. Isso reduz a superfície de ataque, garantindo que a rede só permita o tráfego exigido por você, no momento necessário.

Proteção contra ameaças

A Central de Segurança inclui funcionalidades avançadas de defesa de nuvem para VMs, segurança de rede e integridade de arquivo. Vamos ver como algumas dessas funcionalidades se aplicam à Tailwind Traders.

Acesso just-in-time à VM A Tailwind Traders vai configurar o acesso just-in-time às VMs. Esse acesso bloqueia por padrão o tráfego para portas de rede específicas de VMs, mas permite o tráfego por um período especificado quando um administrador o solicita e aprova.

Controles de aplicativo adaptáveis A Tailwind Traders pode controlar quais aplicativos podem ser executados em suas VMs. Em segundo plano, a Central de Segurança usa machine learning para examinar os processos em execução em uma VM. Ela cria regras de exceção para cada grupo de recursos que contém as VMs e fornece recomendações. Esse processo fornece alertas que informam a empresa sobre aplicativos não autorizados em execução em suas VMs.

Proteção de rede adaptável A Central de Segurança pode monitorar os padrões de tráfego de Internet das VMs e comparar esses padrões com as configurações atuais de NSG (grupo de segurança de rede) da empresa. Em seguida, a Central de Segurança pode recomendar que os NSGs sejam bloqueados ainda mais e fornecer etapas de correção.

Monitoramento de integridade do arquivo A Tailwind Traders também pode configurar o monitoramento de alterações em arquivos importantes no Windows e no Linux, de configurações do Registro, de aplicativos e de outros aspectos que possam indicar um ataque de segurança.

Detectar e responder a ameaças de segurança usando o Azure Sentinel

O gerenciamento da segurança em grande escala pode se beneficiar de um sistema de SIEM (gerenciamento de evento e informações de segurança) dedicado. O sistema de SIEM agrega dados de segurança de várias fontes diferentes (contanto que essas fontes sejam compatíveis com um formato padrão aberto de registro em log). Ele também fornece recursos de detecção e resposta a ameaças.

O Azure Sentinel é o sistema de SIEM baseado em nuvem da Microsoft. Ele usa análise de segurança e análise de ameaças inteligentes

Funcionalidades do Azure Sentinel

O Azure Sentinel permite que você:

Coletar dados de nuvem em escala Colete dados de todos os usuários, dispositivos, aplicativos e infraestrutura, tanto locais quanto de várias nuvens.

Detectar ameaças não detectadas anteriormente Minimize falsos positivos usando a análise abrangente e a inteligência contra ameaças da Microsoft.

Investigar ameaças com inteligência artificial Examine atividades suspeitas em escala, aproveitando a longa experiência em segurança cibernética da Microsoft.

Responder a incidentes rapidamente Use a orquestração e a automação internas para tarefas comuns.

O Azure Key Vault é um serviço de nuvem centralizado para armazenar segredos do aplicativo em um só local centralizado. Ele oferece acesso seguro a informações confidenciais fornecendo controle de acesso e funcionalidades de registro em log.

O Host Dedicado do Azure fornece servidores físicos dedicados para hospedar as VMs do Azure para Windows e Linux.

Depois que um host dedicado é provisionado, o Azure o atribui ao servidor físico no datacenter de nuvem da Microsoft.

Para alta disponibilidade, você pode provisionar vários hosts em um *grupo de hosts* e implantar suas VMs nesse grupo. VMs em hosts dedicados também podem aproveitar o *controle de manutenção*. Esse recurso permite controlar quando ocorrem atualizações de manutenção regulares, dentro de uma janela ininterrupta de 35 dias.

Exercícios

1. Como a Tailwind Traders pode impor que apenas determinados aplicativos sejam executados em suas VMs?

- ○ Conecte as VMs ao Azure Sentinel.
- ◉ Crie uma regra de controle de aplicativo na Central de Segurança do Azure.

  ✔ **A resposta está correta. Com a Central de Segurança do Azure, você pode definir uma lista de aplicativos permitidos para que somente os aplicativos permitidos possam ser executados. A Central de Segurança do Azure também pode detectar e bloquear a instalação de malware nas VMs.**
- ○ Execute periodicamente um script que liste os processos em execução em cada VM. Então, o gerente de TI pode desligar todos os aplicativos que não deveriam estar em execução.

2. Qual é a maneira mais fácil para a Tailwind Traders combinar os dados de segurança de todas as ferramentas de monitoramento em um só relatório, com base no qual eles possam tomar medidas?

- ◉ Colete dados de segurança no Azure Sentinel.

  ✔ **A resposta está correta. O Azure Sentinel é o SIEM baseado em nuvem da Microsoft. Um SIEM agrega dados de segurança de várias fontes diferentes a fim de fornecer funcionalidades adicionais para a detecção de – e a resposta a – ameaças.**
- ○ Crie uma ferramenta personalizada que colete dados de segurança e exiba um relatório por meio de um aplicativo Web.
- ○ Examine cada log de segurança diariamente e envie um resumo por email à equipe.

3. Qual é a melhor maneira para a Tailwind Traders armazenar seus certificados com segurança, para que eles fiquem acessíveis às VMs da nuvem?

- ○ Coloque os certificados em um compartilhamento de rede.
- ○ Armazene-os em uma VM protegida por uma senha.
- ◉ Armazene os certificados no Azure Key Vault.

  ✔ **A resposta está correta. O Azure Key Vault permite que você armazene seus segredos em um só local centralizado. Com o Key Vault, também fica mais fácil registrar e renovar certificados de CAs (autoridades de certificação) públicas.**

4. Como a Tailwind Traders verifica se determinadas cargas de trabalho de VM estão fisicamente isoladas das cargas de trabalho executadas por outros clientes do Azure?

- ○ Configure a rede para que as VMs em um mesmo host físico fiquem isoladas.
- ○ Isso não é possível. Essas cargas de trabalho precisam ser executadas localmente.
- ◉ Execute as VMs no Host Dedicado do Azure.

  ✔ **A resposta está correta. O Host Dedicado do Azure fornece servidores físicos dedicados para hospedar as VMs do Azure para Windows e Linux.**

Resumo

Central de Segurança do Azure

Confira o módulo Resolver as ameaças de segurança com a Central de Segurança do Azure para usar as funcionalidades de alerta da Central de Segurança do Azure para inspecionar e responder às ameaças.

Em seguida, examine o Guia de planejamento e operações para otimizar o uso da Central de Segurança com base nos requisitos de segurança e no modelo de gerenciamento de nuvem da organização.

Azure Sentinel

O módulo Criar uma estratégia de monitoramento holística no Azure fornece mais detalhes sobre como o Azure Sentinel pode ajudar a monitorar e responder a ameaças de segurança em toda a organização.

Saiba também como conectar fontes de dados ao Azure Sentinel.

Cofre de Chave do Azure

Adquira experiência prática adicional com o Azure Key Vault em Gerenciar segredos nos aplicativos de servidor com o Azure Key Vault e Configurar e gerenciar segredos no Azure Key Vault.

Um *firewall* é um dispositivo de segurança de rede que monitora o tráfego de rede de entrada e saída e decide se deve permitir ou bloquear o tráfego específico com base em um conjunto definido de regras de segurança. Você pode criar regras de firewall que especificam intervalos de endereços IP específicos. Somente clientes com endereços IP concedidos dentro desses intervalos têm permissão para acessar o servidor de destino. Em geral, as regras de firewall também podem incluir informações de porta e protocolo de rede específicas.

O que é o Firewall do Azure?

O Firewall do Azure é um serviço de segurança de rede gerenciado e baseado em nuvem que ajuda a proteger recursos nas redes virtuais do Azure. Uma rede virtual é semelhante a uma rede tradicional que você operaria em seu datacenter. É um bloco de construção fundamental para sua rede privada que permite que

máquinas virtuais e outros recursos de computação se comuniquem com segurança entre si, pela Internet e pelas redes locais.

O Firewall do Azure é um firewall *com estado*. Um firewall com estado analisa o contexto completo de uma conexão de rede, não apenas um pacote individual de tráfego de rede. O Firewall do Azure apresenta alta disponibilidade e escalabilidade de nuvem irrestrita.

O Gateway de Aplicativo do Azure também fornece um firewall, chamado de *WAF (firewall do aplicativo Web)*. O WAF fornece proteção de entrada centralizada para seus aplicativos Web contra explorações e vulnerabilidades comuns. O Azure Front Door e a Rede de Distribuição de Conteúdo do Azure também fornecem serviços de WAF.

O que são ataques de DDoS?

Um ataque de negação de serviço distribuído tenta sobrecarregar e esgotar os recursos de um aplicativo, tornando-o lento ou sem resposta para usuários legítimos. Os ataques de DDoS podem ter como alvo qualquer recurso acessível publicamente pela Internet, incluindo sites.

O que é a Proteção contra DDoS do Azure?

A Proteção contra DDoS do Azure (Standard) ajuda a proteger seus recursos do Azure contra ataques de DDoS.

Ao combinar a Proteção contra DDoS com práticas recomendadas de design de aplicativo, você ajuda a fornecer uma defesa contra ataques de DDoS. A Proteção contra DDoS usa a escala e a elasticidade da rede global da Microsoft para levar capacidade de mitigação de DDoS a todas as regiões do Azure. O serviço de Proteção contra DDoS ajuda a proteger seus aplicativos do Azure analisando e descartando o tráfego de DDoS na borda da rede do Azure, antes que ele possa afetar a disponibilidade do serviço.

A Proteção contra DDoS oferece estas camadas de serviço:

Basic

A camada de serviço Básica é automaticamente habilitada de modo gratuito como parte da sua assinatura do Azure.

O monitoramento de tráfego sempre ativo e a mitigação em tempo real de ataques comuns no nível de rede fornecem os mesmos tipos de proteção usados pelos serviços online da Microsoft. A camada de serviço Básica garante que a própria infraestrutura do Azure não seja afetada durante um ataque de DDoS em grande escala.

A rede global do Azure é usada para distribuir e atenuar o tráfego de ataques entre regiões do Azure.

Standard

A camada de serviço Standard fornece funcionalidades de mitigação adicionais ajustadas especificamente para os recursos de Rede Virtual do Azure. A Proteção contra DDoS Standard é relativamente fácil de habilitar e não requer alterações aos aplicativos.

A camada Standard fornece monitoramento de tráfego sempre ativo e mitigação em tempo real de ataques comuns no nível de rede. Ela oferece as mesmas defesas que os serviços online da Microsoft usam.

As políticas de proteção são ajustadas por meio do monitoramento de tráfego dedicado e de algoritmos de aprendizado de máquina. As políticas são aplicadas a endereços IP públicos associados aos recursos implantados em redes virtuais, como o Azure Load Balancer e o Gateway de Aplicativo.

A rede global do Azure é usada para distribuir e atenuar o tráfego de ataques entre regiões do Azure.

A camada de serviço Standard pode ajudar a evitar:

Ataques volumétricos

A meta desse ataque é inundar a camada de rede com uma quantidade significativa de tráfego aparentemente legítimo.

Ataques de protocolo

Esses ataques renderizam um destino inacessível explorando uma vulnerabilidade na pilha de protocolos das camadas 3 e 4.

Ataques de camada de recurso (camada de aplicativo) (somente com o firewall do aplicativo Web)

Esses ataques são direcionados a pacotes de aplicativo Web para interromper a transmissão de dados entre os hosts. Você precisa de um WAF (firewall do aplicativo Web) para proteger-se contra ataques L7. A

Proteção contra DDoS Standard protege o WAF contra ataques volumétricos e de protocolo.

O que são os grupos de segurança de rede do Azure?

Um grupo de segurança de rede permite filtrar o tráfego de rede proveniente dos recursos do Azure e destinado a eles em uma rede virtual do Azure. Considere os NSGs como um firewall interno. Um NSG pode conter várias regras de segurança de entrada e saída que permitem a filtragem do tráfego para e de recursos por endereço IP de origem e de destino, porta e protocolo.

Proteger a camada do perímetro

A camada do perímetro refere-se a proteger os recursos da sua organização contra ataques baseados em rede. Identificar esses ataques, alertar as equipes de segurança apropriadas e eliminar seu impacto são aspectos importantes para manter sua rede segura. Para fazer isso:

Use a Proteção contra DDoS do Azure para filtrar ataques em grande escala antes que eles possam causar uma negação de serviço para os usuários.

Use firewalls de perímetro com o Firewall do Azure para identificar e alertar sobre ataques maliciosos contra a rede.

Proteger a camada de rede

Essa camada concentra-se em limitar a conectividade de rede entre todos os recursos para permitir apenas o necessário. Segmente seus recursos e use os controles de nível de rede para restringir a comunicação apenas ao que é necessário.

Ao restringir a conectividade, você reduz o risco de movimento lateral em toda a rede contra um ataque. Use grupos de segurança de rede para criar regras que definem a comunicação de entrada e saída permitida nessa camada. Aqui estão algumas práticas recomendadas:

Limitar a comunicação entre os recursos segmentando sua rede e configurando os controles de acesso.

Negue por padrão.

Restringir o acesso à Internet de entrada e limite a saída quando apropriado.

Implemente a conectividade segura com as redes locais.

Combinar serviços

Você pode combinar os serviços de segurança e de rede do Azure para gerenciar a segurança da rede e fornecer maior proteção em camadas. Veja algumas maneiras de combinar serviços:

Grupos de segurança de rede e Firewall do Azure

O Firewall do Azure complementa a funcionalidade dos grupos de segurança de rede. Juntos, eles fornecem uma melhor segurança de rede de defesa aprofundada.

Os grupos de segurança de rede fornecem filtragem de tráfego de camada de rede distribuída para limitar o tráfego aos recursos dentro das redes virtuais em cada assinatura.

O Firewall do Azure é um firewall de rede como serviço totalmente centralizado e com estado. Ele fornece proteção no nível da rede e do aplicativo em diferentes assinaturas e redes virtuais.

Firewall do aplicativo Web do Gateway de Aplicativo do Azure e Firewall do Azure

O WAF (firewall do aplicativo Web) é um recurso do Gateway de Aplicativo do Azure que fornece aos seus aplicativos Web proteção de entrada centralizada contra explorações e vulnerabilidades comuns.

O Firewall do Azure fornece:

- Proteção de entrada para protocolos não HTTP/S (por exemplo, RDP, SSH e FTP).
- Proteção em nível de rede de saída para todas as portas e protocolos.
- Proteção em nível de aplicativo para HTTP/S de saída.

Combiná-los fornece mais camadas de proteção.

Verificar seus conhecimentos

1. Um invasor pode derrubar seu site enviando um grande volume de tráfego de rede para seus servidores. Qual serviço do Azure pode ajudar a Tailwind Traders a proteger sua instância do Serviço de Aplicativo contra esse tipo de ataque?

- ○ Firewall do Azure
- ○ Grupos de segurança de rede
- ◉ Proteção contra DDoS do Azure

✔ **A proteção contra DDoS ajuda a proteger os recursos do Azure contra ataques de DDoS. Um ataque de DDoS tenta sobrecarregar e esgotar os recursos de um aplicativo, tornando o aplicativo lento ou sem resposta a usuários legítimos.**

2. Qual é a melhor maneira de a Tailwind Trades limitar todo o tráfego de saída de VMs para hosts conhecidos?

- ○ Configurar a Proteção contra DDoS do Azure para limitar o acesso à rede a hosts e portas confiáveis.
- ◉ Criar regras de aplicativo no Firewall do Azure.

✔ **O Firewall do Azure permite limitar o tráfego de HTTP/S de saída a uma lista especificada de FQDNs (nomes de domínio totalmente qualificados).**

- ○ Garantir que todos os aplicativos em execução se comuniquem apenas com portas e hosts confiáveis.

3. Como a Tailwind Traders pode implementar com mais facilidade uma política de *negar por padrão* para que as VMs não possam se conectar entre si?

- ○ Aloque cada VM em uma rede virtual própria.
- ◉ Crie uma regra de grupo de segurança de rede que impeça o acesso de outra VM na mesma rede.

✔ **Uma regra de grupo de segurança de rede permite filtrar o tráfego de e para os recursos por endereço IP de origem e de destino, porta e protocolo.**

- ○ Configure a Proteção contra DDoS do Azure para limitar o acesso à rede na rede virtual.

Parte 5: descrever recursos de identidade, governança, privacidade e conformidade

O que é a autenticação?

Autenticação é o processo de estabelecer a identidade de uma pessoa ou serviço que deseja acessar um recurso. Ela envolve o ato de solicitar credenciais legítimas de uma parte e fornece a base para criação de uma entidade de segurança para controle de acesso e identidade. Estabelece se o usuário é quem diz ser.

O que é autorização?

A autenticação estabelece a identidade do usuário, enquanto a autorização é o processo de estabelecer o nível de acesso que uma pessoa ou um serviço autenticado tem. Especifica quais dados podem ser acessados e que a pessoa ou serviço pode fazer com eles.

O que é o Azure Active Directory AAD?

o Azure AD (Azure Active Directory) fornece serviços de **identidade** baseado em nuvem e serviço de gerenciamento de acesso.

Quando você protege identidades locais com o Active Directory, a Microsoft não monitora tentativas de conexão. Quando você conecta o Active Directory ao Azure AD, a Microsoft pode ajudar a protegê-lo detectando tentativas de conexão suspeitas sem custo adicional. Por exemplo, o Azure AD pode detectar tentativas de conexão de locais inesperados ou dispositivos desconhecidos.

O Azure AD é para:

Administradores de TI

Os administradores podem usar o Azure AD para controlar o acesso a aplicativos e recursos com base em seus requisitos de negócios.

Desenvolvedores de aplicativos

Os desenvolvedores podem usar o Azure AD para fornecer uma abordagem baseada em padrões para adicionar funcionalidade a aplicativos que eles criam, como adicionar a funcionalidade de SSO a um aplicativo ou habilitar um aplicativo para trabalhar com as credenciais existentes de um usuário.

Usuários

Os usuários podem gerenciar suas identidades. Por exemplo, a redefinição de senha por autoatendimento permite que os usuários alterem ou redefinam a senha sem envolvimento de um administrador de TI nem do suporte técnico.

Assinantes do serviço online

Os assinantes do Microsoft 365, do Microsoft Office 365, do Azure e do Microsoft Dynamics CRM Online já estão usando o Azure AD.

Um *locatário* é uma representação de uma organização. Normalmente, um locatário é separado de outros locatários e tem a própria identidade.

Cada locatário do Microsoft 365, do Office 365, do Azure e do Dynamics CRM Online é automaticamente um locatário do Azure AD.

Como posso conectar o Active Directory ao Azure AD?
Conectar o Active Directory ao Azure AD permite que você proporcione uma experiência de identidade consistente para seus usuários.
Há algumas maneiras de conectar sua instalação existente do Active Directory ao Azure AD. Talvez o método mais popular seja usar o Azure AD Connect.
O Azure AD Connect sincroniza identidades de usuário entre o Active Directory local e o Azure AD. O Azure AD Connect sincroniza alterações entre os dois sistemas de identidade, o que permite que você use recursos como SSO, autenticação multifator e redefinição de senha por autoatendimento em ambos.

A redefinição de senha por autoatendimento impede que os usuários usem senhas comprometidas conhecidas.

Exercícios

1. Como o departamento de TI pode garantir que os funcionários nas lojas de varejo da empresa possam acessar aplicativos da empresa somente de dispositivos tablet aprovados?

- ○ SSO
- ◉ Acesso Condicional
  - ✔ O acesso condicional permite que você exija que os usuários acessem seus aplicativos somente de dispositivos aprovados ou gerenciados.
- ○ Autenticação multifator

2. Como o departamento de TI pode usar propriedades biométricas, como reconhecimento facial, para permitir que os motoristas de entrega comprovem suas identidades?

- ○ SSO
- ○ Acesso Condicional
- ◉ Autenticação multifator
  - ✔ A autenticação usando a autenticação multifator pode incluir algo que o usuário sabe, algo que o usuário tem e algo que o usuário é.

3. Como o departamento de TI pode reduzir o número de vezes que os usuários precisam ser autenticados para acessar vários aplicativos?

- ◉ SSO
  - ✔ O SSO permite que o usuário se lembre de apenas uma ID e uma senha para acessar vários aplicativos.
- ○ Acesso Condicional
- ○ Autenticacão multifator

Resumo

A AuthN (autenticação): estabelece a identidade do usuário.

A AuthZ (autorização): estabelece o nível de acesso que um usuário autenticado tem.

O SSO (logon único): permite que um usuário entre uma vez e use essa credencial para acessar vários recursos e aplicativos.

O Azure AD (Azure Active Directory): é um serviço de gerenciamento de identidade e acesso baseado em nuvem. O Azure AD permite que a organização controle o acesso a aplicativos e recursos com base em seus requisitos empresariais.

A Autenticação Multifator do Azure AD: fornece segurança adicional para as identidades, exigindo dois ou mais elementos para a autenticação completa. De modo geral, a autenticação multifator pode incluir algo que o usuário sabe, algo que o usuário tem e algo que o usuário é.

O Acesso Condicional: é uma ferramenta usada pelo Azure AD para permitir ou negar o acesso a recursos com base em sinais de identidade, como a localização do usuário.

Quais níveis de bloqueio estão disponíveis?
Você pode aplicar bloqueios a uma assinatura, a um grupo de recursos ou a um recurso individual. É possível definir o nível de bloqueio como **CanNotDelete** ou **ReadOnly**.

CanNotDelete significa que as pessoas autorizadas ainda podem ler e modificar um recurso, mas não podem excluir o recurso sem antes remover o bloqueio.

ReadOnly significa que pessoas autorizadas podem ler um recurso, mas não podem excluir nem alterar o recurso. A aplicação desse bloqueio é como restringir todos os usuários autorizados às permissões concedidas pela função **Leitor** no RBAC do Azure.

Combinar bloqueios de recursos com o Azure Blueprints
E se um administrador de nuvem excluir acidentalmente um bloqueio de recurso? Se o bloqueio de recurso for removido, os recursos associados a eles poderão ser alterados ou excluídos.

Para tornar o processo de proteção mais robusto, você pode combinar bloqueios de recursos com o Azure Blueprints. O Azure Blueprints permite que você defina o conjunto de recursos padrão de recursos do Azure necessário para a sua organização. Por exemplo, você pode definir um blueprint que especifica que determinado bloqueio de recurso precisa existir. O Azure Blueprints poderá substituir automaticamente o bloqueio de recurso se esse bloqueio for removido.

O Azure Policy permite que você defina políticas individuais e *grupos* de políticas relacionadas, conhecidas como *iniciativas*. O Azure Policy avalia seus recursos e realça os que não estão em conformidade com as políticas criadas por você. Ele também pode impedir a criação de recursos sem conformidade.

O Azure Policy vem com definições de iniciativa e política internas para Armazenamento, Rede, Computação, Central de Segurança e Monitoramento. Por exemplo, se você definir uma política que permita que apenas um determinado tamanho de SKU (unidade de manutenção de estoque) para VMs (máquinas virtuais) seja usado em seu ambiente, essa política será invocada quando você criar VMs e sempre que você redimensionar as VMs existentes. O Azure Policy também avalia e monitora todas as VMs atuais do ambiente.
A implementação de uma política no Azure Policy envolve três tarefas:

1. Criar uma definição da política.
2. Atribuir a definição aos recursos.
3. Examinar os resultados da avaliação.

A Tailwind Traders deseja limitar a localização em que os recursos podem ser implantados à região **Leste dos EUA**. Ela tem dois motivos:

Melhor controle de custos Para controlar os custos, a Tailwind Traders usa assinaturas diferentes para acompanhar as implantações em cada uma das localizações regionais. A política garantirá que todos os recursos sejam implantados na região **Leste dos EUA**.

Cumprir a conformidade de segurança e residência de dados A Tailwind Traders precisa seguir uma regra de conformidade que indica o local em que os dados do cliente podem ser armazenados. Aqui, os dados do cliente precisam ser armazenados na região **Leste dos EUA**.

Exercícios

1. Como a Tailwind Traders pode permitir que alguns usuários controlem as máquinas virtuais em cada ambiente, mas impedir que eles modifiquem a rede e outros recursos no mesmo grupo de recursos ou na mesma assinatura do Azure?

- ○ Crie uma atribuição de função por meio do RBAC do Azure (controle de acesso baseado em função do Azure).

  ✔ **A resposta está correta. O RBAC do Azure permite que você crie funções que definem as permissões de acesso. Você pode criar uma função que limita o acesso somente às máquinas virtuais e uma segunda função que fornece aos administradores acesso a tudo.**

- ◉ Criar uma política no Azure Policy que audita o uso de recursos.

  ✘ **A resposta está incorreta. Embora você possa auditar como os recursos são usados, há uma forma de *impedir* os usuários de alterar os recursos que eles não devem acessar?**

- ○ Dividir o ambiente em grupos de recursos separados.

2. Qual é a melhor maneira para a Tailwind Traders garantir que a equipe implante apenas tamanhos econômicos de SKU de máquina virtual?

- ○ Criar uma política no Azure Policy que especifique os tamanhos de SKU permitidos.

  ✔ **A resposta está correta. Depois que você habilita essa política, ela é aplicada quando as máquinas virtuais são criadas ou as existentes são redimensionadas. O Azure Policy também avalia as máquinas virtuais atuais do ambiente.**

- ○ Inspecionar com frequência a implantação manualmente para ver quais tamanhos de SKU são usados.

- ◉ Criar uma função RBAC do Azure que define os tamanhos de SKU de máquina virtual permitidos.

  ✘ **A resposta está incorreta. O RBAC do Azure permite que você crie funções que definem as permissões de acesso, mas não permite que você defina tamanhos de SKU de máquina virtual permitidos.**

3. Qual é, provavelmente, a melhor maneira para a Tailwind Traders identificar a qual departamento de cobrança cada recurso do Azure pertence?

- ○ Acompanhar o uso de recursos em uma planilha.

- ○ Dividir a implantação em assinaturas separadas do Azure, em que cada assinatura pertence ao próprio departamento de cobrança.

- ◉ Aplicar uma marca a cada recurso que inclua o departamento de cobrança associado.

  ✔ **A resposta está correta. As marcas fornecem informações extras ou metadados sobre os recursos. A equipe pode criar uma marca chamada BillingDept, cujo valor é o nome do departamento de cobrança. Você poderá usar o Azure Policy para garantir que as marcas apropriadas sejam atribuídas quando os recursos forem provisionados.**

Resumo

100 XP

2 minutos

Você recebeu a tarefa de definir e implementar a estratégia de governança da Tailwind Traders.

A governança de nuvem exige uma boa coleta de requisitos e análise. A boa notícia é que o Cloud Adoption Framework para Azure pode ajudar você a definir e implementar sua estratégia de governança. Há vários serviços e recursos no Azure que dão suporte a esses esforços:

- O RBAC do Azure (controle de acesso baseado em função do Azure) permite que você crie funções que definem permissões de acesso.
- Os bloqueios de recursos impedem que os recursos sejam excluídos ou alterados acidentalmente.
- As marcas de recursos fornecem informações extras ou metadados sobre os recursos.
- O Azure Policy é um serviço do Azure que permite criar, atribuir e gerenciar políticas que controlam ou auditam os recursos.
- O Azure Blueprints permite que você defina um conjunto repetível de ferramentas de governança e de recursos padrão do Azure necessário para a sua organização.

Conheça os padrões de privacidade, conformidade e proteção de dados do Azure

Exercícios

Verificar seus conhecimentos

1. Onde a equipe pode acessar detalhes sobre os dados pessoais que a Microsoft processa e como eles são processados, incluindo os da Cortana?

- ○ Política de Privacidade da Microsoft
  - ✔ **A resposta está correta. A Política de Privacidade da Microsoft fornece informações relevantes sobre serviços específicos, incluindo a Cortana.**
- ◉ A documentação de conformidade do Azure
  - ✘ **A resposta está incorreta. A documentação de conformidade ajuda você a entender os padrões legais e regulatórios no Azure.**
- ○ Ofertas de conformidade da Microsoft

2. Onde a equipe jurídica pode acessar informações sobre como a nuvem da Microsoft ajuda a proteger dados confidenciais e a manter a conformidade as leis e os regulamentos aplicáveis?

- ○ Política de Privacidade da Microsoft
- ◉ Central de Confiabilidade
  - ✔ **A resposta está correta. A Central de Confiabilidade é um excelente recurso para as pessoas de sua organização que podem desempenhar funções de segurança, privacidade e conformidade.**
- ○ Termos de serviços online

3. Onde o departamento de TI pode encontrar blueprints de referência que podem ser aplicados diretamente às assinaturas do Azure?

- (•) Termos de serviços online
  - ✗ A resposta está incorreta. Os Termos dos Serviços Online são um contrato legal entre a Microsoft e o cliente que detalha as obrigações das duas partes em relação ao processamento e à segurança de dados do cliente e dados pessoais.
- ( ) Documentação de conformidade do Azure
  - ✓ A resposta está correta. A documentação de conformidade fornece blueprints de referência, ou definições de política, para padrões comuns que podem ser aplicados à sua assinatura do Azure.

Parte 6: descrever os contratos de nível de serviço e gerenciamento de custos do Azure

A Calculadora de TCO ajuda a estimar a economia de custos de operar sua solução no Azure ao longo do tempo em comparação com a operação no datacenter local.

Um SLA (Contrato de Nível de Serviço) é o contrato formal entre uma empresa de serviços e o cliente. No caso do Azure, esse contrato define os padrões de desempenho com os quais a Microsoft se compromete a fornecer para seus clientes.
Produtos gratuitos normalmente não têm um SLA.

Exercícios

1. Qual é o SLA para Azure Mapas em termos de tempo de atividade garantido?

- ( ) 99%
- (•) 99,9%
  - ✓ Correto. O SLA para Azure Mapas informa o SLA.
- ( ) 99,99%

2. Qual é o novo SLA composto? Lembre-se de que o novo SLA inclui uma terceira máquina virtual e o Azure Mapas.

- ( ) 99,58%
  - ✓ Correto. Para computar o SLA composto para um conjunto de serviços, você multiplica o SLA de cada serviço individual.
- ( ) 99,78%
- (•) 99,99%
  - ✗ Incorreto. O SLA composto é menor do que o SLA individual mais alto, pois adicionar complexidade aumenta levemente o risco de falha.

3. Adicionar uma terceira máquina virtual reduz o SLA composto. Como a Tailwind Traders pode compensar essa redução?

- ○ Aumentar o tamanho de cada máquina virtual.
- ◉ Implantar instâncias extras das mesmas máquinas virtuais em diferentes zonas de disponibilidade na mesma região do Azure.

  ✔ **Correto. Se uma zona de disponibilidade for afetada, a instância de máquina virtual na outra zona de disponibilidade não deverá ser afetada.**
- ○ Não fazer nada. Usar o Azure Load Balancer aumenta o SLA para máquinas virtuais.

4. Que abordagem a empresa pode adotar para adicionar a versão prévia do serviço de RA (realidade aumentada) à sua arquitetura?

- ○ O aplicativo Pedidos Especiais já está em produção. A empresa não deve considerar o serviço de RA até que ele atinja a GA (disponibilidade geral).
- ○ O aplicativo Pedidos Especiais destina-se principalmente a uso por funcionários de varejo. A empresa pode integrar o serviço de RA agora porque o tempo de inatividade ou as possíveis falhas não são um fator importante.
- ◉ A equipe de desenvolvimento pode criar uma versão de protótipo do aplicativo que inclui o serviço de RA que ela testa com os funcionários de varejo selecionados.

  ✔ **Correto. Depois que o serviço de RA atingir a GA (disponibilidade geral), a equipe poderá distribuí-lo para a produção.**