

Programa de Certificação AZ-900



Raphael Andrade

TFTEC Treinamentos Online

Introdução

O exame de certificação AZ-900, Microsoft Azure Fundamentals, foi desenvolvido para candidatos que desejam demonstrar conhecimento básico de serviços em nuvem e como esses serviços são fornecidos com Microsoft Azure.

O exame é destinado a candidatos com formação não técnica, como aqueles envolvido na venda ou compra de soluções e serviços baseados em nuvem ou que tenham algum envolvimento com soluções e serviços baseados em nuvem, bem como aqueles com formação técnica que precisam validar seu conhecimento de nível fundamental sobre serviços em nuvem. Não é necessária experiência técnica em TI no entanto, algum conhecimento ou experiência geral em TI seria benéfico.

Este exame pode ser realizado como uma primeira etapa opcional para aprender sobre os serviços em nuvem e como esses conceitos são exemplificados pelo Microsoft Azure. Pode ser considerado um precursor do Microsoft Azure ou Microsoft cloud exames de serviços. Embora seja um primeiro passo benéfico, validar o conhecimento em nível fundamental, tomar esse exame não é um pré-requisito antes de fazer outras certificações baseadas no Azure.

O exame inclui seis áreas de estudo. As porcentagens indicam o peso relativo de cada área no exame. Quanto maior a porcentagem, mais perguntas o exame conterá. Certifique-se de ler o exame página para detalhes sobre quais habilidades são abordadas em cada área.

- Módulo 01 - Descrever os conceitos do cloud (20-25%)
- Módulo 02 - Descrever os principais serviços do Azure (15-20%)
- Módulo 03 - Descrever as principais soluções e ferramentas de administração no Azure (10-15%)
- Módulo 04 - Descrever os recursos gerais de segurança e segurança de rede (10-15%)
- Módulo 05 - Descrever recursos de identidade, governança, privacidade e conformidade (20-25%)
- Módulo 06 - Descrever a administração de custos do Azure e Service Level Agreements (10-15%)

Módulo01

Computação em nuvem

Cloud computing é a prestação de serviços de computação - servidores, armazenamento, bancos de dados, rede, software, análises, inteligência e muito mais - pela Internet (nuvem), permitindo inovação mais rápida, recursos flexíveis e economias de escala. Normalmente, você paga apenas pelos serviços em nuvem que usa, ajudando a diminuir seus custos operacionais, execute sua infraestrutura com mais eficiência e dimensione conforme as necessidades da sua empresa mudam.

A empresa que fornece esses serviços é chamada de provedor de nuvem. Alguns exemplos de provedores são Microsoft Azure, Amazon Web Services (AWS) e Google Cloud Platform (GCP). O provedor de nuvem é responsável pelo hardware físico necessário para executar seu trabalho e por mantê-lo atualizado.

Cada empresa é única e tem necessidades diferentes. Para atender a essas necessidades, os provedores de computação em nuvem oferecem uma ampla gama de serviços. Normalmente, esses serviços incluem:

Poder Computacional - como servidores Linux ou aplicativos da web.

Armazenamento - como arquivos e bancos de dados.

Rede - como conexões seguras entre o provedor de nuvem e sua empresa.

Analytics - como visualizar dados de telemetria e desempenho.

Conceitos chave

Os serviços em nuvem são uma grande mudança da maneira tradicional como as empresas pensam sobre os recursos de TI. Serviços na nuvem possuem características e considerações, algumas das quais são descritas e explicadas abaixo:

Alta disponibilidade (High availability): A capacidade de manter os serviços em operação por longos períodos, com muito pouco tempo de inatividade, dependendo do serviço em questão.

Escalabilidade (Scalability): A capacidade de aumentar ou diminuir recursos para qualquer carga de trabalho. Você pode adicionar mais recursos para atender uma carga de trabalho (conhecida como expansão) ou adicionar recursos adicionais para gerenciar um aumento na demanda pelo recurso existente (conhecido como ampliação). A escalabilidade não precisa ser feita automaticamente.

Elasticidade (Elasticity): A capacidade de aumentar ou diminuir automática ou dinamicamente os recursos, conforme necessário. Elástico os recursos correspondem às necessidades atuais e os recursos são adicionados ou removidos automaticamente para atender a futuras precisa quando é necessário e da localização geográfica mais vantajosa. Uma distinção entre escalabilidade e elasticidade é que a elasticidade é feita automaticamente.

Agilidade (Agility): A capacidade de reagir rapidamente. Os serviços em nuvem podem alocar e desalocar recursos rapidamente. Eles são fornecidos sob demanda via autoatendimento, para que grandes quantidades de recursos de computação possam ser provisionadas em minutos. Não há intervenção manual no provisionamento ou desprovisionamento de serviços.

Tolerância a falhas (Fault tolerance): A capacidade de permanecer em funcionamento, mesmo no caso de um componente ou serviço que não mais tempo de funcionamento. Normalmente, a redundância é incorporada à arquitetura de serviços em nuvem, portanto, se um componente falhar, um componente de backup toma seu lugar. Diz-se que o tipo de serviço é tolerante a falhas.

Recuperação de desastres (Disaster recovery): A capacidade de se recuperar de um evento que desativou um serviço de nuvem. Nuvem a recuperação de desastre de serviços pode acontecer muito rapidamente, com automação e serviços disponíveis usar.

Alcance global (Global reach): A capacidade de atingir públicos-alvo em todo o mundo. Os serviços em nuvem podem ter presença em várias regiões do mundo que você pode acessar, oferecendo

Segurança (Security): Os provedores de nuvem oferecem um amplo conjunto de políticas, tecnologias, controles e tecnologia especializada habilidades que podem fornecer melhor segurança do que a maioria das organizações pode alcançar. O resultado é segurança reforçada, que ajuda a proteger dados, aplicativos e infraestrutura contra ameaças em potencial.

Economias de escala (economies of scale)

O conceito de economia de escala é a capacidade de reduzir custos e obter eficiência ao operar em uma escala maior em comparação com a operação em escala menor.

Os provedores de nuvem são empresas muito grandes e podem aproveitar os benefícios de economias de escala, e depois repassar esses benefícios aos seus clientes.

Isso é aparente para os usuários finais de várias maneiras, uma das quais é a capacidade de adquirir hardware em um custo mais baixo do que se um único usuário ou empresa menor estivesse comprando.



Os custos de armazenamento, por exemplo, diminuíram significativamente na última década devido, em parte, aos fornecedores de nuvem capacidade de comprar grandes quantidades de armazenamento com descontos significativos. Eles então podem usar esse armazenamento com mais eficiência e repassar esses benefícios aos usuários finais na forma de preços mais baixos.

✓ Existem limites para os benefícios que as grandes organizações podem obter por meio de economias de escala. Um produto inevitavelmente terá um custo básico subjacente, pois se torna mais uma mercadoria, com base no que custa para produzir. A concorrência também é outro fator que afeta os custos dos serviços em nuvem.

CapEx vs OpEx

Nos anos anteriores, as empresas iniciantes precisavam adquirir instalações físicas e infraestrutura para começar seus negócios e começar a negociar. Foram necessárias grandes quantias para criar um negócio e executando ou para expandir uma empresa existente.

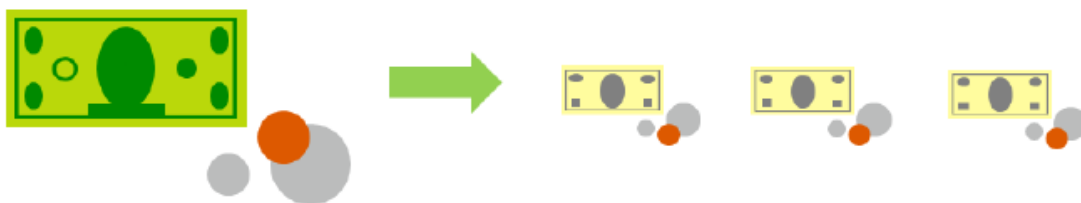
Eles teriam que comprar novos datacenters ou novos servidores para permitir que eles criem serviços, que eles poderiam oferecer aos seus clientes. Isso não é mais o caso.

Hoje, as organizações podem se inscrever para um serviço de um provedor de nuvem para começar a funcionar. Isso permite começar a vender ou prestar serviços a seus clientes mais rapidamente, sem a necessidade de Custos antecipados.

Essas duas abordagens ao investimento são conhecidas como:

Despesa de capital (Capital Expenditure) - (CapEx): é o gasto de dinheiro em infraestrutura física antecipadamente, e deduzindo essa despesa da sua conta fiscal ao longo do tempo. CapEx é um custo inicial que tem um valor isso reduz com o tempo.

Despesas operacionais (Operational Expenditure) - (OpEx): gastam dinheiro em serviços ou produtos agora e estão sendo cobrado por eles agora. Você pode deduzir essa despesa da sua conta de imposto no mesmo ano. Não há up custo inicial, você paga por um serviço ou produto ao usá-lo.



As empresas que desejam iniciar um novo negócio ou aumentar seus negócios não precisam incorrer em custos iniciais para experimente um novo produto ou serviço para os clientes. Em vez disso, eles podem entrar no mercado imediatamente e pagar tanto ou tão pouco para a infraestrutura quanto os negócios exigirem. Eles também podem rescindir esse custo se e quando eles precisam.

Se seu serviço estiver ocupado e você consumir muitos recursos em um mês, receberá uma fatura grande. E se esses serviços forem mínimos e não usarem muitos recursos, você receberá uma fatura menor.

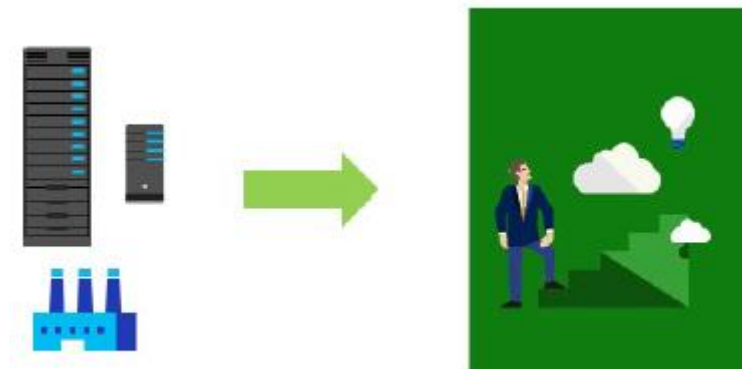
Uma empresa ainda pode usar a estratégia de despesas de CapEx, se desejar, mas não é mais um requisito que eles fazem isso.

Modelo baseado no consumo (consumption-based model)

Os provedores de serviços em nuvem operam em um modelo baseado no consumo, o que significa que os usuários finais pagam apenas pelos recursos que eles usam. Tudo o que eles usam é o que pagam.

Esse modelo baseado em consumo traz muitos benefícios, incluindo:

- Sem custos iniciais.
- Não há necessidade de comprar e gerenciar infraestrutura dispendiosa que eles possam ou não usar ao máximo.
- A capacidade de pagar por recursos adicionais quando necessários.
- A capacidade de parar de pagar por recursos que não são mais necessários.



Tipos de modelos de nuvem

Nuvem pública (Public Cloud)

Uma nuvem pública é de propriedade do provedor de serviços em nuvem (também conhecido como provedor de hospedagem). Fornece recursos e serviços para várias organizações e usuários, que se conectam ao serviço de nuvem por meio de um servidor seguro conexão de rede, geralmente pela Internet.



Os modelos de nuvem pública têm as seguintes características:

Propriedade. Esses são os recursos que uma organização ou usuário final usa. Exemplos incluem armazenamento e Poder de processamento. Os recursos não pertencem à organização que os está utilizando, mas eles pertencem e são operados por terceiros, como o provedor de serviços em nuvem.

Vários usuários finais. Os modos de nuvem pública podem disponibilizar seus recursos para várias organizações.

Acesso público: Isso fornece acesso ao público.

Disponibilidade: Este é o modelo de implantação do tipo nuvem mais comum.

Conectividade: Usuários e organizações geralmente estão conectados à nuvem pública pela Internet usando um navegador da web.

Habilidades: As nuvens públicas não requerem conhecimento técnico profundo para configurar e usar seus recursos.

Com uma nuvem pública, não há hardware local para gerenciar ou manter atualizado; tudo corre no hardware do provedor de nuvem. Em alguns casos, os usuários da nuvem podem economizar custos adicionais compartilhando a computação recursos com outros usuários da nuvem.

Um cenário de caso de uso comum é implantar um aplicativo Web ou um site de blog em hardware e recursos de propriedade de um provedor de nuvem. O uso de uma nuvem pública nesse cenário permite que os usuários da nuvem obtenham suas site ou blog rapidamente, e concentre-se em manter o site sem ter que se preocupar com compra, gerenciamento ou manutenção do hardware no qual é executado.

As empresas podem usar várias empresas prestadoras de serviços de nuvem pública em escala variável. Microsoft Azure é um exemplo de um provedor de nuvem pública.

Nuvem Privada (Private Cloud)

Uma nuvem privada pertence e é operada pela organização que usa os recursos dessa nuvem. Eles criar um ambiente de nuvem em seu próprio datacenter e fornecer acesso de autoatendimento para calcular recursos para usuários dentro de sua organização.

A organização continua sendo o proprietário, inteiramente responsável pela operação dos serviços que prestam.

Os modelos de nuvem privada têm as seguintes características:

Propriedade: O proprietário e o usuário dos serviços em nuvem são os mesmos.

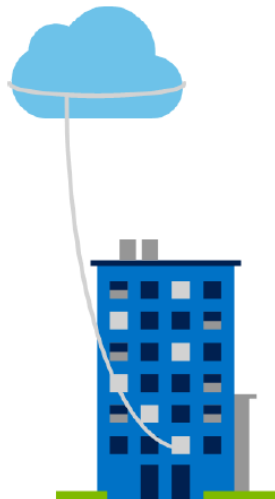
Hardware: O proprietário é inteiramente responsável pela compra, manutenção e gerenciamento do hardware em nuvem.

Usuários: Uma nuvem privada opera apenas dentro de uma organização e os recursos de computação em nuvem são usados exclusivamente por uma única empresa ou organização.

Conectividade: Uma conexão com uma nuvem privada geralmente é feita através de uma rede privada altamente seguro.

Acesso público: Não fornece acesso ao público.

habilidades. Requer profundo conhecimento técnico para configurar, gerenciar e manter.



Um cenário de caso de uso para uma nuvem privada seria quando uma organização tivesse dados que não podem ser colocados no diretório nuvem pública, talvez por razões legais. Por exemplo, eles podem ter dados médicos que não podem ser expostos publicamente.

Outro cenário pode ser onde a política do governo exija que dados específicos sejam mantidos no país ou em particular.

Uma nuvem privada também pode fornecer funcionalidade de nuvem para clientes externos ou para clientes internos específicos ou para departamentos como Contabilidade ou Recursos Humanos.

Nuvem híbrida (Hybrid Cloud)

Uma nuvem híbrida combina nuvens públicas e privadas, permitindo que você execute seus aplicativos no local mais apropriado.

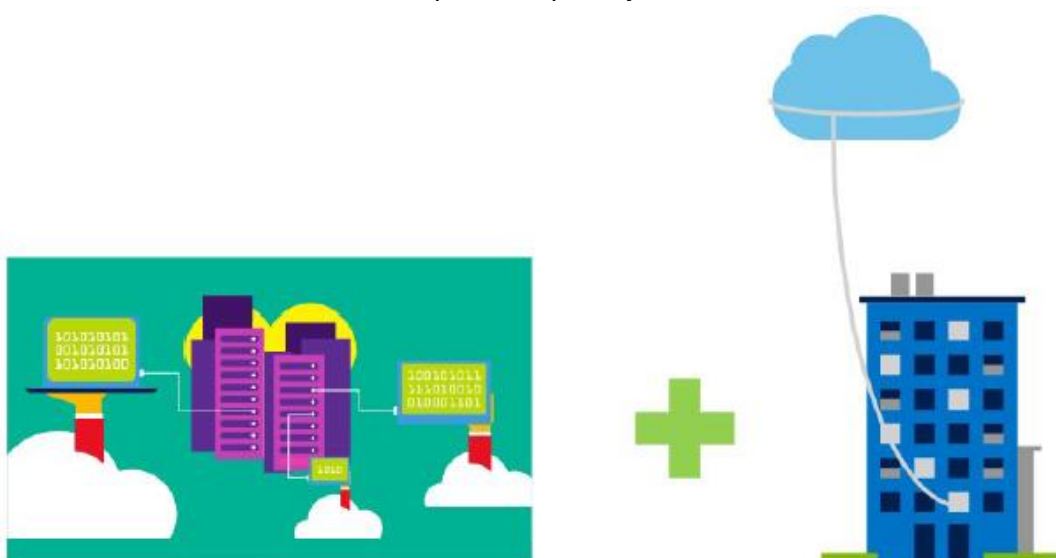
Os modelos de nuvem híbrida têm as seguintes características:

Localização do recurso: Recursos específicos são executados ou são usados em uma nuvem pública e outros são executados ou são usados em uma nuvem privada.

Custo e eficiência: Modelos de nuvem híbrida permitem que uma organização aproveite alguns dos benefícios de custo, eficiência e escala disponíveis com um modelo de nuvem pública.

Controle: As organizações mantêm o controle de gerenciamento em nuvens privadas.

Habilidades: Ainda são necessárias habilidades técnicas para manter a nuvem privada e garantir os dois modelos de nuvem podem operar juntos.



Um exemplo de cenário de uso de nuvem híbrida seria hospedar um site na nuvem pública e vincular para um banco de dados altamente seguro hospedado em uma nuvem privada.

Os cenários de nuvem híbrida podem ser úteis quando as organizações têm algumas coisas que não podem ser colocadas em público nuvem, possivelmente por razões

legais. Por exemplo, você pode ter dados médicos que não podem ser expostos publicamente.

Outro exemplo é um ou mais aplicativos executados em hardware antigo que não podem ser atualizados. Nesse caso, você pode manter o sistema antigo em execução localmente em sua nuvem privada e conectá-lo à nuvem pública para autorização ou armazenamento.

Comparações dos modelos de nuvem

Abaixo está um resumo de algumas das vantagens e desvantagens de nuvens públicas, privadas e híbridas.

Nuvem pública

Vantagens:

Nenhum CapEx: Você não precisa comprar um novo servidor para poder escalar.

Agilidade. Os aplicativos podem ser acessados rapidamente e desprovisionados sempre que necessário.

Modelo baseado no consumo: As organizações pagam apenas pelo que usam e operam sob uma Modelo OpEx.

Manutenção: As organizações não têm responsabilidade pela manutenção ou atualizações de hardware.

Habilidades: Não são necessárias habilidades técnicas profundas para implantar, usar e obter os benefícios de uma nuvem pública.

As organizações podem aproveitar as habilidades e conhecimentos do provedor de nuvem para garantir que as cargas de trabalho sejam seguras e altamente disponíveis.

Desvantagens:

Segurança: Pode haver requisitos de segurança específicos que não podem ser atendidos usando a nuvem pública.

Conformidade: Pode haver políticas governamentais, padrões do setor ou requisitos legais que nuvens públicas não podem se encontrar.

Propriedade: As organizações não possuem o hardware ou serviços e não podem gerenciá-los, pois pode desejar.

Cenários específicos: Se as organizações tiverem um requisito comercial exclusivo, como precisar para manter um aplicativo herdado, pode ser difícil atender a esse requisito com serviços de nuvem pública.

Nuvem privada

Vantagens:

Controle: As organizações têm controle completo sobre os recursos.

Segurança: As organizações têm controle total sobre a segurança.

Conformidade: Se as organizações tiverem requisitos de segurança, conformidade ou legais muito rígidos, uma empresa privada nuvem pode ser a única opção viável.

Cenários específicos: Se uma organização tiver um cenário específico que não seja facilmente suportado por um público provedor de nuvem (como precisar manter um aplicativo herdado), talvez seja preferível executar a aplicação localmente.

Desvantagens:

CapEx inicial: O hardware deve ser adquirido para inicialização e manutenção.

Agilidade: Nuvens privadas não são tão ágeis quanto nuvens públicas, porque você precisa comprar e configurar toda a infraestrutura subjacente antes que possam ser aproveitadas.

Manutenção: As organizações têm a responsabilidade pela manutenção e atualizações de hardware.

Habilidades: As nuvens privadas exigem habilidades e conhecimentos internos de TI que podem ser difíceis de obter ou custar caro.

Nuvem híbrida

Vantagens:

Flexibilidade: O cenário mais flexível: com uma configuração de nuvem híbrida, uma organização pode decidir executar seus aplicativos em uma nuvem privada ou em uma nuvem pública.

Custos: As organizações podem tirar proveito das economias de escala dos fornecedores de nuvem pública para serviços e recursos como desejarem. Isso permite que eles acessem um armazenamento mais barato do que podem fornecer a si mesmos.

Controle: As organizações ainda podem acessar recursos sobre os quais têm controle total.

Segurança: As organizações ainda podem acessar recursos pelos quais são responsáveis pela segurança.

Conformidade: As organizações mantêm a capacidade de cumprir rígidas normas de segurança, conformidade ou requisitos legais conforme necessário.

Cenários específicos: As organizações mantêm a capacidade de suportar cenários específicos não facilmente suportado por um provedor de nuvem pública, como a execução de aplicativos herdados. Nesse caso, eles podem manter o sistema antigo em execução localmente e conecte-o à nuvem pública para autorização ou

armazenamento. Além disso, eles podem hospedar um site na nuvem pública e vinculá-lo a um site altamente seguro com banco de dados hospedado em sua nuvem privada.

Desvantagens:

CapEx inicial: O CapEx inicial ainda é necessário antes que as organizações possam aproveitar uma nuvem privada.

Custos: Comprar e manter uma nuvem privada para uso junto à nuvem pública pode ser mais

mais caro do que selecionar um único modelo de implantação.

Habilidades: Ainda são necessárias habilidades técnicas profundas para poder configurar uma nuvem privada.

Facilidade de gerenciamento. As organizações precisam garantir que haja diretrizes claras para evitar confusão, complicações ou mau uso.

Tipos de serviços em nuvem

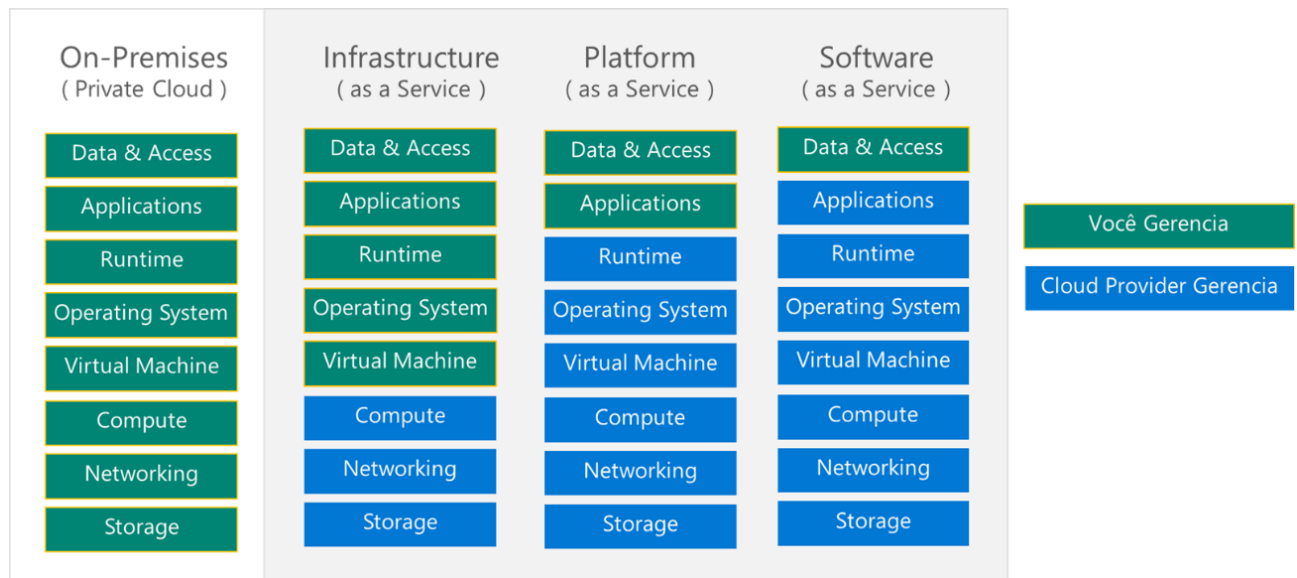
Modelo de responsabilidade compartilhada

A importância de entender o modelo de responsabilidade compartilhada é essencial para os clientes que estão movendo-se para a nuvem. Os provedores de nuvem oferecem vantagens consideráveis para os esforços de segurança e conformidade, mas essas vantagens não impedem o cliente de proteger seus usuários, aplicativos e serviços ofertados.

O modelo de responsabilidade compartilhada garante que as cargas de trabalho na nuvem sejam executadas com segurança e de maneira bem gerenciada.

Dependendo do serviço que você está usando, o provedor de nuvem é responsável por alguns aspectos do gerenciamento de carga de trabalho e o cliente ou usuário final é responsável por outros aspectos da carga de trabalho gestão e, em alguns casos, ambos compartilham uma responsabilidade.

A lista a seguir de tipos de serviço em nuvem descreve as responsabilidades de gerenciamento para o usuário e os provedores de nuvem em comparação com os sistemas locais:



O **IaaS** requer o maior gerenciamento de usuários de todos os serviços em nuvem. O usuário é responsável por gerenciar os sistemas operacionais, dados e aplicativos.

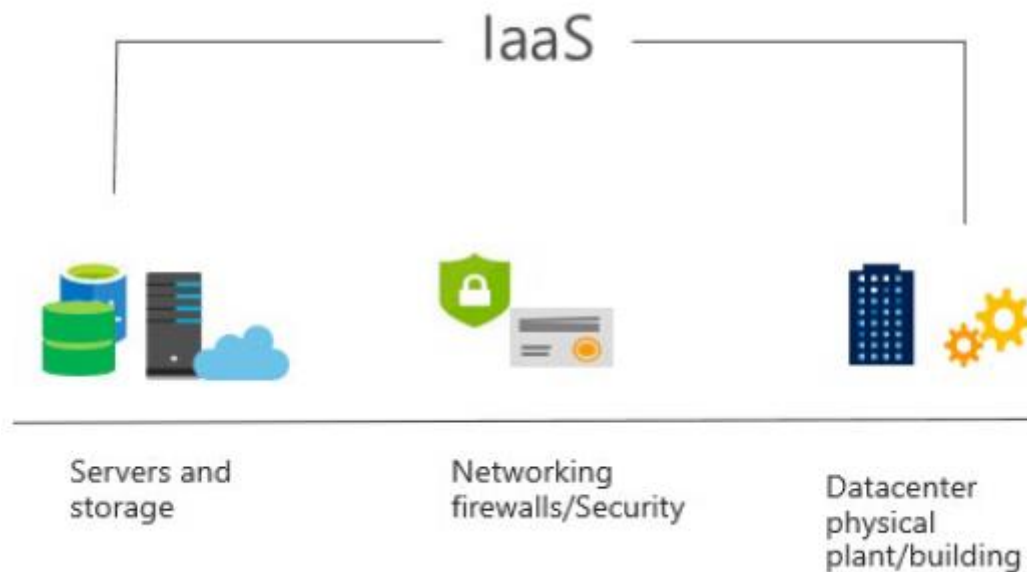
O **PaaS** requer menos gerenciamento de usuários. O provedor de nuvem gerencia os sistemas operacionais e o usuário é responsável pelos aplicativos e dados que executam e armazenam.

O **SaaS** requer o mínimo de gerenciamento. O provedor de nuvem é responsável por gerenciar tudo, e o usuário final apenas usa o software.

✓ É importante que os usuários da nuvem entendam pelo que são responsáveis, para garantir suas cargas de trabalho são gerenciados corretamente e não sofrem nenhum tempo de inatividade.

IaaS

O IaaS é a categoria mais básica de serviços de computação em nuvem. Com o IaaS, você aluga servidores de infraestrutura de TI e máquinas virtuais (VMs), armazenamento, redes e sistemas operacionais de um provedor de nuvem em um pagamento conforme o uso. É uma infraestrutura de computação instantânea, provisionada e gerenciada pela Internet.



Características

Custos iniciais: O IaaS não tem custos iniciais. Os usuários pagam apenas pelo que consomem.

Propriedade do usuário: O usuário é responsável pela compra, instalação, configuração e gerenciamento de seus próprios sistemas operacionais de software, middleware e aplicativos.

Propriedade do provedor de nuvem: O provedor de nuvem é responsável por garantir que a nuvem subjacente infraestrutura (como máquinas virtuais, armazenamento e rede) está disponível para o usuário.

Cenários de uso comum

Migrando cargas de trabalho: Normalmente, as instalações de IaaS são gerenciadas de maneira semelhante à infraestrutura local e forneça um caminho de migração fácil para mover aplicativos existentes para a nuvem.

Teste e desenvolvimento: As equipes podem configurar e desmontar rapidamente ambientes de teste e desenvolvimento, trazendo novos aplicativos para o mercado mais rapidamente. O IaaS aumenta a escala dos ambientes de teste de desenvolvimento e para baixo rápido e econômico.

Hospedagem de sites: A execução de sites usando IaaS pode ser mais barata que a hospedagem na web tradicional.

Armazenamento, backup e recuperação: As organizações evitam os gastos de capital e a complexidade do armazenamento gerenciamento, que normalmente exige uma equipe qualificada para gerenciar dados e atender às exigências legais e de conformidade requisitos.

O IaaS é útil para gerenciar a demanda imprevisível e as crescentes necessidades de armazenamento.

Também pode simplificar o planejamento e o gerenciamento de sistemas de backup e recuperação.

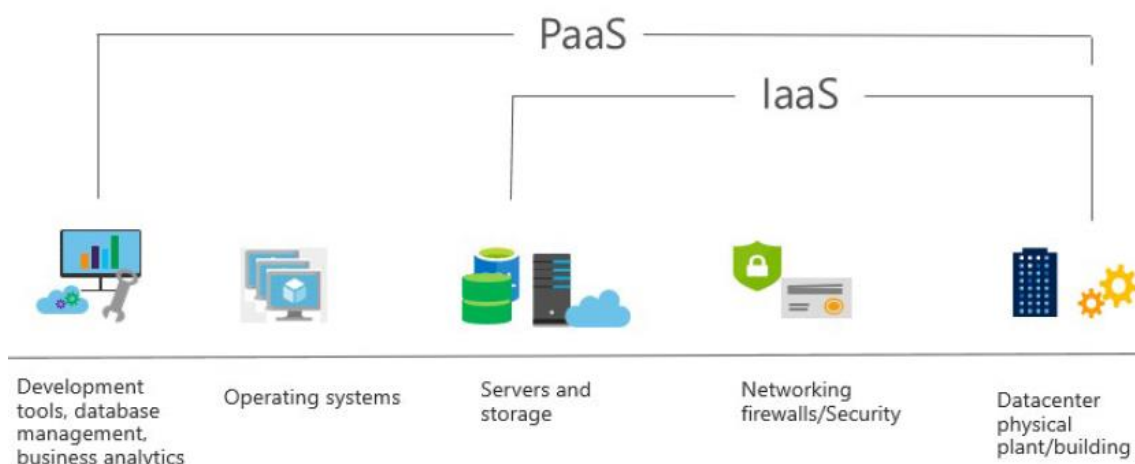
✓ Ao usar o IaaS, garantir que um serviço esteja em funcionamento é uma responsabilidade compartilhada: a nuvem o provedor é responsável por garantir que a infraestrutura da nuvem esteja funcionando corretamente; o cliente da nuvem é responsável por garantir que o serviço que eles estão usando esteja configurado corretamente, atualizado e disponível para seus clientes.

PaaS

O PaaS fornece um ambiente para criar, testar e implantar aplicativos de software. O objetivo do PaaS é ajudar a criar um aplicativo o mais rápido possível, sem precisar se preocupar em gerenciar a infraestrutura subjacente.

Por exemplo, ao implantar um aplicativo Web usando PaaS, você não precisa instalar um sistema operacional, servidor web ou mesmo atualizações do sistema. PaaS é um desenvolvimento completo e ambiente de implantação na nuvem, com recursos que permitem às organizações fornecer tudo de aplicativos simples baseados em nuvem a sofisticados aplicativos empresariais habilitados para nuvem.

Os recursos são adquiridos de um provedor de serviços em nuvem com base no pagamento conforme o uso e acessados por uma conexão segura à Internet.



Características de PaaS

Custos iniciais. Não há custos iniciais, e os usuários pagam apenas pelo que consomem. Propriedade do usuário. O usuário é responsável pelo desenvolvimento de seus próprios aplicativos. Contudo, eles não são responsáveis por gerenciar o servidor ou a infraestrutura. Isso permite que o usuário se concentre no aplicativo ou carga de trabalho que eles desejam executar.

Propriedade do provedor de nuvem. O provedor de nuvem é responsável pelo gerenciamento do sistema operacional e configuração de rede e serviço. Os provedores de nuvem geralmente são responsáveis por tudo, além de o aplicativo que um usuário deseja executar. Eles fornecem uma plataforma gerenciada completa na qual executar uma aplicação.

Cenários de uso comum

Estrutura de desenvolvimento: O PaaS fornece uma estrutura que os desenvolvedores podem desenvolver para desenvolver ou personalizar aplicativos baseados em nuvem. Semelhante à maneira como você cria uma macro do Microsoft Excel, o PaaS permite desenvolvedores criam aplicativos usando componentes de software internos.

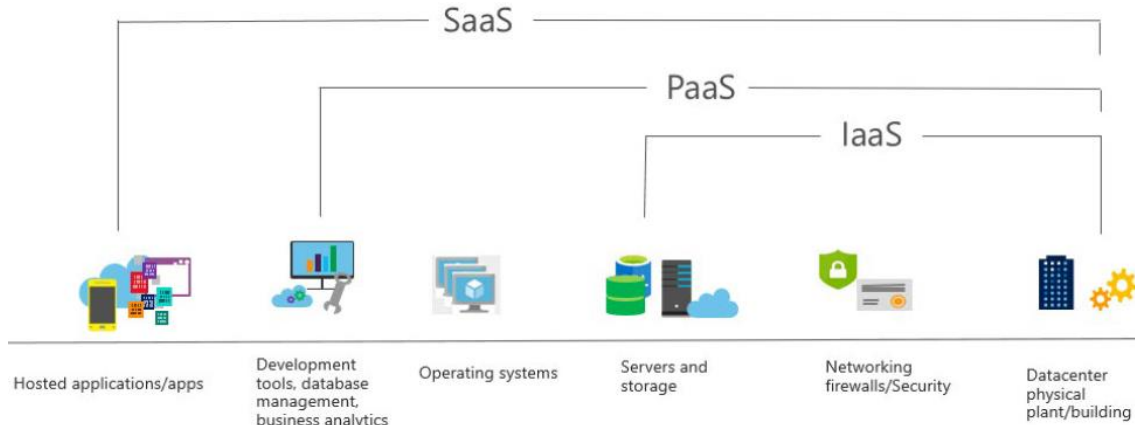
Recursos da nuvem, como escalabilidade, disponibilidade de alta disponibilidade e capacidade de vários locatários, reduzindo a quantidade de codificação que desenvolvedores devem fazer.

Análise ou inteligência comercial: As ferramentas fornecidas como um serviço com PaaS permitem que as organizações a analisar e extrair seus dados. Eles podem encontrar ideias e padrões e prever resultados para melhorar decisões de negócios, como previsão, design de produto e retorno do investimento.

SaaS

O SaaS é um software que é hospedado e gerenciado centralmente para o cliente final. Permite que os usuários se conectem a e use aplicativos baseados na nuvem pela Internet. Exemplos comuns são e-mail, calendários e ferramentas de escritório como o Microsoft Office 365.

O SaaS normalmente é licenciado por meio de uma assinatura mensal ou anual e o Office 365 é um exemplo de SaaS Programas.



Características SaaS

Custos iniciais. Os usuários não têm custos iniciais; eles pagam uma assinatura, geralmente mensalmente ou anualmente base.

Propriedade do usuário. Os usuários apenas usam o software do aplicativo; eles não são responsáveis por qualquer manutenção ou gerenciamento desse software.

Propriedade do provedor de nuvem. O provedor de nuvem é responsável pelo fornecimento, gerenciamento e manutenção do software aplicativo.

Cenários de uso comum

Exemplos de serviços Microsoft SaaS incluem Office 365, Skype e Microsoft Dynamics CRM Online.

Comparação de serviços em nuvem

Existem vantagens e desvantagens para os serviços em nuvem IaaS, PaaS e SaaS.

IaaS

O IaaS é a categoria mais flexível de serviços em nuvem. Seu objetivo é fornecer controle total sobre o hardware que executa seu aplicativo. Em vez de comprar hardware, com o IaaS, você o aluga.

Vantagens:

Nenhum CapEx: Os usuários não têm custos iniciais.

Agilidade: Os aplicativos podem ser acessados rapidamente e desprovisionados sempre que necessário.

Modelo baseado no consumo: As organizações pagam apenas pelo que usam e operam sob um Modelo OpEx.

Habilidades: Não são necessárias habilidades técnicas profundas para implantar, usar e obter os benefícios de uma nuvem pública.

As organizações podem aproveitar as habilidades e conhecimentos do provedor de nuvem para garantir que as cargas de trabalho sejam seguras e altamente disponíveis.

Benefícios da nuvem: As organizações podem aproveitar as habilidades e conhecimentos do provedor de nuvem para garantir as cargas de trabalho são tornadas seguras e altamente disponíveis.

Flexibilidade: o IaaS é o serviço em nuvem mais flexível, pois você tem controle para configurar e gerenciar o hardware executando seu aplicativo.

Desvantagens:

Gerenciamento: O modelo de responsabilidade compartilhada se aplica; o usuário gerencia e mantém os serviços que eles provisionaram e o provedor de nuvem gerencia e mantém a infraestrutura de nuvem.

PaaS

O PaaS oferece os mesmos benefícios e considerações que o IaaS, mas existem alguns benefícios adicionais.

Vantagens:

Nenhum CapEx: Os usuários não têm custos iniciais.

Agilidade: O PaaS é mais ágil que o IaaS e os usuários não precisam configurar servidores para executar formulários.

Modelo baseado no consumo: Os usuários pagam apenas pelo que usam e operam em um modelo OpEx.

Habilidades: Não são necessárias habilidades técnicas profundas para implantar, usar e obter os benefícios do PaaS.

Benefícios da nuvem: Os usuários podem aproveitar as habilidades e conhecimentos do provedor de nuvem para garantir suas cargas de trabalho são tornadas seguras e altamente disponíveis. Além disso, os usuários podem obter acesso a mais ferramentas e conjuntos de ferramentas de desenvolvimento de ponta. Eles podem aplicar essas ferramentas e conjuntos de ferramentas ao ciclo de vida de um aplicativo.

Produtividade: Os usuários podem se concentrar apenas no desenvolvimento de aplicativos, pois todo o gerenciamento da plataforma é tratado pelo provedor de nuvem. Trabalhar com equipes distribuídas como serviços é mais fácil, pois a plataforma é acessada pela Internet e pode ser disponibilizada globalmente mais facilmente.

Desvantagens:

Limitações da plataforma: Pode haver algumas limitações em uma plataforma em nuvem que podem afetar como um aplicativo é executado. Quaisquer limitações devem ser levadas em consideração ao considerar qual PaaS plataforma é mais adequada para uma carga de trabalho.

SaaS

O SaaS é um software que é hospedado e gerenciado centralmente para o cliente final. Geralmente é baseado em uma arquitetura em que uma versão do aplicativo é usada por todos os clientes e licenciada por meio de uma assinatura mensal ou anual

O SaaS oferece os mesmos benefícios que o IaaS, mas novamente existem alguns benefícios adicionais.

Vantagens:

Nenhum CapEx: Os usuários não têm custos iniciais.

Agilidade: Os usuários podem fornecer à equipe acesso ao software mais recente de maneira rápida e fácil.

Modelo de precificação de acordo com o uso: os usuários pagam pelo software que usam em um modelo de assinatura, geralmente mensalmente ou anualmente, independentemente de quanto eles usam o software.

Flexibilidade: Os usuários podem acessar os mesmos dados do aplicativo de qualquer lugar.

Desvantagens:

Limitações do software: Pode haver algumas limitações em um aplicativo de software que podem afetar como os usuários trabalham. Quaisquer limitações devem ser levadas em consideração ao considerar qual PaaS plataforma é mais adequada para uma carga de trabalho.

✓ IaaS, PaaS e SaaS contêm níveis diferentes de serviços gerenciados. Você pode facilmente usar uma combinação desses tipos de infraestrutura. Você pode usar o Office 365 nos computadores da sua empresa (SaaS) e no Azure, você pode hospedar suas VMs (IaaS) e usar o Banco de Dados SQL do Azure (PaaS) para armazenar seus dados.

Com a flexibilidade da nuvem, você pode usar qualquer combinação que forneça o resultado máximo.

Revisão – Questões Módulo 01

Review Question 1

Which of the following describes a benefit of cloud services?

- A. Economies of scale
- B. Fixed workloads
- C. Unpredictable costs

Review Question 2

Which of the following refers to spending money upfront and then deducting that expense over time?

- A. Capital expenditure
- B. Operational expenditures
- C. Supply and demand

Review Question 3

Which of the following refers to making a service available with no downtime for an extended period of time?

- A. Agility
- B. Fault tolerance
- C. High availability
- D. Performance

Review Question 4

Microsoft Office 365 is an example of?

- A. Infrastructure as a Service
- B. Platform as a Service
- C. Software as a Service

Review Question 5

Which cloud model provides the greatest degree of ownership and control?

- A. Hybrid
- B. Private
- C. Public

Review Question 6

Which cloud model provides the greatest degree of flexibility?

- A. Public
- B. Private
- C. Hybrid

Review Question 7

Which of the following describes a public cloud?

- A. Is owned and operated by the organization that uses the resources from that cloud.
- B. Lets organizations run applications in the cloud or on-premises.
- C. Provides resources and services to multiple organizations and users, who connect through a secure network connection.

Review Question 8

Which of the following describes Platform as a Service (PaaS)?

- A. Users are responsible for purchasing, installing, configuring, and managing their own software—operating systems, middleware, and applications.
- B. Users create and deploy applications quickly without having to worry about managing the underlying infrastructure.
- C. Users pay an annual or monthly subscription.

Review Question 9

You have legacy applications that require specialized mainframe hardware and you have newer shared applications. Which cloud deployment model would be best for you?

- A. Public cloud
- B. Private cloud
- C. Hybrid cloud

Review Question 10

Which of the following requires the most user management of the cloud services?

- A. Infrastructure as a Service
- B. Platform as a Service
- C. Software as a Service

Resumo do Módulo 1

Neste módulo, você aprendeu sobre a computação em nuvem, o que é e quais são suas principais características. Você aprendeu sobre os diferentes tipos de modelos de nuvem disponíveis e as considerações sobre o uso desses diferentes modelos. Você também aprendeu sobre os diferentes serviços em nuvem disponíveis, os benefícios de usando os diferentes tipos e as responsabilidades de gerenciamento em cada tipo de serviço.

Por que serviços em nuvem?

Você aprendeu sobre o que é computação em nuvem e por que você deve considerar o uso de serviços de nuvem.

Você aprendeu quais são alguns dos principais termos e conceitos, como **alta disponibilidade, agilidade, elasticidade, tolerância a falhas, alcance global, CapEx versus OpEX** no contexto da computação em nuvem, economia de escala e o modelo de custo baseado no consumo.

Tipos de modelos de nuvem

Você aprendeu sobre os modelos de nuvem pública, nuvem privada e nuvem híbrida e quais os são as principais características de cada modelo. Você também aprendeu como eles se comparam, quais considerações você precisa levar em consideração ao usá-los e quando você pode usá-los.

Tipos de serviços em nuvem

Você aprendeu sobre os diferentes tipos de serviço em nuvem disponíveis, **IaaS, PaaS e SaaS**.

Você aprendeu quais são as principais características de cada serviço, como elas se comparam, que considerações você precisa levar em consideração ao usá-los e quando poderá usá-los.

Respostas da revisão

Questão 01: Economies of scale

Explicação: Economias de escala. Economias de escala é a capacidade de fazer as coisas de maneira mais barata e eficiente quando operando em uma escala maior em comparação com operando em uma escala menor.

Questão 02: Capital expenditure

Explicação: Despesas de capital. O gasto de capital refere-se ao gasto de dinheiro em infraestrutura física antecipadamente, e deduzindo essa despesa da sua conta de imposto ao longo do tempo.

Questão 03: High availability

Explicação: Alta disponibilidade. A alta disponibilidade mantém os serviços em funcionamento por muitos períodos, com muito pouco tempo de inatividade, dependendo do serviço questão.

Questão 04: Software as a Service

Explicação: Software como serviço. O SaaS normalmente é licenciado por meio de uma assinatura mensal ou anual.

Questão 05: Private

Explicação: Privado. A nuvem privada fornece o maior grau de propriedade e controle.

Questão 06: Hybrid

Explicação: Híbrido. O modelo de nuvem híbrida oferece o maior grau de flexibilidade, pois você tem a opção de escolher público ou privado, dependendo de suas necessidades.

Questão 07: Provides resources and services to multiple organizations and users, who connect through a secure network connection.

Explicação: A nuvem pública fornece recursos e serviços para várias organizações e usuários que se conectam por meio de uma conexão de rede segura.

Questão 08: Users create and deploy applications quickly without having to worry about managing the underlying infrastructure.

Explicação: O PaaS permite que os usuários criem e implantem aplicativos rapidamente, sem precisar se preocupar em gerenciar a infra-estrutura subjacente.

Questão 09: Hybrid cloud

Explicação: Nuvem híbrida. Uma nuvem híbrida é uma nuvem pública e privada combinada. Você pode executar seus aplicativos mais recentes em hardware comum que você aluga da nuvem pública e mantém seu hardware especializado em mainframe no local.

Questão 10: Infrastructure as a Service

Explicação: Infraestrutura como um serviço. A infra-estrutura como um serviço requer o gerenciamento mais dos serviços em nuvem.

Módulo 02

Arquitetura dos principais componentes do Azure

Regiões

O Microsoft Azure é composto de datacenters localizados em todo o mundo. Esses datacenters são organizados e disponibilizados aos usuários finais por regiões. Uma região é uma área geográfica do planeta que contém pelo menos um, mas potencialmente vários datacenters que estão próximos e conectados em rede com um link de baixa latência.

Alguns exemplos de regiões são Oeste dos EUA, Canadá Central, Europa Ocidental, Austrália Oriental e Japão Ocidental. Até no momento o Azure está disponível em 60 regiões e em 140 países.



O que você deve saber sobre regiões

- O Azure tem mais regiões globais do que qualquer outro provedor de nuvem.
- As regiões fornecem aos clientes a flexibilidade e a escala necessárias para aproximar os aplicativos de seus usuários.
- As regiões preservam a residência de dados e oferecem opções abrangentes de conformidade e resiliência para clientes.
- Para a maioria dos serviços do Azure, quando você implanta um recurso, escolhe a região em que deseja seu recurso a ser implantado.
- Alguns serviços ou recursos da máquina virtual estão disponíveis apenas em determinadas regiões, como locais específicos, tamanhos de máquina ou tipos de armazenamento.

- Existem também alguns serviços globais do Azure que não exigem a seleção de uma região, como a Microsoft Azure Active Directory, Traffic Manager do Microsoft Azure ou DNS do Azure.

Region Pairs

Cada região do Azure está emparelhada com outra região na mesma geografia, formando um region pair. A exceção é o sul do Brasil, que está emparelhado com uma região fora de sua geografia.

Region		Region
North Central US		South Central US
East US		West US
West US 2		West Central US
US East 2		Central US
Canada Central		Canada East
North Europe		West Europe
UK West		UK South
Germany Central		Germany Northeast
South East Asia		East Asia
East China		North China
Japan East		Japan West
Australia Southeast		Australia East
India South		India Central
Brazil South (Primary)		South Central US

Informações sobre pares regionais:

- Isolamento físico. Quando possível, o Azure prefere pelo menos 300 milhas de separação entre datacenters em um par regional, embora isso não seja prático ou possível em todas as regiões. Datacenter físico separado reduz a probabilidade de desastres naturais, agitação civil, falta de energia ou rede física interrupções que afetam as duas regiões ao mesmo tempo.
- Replicação fornecida pela plataforma. Alguns serviços, como armazenamento georredundante, fornecem replicação para a região emparelhada.
- Ordem de recuperação da região. No caso de uma grande interrupção, a recuperação de uma região é priorizada por par. Os aplicativos implantados em regiões emparelhadas têm a garantia de ter uma das regiões recuperadas com prioridade.

- Atualizações sequenciais. As atualizações planejadas do sistema Azure são lançadas para regiões emparelhadas sequencialmente (não ao mesmo tempo) para minimizar o tempo de inatividade, o efeito de bugs e falhas lógicas no evento raro de uma atualização ruim.
- Residência de dados. Uma região reside dentro da mesma geografia que seu par (exceto o Sul do Brasil) para atender aos requisitos de residência de dados para fins de jurisdição fiscal e de aplicação da lei.

Geographies


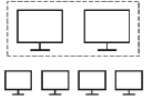
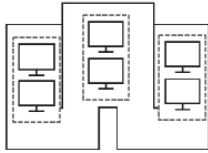
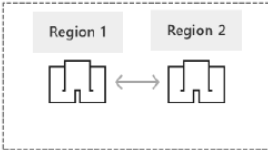
Uma geografia é uma composição que normalmente contém duas ou mais regiões e que preserva a residência de dados e limites de conformidade.

As geografias permitem que clientes com necessidades específicas de residência e conformidade de dados mantenham seus dados e aplicativos compliance.

As geografias garantem que a residência, a soberania, a conformidade e a resiliência dos dados. Os requisitos são respeitados dentro dos limites geográficos. As geografias são tolerantes a falhas para suportar falha completa da região através da conexão com a infraestrutura de rede dedicada de alta capacidade.

As geografias são divididas nas Américas, Europa, Ásia-Pacífico, Oriente Médio e África.

Availability options

VM SLA 99.9% with Premium Storage	VM SLA 99.95%	VM SLA 99.99%	MULTI-REGION DISASTER RECOVERY
			
SINGLE VM Easier lift and shift	AVAILABILITY SETS Protecting against failures within datacenters	AVAILABILITY ZONES Protection from entire datacenter failures	REGION PAIRS Regional protection within Data Residency Boundaries

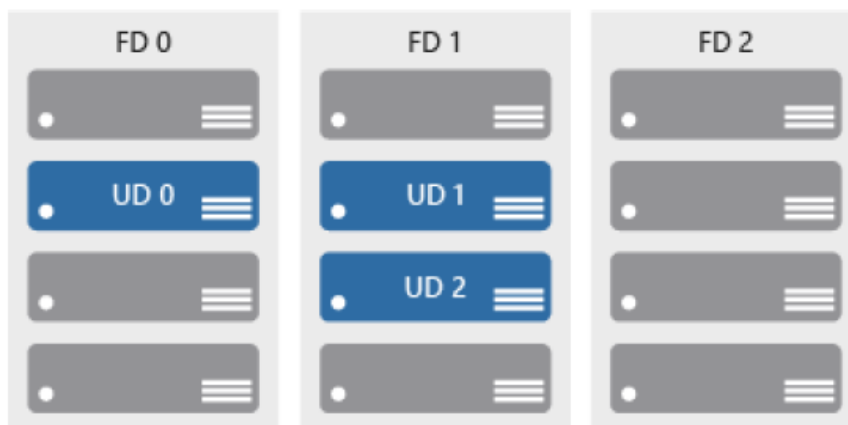
- Uma única máquina virtual com armazenamento premium tem um SLA de 99,9%. Você pode migrar rapidamente as máquinas virtuais existentes para o Azure por meio de "levantamento e troca". Elevação e deslocamento é uma opção sem código, onde cada o aplicativo é migrado como está fornecendo os benefícios da nuvem sem os riscos ou custos de criar alterações de código.
- Ao colocar máquinas virtuais em um conjunto de disponibilidade, você protege contra falhas e aumentos do datacenter o SLA para 99,95%.
-

- A adição de máquinas virtuais às zonas de disponibilidade protege contra falhas inteiras do datacenter e aumenta a SLA para 99,99%. Esse é o nível mais alto de proteção fornecido.
- Para recuperação de desastre com várias regiões, os pares de regiões protegem e fornecem limites de residência de dados.

Availability Sets

Availability Sets são uma maneira de garantir que seu aplicativo permaneça on-line se uma manutenção de alto impacto é necessária, ou ocorrer uma falha no hardware.

Availability são compostos de Update domains (UD) and Fault domains (FD).

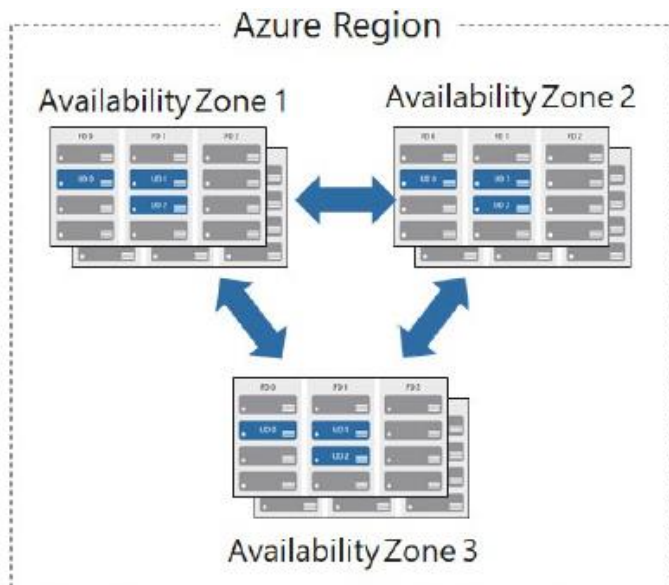


Update Domain: Quando ocorre um evento de manutenção (como uma atualização de desempenho ou um problema crítico, patch de segurança aplicado ao host), a atualização é sequenciada através dos domínios de atualização. Sequenciamento atualizações usando domínios de atualização garante que todo o datacenter não esteja disponível durante a plataforma atualizações e correções. Os domínios de atualização são uma seção lógica do datacenter e são implementados com software e lógica.

Fault Domain: Fault Domains proporcionam a separação física de sua carga de trabalho entre diferentes hardwares no datacenter. Isso inclui energia, refrigeração e hardware de rede que suporta os servidores físicos localizados em racks de servidor. Caso o hardware que suporta um rack de servidor se torne indisponível, apenas esse rack de servidores seria afetado pela interrupção.

Availability Zones

As zonas de disponibilidade são locais fisicamente separados em uma região do Azure que usam conjuntos de disponibilidade para fornecer tolerância a falhas adicional.



Recurso Availability Zone

Cada zona de disponibilidade é um limite de isolamento que contém um ou mais datacenters equipados com energia, refrigeração e rede independentes.

- Se uma zona de disponibilidade cair, a outra continuará funcionando.
- As zonas de disponibilidade geralmente são conectadas entre si por meio de fibra ótica privada muito rápida redes.
- As zonas de disponibilidade permitem que os clientes executem aplicativos de missão crítica com alta disponibilidade e replicação de baixa latência.
- As zonas de disponibilidade são oferecidas como um serviço no Azure e, para garantir a resiliência, há um mínimo de três zonas separadas em todas as regiões ativas.

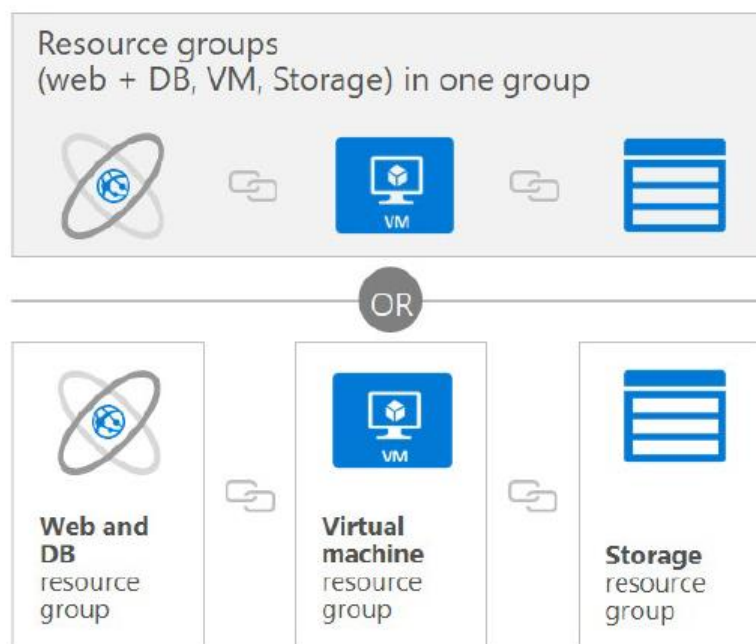
Resource Groups

Um grupo de recursos é uma unidade de gerenciamento para seus recursos no Azure. Você pode pensar no seu recurso grupo como um contêiner que permite agregar e gerenciar todos os recursos necessários para a sua aplicação em uma única unidade gerenciável. Isso permite que você gerencie o aplicativo coletivamente sobre seus ciclos de vida, em vez de gerenciar componentes individualmente.

Você pode gerenciar e aplicar os seguintes recursos no nível do grupo de recursos:

- Medição e cobrança
- Políticas
- Monitoramento e alertas
- Cotas
- Controle de acesso

Lembre-se de que quando você exclui um grupo de recursos, exclui todos os recursos contidos nele.



Considerações

Ao criar e colocar recursos dentro de grupos de recursos, existem algumas considerações:

- Cada recurso deve existir em um e apenas um grupo de recursos.
- Um grupo de recursos pode conter recursos que residem em diferentes regiões.
- Você decide como deseja alocar recursos para grupos de recursos com base no que mais sentido para sua organização.
-

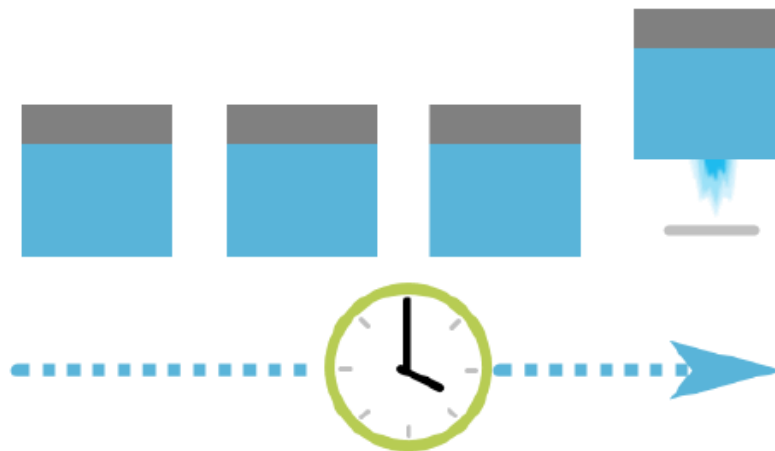
- Você pode adicionar ou remover um recurso a um grupo de recursos a qualquer momento.
- Você pode mover um recurso de um grupo de recursos para outro.
- Os recursos para um aplicativo não precisam existir no mesmo grupo de recursos. No entanto, é recomendado que você os mantenha no mesmo grupo de recursos para facilitar o gerenciamento.

Azure Resource Manager

O Azure Resource Manager é uma camada de gerenciamento na qual grupos de recursos e todos os recursos dentro são criados, configurados, gerenciados e excluídos. Ele fornece uma camada de gerenciamento consistente que permite você automatiza a implantação e a configuração de recursos usando diferentes automações e scripts ferramentas, como Microsoft Azure PowerShell, interface de linha de comando do Azure (CLI do Azure), portal do Azure, REST API e SDKs do cliente.

Com o Azure Resource Manager, você pode:

- **Implantar recursos de aplicativos.** Atualize, gerencie e exclua todos os recursos da sua solução em uma operação coordenada única.



- **Organize recursos.** Gerencie sua infraestrutura por meio de modelos declarativos em vez de scripts. Você pode ver quais recursos estão vinculados por uma dependência e pode aplicar tags aos recursos para categorizá-los para tarefas de gerenciamento, como cobrança.



- **Controlar o acesso e os recursos.** Você pode controlar quem em sua organização pode executar ações no Recursos. Você gerencia permissões definindo funções, adicionando usuários ou grupos às funções e aplicação de políticas no nível do grupo de recursos. Exemplos de elementos que você pode querer controlar são: imposição convenção de nomenclatura de recursos, limitando quais tipos e instâncias de recursos podem ser implantados, ou limitar quais regiões podem hospedar um tipo de recurso.



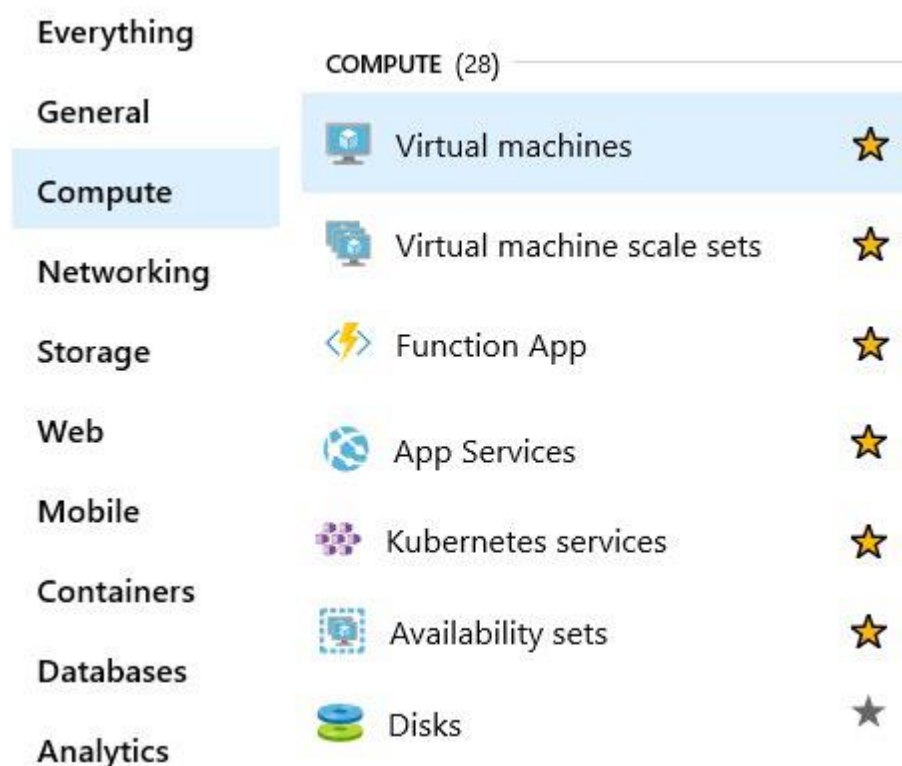
Principais serviços e produtos do Azure

Azure compute

O Azure compute é um serviço de computação sob demanda para executar aplicativos baseados em nuvem. Fornece recursos de computação, como discos, processadores, memória, rede e sistemas operacionais.

Os recursos estão disponíveis sob demanda e geralmente podem ser disponibilizados em minutos ou até segundos.

Você paga apenas pelos recursos que usa e somente enquanto os estiver usando. Existem muitos serviços de computação, dois dos mais comuns são: máquinas virtuais e contêineres.



Azure compute services

Programa de Certificação AZ-900

Virtual Machines (VMs) são emulações de software de computadores físicos. Eles incluem um processador virtual, recursos de memória, armazenamento e rede. Eles hospedam um sistema operacional e você pode instalar e execute o software como um computador físico.

Ao usar um cliente de área de trabalho remota, você pode usar e controle a máquina virtual como se estivesse sentado na frente dela.

- O Azure suporta uma ampla variedade de soluções de computação para desenvolvimento e teste, execução de aplicativos, e estendendo seu datacenter, incluindo Linux, Windows Server, Microsoft SQL Server, Oracle, IBM e SAP.
- O Azure também possui muitos serviços que podem executar máquinas virtuais, cada um oferecendo opções diferentes, dependendo em suas necessidades. Alguns dos serviços mais importantes são Conjuntos de Escala de VM, Serviços de Aplicativo e Funções do Azure.

Azure virtual machines



As Virtual Machines do Azure permitem criar e usar máquinas virtuais na nuvem. Ele fornece IaaS e pode ser usado de várias maneiras diferentes. Quando você precisa de controle total sobre um sistema operacional e ambiente, VMs do Azure são uma escolha ideal.

Assim como um computador físico, você pode personalizar todos os softwares em execução na VM. Isso é particularmente útil quando você está executando um software personalizado ou com configurações de hospedagem customizadas.

VM scale sets



Virtual Machine Scale Set são recursos de computação do Azure que você pode usar para implantar e gerenciar um conjunto de VMs idênticas. Com todas as VMs configuradas da mesma forma, os conjuntos de dimensionamento de VMs são projetados para oferecer suporte a verdadeiras escalas automáticas - não é necessário

Programa de Certificação AZ-900

pré-provisionamento de VMs - e, como tal, facilita a criação em larga escala serviços direcionados a grande computação, big data e cargas de trabalho em contêiner.

Então, conforme a demanda aumenta mais instâncias de máquinas virtuais podem ser adicionadas e, conforme a demanda diminui, as instâncias de máquinas virtuais podem ser removidas. O processo pode ser manual, automatizado ou uma combinação de ambos.

App services



Com o App services, você pode criar, implantar e dimensionar rapidamente aplicativos da Web, móveis e API de nível empresarial executando em qualquer plataforma.

Você pode atender a rigoroso desempenho, escalabilidade, segurança e conformidade requisitos ao usar uma plataforma totalmente gerenciada para executar a manutenção da infraestrutura. Serviços de aplicativos é uma oferta de plataforma como serviço (PaaS).

Functions



O Azure Functions é ideal quando você está preocupado apenas com o código executando o serviço e não a plataforma ou infraestrutura subjacente.

Eles são comumente usados quando você precisa realizar trabalhos em resposta a um evento (geralmente por meio de uma solicitação REST), cronômetro ou mensagem de outro serviço do Azure e quando esse trabalho pode ser concluído rapidamente, em segundos ou menos.

Container services

Contêineres são um ambiente de virtualização.

Contêineres referenciam o sistema operacional do ambiente host que executa o contêiner.

- Ao contrário das máquinas virtuais, você não gerencia o sistema operacional.
- Os contêineres são leves e foram projetados para serem criados, redimensionados e parados dinamicamente.

Programa de Certificação AZ-900



- Os contêineres permitem responder a alterações sob demanda e reiniciar rapidamente em caso de falha ou interrupção de hardware.
- O Azure suporta contêineres do Docker.

Há duas maneiras de gerenciar os contêineres baseados no Docker e na Microsoft no Azure:

Azure Container Instances



Instâncias de Contêiner do Azure oferece a maneira mais rápida e simples de executar um contêiner no Azure sem ter que gerenciar qualquer máquina virtual ou adotar serviços adicionais. É uma oferta PaaS que permite você deve enviar seus contêineres, que serão executados para você.

Azure Kubernetes Service



O Serviço Kubernetes do Azure (AKS) é um serviço completo de orquestração para contêineres com distribuição arquiteturas e grandes volumes de contêineres. A orquestração é a tarefa de automatizar e gerenciar um grande número de contêineres e como eles interagem.

Azure network services

O Azure Networking permite conectar serviços e infraestrutura em nuvem e local para fornecer seus clientes e usuários a melhor experiência possível. Depois que os recursos são movidos para o Azure, eles exigem a mesma funcionalidade de rede que uma implantação local.

Em cenários específicos, eles podem exigir algum nível de isolamento da rede. Os componentes de rede do Azure oferecem uma variedade de funcionalidades e serviços que pode ajudar as organizações a projetar e criar serviços de infraestrutura em nuvem que atendam aos seus requisitos.

Alguns dos tipos de serviço de rede mais comuns no Azure são discutidos nas seções a seguir.

Programa de Certificação AZ-900

Azure Virtual Network



O Azure Virtual Network permite que muitos tipos de recursos do Azure, como VMs do Azure, se comuniquem com segurança entre si, a Internet e as redes locais. Uma rede virtual tem como escopo uma única região; no entanto, várias redes virtuais de diferentes regiões podem ser conectadas usando rede virtual.

Com a Rede Virtual do Azure, você pode fornecer isolamento, segmentação, comunicação com recursos locais e na nuvem, roteamento e filtragem do tráfego de rede.

Azure Load Balancer



O Azure Load Balancer pode fornecer escala para seus aplicativos e criar alta disponibilidade para seus Serviços. O Load Balancer suporta cenários de entrada e saída, fornece baixa latência e alta throughput e dimensiona até milhões de fluxos para todo o TCP (Transmission Control Protocol) e UDP (Datagram Protocol).

Você pode usar o Load Balancer com tráfego de entrada da Internet, interno tráfego nos serviços do Azure, encaminhamento de porta para tráfego específico ou conectividade de saída para VMs em sua rede virtual.

VPN gateway



Um gateway de VPN é um tipo específico de gateway de rede virtual usado para enviar tráfego criptografado entre uma Rede Virtual do Azure e um local no local pela Internet pública. Fornece uma conexão mais segura do local para o Azure pela Internet.

Azure Application Gateway



O Azure Application Gateway é um balanceador de carga de tráfego da Web que permite gerenciar o tráfego para o seu Aplicativos da web. É a conexão através da qual os usuários se conectam ao seu aplicativo. Com Aplicação Gateway, você pode rotear o tráfego com base no endereço IP e na porta de origem para um endereço IP e uma porta de destino.

Você também pode ajudar a proteger um aplicativo Web com um firewall, redirecionamento, afinidade de sessão a mantenha um usuário no mesmo servidor e muitas outras opções de configuração.

Content Delivery Network



Uma rede de entrega de conteúdo (CDN) 20 é uma rede distribuída de servidores que podem fornecer com eficiência web conteúdo para os usuários. É uma maneira de obter conteúdo para os usuários em sua região local para minimizar a latência. CDN pode ser hospedado no Azure ou em qualquer outro local.

Você pode armazenar em cache o conteúdo em nós físicos estrategicamente posicionados mundo e proporcionam melhor desempenho aos usuários finais. Cenários de uso típicos incluem aplicativos da web contendo conteúdo multimídia, um evento de lançamento de produto em uma região ou qualquer evento em que você espere um alto requisito de largura de banda em uma região.

Azure storage services

Azure Storage

O Azure Storage é um serviço que você pode usar para armazenar arquivos, mensagens, tabelas e outros tipos de informações.

Você pode usar o Armazenamento do Azure por conta própria (por exemplo, como um compartilhamento de arquivo), mas os desenvolvedores também costumam usá-lo como uma loja para dados de trabalho. Essas lojas podem ser usadas por sites, aplicativos móveis, aplicativos de desktop e muitos outros tipos de soluções personalizadas.

Programa de Certificação AZ-900



O Armazenamento do Azure também é usado pelas máquinas virtuais IaaS e PaaS serviços na nuvem.

Alguns dos tipos mais comuns de serviço de armazenamento no Azure são **disks, files, objects, queues, and tables**.

Disk storage



O disk storage fornece discos para máquinas virtuais, aplicativos e outros serviços para acessar e usar como eles precisam, semelhante ao que precisariam em cenários locais. O armazenamento em disco permite que os dados sejam persistentemente armazenados e acessados a partir de um disco rígido virtual conectado.

Os discos podem ser gerenciados ou não gerenciados pelo Azure e, portanto, gerenciado e configurado pelo usuário. Os cenários típicos para usar o armazenamento em disco são se você deseja elevar e mudar aplicativos que leem e gravam dados em discos persistentes ou se você estiver armazenando dados que não precisam ser acessados de fora da máquina virtual à qual o disco está conectado.

Os discos têm vários tamanhos e níveis de desempenho diferentes, desde unidades de estado sólido (SSDs) até unidades de disco rígido giratórias (HDDs), com diferentes capacidades de desempenho. Detalhes sobre preços estão disponíveis em a página de preços de discos gerenciados.

Containers (Blobs)



O armazenamento de Blob do Azure é a solução de armazenamento de objetos da Microsoft para a nuvem. O armazenamento de blob é otimizado para armazenando grandes quantidades de dados não estruturados, como texto ou dados binários.

O armazenamento de blob é ideal para:

- Servindo imagens ou documentos diretamente para um navegador.
- Armazenando arquivos para acesso distribuído.
- Streaming de vídeo e áudio.
- Armazenamento de dados para backup e restauração, recuperação de desastres e arquivamento.

- Armazenando dados para análise por um serviço local ou hospedado no Azure.

Files



Azure Files permite configurar compartilhamentos de arquivos de rede altamente disponíveis que podem ser acessados usando o protocolo SMB (Server Message Block) padrão. Isso significa que várias VMs podem compartilhar os mesmos arquivos com acesso de leitura e gravação. Você também pode ler os arquivos usando a interface REST ou o cliente de armazenamento bibliotecas.

Uma coisa que distingue os arquivos do Azure dos arquivos em um compartilhamento corporativo é que você pode acessar os arquivos de qualquer lugar do mundo usando um URL que aponte para o arquivo e inclua uma assinatura de acesso compartilhado (SAS).

Você pode gerar tokens SAS; eles permitem acesso específico a um ativo privado para uma determinada quantidade de tempo.

Os compartilhamentos de arquivos podem ser usados para muitos cenários comuns:

- Muitos aplicativos locais usam compartilhamentos de arquivos. Esse recurso facilita a migração desses aplicativos que compartilham dados com o Azure. Se você montar o compartilhamento de arquivos na mesma letra de unidade que o local uso do aplicativo, a parte do aplicativo que acessa o compartilhamento de arquivos deve funcionar com se houver, muda.
- Os arquivos de configuração podem ser armazenados em um compartilhamento de arquivos e acessados a partir de várias VMs. Ferramentas e utilitários usados por vários desenvolvedores em um grupo pode ser armazenado em um compartilhamento de arquivos, garantindo que todos possam encontrar eles e que eles usam a mesma versão.
- Logs de diagnóstico, métricas e despejos de falhas são apenas três exemplos de dados que podem ser gravados em um compartilhamento e processado ou analisado posteriormente.

Queues



The Azure Queue service é usado para armazenar e recuperar mensagens. As mensagens da fila podem ter até 64 KB em tamanho e uma fila podem conter milhões de mensagens. Filas geralmente são usadas para armazenar listas de mensagens para ser processado de forma assíncrona.

Por exemplo, suponha que você deseja que seus clientes possam fazer upload de fotos e que deseja criar miniaturas para cada foto. Você pode esperar que seu cliente crie as miniaturas ao fazer o upload as fotos. Uma alternativa seria usar uma fila. Quando o cliente terminar o upload, escreva uma mensagem para a fila.

Em seguida, faça com que uma Função do Azure recupere a mensagem da fila e crie o miniaturas. Cada uma das partes desse processamento pode ser dimensionada separadamente, oferecendo mais controle quando ajustando-o para seu uso.

Tables



Azure Table storages armazena grandes quantidades de dados estruturados. O serviço é um armazenamento de dados NoSQL que aceita chamadas autenticadas de dentro e de fora da nuvem do Azure. As tabelas do Azure são ideais para armazenar dados estruturados e não relacionais.

Os usos comuns do armazenamento de tabelas incluem:

- Armazenar TBs de dados estruturados capazes de atender a aplicativos de escala da web.
- Armazenar conjuntos de dados que não exijam junções complexas, chaves estrangeiras ou procedimentos armazenados e podem ser desnormalizado para acesso rápido.
- Consulta rápida de dados usando um índice em cluster.

Você pode usar o armazenamento de tabelas para armazenar e consultar conjuntos enormes de dados estruturados não relacionais e suas tabelas aumentará conforme a demanda aumentar.

Azure database services

Os serviços de banco de dados do Azure são serviços de banco de dados PaaS totalmente gerenciados que liberam um tempo valioso que você, caso contrário, gaste gerenciando seu banco de dados. Desempenho de nível empresarial com alta disponibilidade incorporada significa que você pode escalar rapidamente e alcançar a distribuição global sem se preocupar com o tempo de inatividade dispendioso.

Os desenvolvedores podem tirar proveito das inovações líderes do setor, como segurança incorporada com monitoramento e detecção de ameaças, ajuste automático para melhorar o desempenho e turnkey global distribuição.

Alguns dos tipos de serviço de dados mais comuns no Azure, como a seguir:

Azure Cosmos DB



Microsoft Azure Cosmos DB é um serviço de banco de dados distribuído globalmente que permite que você elasticamente e dimensione de maneira independente a taxa de transferência e o armazenamento em qualquer número de regiões geográficas do Azure. Isto suporta dados sem esquema que permitem criar aplicativos altamente responsivos e Always On para suportar dados em constante mudança.

Você pode usar o Cosmos DB para armazenar dados atualizados e mantidos pelos usuários em todo o mundo. Isso facilita a criação de aplicativos escaláveis e altamente responsivos em escala global.

Azure SQL Database



Azure SQL Database é um banco de dados relacional como serviço (DaaS) baseado na versão estável mais recente do Mecanismo de banco de dados Microsoft SQL Server. O SQL Database é um banco de dados de alto desempenho, confiável, totalmente gerenciado e banco de dados seguro que você pode usar para criar aplicativos e sites controlados por dados na programação idioma de sua escolha sem a necessidade de gerenciar a infraestrutura.

Azure Database Migration

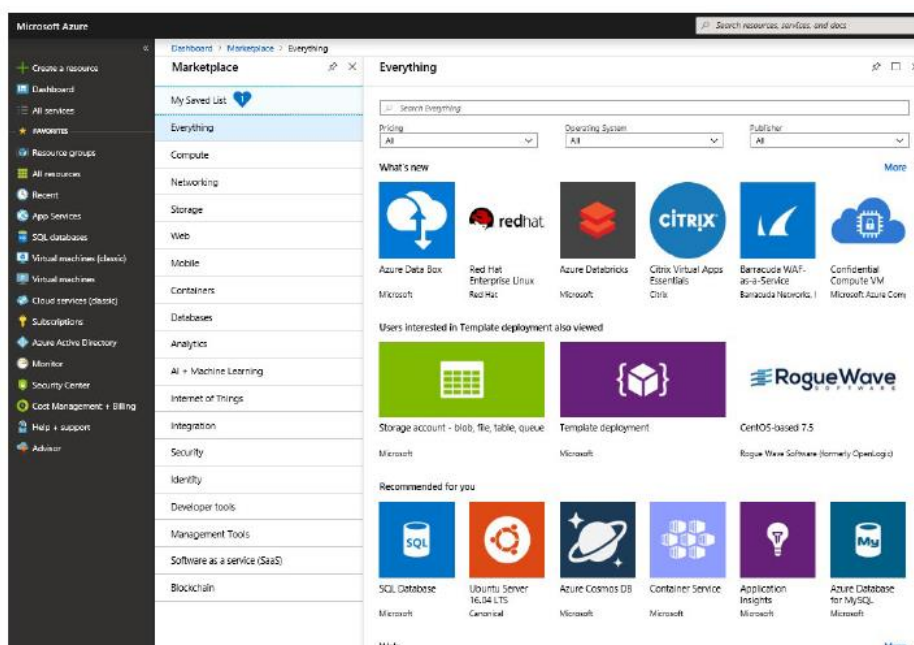
The Azure Database Migration Service é um serviço totalmente gerenciado projetado para permitir migrações de várias fontes de banco de dados para plataformas de dados do Azure com tempo de inatividade mínimo (online migrações).

O serviço usa o Microsoft Data Migration Assistant para gerar relatórios de avaliação que forneça recomendações para ajudá-lo nas alterações necessárias antes de executar uma migração.

Depois de avaliar e executar qualquer correção necessária, você estará pronto para iniciar o processo de migração. O Serviço de Migração de Banco de Dados do Azure executa todas as etapas necessárias.

Azure Marketplace

O Azure Marketplace é um serviço no Azure que ajuda a conectar usuários finais com parceiros da Microsoft, independentes fornecedores de software (ISVs) e startups que oferecem suas soluções e serviços, que são otimizados para execução no Azure. O Azure Marketplace permite que os clientes - principalmente profissionais de TI e nuvem desenvolvedores - para encontrar, experimentar, comprar e provisionar aplicativos e serviços de centenas de prestadores de serviços, todos certificados para execução no Azure.



O catálogo de soluções abrange várias categorias do setor, incluindo, entre outros: contêiner de código aberto plataformas, imagens de máquinas virtuais, bancos de

dados, software de criação e implantação de aplicativos, desenvolvedor ferramentas, detecção de ameaças e blockchain.

Usando o Azure Marketplace, você pode provisionar soluções de ponta a ponta rápida e confiável, hospedado em seu próprio ambiente do Azure. No momento da redação deste artigo, isso inclui mais de 17.000 listagens.

Embora o Azure Marketplace seja projetado para profissionais de TI e desenvolvedores de nuvem interessados em comerciais e software de TI, os Microsoft Partners também o usam como ponto de partida para todas as atividades conjuntas de entrada no mercado.

Azure Solutions

Internet of Things (IoT)

As pessoas podem acessar mais informações do que nunca. Tudo começou com assistentes digitais pessoais (PDAs), depois se transformou em smartphones. Agora existem relógios inteligentes, termostatos inteligentes e até geladeiras inteligentes.

Computadores pessoais costumavam ser a regra. Agora a internet permite que qualquer item on-line possa acessar informações valiosas. A Internet das Coisas (IoT) é a capacidade dos dispositivos de reunir e, em seguida retransmitir informações para análise de dados.

Os tipos de serviço da IoT do Azure são o Azure IoT Central e o Azure IoT Hub.

IoT Central



A IoT Central é uma solução global de software como serviço (SaaS) da IoT, totalmente gerenciada, que facilmente conecte, monitore e gerencie seus ativos de IoT em escala. Não é necessário nenhum conhecimento em nuvem para usar o IoT Central. Como resultado, você pode levar seus produtos conectados ao mercado mais rapidamente, mantendo o foco nos seus clientes.

Azure IoT Hub



O Azure IoT Hub é um serviço gerenciado hospedado na nuvem que atua como um hub central de mensagens para comunicação bidirecional entre seu aplicativo IoT e os dispositivos que ele gerencia. Você pode usar a IoT do Azure Hub para criar soluções de IoT com comunicações confiáveis e seguras entre milhões de dispositivos de IoT e um back-end da solução hospedada na nuvem. Você pode conectar praticamente qualquer dispositivo ao seu Hub IoT.

O Hub IoT suporta comunicações do dispositivo para a nuvem e da nuvem para o dispositivo. Isto também suporta vários padrões de mensagens, como telemetria de dispositivo para nuvem, upload de arquivos de dispositivos, métodos de solicitação e resposta para controlar seus dispositivos a partir da nuvem. O monitoramento do Hub IoT ajuda você a manter a integridade de sua solução rastreando eventos como criação de dispositivo, falhas de dispositivo e dispositivos conexões.

Os recursos do IoT Hub ajudam a criar soluções de IoT escalonáveis e com todos os recursos, como gerenciamento industrial de equipamentos usados na fábrica, rastreamento de ativos valiosos na área da saúde e monitoramento de edifícios e uso em escritórios.

Big Data and Analytics

Os dados são fornecidos em todos os tipos de formas e formatos. Quando falamos sobre Big Data, estamos nos referindo a grandes volumes de dados. Dados de sistemas climáticos, sistemas de comunicação, plataformas de imagem e muitos outros cenários geram grandes quantidades de dados. Essa quantidade de dados se torna cada vez mais difícil de fazer senso e tomar decisões ao redor. Os volumes são tão grandes que as formas tradicionais de processamento e as análises não são mais apropriadas.

As tecnologias de cluster de código aberto foram desenvolvidas ao longo do tempo para tentar lidar com esses grandes conjuntos de dados. O Microsoft Azure suporta uma ampla variedade de tecnologias e serviços para fornecer big data e soluções analíticas. Alguns dos tipos mais comuns de serviços de big data e de análise no Azure são o Azure SQL Data Warehouse, HDInsight e Data Lake Analytics.

Azure SQL Data Warehouse (nome modificado recentemente para Azure Synapse Analytics)



O Azure SQL Data Warehouse é um Enterprise Data Warehouse (EDW) baseado em nuvem que utiliza o MPP para executar consultas complexas rapidamente entre petabytes de dados. Você pode usar o SQL Data Warehouse como um componente chave na solução de big data, importando o big data para o SQL Data Warehouse com o PolyBase Transact Consultas SQL (T-SQL) e use o poder do MPP para executar análises de alto desempenho.

Uma vez que os dados são armazenados no SQL Data Warehouse, você pode executar análises em grande escala. Comparado ao banco de dados tradicional sistemas, as consultas de análise terminam em segundos em vez de minutos ou horas em vez de dias.

Azure HDInsight



O Azure HDInsight é um serviço de análise de código aberto totalmente planejado para empresas. É um serviço de nuvem isso torna mais fácil, mais rápido e mais econômico processar grandes quantidades de dados. O HDInsight permite você executa estruturas populares de código-fonte aberto e cria tipos de cluster como **Apache Spark, Apache Hadoop, Apache Kafka, Apache HBase, Apache Storm, Machine Learning Services**.

HDInsight também suporta uma ampla variedade de cenários, como extração, transformação e carregamento (ETL); dados armazenados, aprendizado de máquina e IoT.

Azure Data Lake Analytics



O Azure Data Lake Analytics é um serviço de análise sob demanda que simplifica o big data. Ao invés de implantar, configurar e ajustar o hardware, você escreve consultas para transformar seus dados e extrair informações valiosas.

O serviço de análise pode lidar com trabalhos de qualquer escala instantaneamente, definindo o mostrador para saber quanta carga que você precisa. Você só paga pelo seu trabalho quando está em execução, tornando-o mais econômico.

Artificial Intelligence

A inteligência artificial, no contexto da computação em nuvem, baseia-se em uma ampla gama de serviços, cujo núcleo é o Machine Learning. O Machine Learning é uma técnica de ciência de dados que permite que os computadores usem os dados existentes para prever comportamentos, resultados e tendências futuras. Usando aprendizado de máquina, computadores aprendem sem ser explicitamente programado.

As previsões do aprendizado de máquina podem tornar os aplicativos e dispositivos mais inteligentes. Por exemplo, quando você compra on-line, o aprendizado de máquina ajuda a recomendar outros produtos que você pode gostar com base no que você comprou. Ou quando o seu cartão de crédito é passado, o aprendizado de máquina compara a transação a um banco de dados de transações e ajuda a detectar fraudes.

E quando o limpador do robô aspira uma sala, a máquina o aprendizado ajuda a decidir se o trabalho está concluído.

Alguns dos tipos de serviço mais comuns de Inteligência Artificial e Machine Learning no Azure são:

Azure Machine Learning Service



O serviço Azure Machine Learning Services fornece um ambiente baseado em nuvem que você pode usar para desenvolver, treinar, testar, implantar, gerenciar e acompanhar modelos de aprendizado de máquina. Ele suporta totalmente tecnologias de código aberto, para que você possa usar dezenas de milhares de pacotes Python de código aberto com componentes de aprendizado de máquina como TensorFlow e scikit-learn. Ferramentas ricas, como blocos de anotações Jupyter ou o Código do Visual Studio.

As ferramentas para IA, facilitam a exploração interativa dos dados, a transformação, o desenvolvimento e o teste de modelos.

O serviço Azure Machine Learning também inclui recursos que automatizam a geração e o ajuste de modelos para ajudá-lo a criar modelos com facilidade, eficiência e precisão. O serviço Azure Machine Learning pode gerar automaticamente um modelo e ajustá-lo para você. Vai deixar que você comece a treinar na sua máquina local e depois expanda para a nuvem.

Quando você tem o modelo certo, você pode implantá-lo facilmente em um contêiner como o Docker no Azure. Use o serviço Machine Learning se você trabalha em um

ambiente Python, você deseja ter mais controle sobre seus algoritmos de aprendizado de máquina ou deseja usar bibliotecas de aprendizado de máquina de código-fonte aberto.

Azure Machine Learning Studio



O Azure Machine Learning Studio é um espaço de trabalho visual colaborativo, de arrastar e soltar, no qual você pode criar, testar e implantar soluções de aprendizado de máquina sem precisar escrever código. Utiliza algoritmos de aprendizado de máquina e módulos de manipulação de dados pré-configurados.

Usar o Machine Learning Studio quando você quiser experimentar modelos de aprendizado de máquina de maneira rápida e fácil, e a máquina já terá embutida algoritmos de aprendizado que são suficientes para suas soluções. Não fornece tanto controle sobre a máquina e algoritmos como Azure Machine Learning Services que discutimos anteriormente.

Serverless Computing

Serverless computing

O Azure Serverless é um ambiente de execução hospedado em nuvem que executa seu código, mas abstrai o ambiente de hospedagem subjacente. Você cria uma instância do serviço e adiciona seu código. Nenhuma configuração ou manutenção da infraestrutura é necessária ou até permitida.

Você configura seus aplicativos Serverless para responder a eventos. Um evento pode ser um terminal REST, um período periódico temporizador ou mesmo uma mensagem recebida de outro serviço do Azure. O aplicativo sem servidor é executado apenas quando é acionado por um evento.

O dimensionamento e o desempenho são tratados automaticamente e você é cobrado apenas pelos recursos exatos que usar. Você nem precisa reservar recursos.

Alguns dos tipos de serviço sem servidor mais comuns no Azure são o Azure Functions, o Azure Logic Apps e Event Grid do Azure.

Azure Functions



O Azure Functions é ideal quando você está preocupado apenas com o código que está executando seu serviço e não com a plataforma ou infraestrutura subjacente. O Azure Functions são comumente usados quando você precisa executar trabalhos em resposta a um evento, geralmente por meio de uma solicitação REST, cronômetro ou mensagem de outro serviço do Azure, e quando esse trabalho puder ser concluído rapidamente, em segundos ou menos.

Os Azure Functions são dimensionados automaticamente e as cobranças são acumuladas somente quando uma função é acionada, portanto, elas são uma escolha sólida quando a demanda é variável. Por exemplo, você pode estar recebendo mensagens de uma solução de IoT que monitora uma frota de veículos de entrega. Você provavelmente terá mais dados chegando durante o horário comercial.

O Azure Functions pode ser expandido para acomodar esses horários de maior movimento. Além disso, os Azure Functions sem estado, eles se comportam como se fossem reiniciados toda vez que respondem a um evento. Isso é ideal para o processamento de dados recebidos.

E se o estado for necessário, eles podem ser conectados a um Serviço de armazenamento do Azure.

Azure Logic Apps



O Logic Apps é um serviço em nuvem que ajuda a automatizar e orquestrar tarefas, processos de negócios e fluxos de trabalho quando você precisa integrar aplicativos, dados, sistemas e serviços em empresas ou organizações.

O Logic Apps simplifica a maneira como você projeta e cria soluções escaláveis - seja na nuvem, localmente ou ambos - para app integration, data integration, system integration, enterprise applications integration (EAI), and business-to-business (B2B) integration.

Os aplicativos lógicos são projetados em um designer baseado na Web e podem executar a lógica acionada pelos serviços do Azure sem escrever nenhum código. Para criar soluções de integração corporativa com os Azure Logic Apps, você pode

escolher de uma galeria com mais de 200 conectores. Isso inclui serviços como Salesforce, SAP, Oracle DB e compartilhamentos de arquivos.

Azure Event Grid



O Event Grid permite criar aplicativos facilmente com arquiteturas baseadas em eventos. É totalmente gerenciado, é um serviço de roteamento inteligente de eventos que usa um modelo de publicação/assinatura para um consumo uniforme de eventos. O Event Grid tem suporte interno para eventos provenientes dos serviços do Azure, como blobs de armazenamento e resources groups.

Você pode usar o Event Grid para dar suporte a seus próprios eventos não baseados no Azure em tempo quase real, usando configurações personalizadas.

Você pode usar filtros para rotear eventos específicos para diferentes pontos de extremidade e garantir que seus eventos sejam entregues de forma confiável.

DevOps

O DevOps (Deployment and Operations) reúne pessoas, processos e tecnologia, automatizando entrega de software para fornecer valor contínuo aos seus usuários. Os Serviços de DevOps do Azure permitem criar, construir e liberar pipelines que fornecem integração, entrega e implantação contínuas para os seus formulários.

Você pode integrar repositórios e testes de aplicativos, executar monitoramento de aplicativos e trabalhar com artefatos de construção. Você também pode trabalhar com itens de backlog, automatizar a infraestrutura de implantação e integrar uma variedade de ferramentas e serviços de terceiros, como Jenkins e Chef.

Todas estas funções e muito mais estão intimamente integradas ao Azure para permitir implantações consistentes e repetíveis, para que seus aplicativos forneçam processos simplificados de criação e lançamento.

Alguns dos principais serviços de DevOps disponíveis no Azure são o Azure DevOps Services e o Azure DevTest Labs.

Azure DevOps Services



O DevOps Services fornece ferramentas de colaboração para o desenvolvimento, incluindo pipelines de alto desempenho, repositórios Git privados, Boards Kanban e ampla carga automatizada. O DevOps Services era conhecido anteriormente como VSTS (Visual Studio Team Services).

Azure Lab Services



O Azure Lab Services é um serviço que ajuda desenvolvedores e testadores a criar rapidamente ambientes no Azure, enquanto minimizando desperdícios e controlando custos. Os usuários podem testar suas versões mais recentes de aplicativos provisionando rapidamente Ambientes Windows e Linux usando modelos e artefatos reutilizáveis. Você pode integrar facilmente seu pipeline de implantação com o DevTest Labs para provisionar ambientes sob demanda.

Com o DevTest Labs você pode aumentar o seu teste de carga provisionando vários agentes de teste e criando dispositivos pré-provisionados ambientes para treinamento e demonstrações. Os Serviços de laboratório eram formalmente conhecidos como DevOps Test.

Azure App Service

Com o Azure App Service, você pode criar rápida e facilmente aplicativos da Web e móveis para qualquer plataforma ou dispositivo. O Serviço de Aplicativo do Azure permite criar e hospedar aplicativos da web, back-ends móveis e APIs RESTful em a linguagem de programação de sua escolha sem gerenciar a infraestrutura. Oferece escala automática e alta disponibilidade, suporta Windows e Linux e permite implantações automatizadas do GitHub, DevOps do Azure ou qualquer repositório Git.

Principais recursos do Azure Service App

Vários idiomas e estruturas: O Serviço de Aplicativo tem suporte de primeira classe para o ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP ou Python. Você também pode executar o PowerShell e outros scripts ou executáveis como serviços em segundo plano.

Programa de Certificação AZ-900

Otimização de DevOps: Configurar integração e implantação contínuas com o Azure DevOps, GitHub, BitBucket, Docker Hub ou Registro de Contêiner do Azure. Promova atualizações por meio de teste e preparo ambientes. Gerencie seus aplicativos no Serviço de Aplicativo usando o Azure PowerShell ou a plataforma cruzada interface da linha de comandos (CLI).

Escala global com alta disponibilidade: Escale para cima ou para fora manualmente ou automaticamente. Hospede seus aplicativos em qualquer lugar da infraestrutura global

de datacenter da Microsoft, e o SLA do Serviço de Aplicativo promete alta disponibilidade.

Conexões com plataformas SaaS e dados locais: Escolha entre mais de 50 conectores para sistemas corporativos (como SAP), serviços SaaS (como Salesforce) e serviços de Internet (como Facebook). Acesse dados locais usando conexões híbridas e redes virtuais do Azure.

Segurança e conformidade: O Serviço de Aplicativo é compatível com ISO, SOC e PCI. Autenticar usuários com o Azure Active Directory ou com login social (Google, Facebook, Twitter e Microsoft). Criar endereço IP restrições e gerenciar identidades de serviço.

Modelos de aplicativos: Escolha entre uma extensa lista de modelos de aplicativos no Azure Marketplace, como WordPress, Joomla e Drupal.

Integração do Visual Studio: As ferramentas dedicadas no Visual Studio agilizam o trabalho de criação, implantação e depuração. API e recursos móveis. O Serviço de Aplicativo fornece suporte CORS chave na mão para cenários de API RESTful e simplifica os cenários de aplicativos móveis, permitindo autenticação, sincronização de dados offline, notificações push e mais.

Código sem servidor: Execute um snippet de código ou script sob demanda sem precisar provisionar ou gerenciar a infraestrutura e pague apenas pelo tempo de computação que seu código realmente usa.

Azure Management Tools

Você pode configurar e gerenciar o Azure usando uma ampla variedade de ferramentas e plataformas. Existem ferramentas disponíveis para a linha de comando, kits de desenvolvimento de software (SDKs) específicos do idioma, ferramentas de desenvolvedor, ferramentas para migração e muitas outras.

Azure Portal



Programa de Certificação AZ-900

O portal do Azure é um site público que você pode acessar com qualquer navegador da web. Depois de fazer login com sua conta do Azure, você pode criar, gerenciar e monitorar quaisquer serviços disponíveis do Azure. Você pode identificar um serviço que você procura, obtenha links para obter ajuda sobre um tópico e implante, gerencie e exclua recursos. Isso também orienta você em tarefas administrativas complexas usando assistentes e dicas de ferramentas.

A exibição do painel fornece detalhes de alto nível sobre o seu ambiente do Azure. Você pode personalizar o como você precisa, movendo e redimensionando blocos, exibindo

apenas serviços de interesse específicos, acessar links para obter ajuda e suporte e fornecer feedback.

O portal não fornece nenhuma maneira de automatizar tarefas repetitivas. Por exemplo, para configurar várias VMs, você precisaria criá-los um por vez, concluindo o assistente para cada VM. Isso pode ser demorado e propenso a erros para tarefas complexas.

Azure PowerShell



O Azure PowerShell é um módulo que você adiciona ao Windows PowerShell ou PowerShell Core que permite que você se conecte à sua assinatura do Azure e gerencie recursos. O Azure PowerShell requer Windows PowerShell para funcionar. O PowerShell fornece serviços como a janela do shell e a análise de comandos. O Azure PowerShell adiciona os comandos específicos do Azure.

Por exemplo, o Azure PowerShell fornece o comando `New-AzVM` que cria uma máquina virtual para você dentro de sua assinatura do Azure. Para usá-lo, inicie o PowerShell, entre na sua conta do Azure usando o comando `Connect-AzureRMAccount` e, em seguida, emita um comando como:

```
New-AzVm `
-ResourceGroupName "TesResourceGroup" `
-Name "Testvm" `
-Image "UbuntuLTS"
...
```

Nota: O PowerShell Core é uma versão multiplataforma do PowerShell executada no Windows, Linux ou macOS.

Azure Command Line Interface (CLI)



A CLI do Azure é um programa de linha de comando de plataforma cruzada que se conecta ao Azure e executa comandos nos recursos do Azure. Plataforma cruzada significa que pode ser executado no Windows, Linux ou macOS.

Por exemplo, para criar uma VM, você abriria uma janela de prompt de comando, entraria no Azure usando o comando `az login`, crie um grupo de recursos e use um comando como:

```
az vm create \  
--resource-group Testrg1 \  
--name Testvm \  
--image UbuntuLTS  
--generate-ssh-keys  
...
```

Azure Cloud Shell



O Azure Cloud Shell é um ambiente de script baseado em navegador no seu portal. Ele fornece a flexibilidade de escolhendo a experiência do shell que melhor se adapta à sua maneira de trabalhar.

Os usuários do Linux podem optar por uma experiência no Bash, enquanto os usuários do Windows podem optar pelo PowerShell. É necessária uma conta de armazenamento para usar o shell da nuvem e você será solicitado a criar uma ao acessar o shell de nuvem do Azure.

Azure Mobile App



O aplicativo móvel do Microsoft Azure permite acessar, gerenciar e monitorar todas as suas contas do Azure e recursos do seu telefone ou tablet iOS ou Android. Depois de instalado, você pode:

- Verifique o status e métricas importantes de seus serviços.

Programa de Certificação AZ-900

- Mantenha-se informado com notificações e alertas sobre importantes problemas de saúde.
- Diagnostique e corrija rapidamente problemas a qualquer momento, em qualquer lugar.
- Analise os alertas mais recentes do Azure.
- Iniciar, parar e reiniciar máquinas virtuais ou aplicativos da web.
- Conecte-se às suas máquinas virtuais.
- Gerenciar permissões com controle de acesso baseado em função (RBAC).
- Use o Azure Cloud Shell para executar scripts salvos ou executar tarefas administrativas ad hoc.

Azure REST API



APIs REST (Representational State Transfer) são terminais de serviço que suportam conjuntos de operações HTTP (métodos), que fornecem criar, recuperar, atualizar ou excluir o acesso aos recursos do serviço. Uma API REST define um conjunto de funções que os desenvolvedores podem executar solicitações e receber respostas via HTTP protocolo como GET e POST.

Azure Advisor

O Azure Advisor é um serviço gratuito incorporado ao Azure que fornece recomendações sobre alta disponibilidade, segurança, desempenho e custo.

O Advisor analisa seus serviços implementados e procura maneiras de melhorar seu ambiente nessas quatro áreas.



Com o Azure Advisor, você pode:

- Receba recomendações proativas, práticas e personalizadas de práticas recomendadas.
- Melhore o desempenho, a segurança e a alta disponibilidade de seus recursos ao identificar oportunidades para reduzir seus custos gerais do Azure.
- Receba recomendações com as ações propostas em linha.
-

Você pode acessar o Azure Advisor pelo portal do Azure. Depois de entrar no portal, selecione Orientador no menu de navegação ou procure-o no menu Todos os serviços. Você pode baixar recomendações do Azure Advisor no formato PDF ou CSV, que você pode então compartilhar.

<div data-bbox="256 309 312 367"></div> <div data-bbox="320 315 542 353">High Availability</div> <div data-bbox="477 528 528 577"></div> <div data-bbox="264 595 745 663">You are following all of our high availability recommendations</div> <div data-bbox="260 658 745 694">See list of high availability recommendations</div>	<div data-bbox="826 309 882 367"></div> <div data-bbox="890 315 1002 353">Security</div> <div data-bbox="821 450 1102 492">4 Recommendations</div> <div data-bbox="826 510 1315 539"></div> <div data-bbox="821 562 1268 622"> <div>4 High impact</div> <div>0 Medium impact</div> <div>0 Low impact</div> </div> <div data-bbox="821 734 1112 777">3 Impacted resources</div>
<div data-bbox="256 875 312 934"></div> <div data-bbox="320 882 494 920">Performance</div> <div data-bbox="477 1099 528 1149"></div> <div data-bbox="280 1167 724 1232">You are following all of our performance recommendations</div> <div data-bbox="276 1227 730 1263">See list of performance recommendations</div>	<div data-bbox="826 875 882 956"></div> <div data-bbox="890 882 1193 920">Operational Excellence</div> <div data-bbox="821 1016 1090 1059">1 Recommendation</div> <div data-bbox="826 1077 1315 1106"></div> <div data-bbox="821 1128 1268 1189"> <div>0 High impact</div> <div>0 Medium impact</div> <div>1 Low impact</div> </div> <div data-bbox="821 1301 1101 1344">1 Impacted resource</div>

Revisão – Questões Módulo 02

Review Question 1

Which of the following ensures data-residency and compliance needs are met for customers who need to keep their data and applications close?

- A. Geographies
- B. Regions
- C. Zones

Review Question 2

As a best practice, all resources that are part of an application and share the same lifecycle should exist in the same?

- A. Availability set
- B. Region
- C. Resource group

Review Question 3

Which Azure compute resource can you use to deploy to manage a set of identical virtual machines?

- A. Virtual machine availability sets
- B. Virtual machine availability zones
- C. Virtual machine scale sets

Review Question 4

Which of the following should you use when you are concerned only about the code running your service and not the underlying platform or infrastructure?

- A. Azure App Service
- B. Azure Container Instances
- C. Azure Functions

Review Question 5

Azure Resource Manager templates use which format?

- A. HTML
- B. JSON
- C. XML

Review Question 6

Which of the following services is a distributed network of servers that can efficiently deliver web content to users?

- A. Azure App Services
- B. Azure Content Delivery Network
- C. Azure Cosmos DB

Review Question 7

Which of the following is optimized for storing massive amounts of unstructured data, such as videos and images?

- A. Blobs
- B. Files
- C. Queues

Review Question 8

Which of the following is part of the Azure Artificial Intelligence service?

- A. HDInsight
- B. Azure Machine Learning service
- C. Azure DevTest Labs

Review Question 9

Which of the following cloud services provides development collaboration tools including high-performance pipelines, free private Git repositories, and configurable Kanban boards?

- A. Azure DevOps Services
- B. Azure Event Grid
- C. HDInsight

Review Question 10

Microsoft Azure datacenters are organized and made available by?

- A. Geographies
- B. Regions
- C. Zones

Resumo do Módulo 2

Neste módulo, você aprendeu sobre os principais componentes de arquitetura do Microsoft Azure, os principais serviços do Azure e soluções e várias ferramentas de gerenciamento disponíveis para gerenciar e configurar o Azure.

Componentes arquiteturais principais do Azure

Nesta lição, aprendemos sobre como os datacenters e serviços do Azure estão localizados e organizados nas regiões e geografias. Também aprendemos como a disponibilidade é alcançada usando zonas e conjuntos de disponibilidade.

Aprendemos sobre como automatizar implantações e configurações de recursos e serviços usando modelos JSON declarativos que utilizam a camada do Azure Resource Manager para criar e configurar recursos. E, finalmente, aprendemos a usar grupos de recursos para gerenciar recursos no Azure.

Serviços e produtos principais do Azure

Nesta lição, aprendemos sobre serviços de computação e o uso de máquinas e contêineres virtuais. Nós adquirimos um entendimento de alguns dos serviços que compõem o serviço de computação, como VMs do Azure, Conjuntos de dimensionamento de VM, serviços e funções de aplicativo, Instâncias de Contêiner do Azure e Serviço Kubernetes do Azure. Nós também aprendemos sobre serviços de rede, como Rede Virtual, Azure Load Balancer, Gateway VPN, Gateway de Aplicativo e Rede de Entrega de Conteúdo do Azure.

Soluções do Azure

Nesta lição, aprendemos sobre soluções como IoT e serviços que fazem parte da oferta de serviços como o Hub IoT do Azure e o Microsoft IoT Central. Discutimos serviços de análise de big data, como o Azure SQL Data Warehouse, HDInsight e Azure Data Lake Analytics. Também aprendemos sobre IA e como utiliza serviços de aprendizado de máquina, como o Azure Machine Learning e o Azure Machine Learning Studio.

Também aprendemos sobre serviços de computação sem servidor, como Funções do Azure, Aplicativos de Lógica do Azure e Grade de Eventos do Azure. Finalmente, aprendemos sobre os serviços de DevOps, como o Azure DevOps e o Azure DevTest Labs.

Ferramentas de gerenciamento do Azure

Nesta lição, aprendemos sobre as ferramentas de gerenciamento disponíveis para gerenciar e configurar o Azure, como Portal do Azure, Azure PowerShell, CLI do Azure e Shell de Nuvem do Azure. Ele também inclui o Azure Advisor, que fornece recomendações sobre alta disponibilidade, segurança, desempenho e custo.

Respostas da revisão

Questão 01: Geographies

Explicação: Geographies. Geographies permite que clientes com necessidades específicas de residência e conformidade de dados mantenham seus dados e aplicativos próximos. As geografias garantem que os requisitos de residência, soberania, conformidade e resiliência de dados sejam atendidos dentro dos limites geográficos.

Questão 02: Resource group

Explicação: Resource group. Para facilitar o gerenciamento, os recursos que fazem parte de um aplicativo e compartilham seu ciclo de vida devem ser colocados no mesmo grupo de recursos.

Questão 03: Virtual machine scale sets

Explicação: Virtual machine scale sets. Virtual machine scale conjuntos permitem implantar e gerenciar um conjunto de máquinas virtuais idênticas.

Questão 04: Azure Functions

Explicação: Azure Functions. Azure Functions são ideais quando você está preocupado apenas com o código que executa seu serviço e não com a plataforma ou infraestrutura subjacente.

Questão 05: JSON

Explicação: JSON. Resource Manager templates são arquivos JSON que definem os recursos que você precisa implantar para sua solução. Você pode usar o modelo para recriar facilmente várias versões da sua infraestrutura, como preparação e produção.

Questão 06: Azure Content Delivery Network

Explicação: Azure Content Delivery Network. A Content Delivery Network é uma rede distribuída de servidores que pode fornecer com eficiência conteúdo da web aos usuários.

Questão 07: Blobs

Explicação: Blobs. Azure Blob storage é a solução de armazenamento de objetos da Microsoft para a nuvem. O armazenamento de blob é otimizado para armazenar grandes quantidades de dados não estruturados, como texto ou dados binários.

Questão 08: Azure Machine Learning service

Explicação: Azure Machine Learning service. Machine Learning service fornece um ambiente baseado em nuvem que você pode usar para desenvolver, treinar, testar, implantar, gerenciar e rastrear modelos de aprendizado de máquina.

Questão 09: Azure DevOps Services

Explicação: Azure DevOps Services. Azure DevOps Services inclui ferramentas de colaboração de desenvolvimento, incluindo pipelines de alto desempenho, repositórios Git privados gratuitos e boards Kanban.

Questão 10: Regions

Explicação: Regions. Os datacenters do Microsoft Azure são organizados e disponibilizados por região.

Modulo03

Segurança, Privacidade, Conformidade e Confiança

Protegendo a conectividade de rede

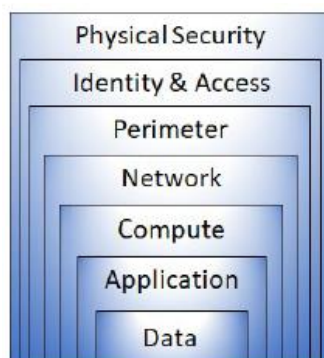
Defesa em profundidade A defesa em profundidade é uma estratégia que emprega uma série de mecanismos para retardar o avanço de um ataque que visa adquirir acesso não autorizado aos dados. O objetivo da defesa em profundidade é proteger e impedir que informações sejam roubadas por indivíduos não autorizados a acessá-las. Os princípios comuns usados para definir uma postura de segurança são confidencialidade, integridade e disponibilidade, conhecidas coletivamente como CIA.

Confidencialidade - O Princípio de menor privilégio restringe o acesso às informações apenas a indivíduos que tenham acesso explícito. Essas informações incluem proteção de senhas de usuários, certificados de acesso remoto e conteúdo de email.

Integridade: A prevenção de alterações não autorizadas nas informações em repouso ou em trânsito. Uma abordagem comum usada na transmissão de dados é o remetente criar uma impressão digital exclusiva dos dados usando um algoritmo de hash unidirecional. O hash é enviado ao destinatário junto com os dados. O hash dos dados é recalculado e comparado ao original pelo destinatário para garantir que os dados não foram perdidos ou modificados em trânsito.

Disponibilidade: Verifique se os serviços estão disponíveis para usuários autorizados. Os ataques de negação de serviço são uma causa predominante de perda de disponibilidade para os usuários.

A defesa em profundidade pode ser visualizada como um conjunto de camadas, com os Dados a serem protegidos no centro. Cada camada fornece proteção para que, se uma camada for violada, uma camada subsequente já esteja em vigor para evitar mais exposições. Essa abordagem elimina a dependência de qualquer camada única de proteção e atua para retardar um ataque e fornecer telemetria de alerta que pode ser acionada, automática ou manualmente.



Segurança física é a primeira linha de defesa para proteger o hardware de computação no datacenter.

Controles de identidade e acesso acessam a infraestrutura e o controle de alterações.

A camada de perímetro usa a proteção de negação de serviço distribuída (DDoS) para filtrar ataques em larga escala antes que eles possam causar uma negação de serviço aos usuários finais.

A camada de rede limita a comunicação entre recursos por meio de controles de segmentação e acesso.

A camada de computação protege o acesso a máquinas virtuais.

A camada de aplicativos garante que os aplicativos estejam seguros e livres de vulnerabilidades.

✓ A Microsoft aplica uma abordagem em camadas à segurança, em nossos datacenters físicos e nos serviços do Azure.

Segurança Compartilhada

Segurança compartilhada À medida que os ambientes de computação passam dos datacenters controlados pelo cliente para os datacenters na nuvem, a responsabilidade da segurança também muda. A segurança agora é uma preocupação compartilhada por provedores e clientes em nuvem.

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Cliente	Cliente	Cliente	Cliente
Client endpoints	Cliente	Cliente	Cliente	Cliente
Account and access management	Cliente	Cliente	Cliente	Cliente
Identity and directory infrastructure	Cliente	Cliente	Microsoft/Cliente	Microsoft/Cliente
Application	Cliente	Cliente	Microsoft/Cliente	Microsoft
Network controls	Cliente	Cliente	Microsoft/Cliente	Microsoft
Operating system	Cliente	Cliente	Microsoft	Microsoft
Physical hosts	Cliente	Microsoft	Microsoft	Microsoft
Physical network	Cliente	Microsoft	Microsoft	Microsoft
Physical datacenter	Cliente	Microsoft	Microsoft	Microsoft

Azure Firewall

Um Firewall é um serviço que concede acesso ao servidor com base no endereço IP de origem de cada solicitação. Você cria regras de firewall que especificam intervalos de endereços IP. Somente clientes desses endereços IP concedidos terão permissão para acessar o servidor. As regras do firewall também incluem informações de porta e protocolo de rede específicas.



O Azure Firewall¹ é um serviço de segurança de rede gerenciado, baseado na nuvem, que protege os recursos da Rede Virtual do Azure. É um firewall totalmente stateful como um serviço com alta disponibilidade incorporada e escalabilidade irrestrita na nuvem. Você pode criar, impor e registrar políticas de conectividade de aplicativos e rede em assinaturas e redes virtuais centralmente. O Firewall do Azure usa um endereço IP público estático para seus recursos de rede virtual, o que permite que firewalls externos identifiquem o tráfego originado na sua rede virtual. O serviço está totalmente integrado ao Azure Monitor para log e análise. O Firewall do Azure fornece muitos recursos, incluindo:

- Alta disponibilidade interna.
- Escalabilidade irrestrita na nuvem.
- Regras de filtragem de entrada e saída.
- Log do Azure Monitor

Cenários de uso comum

Você geralmente implanta o Firewall do Azure em uma rede virtual central para controlar o acesso geral à rede. Com o Firewall do Azure, você pode configurar:

- Regras de aplicativo que definem nomes de domínio totalmente qualificados (FQDNs) que podem ser acessados a partir de uma sub-rede.
- Regras de rede que definem endereço de origem, protocolo, porta de destino e endereço de destino.

✓ O Azure Application Gateway também fornece um firewall, chamado WAF (Web Application Firewall). O WAF fornece proteção centralizada de entrada para seus aplicativos da Web contra explorações e vulnerabilidades comuns.

Azure DDoS Protection

Os ataques DDoS tentam sobrecarregar e esgotar os recursos de um aplicativo, tornando o aplicativo lento ou sem resposta a usuários legítimos. Os ataques DDoS podem ser direcionados para qualquer terminal acessível publicamente pela Internet. Portanto, qualquer recurso exposto à Internet, como um site, está potencialmente em risco de um

ataque DDoS. Quando você combina a Proteção DDoS do Azure com as práticas recomendadas de design de aplicativos, ajuda a fornecer defesa contra ataques DDoS. A proteção contra DDoS aproveita a escala e a elasticidade da rede global da Microsoft para oferecer capacidade de mitigação de DDoS a todas as regiões do Azure. O serviço Azure DDoS Protection protege seus aplicativos do Azure limpando o tráfego na borda da rede do Azure antes que possa afetar a disponibilidade do serviço. Camadas do serviço de proteção contra DDoS do Azure O Azure DDoS Protection fornece as seguintes camadas de serviço:

- **Básico.** A camada de serviço Básico é ativada automaticamente como parte da plataforma do Azure. O monitoramento do tráfego sempre ativo e a atenuação em tempo real de ataques comuns no nível da rede fornecem as mesmas defesas que os serviços online da Microsoft usam. A rede global do Azure é usada para distribuir e atenuar o tráfego de ataques entre regiões.
- **Padrão.** A camada de serviço Padrão fornece recursos de mitigação adicionais ajustados especificamente aos recursos da Rede Virtual do Microsoft Azure. O padrão de proteção DDoS é simples de ativar e não requer alterações no aplicativo. As políticas de proteção são ajustadas por meio de monitoramento de tráfego dedicado e algoritmos de aprendizado de máquina. As políticas são aplicadas a endereços IP públicos associados a recursos implantados em redes virtuais, como o Azure Load Balancer e o Application Gateway.

Proteção padrão DDoS

A proteção padrão DDoS pode atenuar os seguintes tipos de ataques:

- **Ataques volumétricos.** O objetivo do ataque é inundar a camada de rede com uma quantidade substancial de tráfego aparentemente legítimo.
- **ataques de protocolo.** Esses ataques tornam um alvo inacessível, explorando uma fraqueza na pilha de protocolos das camadas 3 e 4.
- **Ataques da camada de recursos (aplicativo).** Esses ataques têm como alvo os pacotes de aplicativos da web para interromper a transmissão de dados entre hosts.

Network Security Groups (NSG)

Network Security Groups⁴ permitem filtrar o tráfego de rede de e para recursos do Azure em uma rede virtual do Azure. Um NSG pode conter várias regras de segurança de entrada e saída que permitem filtrar o tráfego de e para recursos por endereço IP, porta e protocolo de origem e destino.

Propriedades Network security rule

Um grupo de segurança de rede pode conter quantas regras você precisar, dentro dos limites de assinatura do Azure. Cada regra especifica as seguintes propriedades:

Property	Explanation
Name	Unique name of the NSG.
Priority	A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers.
Source or Destination	Individual IP address or IP address range, service tag, or application security group.
Protocol	TCP, UDP, or Any.
Direction	Whether the rule applies to inbound or outbound traffic.
Port Range	An individual port or range of ports.
Action	Allow or Deny.

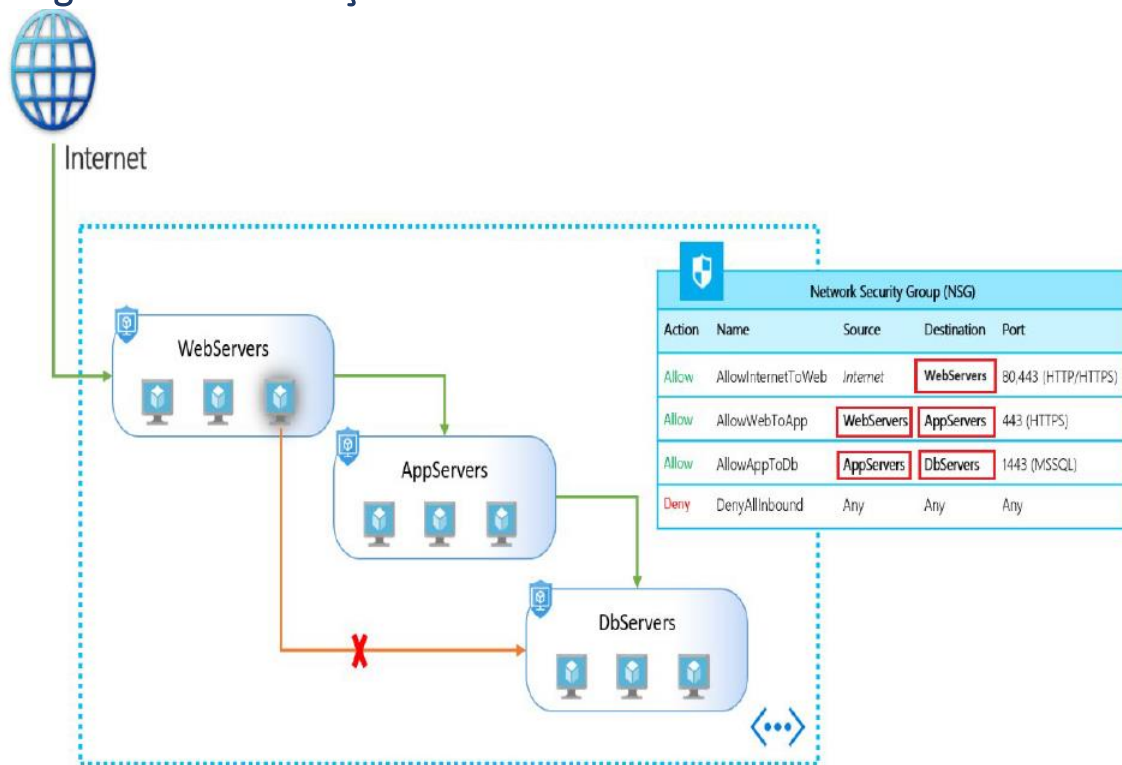
Quando você cria um grupo de segurança de rede, o Azure cria uma série de regras padrões para fornecer um nível de linha de base de segurança. Você não pode remover as regras padrões, mas pode substituí-las criando novas regras com prioridades mais altas.

Application Security Groups (ASG)

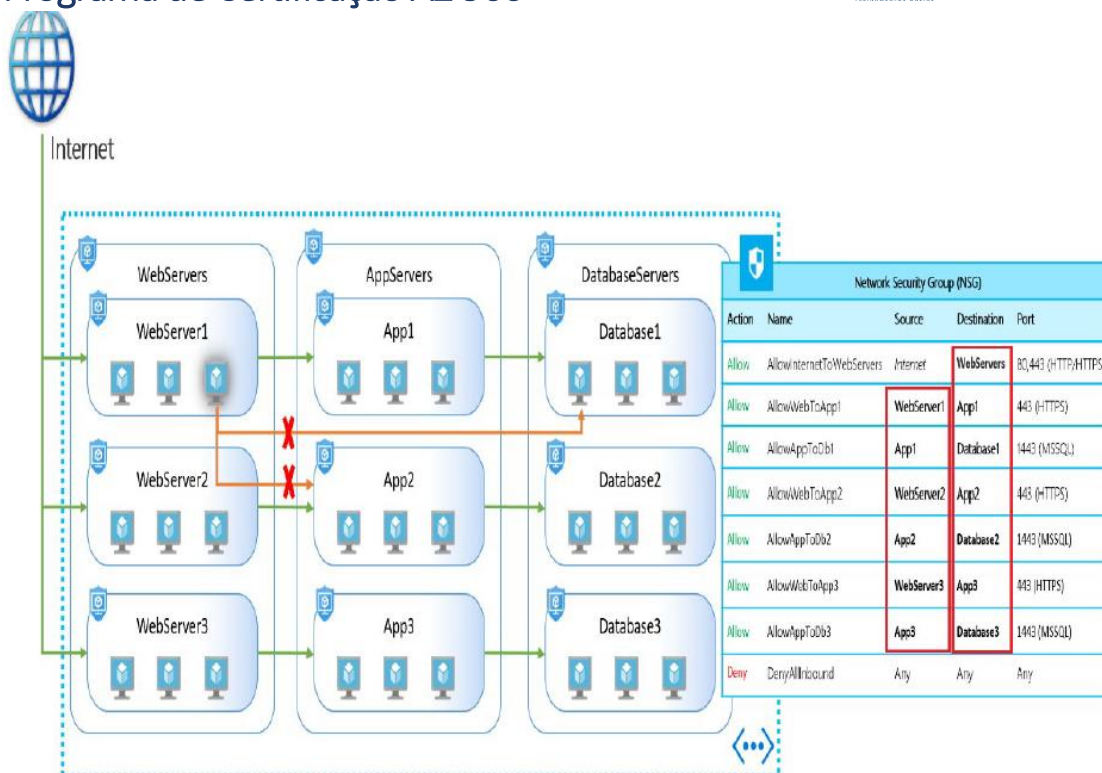
Os Application Security Groups permitem configurar a segurança da rede como uma extensão natural da estrutura de um aplicativo, permitindo agrupar máquinas virtuais e definir políticas de segurança de rede com base nesses grupos. Esse recurso permite reutilizar sua política de segurança em grande escala sem manutenção manual de endereços IP explícitos. A plataforma lida com a complexidade de endereços IP explícitos e vários conjuntos de regras, permitindo que você se concentre na sua lógica de negócios.

Exemplo

Um ASG permite agrupar servidores com requisitos semelhantes de filtragem de portas e agrupar servidores com funções semelhantes, como servidores Web. No exemplo abaixo, temos ASGs definidos para servidores da Web, AppServers e DbServers e setas verdes e vermelhas indicando quais caminhos de tráfego de rede são permitidos e quais não são.



No exemplo abaixo, vários aplicativos são implantados na mesma rede virtual. Com base nas regras de segurança descritas, as cargas de trabalho são isoladas uma da outra. Se uma VM de um dos aplicativos for comprometida, a exploração lateral será limitada, minimizando o impacto potencial de um invasor. Neste exemplo, vamos supor que uma das VMs do servidor Web do aplicativo1 esteja comprometida, o restante do aplicativo continuará protegido, mesmo o acesso a cargas de trabalho críticas, como servidores de banco de dados, ainda estará inacessível. Essa implementação fornece várias camadas extras de segurança à sua rede, tornando essa invasão menos prejudicial e fácil de reagir a esses eventos.



Os ASGs ajudam a simplificar como você pode filtrar e controlar o tráfego de rede que entra em sua organização e como esse tráfego de rede pode se mover. Eles permitem isolar várias cargas de trabalho e fornecer níveis adicionais de proteção para sua rede virtual de maneira mais fácil de gerenciar.

Escolhendo soluções de segurança de rede do Azure

Ao considerar sua solução de segurança do Azure, considere todos os elementos de defesa em profundidade.

Camada de perímetro

A camada de perímetro da rede visa proteger as organizações contra ataques baseados na rede contra seus recursos. Identificar esses ataques, alertar e eliminar seu impacto é importante para manter sua rede segura. Para fazer isso:

- Use a Proteção DDoS do Azure para filtrar ataques em larga escala antes que eles possam causar uma negação de serviço para os usuários finais.
- Use firewalls de perímetro com o Firewall do Azure para identificar e alertar sobre ataques maliciosos contra sua rede.

Camada de rede

Nesta camada, o foco é limitar a conectividade de rede em todos os seus recursos para permitir apenas o necessário. Segmente seus recursos e use controles no nível da rede para restringir a comunicação apenas ao necessário. Ao restringir a conectividade, você reduz o risco de movimento lateral em toda a sua rede devido a um ataque. Use NSGs

Programa de Certificação AZ-900

para criar regras sobre a comunicação de entrada e saída nesta camada. Como práticas recomendadas:

- Limite a comunicação entre recursos, segmentando sua rede e configurando controles de acesso.
- Negar por padrão.
- Restrinja o acesso à Internet de entrada e limite a saída, quando apropriado.
- Implementar conectividade segura para redes locais.

Combinando serviços

Você também pode combinar vários serviços de rede e segurança do Azure para gerenciar a segurança da rede e fornecer maior proteção em camadas. A seguir, exemplos de serviços combinados:

- **Network security groups and Azure Firewall.** O Firewall do Azure complementa a funcionalidade do grupo de segurança de rede. Juntos, eles fornecem melhor segurança de rede de defesa em profundidade. Os grupos de segurança de rede fornecem filtragem de tráfego de camada de rede distribuída para limitar o tráfego a recursos dentro de redes virtuais em cada assinatura. O Firewall do Azure é um firewall como serviço de rede centralizado e totalmente estável, que fornece proteção no nível da rede e de aplicativos em diferentes assinaturas e redes virtuais.
- **WAF do Gateway de Aplicativo e Firewall do Azure.** WAF é um recurso do Application Gateway que fornece aos aplicativos da Web proteção centralizada de entrada contra explorações e vulnerabilidades comuns. O Firewall do Azure fornece proteção de entrada para protocolos não HTTP / S (por exemplo, RDP, SSH, FTP), proteção no nível da rede de saída para todas as portas e protocolos e proteção no nível do aplicativo para HTTP / S de saída. A combinação de ambos fornece camadas adicionais de proteção.

Serviços principais de identidade do Azure

Autenticação e autorização

Dois conceitos fundamentais que precisam ser entendidos quando se fala em identidade e acesso são autenticação e autorização. Eles sustentam tudo o que acontece e ocorre sequencialmente em qualquer identidade e processo de acesso:

- **Autenticação.** Autenticação é o processo de estabelecer a identidade de uma pessoa ou serviço procurando acessar um recurso. Envolve o ato de desafiar uma parte por credenciais legítimas e fornece a base para a criação de um objeto de segurança para uso de identidade e controle de acesso. Estabelece se eles são quem eles dizem que são.
- **Autorização.** Autorização é o processo de estabelecer qual nível de acesso um servidor autenticado pessoa ou serviço possui. Ele especifica quais dados eles têm permissão para acessar e o que podem fazer com eles.

Azure Active Directory

Azure Active Directory (Azure AD)



O Azure Active Directory é um serviço de gerenciamento de acesso e identidade baseado em nuvem da Microsoft. Azure AD ajuda os funcionários de uma organização a entrar e acessar recursos:

Recursos externos podem incluir o Microsoft Office 365, o portal do Azure e milhares de outros aplicativos de software como serviço (SaaS).

Os recursos internos podem incluir aplicativos na sua rede corporativa e intranet, juntamente com qualquer nuvem aplicativos desenvolvidos por sua própria organização.

O Azure AD fornece serviços como:

Autenticação. Isso inclui verificar a identidade para acessar aplicativos e recursos e fornecer funcionalidade, como redefinição de senha de autoatendimento, autenticação multifator (MFA), um recurso banido lista de senhas e serviços de bloqueio inteligente.

Logon único (SSO). O SSO permite que os usuários se lembrem de apenas um ID e uma senha para acessar múltiplas aplicações. Uma única identidade está vinculada a um usuário, simplificando o modelo de segurança. Como usuários mudar de função ou deixar uma organização, as modificações de acesso estão vinculadas a essa identidade, reduzindo bastante o esforço necessário para alterar ou desativar contas.

Programa de Certificação AZ-900

Gerenciamento de aplicativos. Você pode gerenciar seus aplicativos em nuvem e locais usando o Azure AD Application Proxy, SSO, portal My apps (também conhecido como painel Access) e aplicativos SaaS.

Serviços de identidade entre empresas (B2B). Gerencie seus usuários convidados e parceiros externos enquanto mantendo o controle sobre seus próprios dados corporativos.

Serviços de identidade entre empresas (B2C). Personalize e controle como os usuários se inscrevem, fazem login e gerenciar seus perfis ao usar seus aplicativos com serviços.

Gerenciamento de dispositivos. Gerencie como sua nuvem ou dispositivos locais acessam seus dados corporativos.

O Azure AD se destina a:

Administradores de TI. Os administradores podem usar o Azure AD para controlar o acesso aos aplicativos e seus recursos, com base nos seus requisitos de negócios.

Desenvolvedores de aplicativos. Os desenvolvedores podem usar o Azure AD para fornecer uma abordagem baseada em padrões para adicionar funcionalidade aos aplicativos que você cria, como adicionar a funcionalidade Logon único a um aplicativo ou permitindo que um aplicativo trabalhe com credenciais preexistentes de um usuário e outras funcionalidades.

Assinantes do Microsoft 365, Microsoft Office 365, Azure ou Microsoft Dynamics CRM Online. Esses assinantes já estão usando o Azure AD. Cada Microsoft 365, Office 365, Azure e Dynamics. O inquilino do CRM Online é automaticamente um inquilino do Azure AD. Você pode começar imediatamente a gerenciar o acesso aos seus aplicativos em nuvem integrados usando o Azure AD.

Azure Multi-Factor Authentication (MFA)

A Autenticação Multifator do Azure fornece segurança adicional para suas identidades, exigindo duas ou mais elementos para autenticação completa. Esses elementos se enquadram em três categorias:

Algo que você sabe que pode ser uma senha ou a resposta para uma pergunta de segurança.

Algo que você possui pode ser um aplicativo móvel que recebe uma notificação ou um gerador de token dispositivo.

Algo que você é tipicamente algum tipo de propriedade biométrica, como impressão digital ou digitalização de rosto usado em muitos dispositivos móveis.



Programa de Certificação AZ-900

O uso do MFA aumenta a segurança da identidade, limitando o impacto da exposição de credenciais. Para se autenticar completamente, um invasor com a senha de usuário também precisaria possuir o telefone ou o telefone impressão digital, por exemplo. A autenticação com apenas um fator é insuficiente e, sem o MFA, um invasor não conseguiria usar essas credenciais para se autenticar. O MFA deve ser ativado sempre que possível, pois o MFA agrega enormes benefícios à segurança.

O MFA vem como parte das seguintes ofertas de serviços do Azure:

- **Licenças do Azure Active Directory Premium.** Essas licenças fornecem o uso completo do Azure Multi-Serviço de Autenticação por Fator (nuvem) ou Servidor de Autenticação Multifator do Azure (local).
- **Autenticação multifator para Office 365.** Um subconjunto dos recursos de Autenticação Multifator do Azure está disponível como parte da sua assinatura do Office 365.
- **Administradores globais do Azure Active Directory.** Como as contas globais de administrador são altamente sensíveis, um subconjunto dos recursos de Autenticação Multifator do Azure está disponível para proteger essas contas.

Ferramentas e recursos de segurança

Azure Security Center



O Azure Security Center é um serviço de monitoramento que fornece proteção contra ameaças em todos os seus serviços no Azure e no local. O Centro de Segurança pode:

- Forneça recomendações de segurança com base em suas configurações, recursos e redes.
- Monitore as configurações de segurança nas cargas de trabalho locais e na nuvem e aplique automaticamente os requisitos de segurança para novos serviços à medida que eles ficam online.
- Monitore continuamente todos os seus serviços e realize avaliações de segurança automáticas para identificar possíveis vulnerabilidades antes que possam ser exploradas.
- Use o aprendizado de máquina para detectar e impedir a instalação de malware em suas máquinas virtuais e Serviços. Você também pode definir uma lista de aplicativos permitidos para garantir que apenas os aplicativos validados possam executar.
- Análise e identifique possíveis ataques de entrada e ajude a investigar ameaças e qualquer pós-violação de atividade que possa ter ocorrido.

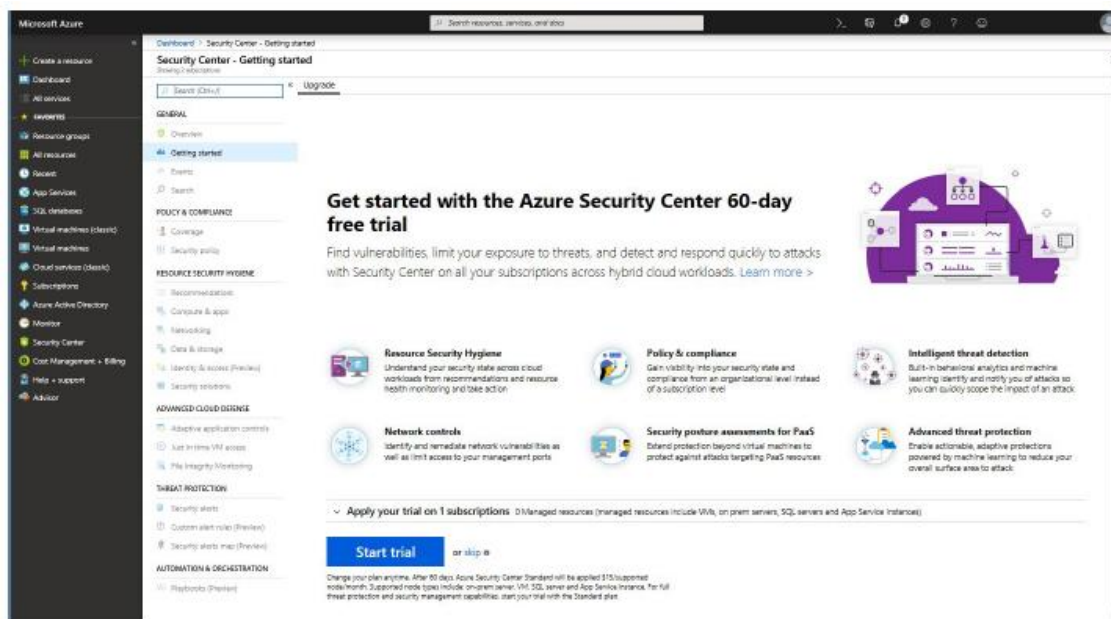
- Fornece controle de acesso just-in-time para portas, reduzindo sua superfície de ataque, assegurando que a rede permite apenas o tráfego necessário.

Versões da Central de Segurança do Azure A Central de Segurança do Azure está disponível em duas camadas:

Free. Disponível como parte da sua assinatura do Azure, esse nível é limitado a avaliações e recomendações apenas dos recursos do Azure.

Padrão. Essa camada fornece um conjunto completo de serviços relacionados à segurança, incluindo monitoramento contínuo, detecção de ameaças, controle de acesso just-in-time para portas e muito mais.

Para acessar o conjunto completo de serviços da Central de Segurança do Azure, você precisará atualizar para uma camada Padrão inscrição. Você pode acessar a avaliação gratuita de 30 dias no painel da Central de Segurança do Azure, no Portal do Azure.



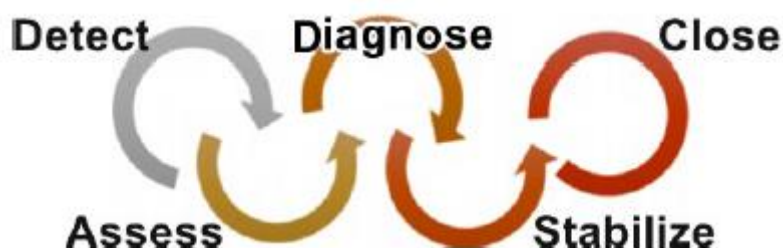
- Para atualizar uma assinatura para a camada Padrão, você deve ter a função de Proprietário da assinatura, Colaborador da assinatura ou Administrador de segurança.
- Após o término do período de avaliação de 30 dias, a Central de Segurança do Azure é precificada conforme detalhes na página de preços da Central de Segurança.

Azure Security Center cenários de uso

Você pode integrar o Security Center em seus fluxos de trabalho e usá-lo de várias maneiras. Aqui estão dois exemplos.

Exemplo 1 - Use o Centro de Segurança para uma resposta a incidentes.

Muitas organizações aprendem a responder a incidentes de segurança somente após sofrer um ataque. Reduzir custos e danos, é importante ter um plano de resposta a incidentes antes que ocorra um ataque. Você pode usar a Central de Segurança do Azure em diferentes estágios de uma resposta a incidentes.



Você pode usar o Centro de Segurança durante os estágios de detecção, avaliação e diagnóstico. Aqui estão exemplos de como o Security Center pode ser útil durante os três estágios iniciais de resposta a incidentes:

- **Detectar.** Revise a primeira indicação de uma investigação de evento. Por exemplo, use o Centro de Segurança painel para revisar a verificação inicial de que um alerta de segurança de alta prioridade foi gerado.
- **Avalie.** Execute a avaliação inicial para obter mais informações sobre a atividade suspeita. Por exemplo, obtenha mais informações sobre o alerta de segurança.
- **Diagnosticar.** Realizar uma investigação técnica e identificar contenção, atenuação e solução alternativa estratégias. Por exemplo, siga as etapas de correção descritas pela Central de Segurança nesse particular alerta de segurança.

Exemplo 2 - Use as recomendações da Central de Segurança para aumentar a segurança.

Você pode reduzir as chances de um evento de segurança significativo configurando uma política de segurança e, em seguida, implementar as recomendações fornecidas pela Central de Segurança do Azure.

Políticas de Segurança e recomendações

Uma política de segurança define o conjunto de controles recomendados para recursos dentro do especificado assinatura ou grupo de recursos. No Security Center, você define políticas de acordo com a sua empresa requisitos de segurança.

A Central de Segurança analisa o estado de segurança dos seus recursos do Azure. Quando o Centro de Segurança identifica vulnerabilidades de segurança em potencial, ele cria recomendações com base nos controles definidos na política. As recomendações orientam você no processo de configuração dos controles de segurança necessários.

Por exemplo, se você tiver cargas de trabalho que não exijam os Dados Transparentes do Azure SQL Database Transparent Data Encryption (TDE) (TDE), desative a política no nível da assinatura e ative-a apenas nos recursos grupos em que o SQL TDE é necessário.

Key Vault

Azure Key Vault

O Azure Key Vault é um serviço de nuvem centralizado para armazenar os segredos de seus aplicativos. O Key Vault ajuda você controle os segredos de seus aplicativos, mantendo-os em um único local central e fornecendo segurança acesso, controle de permissões e recursos de log de acesso.



Cenários de uso

- **Gerenciamento de secrets.** Você pode usar o Key Vault para armazenar e controlar com segurança o acesso a tokens, senhas, certificados, chaves da interface de programação de aplicativos (API) e outros segredos.
- **Gerenciamento de chaves.** Você também pode usar o Key Vault como uma solução de gerenciamento de chaves. O Key Vault torna É mais fácil criar e controlar as chaves de criptografia usadas para criptografar seus dados.
- **Gerenciamento de certificados.** O Key Vault permite provisionar, gerenciar e implantar seus serviços públicos e privados. Certificados SSL / TLS (Secure Sockets Layer / Transport Layer Security) para o Azure e internamente conectado, recursos mais facilmente.
- **Armazene segredos apoiados por módulos de segurança de hardware (HSMs).** Os segredos e chaves podem ser protegidos por software ou pelos HSMs validados pelo FIPS 140-2 Nível 2.

Principais benefícios do Vault

Os benefícios do uso do Key Vault incluem:

- **Segredos centralizados de aplicativos.** A centralização do armazenamento para segredos de aplicativos permite controlar sua distribuição e reduz as chances de vazamento acidental de segredos.
- **Segredos e chaves armazenados com segurança.** O Azure usa algoritmos padrão do setor, tamanhos de chave e HSMs, e o acesso requer autenticação e autorização adequadas.
- **Monitore o acesso e o uso.** Usando o Key Vault, você pode monitorar e controlar o acesso aos segredos da empresa.
- **Administração simplificada de segredos de aplicativos.** O Key Vault facilita o registro e a renovação certificados de autoridades de certificação públicas (CAs). Você também pode ampliar e replicar o conteúdo em regiões e use ferramentas padrão de gerenciamento de certificados.
- **Integre-se com outros serviços do Azure.** Você pode integrar o Key Vault a contas de armazenamento, contêineres registros, hubs de eventos e muitos mais serviços do Azure.

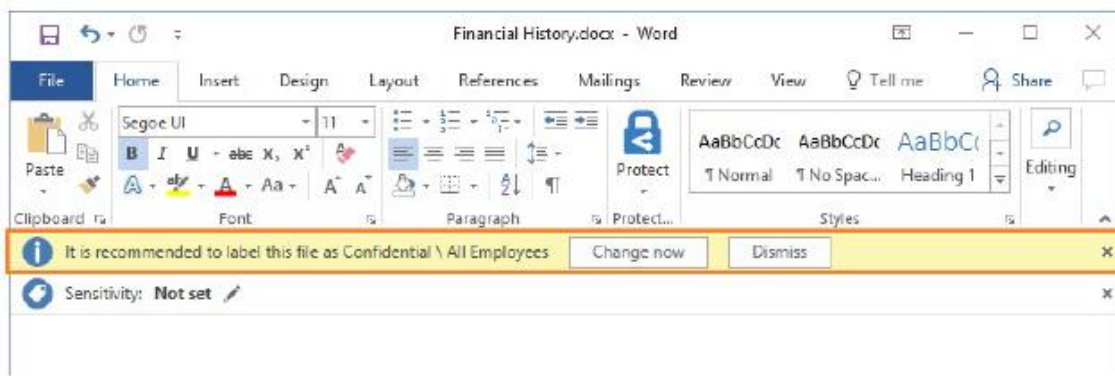
Azure Information Protection (AIP)



O Azure Information Protection é uma solução baseada em nuvem que ajuda as organizações a classificar e (opcionalmente) proteja seus documentos e e-mails aplicando etiquetas. As etiquetas podem ser aplicadas automaticamente (por administradores que definem regras e condições), manualmente (pelos usuários) ou com uma combinação de ambos (onde os usuários são guiados por recomendações).

Cenário de uso

A captura de tela a seguir é um exemplo de MSIP em ação no computador de um usuário. Neste exemplo, o administrador configurou um rótulo com regras que detectam dados confidenciais. Quando um usuário salva um Documento do Word que contém um número de cartão de crédito, uma dica de ferramenta personalizada é exibida. A dica de ferramenta recomenda rotular o arquivo como Confidencial / Todos os funcionários, que é um rótulo que o administrador configurou. Esta etiqueta classifica o documento e o protege.



Depois que seu conteúdo é classificado (e opcionalmente protegido), você pode acompanhar e controlar como o conteúdo é usado. Por exemplo, você pode analisar os fluxos de dados para obter informações sobre seus negócios; detectar comportamentos de risco e tomar medidas corretivas; rastrear o acesso a documentos; e evitar vazamento ou uso indevido de dados.

Proteção Avançada contra Ameaças (ATP) do Azure



A Proteção Avançada contra Ameaças do Azure¹⁴ é uma solução de segurança baseada em nuvem que identifica, detecta e ajuda a investigar ameaças avançadas, identidades comprometidas e ações internas maliciosas direcionadas a sua organização. O Azure ATP é capaz de detectar ataques e técnicas maliciosas conhecidas, segurança problemas e riscos na sua rede.

Componentes do Azure ATP

- **Portal ATP do Azure.** O Azure ATP possui seu próprio portal, através do qual você pode monitorar e responder a atividade suspeita. O portal do Azure ATP permite criar sua instância do Azure ATP e exibir os dados recebidos dos sensores do Azure ATP. Você também pode usar o portal para monitorar, gerenciar e investigar ameaças no seu ambiente de rede.
- **Azure ATP sensor.** Os sensores ATP do Azure são instalados diretamente nos controladores de domínio. O sensor monitora o tráfego do controlador de domínio sem exigir um servidor dedicado ou configurar o espelhamento de porta.
- **Azure ATP cloud service.** O serviço de nuvem ATP do Azure é executado na infraestrutura do Azure e está atualmente implantado nos Estados Unidos, Europa e Ásia. O serviço de nuvem ATP do Azure está conectado ao Microsoft gráfico de segurança inteligente.

Azure Advanced Threat Protection | contoso-corp | Timeline

4:04 PM Today

Honeytoken activity Updated OPEN

The following activities were performed by **Bob Minion**:

- Logged in to 2 computers via **Contoso-DC**.
- Authenticated from 2 computers using Kerberos when accessing 5 resources against **Contoso-DC**.
- Authenticated from **ITARGET-T4705** using NTLM against corporate resources via **Contoso-DC**.

Started at 3:08 PM Jan 22, 2018

3:23 PM Jan 22, 2018

Remote execution attempt detected OPEN

The following remote execution attempts were performed on **Contoso-DC** from **ALICE-DESKTOP**:

- Attempted remote execution of one or more WMI methods by **AdminUser**.

3:06 PM Jan 22, 2018

Suspicious service creation OPEN

AdminUser created 10 services in order to execute potentially malicious commands on **Contoso-DC**.

3:03 PM Jan 22, 2018

Brute force attack using LDAP simple bind OPEN

200 password guess attempts were made on 2 accounts from **ALICE-DESKTOP**. 2 account passwords were successfully guessed.

2:59 PM Jan 22, 2018

Reconnaissance using account enumeration OPEN

Suspicious account enumeration activity using Kerberos protocol, originating from **ALICE-DESKTOP**, was detected. The attacker performed a total of 101 guess attempts for account names. 2 guess attempts matched existing account names in Active Directory.

12:38 PM Jan 21, 2018

Malicious replication of directory services OPEN

Malicious replication requests were attempted by **Alice Liddel**, from **ALICE-DESKTOP** against **Contoso-DC**.

11:59 AM Jan 21, 2018

Reconnaissance using DNS OPEN

Suspicious DNS activity was observed, originating from **ALICE-DESKTOP** (which is not a DNS server) against **Contoso-DC**.

O ATP do Azure está disponível como parte do pacote Enterprise Mobility + Security 5 (SEM E5).

Metodologias de Governança do Azure

Azure Policy



Azure Policy é um serviço no Azure que você usa para criar, atribuir e gerenciar políticas. Essas políticas impõem regras e efeitos diferentes sobre seus recursos, para que esses recursos permaneçam em conformidade com seus padrões corporativos e acordos de nível de serviço (SLAs).

A Política do Azure faz isso usando políticas e iniciativas. Ele executa avaliações de seus recursos e verifica se há aqueles que não são compatíveis com as políticas que você criou. Por exemplo, você pode ter uma política para permitir apenas um determinado tamanho de SKU (unidade de manutenção de estoque) de máquinas virtuais (VMs) em seu ambiente. Depois de implementar Nesta política, ele avaliará os recursos ao criar ou atualizar os existentes. Também avalie seus recursos existentes.

A Política do Azure vem com várias definições internas de política e iniciativa que você pode usar, em categorias como Armazenamento, Rede, Computação, Centro de Segurança e Monitoramento.

A Política do Azure também pode se integrar ao Azure DevOps, aplicando qualquer integração e entrega contínuas políticas de pipeline que se aplicam à pré-implantação e pós-implantação de seus aplicativos.

A Política do Azure também pode corrigir automaticamente os recursos e configurações considerados não compatíveis, garantindo assim a integridade do estado dos recursos.

Implementando a Política do Azure

Existem três etapas para criar uma implementação de uma política do Azure.



Create a policy definition

Uma definição de política expressa o que avaliar e que ação tomar. Por exemplo, você pode impedir VMs sejam implantadas se expostas a um endereço IP público. Você também pode impedir um disco rígido de ser usado ao implantar VMs para controlar custos.

Toda definição de política possui condições sob as quais é aplicada. E, tem um efeito acompanhante que ocorre se as condições forem atendidas. Aqui estão alguns exemplos de definições de política:

- **SKUs de conta de armazenamento permitidos.** Essa definição de política possui um conjunto de condições / regras que determinam se uma conta de armazenamento que está sendo implantada está dentro de um conjunto de tamanhos de SKU. Seu efeito é negar tudo contas de armazenamento que não aderem ao conjunto de tamanhos de SKU definidos.
- **Tipo de recurso permitido.** Essa definição de política possui um conjunto de condições / regras para especificar o recurso tipos que sua organização pode implantar. Seu efeito é negar todos os recursos que não fazem parte desta lista definida.
- **Locais permitidos.** Esta política permite restringir os locais que sua organização pode especificar ao implantar recursos. Seu efeito é usado para impor seus requisitos de conformidade geográfica.
- **SKUs de máquina virtual permitidos.** Esta política permite especificar um conjunto de SKUs de VM que sua organização pode implantar.

Atribuir uma definição a um escopo de recursos

Para implementar suas definições de política, atribua-as aos recursos. Uma atribuição de política é uma política definição que foi designada para ocorrer dentro de um escopo específico. Esse escopo pode variar de grupo de gerenciamento para um grupo de recursos. As atribuições de política são herdadas por todos os recursos filho. Isso significa que, se uma política é aplicada a um grupo de recursos, ela é aplicada a todos os recursos desse recurso grupo. No entanto, você pode excluir um sub-escopo da atribuição de diretiva.

Análise os resultados da avaliação de políticas

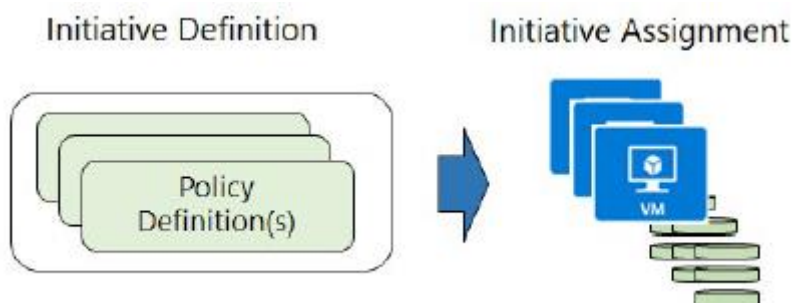
Quando uma condição é avaliada em relação aos recursos existentes, ela é marcada como compatível ou não.

Você pode revisar os resultados da política não conforme e executar as ações necessárias.

✓ A avaliação da política acontece uma vez por hora, o que significa que se você fizer alterações na sua política definição e criar uma atribuição de política, ela será reavaliada sobre seus recursos dentro de uma hora.

Policy Initiatives

Policy Initiatives trabalha com políticas do Azure.



Definições de iniciativa

Uma definição de iniciativa é um conjunto de definições de política para ajudar a rastrear seu estado de conformidade para um objetivo maior.

As atribuições de iniciativa reduzem a necessidade de fazer várias definições de iniciativa para cada escopo.

Por exemplo, você pode criar uma iniciativa chamada Habilitar Monitoramento na Central de Segurança do Azure, com uma meta para monitorar todas as recomendações de segurança disponíveis na Central de Segurança do Azure.

Sob essa iniciativa, você teria as seguintes definições de política:

- *Monitorar banco de dados SQL não criptografado na Central de Segurança* - Para monitorar bancos de dados SQL não criptografados e servidores.
- *Monitorar vulnerabilidades do SO na Central de Segurança* - Para monitorar servidores que não atendem aos requisitos configurados linha de base.
- *Monitorar o Endpoint Protection ausente na Central de Segurança* - Para monitorar servidores sem um dispositivo instalado agente de proteção de terminais.

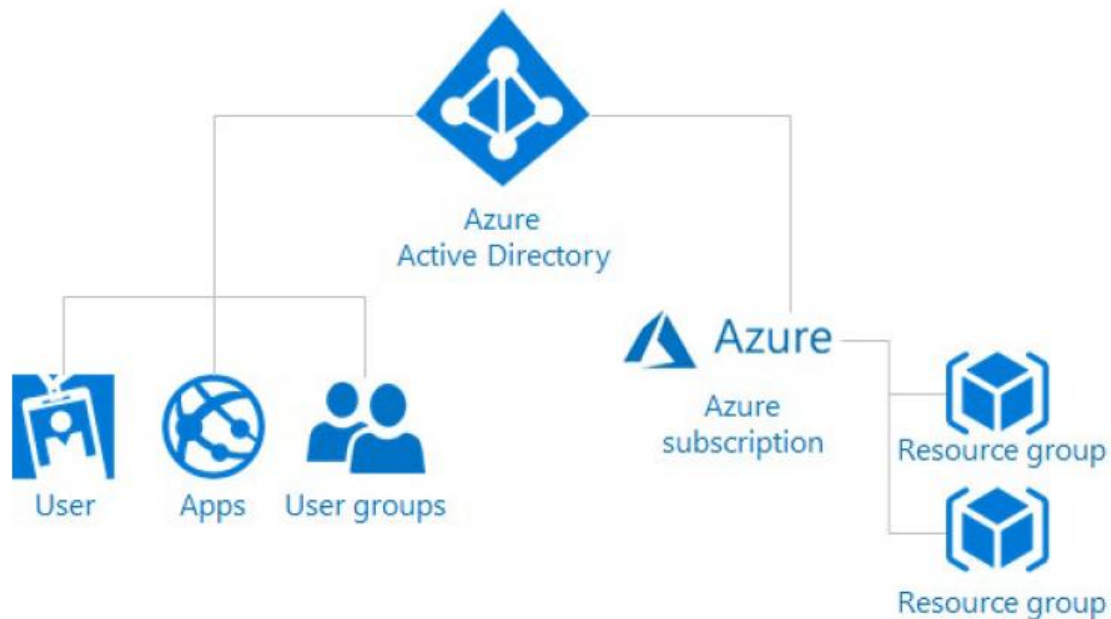
Atribuições da iniciativa

Como uma atribuição de política, uma atribuição de iniciativa é uma definição de iniciativa atribuída a um escopo específico.

As atribuições de iniciativa reduzem a necessidade de fazer várias definições de iniciativa para cada escopo. Este escopo também pode variar de um grupo de gerenciamento a um grupo de recursos.

✓ Mesmo que você tenha uma única política, recomendamos o uso de iniciativas se você aumentar o número de políticas ao longo do tempo.

Role-Based Access Control (RBAC)



O controle de acesso baseado em funções fornece gerenciamento de acesso refinado para recursos do Azure, permitindo você conceder aos usuários apenas os direitos necessários para executar seus trabalhos. O RBAC é fornecido sem custo adicional para todos os assinantes do Azure.

Cenários de uso

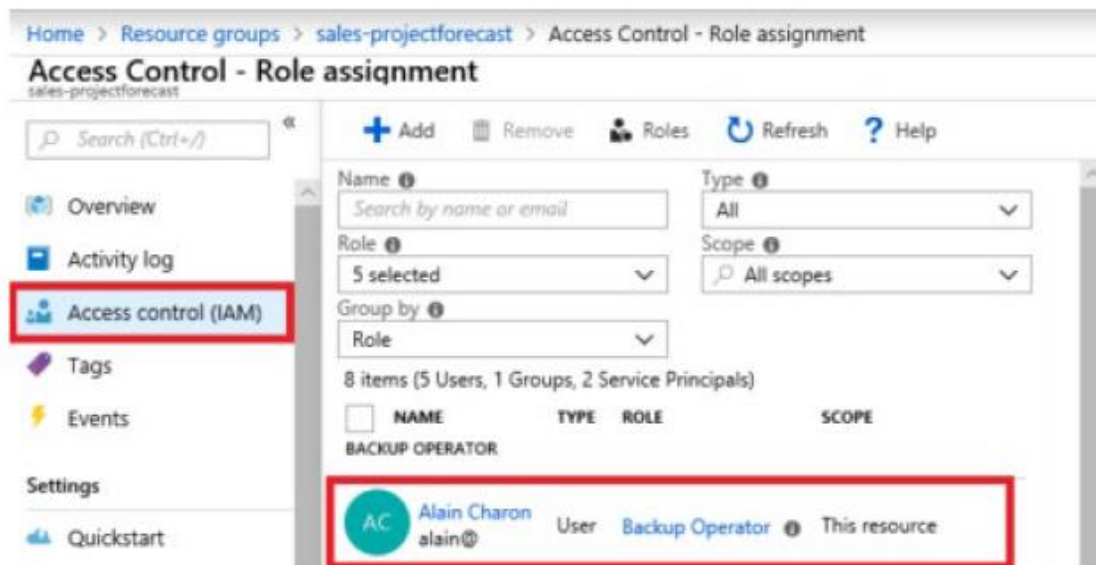
Exemplos de quando você pode usar o RBAC incluem quando você deseja:

Permitir que um usuário gerencie VMs em uma assinatura e outro usuário gerencie redes virtuais.

- Permitir que um grupo de administradores de banco de dados (DBA) gerencie bancos de dados SQL em uma assinatura.
- Permitir que um usuário gerencie todos os recursos em um grupo de recursos, como VMs, sites e sub-redes.
- Permitir que um aplicativo acesse todos os recursos em um grupo de recursos.

Para exibir permissões de acesso, acesse o painel Controle de Acesso (IAM) no portal do Azure. Essa lâmina mostra quem tem acesso a uma área e seu papel. Usando esse mesmo blade, você também pode conceder ou remover acesso.

A seguir, mostra um exemplo do painel Controle de Acesso (IAM) para um grupo de recursos. Neste exemplo, Alain Charon recebeu a função de Operador de Backup para este grupo de recursos.



O RBAC usa um modelo de permissão. Isso significa que, quando você recebe uma função, o RBAC permite que você execute determinadas ações, como ler, gravar ou excluir. Portanto, se uma atribuição de função conceder permissões de leitura para um grupo de recursos, e uma atribuição de função diferente concede permissões de gravação para o mesmo grupo de recursos, você terá permissões de gravação nesse grupo de recursos.

Melhores Práticas

A lista a seguir detalha as práticas recomendadas do RBAC:

- Usando o RBAC, separe tarefas na sua equipe e conceda apenas a quantidade de acesso aos usuários que eles precisam executar seus trabalhos. Em vez de conceder permissões irrestritas a todos no seu Azure assinatura ou recursos, permita apenas determinadas ações no nível do escopo.
- Ao planejar sua estratégia de controle de acesso, conceda aos usuários o nível de privilégio mais baixo necessário.

Resource locks

Bloqueios de recursos ajudam a impedir a exclusão ou modificação acidental de seus recursos do Azure. Você pode gerenciar esses bloqueios no portal do Azure. Para visualizar, adicionar ou excluir bloqueios, vá para o item CONFIGURAÇÕES seção do painel de configurações de qualquer recurso.

RG-Backup - Locks
Resource group

Add lock

Lock name	Lock type
RGLock ✓	Read-only
Notes	Delete

OK Cancel

Pode ser necessário bloquear uma assinatura, grupo de recursos ou recurso para impedir que outros usuários em sua organização acidentalmente excluir ou modificar recursos críticos. Você pode definir o nível de bloqueio como CanNotDelete ou ReadOnly:

- **CanNotDelete** significa que administradores autorizados ainda podem ler e modificar um recurso, mas não podem excluir o recurso.
- **ReadOnly** significa que administradores autorizados podem ler um recurso, mas não podem excluir ou atualizar o recurso. A aplicação desse bloqueio é como restringir todos os usuários autorizados às permissões concedidas pelo Reader role.

Blueprints do Azure



O Azure Blueprints²⁰ permite que os arquitetos em nuvem definam um conjunto repetível de recursos do Azure que implementam e aderem aos padrões, padrões e requisitos de uma organização. O Azure Blueprint permite que as equipes de desenvolvimento criem e implantem rapidamente novos ambientes com o conhecimento que eles estão criando dentro da conformidade organizacional com um conjunto de componentes internos que aceleram o desenvolvimento e a entrega. O Azure Blueprint é uma maneira declarativa de orquestrar a implantação de vários modelos de recursos e outros artefatos, como:

- Atribuições de função
- Atribuições de política
- Modelos do Azure Resource Manager
- Grupos de recursos

Processo do Blueprint

O processo de implementação do Azure Blueprint consiste nos seguintes itens de alto nível etapas:

1. Crie um Blueprint do Azure.
2. Atribua o blueprint.
3. Acompanhe as atribuições do blueprint.

Com o Azure Blueprint, a relação entre a definição do blueprint (o que deve ser implantado) e a atribuição do blueprint (o que foi implantado) é preservada. Essa conexão oferece suporte ao rastreamento e auditoria aprimorados da implantação.

Os Blueprints do Azure são diferentes dos Modelos do Azure Resource Manager. Quando os Modelos do Azure Resource Manager implantam recursos, eles não têm um relacionamento ativo com os recursos implantados (eles existem em um ambiente local ou no controle de origem). Por outro lado, com o Azure Blueprint, cada implantação está vinculada a um pacote do Azure Blueprint. Isso significa que o relacionamento com os recursos será mantido, mesmo após a implantação. Manter relacionamentos, dessa maneira, melhora os recursos de auditoria e rastreamento.

Cenário de uso

A adesão aos requisitos de segurança ou conformidade, sejam do governo ou do setor, pode ser difícil e demorada. Para ajudá-lo na auditoria, rastreabilidade e conformidade com suas implantações, use os artefatos e ferramentas do Azure Blueprint. A papelada demorada não é mais necessária e seu caminho para a certificação é acelerado. O Azure Blueprint também é útil nos cenários do Azure DevOps, onde os blueprints são associados a artefatos de compilação específicos e pipelines de lançamento e podem ser rastreados com mais rigor.

Governança de assinaturas

Discutiremos e definiremos as assinaturas com mais detalhes posteriormente no curso, no entanto, desejamos mencioná-las brevemente aqui no contexto da governança. Existem principalmente três aspectos a serem considerados em relação à criação e gerenciamento de assinaturas: Faturamento, Controle de acesso e limites de assinatura.

- **Billing:** os relatórios podem ser gerados por assinaturas. Se você tiver vários departamentos internos e precisar fazer um estorno, um cenário possível é criar assinaturas por departamento ou projeto.
- **Controle de acesso:** uma assinatura é um limite de implantação para os recursos do Azure e toda assinatura é associada a um inquilino do Azure AD que fornece aos administradores a capacidade de configurar o RBAC (controle de acesso baseado em função). Ao projetar um modelo de assinatura, deve-se considerar o fator de

Programa de Certificação AZ-900

limite de implantação, alguns clientes têm assinaturas separadas para Desenvolvimento e Produção, cada um completamente isolado um do outro da perspectiva de recursos e gerenciado usando o RBAC.

- **Limites de assinatura:** as assinaturas também estão vinculadas a algumas limitações rígidas. Por exemplo, o número máximo de circuitos da Rota Express por assinatura é 10. Esses limites devem ser considerados durante a fase de design, se houver necessidade de ultrapassar esses limites em cenários específicos, então poderão ser necessárias assinaturas adicionais. Se você atingir um limite rígido, não há flexibilidade.

Também estão disponíveis para ajudar no gerenciamento de assinaturas grupos de gerenciamento, que gerenciam acesso, políticas e conformidade em várias assinaturas do Azure. Discutiremos isso com mais detalhes posteriormente.

Monitoramento e geração de relatórios no Azure

Tags

Você aplica Tags aos recursos do Azure, fornecendo metadados para organizá-los logicamente em uma taxonomia. Cada tag consiste em um nome e um par de valores. Por exemplo, você pode aplicar o nome Ambiente e o valor Produção a todos os recursos em produção ou marcar pelos departamentos da empresa. Por exemplo, o nome do departamento com um valor de TI.

Name	Value
Environment	Production
Department	IT

Depois de aplicar as tags, você pode recuperar todos os recursos em sua assinatura com esse nome e valor. As tags permitem recuperar recursos relacionados de diferentes grupos de recursos. Essa abordagem é útil quando você precisa organizar recursos para cobrança ou gerenciamento.

Limitações de tags

Existem algumas limitações no uso de tags, como:

- Nem todos os tipos de recursos suportam tags.
- Cada recurso ou grupo de recursos pode ter no máximo 50 pares de nome / valor de tag. Atualmente, as contas de armazenamento suportam apenas 15 tags, mas esse limite será aumentado para 50 em uma versão futura. Se você precisar aplicar mais tags que o número máximo permitido, use uma sequência JSON para o valor da tag. A cadeia JSON pode conter muitos valores aplicados a um único nome de tag. Um grupo de recursos pode conter muitos recursos, cada um com 50 pares de nome / valor de marca.
- O nome da tag é limitado a 512 caracteres e o valor da tag é limitado a 256 caracteres. Para contas de armazenamento, o nome da marca é limitado a 128 caracteres e o valor da marca é limitado a 256 caracteres.
- Máquinas virtuais e conjuntos de dimensionamento de máquinas virtuais são limitados a um total de 2048 caracteres para todos os nomes e valores de tags.
- As tags aplicadas ao grupo de recursos não são herdadas pelos recursos desse grupo de recursos.

✓ Você pode usar a Política do Azure para impor tags e regras de marcação de recursos.

Azure Monitor



O **Azure Monitor** maximiza a disponibilidade e o desempenho de seus aplicativos, fornecendo uma solução abrangente para coletar, analisar e atuar na telemetria de seus ambientes na nuvem e no local. Ajuda a entender o desempenho de seus aplicativos e identifica proativamente os problemas que os afetam e os recursos dos quais dependem.

Quais dados o Azure Monitor coleta? O Azure Monitor pode coletar dados de várias fontes. Você pode pensar em monitorar dados para seus aplicativos em camadas que vão desde seu aplicativo, qualquer sistema operacional e serviços em que ele confia, até a própria plataforma. O Azure Monitor coleta dados de cada uma das seguintes camadas:

- **Dados de monitoramento de aplicativos:** dados sobre o desempenho e a funcionalidade do código que você escreveu, independentemente da plataforma.
- **Dados de monitoramento do SO convidado:** Dados sobre o sistema operacional no qual seu aplicativo está sendo executado. Isso pode estar em execução no Azure, outra nuvem ou local.
- **Dados de monitoramento de recursos do Azure:** dados sobre a operação de um recurso do Azure.
- **Dados de monitoramento de assinatura do Azure:** dados sobre a operação e gerenciamento de uma assinatura do Azure, bem como dados sobre a integridade e operação do próprio Azure.
- **Dados de monitoramento do tenant do Azure:** dados sobre a operação de serviços do Azure em nível de inquilino, como o Azure Active Directory.

Configurações de diagnóstico

Assim que você cria uma assinatura do Azure e começa a adicionar recursos como máquinas virtuais e aplicativos Web, o Azure Monitor começa a coletar dados.

- **Os logs de atividades** registram quando os recursos são criados ou modificados.
- **As métricas** informam o desempenho do recurso e os recursos consumidos.

Ativando os diagnósticos

Você pode estender os dados que você está coletando para a operação real dos recursos, ativando os diagnósticos e adicionando um agente para calcular recursos. Nas configurações de recurso, você pode ativar o Diagnóstico

- **Ativar o monitoramento em nível de convidado**
- **Contadores de desempenho:** colete dados de desempenho
- **Logs de eventos:** habilite vários logs de eventos

Programa de Certificação AZ-900



- **Crash Dumps:** habilite ou desabilite
- **Dissipadores:** envie seus dados de diagnóstico para outros serviços para obter mais análises.
- **Agente:** defina as configurações do agente Serviço.

Azure Health Service



O Azure Service Health é um conjunto de experiências que podem orientar e oferecer suporte personalizado quando problemas com os serviços do Azure afetam você. Ele pode notificar, ativar e entender o impacto dos problemas e recuperar o upgrade à medida do problema resolvido. O Azure Service Health também pode usar e preparar a manutenção planejada e alterações que podem afetar a disponibilidade de seus recursos. A Integridade do Serviço do Azure é composta pelo seguinte:

O Azure Status fornece uma visão global do estado de integridade dos serviços do Azure. Com o Status do Azure, você pode obter informações atualizadas sobre a disponibilidade do serviço. Todos têm acesso ao Status do Azure e podem exibir todos os serviços que estão relacionados ao seu estado de integridade.

O Service Health selecionou um painel personalizável que rastreia ou o estado dos seus serviços do Azure nas regiões em que você usa. Nesse painel, você pode rastrear eventos ativos, como problemas de serviço em andamento, manutenção planejada futura ou avisos de integridade relevante. Quando os eventos se tornam inativos, eles são proibidos no seu histórico de saúde por até 90 dias. Por fim, você pode usar o painel de Integridade do Serviço para criar e gerenciar alertas de Integridade do serviço, que notifica você sempre que houver problemas de serviço que afetem.

O Resource Health de ajuda para diagnosticar e obter suporte quando um problema de serviço do Azure afeta seus recursos. Ele fornece detalhes sobre o estado atual e o passado de seus recursos. Ele também fornece suporte técnico para usuários com problemas de mitigação. Em contraste com o Status do Azure, que informa sobre problemas de serviço que afetam um conjunto amplo de clientes do Azure, uma Integridade de Recursos fornecidos como painel personalizado pela integridade de seus recursos. A Integridade dos Recursos mostra os horários em que seus recursos estavam indisponíveis devido a problemas de serviço do Azure. É mais fácil entender se um SLA foi violado.

Juntos, os componentes de Integridade do Serviço do Azure permitem uma visão abrangente do status de integridade do Azure, sem nível de granularidade mais relevante para você.

Monitorando aplicativos e serviços

O monitoramento de dados é útil apenas para melhorar sua visibilidade das operações no seu ambiente de computação. O Azure Monitor inclui vários recursos e ferramentas que incluem informações valiosas sobre seus aplicativos e os outros recursos dos quais eles podem depender. Como soluções e recursos de monitoramento, como Application Insights e Container Insights, acesse uma visão mais detalhada dos diferentes aspectos do aplicativo e dos serviços do Azure.

Os recursos do Azure Monitor podem ser organizados em quatro categorias, essas categorias são: Analisar, Responder, Visualizar e Integrar.

Analisar

- **O Application Insights** é um serviço que monitora a disponibilidade, o desempenho e o uso de seus aplicativos Web, estejam eles hospedados na nuvem ou no local. Ele aproveita a poderosa plataforma de análise de dados no Log Analytics para fornecer informações mais detalhadas sobre as operações do seu aplicativo. O Application Insights pode diagnosticar erros, sem esperar que um usuário os relate. O Application Insights inclui pontos de conexão com uma variedade de ferramentas de desenvolvimento e se integra ao Microsoft Visual Studio para dar suporte aos processos do DevOps.
- **O Monitor do Azure** para contêineres é um serviço projetado para monitorar o desempenho de cargas de trabalho de contêiner, implantadas em clusters Kubernetes gerenciados hospedados no Serviço de Kubernetes do Azure (AKS). Ele oferece visibilidade do desempenho, coletando métricas de memória e processador de controladores, nós e contêineres, disponíveis no Kubernetes por meio da API de métricas. Os logs do contêiner também são coletados.
- **O Azure Monitor for VMs** é um serviço que monitora suas VMs do Azure em escala, analisando o desempenho e a integridade de suas VMs Windows e Linux (incluindo os diferentes processos e dependências interconectadas de outros recursos e processos externos). O Azure Monitor para VMs inclui suporte para monitorar dependências de aplicativos e desempenho para VMs hospedadas no local e para VMs hospedadas com outros provedores de nuvem.

A integração de um ou todos esses serviços de monitoramento ao Azure Service Health tem benefícios adicionais. Manter-se informado sobre o status de integridade dos serviços do Azure ajudará você a entender se e quando um problema que afeta um serviço do Azure está afetando seu ambiente. O que pode parecer um problema localizado pode ser o resultado de um problema mais amplo, e o Azure Service Health fornece esse tipo de insight. A Integridade do Serviço do Azure identifica quaisquer problemas nos serviços do Azure que possam afetar seu aplicativo. O Azure Service Health também ajuda a planejar a manutenção agendada.

Responder

Além de permitir que você analise seus dados de monitoramento interativamente, uma solução de monitoramento eficaz deve responder proativamente a quaisquer condições críticas identificadas nos dados que ele coleta. Isso pode envolver, por exemplo, o envio de um texto ou email para um administrador responsável por investigar um problema ou o lançamento de um processo automatizado que tenta corrigir uma condição de erro.

- **Alertas.** O Azure Monitor notifica proativamente você sobre condições críticas usando Alertas e pode potencialmente tentar executar ações corretivas. As regras de alerta baseadas em métricas podem fornecer alertas quase em tempo real, com base em valores numéricos. Regras de alerta baseadas em logs permitem lógica complexa entre dados, de várias fontes.
- **Escala automática.** O Azure Monitor usa a Escala Automática para garantir que você tenha a quantidade certa de recursos em execução para gerenciar a carga no seu aplicativo com eficiência. A escala automática permite criar regras que usam métricas, coletadas pelo Azure Monitor, para determinar quando adicionar recursos automaticamente para lidar com aumentos de carga. A escala automática também pode ajudar a reduzir os custos do Azure, removendo recursos que não estão sendo usados. Você pode especificar um número mínimo e máximo de instâncias e fornecer a lógica que determina quando a Escala Automática deve aumentar ou diminuir os recursos.

Visualizar

visualizações, como gráficos e tabelas, são ferramentas eficazes para resumir dados de monitoramento e apresentar dados a diferentes públicos. O Azure Monitor possui seus próprios recursos para visualizar dados de monitoramento e aproveita outros serviços do Azure para publicar dados para diferentes públicos. Outras ferramentas que você pode usar para visualizar dados, para públicos e cenários específicos, incluem:

- Painéis
- Exibições
- Power BI

Integração

Geralmente, você precisa integrar o Azure Monitor a outros sistemas e criar soluções personalizadas que usam seus dados de monitoramento. Outros serviços do Azure podem trabalhar com o Azure Monitor para fornecer essa integração.

Padrões de privacidade, conformidade e proteção de dados

Termos e requisitos de conformidade

Ao selecionar um provedor de nuvem para hospedar suas soluções, você deve entender como esse fornecedor pode ajudá-lo a cumprir regulamentos e normas. Algumas perguntas a serem feitas sobre um provedor em potencial incluem:

- Quão compatível é o provedor de nuvem quando se trata de manipular dados confidenciais?
- Qual é a conformidade dos serviços oferecidos pelo provedor de nuvem?
- Como posso implantar minhas próprias soluções baseadas em nuvem em cenários com requisitos de credenciamento ou conformidade?

A Microsoft investe fortemente no desenvolvimento de processos de conformidade robustos e inovadores. A estrutura de conformidade da Microsoft para serviços online mapeia os controles para vários padrões regulatórios. Isso permite que a Microsoft projete e construa serviços usando um conjunto comum de controles, simplificando a conformidade através de uma série de regulamentos hoje e à medida que evoluem no futuro. Embora a imagem a seguir não seja uma lista completa de ofertas de conformidade, ela fornecerá uma ideia do nível de ofertas de conformidade disponíveis no Azure.

Global	<input checked="" type="checkbox"/> ISO 27001:2013	<input checked="" type="checkbox"/> ISO 22301:2012	<input checked="" type="checkbox"/> SOC 1 Type 2	<input checked="" type="checkbox"/> CSA STAR Certification
	<input checked="" type="checkbox"/> ISO 27017:2015	<input checked="" type="checkbox"/> ISO 9001:2015	<input checked="" type="checkbox"/> SOC 2 Type 2	<input checked="" type="checkbox"/> CSA STAR Attestation
	<input checked="" type="checkbox"/> ISO 27018:2014	<input checked="" type="checkbox"/> ISO 20000-1:2011	<input checked="" type="checkbox"/> SOC 3	<input checked="" type="checkbox"/> CSA STAR Self-Assessment
US Gov	<input checked="" type="checkbox"/> FedRAMP High	<input checked="" type="checkbox"/> DFARS	<input checked="" type="checkbox"/> DoE 10 CFR Part 810	<input checked="" type="checkbox"/> WCAG 2.0 (ISO 40500:2012)
	<input checked="" type="checkbox"/> FedRAMP Moderate	<input checked="" type="checkbox"/> DoD DISA SRG Level 5	<input checked="" type="checkbox"/> NIST SP 800-171	<input checked="" type="checkbox"/> FIPS 140-2
	<input checked="" type="checkbox"/> EAR	<input checked="" type="checkbox"/> DoD DISA SRG Level 4	<input checked="" type="checkbox"/> NIST CSF	<input checked="" type="checkbox"/> ITAR
Industry	<input checked="" type="checkbox"/> PCI DSS Level 1	<input checked="" type="checkbox"/> DoD DISA SRG Level 2	<input checked="" type="checkbox"/> Section 508 VPATs	<input checked="" type="checkbox"/> CJIS
	<input checked="" type="checkbox"/> GLBA	<input checked="" type="checkbox"/> FCA (UK)	<input checked="" type="checkbox"/> 21 CFR Part 11 (GxP)	<input checked="" type="checkbox"/> IRS 1075
	<input checked="" type="checkbox"/> FFIEC	<input checked="" type="checkbox"/> MAS + ABS (Singapore)	<input checked="" type="checkbox"/> MARS-E	<input checked="" type="checkbox"/> CDSA
Regional	<input checked="" type="checkbox"/> Shared Assessments	<input checked="" type="checkbox"/> 23 NYCRR 500	<input checked="" type="checkbox"/> NHS IG Toolkit (UK)	<input checked="" type="checkbox"/> MPAA
	<input checked="" type="checkbox"/> FISC (Japan)	<input checked="" type="checkbox"/> HIPAA BAA	<input checked="" type="checkbox"/> NEN 7510:2011 (Netherlands)	<input checked="" type="checkbox"/> DPP (UK)
	<input checked="" type="checkbox"/> APRA (Australia)	<input checked="" type="checkbox"/> HITRUST	<input checked="" type="checkbox"/> FERPA	<input checked="" type="checkbox"/> FACT (UK)
	<input checked="" type="checkbox"/> Argentina PDPA	<input checked="" type="checkbox"/> China TRUCS / CCCPPF	<input checked="" type="checkbox"/> Germany IT-Grundschutz	<input checked="" type="checkbox"/> SOX
	<input checked="" type="checkbox"/> Australia IRAP Unclassified	<input checked="" type="checkbox"/> EN 301 549	<input checked="" type="checkbox"/> India MeitY	<input checked="" type="checkbox"/> Singapore MTCS Level 3
	<input checked="" type="checkbox"/> Australia IRAP PROTECTED	<input checked="" type="checkbox"/> EU ENISA IAF	<input checked="" type="checkbox"/> Japan CS Mark Gold	<input checked="" type="checkbox"/> Spain ENS
	<input checked="" type="checkbox"/> Canada Privacy Laws	<input checked="" type="checkbox"/> EU Model Clauses	<input checked="" type="checkbox"/> Japan My Number Act	<input checked="" type="checkbox"/> Spain DPA
	<input checked="" type="checkbox"/> China GB 18030:2005	<input checked="" type="checkbox"/> EU – US Privacy Shield	<input checked="" type="checkbox"/> Netherlands BIR 2012	<input checked="" type="checkbox"/> UK Cyber Essentials Plus
	<input checked="" type="checkbox"/> China DJCP (MLPS) Level 3	<input checked="" type="checkbox"/> Germany C5	<input checked="" type="checkbox"/> New Zealand Gov CC	<input checked="" type="checkbox"/> UK G-Cloud
				<input checked="" type="checkbox"/> UK PASF

Ofertas de conformidade:

A lista a seguir fornece detalhes sobre algumas das ofertas de conformidade disponíveis no Azure:

- **CJIS.** Qualquer estado ou agência local dos EUA que deseje acessar o banco de dados dos Serviços de Informações sobre Justiça Criminal (CJIS) do FBI deve aderir à Política de Segurança do CJIS. O Azure é o único grande provedor de nuvem que

Programa de Certificação AZ-900



se compromete contratualmente a cumprir a Política de Segurança CJIS, que compromete a Microsoft a cumprir os mesmos requisitos que as entidades policiais e de segurança pública devem atender.

- **Certificação CSA STAR.** O Azure, Intune e Microsoft Power BI obtiveram a certificação STAR, que envolve uma rigorosa avaliação independente de terceiros da postura de segurança de um provedor de nuvem. Esta certificação STAR baseia-se na obtenção da certificação ISO / IEC 27001 e no atendimento aos critérios especificados no CCM. Isso demonstra que um provedor de serviços em nuvem está em conformidade com os requisitos aplicáveis a ISO / IEC 27001, abordou questões críticas à segurança da nuvem, conforme descrito no CCM, e foi avaliada em relação ao STAR Capability Maturity Model para o gerenciamento de atividades nas áreas de controle do CCM.
- **Regulamento Geral de Proteção de Dados (GDPR).** Em 25 de maio de 2018, uma lei de privacidade europeia - GDPR - está em vigor. O GDPR impõe novas regras a empresas, agências governamentais, organizações sem fins lucrativos e outras organizações que oferecem bens e serviços a pessoas na União Europeia (UE) ou que coletam e analisam dados vinculados a residentes na UE. O GDPR se aplica independentemente da sua localização.
- **Cláusulas modelo da UE.** A Microsoft oferece aos clientes cláusulas contratuais padrão da UE que fornecem garantias contratuais sobre transferências de dados pessoais para fora da UE. A Microsoft é a primeira empresa a receber aprovação conjunta do Grupo de Trabalho do Artigo 29 da UE que as proteções contratuais de privacidade que o Azure oferece aos clientes corporativos em nuvem atendem aos padrões atuais da UE para transferências internacionais de dados. Isso garante que os clientes do Azure possam usar os serviços da Microsoft para mover dados livremente através da nuvem da Microsoft da Europa para o resto do mundo.
- **HIPAA.** A Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA) é uma lei federal dos EUA que regula as Informações de Saúde Protegidas (PHI) dos pacientes. O Azure oferece aos clientes um Contrato de Associado de Negócios HIPAA (BAA), estipulando a adesão a determinadas disposições de segurança e privacidade no HIPAA e na Lei HITECH. Para ajudar os clientes em seus esforços individuais de conformidade, a Microsoft oferece um BAA para os clientes do Azure como um adendo de contrato.
- **ISO / IEC 27018.** A Microsoft é o primeiro provedor de nuvem a adotar o código de práticas ISO / IEC 27018, cobrindo o processamento de informações pessoais por provedores de serviços em nuvem.
- **Segurança na nuvem em várias camadas (MTCS) em Cingapura.** Após avaliações rigorosas conduzidas pelo Organismo de Certificação MTCS, os serviços em nuvem da Microsoft receberam a Certificação MTCS 584: 2013 nas três classificações de serviço - Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e SaaS. A Microsoft foi o primeiro provedor de soluções em nuvem (CSP) a receber essa certificação nas três classificações.

Programa de Certificação AZ-900



- **Controles da organização de serviço (SOC) 1, 2 e 3.** Os serviços em nuvem cobertos pela Microsoft são auditados pelo menos anualmente na estrutura de relatórios do SOC por auditores independentes. A auditoria dos serviços em nuvem da Microsoft abrange controles de segurança, disponibilidade, integridade do processamento e confidencialidade dos dados, conforme aplicável aos princípios de confiança no escopo de cada serviço.
- **Estrutura de segurança cibernética do Instituto Nacional de Padrões e Tecnologia (NIST).** O NSIT CSF é uma Estrutura voluntária que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos relacionados à segurança cibernética. Os serviços em nuvem da Microsoft foram submetidos a auditorias moderadas e altas, independentes e de alto nível, do Federal Management Program (FedRAMP) e são certificadas de acordo com os padrões FedRAMP. Além disso, por meio de uma avaliação validada realizada pela Health Information Trust Alliance (HITRUST), uma organização líder em desenvolvimento e acreditação de padrões de segurança e privacidade, o Office 365 é certificado para os objetivos especificados no NIST CSF.
- **G-Cloud do governo do Reino Unido.** O governo do Reino Unido G-Cloud é uma certificação de computação em nuvem para serviços usados por entidades governamentais no Reino Unido. O Azure recebeu credenciamento oficial do credenciador do governo do Reino Unido.

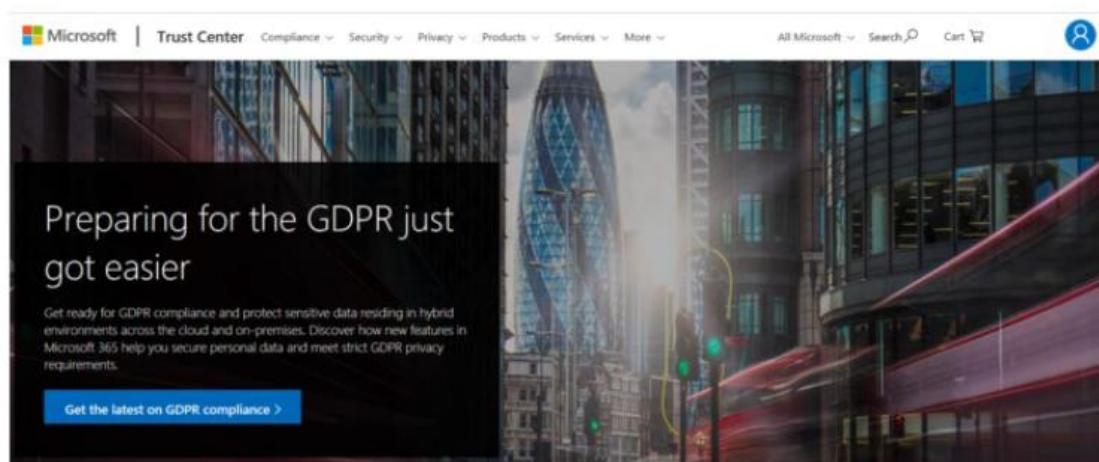
✓ A Microsoft fornece o conjunto mais abrangente de ofertas de conformidade (incluindo certificações e atestados) de qualquer provedor de serviços em nuvem.

Declaração de Privacidade da Microsoft

A declaração de privacidade da Microsoft explica quais dados pessoais a Microsoft processa, como a Microsoft os processa e com que finalidades. Esta declaração de privacidade explica os dados pessoais que a Microsoft processa, como a Microsoft os processa e com que finalidades. A Microsoft oferece uma ampla gama de produtos, incluindo produtos de servidor usados para ajudar a operar empresas em todo o mundo, dispositivos que você usa em sua casa, software que os alunos usam na escola e desenvolvedores de serviços para criar e hospedar o que vem a seguir. As referências aos produtos da Microsoft nesta declaração incluem serviços, sites, aplicativos, software, servidores e dispositivos da Microsoft. Leia os detalhes específicos do produto nesta declaração de privacidade, que fornecem informações adicionais relevantes. Esta declaração se aplica às interações que a Microsoft mantém com você e os produtos Microsoft listados abaixo, bem como com outros produtos Microsoft que exibem esta declaração.

Central de Confiabilidade

O Trust Center é um recurso do site que contém informações e detalhes sobre como a Microsoft implementa e suporta segurança, privacidade, conformidade e transparência em todos os produtos e serviços em nuvem da Microsoft. O Trust Center é uma parte importante da Microsoft Trusted Cloud Initiative e fornece suporte e recursos para a comunidade legal e de conformidade.



O site da Central de Confiabilidade fornece:

- Informações detalhadas sobre segurança, privacidade, ofertas de conformidade, políticas, recursos e práticas nos produtos em nuvem da Microsoft.
- Recursos recomendados na forma de uma lista com curadoria dos recursos mais aplicáveis e amplamente utilizados para cada tópico.
- Informações específicas para as principais funções organizacionais, incluindo gerentes de negócios, administradores de inquilinos ou equipes de segurança de dados, responsáveis pela avaliação de riscos e privacidade e equipes de conformidade legal.
- Pesquisa de documentos entre empresas, que será lançada em breve e permitirá que os clientes existentes de serviços em nuvem pesquisem o Service Trust Portal.
- Orientação e suporte diretos para quando você não encontrar o que está procurando.

Portal de Confiança de Serviço

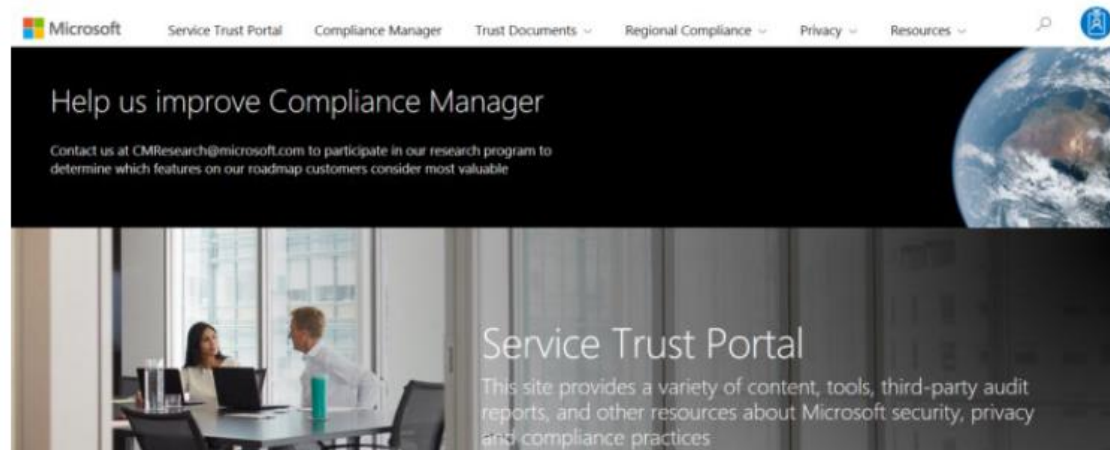
O Portal de Confiança de Serviço (STP) hospeda o serviço Gerenciador de Conformidade e é o site público da Microsoft para publicação de relatórios de auditoria e outras informações relacionadas à conformidade relevantes para os serviços em nuvem da Microsoft. Os usuários do STP podem baixar relatórios de auditoria produzidos por auditores externos e obter informações de relatórios criados pela Microsoft, que fornecem detalhes sobre como a Microsoft cria e opera seus serviços em nuvem.

Programa de Certificação AZ-900



O STP também inclui informações sobre como os serviços online da Microsoft podem ajudar sua organização a manter e rastrear a conformidade com padrões, leis e regulamentos, como:

- ISO
- SOC
- NIST
- FedRAMP
- GDPR



O STP é um recurso complementar da Central de Confiabilidade e permite:

- Acessar relatórios de auditoria nos serviços de nuvem da Microsoft em uma única página.
- Acesse os guias de conformidade para ajudá-lo a entender como você pode usar os recursos do serviço de nuvem da Microsoft para gerenciar a conformidade com vários regulamentos.
- Acesse documentos confiáveis para ajudar você a entender como os serviços em nuvem da Microsoft ajudam a proteger seus dados.

Acessando o STP

Para acessar alguns materiais do STP, você deve entrar como um usuário autenticado com sua conta de serviços em nuvem da Microsoft (uma conta da organização do Azure AD ou uma conta da Microsoft) e depois revisar e aceitar o Contrato de Não Divulgação de Materiais de Conformidade da Microsoft.

Os clientes existentes podem acessar o STP na página do Service Trust Portal, com uma das seguintes assinaturas online (avaliação ou paga):

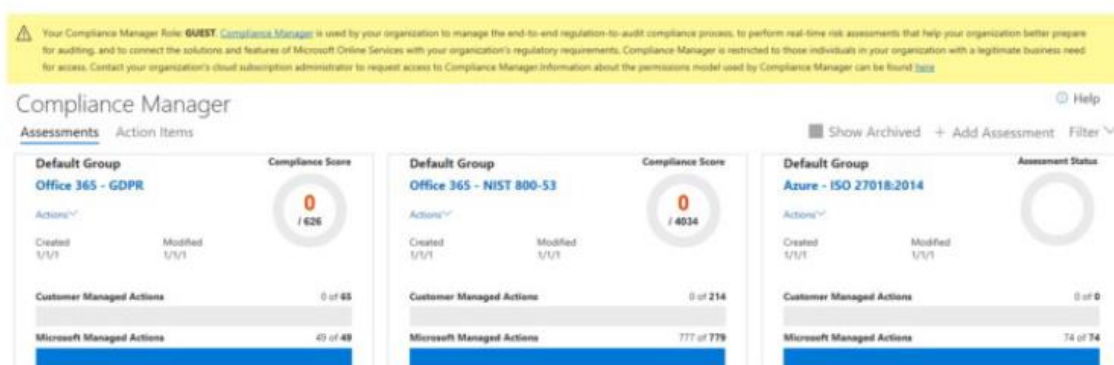
- Office 365
- Dynamics 365
- AZURE

Gerenciador de conformidade

O Compliance Manager é um painel de avaliação de risco baseado em fluxo de trabalho no Trust Portal que permite rastrear, atribuir e verificar as atividades de conformidade regulamentar da sua organização relacionadas aos serviços profissionais da Microsoft e serviços em nuvem da Microsoft, como o Office 365, Dynamics 365 e Azure.

O Compliance Manager fornece os seguintes recursos:

- Informações detalhadas fornecidas pela Microsoft a auditores e reguladores, como parte de várias auditorias de terceiros dos serviços em nuvem da Microsoft em relação a vários padrões (por exemplo, ISO 27001, ISO 27018 e NIST).
- Informações que a Microsoft compila internamente para conformidade com regulamentos (como HIPAA e GDPR da UE).
- Autoavaliação de uma organização quanto à sua própria conformidade com esses padrões e regulamentações.
- Permite atribuir, rastrear e registrar atividades relacionadas à conformidade e avaliação, o que pode ajudar sua organização a atravessar as barreiras da equipe para atingir as metas de conformidade da organização.
- Fornece uma pontuação de conformidade para ajudá-lo a acompanhar o seu progresso e priorizar os controles de auditoria que ajudarão a reduzir a exposição da organização ao risco.
- Fornece um repositório seguro no qual fazer upload e gerenciar evidências e outros artefatos relacionados às atividades de conformidade.
- Produz relatórios detalhados no Microsoft Excel que documentam as atividades de conformidade realizadas pela Microsoft e sua organização, que podem ser fornecidas aos auditores, reguladores e outras partes interessadas na conformidade.



O Compliance Manager fornece avaliações de risco em andamento com uma referência de pontuação baseada em risco exibida em uma exibição de painel para regulamentos e normas. Como alternativa, você pode criar avaliações para os regulamentos ou padrões que são mais importantes para sua organização.

Como parte da avaliação de riscos, o Compliance Manager também fornece as ações recomendadas que você pode executar para melhorar sua conformidade regulatória. Você pode visualizar todos os itens de ação ou selecionar os itens de ação que correspondem a uma certificação específica.

✓ O Compliance Manager é um painel que fornece um resumo da proteção de dados e estatura de conformidade e recomendações para melhorar a proteção e conformidade de dados. As ações do cliente fornecidas no Compliance Manager são apenas recomendações; cabe a cada organização avaliar a eficácia dessas recomendações em seu respectivo ambiente regulatório antes da implementação. As recomendações encontradas no Gerente de conformidade não devem ser interpretadas como uma garantia de conformidade.

Azure Government services

O Azure Government services é uma instância separada do serviço do Microsoft Azure. Ele atende às necessidades de segurança e conformidade das agências federais dos EUA, governos estaduais e locais e seus fornecedores de soluções. O Governo do Azure oferece isolamento físico de implantações fora dos EUA e fornece pessoal dos EUA rastreado.

Azure Government services tratam dados que estão sujeitos a certos regulamentos e requisitos governamentais, como FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4 e CJIS. Para fornecer o mais alto nível de segurança e conformidade, o Governo do Azure usa datacenters e redes fisicamente isolados (localizados apenas nos EUA).

Os clientes do Governo do Azure (governo federal, estadual e local dos EUA ou seus parceiros) estão sujeitos à validação da elegibilidade. Azure Government services fornece a conformidade mais ampla e a aprovação do Departamento de Defesa (DoD) de nível 5. Você pode escolher entre seis regiões de data center exclusivas do governo, incluindo duas regiões com uma Autorização Provisória de Nível 5 de Impacto. O Azure Government services também oferece as mais certificações de conformidade de qualquer provedor de nuvem.

Azure China 21 Vianet

Azure China é operado pela 21Vianet (Azure China 21Vianet) é uma instância fisicamente separada de serviços em nuvem localizados na China, operados e transacionados independentemente pela Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), uma subsidiária integral da Beijing 21Vianet Broadband Data Center Co., Ltd.

Os serviços do Azure são baseados nas mesmas tecnologias do Azure, Office 365 e Power BI que compõem o serviço de nuvem global da Microsoft, com níveis de serviço comparáveis. Acordos e contratos para o Azure na China, onde aplicável, são assinados entre os clientes e a 21Vianet.

Como o primeiro provedor de serviços de nuvem pública estrangeira oferecido na China, em conformidade com os regulamentos governamentais, o Azure China 21Vianet fornece segurança de classe mundial, conforme discutido no Trust Center, conforme exigido pelos regulamentos chineses para todos os sistemas e aplicativos criados em sua arquitetura.

O Azure inclui os principais componentes de IaaS, PaaS e SaaS. Esses componentes incluem rede, armazenamento, gerenciamento de dados, gerenciamento de identidades e muitos outros serviços.

O Azure China 21Vianet suporta a maioria dos mesmos serviços que o Azure global possui, como replicação de dados geossíncronos e dimensionamento automático. Mesmo se você já usa serviços globais do Azure, para operar na China, pode ser necessário re-hospedar ou refatorar alguns ou todos os seus aplicativos ou serviços.

De acordo com o Regulamento de telecomunicações da China (em chinês), os provedores de serviços em nuvem (IaaS e PaaS) devem ter permissões de telecomunicações de valor agregado. Somente empresas registradas localmente com menos de 50% de investimento estrangeiro se qualificam para essas licenças. Para cumprir esse regulamento, o serviço Azure na China é operado pela 21Vianet, com base nas tecnologias licenciadas pela Microsoft.

Revisão – Questões Módulo 03

Review Question 1

Which of the following could grant or deny access based on the originating IP address?

- A. Azure Active Directory
- B. Fixed workloads
- C. Unpredictable costs

Review Question 2

Which of the following could require both a password and a security question for full authentication?

- A. Azure Active Directory
- B. Fixed workloads
- C. Unpredictable costs

Review Question 3

Which of the following services would you use to filter internet traffic in your Azure virtual network?

- A. Azure Firewall
- B. Network Security Group
- C. VPN Gateway

Review Question 4

Which of the following lets you store passwords in Azure so you can centrally manage them for your services and applications?

- A. Azure Advanced Threat Protection
- B. Azure Key Vault
- C. Azure Security Center

Review Question 5

Which of the following should you use to download published audit reports and how Microsoft builds and operates its cloud services?

- A. Azure Policy
- B. Azure Service Health
- C. Service Trust Portal

Review Question 6

Which of the following provides information about planned maintenance and changes that could affect the availability of your resources?

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Service Health

Review Question 7

Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?

- A. Microsoft Privacy Statement
- B. Compliance Manager
- C. Azure Service Health

Review Question 8

Which of the following can be used to help you enforce resource tagging so you can manage billing?

- A. Azure Policy
- B. Azure Service Health
- C. Compliance Manager

Review Question 9

Which of the following can be used to define a repeatable set of Azure resources that implement organizational requirements?

- A. Azure Blueprint
- B. Azure Policy
- C. Azure Resource Groups

Review Question 10

Which of the following lets you grant users only the rights they need to perform their jobs?

- A. Azure Policy
- B. Compliance Manager
- C. Role-Based Access Control

Resumo do Módulo 3

Neste módulo, você aprendeu sobre a segurança da conectividade de rede no Azure, serviços de identidade, ferramentas e recursos de segurança, metodologias de governança do Azure, monitoramento e relatórios no Azure e padrões de privacidade, conformidade e proteção de dados no Azure.

Protegendo a conectividade de rede no Azure

Nesta lição, você aprendeu sobre os Firewalls do Azure, a proteção DDos do Azure, os NSGs e a escolha do Azure soluções de segurança de rede.

Serviços de identidade do Azure

Nesta lição, você aprendeu sobre autenticação e autorização, Azure AD e MFA. Ferramentas e recursos de segurança Nesta lição, você aprendeu sobre a Central de Segurança do Azure e alguns cenários de uso, Key Vault, MSIP, e Azure ATP.

Metodologias de governança do Azure

Nesta lição, você aprendeu sobre a Política, políticas, iniciativas, RBAC, bloqueios, Azure Advisor, segurança do Azure assistência e Azure Blueprint.

Monitorando e relatórios no Azure

Nesta lição, você aprendeu sobre o Azure Monitor e o Azure Service Health.

Padrões de privacidade, conformidade e proteção de dados no Azure

Nesta lição, você aprendeu sobre os termos e requisitos de conformidade, a Declaração de Privacidade da Microsoft, Central de Confiabilidade, Portal de Confiança de Serviço, Gerenciador de Conformidade, Governo do Azure e Azure China.

Revisão de respostas

Questão 1: Azure Firewall

Explicação: *O Firewall do Azure concede acesso ao servidor com base no endereço IP de origem de cada solicitação. Você cria regras de firewall que especificam intervalos de endereços IP. Somente clientes desses endereços IP concedidos serão ter permissão para acessar o servidor. As regras do firewall também incluem informações de porta e protocolo de rede específicas.*

Questão 2: Multi-Factor Authentication

Explicação: *O MFA pode exigir dois ou mais elementos para autenticação completa.*

Questão 3: Network Security Group

Explicação: *Os NSGs permitem filtrar o tráfego de rede de e para recursos do Azure em um Rede virtual do Azure. Um NSG pode conter várias regras de segurança de entrada e saída que permitem que você para filtrar o tráfego de e para recursos por endereço IP, porta e protocolo de origem e destino.*

Questão 4: Azure Key Vault

Explicação: *O Azure Key Vault é um serviço de nuvem centralizado para armazenar os segredos de seus aplicativos. Azure Key Vault ajuda a controlar os segredos de seus aplicativos, mantendo-os em um único local central e fornecendo acesso seguro, controle de permissões e recursos de log de acesso.*

Questão 5: Services Trust Portal

Explicação: *O Service Trust Portal é o site público da Microsoft para publicação de relatórios de auditoria e outras informações relacionadas à conformidade relevantes para os serviços em nuvem da Microsoft. Usuários do STP podem baixar auditoria relatórios produzidos por auditores externos e obtenha informações de relatórios criados pela Microsoft que fornecem detalhes sobre como a Microsoft cria e opera seus serviços em nuvem.*

Questão 6: Azure Service Health

Explicação: *O Azure Service Health é um conjunto de experiências que fornece orientação personalizada e suporte quando problemas com os serviços do Azure afetam você. Ele pode notificá-lo, ajudá-lo a entender o impacto de e mantenha-o atualizado à medida que o problema for resolvido. O Azure Service Health também pode ajudar você a se preparar para manutenção planejada e alterações que podem afetar a disponibilidade de seus recursos.*

Questão 7: Microsoft Privacy Statement

Explicação: *A Declaração de Privacidade da Microsoft explica quais dados pessoais a Microsoft processa, como a Microsoft a processa e para quais fins.*

Questão 8: Azure Policy

Explicação: *Azure Policy pode ser usada para impor valores e regras de marcação de recursos.*

Questão 9: Azure Blueprint

Explicação: *Azure Blueprints permitem que os arquitetos em nuvem definam um conjunto repetível de recursos do Azure que implementar e aderir aos padrões, padrões e requisitos de uma organização. O Azure Blueprint permite equipes de desenvolvimento para criar e implantar rapidamente novos ambientes com o conhecimento que eles estão construindo dentro da conformidade organizacional com um conjunto de componentes internos que aceleram o desenvolvimento e a entrega.*

Questão 10: Role-Based Access Control

Explicação: *Controle de acesso baseado em função (RBAC). O RBAC permite conceder aos usuários apenas os direitos necessários para executar seus jobs.*