## caso de uso (**A Contoso, Ltd.**

**Pergunta #203**

Informações introdutórias Estudo de caso -  
  
Para iniciar o estudo de caso -  
Para exibir a primeira questão neste estudo de caso, clique no botão Avançar. Use os botões no painel esquerdo para explorar o conteúdo do estudo de caso antes de responder às perguntas. Clicar nesses botões exibe informações como requisitos de negócios, ambiente existente e declarações de problemas. Se o estudo de caso tiver uma guia Todas as informações, observe que as informações exibidas são idênticas às informações exibidas nas guias subsequentes. Quando estiver pronto para responder a uma pergunta, clique no botão Pergunta para retornar à pergunta.  
  
Visão geral -  
**A Contoso, Ltd.** é uma empresa de pesquisa que tem um escritório principal em Montreal.  
  
Ambiente existente -  
  
Ambiente técnico -  
A rede local contém um único domínio do Active Directory chamado contoso.com.  
A Contoso tem uma única assinatura do Azure.  
  
Parcerias comerciais -  
A Contoso tem uma parceria comercial com a Fabrikam, Inc. Os usuários da Fabrikam acessam alguns aplicativos da Contoso pela Internet usando  
contas de convidado do Azure Active Directory (Azure AD).  
  
Requisitos -  
  
Alterações planejadas -  
A Contoso planeja implantar dois aplicativos chamados App1 e App2 no Azure.  
  
App1 -  
O App1 será um aplicativo da Web Python hospedado no Azure App Service que requer um tempo de execução do Linux. Os usuários da Contoso e da Fabrikam acessarão o App1.  
O App1 acessará vários serviços que exigem credenciais de terceiros e sequências de acesso. As credenciais e as strings de acesso são armazenadas no Azure Key Vault.  
O App1 terá seis instâncias: três na região do Azure East US e três na região do Azure West Europe.  
O App1 tem os seguintes requisitos de dados:  
Cada instância gravará dados em um armazenamento de dados na mesma zona de disponibilidade da instância.  
Os dados gravados por qualquer instância do App1 devem ser visíveis para todas as instâncias do App1.  
O App1 só poderá ser acessado pela Internet. O App1 tem os seguintes requisitos de conexão:  
As conexões com o App1 devem passar por um firewall de aplicativo da Web (WAF).  
As conexões com o App1 devem ter balanceamento de carga ativo-ativo entre as instâncias.  
Todas as conexões com o App1 da América do Norte devem ser direcionadas para a região Leste dos EUA. Todas as outras conexões devem ser direcionadas para a região Oeste da Europa.  
A cada hora, você executará uma tarefa de manutenção invocando um script do PowerShell que copia arquivos de todas as instâncias do App1. O script do PowerShell será executado de um local central.  
  
App2 -  
O App2 será um aplicativo .NET hospedado no App Service que requer um tempo de execução do Windows. O App2 tem os seguintes requisitos de armazenamento de arquivos:  
Salvar arquivos em uma conta do Azure Storage.  
Replique arquivos para um local local.  
Garanta que os clientes locais possam ler os arquivos pela LAN usando o protocolo SMB.  
Você precisa monitorar o App2 para analisar quanto tempo leva para executar diferentes transações no aplicativo. A solução não deve exigir alterações no código do aplicativo.  
Requisitos de desenvolvimento de aplicativos  
Os desenvolvedores de aplicativos desenvolverão constantemente novas versões do App1 e do App2. O processo de desenvolvimento deve atender aos seguintes requisitos:  
Uma instância de preparo de uma nova versão do aplicativo deve ser implantada no host do aplicativo antes que a nova versão seja usada na produção.  
Após testar a nova versão, a versão de preparo do aplicativo substituirá a versão de produção.  
  
A mudança para a nova versão do aplicativo de preparo para produção deve ocorrer sem qualquer tempo de inatividade do aplicativo.  
  
Requisitos de identidade -  
A Contoso identifica os seguintes requisitos para gerenciar o acesso da Fabrikam aos recursos:  
Todo mês, um gerente de conta na Fabrikam deve revisar quais usuários da Fabrikam têm permissões de acesso ao App1. Contas que não precisam mais de permissões devem ser removidas como convidados.  
A solução deve minimizar o esforço de desenvolvimento.  
  
Requisito de segurança -  
Todos os segredos usados pelos serviços do Azure devem ser armazenados no Azure Key Vault.  
Os serviços que exigem credenciais devem ter as credenciais vinculadas à instância do serviço. As credenciais NÃO devem ser compartilhadas entre os serviços. Pergunta Você precisa recomendar uma solução para a tarefa de manutenção do App1. A solução deve minimizar os custos.  
O que você deve incluir na recomendação?

1. um aplicativo lógico do Azure
2. uma função do Azure
3. uma máquina virtual do Azure
4. um WebJob de serviço de aplicativo

A cada hora, você executará uma tarefa de manutenção invocando um script do PowerShell que copia arquivos de todas as instâncias do App1. O script do PowerShell será executado de um local central.  
O App1 terá seis instâncias: três na região do Azure East US e três na região do Azure West Europe.  
Você pode criar e gerenciar fluxos de trabalho com o Azure PowerShell no Azure Logic Apps.  
Você pode criar um aplicativo lógico de consumo no Azure Logic Apps multilocatário usando o arquivo JSON para uma definição de fluxo de trabalho do aplicativo lógico. Você pode então gerenciar seu aplicativo lógico executando os cmdlets no módulo Az.LogicApp PowerShell.  
Referência:  
<https://docs.microsoft.com/en-us/azure/logic-apps/quickstart-logic-apps-azure-powershell>

**Pergunta #204**

Informações introdutórias Estudo de caso -  
  
Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.  
  
Pergunta Você precisa recomendar uma solução que atenda aos requisitos de desenvolvimento do aplicativo.  
O que você deve incluir na recomendação?

1. o serviço de configuração de aplicativo do Azure
2. uma instância do Registro de Contêiner do Azure
3. slots de implantação
4. Fontes de Integração Contínua/Implantação Contínua (CI/CD)

Ao implantar seu aplicativo Web, aplicativo Web no Linux, back-end móvel ou aplicativo de API no Azure App Service, você pode usar um slot de implantação separado em vez do slot de produção padrão quando estiver executando no nível de plano Standard, Premium ou Isolated App Service. Os slots de implantação são aplicativos ativos com seus próprios nomes de host.  
Os elementos de conteúdo e configurações do aplicativo podem ser trocados entre dois slots de implantação, incluindo o slot de produção.  
Implantar seu aplicativo em um slot de não produção tem os seguintes benefícios:  
\* Você pode validar as alterações do aplicativo em um slot de implantação de preparo antes de trocá-lo pelo slot de produção.  
\* Implantar um aplicativo em um slot primeiro e trocá-lo para produção garante que todas as instâncias do slot sejam aquecidas antes de serem trocadas para produção.  
Isso elimina o tempo de inatividade quando você implanta seu aplicativo.  
\* Após uma troca, o slot com o aplicativo previamente preparado agora tem o aplicativo de produção anterior. Se as alterações trocadas para o slot de produção não forem como você espera, você pode executar a mesma troca imediatamente para obter seu "último site bom conhecido" de volta.  
Observação: Requisitos de desenvolvimento de aplicativos  
Os desenvolvedores de aplicativos desenvolverão constantemente novas versões do App1 e do App2. O processo de desenvolvimento deve atender aos seguintes requisitos:  
ג€¢ Uma instância de preparo de uma nova versão do aplicativo deve ser implantada no host do aplicativo antes que a nova versão seja usada na produção.  
ג€¢ Após testar a nova versão, a versão de preparo do aplicativo substituirá a versão de produção.  
ג€¢ A mudança para a nova versão do aplicativo de preparo para produção deve ocorrer sem nenhum tempo de inatividade do aplicativo.  
Referência:  
<https://docs.microsoft.com/en-us/azure/app-service/deploy-staging-slots>

**Pergunta #205**

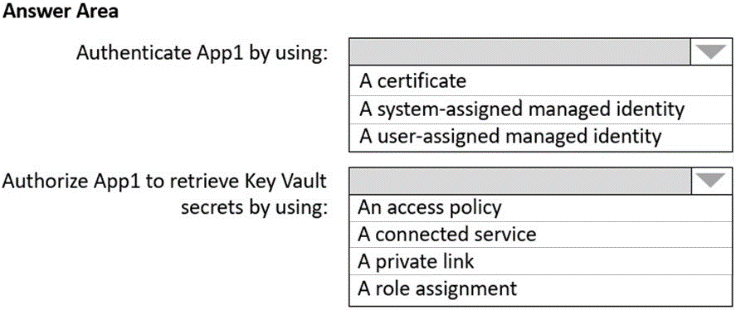
Informações introdutórias Estudo de caso -  
  
Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.  
  
Pergunta Você precisa recomendar uma arquitetura do App Service que atenda aos requisitos do App1. A solução deve minimizar os custos.  
O que você deve recomendar?

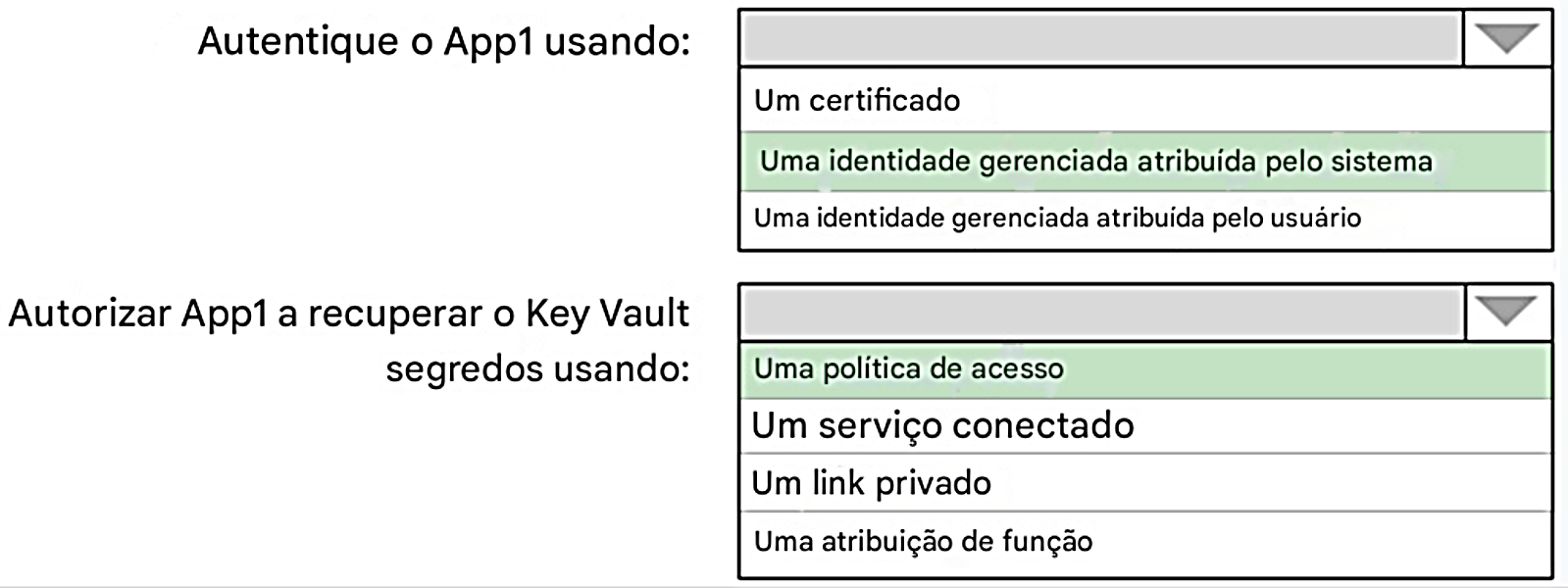
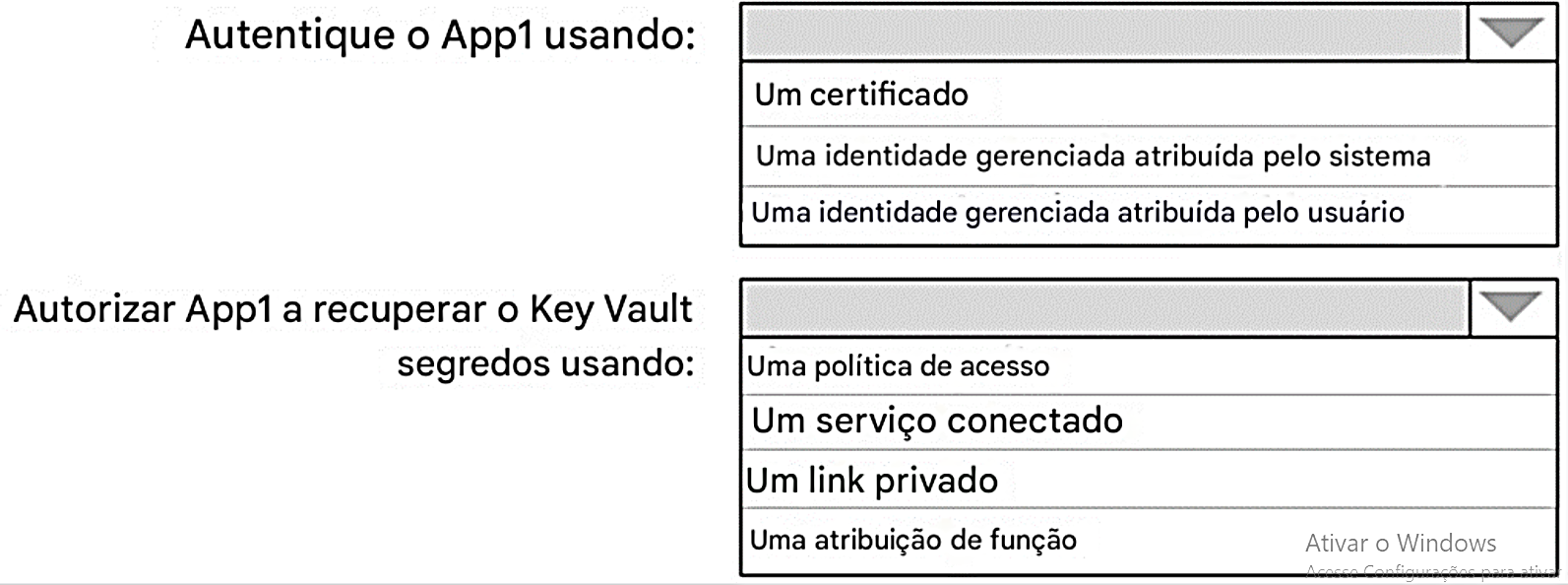
1. um App Service Environment (ASE) por zona de disponibilidade
2. um App Service Environment (ASE) por região
3. um plano de serviço de aplicativo por região
4. um plano de serviço de aplicativo por zona de disponibilidade

O App1 tem os seguintes requisitos de dados:  
Cada instância gravará dados em um repositório de dados na mesma zona de disponibilidade que a instância.  
Os dados gravados por qualquer instância do App1 devem ser visíveis para todas as instâncias do App1.  
Observação: o Azure App Service Environment v2 é um recurso do Azure App Service que fornece um ambiente totalmente isolado e dedicado para executar  
aplicativos do App Service com segurança em alta escala.  
Os clientes podem criar vários ASEs em uma única região do Azure ou em várias regiões do Azure. Essa flexibilidade torna os ASEs ideais para dimensionar horizontalmente camadas de aplicativos sem estado em suporte a altas cargas de trabalho de solicitações por segundo (RPS).  
Referência:  
<https://docs.microsoft.com/en-us/azure/app-service/environment/intro>

**Pergunta #206**

Informações introdutórias Estudo de caso –

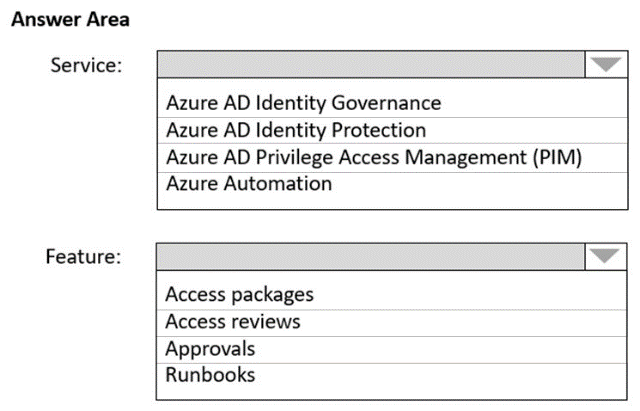
Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.  
  
pergunta você precisa recomendar uma solução para garantir que o App1 possa acessar as credenciais de terceiros e as sequências de acesso. A solução deve atender aos requisitos de segurança.  
O que você deve incluir na recomendação?   
  


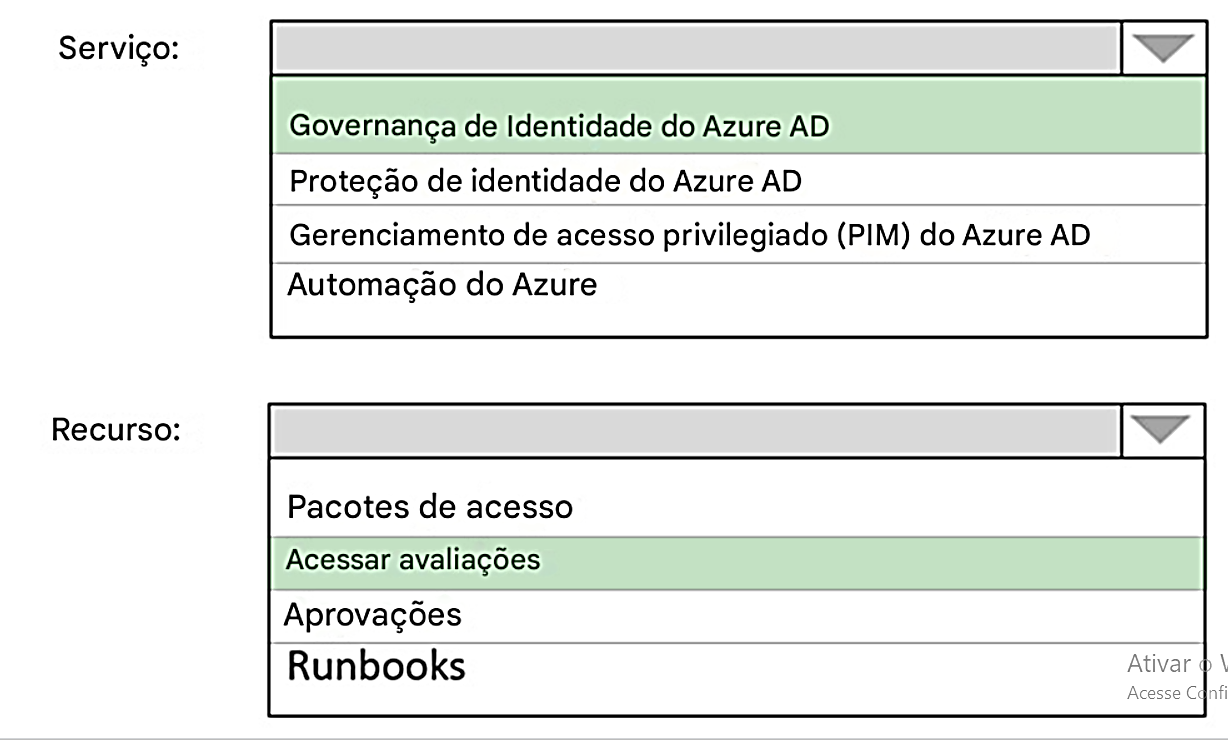
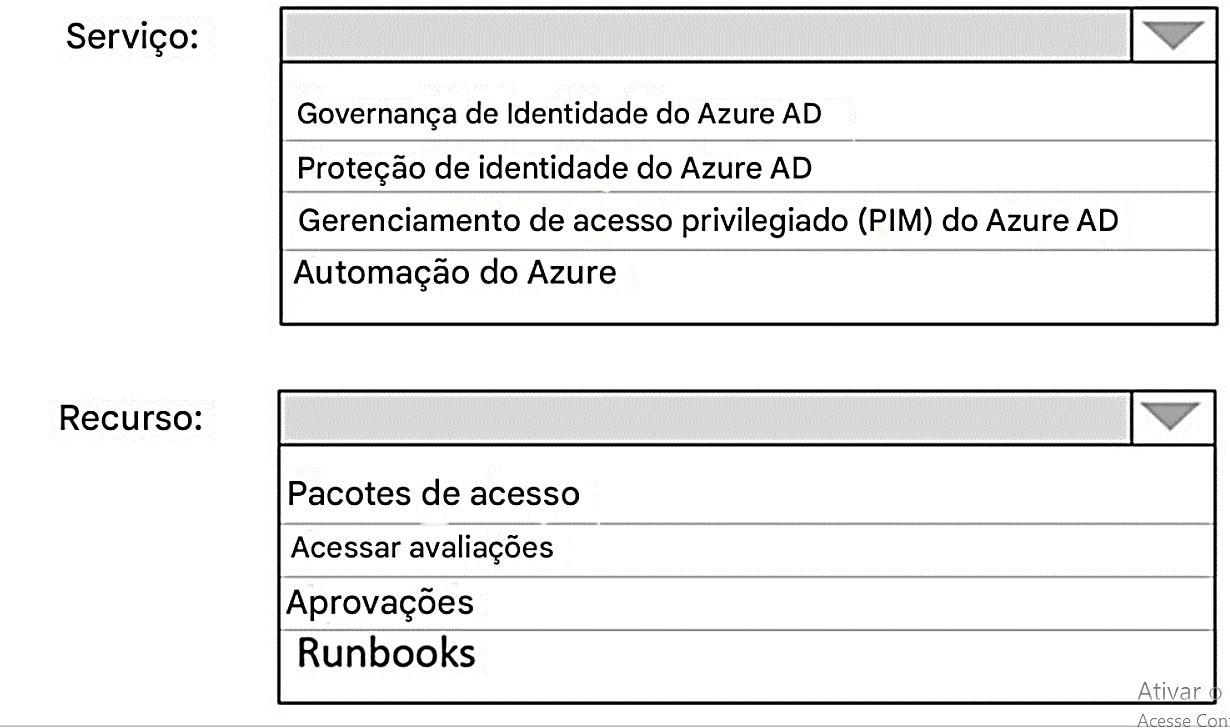


**Resposta correta:**  
  
Cenário: Requisito de segurança -  
Todos os segredos usados pelos serviços do Azure devem ser armazenados no Azure Key Vault.  
Os serviços que exigem credenciais devem ter as credenciais vinculadas à instância do serviço. As credenciais NÃO devem ser compartilhadas entre os serviços.  
Caixa 1: Uma identidade gerenciada atribuída pelo sistema  
Ninguém sabe as credenciais das identidades gerenciadas.  
As identidades gerenciadas existem em dois formatos:  
\* Atribuída pelo sistema: neste cenário, a identidade é vinculada a um único recurso do Azure, por exemplo, uma máquina virtual, um aplicativo lógico, uma conta de armazenamento, aplicativo da Web, função, etc., quase tudo. Em seguida, elas também ג€vivemג€ com o recurso do Azure, o que significa que são excluídas quando o recurso do Azure é excluído.  
\* Identidade gerenciada atribuída pelo usuário (incorreto para esta pergunta), o que significa que você primeiro precisa criá-la como um recurso autônomo do Azure por si só, depois disso ela pode ser vinculada a vários recursos do Azure.  
  
Caixa 2: Uma política de acesso -  
Configure uma política de acesso para a identidade gerenciada atribuída pelo sistema.  
  
Observação: Conceder acesso -  
A identidade gerenciada precisa receber acesso para ler o segredo que armazenaremos no Key Vault.  
1. Navegue até o Key Vault recém-criado  
2. Selecione Política de acesso no menu do lado esquerdo.  
3. Selecione Adicionar política de acesso  
4. Etc.  
Referência:  
<https://devblogs.microsoft.com/devops/demystifying-service-principals-managed-identities/> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad>

**Pergunta nº 217**

Informações introdutórias Estudo de caso -  
  
Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.

Pergunta  O que você deve implementar para atender aos requisitos de identidade? .  
   




**Resposta correta:**   
Requisitos: Requisitos de identidade  
A Contoso identifica os seguintes requisitos para gerenciar o acesso da Fabrikam aos recursos:  
\* Todo mês, um gerente de conta na Fabrikam deve revisar quais usuários da Fabrikam têm permissões de acesso ao App1. Contas que não precisam mais de permissões devem ser removidas como convidados.  
\* A solução deve minimizar o esforço de desenvolvimento.  
Caixa 1: Governança de identidade do Azure AD  
Incorreto:  
Não PIM: Os requisitos do ciclo de vida devem ser atendidos.  
  
Caixa 2: Revisões de acesso -  
As revisões de acesso do Azure Active Directory (Azure AD) permitem que as organizações gerenciem com eficiência associações de grupo, acesso a aplicativos empresariais e atribuições de função. O acesso do usuário pode ser revisado regularmente para garantir que apenas as pessoas certas tenham acesso contínuo.  
Referência:  
<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

**Pergunta nº 218**

Informações introdutórias Estudo de caso -  
   
 Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.

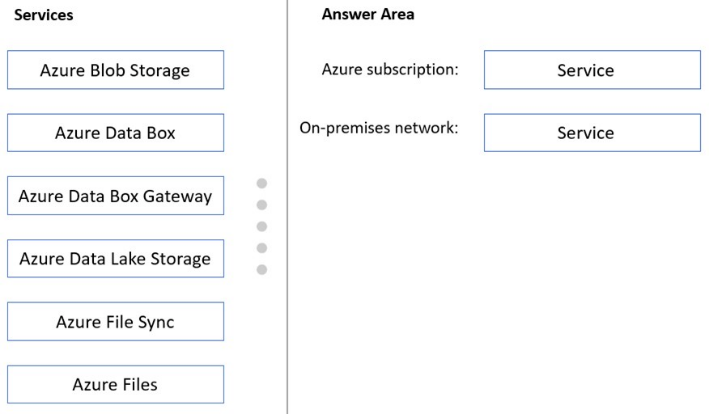
Pergunta O que você deve recomendar para atender aos requisitos de monitoramento do App2?

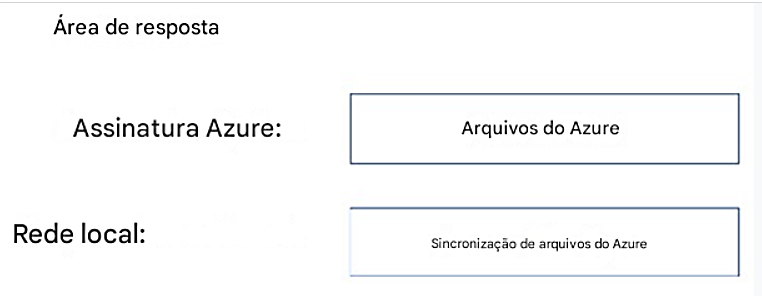
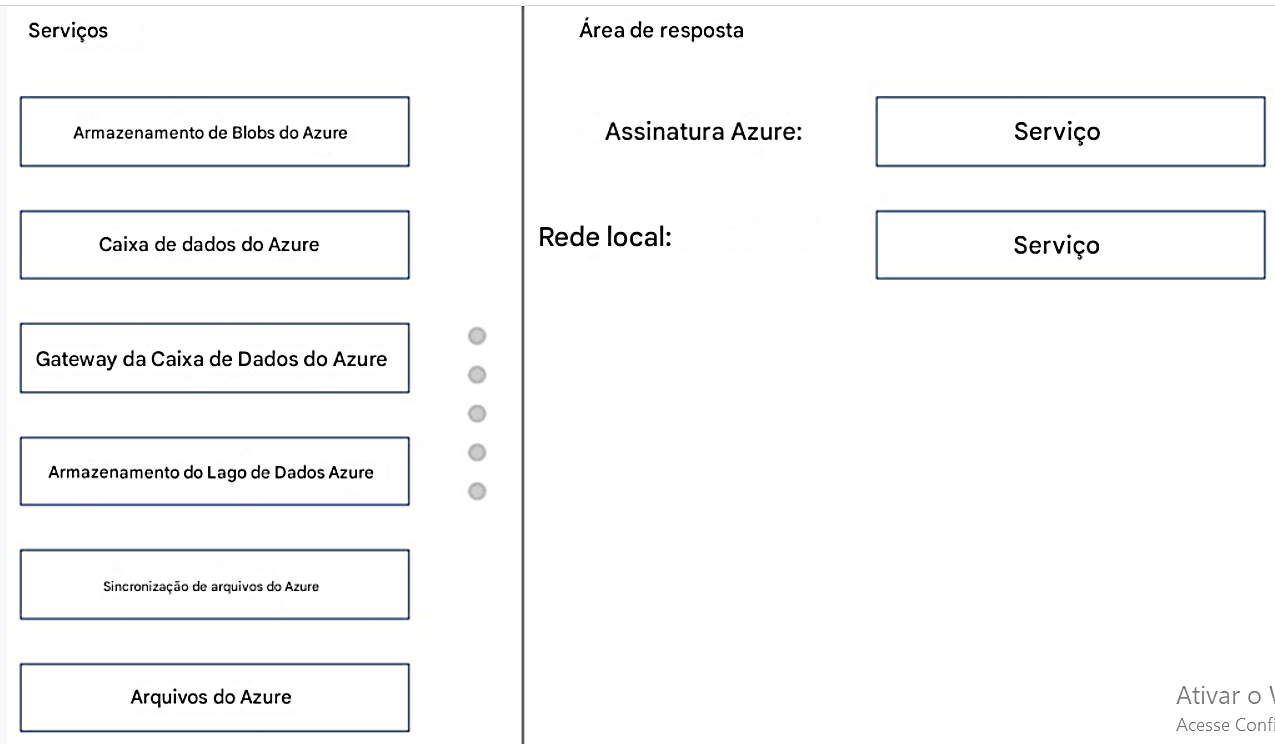
1. Insights de VM
2. Insights de aplicativos do Azure
3. Microsoft Sentinel
4. Insights sobre contêineres

Cenário: Você precisa monitorar o App2 para analisar quanto tempo leva para executar diferentes transações dentro do aplicativo. A solução não deve exigir alterações no código do aplicativo.  
Diagnóstico unificado de transações entre componentes.  
A experiência de diagnóstico unificado correlaciona automaticamente a telemetria do lado do servidor de todos os seus componentes monitorados do Application Insights em uma única exibição. Não importa se você tem vários recursos. O Application Insights detecta o relacionamento subjacente e permite que você diagnostique facilmente o componente do aplicativo, a dependência ou a exceção que causou uma lentidão ou falha na transação.  
Observação: os componentes são partes implantáveis independentemente do seu aplicativo distribuído/microsserviços. Os desenvolvedores e as equipes de operações têm visibilidade em nível de código ou acesso à telemetria gerada por esses componentes do aplicativo.  
Referência:  
<https://docs.microsoft.com/en-us/azure/azure-monitor/app/transaction-diagnostics>

**Pergunta #221**

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.

Pergunta  Você precisa recomendar uma solução que atenda aos requisitos de armazenamento de arquivos para o App2.  
O que você deve implantar na assinatura do Azure e na rede local?   
   




**Resposta correta:**   
Caixa 1: Arquivos do Azure -  
Cenário: O App2 tem os seguintes requisitos de armazenamento de arquivos:  
✑ Salvar arquivos em uma conta do Armazenamento do Azure.  
✑ Replique arquivos para um local local.  
✑ Garanta que os clientes locais possam ler os arquivos pela LAN usando o protocolo SMB.  
  
Caixa 2: Sincronização de arquivos do Azure -  
Use a Sincronização de arquivos do Azure para centralizar os compartilhamentos de arquivos da sua organização no Arquivos do Azure, mantendo a flexibilidade, o desempenho e a compatibilidade de um servidor de arquivos local. A Sincronização de arquivos do Azure transforma o Windows Server em um cache rápido do seu compartilhamento de arquivos do Azure. Você pode usar qualquer protocolo disponível no Windows Server para acessar seus dados localmente, incluindo SMB, NFS e FTPS. Você pode ter quantos caches precisar em todo o mundo.  
Referência:  
<https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide>

**Pergunta #222**

Informações introdutórias Estudo de caso -  
  
Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.

 Pergunta Você precisa recomendar uma solução que atenda aos requisitos de dados para o App1.  
O que você deve recomendar para implantar em cada zona de disponibilidade que contém uma instância do App1?

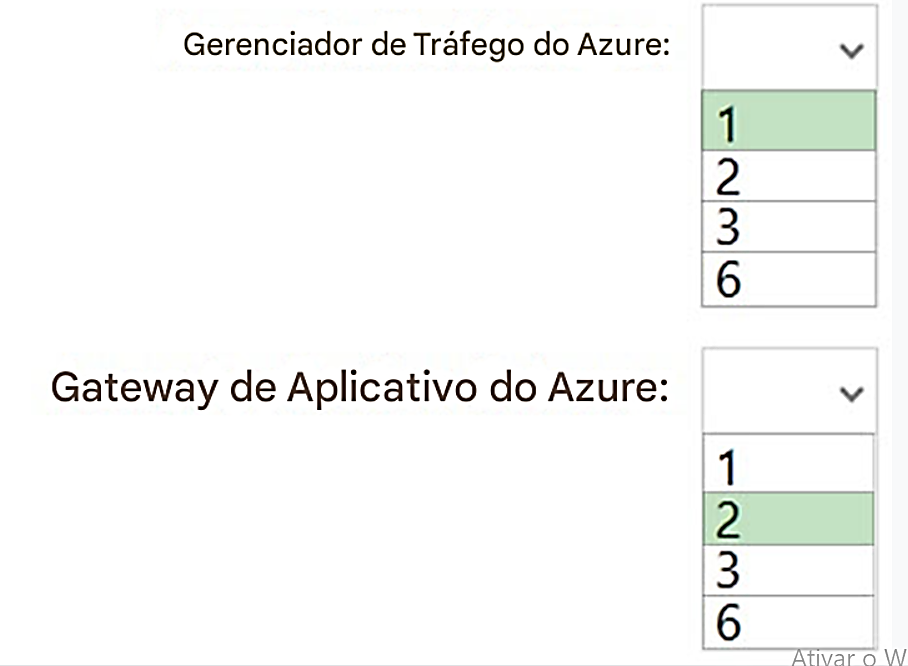
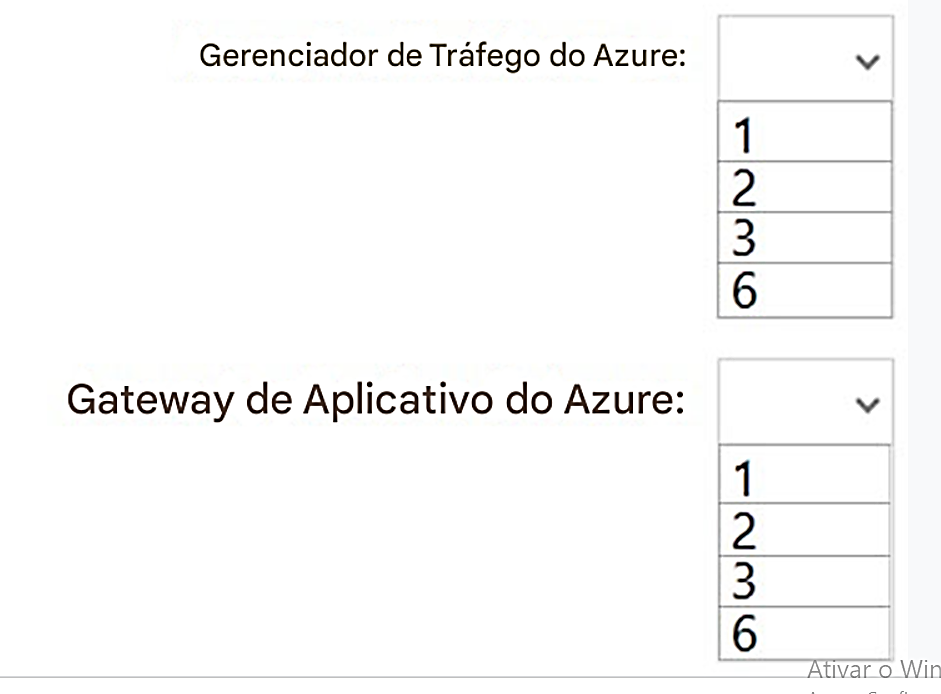
1. um Azure Cosmos DB que usa gravações multirregionais
2. um armazenamento do Azure Data Lake que usa armazenamento redundante de zona geográfica (GZRS)
3. uma conta de armazenamento do Azure que usa armazenamento redundante de zona geográfica (GZRS)

Cenário: O App1 tem os seguintes requisitos de dados:  
✑ Cada instância gravará dados em um armazenamento de dados na mesma zona de disponibilidade da instância.  
✑ Os dados gravados por qualquer instância do App1 devem ser visíveis para todas as instâncias do App1.  
Azure Cosmos DB: Cada partição em todas as regiões é replicada. Cada região contém todas as partições de dados de um contêiner do Azure Cosmos e pode atender leituras e gravações quando as gravações multirregionais estão habilitadas.  
Respostas incorretas:  
B, D: O GZRS protege contra falhas. O armazenamento georredundante (com GRS ou GZRS) replica seus dados para outro local físico na região secundária para proteger contra interrupções regionais. No entanto, esses dados estão disponíveis para leitura somente se o cliente ou a Microsoft iniciar um failover da região primária para a secundária.  
C: A replicação geográfica ativa é projetada como uma solução de continuidade de negócios que permite executar uma recuperação rápida de desastres de bancos de dados individuais em caso de um desastre regional ou uma interrupção em grande escala. Depois que a geo-replicação estiver configurada, você pode iniciar um geo-failover para um geo-secundário em uma região diferente do Azure. O geo-failover é iniciado programaticamente pelo aplicativo ou manualmente pelo usuário.  
Referência:  
<https://docs.microsoft.com/en-us/azure/cosmos-db/high-availability>

**Pergunta #223**

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
A Contoso, Ltd. é uma empresa de pesquisa que tem um escritório principal em Montreal.

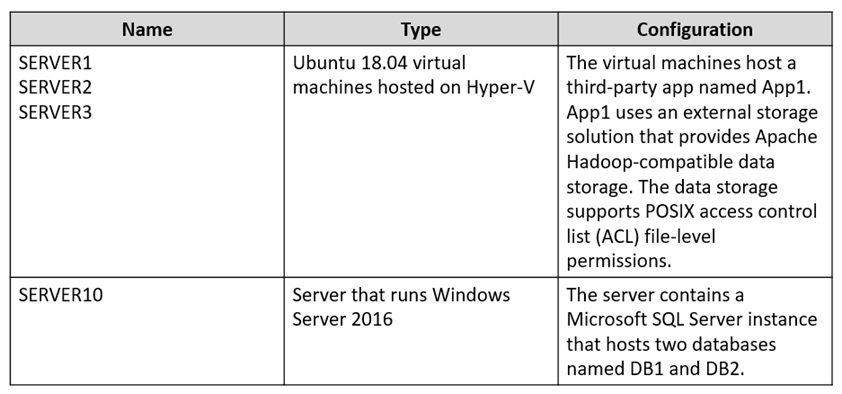
Pergunta  Você está avaliando se deve usar o Azure Traffic Manager e o Azure Application Gateway para atender aos requisitos de conexão do App1.  
Qual é o número mínimo de instâncias necessárias para cada serviço?   
  

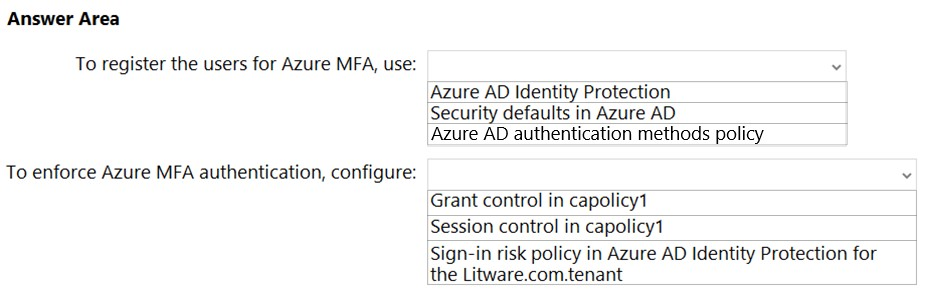



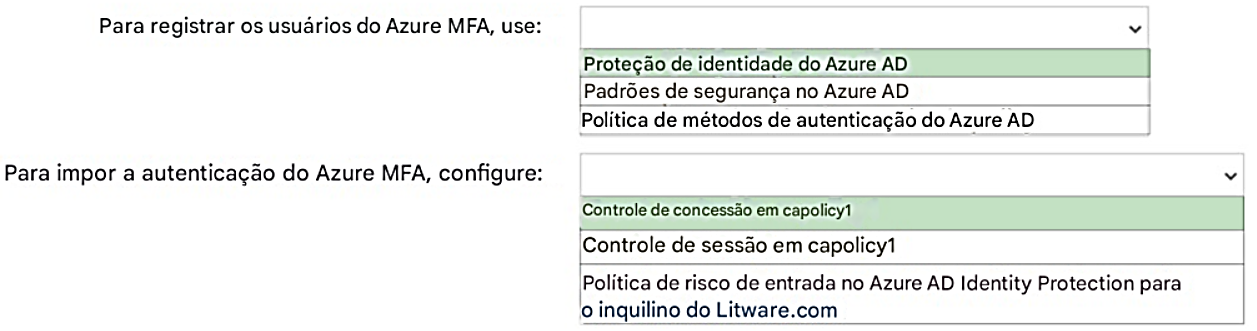
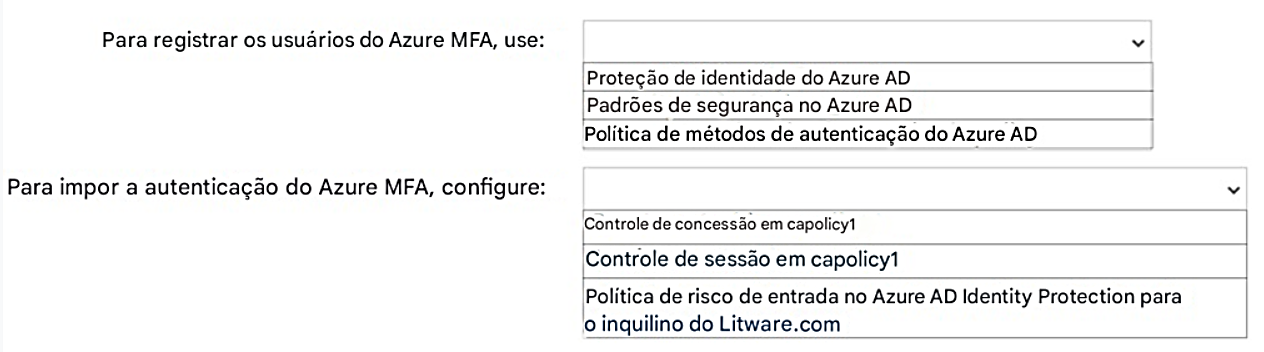
**Resposta correta:**   
Caixa 1: 1 -  
O App1 só poderá ser acessado pela Internet. O App1 tem os seguintes requisitos de conexão:  
ג€¢ As conexões com o App1 devem ter balanceamento de carga ativo-ativo entre as instâncias.  
ג€¢ Todas as conexões com o App1 da América do Norte devem ser direcionadas para a região Leste dos EUA. Todas as outras conexões devem ser direcionadas para a região Oeste da Europa.  
O App1 terá seis instâncias: três na região Leste dos EUA do Azure e três na região Oeste da Europa do Azure.  
Observação: o Azure Traffic Manager é um balanceador de carga de tráfego baseado em DNS. Este serviço permite que você distribua o tráfego para seus aplicativos públicos nas  
regiões globais do Azure.  
  
Caixa 2: 2 -  
Para cargas de trabalho de produção, execute pelo menos duas instâncias de gateway.  
Uma única implantação do Application Gateway pode executar várias instâncias do gateway.  
Use um Application Gateway na região Leste dos EUA e um na região Oeste da Europa.  
Referência:  
<https://docs.microsoft.com/en-us/azure/architecture/high-availability/reference-architecture-traffic-manager-application-gateway>

## caso de uso (Litware, Inc.)

**Pergunta nº 201**

Estudo de caso -  
  
Para iniciar o estudo de caso -  
Para exibir a primeira questão neste estudo de caso, clique no botão Avançar. Use os botões no painel esquerdo para explorar o conteúdo do estudo de caso antes de responder às perguntas. Clicar nesses botões exibe informações como requisitos de negócios, ambiente existente e declarações de problemas. Se o estudo de caso tiver uma guia Todas as informações, observe que as informações exibidas são idênticas às informações exibidas nas guias subsequentes. Quando estiver pronto para responder a uma pergunta, clique no botão Pergunta para retornar à pergunta.  
  
Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Ambiente existente -  
  
Ambiente de identidade -  
A rede contém uma floresta do Active Directory chamada litware.com que está vinculada a um locatário do Azure Active Directory (Azure AD) chamado litware.com. Todos os usuários têm licenças do Azure Active Directory Premium P2.  
A Litware tem um segundo locatário do Azure AD chamado dev.litware.com que é usado como um ambiente de desenvolvimento.  
O locatário litware.com tem uma política de acesso condicional chamada Capolicy1. A Capolicy1 exige que, quando os usuários gerenciam a assinatura do Azure para um ambiente de produção usando o portal do Azure, eles devem se conectar a partir de um dispositivo híbrido ingressado no Azure AD.  
  
Ambiente do Azure -  
A Litware tem 10 assinaturas do Azure vinculadas ao locatário Litware.com e cinco assinaturas do Azure vinculadas ao locatário dev.litware.com. Todas as assinaturas estão em um Enterprise Agreement (EA).  
O locatário litware.com contém uma função personalizada de controle de acesso baseado em função do Azure (Azure RBAC) chamada Role1 que concede a permissão de leitura DataActions aos blobs e arquivos no Azure Storage.  
  
Ambiente local -  
A rede local da Litware contém os recursos mostrados na tabela a seguir.  
  
  
Ambiente de rede -  
A Litware tem conectividade ExpressRoute com o Azure.  
Alterações e requisitos planejados  
  
Alterações planejadas -  
A Litware planeja implementar as seguintes alterações:  
Migrar DB1 e DB2 para o Azure.  
Migrar App1 para máquinas virtuais do Azure.  
Migrar o armazenamento externo usado pelo App1 para o Azure Storage.  
Implantar as máquinas virtuais do Azure que hospedarão o App1 em hosts dedicados do Azure.  
  
Requisitos de autenticação e autorização  
A Litware identifica os seguintes requisitos de autenticação e autorização:  
Somente usuários que gerenciam o ambiente de produção usando o portal do Azure devem se conectar de um dispositivo híbrido ingressado no Azure AD e autenticar usando  
o Azure Multi-Factor Authentication (MFA).  
A função RBAC interna do Network Contributor deve ser usada para conceder permissões aos administradores de rede para todas as redes virtuais em todas as assinaturas do Azure.  
Para acessar os recursos no Azure, o App1 deve usar a identidade gerenciada das máquinas virtuais que hospedarão o aplicativo.  
As funções RBAC devem ser aplicadas a grupos de gerenciamento.  
  
Requisitos de resiliência -  
A Litware identifica os seguintes requisitos de resiliência:  
Depois de migrados para o Azure, o DB1 e o DB2 devem atender aos seguintes requisitos:  
- Manter a disponibilidade se duas zonas de disponibilidade na região local do Azure falharem.  
- Fazer failover automaticamente.  
- Minimizar a latência de E/S.  
O App1 deve atender aos seguintes requisitos:  
- Ser hospedado em uma região do Azure que ofereça suporte a zonas de disponibilidade.  
- Ser hospedado em máquinas virtuais do Azure que ofereçam suporte ao dimensionamento automático.  
- Manter a disponibilidade se duas zonas de disponibilidade na região local do Azure falharem.  
Requisitos de segurança e conformidade  
A Litware identifica os seguintes requisitos de segurança e conformidade:  
Depois que o App1 for migrado para o Azure, você deve garantir que novos dados possam ser gravados no aplicativo e que a modificação de dados novos e existentes seja impedida por um período de três anos.  
Usuários e serviços locais devem conseguir acessar a conta do Azure Storage que hospedará os dados no App1.  
O acesso ao ponto de extremidade público da conta do Azure Storage que hospedará os dados do App1 deve ser impedido.  
Todos os bancos de dados SQL do Azure no ambiente de produção devem ter o Transparent Data Encryption (TDE) habilitado.  
O App1 NÃO deve compartilhar hardware físico com outras cargas de trabalho.  
  
Requisitos de negócios -  
A Litware identifica os seguintes requisitos de negócios:  
Minimizar o esforço administrativo.  
Minimizar os custos.

Pergunta  Você precisa garantir que os usuários que gerenciam o ambiente de produção estejam registrados no Azure MFA e devem autenticar usando o Azure MFA ao entrar no portal do Azure. A solução deve atender aos requisitos de autenticação e autorização.  
O que você deve fazer? .  
   
   




**Resposta correta:**  
  
Caixa 1: Proteção de identidade do Azure AD  
Somente usuários que gerenciam o ambiente de produção usando o portal do Azure devem se conectar de um dispositivo híbrido ingressado no Azure AD e autenticar usando  
a Autenticação multifator (MFA) do Azure.  
  
Observação: Configuração de política -  
1. Navegue até o portal do Azure.  
2. Navegue até Azure Active Directory > Segurança > Proteção de identidade > Política de registro MFA.  
3. Em Atribuições  
4. Usuários - Escolha Todos os usuários ou Selecionar indivíduos e grupos se estiver limitando sua implementação.  
5. Opcionalmente, você pode optar por excluir usuários da política.  
6. Aplicar política - Ativado  
7. Salvar  
Caixa 2: Conceder controle em capolicy1  
O locatário litware.com tem uma política de acesso condicional chamada Capolicy1. O Capolicy1 exige que, quando os usuários gerenciam a assinatura do Azure para um ambiente de produção usando o portal do Azure, eles devem se conectar de um dispositivo híbrido ingressado no Azure AD.  
Observação: precisamos configurar as condições de política para capolicy1 que solicitam MFA.  
Referência:  
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa>

**Pergunta #202**

Informações introdutórias Estudo de caso -  
   
Visão geral -  
**Litware, Inc.** é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Pergunta Após migrar o App1 para o Azure, você precisa impor os requisitos de modificação de dados para atender aos requisitos de segurança e conformidade.  
O que você deve fazer?

1. **UM**

Crie uma política de acesso para o serviço de blob.

1. **B**

Implementar bloqueios de recursos do Azure.

1. **C**

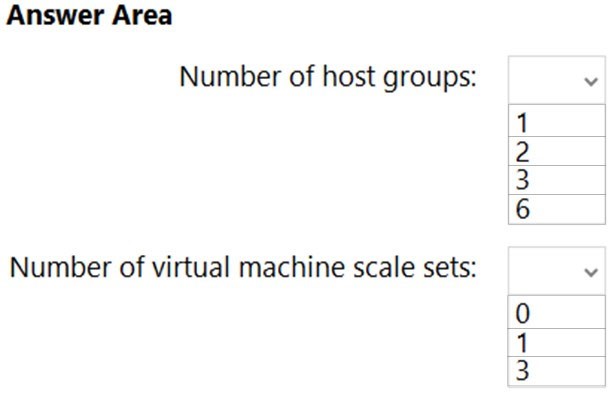
Crie atribuições do Azure RBAC.

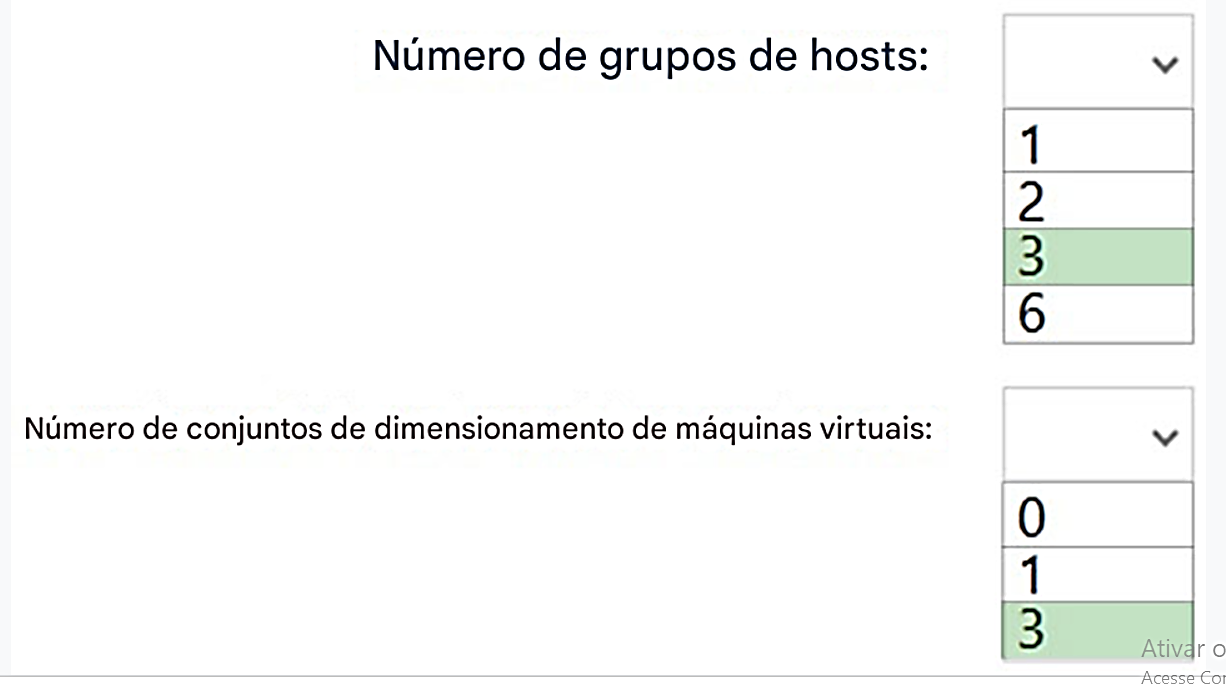
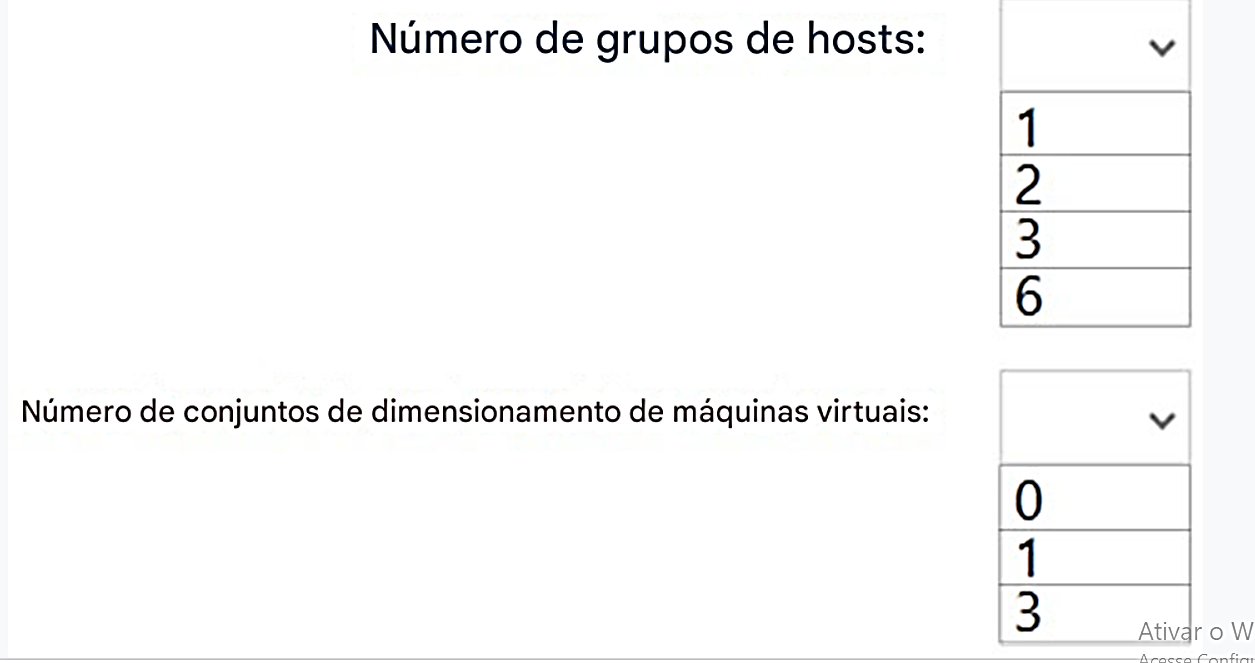
1. **E**

Modifique o nível de acesso do serviço blob.

**Resposta correta:**  
A  
Cenário: Depois que o App1 for migrado para o Azure, você deve garantir que novos dados possam ser gravados no aplicativo, e a modificação de dados novos e existentes seja impedida por um período de três anos.  
Como administrador, você pode bloquear uma assinatura, grupo de recursos ou recurso para impedir que outros usuários em sua organização excluam ou modifiquem acidentalmente recursos críticos. O bloqueio substitui quaisquer permissões que o usuário possa ter.  
Referência:  
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

**Pergunta #209**

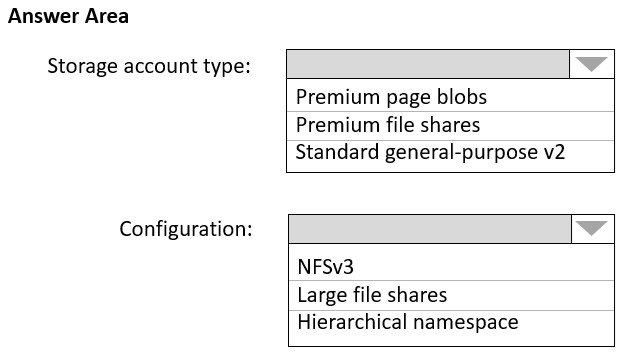
Informações introdutórias Estudo de caso -  
   
 Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Pergunta  Você planeja migrar o App1 para o Azure.  
Você precisa recomendar uma solução de alta disponibilidade para o App1. A solução deve atender aos requisitos de resiliência.  
O que você deve incluir na recomendação? .  
   
   


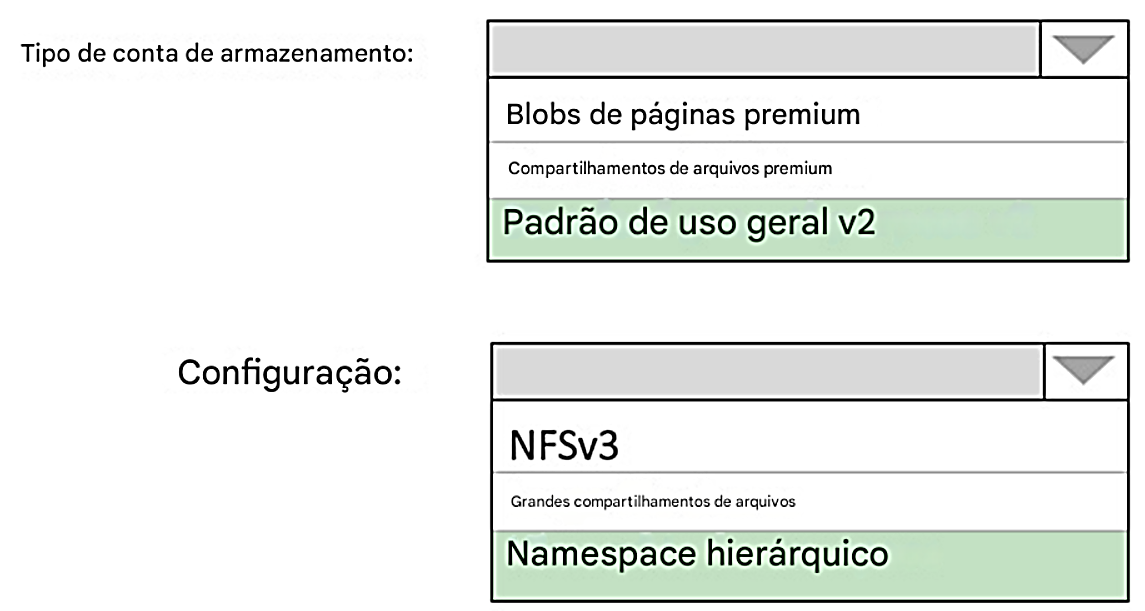
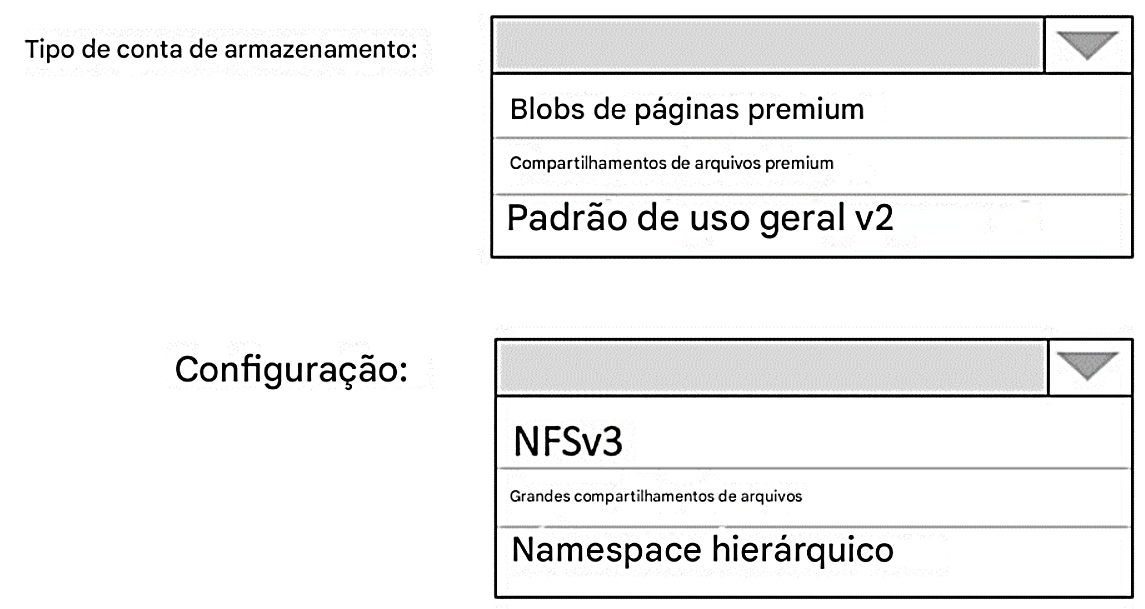


**Resposta correta:**  
  
Caixa 1: 3 -  
Precisa de três grupos de hosts para atender ao terceiro requisito do cenário abaixo.  
Cenário: O App1 deve atender aos seguintes requisitos:  
Ser hospedado em uma região do Azure que ofereça suporte a zonas de disponibilidade.  
Ser hospedado em máquinas virtuais do Azure que ofereçam suporte ao dimensionamento automático.  
Manter a disponibilidade se duas zonas de disponibilidade na região local do Azure falharem.  
  
Caixa 2: 3 -  
A configuração de disponibilidade do seu grupo de hosts deve corresponder ao seu conjunto de dimensionamento.  
\* O grupo de hosts e o conjunto de dimensionamento devem estar usando a mesma zona de disponibilidade.  
\* A contagem de domínio de falha para o nível do grupo de hosts deve corresponder à contagem de domínio de falha para seu conjunto de dimensionamento.  
Referência:  
<https://docs.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts>

**Pergunta nº 210**

Shape

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Pergunta  Você planeja migrar o App1 para o Azure.  
Você precisa recomendar uma solução de armazenamento para o App1 que atenda aos requisitos de segurança e conformidade.  
Que tipo de armazenamento você deve recomendar e como deve recomendar a configuração do armazenamento? .  
   




**Resposta correta:**  
  
Caixa 1: Padrão de uso geral v2  
O padrão de uso geral v2 oferece suporte ao Blob Storage.  
O Azure Storage fornece proteção de dados para o Blob Storage e o Azure Data Lake Storage Gen2.  
Cenário:  
A Litware identifica os seguintes requisitos de segurança e conformidade:  
✑ Depois que o App1 for migrado para o Azure, você deve garantir que novos dados possam ser gravados no aplicativo e que a modificação de dados novos e existentes seja impedida por um período de três anos.  
✑ Usuários e serviços locais devem conseguir acessar a conta do Azure Storage que hospedará os dados no App1.  
✑ O acesso ao ponto de extremidade público da conta do Azure Storage que hospedará os dados do App1 deve ser impedido.  
Todos os bancos de dados SQL do Azure no ambiente de produção devem ter o Transparent Data Encryption (TDE) habilitado.  
  
✑ O App1 NÃO deve compartilhar hardware físico com outras cargas de trabalho.  
  
Caixa 2: Namespace hierárquico -  
Cenário: Plano: migrar o App1 para máquinas virtuais do Azure.  
O Azure Data Lake Storage Gen2 implementa um modelo de controle de acesso que oferece suporte ao controle de acesso baseado em função do Azure (Azure RBAC) e listas de controle de acesso (ACLs) semelhantes a POSIX.  
O Data Lake Storage Gen2 e o protocolo Network File System (NFS) 3.0 exigem uma conta de armazenamento com um namespace hierárquico habilitado.  
Referência:  
<https://docs.microsoft.com/en-us/azure/storage/blobs/data-protection-overview> <https://docs.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview>

**Pergunta nº 211**

Shape

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Pergunta Você planeja migrar o App1 para o Azure.  
Você precisa recomendar uma solução de conectividade de rede para a conta do Azure Storage que hospedará os dados do App1. A solução deve atender aos requisitos de segurança e conformidade.  
O que você deve incluir na recomendação?

1. **UM**

Microsoft procurando um circuito ExpressRoute

1. **B**

Peering público do Azure para um circuito ExpressRoute

1. **C**

um ponto de extremidade de serviço que tem uma política de ponto de extremidade de serviço

1. **E**

um ponto final privado

**Resposta correta:**  
D O  
Private Endpoint se conecta com segurança a contas de armazenamento de redes locais que se conectam à VNet usando VPN ou ExpressRoutes com peering privado.  
O Private Endpoint também protege sua conta de armazenamento configurando o firewall de armazenamento para bloquear todas as conexões no endpoint público para o serviço de armazenamento.  
Respostas incorretas:  
A: O peering da Microsoft fornece acesso aos serviços públicos do Azure por meio de endpoints públicos com endereços IP públicos, o que não deve ser permitido.  
B: O peering público do Azure foi descontinuado.  
C: Por padrão, os Service Endpoints são habilitados em sub-redes configuradas em redes virtuais do Azure. Os endpoints não podem ser usados para tráfego de suas instalações para serviços do Azure.  
Referência:  
<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings>

**Pergunta #212**

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Pergunta Você precisa implementar as atribuições de função do Azure RBAC para a função Network Contributor. A solução deve atender aos requisitos de autenticação e autorização.  
Qual é o número mínimo de atribuições que você deve usar?

1. **UM**

1

1. **B**

2

1. **C**

5

1. **E**

10

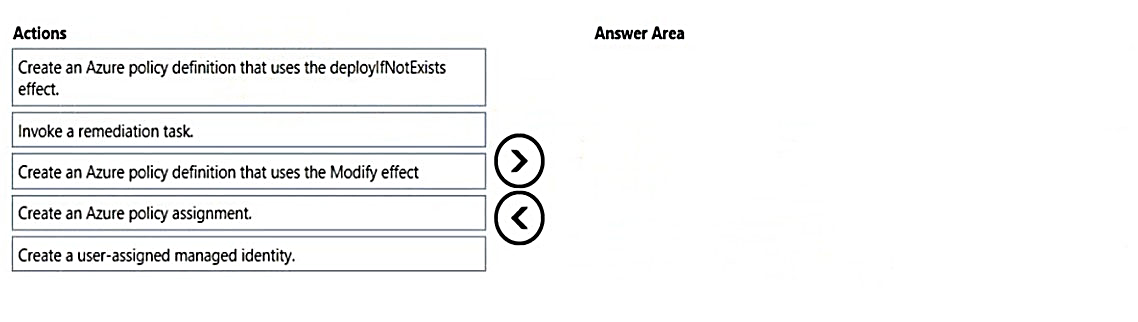
1. **E**

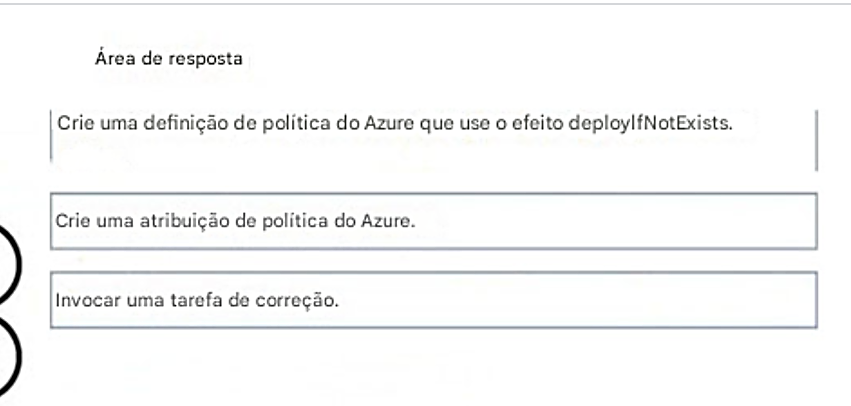
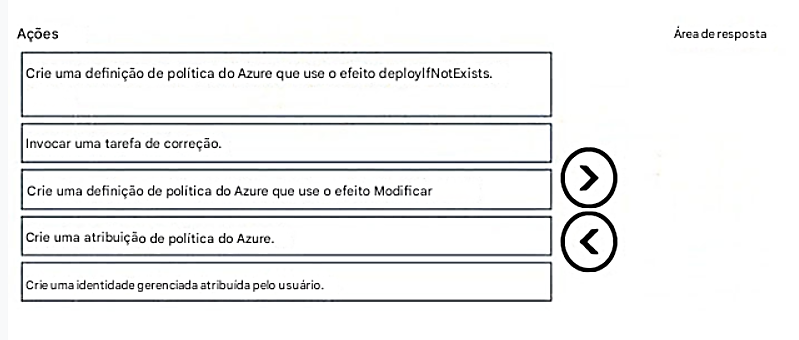
15

**Resposta correta:**  
B  
Cenário: A função RBAC interna do Network Contributor deve ser usada para conceder permissões aos administradores de rede para todas as redes virtuais em todas as assinaturas do Azure.  
As funções RBAC devem ser aplicadas no nível mais alto possível.

**Pergunta nº 213**

Shape

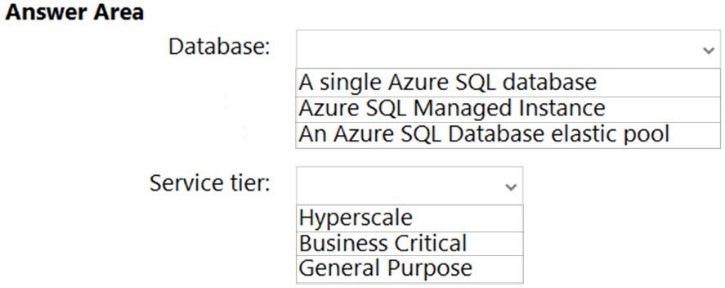
Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Pergunta  Você precisa configurar uma política do Azure para garantir que os bancos de dados SQL do Azure tenham a Criptografia Transparente de Dados (TDE) habilitada. A solução deve atender aos requisitos de segurança e conformidade.  
Quais três ações você deve executar em sequência?   


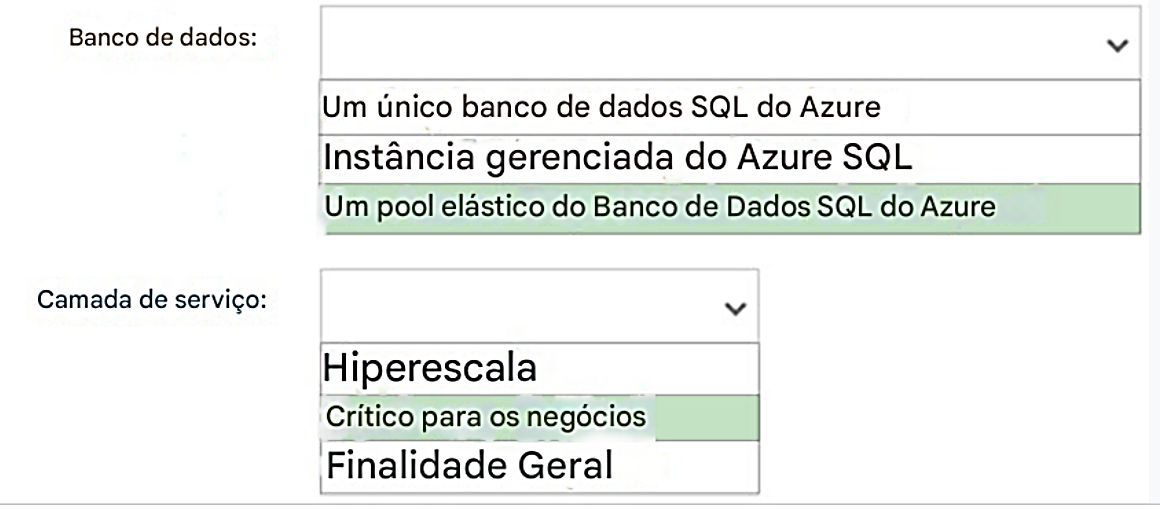
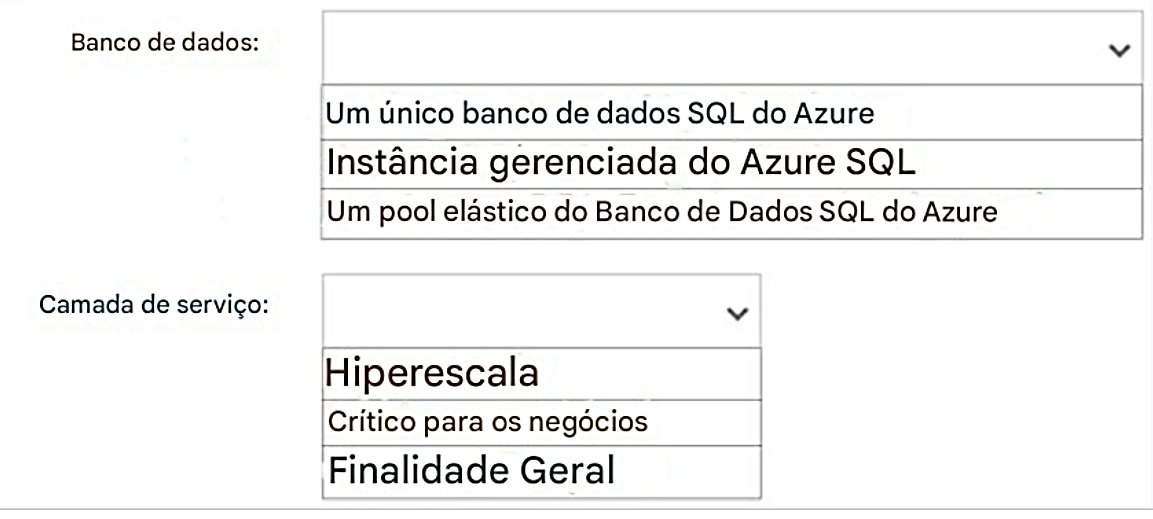


**Resposta correta:**  
  
Etapa 1: criar uma definição de política do Azure que use o deployIfNotExists  
A primeira etapa é definir as funções que o deployIfNotExists e o modify precisam na definição de política para implantar com êxito o conteúdo do seu modelo incluído.  
Etapa 2: criar uma atribuição de política do Azure  
Ao criar uma atribuição usando o portal, o Azure Policy gera a identidade gerenciada e concede a ela as funções definidas em roleDefinitionIds.  
Etapa 3: invocar uma tarefa de correção.  
Os recursos que não são compatíveis com um deployIfNotExists ou modify policy podem ser colocados em um estado compatível por meio da correção. A correção é realizada instruindo o Azure Policy a executar o efeito deployIfNotExists ou as operações modify da política atribuída em seus recursos e assinaturas existentes, seja essa atribuição para um grupo de gerenciamento, uma assinatura, um grupo de recursos ou um recurso individual.  
Durante a avaliação, a atribuição de política com os efeitos deployIfNotExists ou modify determina se há recursos ou assinaturas não compatíveis. Quando recursos ou assinaturas não compatíveis são encontrados, os detalhes são fornecidos na página Correção.  
Referência:  
<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

**Pergunta #220**

Shape

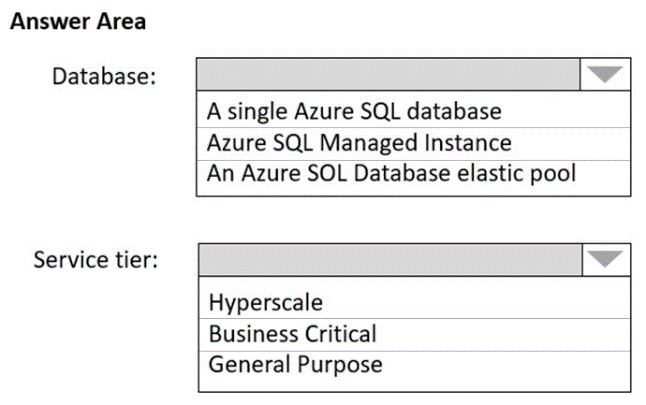
Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
Ambiente existente -  
  
Pergunta  Você planeja migrar DB1 e DB2 para o Azure.  
Você precisa garantir que o banco de dados do Azure e a camada de serviço atendam aos requisitos de resiliência e negócios.  
O que você deve configurar? .  
   
   


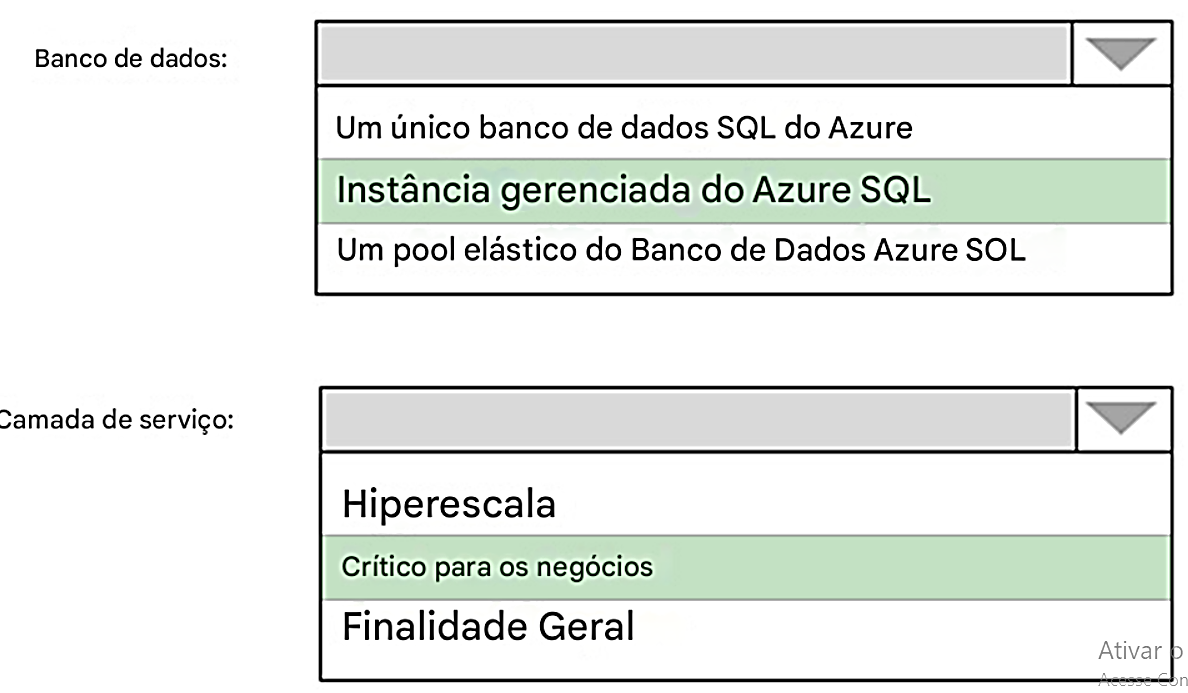
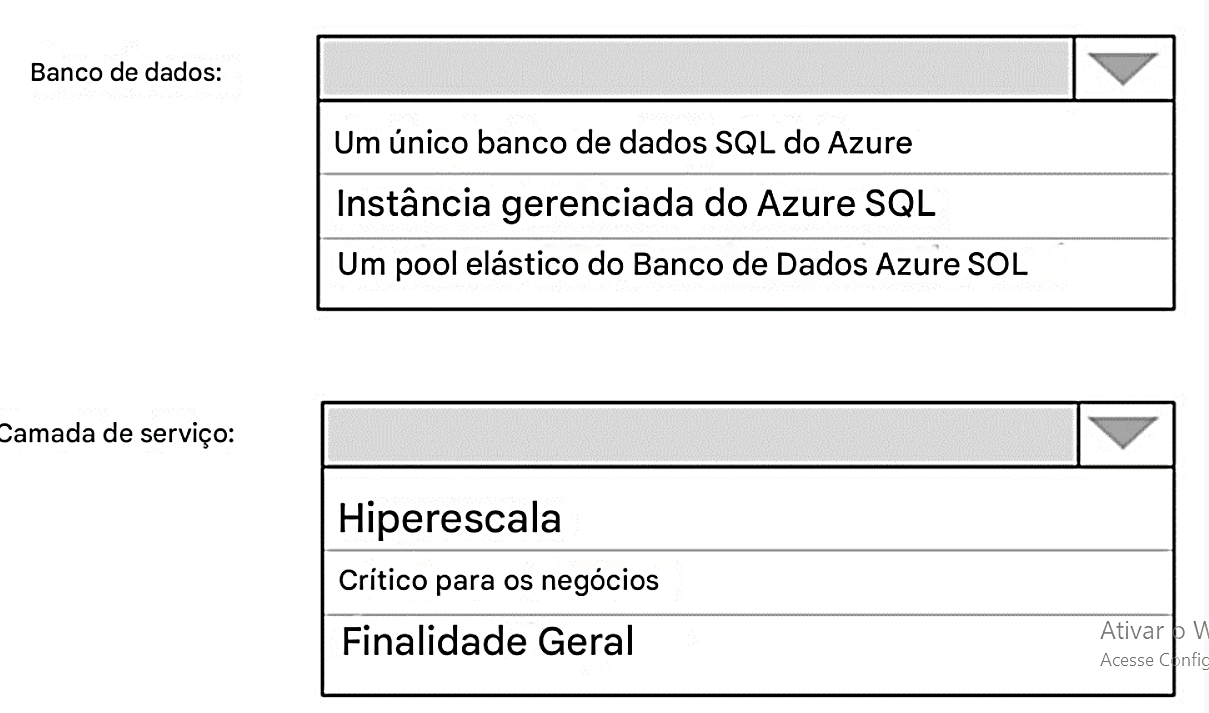


**Resposta correta:**   
Caixa 1: Um  
cenário de pool elástico do Banco de Dados SQL do Azure:  
\* Requisitos de resiliência. Depois de migrados para o Azure, o DB1 e o DB2 devem atender aos seguintes requisitos:  
Manter a disponibilidade se duas zonas de disponibilidade na região local do Azure falharem.  
Fazer failover automaticamente.  
Minimizar a latência de E/S.  
\* A Litware identifica os seguintes requisitos de negócios:  
Minimizar o esforço administrativo.  
Minimizar os custos.  
Caixa 2: Crítico para os negócios

**Pergunta #224**

Shape

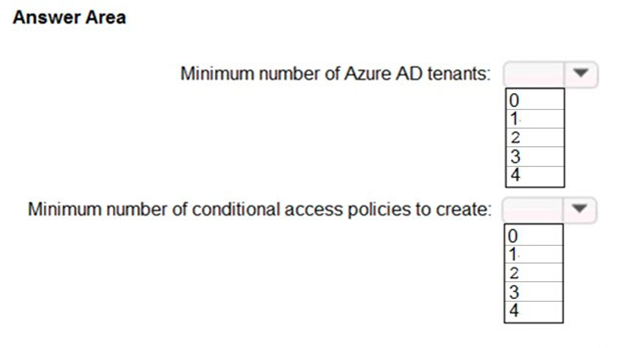
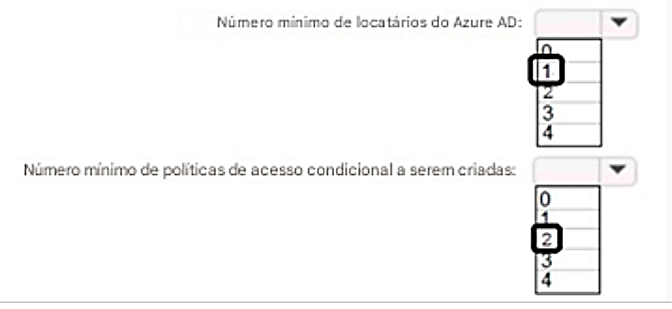
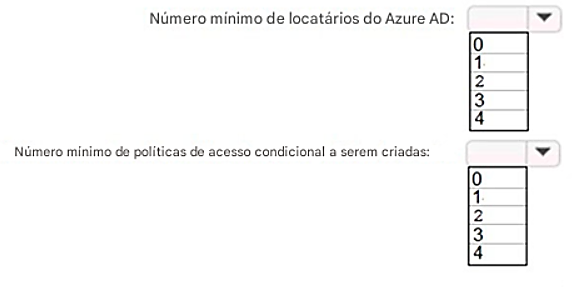
Informações introdutórias Estudo de caso -  
   
   
Visão geral -  
Litware, Inc. é uma empresa financeira de médio porte que tem um escritório principal em Boston.  
  
 Pergunta  Como os bancos de dados DB1 e DB2 migrados devem ser implementados no Azure?  
   




**Resposta correta:**   
Caixa 1: Instância gerenciada do SQL -  
Cenário: Depois de migrados para o Azure, o DB1 e o DB2 devem atender aos seguintes requisitos:  
✑ Manter a disponibilidade se duas zonas de disponibilidade na região local do Azure falharem.  
✑ Fazer failover automaticamente.  
✑ Minimizar a latência de E/S.  
O recurso de grupos de failover automático permite que você gerencie a replicação e o failover de um grupo de bancos de dados em um servidor ou todos os bancos de dados em uma instância gerenciada para outra região. É uma abstração declarativa sobre o recurso de replicação geográfica ativa existente, projetada para simplificar a implantação e o gerenciamento de bancos de dados replicados geograficamente em escala. Você pode iniciar um failover geográfico manualmente ou delegá-lo ao serviço do Azure com base em uma política definida pelo usuário. A última opção permite que você recupere automaticamente vários bancos de dados relacionados em uma região secundária após uma falha catastrófica ou outro evento não planejado que resulte em perda total ou parcial da disponibilidade do Banco de Dados SQL ou da Instância Gerenciada do SQL na região primária.  
  
Caixa 2: Crítico para os negócios -  
A Instância Gerenciada do SQL está disponível em duas camadas de serviço:  
Propósito geral: Projetado para aplicativos com requisitos típicos de desempenho e latência de E/S.  
Crítico para os negócios: Projetado para aplicativos com baixos requisitos de latência de E/S e impacto mínimo das operações de manutenção subjacentes na carga de trabalho.  
Referência:  
<https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-overview> <https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview>

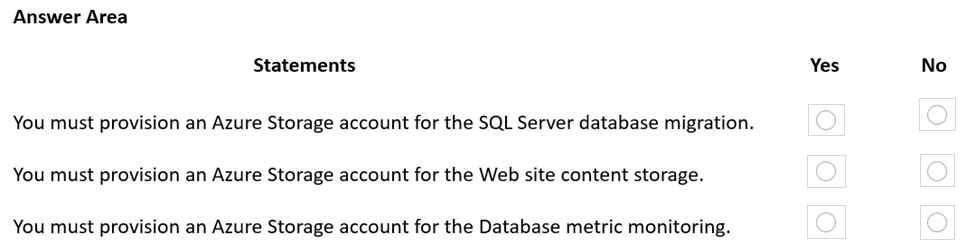
## caso de uso (Fabrikam, Inc.)

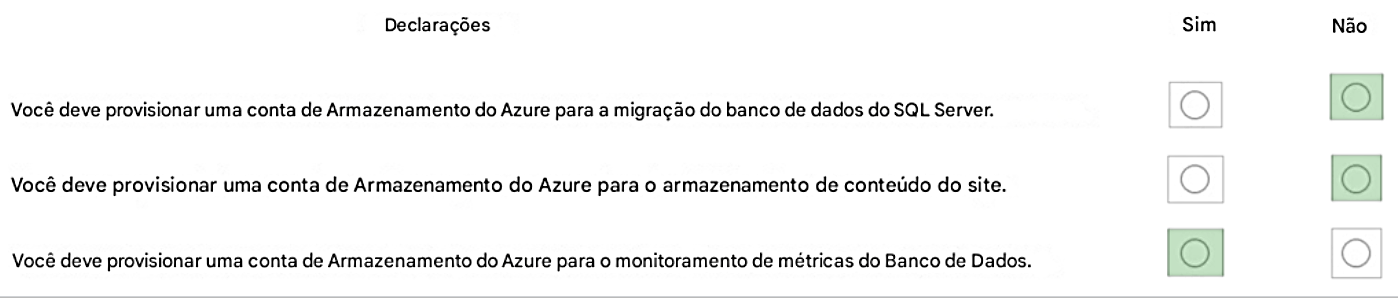
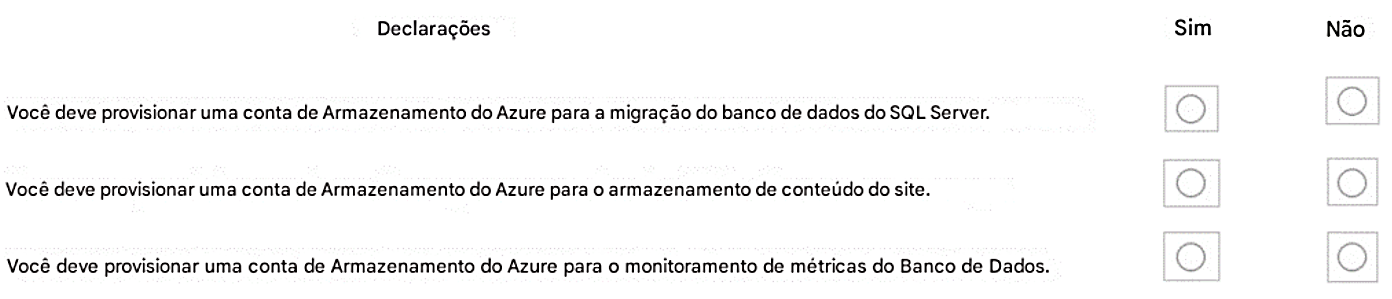
**Pergunta nº 109**

Estudo de caso  
  
Para iniciar o estudo de caso  
-  
Para exibir a primeira questão neste estudo de caso, clique no botão Avançar. Use os botões no painel esquerdo para explorar o conteúdo do estudo de caso antes de responder às perguntas. Clicar nesses botões exibe informações como requisitos de negócios, ambiente existente e declarações de problemas. Se o estudo de caso tiver uma guia Todas as informações, observe que as informações exibidas são idênticas às informações exibidas nas guias subsequentes. Quando estiver pronto para responder a uma pergunta, clique no botão Pergunta para retornar à pergunta.  
  
  
Visão geral  
-  
  
**Fabrikam, Inc.** é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã, Berlim e Roma.  
  
Ambiente existente: Ambiente do Active Directory  
  
A rede contém duas florestas do Active Directory chamadas corp.fabrikam.com e rd.fabrikam.com. Não há relações de confiança entre as florestas.  
  
Corp.fabrikam.com é uma floresta de produção que contém identidades usadas para autenticação interna de usuários e computadores.  
  
Rd.fabrikam.com é usado apenas pelo departamento de pesquisa e desenvolvimento (P&D). O departamento de P&D está restrito a usar apenas recursos locais.  
  
Ambiente existente: Infraestrutura de rede  
  
Cada escritório contém pelo menos um controlador de domínio do domínio corp.fabrikam.com. O escritório principal contém todos os controladores de domínio para a floresta rd.fabrikam.com.  
  
Todos os escritórios têm uma conexão de alta velocidade com a internet.  
  
Um aplicativo existente chamado WebApp1 é hospedado no data center do escritório de Londres. O WebApp1 é usado pelos clientes para fazer e rastrear pedidos. O WebApp1 tem uma camada da web que usa o Microsoft Internet Information Services (IIS) e uma camada de banco de dados que executa o Microsoft SQL Server 2016. A camada da web e a camada de banco de dados são implantadas em máquinas virtuais que são executadas no Hyper-V.  
  
O departamento de TI atualmente usa um ambiente Hyper-V separado para testar atualizações do WebApp1.  
  
A Fabrikam compra todas as licenças da Microsoft por meio de um Microsoft Enterprise Agreement que inclui Software Assurance.  
  
Ambiente existente: Declarações de problemas  
  
O uso do WebApp1 é imprevisível. Em horários de pico, os usuários geralmente relatam atrasos. Em outros momentos, muitos recursos do WebApp1 são subutilizados.  
  
  
Requisitos: Alterações planejadas  
-  
  
A Fabrikam planeja mover a maioria de suas cargas de trabalho de produção para o Azure durante os próximos anos, incluindo máquinas virtuais que dependem do Active Directory para autenticação.  
  
Como um de seus primeiros projetos, a empresa planeja estabelecer um modelo de identidade híbrido, facilitando uma futura implantação do Microsoft 365.  
  
Todas as operações de P&D permanecerão no local.  
  
A Fabrikam planeja migrar as instâncias de produção e teste do WebApp1 para o Azure.  
  
Requisitos: Requisitos técnicos  
  
A Fabrikam identifica os seguintes requisitos técnicos:  
  
• O conteúdo do site deve ser facilmente atualizado a partir de um único ponto.  
• A entrada do usuário deve ser minimizada ao provisionar novas instâncias de aplicativo da web.  
• Sempre que possível, as licenças locais existentes devem ser usadas para reduzir custos.  
• Os usuários devem sempre autenticar usando sua identidade UPN corp.fabrikam.com.  
• Quaisquer novas implantações no Azure devem ser redundantes no caso de falha de uma região do Azure.  
• Sempre que possível, as soluções devem ser implantadas no Azure usando o nível de preços Standard do Azure App Service.  
• Um grupo de distribuição de e-mail chamado Suporte de TI deve ser notificado sobre quaisquer problemas relacionados aos serviços de sincronização de diretório.  
• No caso de falha de um link entre o Azure e a rede local, certifique-se de que as máquinas virtuais hospedadas no Azure possam ser autenticadas no Active Directory.  
• A sincronização de diretórios entre o Azure Active Directory (Azure AD) e corp.fabrikam.com não deve ser afetada por uma falha de link entre o Azure e a rede local.  
  
Requisitos: Requisitos do banco de dados  
  
A Fabrikam identifica os seguintes requisitos de banco de dados:  
  
• As métricas do banco de dados para a instância de produção do WebApp1 devem estar disponíveis para análise para que os administradores do banco de dados possam otimizar as configurações de desempenho.  
• Para evitar a interrupção do acesso do cliente, o tempo de inatividade do banco de dados deve ser minimizado quando os bancos de dados são migrados.  
• Os backups do banco de dados devem ser mantidos por no mínimo sete anos para atender aos requisitos de conformidade.  
  
Requisitos: Requisitos de segurança  
  
A Fabrikam identifica os seguintes requisitos de segurança:  
  
• As informações da empresa, incluindo políticas, modelos e dados, devem ser inacessíveis a qualquer pessoa de fora da empresa.  
• Os usuários na rede local devem ser capazes de se autenticar em corp.fabrikam.com se um link de internet falhar.  
• Os administradores devem ser capazes de se autenticar no portal do Azure usando suas credenciais corp.fabrikam.com.  
• Todo acesso administrativo ao portal do Azure deve ser protegido usando autenticação multifator (MFA).  
• O teste de atualizações do WebApp1 não deve ser visível a ninguém de fora da empresa.  
  
  
Para atender aos requisitos de autenticação da Fabrikam, o que você deve incluir na solução? .  
  
   
  
  
  


**Pergunta nº 207**

Informações introdutórias Estudo de caso -  
   
 Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta  Você está avaliando os componentes da migração para o Azure que exigem que você provisione uma conta do Azure Storage.   
   
   




**Resposta correta:**  
  
Caixa 1: Não -  
A migração online funcionará bem. Não requer uma conta do Azure Storage.  
  
Caixa 2: Não -  
Os dados do site podem ser migrados para o serviço de aplicativo do Azure.  
  
Caixa 3: Sim -  
Cenário: As métricas do banco de dados para a instância de produção do WebApp1 devem estar disponíveis para análise para que os administradores do banco de dados possam otimizar as configurações de desempenho.  
Referência:  
<https://azure.microsoft.com/en-au/services/sql-server-stretch-database/>

**Pergunta #208**

Informações introdutórias Estudo de caso -  
   
Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta O que você deve incluir na estratégia de gerenciamento de identidade para dar suporte às mudanças planejadas?

1. **UM**

Implante controladores de domínio para corp.fabrikam.com em redes virtuais no Azure.

1. **B**

Mova todos os controladores de domínio de corp.fabrikam.com para redes virtuais no Azure.

1. **C**

Implante um novo locatário do Azure AD para autenticação de novos projetos de P&D.

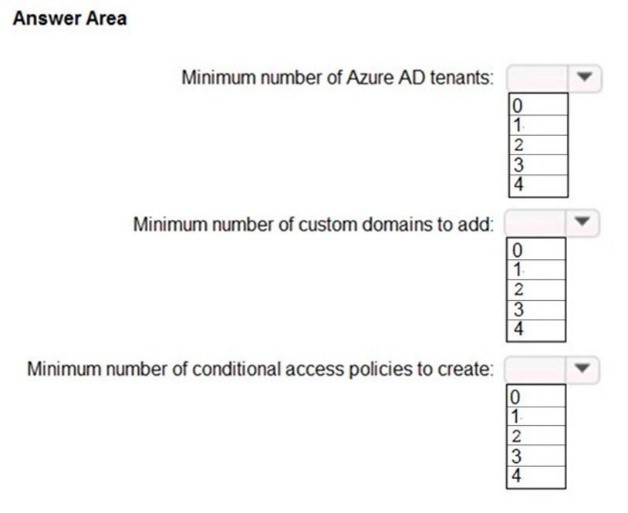
1. **E**

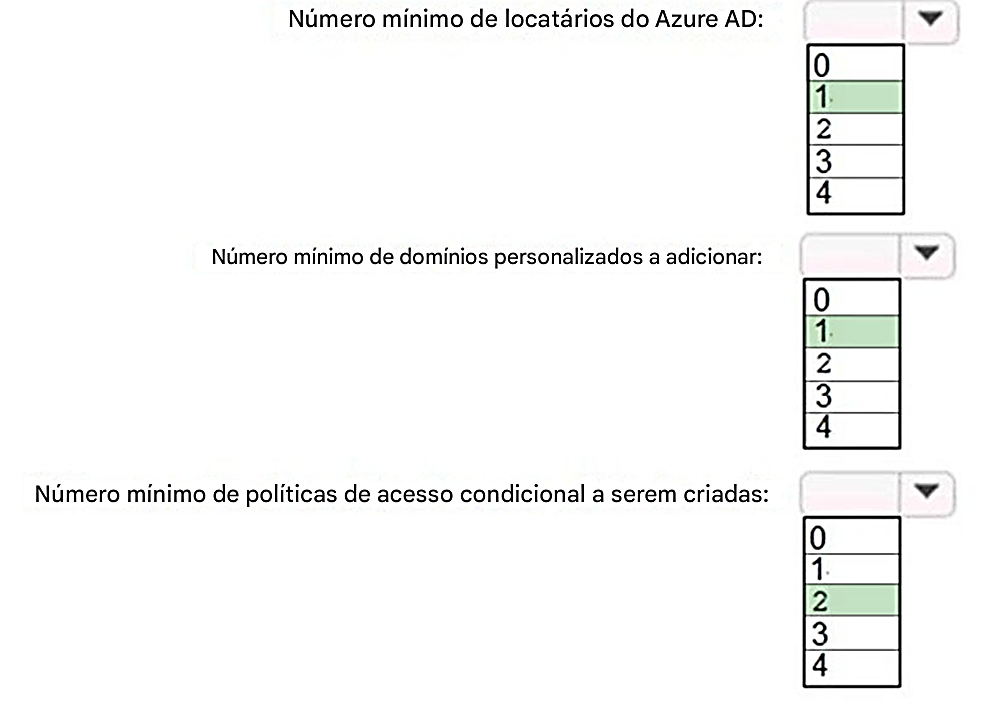
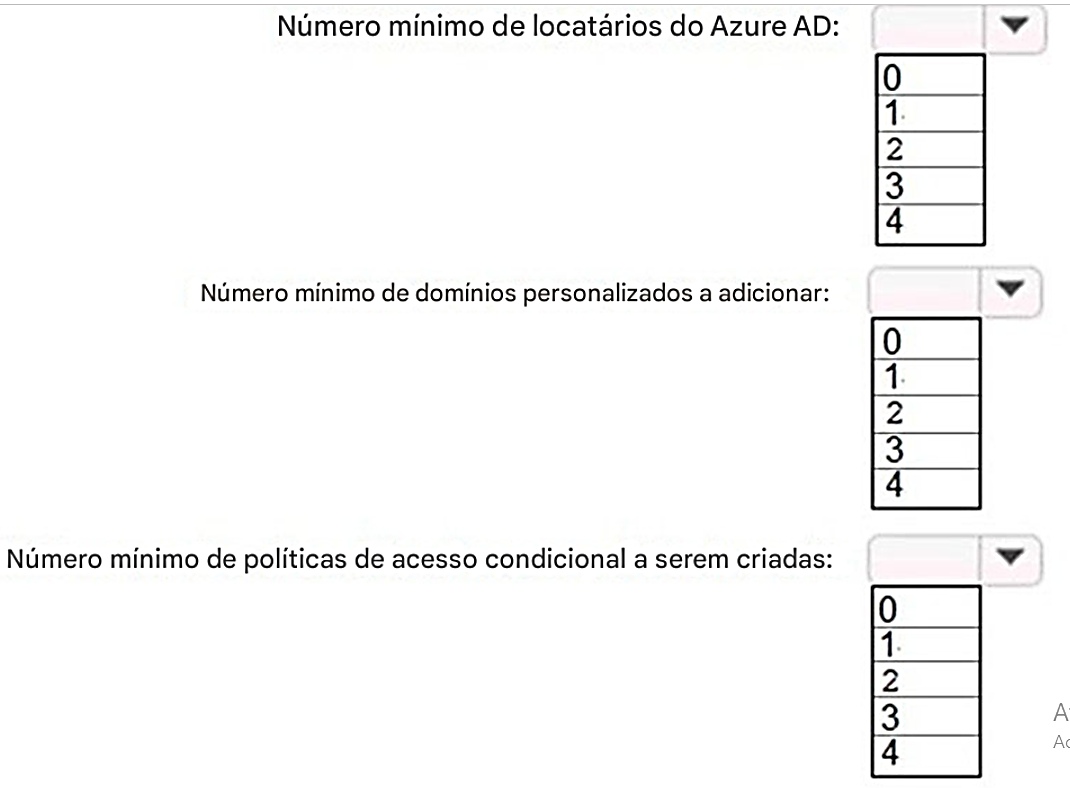
Implante controladores de domínio para a floresta rd.fabrikam.com em redes virtuais no Azure.

**Resposta correta:**  
A  
sincronização de diretório entre o Azure Active Directory (Azure AD) e corp.fabrikam.com não deve ser afetada por uma falha de link entre o Azure e a rede local. (Isso requer controladores de domínio no Azure).  
Os usuários na rede local devem conseguir se autenticar em corp.fabrikam.com se um link de Internet falhar. (Isso requer controladores de domínio locais).

**Pergunta nº 214**

Informações introdutórias Estudo de caso -  
  
   
Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta  Para atender aos requisitos de autenticação da Fabrikam, o que você deve incluir na solução? .  
   
   




**Resposta correta:**  
  
Caixa 1: 1 -  
Um único locatário do Azure AD é necessário, pois apenas o locatário Corp é migrado.  
  
Caixa 2: 1 -  
  
Caixa 3: 2 -  
Uma política de acesso condicional para Autenticação Multifator (MFA) será usada para acesso administrativo e uma segunda política de acesso condicional para impedir acesso externo.  
Referência:  
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa>

**Pergunta nº 215**

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta Você precisa recomendar uma solução de notificação para o grupo de distribuição de Suporte de TI.  
O que você deve incluir na recomendação?

1. **UM**

uma conta SendGrid com relatórios avançados

1. **B**

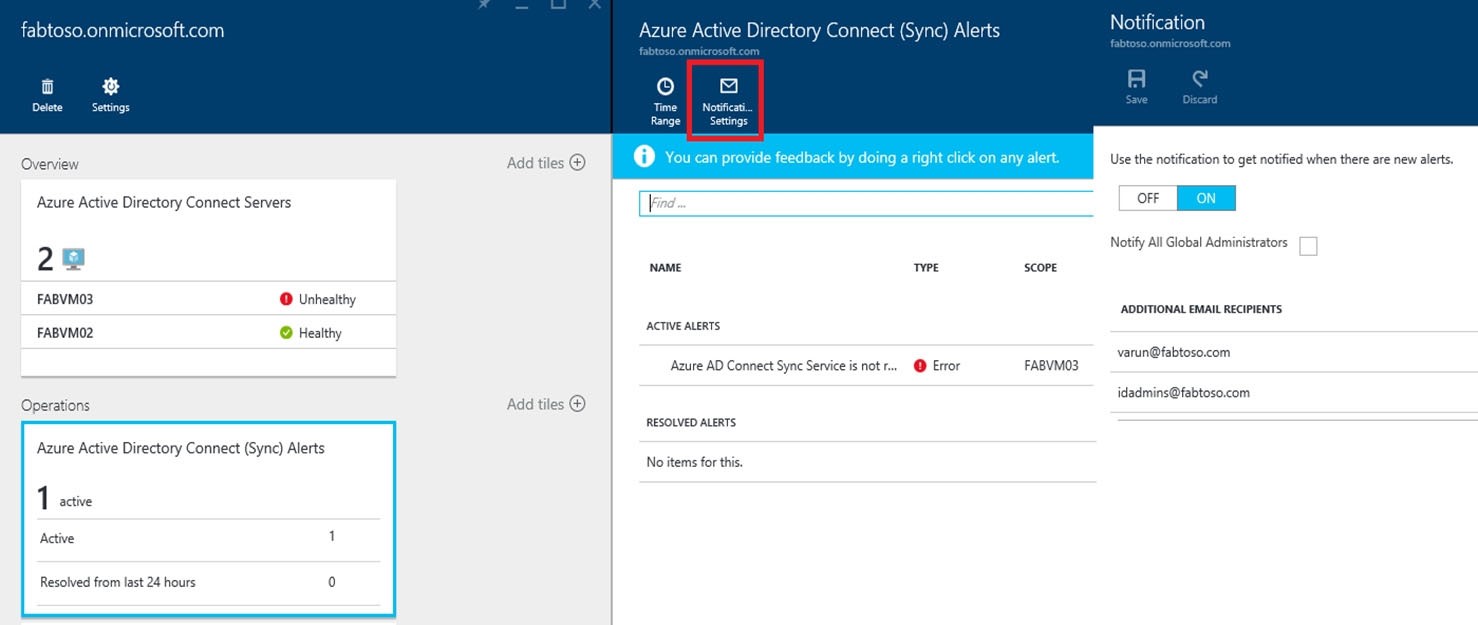
um grupo de ação

1. **C**

Observador de rede do Azure

1. **E**

Azure AD Connect Saúde

**Resposta correta:**D [?️](https://www.secexams.com/exams/Microsoft/az-305/view/)Um grupo de distribuição de e-mail chamado Suporte de TI deve ser notificado sobre quaisquer problemas relacionados aos serviços de sincronização de diretório.  
Observação: você pode configurar o serviço Azure AD Connect Health para enviar notificações por e-mail quando alertas indicarem que sua infraestrutura de identidade não está íntegra. Isso ocorre quando um alerta é gerado e quando ele é resolvido.  
  
Referência:  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations>

**Pergunta nº 216**

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta Você precisa recomendar uma solução para atender aos requisitos de retenção do banco de dados.  
O que você deve recomendar?

1. **UM**

Configure uma política de retenção de longo prazo para o banco de dados.

1. **B**

Configurar o Azure Site Recovery.

1. **C**

Use backups automáticos do Banco de Dados SQL do Azure.

1. **E**

Configurar geo-replicação do banco de dados.

**Resposta correta:**A [?️](https://www.secexams.com/exams/Microsoft/az-305/view/)Cenário: Os backups de banco de dados devem ser retidos por um mínimo de sete anos para atender aos requisitos de conformidade.  
Muitos aplicativos têm fins regulatórios, de conformidade ou outros fins comerciais que exigem que você retenha backups de banco de dados além dos 7 a 35 dias fornecidos pelos  
backups automáticos do Banco de Dados SQL do Azure e da Instância Gerenciada do SQL do Azure. Ao usar o recurso de retenção de longo prazo (LTR), você pode armazenar  
backups completos especificados do Banco de Dados SQL e da Instância Gerenciada do SQL no armazenamento de Blobs do Azure com redundância configurada por até 10 anos. Os backups LTR podem então ser restaurados como um novo banco de dados.  
Referência:  
<https://docs.microsoft.com/en-us/azure/azure-sql/database/long-term-retention-overview>

**Pergunta nº 219**

Informações introdutórias Estudo de caso -  
  
 Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta Você precisa recomendar uma estratégia de armazenamento de dados para o WebApp1.  
O que você deve incluir na recomendação?

1. **UM**

uma máquina virtual do Azure que executa o SQL Server

1. **B**

um banco de dados SQL do Azure DTU de tamanho fixo

1. **C**

um pool elástico do Banco de Dados SQL do Azure

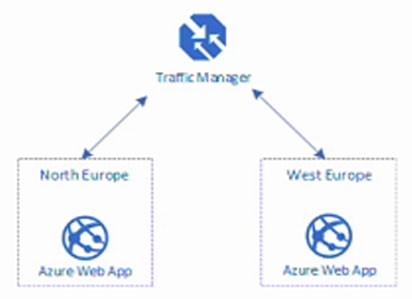
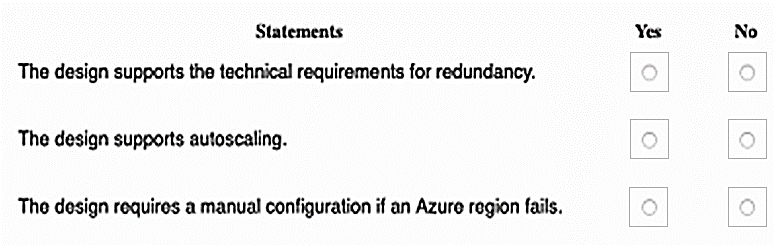
1. **E**

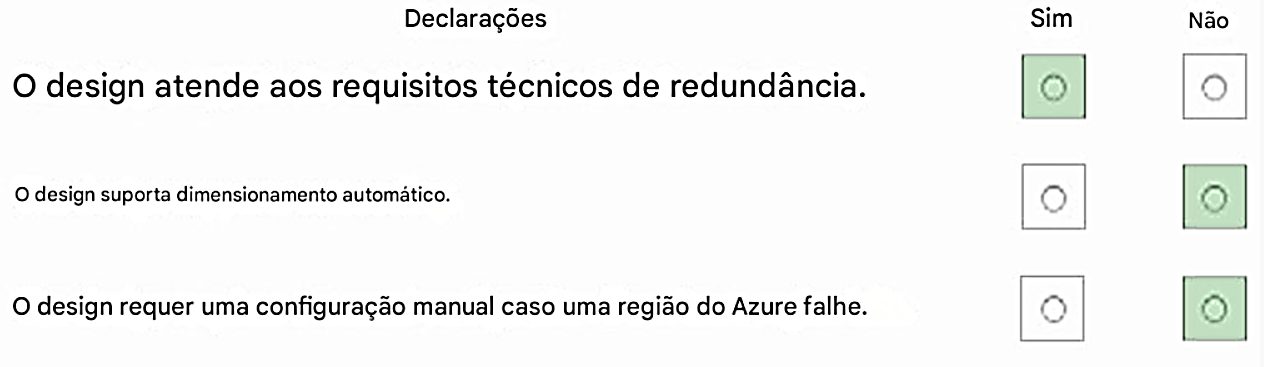
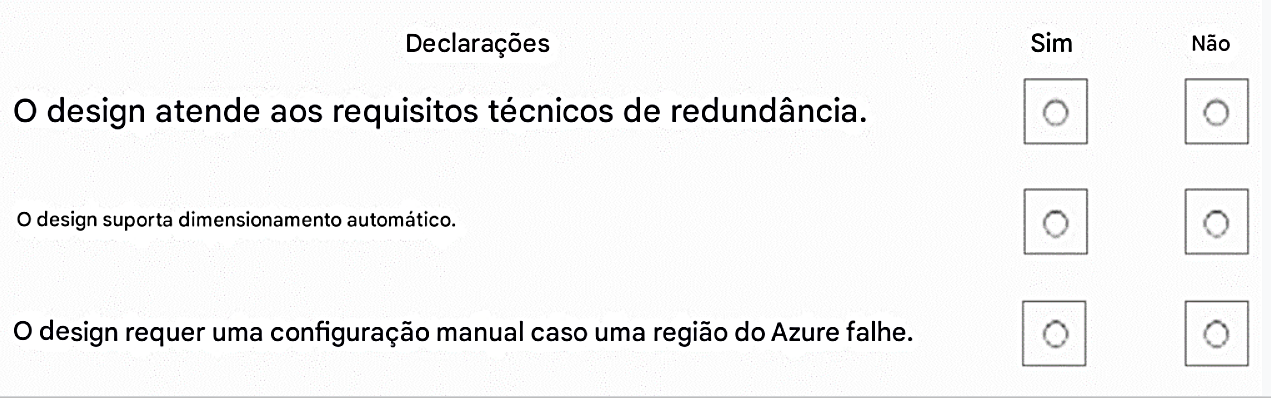
um banco de dados SQL do Azure baseado em vCore

**Resposta correta:**D [?️](https://www.secexams.com/exams/Microsoft/az-305/view/)O uso do WebApp1 é imprevisível. Em horários de pico, os usuários geralmente relatam atrasos. Em outros momentos, muitos recursos do WebApp1 são subutilizados.  
As métricas do banco de dados para a instância de produção do WebApp1 devem estar disponíveis para análise para que os administradores do banco de dados possam otimizar as configurações de desempenho.  
Observação: um núcleo virtual (vCore) representa uma CPU lógica e oferece a opção de escolher entre gerações de hardware e as características físicas do hardware (por exemplo, o número de núcleos, a memória e o tamanho do armazenamento). O modelo de compra baseado em vCore oferece flexibilidade, controle, transparência do consumo de recursos individuais e uma maneira direta de traduzir os requisitos de carga de trabalho locais para a nuvem. Este modelo otimiza o preço e permite que você escolha recursos de computação, memória e armazenamento com base nas suas necessidades de carga de trabalho.  
Incorreto:  
Não C: Os pools elásticos do Banco de Dados SQL do Azure são uma solução simples e econômica para gerenciar e dimensionar vários bancos de dados, não para um único banco de dados.  
Referência:  
<https://docs.microsoft.com/en-us/azure/azure-sql/database/service-tiers-sql-database-vcore>

**Pergunta #225**

Informações introdutórias Estudo de caso -  
   
 Visão geral -  
Fabrikam, Inc. é uma empresa de engenharia que tem escritórios em toda a Europa. A empresa tem um escritório principal em Londres e três filiais em Amsterdã,  
Berlim e Roma.

Pergunta  Você projeta uma solução para a camada da web do WebApp1, conforme mostrado na exposição.  
  
Para cada uma das seguintes afirmações, selecione Sim se a afirmação for verdadeira. Caso contrário, selecione Não.  
   
   




**Resposta correta:**   
Caixa 1: Sim -  
Todas as novas implantações no Azure devem ser redundantes caso uma região do Azure falhe.  
O Traffic Manager é resiliente a falhas, incluindo a falha de uma região inteira do Azure.  
  
Caixa 2: Não -  
O Traffic Manager fornece balanceamento de carga, mas não dimensionamento automático.  
  
Caixa 3: Não -  
Failover automático usando o Azure Traffic Manager: quando você tem arquiteturas complexas e vários conjuntos de recursos capazes de executar a mesma função, você pode configurar o Azure Traffic Manager (com base no DNS) para verificar a integridade dos seus recursos e rotear o tráfego do recurso não íntegro para o recurso íntegro.  
Referência:  
<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview> <https://docs.microsoft.com/en-us/azure/networking/disaster-recovery-dns-traffic-manager>