Microsoft.AZ-700J.v2026-08-18.q149

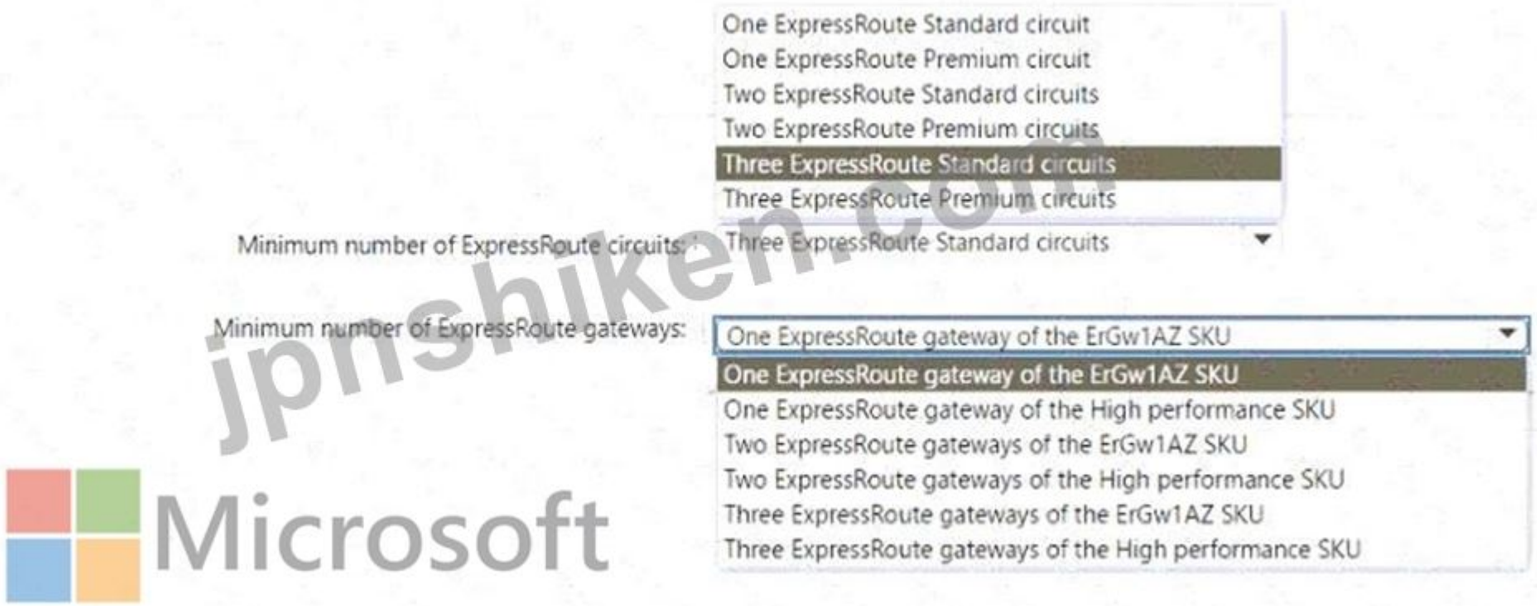
試験コード：	AZ-700J
試験名称：	Designing and Implementing Microsoft Azure Networking Solutions (AZ-700日本語版)
認証ベンダー：	Microsoft
無料問題の数：	149
バージョン：	v2026-08-18
ページの閲覧量：	105
問題集の閲覧量：	1521

https://www.jpnshiken.com/shiken/Microsoft.AZ-700J.v2026-08-18.q149.html

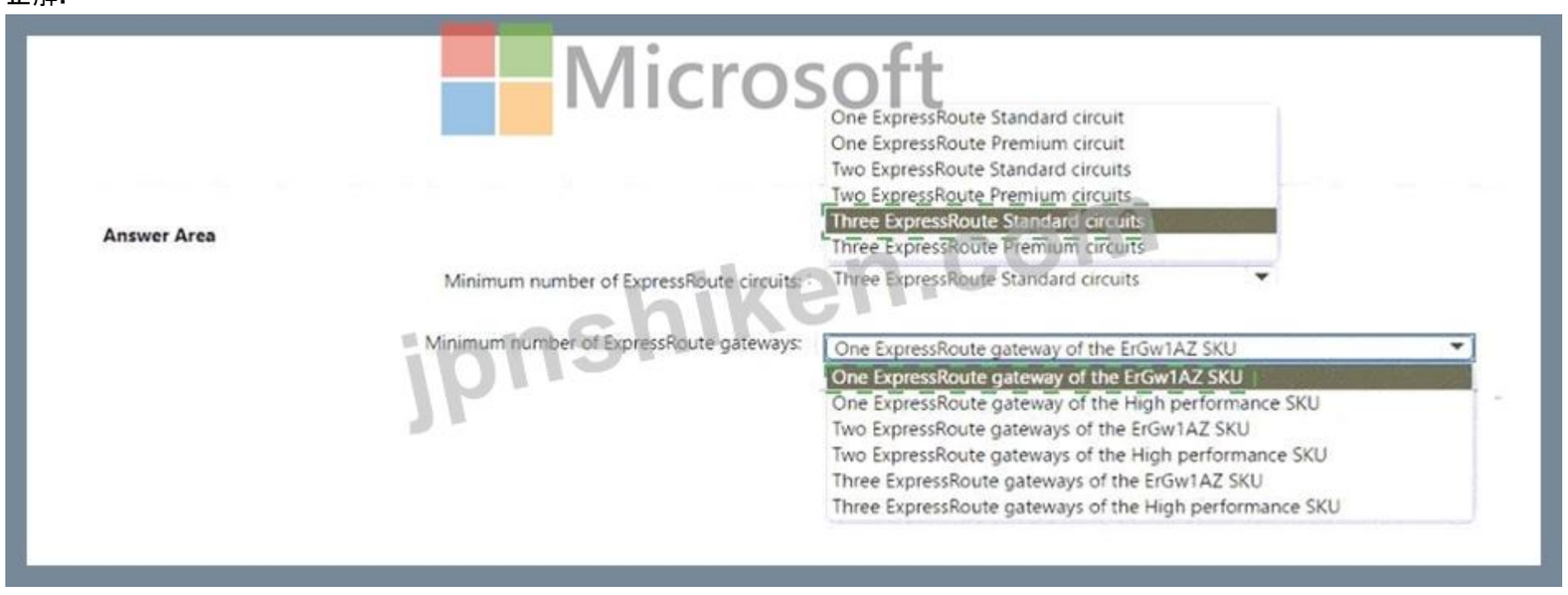
質問: **1**
Azure仮想ネットワーク内のサブネットのIPアドレス割り当てを計画しています。サブネット内でIPアドレスが必要なリソースの種類はどれですか？
A. Azure 仮想ネットワーク NAT
B. サービスエンドポイント
C. プライベートエンドポイント
D. 仮想ネットワークピアリング
正解: (正解を表示します)

質問: **2**
オンプレミスのデータセンターがあります。
Azureサブスクリプションには、米国東部Azureリージョンに10台の仮想マシンとVNe1Iという仮想ネットワークが含まれています。これらの仮想マシンはVNet1に接続され、3つの可用性ゾーンにレプリケートされています。
ExpressRouteを使用してデータセンターをVNetl1に接続する必要があります。ソリューションは以下の要件を満たす必要があります。
* 2 つの可用性ゾーンに障害が発生した場合でも、仮想マシンへの接続を維持します。
* 1000Mbps接続をサポート
解答には何を含めるべきですか？回答するには、回答エリアで適切な選択肢を選択してください。注意：
正しい選択ごとに 1 ポイントが与えられます。

Answer Area



正解:



Explanation:

質問: **3**

次の表に示す仮想マシンを含む Azure サブスクリプションがあります。

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1 と Subnet2 は、次の送信規則を持つ NSG1 という名前のネットワーク セキュリティ グループ (NSG) に関連付けられています。

* 優先度: 100
* ポート: 任意
* プロトコル: 任意
* 出典: 任意
* 宛先: ストレージ
* アクション: 拒否

次の設定を持つプライベート エンドポイントを作成します。

* 名前: プライベート1
* リソースの種類: Microsoft.Storage/storageAccounts
* リソース: ストレージ1
* ターゲットサブリソース: blob
* 仮想ネットワーク: Vnet1
* サブネット: サブネット1

以下の各文について、該当する場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:
Yes, Yes, Yes
NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint.So the NSG1 doesn't limit storage access from either VM1 or VM2. https://docs.microsoft.com/en-us/azure/storage
/common/storage-private-endpoints#network-security-group-rules-for-subnets-with-private-endpoints

質問: **4**
次の表に示すサブネットを含むAzure仮想ネットワークがあります。

Name	IP address space
AzureFirewallSubnet	192.168.1.0/24
Subnet2	192.168.2.0/24

AzureファイアウォールをAzureFirewallSubnetにデプロイします。Subnet2からファイアウォールを介してすべてのトラフィックをルーティングします。
Subnet2上のすべてのホストがhttps ://*.contoso.comにある外部サイトにアクセスできることを確認する必要があります。
あなたは何をするべきか？
A. ファイアウォールポリシーで、ネットワークルールを作成します。
B. ネットワークセキュリティグループ (NSG) を作成し、NSGをSubnet2に関連付けます。
C. ファイアウォールポリシーで、アプリケーションルールを作成します。
D. ファイアウォールポリシーで、DNATルールを作成します。
正解: **(**正解を表示します**)**

質問: **5**
App1 という名前の Web アプリをホストし、次のような構成を持つオンプレミスの Web サーバーがあります。
* IPアドレス 131.107.50.60
* FQDN server1.contoso.com
Azure サブスクリプションをお持ちです。
Azure Front Door を使用して App1 を公開する必要があります。ソリューションは以下の要件を満たしている必要があります。
* インターネット ユーザーが appl.contoso.com の FQDN を使用して App1 に接続できることを確認します。
* サーバー 1 を Azure に移行した場合に、Front Door の構成に必要な変更を最小限に抑えます。
解決策には何を含めるべきですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

質問: **6**

タスク7

サブネット4-1に100台の仮想マシンをデプロイする予定です。これらの仮想マシンにはパブリックIPアドレスは割り当てられません。これらの仮想マシンは、サードパーティがホストする同じAPIを呼び出します。仮想マシンは、このAPIに対して1分あたり10,000回以上の呼び出しを行う予定です。

SNATポート枯渇のリスクを最小限に抑える必要があります。ソリューションは管理作業を最小限に抑える必要があります。

正解:

See the Explanation below for step by step instructions.

Explanation:

To minimize the risk of SNAT port exhaustion for your 100 virtual machines in subnet4-1, while ensuring minimal administrative effort, you can use an Azure NAT Gateway. This service provides scalable and resilient outbound connectivity for virtual networks, dynamically allocating SNAT ports to avoid exhaustion.

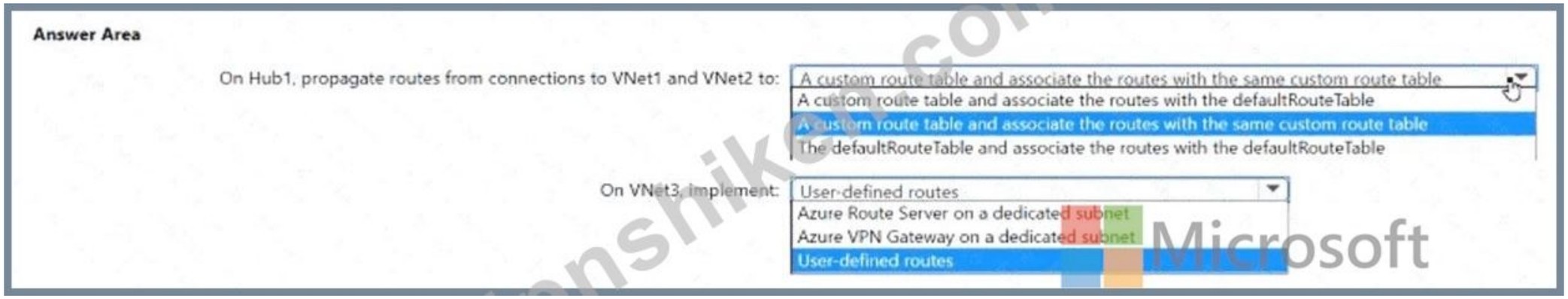
* Navigate to the Azure Portal.
* Search for "NAT gateways" and select it.
* Click on "Create".
* Enter the following details:
* Subscription: Select your subscription.
* Resource Group: Select an existing resource group or create a new one.
* Name: Enter a name for the NAT gateway (e.g., NATGateway-Subnet4-1).
* Region: Select the region where your virtual network is located.

* Click on "Next: Outbound IP".
* Choose whether to use existing public IP addresses or create new ones.
* If creating new ones, click on "Add new" and configure the new public IP addresses.
* Click on "Next: Subnet".
* Click on "Associate subnet".
* Select the virtual network that contains subnet4-1.
* Select subnet4-1 from the list of subnets.
* Click on "OK".
* Review your settings to ensure everything is correct.
* Click on "Review + create" and then "Create".
* Azure NAT Gateway: This service provides outbound connectivity for virtual networks, dynamically allocating SNAT ports across all VM instances within a subnet. This dynamic allocation helps prevent SNAT port exhaustion, especially in scenarios with high outbound connection volumes12.
* Dynamic SNAT Port Allocation: Unlike static allocation methods, NAT Gateway dynamically allocates SNAT ports based on demand, ensuring efficient use of available ports and reducing the risk of exhaustion2.
Step-by-Step SolutionStep 1: Create a NAT GatewayStep 2: Configure Outbound IP AddressesStep 3:
Associate the NAT Gateway with Subnet4-1Step 4: Review and CreateExplanationBy following these steps, you can ensure that your 100 virtual machines in subnet4-1 can make the necessary API calls without running into SNAT port exhaustion, all while minimizing administrative effort.

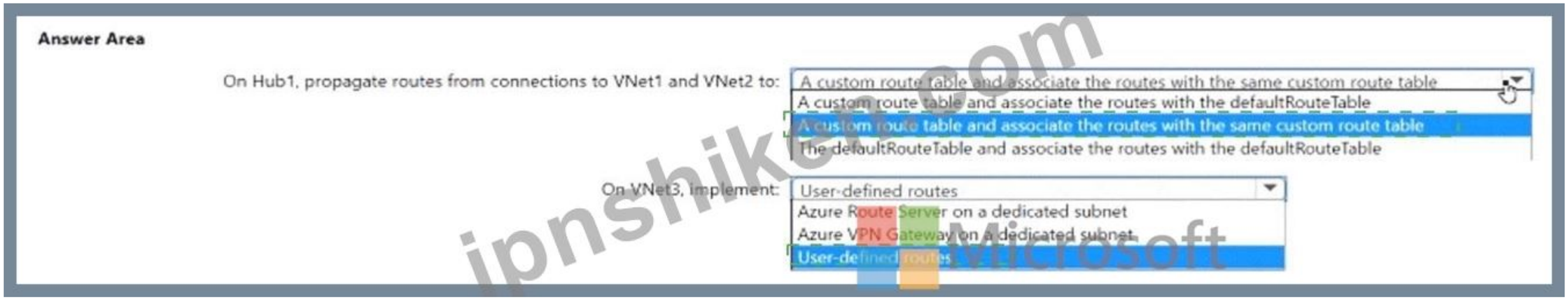
質問: 7
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
VWAN1	Azure Virtual WAN	Standard Virtual WAN
Hub1	Azure Virtual WAN hub	Hub for VWAN1
VNet1	Virtual network	Connected to Hub1
VNet2	Virtual network	Connected to Hub1
VNet3	Virtual network	Peered with VNet2
NVA1	Virtual machine	Hosts a routing appliance deployed to VNet2

NVA1 と Hub1 の間に BGP ピアリングを確立します。
BGPピアリングを使用して、Hub1経由でVNet1とVNet3間のトランジット接続を実装する必要があります。ソリューションはコストを最小限に抑える必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

質問: **8**

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Description
App1	Web app
FD1	Azure Front Door Premium profile that has an endpoint and an origin group

次の要件を満たすようにソリューションを構成する必要があります。

* App1にはプライベートエンドポイントを割り当てる必要があります
* インターネットから App1 へのアクセスは FD1 経由でルーティングする必要があります。

FD1 では何を設定する必要がありますか?

A. トラフィックをリダイレクトするセキュリティポリシー

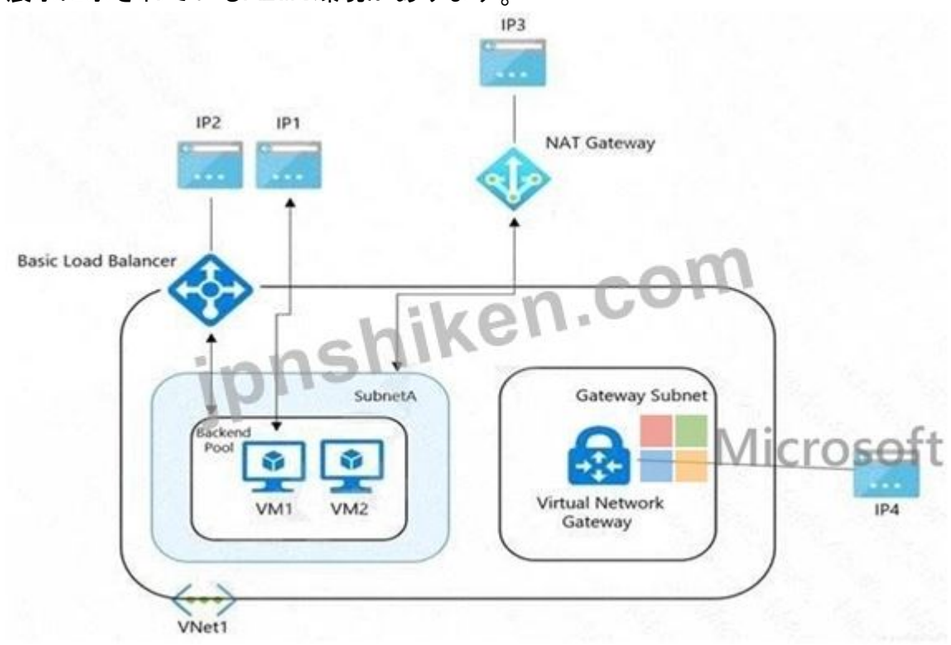
B. ルート設定の上書きアクションを持つルール

C. Azure Private Link サービスを有効にするオリジン

D. トラフィックをリダイレクトするルート
正解: (正解を表示します)

質問: **9**
VM1 という仮想マシンと NSG1 というネットワーク セキュリティ グループ (NSG) を含む Azure サブスクリプションがあります。NSG1 にはデフォルトのルールが設定されており、VM1 は Windows Server を実行し、NIC1 という 1 つの NIC が含まれています。NIC1 は NSG1 に関連付けられています。
VM1 上の Azure Instance Metadata Service (IMDS) REST API へのアクセスを防止する必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。
NSG1に何を追加すべきでしょうか?
A. サービスタグへのトラフィックをブロックする送信ルール
B. IPアドレスへのトラフィックをブロックする受信ルール
C. IPアドレスへのトラフィックをブロックする送信ルール
D. アプリケーション セキュリティ グループへのトラフィックをブロックする受信および送信のルール。
正解: (正解を表示します)

質問: **10**
展示に示されているAzure環境があります。



VM1は、インスタンスレベルのパブリックIPアドレス（ILPIP）を持つ仮想マシンです。
Basic Load Balancerは、パブリックIPアドレスを使用します。VM1とVM2はバックエンドプールにあります。
NATゲートウェイは、SubnetAに関連付けられているIP3という名前のパブリックIPアドレスを使用します。
VNet1には、IP4という名前のパブリックIPアドレスを持つ仮想ネットワークゲートウェイがあります。
VM1からインターネットへのアウトバウンドトラフィックを開始する場合、どのパブリックアドレスが使用されますか？
A. IP4
B. IP1
C. IP2

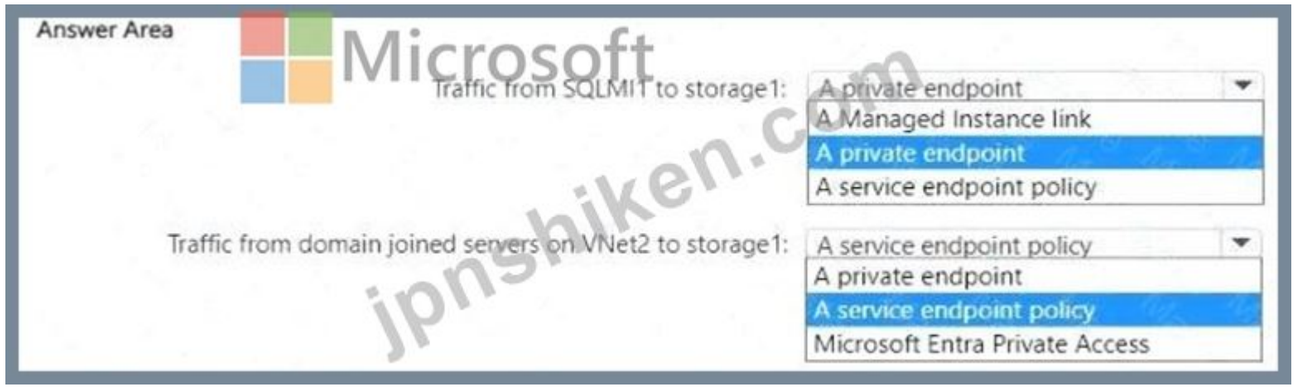
D. IP3
正解: **(**正解を表示します**)**

質問: **11**
AzFW1 という名前の Azure Firewall Standard のインスタンスを含む Azure サブスクリプションがあります。以下を有効にする予定です。
* TLS検査
* 脅威情報
* ネットワーク侵入検知および防止システム（IDPS）
AzFW1 を使用すると何が可能になりますか?
A. TLS 検査、脅威インテリジェンス、IDPS
B. 脅威インテリジェンスとIDPSのみ
C. 脅威情報のみ
D. TLS検査とIDPSのみ
E. TLS 検査のみ
正解: **C (**コメントを発表する**)**

質問: **12**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Location	Description
SQLMI1	Azure SQL Managed Instance	US East	Managed instance connected to VNet1
contoso.com	Microsoft Entra Domain Services	US East	Domain connected to VNet2
VNet1	Virtual network	US East	*None*
VNet2	Virtual network	US East	*None*
storage1	Storage account	US East	*None*

次のシナリオでは、ネットワーク トラフィックが Azure バックボーン ネットワーク経由でルーティングされるようにする必要があります。
* SQIMI1からストレージ1へのトラフィック
* VNet2 上のドメイン参加サーバーからストレージ 1 へのトラフィック
ソリューションではコストを最小限に抑える必要があります。
各シナリオでは何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

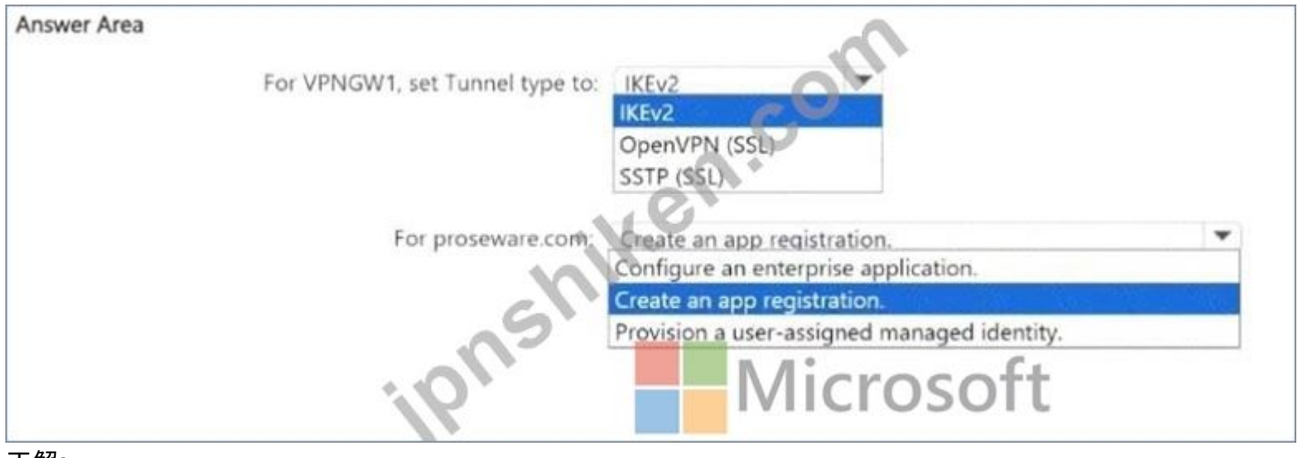
Explanation:

質問: **13**

接続要件を満たすように P2S VPN を構成する必要があります。

どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Explanation:

質問: 14

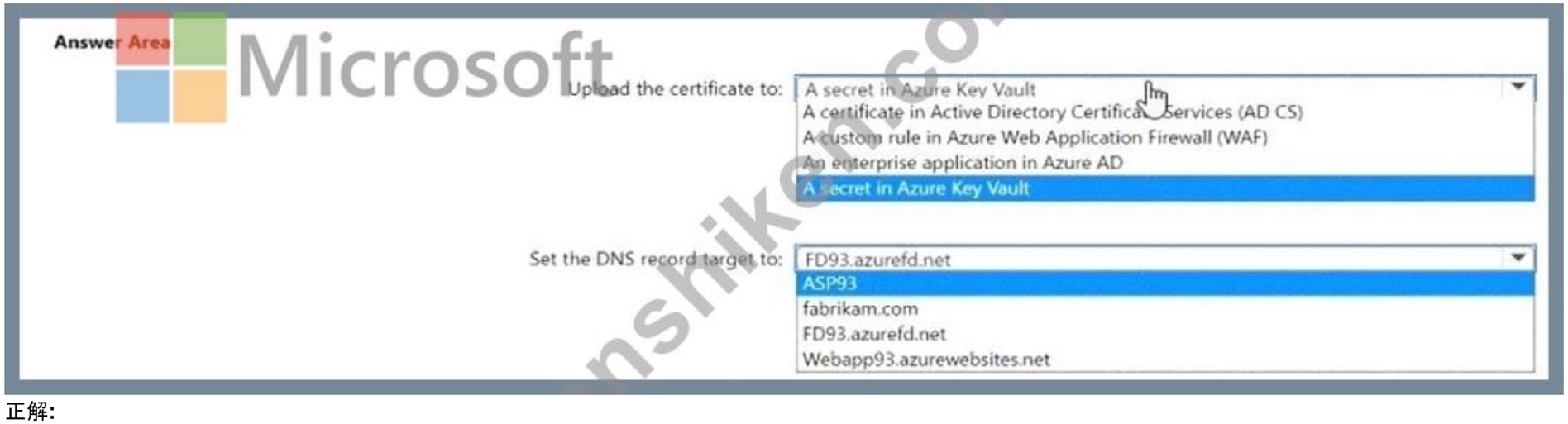
次の表に示すリソースを含む Azure Front Door の展開を計画しています。

Name	Type
ASP93	App Service plan
Webapp93.azurewebsites.net	App Service
FD93.azurefd.net	Front Door

ユーザーは、https://www.fabrikarn.com の URL を使用して、Front Door 経由で App Service に接続します。

www.fabfikam.com のホスト名の証明書を取得します。

www.fabrikam.com の DNS レコードを構成し、証明書を Azure にアップロードする必要があります。どうすればよいでしょうか？回答するには、回答エリアで適切な選択肢を選択してください。注: 正解は 1 点です。



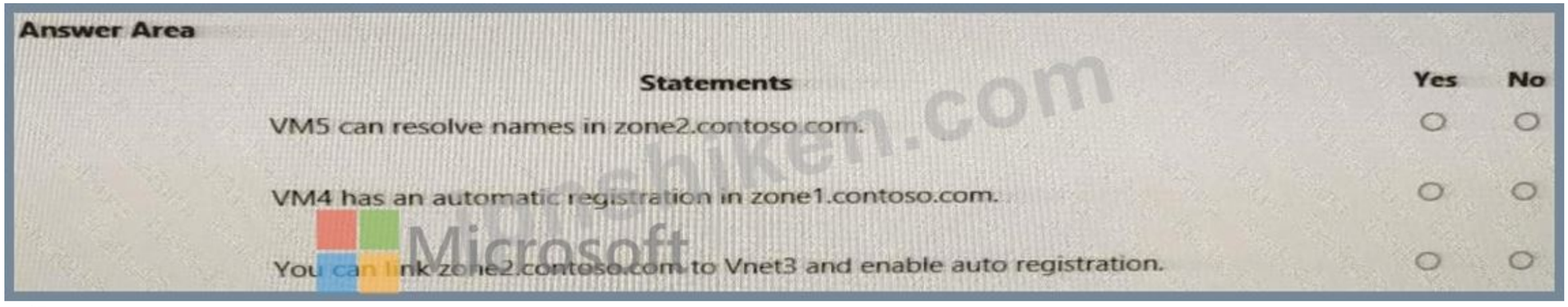
正解:

Explanation:

質問: **15**

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

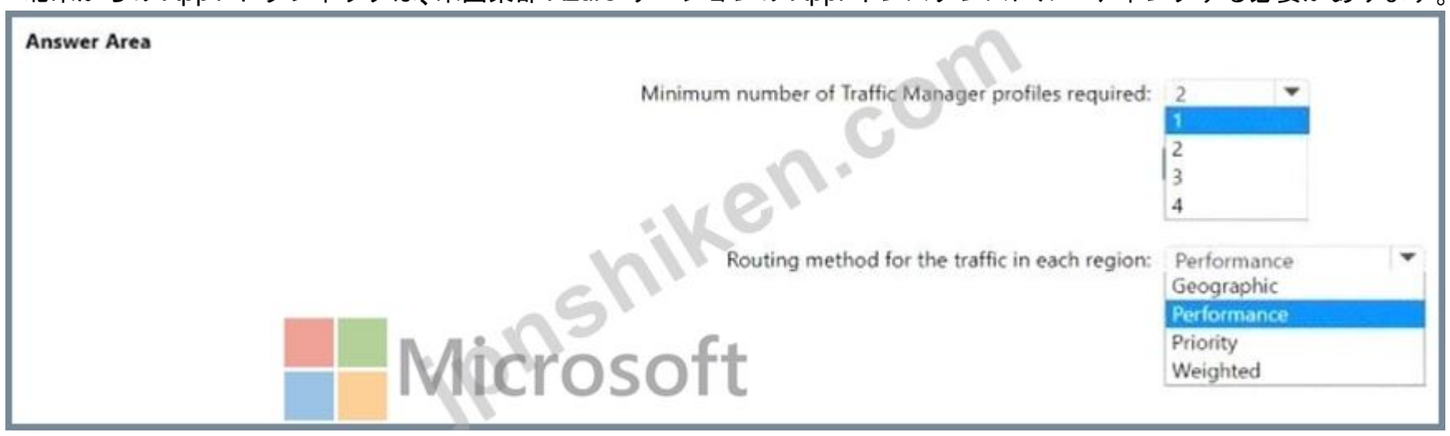
質問: **16**

Appl という名前のアプリを含む Azure サブスクリプションがあります。App1 は、次の表に示す Azure App Service インスタンスでホストされています。

Name	Location
AppSrv1	East US
AppSrv2	East US
AppSrv3	North Europe
AppSrv4	North Europe

次の要件を満たすには、Azure Traffic Manager を実装する必要があります。

* App1 トラフィックは、各 Azure リージョン内の各 App Service インスタンスに均等に割り当てる必要があります。
* 北ヨーロッパからの App1 トラフィックは、北ヨーロッパ リージョンの Appl インスタンスにルーティングする必要があります。
* 北米からの App1 トラフィックは、米国東部 Azure リージョンの Appl インスタンスにルーティングする必要があります。

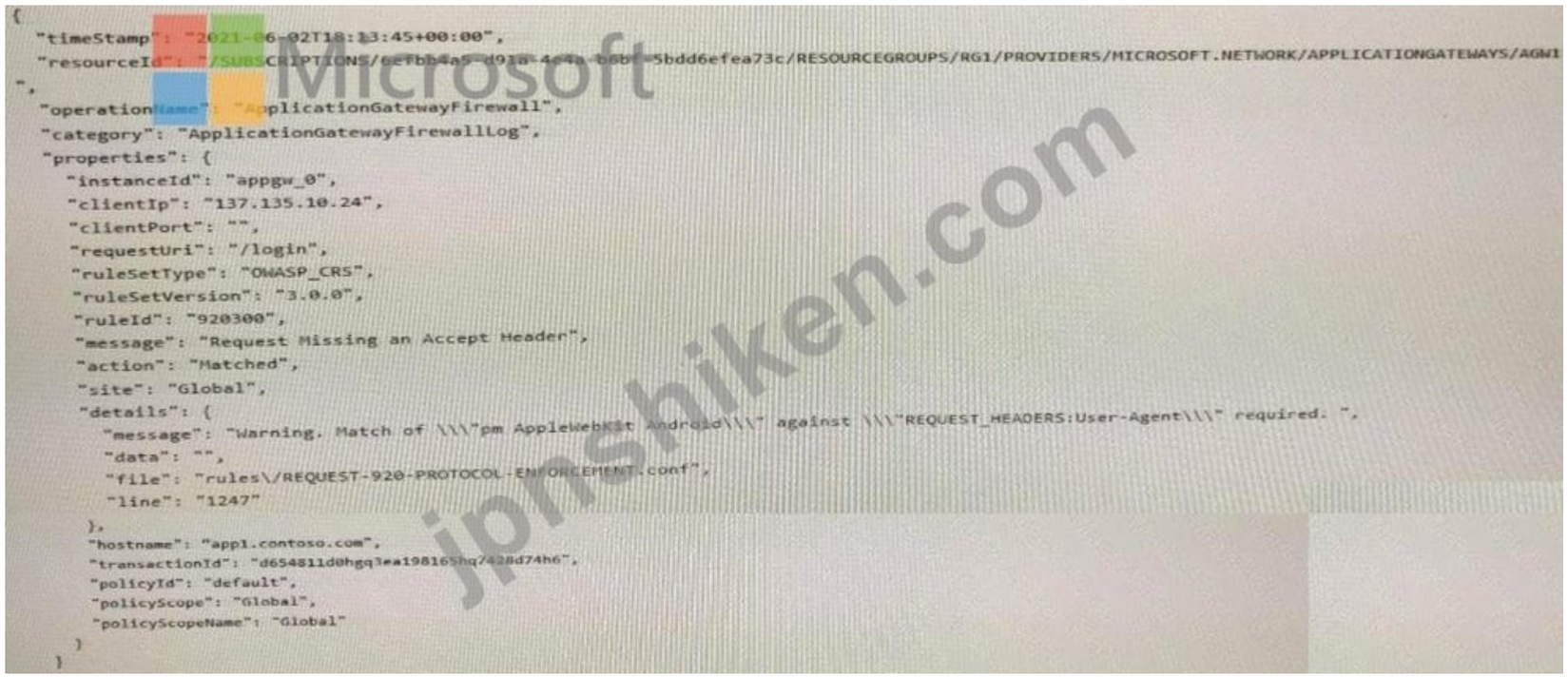


正解:

Explanation:

質問: **17**
FD1からの接続のみを許可するように、APPGWI-WAFPolicyのカスタムルールを設定する必要があります。ソリューションは計画されている変更をサポートする必要があります。
どのマッチタイプとマッチ変数を選択する必要がありますか?
A. 文字列とリクエストCookie
B. 文字列とリクエストヘッダー
C. IPアドレスとRemoteAddr
D. 地理的位置とRemoteAddr
正解: **(**正解を表示します**)**

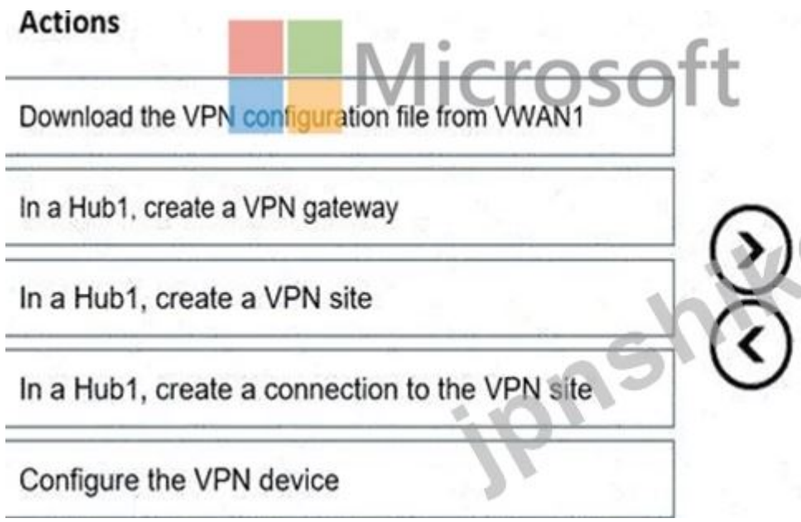
質問: **18**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Web Application Firewall（WAF）が有効になっているAzureアプリケーションゲートウェイがあります。
トラフィックをアプリケーションゲートウェイのURLに転送するようにアプリケーションゲートウェイを構成します。
URLにアクセスしようとすると、HTTP403エラーが発生します。診断ログを表示して、次のエラーを発見します。



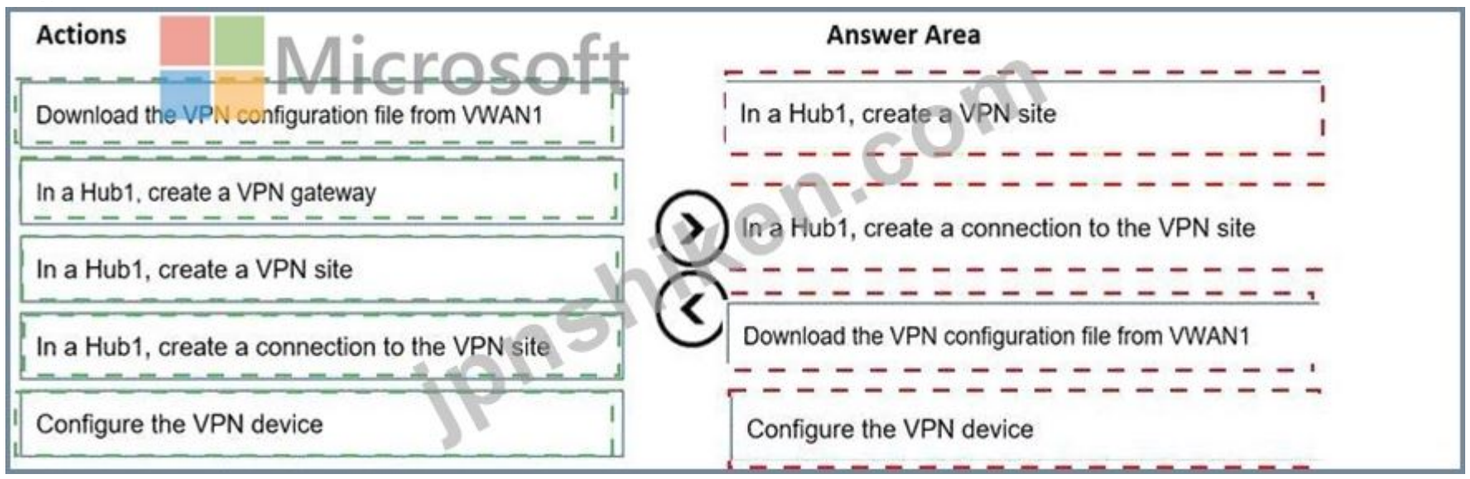
URLがアプリケーションゲートウェイを介してアクセス可能であることを確認する必要があります。
解決策 :137.135.10.24を含むWAFポリシー除外リクエストヘッダーを作成します。
これはヤギに会いますか？

A. はい
B. いいえ
正解: **(**正解を表示します**)**

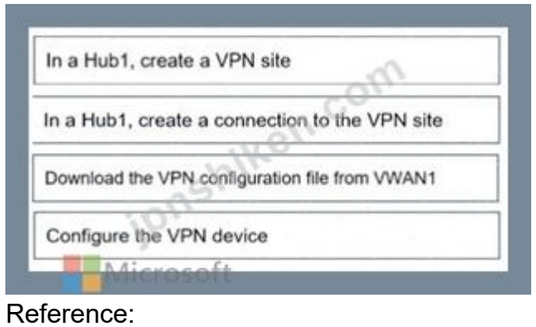
質問: **19**
オンプレミスのサイトが 3 つあります。各サイトにはサードパーティの VPN デバイスが設置されています。
VWAN1 という名前の Azure 仮想 WAN があり、Hub1 というハブがあります。Hub1 は、サイト間 VPN 接続を使用して、3 つのオンプレミス サイトのうち 2 つに接続します。
Hub1 を使用して、3 番目のサイトを他の 2 つのサイトに接続する必要があります。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal

質問: **20**
次の表に示す Azure 仮想ネットワークがあります。

Name	Subnet	Subnet address space	Peered with
Vnet1	Subnet1-1	10.1.1.0/24	Vnet3
Vnet2	Subnet2-1	10.2.1.0/24	Vnet3
Vnet3	AzureFirewallSubnet	10.3.1.0/24	Vnet1, Vnet2

Azure Firewall を Vnet3 にデプロイします。
Subnet1-1からSubnet2-1へのトラフィックがファイアウォールを通過するようにする必要があります。どのような設定が必要ですか？
A. Subnet1-1とSubnet2-1に関連付けられたルートテーブル
B. AzureFitewallSubnet に関連付けられたルート テーブル
C. Azure プライベート DNS ゾーン
D. Vnet1 と Vnet2 間のピアリングリンク
正解: (正解を表示します)

質問: **21**
VNetGwy1 という名前の仮想ネットワーク ゲートウェイを含む Azure サブスクリプションがあります。VNetGwy1 のパブリック IP アドレスは 20.25.32.214 です。
VNetGwy1のヘルスプローブをクエリする必要があります。
URI をどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

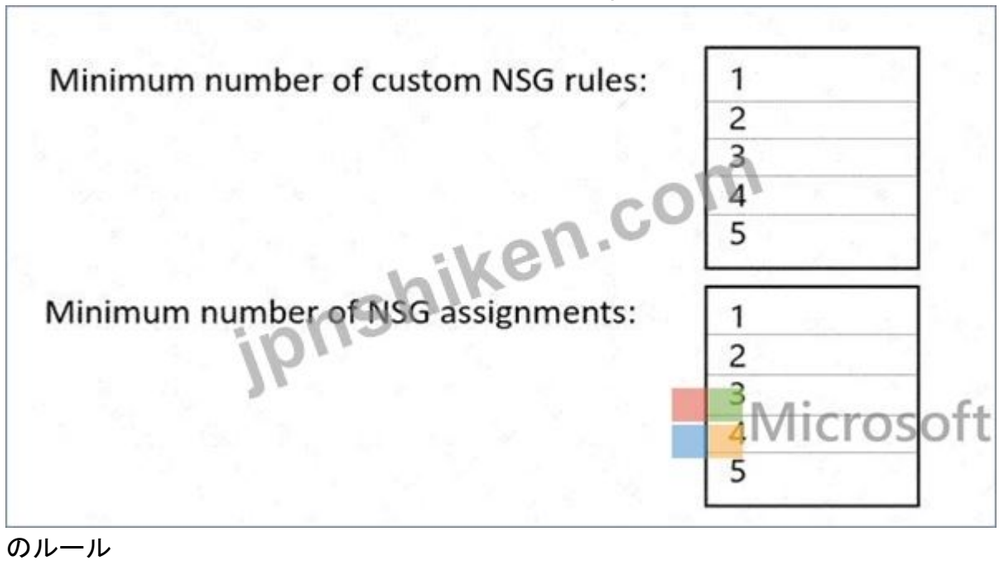
Explanation:

質問: **22**
Site1 という名前のオンプレミス ネットワークがあります。
Azureサブスクリプションには、storage1というストレージアカウントとVNet1という仮想ネットワークが含まれています。VNet1には、Subnet1というサブネットが含まれています。storage1のプライベートエンドポイントはSubnet1に接続されており、Site1はサイト間(S2S)VPNを使用してVNet1に接続されています。
ネットワーク セキュリティ グループ (NSG) を使用して、Site1 から storage1 へのアクセスを制御する必要があります。
まず何をすべきでしょうか?
A. ルート テーブルを Subnet1 に関連付けます。

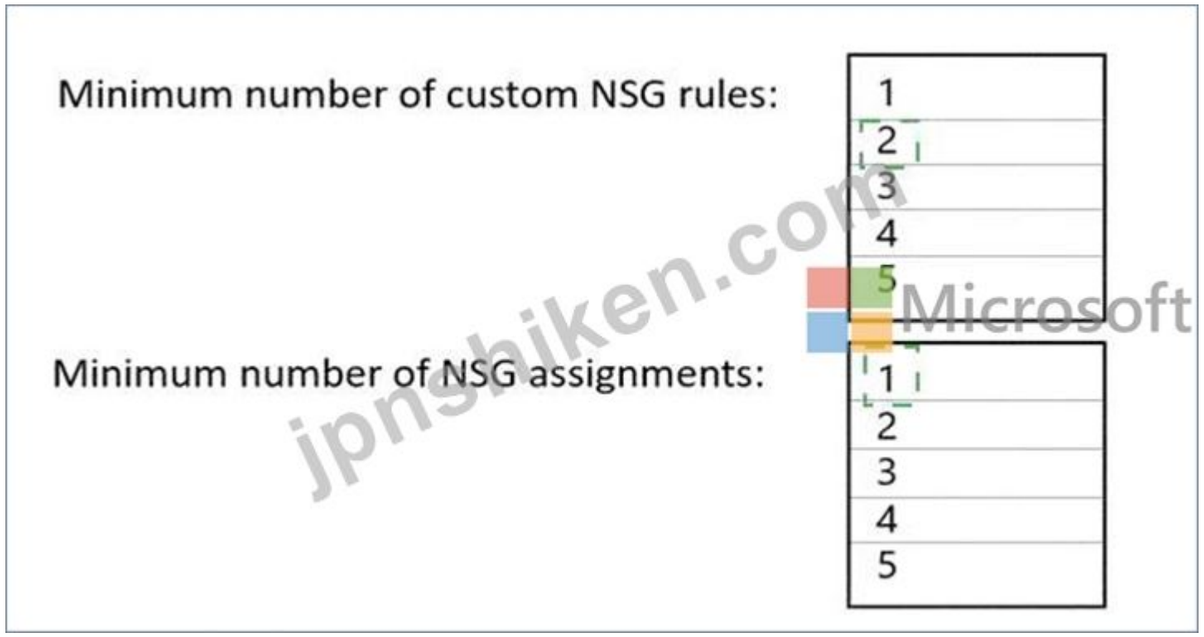
B. Subnet1 にサブネット委任を作成します。
C. NAT ゲートウェイを Subnet1 に関連付けます。
D. Subnet1 上のプライベート エンドポイントのネットワーク ポリシーを構成します。
正解: **(**正解を表示します**)**

質問: **23**
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には、Subnet1 という名前のサブネットが含まれています。
Subnet1 にプライベート エンドポイントを追加する予定です。
ユーザー定義のルートを使用して、プライベート エンドポイントと Azure Private Link サービス間のトラフィックをルーティングできることを確認する必要があります。
Subnet1 で最初に何をすべきでしょうか?
A. ネットワーク ポリシーを有効にします。
B. 委任を有効にします。
C. サービス エンドポイントを作成します。
D. 標準の Azure ロード バランサーをプロビジョニングします。
正解: **B (**コメントを発表する**)**

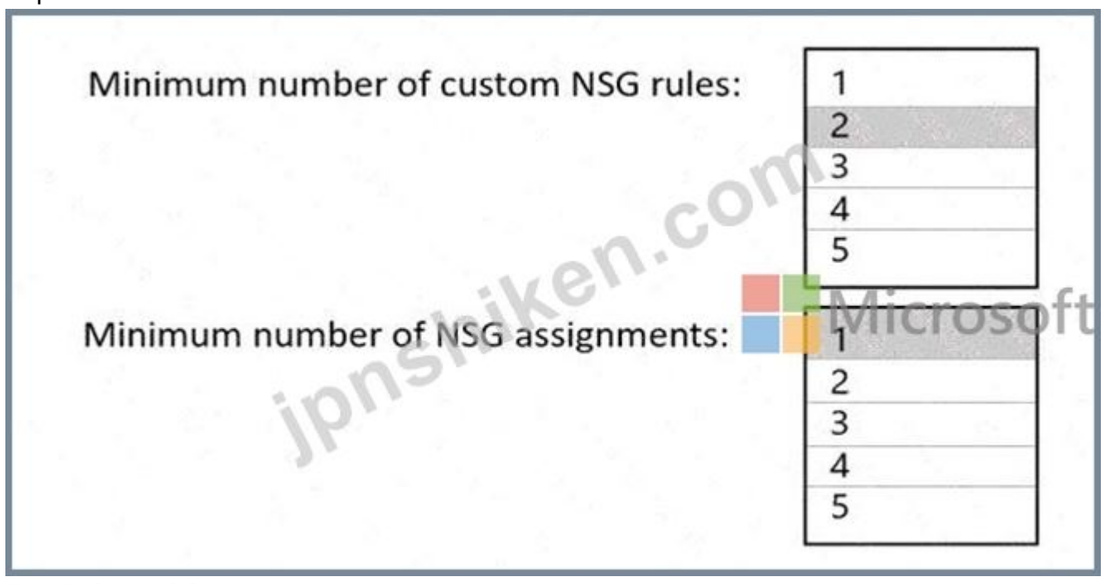
質問: **24**
VMScaleSet1 から VMScaleSet2 へのトラフィックを制限する必要があります。ソリューションは仮想ネットワークの要件を満たしている必要があります。
必要なカスタム NSG ルールと NSG 割り当ての最小数はいくつですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



のルール
正解:



Explanation:



Box 2: One NSG

The minimum requirement is one NSG. You could attach the NSG to VMScaleSet1 and restrict outbound traffic, or you could attach the NSG to VMScaleSet2 and restrict inbound traffic. Either way you would need two custom NSG rules.

Box 1: Two custom rules

With the NSG attached to VMScaleSet2, you would need to create a custom rule blocking all traffic from VMScaleSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.

The default rules in the NSG will allow all other traffic to VMScaleSet2.

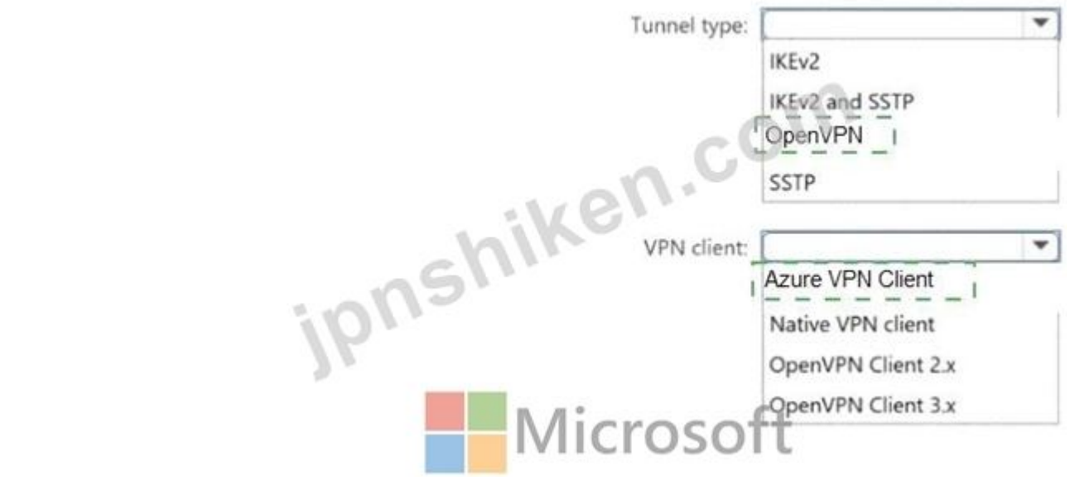
質問: 25

VNet1 という仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には Subnet1 というサブネットが含まれています。Subnet1 に、AppGw1 という Azure Application Gateway v2 インスタンスをデプロイします。NSG1 というネットワーク セキュリティ グループ (NSG) を作成し、NSG1 を Subnet1 にリンクします。
AppGw1 が VNet1 から発信されるトラフィックのみを負荷分散するようにする必要があります。このソリューションは、AppGw1 の機能への影響を最小限に抑える必要があります。
NSG1に何を追加すべきでしょうか?
A. 優先度4096ですべてのインターネットトラフィックをブロックする受信ルール
B. 優先度4096ですべてのインターネットトラフィックをブロックする送信ルール
C. 優先度100ですべてのインターネットトラフィックをブロックする受信ルール
D. 優先度100ですべてのインターネットトラフィックをブロックする送信ルール
正解: **(**正解を表示します**)**

質問: **26**
会社にはAzureサブスクリプションがあり、そこにはVNet1という仮想ネットワークとvGW1というAzure VPNゲートウェイが含まれています。会社にはWindows 11デバイスを所有するユーザーが50人います。
ユーザーがVNet1上のリソースにアクセスできるようにする必要があります。ソリューションは以下の要件を満たす必要があります。
* ユーザーが vGW1 へのポイントツーサイト (P2S) VPN 接続を確立できることを確認します。
* ユーザーが Microsoft Entra 資格情報のみを使用して認証できることを確認します。ユーザーのデバイスでどのタイプのトンネルを構成し、どの VPN クライアントを構成する必要がありますか? 回答するには、回答領域で適切なオプションを選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area

正解:

Answer Area



Explanation:

Answer Area

質問: **27**

次の表に示す Azure 仮想ネットワークがあります。

Name	Resource group	Location
Vnet1	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

次の表に示す Azure リソースがあります。

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
st1	Storage account	*Not applicable*	RG5	UK West

Azure Network Watcher の接続モニターを使用して、リソース間の待機時間を確認する必要があります。
作成する必要がある接続モニターの最小数は何ですか?

A. 5
B. 2
C. 3
D. 1
E. 4
正解: **(**正解を表示します**)**

質問: **28**
仮想ネットワークを含む Azure サブスクリプションがあります。
Azure VPNゲートウェイと90個のサイト間VPN接続をデプロイする予定です。ソリューションは以下の要件を満たす必要があります。
* Azure データセンターに障害が発生した場合でも、サイト間 VPN 接続が引き続き利用可能であることを確認します。
* コストを最小限に抑えます。
どのゲートウェイ SKU を指定する必要がありますか?

A. VpnGw4AZ
B. VpnGw2AZ
C. VpnGwIAZ
D. VpnGwSAZ
正解: **(**正解を表示します**)**

質問: **29**
LB1 という名前の内部基本 Azure ロード バランサーがあり、2 つのフロントエンド IP アドレスがあります。LB1 のバックエンド プールには、VM1 および VM2 という名前の 2 つの Azure 仮想マシンが含まれています。
次の表に示すように、LB1 でルールを構成する必要があります。

Rule	Frontend IP address	Protocol	ILB1 port	Destination	VM port
1	65.52.0.1	TCP	80	IP address of the NIC of VM1 and VM2	80
2	65.52.0.2	TCP	80	IP address of the NIC of VM1 and VM2	80

それぞれのルールに対して何をすべきでしょうか?
A. フローティング IP を無効にします。
B. セッションの永続性を無効に設定します。
C. セッションの永続性を有効に設定します。
D. フローティング IP を有効にします。
正解: (正解を表示します)

質問: **30**
VNet1、VNet2、VNet3、VNet4 という名前の 4 つの仮想ネットワークを含む Azure サブスクリプションがあります。
仮想ネットワーク ピアリングを使用して、ハブ アンド スポーク トポロジを展開する予定です。
VNet1をハブネットワークとして構成する必要があります。ソリューションは以下の要件を満たす必要があります。
* スポーク間の推移的ルーティングをサポートします。
* ネットワーク スループットを最大化します。
ソリューションには何を含めるべきですか?
A. Azure VPN ゲートウェイ
B. Azure ファイアウォール
C. Azure ルート サーバー
D. Azure プライベート リンク
正解: (正解を表示します)

質問: **31**
Vnetl という名前の仮想ネットワークを含む Azure サブスクリプションがあります。Vnetl には /24 の IPv4 アドレス空間があります。
Vnet1 を細分化する必要があります。このソリューションでは、使用可能なサブネットの数を最大化する必要があります。
作成できる IPv4 サブネットの最大数はいくつですか。また、サブネットごとに使用できる IP アドレスの数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

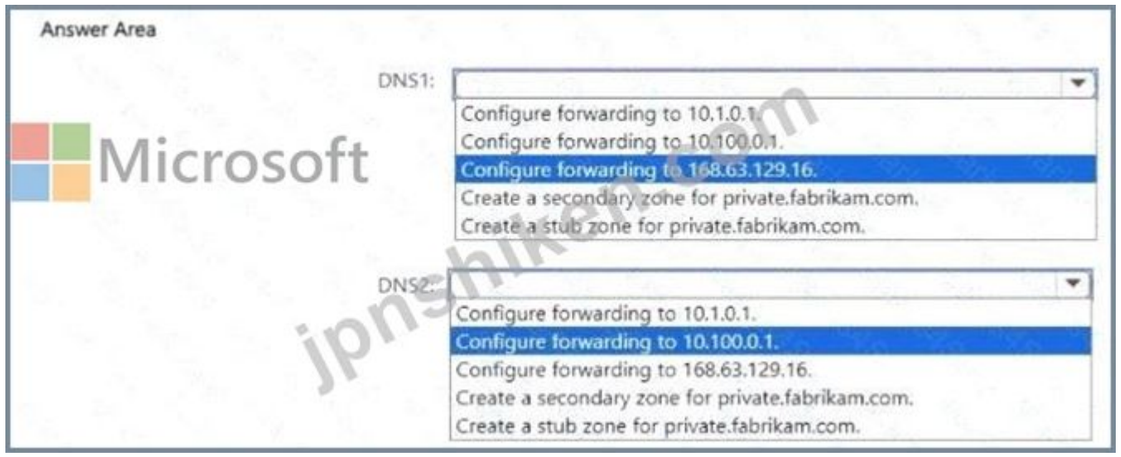
正解:

Explanation:

質問: **32**
Admin1 という名前のユーザーと RG1 という名前のリソース グループを含む Azure サブスクリプションがあります。
RG1 には、NW1 という名前の Azure Network Watcher インスタンスが含まれています。
Admin1 が NW1 をロックできることを確認する必要があります。このソリューションでは、最小特権の原則を使用する必要があります。
Admin1 にどの役割を割り当てる必要がありますか?
A. ユーザー アクセス管理者
B. ネットワーク貢献者
C. 監視貢献者
D. リソース ポリシーの貢献者
正解: **(**正解を表示します**)**

質問: **33**
オンプレミスネットワークには、Windows Server 2022 を実行する DNS1 というサーバーが含まれています。DNS1 は DNS サーバーの役割を持ち、IP アドレスは 10.1.0.1 です。ネットワークには、名前解決に DNS1 を使用するコンピューターが含まれています。

次の表に示すリソースを含む Azure サブスクリプションがあります。



正解:

Explanation:

質問: **34**

次の表に示すように、米国東部 Azure リージョンに 3 つの仮想ネットワークを含む Azure 展開を計画しています。

Name	Description
Vnet1	Hub virtual network for shared services
Vnet2	Virtual machines for the IT department
Vnet3	Virtual machines for the research department

サイト間 VPN は、Vnet1 を会社のオンプレミス ネットワークに接続します。

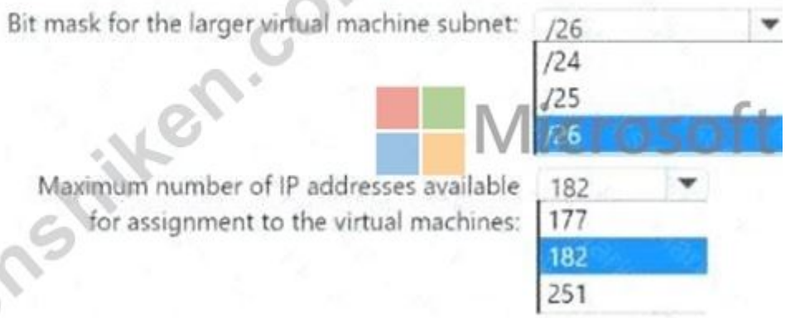
すべての仮想ネットワーク上の仮想マシンがオンプレミス ネットワークと通信できるようにするソリューションを推奨する必要があります。ソリューションではコストを最小限に抑える必要があります。

Vnet2 と Vnet3 には何をお勧めしますか?

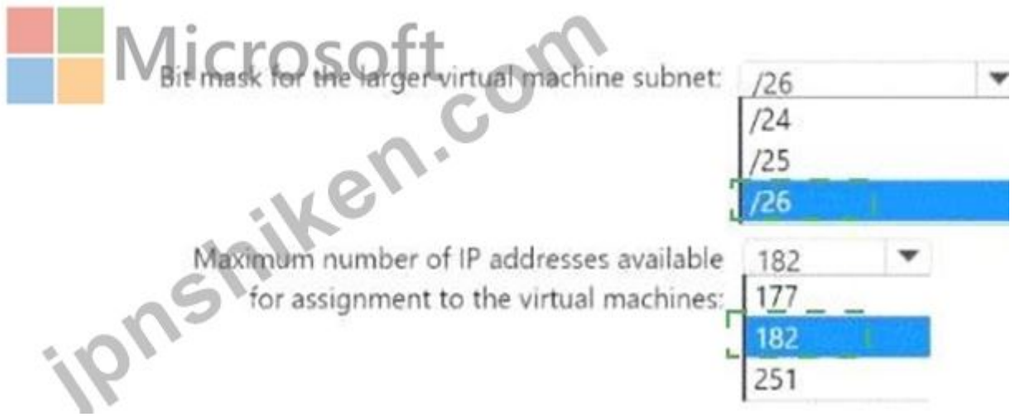
A. ルートテーブル

B. VNet 間の VPN 接続
C. ピアリング
D. サービスエンドポイント
正解: (正解を表示します)

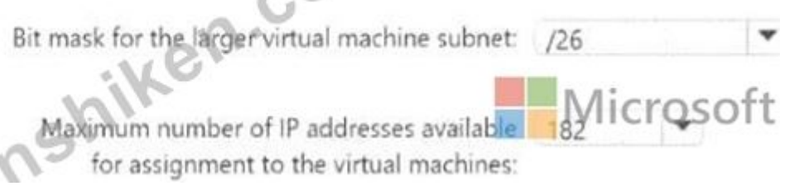
質問: **35**
VNet1 という仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 は IP アドレス空間 192.168.0.0/24 を使用します。VNet1 に Azure 仮想マシンと Azure Bastion をデプロイする予定です。
VNet1 の IP サブネット構成を推奨する必要があります。このソリューションでは、仮想マシンに割り当て可能な IP アドレスの数を最大化する必要があります。どのような構成を推奨すべきでしょうか？回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area



正解:
Answer Area



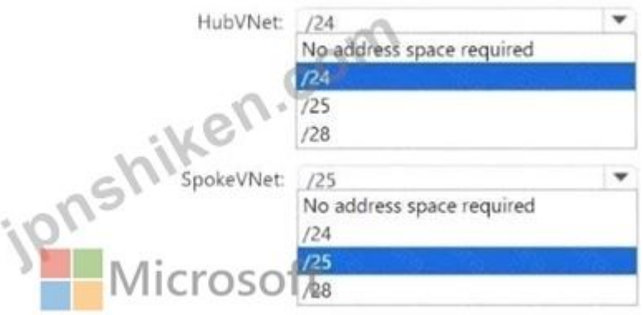
Explanation:
Answer Area



質問: **36**

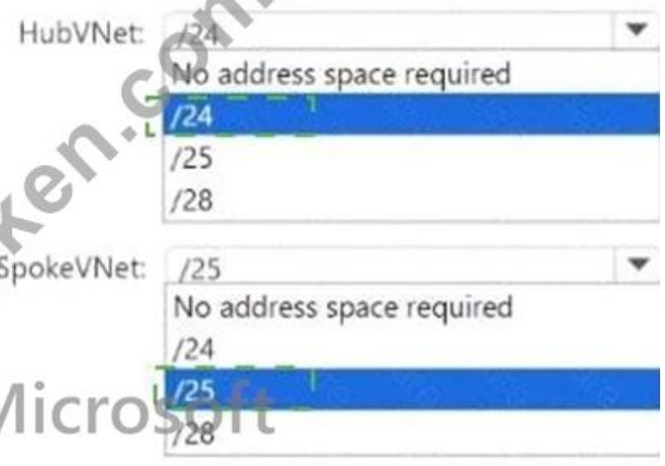
PRDNS1をHubVNetとSpokeVNetに計画的に展開するために、どのIPアドレス空間を割り当てるかを特定する必要があります。ソリューションは、各仮想ネットワークについて何を特定する必要がありますか？という一般的な要件を満たす必要があります。回答するには、回答エリアから適切な選択肢を選択してください。注：正しい選択肢は1つにつき1ポイント付与されます。

Answer Area



正解:

Answer Area



Explanation:

Answer Area

質問: **37**

オンプレミス ネットワークには、Server 1 という名前の DNS サーバーが含まれています。

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
VNet1	Virtual network	*None*
VM1	Virtual machine	Connected to VNet1 Connected to storage1 by using a private endpoint
storage1	Storage account	*None*

オンプレミス ネットワークは、サイト間 (S2S) VPN を使用して VNet1 に接続されます。
Server1がstorage1のDNS名を解決できることを確認する必要があります。ソリューションはコストと管理作業を最小限に抑える必要があります。
何を使うべきでしょうか?
A. Azure パブリック DNS ゾーン
B. DNS サービスをホストする Azure 仮想マシン
C. Azure プライベート DNS ゾーン
D. Azure DNS プライベート リゾルバー
正解: **D (**コメントを発表する**)**

質問: **38**
ストレージ2へのアクセスを提供する必要があります。ソリューションは、PaaSネットワーク要件とビジネス要件を満たす必要があります。
どの接続方法を使用すればよいですか?
A. サービスエンドポイント
B. プライベートエンドポイント
C. Azure ファイアウォール
D. 青い玄関
正解: **(**正解を表示します**)**
Topic 2, Contoso Case Study 2
Overview
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab. note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Existing Environment:
Azure Network Infrastructure
Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.
The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Connected to	Network security group (NSG)
VM1	Vnet1/Subnet1	NSG1
VM2	Vnet1/Subnet2	NSG2
VM3	Vnet2/Default	NSG3
VM4	Vnet3/Default	NSG4
VM5	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements:

Virtual Network Requirements

Contoso has the following virtual networks requirements:

* Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

Two container groups that connect to Vnet6
Three virtual machines that connect to Vnet6
Allow VPN connections to be established to Vnet6
Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network
* The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
* A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.
Network Security Requirements
Contoso has the following network security requirements:
* Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.
* Enable NSG flow logs for NSG3 and NSG4.
* Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

* Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

質問: 39
VM1 という仮想マシンと Vnet1 という仮想ネットワークを含む Azure サブスクリプションがあります。Vnet1 には、Subnet1、Subnet2、GatewaySubnet という 3 つのサブネットが含まれていま す。VM1 は Subnet 1 に接続されています。
ネットワーク トラフィックのルーティングと検査を実行する VM2 という名前の新しい仮想マシンを展開する予定です。
VM1 からインターネットへのすべてのトラフィックが VM2 を経由してルーティングされるようにする必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:
Answer Area

Explanation:

Answer Area

質問: 40

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
App1	Azure App Service app	Accessed by using a URL of https://app1.contoso.com/
FD1	Azure Front Door Premium profile	Configured as an endpoint for App1
contoso.com	Azure DNS zone	Contains a DNS CNAME record for App1 that resolves to an FQDN of app1.azurewebsites.net

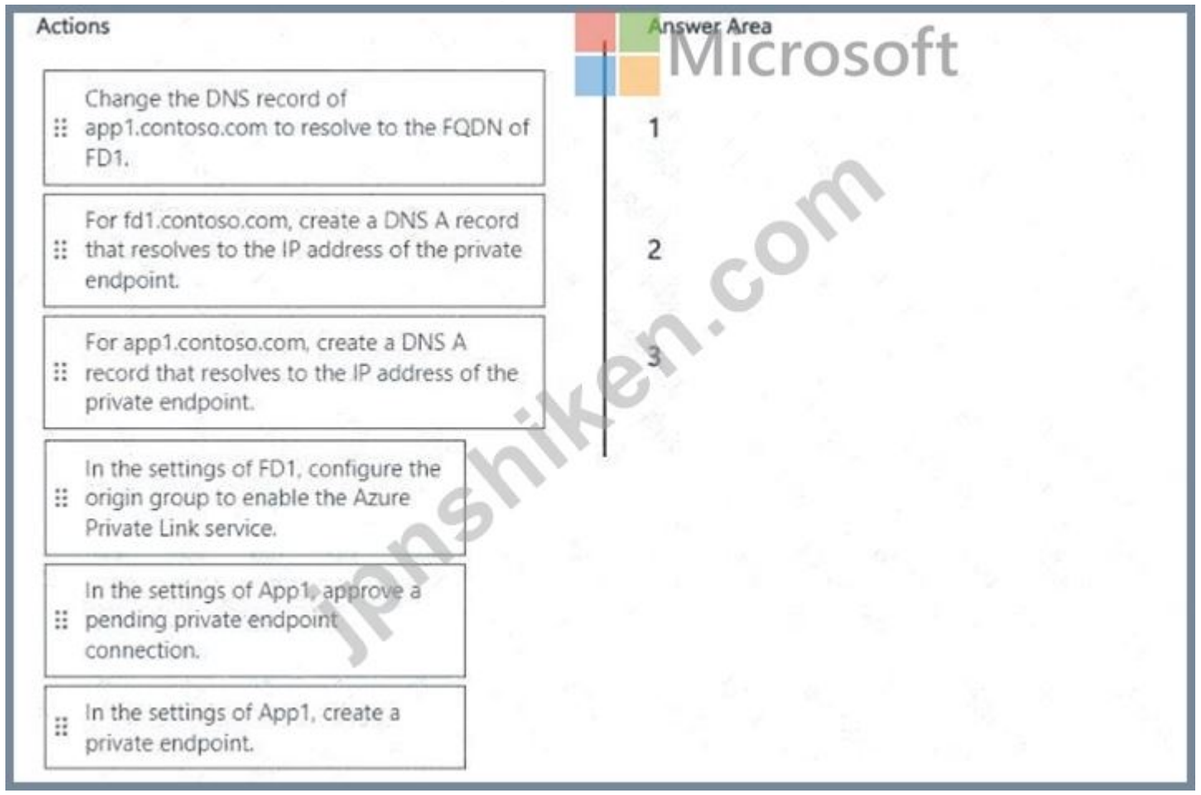
ユーザーが App1 に直接接続していることがわかります。

以下の要件を満たす必要があります:

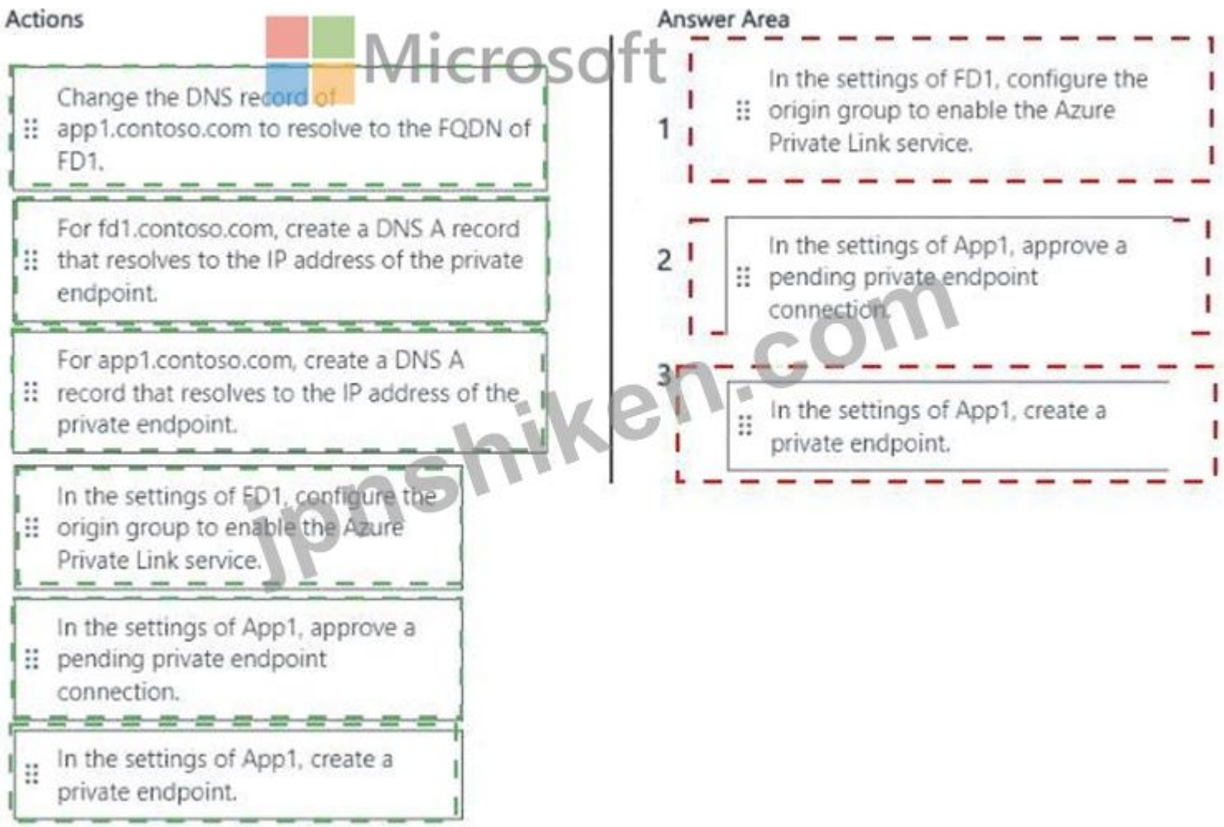
* 管理者はプライベート エンドポイントを使用してのみ App1 にアクセスする必要があります。
* App1 へのすべてのユーザー接続は FD1 を経由してルーティングされる必要があります。
* App1 への接続のダウンタイムを最小限に抑える必要があります。

順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

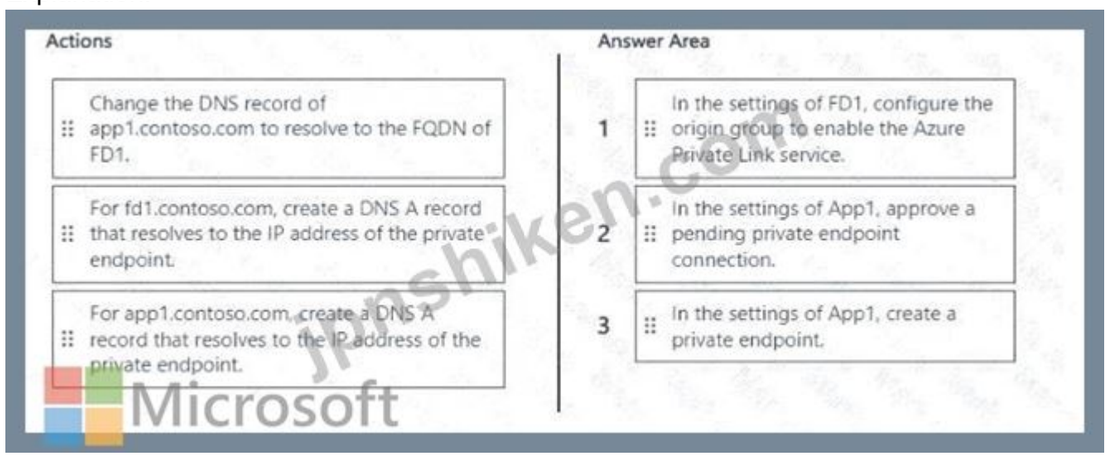
注意：正解の選択肢の順序は複数あります。正解の選択肢のいずれかを選択しても、得点は付与されます。



正解:



Explanation:



質問: **41**

NSG1 という名前のネットワーク セキュリティ グループがあります。

NSG1 のネットワーク セキュリティ グループ (NSG) フロー ログを有効にする必要があります。ソリューションは保持ポリシーをサポートしている必要があります。

最初に何を作成すればよいですか?

A. 標準の汎用 v2 Azure ストレージ アカウント

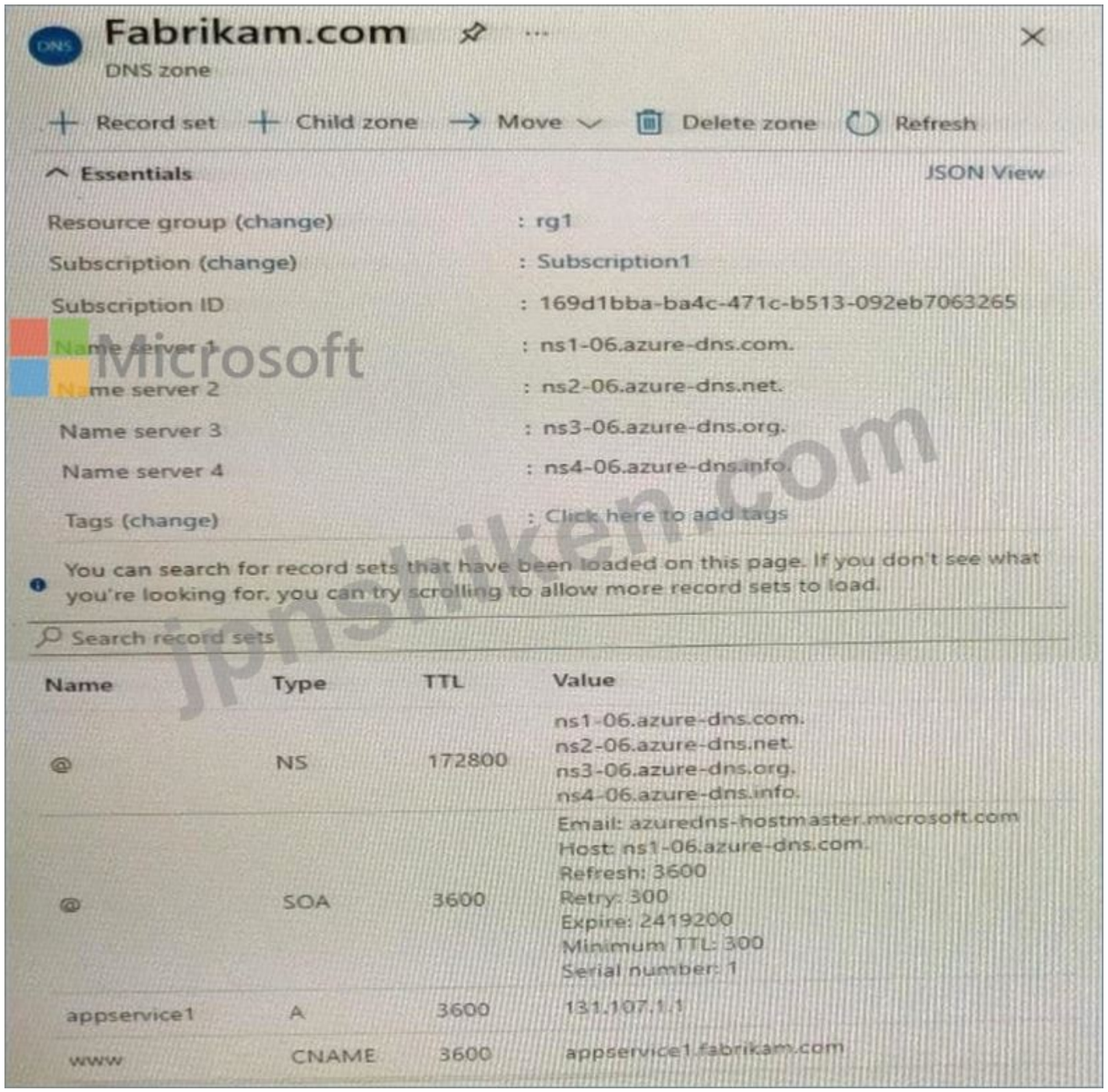
B. Azure Log Analytics ワークスペース

C. プレミアム ブロック BLOB Azure ストレージ アカウント

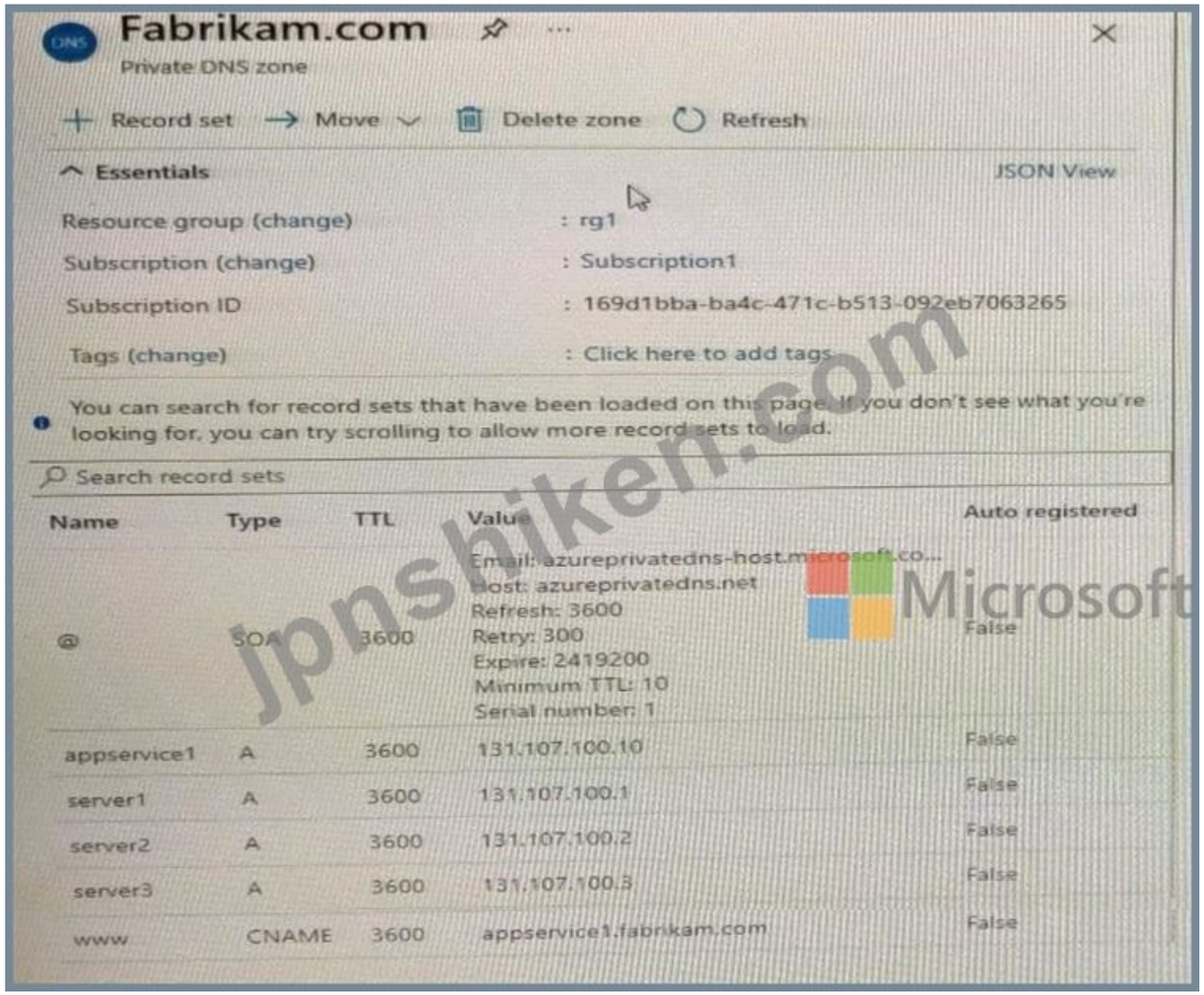
D. 標準の汎用 v1 Azure ストレージ アカウント
正解: **(**正解を表示します**)**

質問: **42**
Site1 という名前のオンプレミス ネットワークがあります。
VNet1 という名前の仮想ネットワークと storage1 という名前のストレージ アカウントを含む Azure サブスクリプションがあります。
Site1 と VNet1 は、サイト間 (S2S) VPN を使用して接続されています。
S2S VPN を使用して、サイト内のサーバーがストレージに接続できることを確認する必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。
VNet1 に何を作成する必要がありますか?
A. サービスエンドポイント
B. プライベートエンドポイント
C. Azure Private Link サービス
D. Azure アプリケーション ゲートウェイ
正解: **B (**コメントを発表する**)**

質問: **43**
Vnet1 と Vnet2 という名前の 2 つの仮想ネットワークを含む Azure サブスクリプションがあります。
fabrikam.com というパブリック DNS ゾーンを登録します。このゾーンは、パブリック DNS ゾーンの図に示すように構成されています。



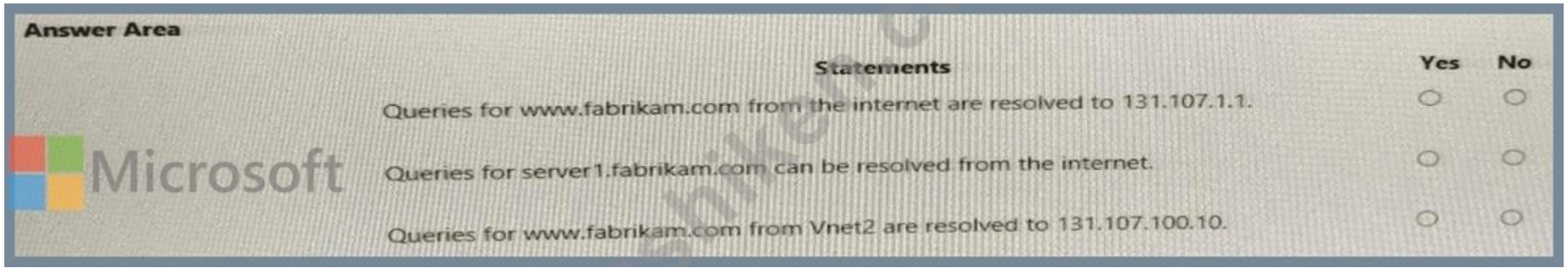
fabrikam.com というプライベート DNS ゾーンがあります。このゾーンは、プライベート DNS ゾーンの図に示されているように構成されています。



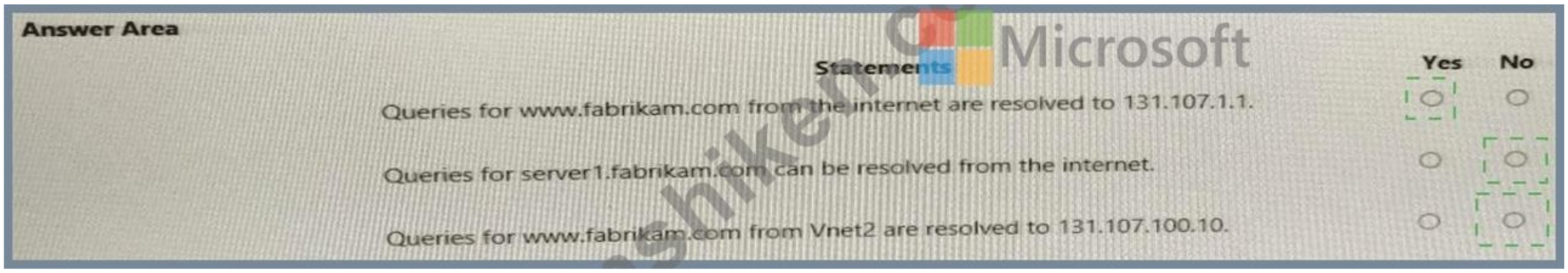
仮想ネットワーク リンクは、仮想ネットワーク リンクの図に示すように構成されています。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

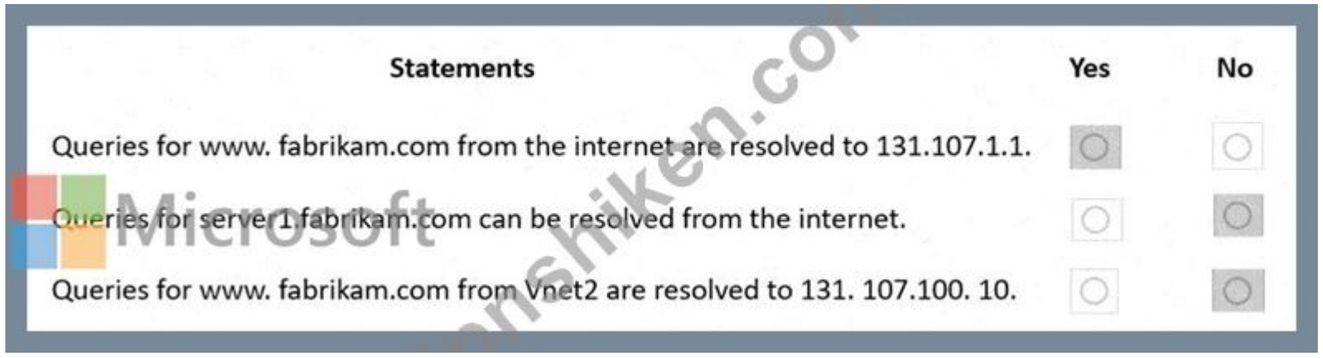
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:



Box 1: Yes

DNS queries from the internet use the public DNS zone. In the public DNS zone, www.fabrikam.com is a CNAME record that resolves to appservice1.fabrikam.com which resolves to 131.107.1.1.

Box 2: No

DNS queries from the internet use the public DNS zone. There is no DNS record for server1.fabrikam.com in the public DNS zone.

Box 3: No

The private DNS zone is linked to VNet1, not VNet2. Therefore, resources in VNet2 cannot query the private DNS zone.

質問: **44**

次の表に示すリソース グループを含む Azure サブスクリプションがあります。

Name	Location
RG1	East US
RG2	UK West

次の表に示す仮想ネットワークがあります。
Vne1l には、VM1 と VM2 という 2 つの仮想マシンが含まれています。Vnet2 には、VM3 と VM4 という 2 つの仮想マシンが含まれています。次の表に示すように、デフォルトのルールのみを含むネットワーク セキュリティ グループ (NSG) があります。

Name	Associated to
Nsg1	Sb1
Nsg2	Network interface of VM2
Nsg3	Network interface of VM3
Nsg4	Sb4

次の表に示す Azure ロード バランサーがあります。

Name	Resource group	Location	Type	Backend pool	Virtual machine	Rule
Lb1	RG1	East US	Public	Vnet1	VM1	Protocol: TCP Port: 80 Backend port: 80
Lb2	RG2	West US	Internal	Vnet2	VM3	Protocol: TCP Port: 1433 Backend port: 1433

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM2 can be added to the backend pool of Lb2.		
VM4 can access VM3 via port 1433 by using the frontend address of Lb2.		
VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.		

正解:

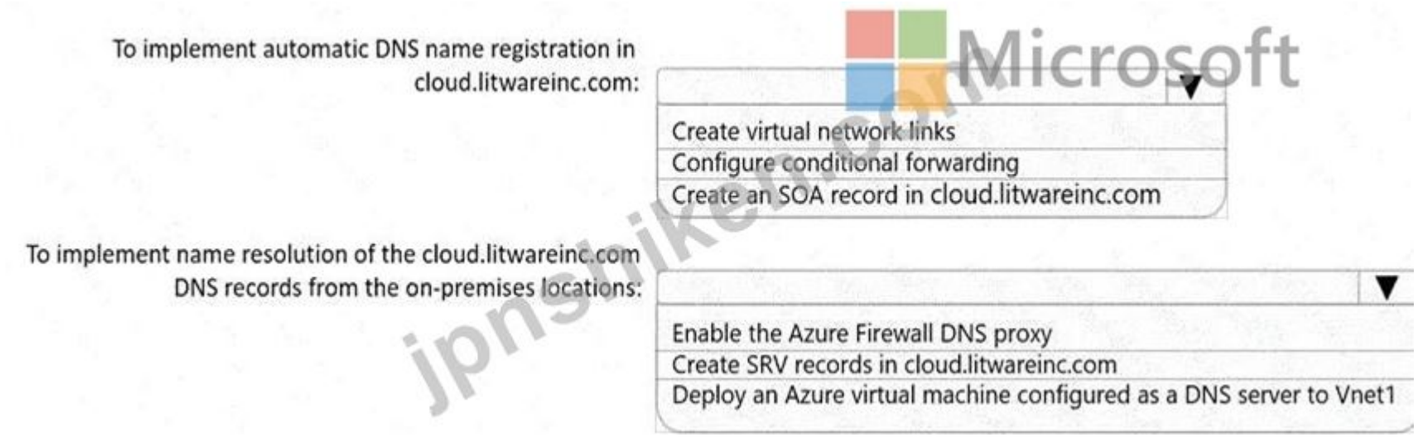
Explanation:

質問: 45

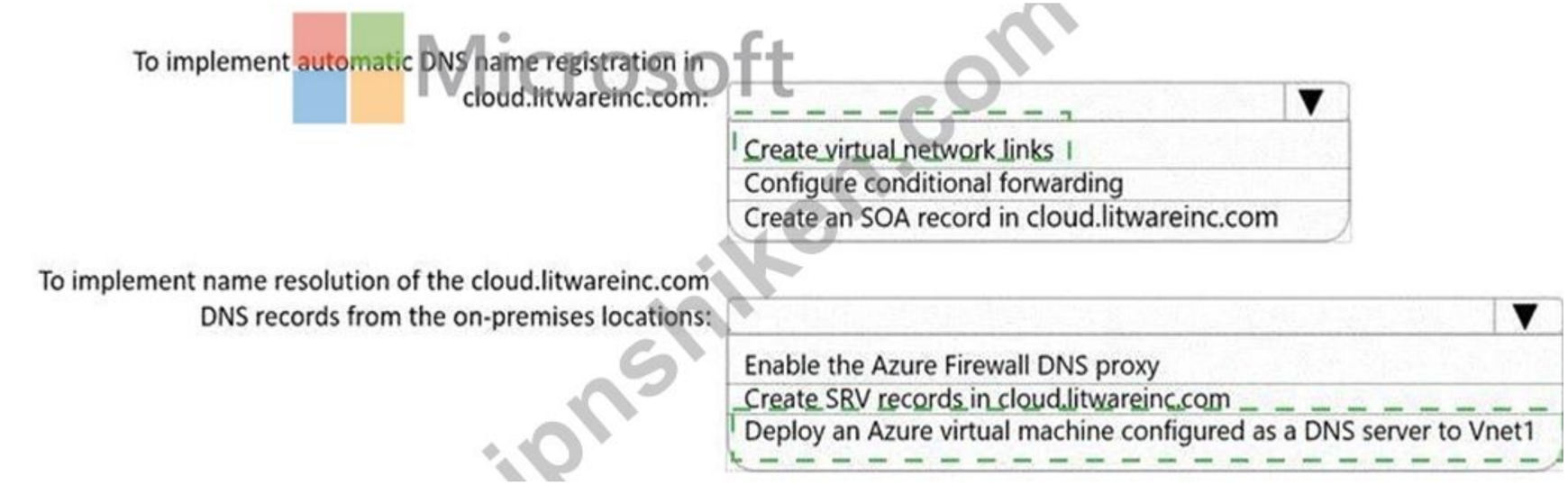
cloud.liwareinc.com の名前解決を実装する必要があります。ソリューションはネットワーク要件を満たしている必要があります。

どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。

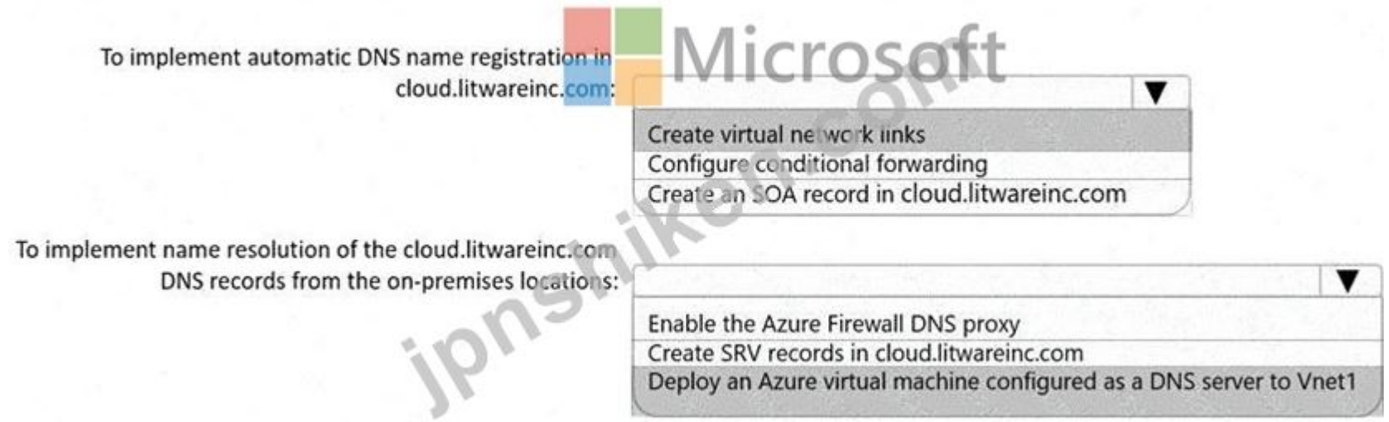
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

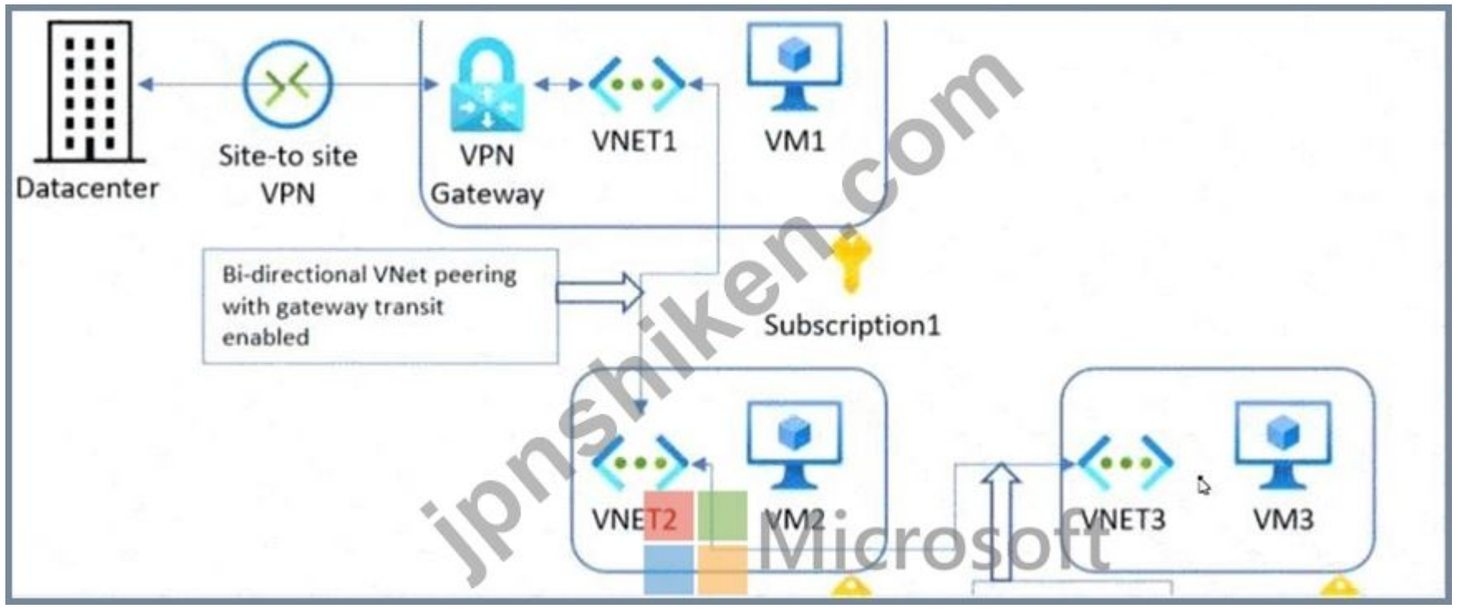


Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role- instances

質問: **46**
次の図に示す Azure 環境があります。



ドロップダウンメニューを使用して、図に示されている情報に基づいて各文を完成させる選択肢を選択してください。注: 正解は1つにつき1ポイントです。

Answer Area

VM1 can communicate with **[answer choice]**

- the on-premises datacenter and VM2 only
  - VM2 only
  - VM2 and VM3 only
  - the on-premises datacenter and VM2 only
- the on-premises datacenter, VM1, and VM3
  - VM1 only
  - VM1 and VM3 only
  - the on-premises datacenter and VM3 only
  - the on-premises datacenter, VM1, and VM3

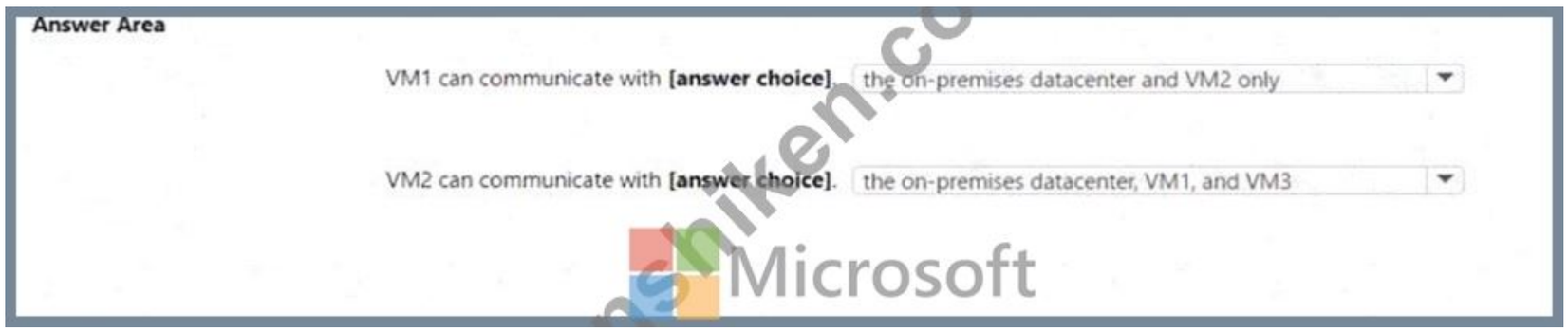
正解:

Answer Area

VM1 can communicate with **[answer choice]**

- the on-premises datacenter and VM2 only
  - VM2 only
  - VM2 and VM3 only
  - the on-premises datacenter and VM2 only
- the on-premises datacenter, VM1, and VM3
  - VM1 only
  - VM1 and VM3 only
  - the on-premises datacenter and VM3 only
  - the on-premises datacenter, VM1, and VM3

Explanation:



質問: **47**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
NSG1	Network security group (NSG)	Linked to Subnet1
ASG1	Application security group	Not linked

サブシェルには、App1 というアプリをホストする 3 つの仮想マシンが含まれています。App1 には SFTP プロトコルを使用してアクセスします。
NSG1 から、ASG1 への受信 SFTP 接続を許可する Rule2 という名前の受信セキュリティ ルールを構成します。
受信SFTP接続がASG1を使用して管理されていることを確認する必要があります。ソリューションは管理作業を最小限に抑える必要があります。
何をすべきでしょうか?
A. ASG1 から、ロールの割り当てを変更します。
B. 各仮想マシンから、ネットワークインターフェースをASG1に関連付けます。
C. Subnet1 からサブネット委任を作成します。
D. NSG1 から、Rule2 の優先順位を変更します。
正解: **B** (コメントを発表する)

質問: **48**
次の表に示すルート テーブルとルートを含む Azure サブスクリプションがあります。

Route table name	Route name	Prefix	Destination
RT1	Default Route	0.0.0.0/0	VirtualNetworkGateway
RT2	Default Route	0.0.0.0/0	Internet

サブスクリプションには、次の表に示すサブネットが含まれています。

Name	Prefix	Route table	Virtual network
Subnet1	10.10.1.0/24	RT1	Vnet1
Subnet2	10.10.2.0/24	RT2	Vnet1
GatewaySubnet	10.10.3.0/24	None	Vnet1

サブスクリプションには、次の表に示す仮想マシンが含まれています。

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

各ローカル ネットワーク ゲートウェイへのサイト間 VPN 接続があります。

以下の各文について、該当する場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

正解:

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

Explanation:

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

質問: **49**
タスク6
サブネット3-2にデプロイされたすべてのホストが、同じ静的パブリックIPアドレスを使用してインターネットに接続できるようにする必要があります。このソリューションでは、サブネットにホストを追加する際の管理作業を最小限に抑える必要があります。
正解:
See the Explanation below for step by step instructions.
Explanation:
Here are the steps and explanations for ensuring that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address:
* To use the same static public IP address for multiple hosts, you need to create a NAT gateway and associate it with subnet3-2. A NAT gateway is a resource that performs network address translation (NAT) for outbound traffic from a subnet1. It allows you to use a single public IP address for multiple private IP addresses2.
* To create a NAT gateway, you need to go to the Azure portal and select Create a resource. Search for NAT gateway, select NAT gateway, then select Create3.
* On the Create a NAT gateway page, enter or select the following information and accept the defaults for the remaining settings:
* Subscription: Select your subscription name
* Resource group: Select your resource group
* Name: Type a unique name for your NAT gateway
* Region: Select the same region as your virtual network
* Public IP address: Select Create new and type a name for your public IP address. Select Standard as the SKU and Static as the assignment method4.
* Select Review + create and then select Create to create your NAT gateway3.
* To associate the NAT gateway with subnet3-2, you need to go to the Virtual networks service in the Azure portal and select your virtual network.
* On the Virtual network page, select Subnets under Settings, and then select subnet3-2 from the list.
* On the Edit subnet page, under NAT gateway, select your NAT gateway from the drop-down list. Then select Save.

質問: **50**
次の表に示す仮想ネットワークを含む Azure サブスクリプションがあります。

Name	Subnet	Peered with
VNet1	Subnet11, Subnet12	VNet2
VNet2	Subnet21	VNet1

サブスクリプションには、次の表に示す仮想マシンが含まれています。

Name	Connected to	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet12	*None*
VM4	Subnet21	*None*

次の構成を持つ LB1 という名前のロード バランサーを作成します。

* SKU: ベーシック
* タイプ: 内部
* サブネット: Subnetl2
* 仮想ネットワーク VNet1

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。注：正しい選択肢は1つにつき1点です。

Answer Area

Statements	Yes	No
LB1 can balance requests between VM1 and VM2.	○	○
LB1 can balance requests between VM2 and VM3.	○	○
LB1 can balance requests between VM3 and VM4.	○	○

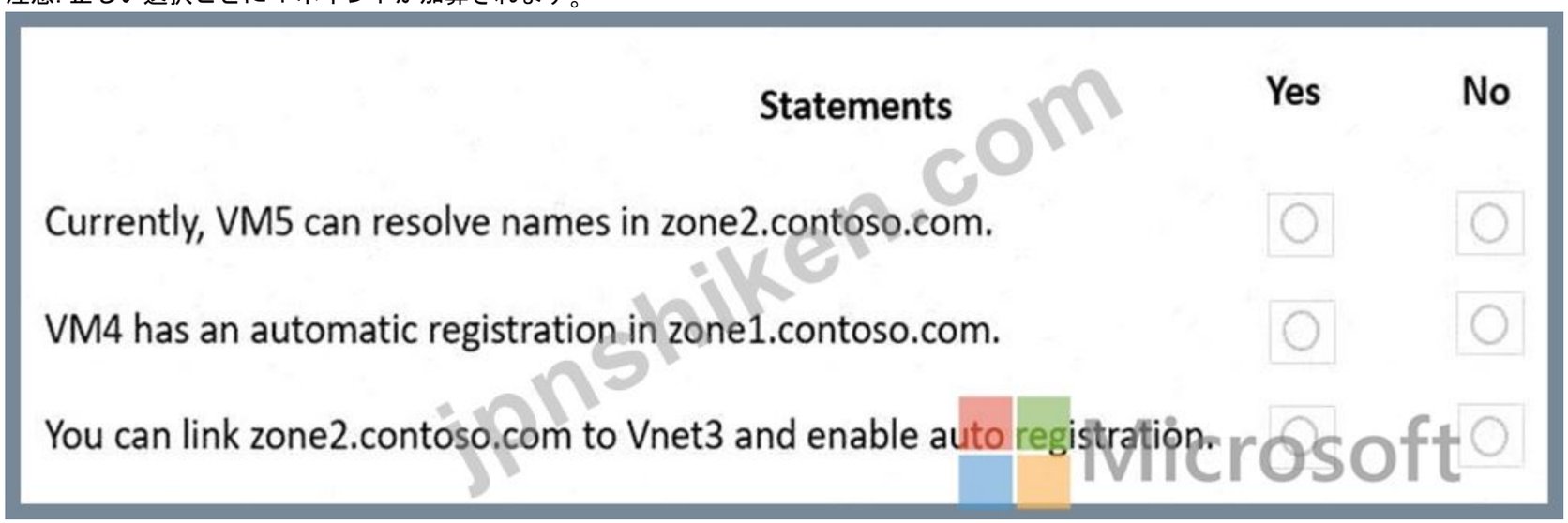
正解:

Answer Area

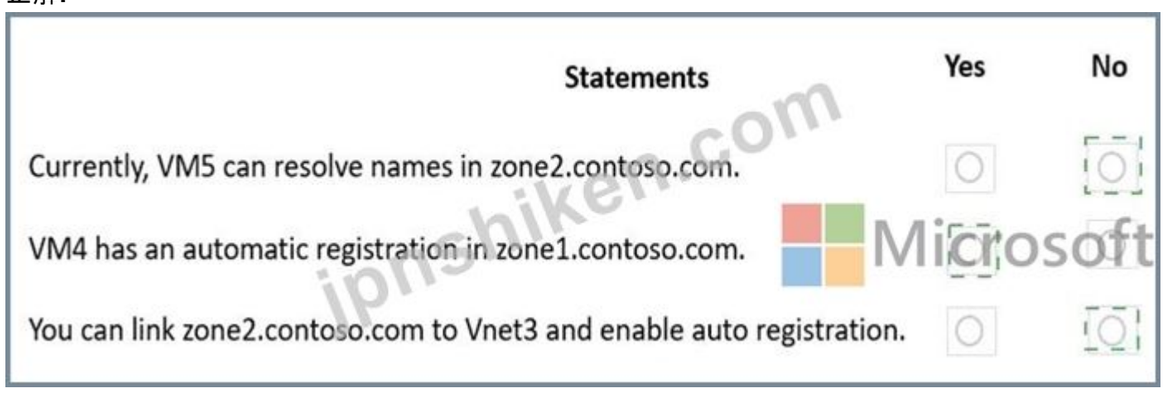
Statements	Yes	No
LB1 can balance requests between VM1 and VM2.	○	○
LB1 can balance requests between VM2 and VM3.	○	○
LB1 can balance requests between VM3 and VM4.	○	○

Explanation:

質問: **51**
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

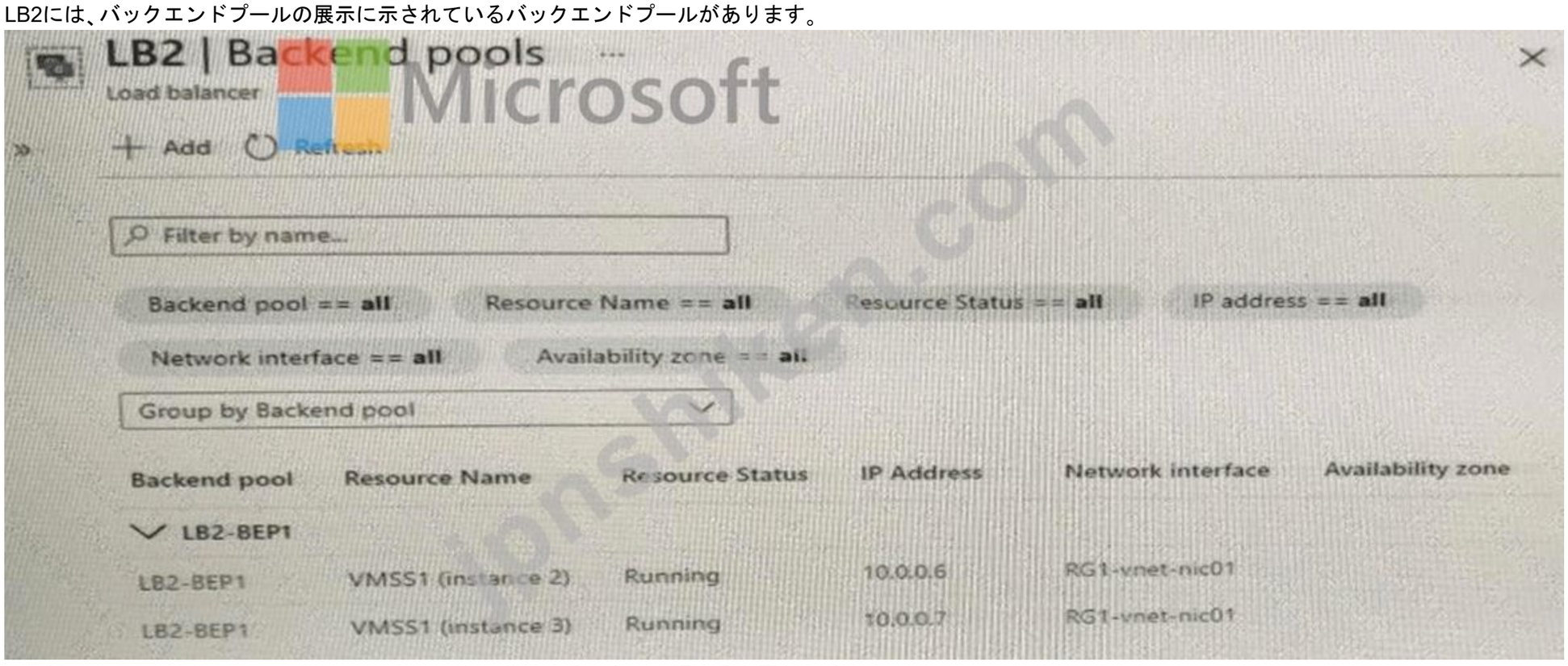
Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	○	○
VM4 has an automatic registration in zone1.contoso.com.	○	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○	○

Box 1: No
Zone2.contoso.com is not linked to any virtual networks. Therefore, no VMs are able to resolve names in the zone.
Box 2: Yes
VM4 is in VNet3. Zone1.contoso.com has a link to VNet3 and auto-registration is enabled on the link.
Box3: No
VNet3 is linked to zone1.contoso.com and auto-registration is enabled on the link. A virtual network can only have one registration zone. You can link zone2.contoso.com to VNet3 but you won't be able to enable auto- registration on the link.

質問: **52**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできなくなり、これらの質問はレビュー画面に表示されなくなります。
AFD1 という名前の Azure Front Door Premium プロファイルと WAF1 という名前の Azure Web アプリケーション ファイアウォール (WAF) ポリシーを含む Azure サブスクリプションがあります。AFD1 は WAF1 に関連付けられています。
AFD1 への受信リクエストのレート制限を構成する必要があります。
解決策: WAF1 の管理ルールを構成します。
これは目標を達成していますか?
A. いいえ
B. はい
正解: **(**正解を表示します**)**

質問: **53**
ロードバランサーの展示にAzureロードバランサーが表示されています。

LB2には、バックエンドプールの展示に示されているバックエンドプールがあります。



LB2がVMSS1のすべてのメンバーにトラフィックを分散することを確認する必要があります。

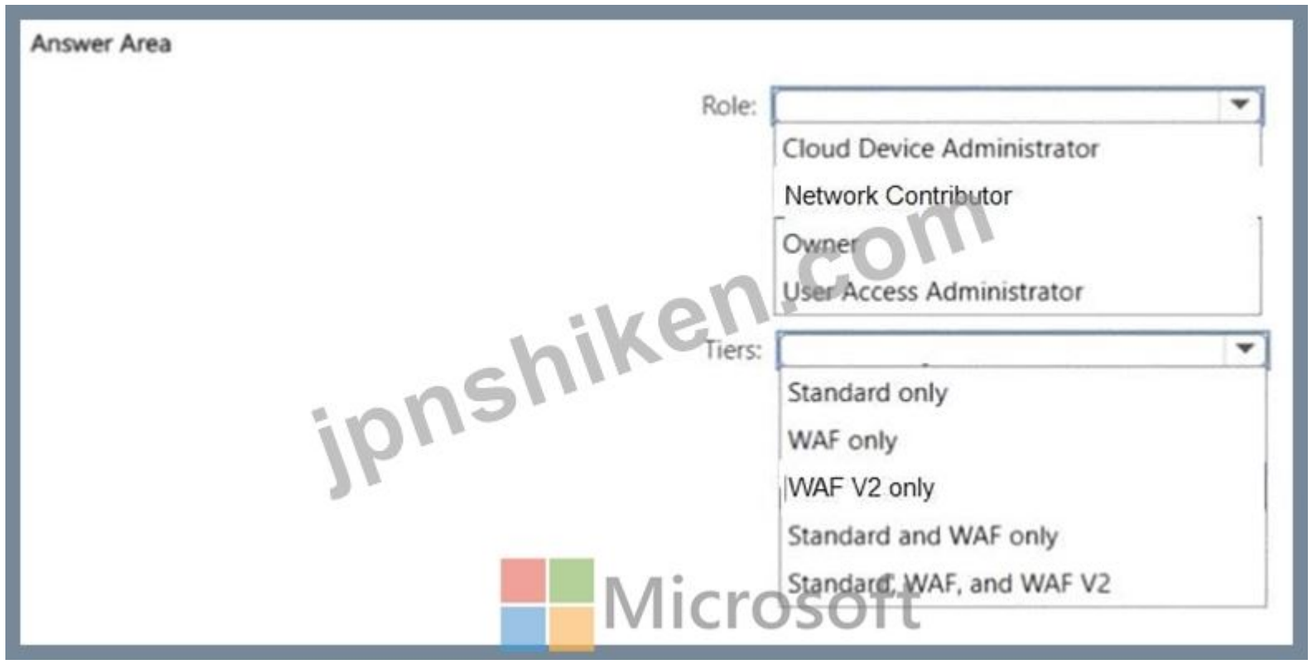
実行する必要がある2つのアクションはどれですか？それぞれの正解は、解決策の一部を示しています。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. VMSS1にネットワークインターフェイスを追加します。
B. ヘルスプローブを構成します。
C. VMSS1の各メンバーにパブリックIPアドレスを追加します。
D. 負荷分散ルールを追加します。
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal?tabs=option-1-create-load-balancer-standard

質問: **54**
Frontend1という名前の単一のフロントエンドとPolicy1という名前のAzureWebアプリケーションファイアウォール（WAF）ポリシーを持つAzure FrontDoorインスタンスがあります。Policy1は、「string1」を含むヘッダーを持つリクエストをhttps://www.contoso.com/redirect1にリダイレクトします。Policy1はFrontend1に関連付けられています。
追加のリダイレクト設定を構成する必要があります。「string2」を含むヘッダーを持つFrontend1へのリクエストは、https://www.contoso.com/redirect2にリダイレクトする必要があります。
実行する必要がある3つのアクションはどれですか？それぞれの正解は、解決策の一部を示しています。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. カスタムルールを作成します。
B. 関連付けを作成します。
C. ポリシーを作成します。
D. フロントエンドホストを作成します。
E. ポリシー1にカスタムルールを追加します。
F. 管理ルールを設定します。
正解: **(**正解を表示します**)**

質問: **55**
AFD1 という名前の Azure Front Door Premium プロファイルと、WAF1 という名前の Azure Web アプリケーション ファイアウォール (WAF) ポリシーを含む Azure サブスクリプションがあります。AFD1 は WAF1 に関連付けられています。
AFD1 への受信リクエストのレート制限を設定する必要があります。
解決策: AFD1 のルール セットにルールを追加します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解: **A (**コメントを発表する**)**

質問: **56**
Azure サブスクリプションをお持ちです。このサブスクリプションには、以下の構成の Azure アプリケーション ゲートウェイが含まれています。
* 名前: AppGW1
* ティアスタンダード V2
* 自動スケーリング: 無効

User1 という名前のユーザーを作成します。
User1 が AppGW1 の階層を変更できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
User1 にはどのロールを割り当てる必要がありますか。また、AppGW1 はどの層に変更できますか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



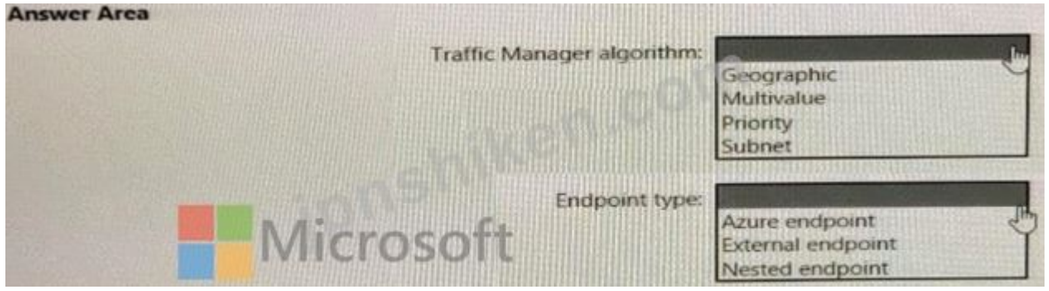
正解:

Explanation:

質問: 57
タスク4
仮想ネットワーク上で管理操作が実行された場合、VNET3 の所有者がアラートを受信するようにする必要があります。
正解:
See the Explanation below for step by step instructions.
Explanation:
To ensure that the owner of VNET3 receives an alert whenever an administrative operation is performed on the virtual network, you can set up an Activity Log Alert in Azure Monitor. Here's how you can do it:
Step-by-Step Solution
Step 1: Create an Activity Log Alert
* Navigate to the Azure Portal.
* Search for "Monitor" and select it.
* In the Monitor blade, select "Alerts" from the left-hand menu.
* Click on "New alert rule".
Step 2: Configure the Alert Rule
* Select the Scope:
* Click on "Select resource".
* Choose "Virtual Network" as the resource type.
* Select VNET3 from the list of virtual networks.
* Define the Condition:
* Click on "Add condition".
* In the "Signal type" dropdown, select "Activity Log".
* Choose "Administrative" as the category.
* Select the specific operations you want to monitor (e.g., Microsoft.Network/virtualNetworks /write for any write operations on the virtual network).
* Set the Alert Details:
* Enter a name for the alert rule (e.g., VNET3 Admin Operations Alert).
* Provide a description if needed.
* Configure the Action Group:
* Click on "Add action group".
* Enter a name for the action group.
* Select the action type (e.g., Email/SMS/Push/Voice).
* Enter the details of the recipient (e.g., the email address of the owner of VNET3).
* Review and Create:
* Review the alert rule settings.

* Click on "Create alert rule".
Explanation:
* Activity Log Alerts: These alerts notify you when specific operations are performed on your Azure resources. By setting up an alert for administrative operations, you ensure that any changes to VNET3 are promptly reported.
* Action Groups: These define the actions to take when an alert is triggered. You can configure notifications via email, SMS, or other methods to ensure the owner of VNET3 is informed immediately.
* Administrative Operations: Monitoring these operations helps in tracking changes and maintaining the security and integrity of your virtual network.
By following these steps, you can ensure that the owner of VNET3 receives timely alerts for any administrative operations performed on the virtual network, helping to maintain oversight and security.

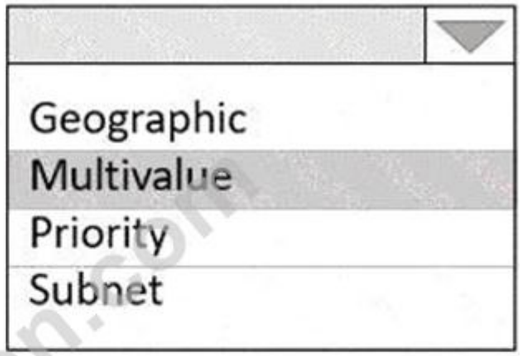
質問**: 58**
会社にはWebサービスのインスタンスが10個あります。各インスタンスは異なるAzureリージョンでホストされており、パブリックエンドポイントを介してアクセスできます。
会社の開発部門では、App1 というアプリケーションを作成しています。10分ごとに、App1 はエンドポイントのリストを使用し、利用可能な最初のエンドポイントに接続します。
Azure Traffic Manager を使用してエンドポイントのリストを管理する予定です。
DNS キャッシュの影響を最小限に抑える Traffic Manager プロファイルを構成する必要があります。
何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



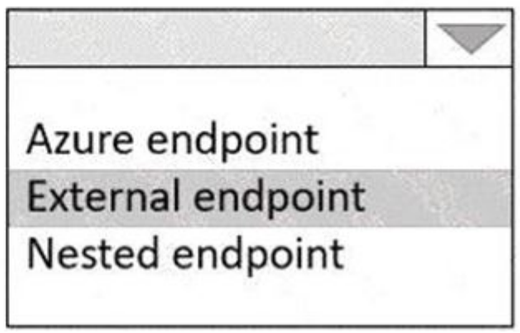
正解**:**

Explanation:

Traffic Manager algorithm:



Endpoint type:



Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types

質問: **59**
次のホストへのアクセスを提供する、AppGW1 という名前の Azure アプリケーション ゲートウェイがあります。
* www.adatum.com
* www.contoso.com
* www.fabrikam.com
AppGW1 には、次の表に示すリスナーがあります。

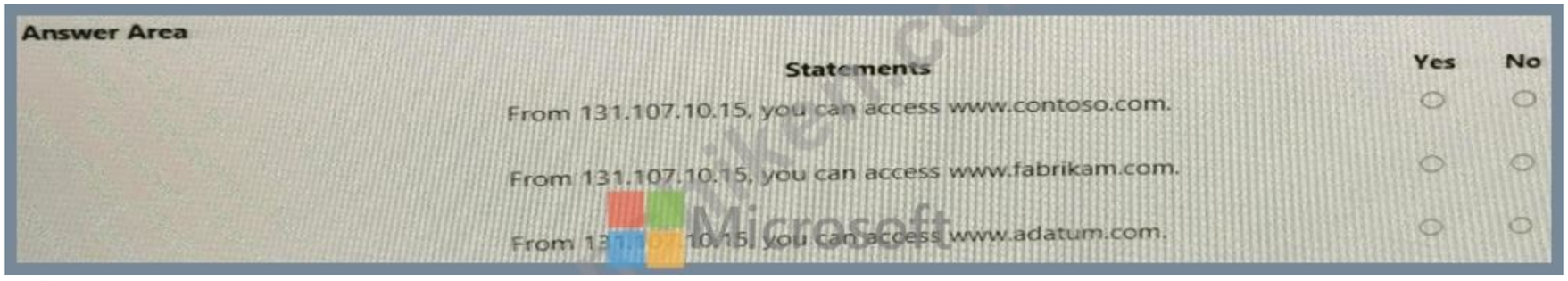
Name	Frontend IP address	Type	Host name
Listen1	Public	Multi site	www.contoso.com
Listen2	Public	Multi site	www.fabrikam.com
Listen3	Public	Multi site	www.adatum.com

次の表に示すように、AppGW1 の Azure Web アプリケーション ファイアウォール (WAF) ポリシーを作成します。

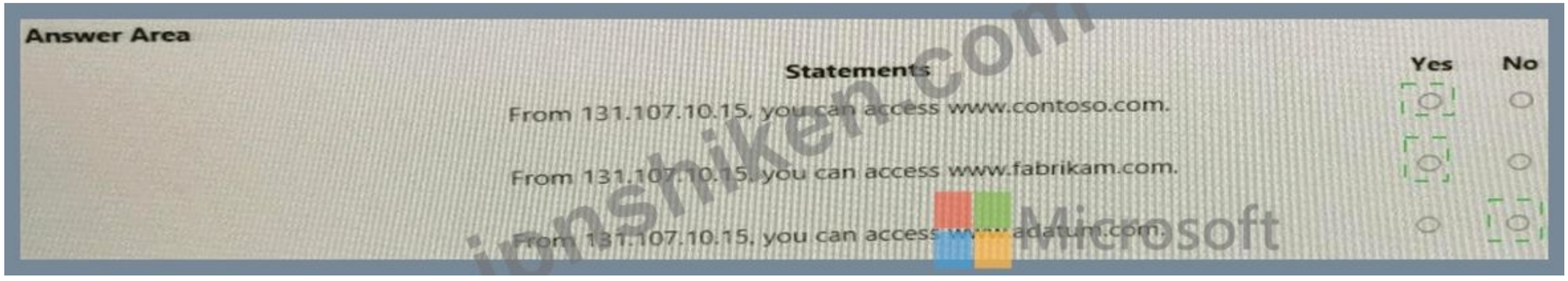
Name	Policy mode	Custom rule		
		Priority	Condition	Association
Policy1	Prevention	50	If IP address does contain 131.107.10.15 then deny traffic.	Application gateway: AppGW1
Policy2	Detection	10	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen1
Policy3	Prevention	70	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen2

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/per-site-policies

質問: **60**
タスク1
サブネットl-2にファイアウォールを導入する予定です。ファイアウォールのIPアドレスは10.1.2.4です。
サブネットl-1からIPアドレス範囲192.168.10.0/24へのトラフィックが、サブネットl-2に導入されるファイアウォールを経由してルーティングされるようにする必要があります。このソリューションは、動的ルーティングプロトコルを使用せずに実現する必要があります。
正解:
See the Explanation below for step by step instructions.
* To deploy a firewall to subnetl-2, you need to create a network virtual appliance (NVA) in the same virtual network as subnetl-2. An NVA is a virtual machine that performs network functions, such as firewall, routing, or load balancing1.
* To create an NVA, you need to create a virtual machine in the Azure portal and select an image that has the firewall software installed. You can choose from the Azure Marketplace or upload your own image2.
* To assign the IP address of 10.1.2.4 to the NVA, you need to create a static private IP address for the network interface of the virtual machine. You can do this in the IP configurations settings of the network interface3.
* To ensure that traffic from subnetl-1 to the IP address range of 192.168.10.0/24 is routed through the NVA, you need to create a user-defined route (UDR) table and associate it with subnetl-1. A UDR table allows you to override the default routing behavior of Azure and specify custom routes for your subnets4.
* To create a UDR table, you need to go to the Route tables service in the Azure portal and select + Create. You can give a name and a resource group for the route table5.
* To create a custom route, you need to select Routes in the route table and select + Add. You can enter the following information for the route5:
* Destination: 192.168.10.0/24
* Next hop type: Virtual appliance
* Next hop address: 10.1.2.4
* To associate the route table with subnetl-1, you need to select Subnets in the route table and select + Associate. You can select the virtual network and subnet that you want to associate with the route table5.

質問: **61**
タスク7
VNET2 上のホストが VNET1 と VNET3 の両方のホストにアクセスできることを確認する必要があります。ソリューションでは、VNET1 と VNET3 上のホストが VNET2 を介して通信できないようにする必要があります。
正解:
See the Explanation below for step by step instructions.
Explanation:
Here are the steps and explanations for ensuring that hosts on VNET2 can access hosts on both VNET1 and VNET3, but hosts on VNET1 and VNET3 cannot communicate through VNET2:
* To connect different virtual networks in Azure, you need to use virtual network peering. Virtual network peering allows you to create low-latency, high-bandwidth connections between virtual networks without using gateways or the internet1.
* To create a virtual network peering, you need to go to the Azure portal and select your virtual network. Then select Peerings under Settings and select + Add2.
* On the Add peering page, enter or select the following information:
* Name: Type a unique name for the peering from the source virtual network to the destination virtual network.
* Virtual network deployment model: Select Resource manager.
* Subscription: Select the subscription that contains the destination virtual network.
* Virtual network: Select the destination virtual network from the list or enter its resource ID.

* Name of the peering from [destination virtual network] to [source virtual network]: Type a unique name for the peering from the destination virtual network to the source virtual network.
* Configure virtual network access settings: Select Enabled to allow resources in both virtual networks to communicate with each other.
* Allow forwarded traffic: Select Disabled to prevent traffic that originates from outside either of the peered virtual networks from being forwarded through either of them.
* Allow gateway transit: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network.
* Use remote gateways: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network as a transit point to another network.
* Select Add to create the peering2.
* Repeat the previous steps to create peerings between VNET2 and VNET1, and between VNET2 and VNET3. This will allow hosts on VNET2 to access hosts on both VNET1 and VNET3.
* To prevent hosts on VNET1 and VNET3 from communicating through VNET2, you need to use network security groups (NSGs) to filter traffic between subnets. NSGs are rules that allow or deny inbound or outbound traffic based on source or destination IP address, port, or protocol3.
* To create an NSG, you need to go to the Azure portal and select Create a resource. Search for network security group and select Network security group. Then select Create4.
* On the Create a network security group page, enter or select the following information:
* Subscription: Select your subscription name.
* Resource group: Select your resource group name.
* Name: Type a unique name for your NSG.
* Region: Select the same region as your virtual networks.
* Select Review + create and then select Create to create your NSG4.
* To add rules to your NSG, you need to go to the Network security groups service in the Azure portal and select your NSG. Then select Inbound security rules or Outbound security rules under Settings and select + Add4.
* On the Add inbound security rule page or Add outbound security rule page, enter or select the following information:
* Source or Destination: Select CIDR block.
* Source CIDR blocks or Destination CIDR blocks: Enter the IP address range of the source or destination subnet that you want to filter. For example, 10.0.1.0/24 for VNET1 subnet 1, 10.0.2.0 /24 for VNET2 subnet 1, and 10.0.3.0/24 for VNET3 subnet 1.
* Protocol: Select Any to apply the rule to any protocol.
* Action: Select Deny to block traffic from or to the source or destination subnet.
* Priority: Enter a number between 100 and 4096 that indicates the order of evaluation for this rule.
Lower numbers have higher priority than higher numbers.
* Name: Type a unique name for your rule.
* Select Add to create your rule4.
* Repeat the previous steps to create inbound and outbound rules for your NSG that deny traffic between VNET1 and VNET3 subnets. For example, you can create an inbound rule that denies traffic from
10.0.1.0/24 (VNET1 subnet 1) to 10.0.3.0/24 (VNET3 subnet 1), and an outbound rule that denies traffic from 10.0.3.0/24 (VNET3 subnet 1) to 10.0.1.0/24 (VNET1 subnet 1).
* To associate your NSG with a subnet, you need to go to the Virtual networks service in the Azure portal and select your virtual network. Then select Subnets under Settings and select the subnet that you want to associate with your NSG5.
* On the Edit subnet page, under Network security group, select your NSG from the drop-down list. Then select Save5.
* Repeat the previous steps to associate your NSG with the subnets in VNET1 and VNET3 that you want to isolate from each other.

質問: **62**
500のセッションホストを持つAzureVirtualDesktopデプロイメントがあります。
インターネットへのすべてのアウトバウンドトラフィックはNATゲートウェイを使用します。
営業時間のピーク時には、インターネットリソースにアクセスできないと報告するユーザーもいます。Azure Monitorでは、多くの失敗したSNAT接続を検出します。
使用可能なSNAT接続を増やす必要があります。
あなたは何をするべきか？
A. パブリックIPアドレスを追加します。
B. NATゲートウェイを別のサブネットにバインドします。
C. アウトバウンドルールを持つAzure Standard LoadBalancerをデプロイします。
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

質問: **63**
FQDN として www.contoso.com を使用する Web サイトを公開する予定です。この Web サイトは、次の表に示す Azure App Service アプリを使用してホストされます。

Name	FQDN	Location	Public IP address
AS1	As1.contoso.com	East US	131.107.100.1
AS2	As2.contoso.com	West US	131.107.200.1

Azure Traffic Manager を使用して、AS1 と AS2 間の www.contoso.com へのトラフィックのルーティングを管理する予定です。
Traffic Manager が www.contoso.com のトラフィックをルーティングするようにする必要があります。
どの DNS レコードを作成する必要がありますか?
A. wmv.contoso.com を 131 107 100 1 と 131 107 200 1 にマッピングする 2 つの A レコード
B. www.contoso.com を TMprofile1.azurefd.net にマッピングする CNAME レコード
C. www.contoso.comをTMprofile1.trafficmanager.netにマッピングするCNAMEレコード
D. 詳細にas1.contoso.comとas2.contoso.comの文字列を含むTXTレコード
正解: **C (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/quickstart-create-traffic-manager-profile
https://docs.microsoft.com/en-us/azure/app-service/configure-domain-traffic-manager

質問: **64**
次の表に示すルートを持つ RT1 という名前のルート テーブルを構成します。

Name	Prefix	Next hop type	Next hop IP address
Route1	0.0.0.0/0	Network virtual appliance (NVA)	192.168.0.4
Route2	10.0.0.0/24	Network virtual appliance (NVA)	192.168.0.4

次の表に示すサブネットを持つ Vnet1 という名前の Azure 仮想ネットワークがあります。

Name	Prefix	Route table
DMZ	192.168.0.0/24	None
FrontEnd	192.168.1.0/24	RT1
BackEnd	192.168.2.0/24	None

次の表に示すリソースがあります。

Name	IP address	Type
NVA1	192.168.0.4	NVA
VM1	192.168.1.4	Virtual machine
VM2	192.168.2.4	Virtual machine

Vnet1 は ExpressRoute 回線に接続します。オンプレミスルーターは以下のルートをアドバタイズします。

* 0.0.0.0/0
* 10.0.0.0/16

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。注：正しい選択肢は1つにつき1点です。

Answer Area

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network.	○	○
Traffic from VM1 is routed to the on-premises network through NVA1.	○	○
Traffic from VM1 is routed to VM2 through NVA1.	○	○

正解:

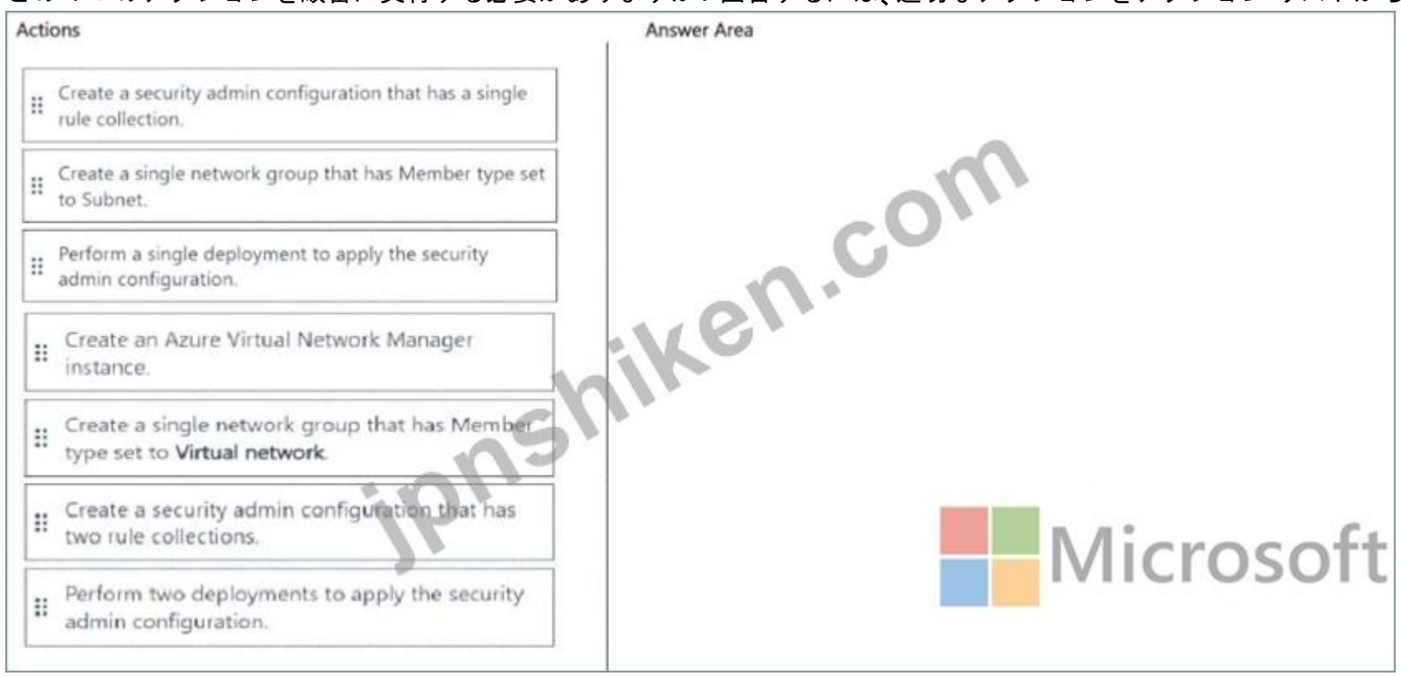
Answer Area

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network.	○	○
Traffic from VM1 is routed to the on-premises network through NVA1.	○	○
Traffic from VM1 is routed to VM2 through NVA1.	○	○

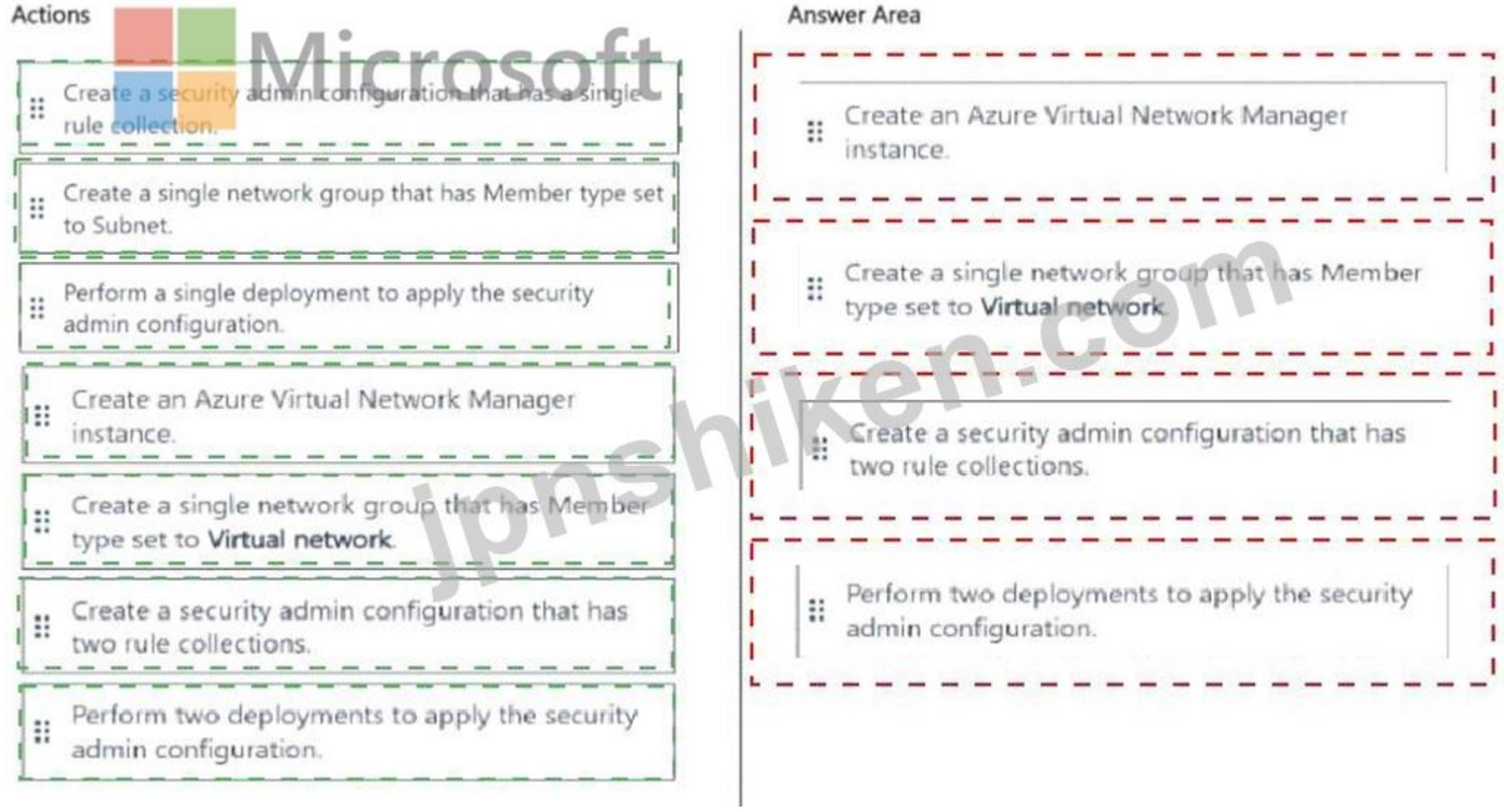
質問: 65

Azure Virtual Network Manager をデプロイする必要があります。ソリューションは計画されている変更をサポートし、接続要件を満たす必要があります。

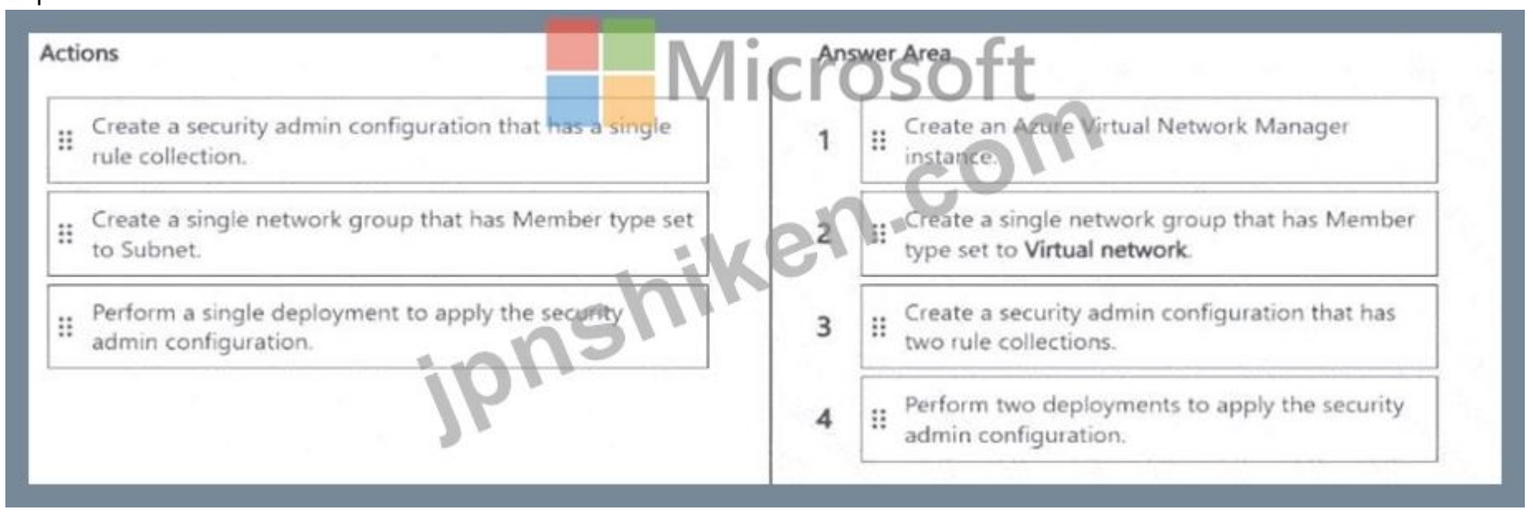
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



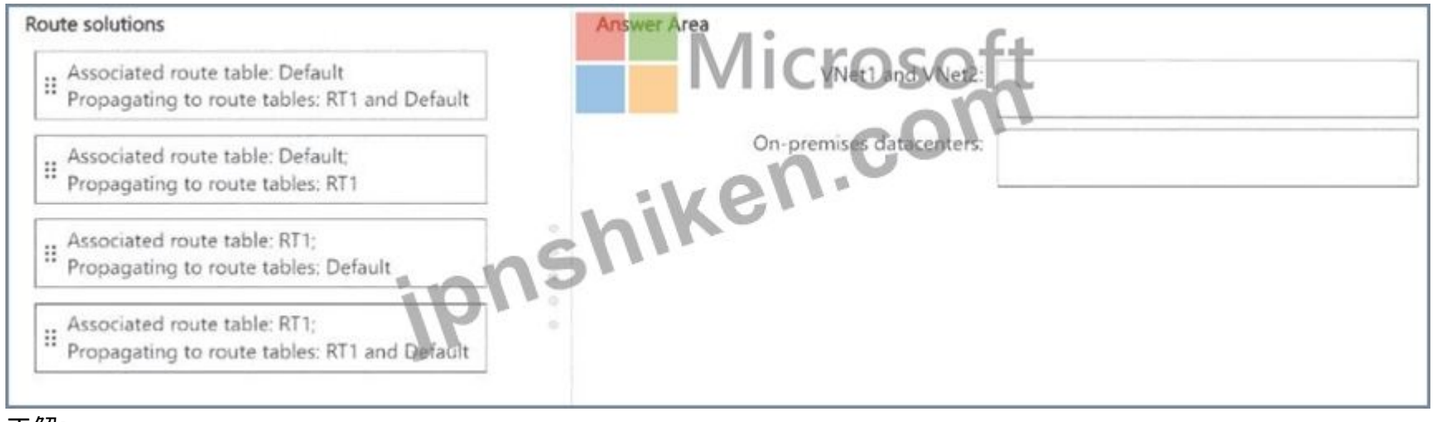
質問: **66**

オンプレミス ネットワークがあります。

仮想ネットワークを含む Azure サブスクリプションがあります。ExpressRoute サービス プロバイダーがあります。

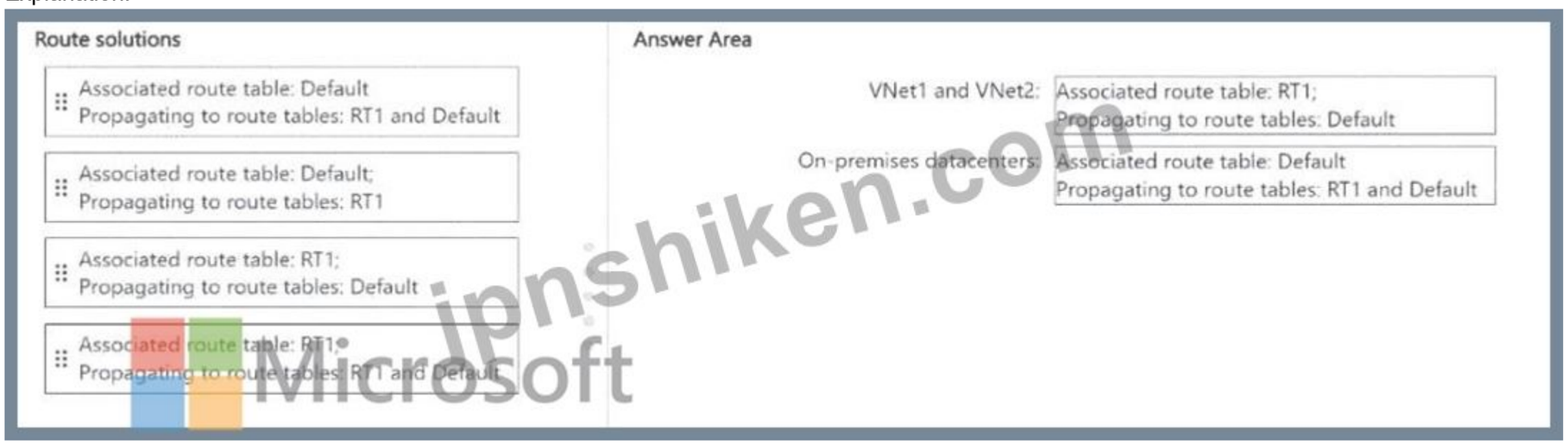
ExpressRoute 回線を使用して、Azure 仮想ネットワークとオンプレミス ネットワークを接続する予定です。
新しいExpressRoute回線を作成します。新しい回線をプロビジョニングする必要があります。サービスプロバイダーに提供する必要がある情報はどれですか？
A. IKEv2共有キー
B. パブリックIPアドレス
C. サービスキー
D. 証明書
正解: **(**正解を表示します**)**

質問: **67**
オンプレミスのデータセンターが 2 つあります。
VNet1、VNet2、VNet3、VNet4 という 4 つの仮想ネットワークを含む Azure サブスクリプションがあります。VWAN1 という Azure 仮想 WAN を作成します。VWAN1 には、オンプレミスのデータセンターと、フルメッシュ トポロジ内のすべての仮想ネットワークに接続された単一の仮想ハブが含まれています。
RT1 という名前のルート テーブルを作成します。
次の要件を満たすように VWAN1 を構成する必要があります。
* VNet1 と VNet2 および両方のオンプレミス データセンター間の接続を許可する必要があります。
* VNet3 と VNet4 および両方のオンプレミス データセンター間の接続を許可する必要があります。
* VNet1 と VNet2 は、VNet3 と VNet4 から分離する必要があります。
VNet1 と VNet2、そして両方のオンプレミスデータセンターのルーティングをどのように構成すればよいでしょうか？ 適切なルートテーブルとルートテーブル伝播を適切な要件に合わせてドラッグしてください。各ルートテーブルとルートテーブル伝播は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Explanation:



質問: **68**

Azure サブスクリプションが 2 つあります。

各サブスクリプションの米国東部 Azure リージョンで次のアクションを実行する必要があります。

* 可用性ゾーン 1 に 50 台の仮想マシンをデプロイします。
* 可用性ゾーン 2 に 50 台の仮想マシンをデプロイします。
* 可用性ゾーン 3 に 50 台の仮想マシンをデプロイします。

作成する必要がある仮想ネットワークと /25 サブネットの最小数はいくつですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

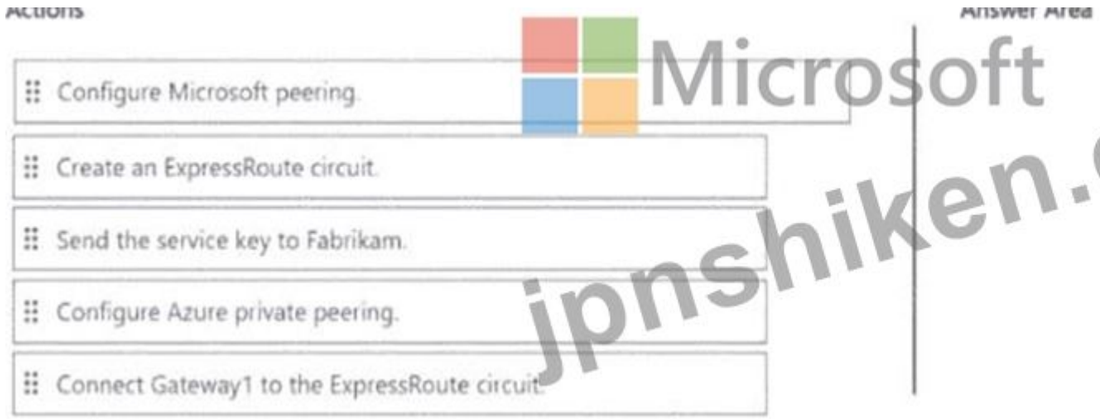
質問: **69**

オンプレミスネットワークがある

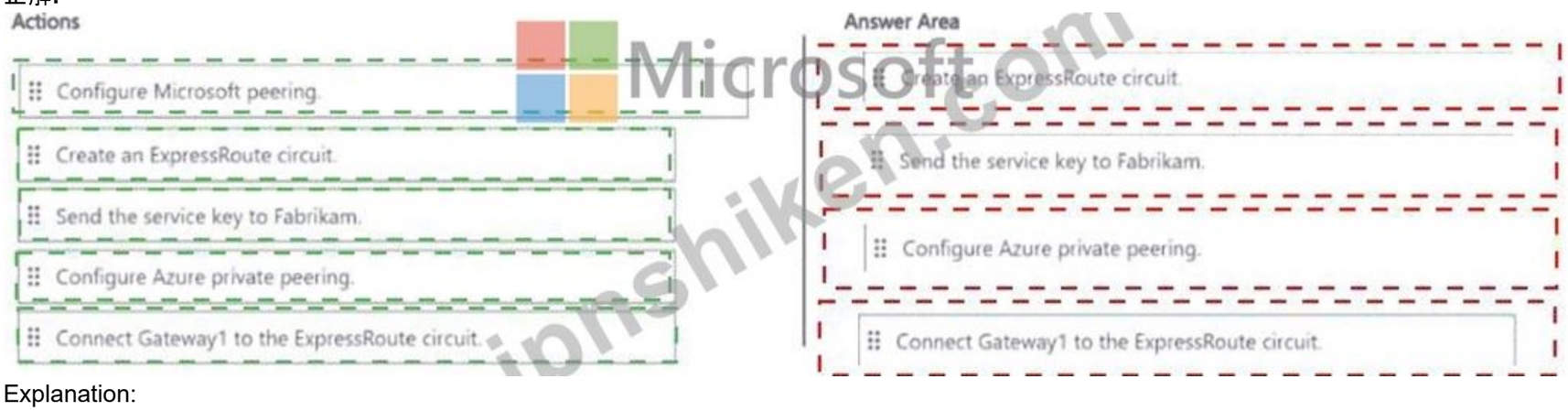
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には、Gateway 1 という名前の ExpressRoute ゲートウェイが含まれています。

Fabrikam, Inc. というサードパーティ プロバイダーの ExpressRoute ソリューションを実装する必要があります。ソリューションでは、オンプレミス ネットワーク上のデバイスが VNet1 上の Azure リソースに接続できることを保証する必要があります。

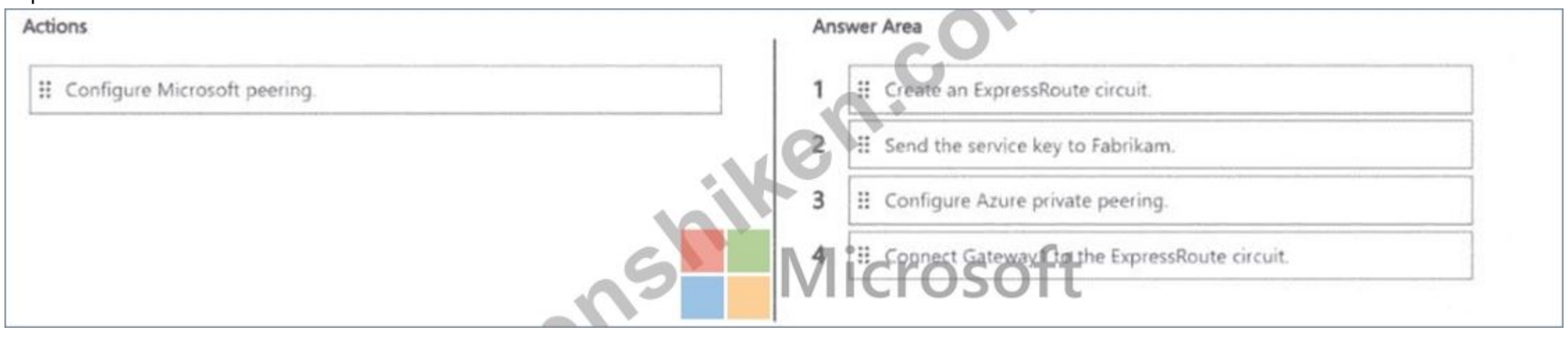
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



質問: **70**

タスク1

VNET1 と VNET2 上の仮想マシンが contoso.azure という DNS ゾーンに自動的に含まれるようにする必要があります。ソリューションでは、VNET1 と VNET2 上の仮想マシンが、どちらの仮想ネットワーク上の仮想マシンの名前も解決できるようにする必要があります。

正解:

See the Explanation below for step by step instructions.

Explanation:

To achieve the task of ensuring that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contoso.azure, and that they can resolve the names of the virtual machines on either virtual network, you can follow these steps:
Step-by-Step Solution
Step 1: Create a Private DNS Zone
* Navigate to the Azure Portal.
* Search for "Private DNS zones" in the search bar and select it.
* Click on "Create".
* Enter the DNS zone name as contoso.azure.
* Select the appropriate subscription and resource group.
* Click on "Review + create" and then "Create".
Step 2: Link VNET1 and VNET2 to the DNS Zone
* Go to the newly created DNS zone (contoso.azure).
* Select "Virtual network links" from the left-hand menu.
* Click on "Add".
* Enter a name for the link (e.g., VNET1-link).
* Select the subscription and virtual network (VNET1).
* Enable auto-registration to ensure that VMs are automatically registered in the DNS zone.
* Click on "OK".
* Repeat the process for VNET2.
Step 3: Configure DNS Settings for VNET1 and VNET2
* Navigate to VNET1 in the Azure Portal.
* Select "DNS servers" under the "Settings" section.
* Ensure that the DNS server is set to "Default (Azure-provided)".
* Repeat the process for VNET2.
Step 4: Verify Name Resolution
* Deploy a virtual machine in VNET1 and another in VNET2.
* Connect to the virtual machines using Remote Desktop Protocol (RDP) or Secure Shell (SSH).
* Test name resolution by pinging the VM in VNET2 from the VM in VNET1 using its hostname (e.
g., ping <VM-name>.contoso.azure).
Explanation:
* Private DNS Zone: This allows you to manage and resolve domain names in a private network without exposing them to the public internet.
* Virtual Network Links: Linking VNET1 and VNET2 to the DNS zone ensures that VMs in these networks can register their DNS records automatically.
* Auto-registration: This feature automatically registers the DNS records of VMs in the linked virtual networks, simplifying management.
* DNS Settings: Using Azure-provided DNS ensures that the VMs can resolve each other's names without additional configuration.
By following these steps, you ensure that virtual machines on VNET1 and VNET2 are included automatically in the DNS zone contoso.azure and can resolve each other's names seamlessly.

質問**: 71**
タスク11
VNET1 上のホストのみが slcnage42150372 ストレージ アカウントにアクセスできるようにする必要があります。このソリューションでは、Azure バックボーン ネットワーク経由でアクセスが行われるようにする必要があります。
正解:

See the Explanation below for step by step instructions.
Explanation:
To ensure that only hosts on VNET1 can access the slcnage42150372 storage account and that access occurs over the Azure backbone network, you can use Azure Private Endpoints. This method secures the connection by assigning a private IP address from your virtual network to the storage account, ensuring that traffic does not traverse the public internet.
Step-by-Step Solution
Step 1: Create a Private Endpoint for the Storage Account
* Navigate to the Azure Portal.
* Search for "Storage accounts" and select the slcnage42150372 storage account.
* In the storage account blade, select "Networking" under the "Security + networking" section.
* Under "Private endpoint connections", click on "Add private endpoint".
* Enter the following details:
* Name: Enter a name for the private endpoint (e.g., PrivateEndpoint-VNET1).
* Region: Select the same region as your virtual network (VNET1).
* Click on "Next: Resource".
Step 2: Configure the Resource
* Select "Target sub-resource": Choose the storage service you want to connect to (e.
g., blob, file, queue, table).
* Click on "Next: Virtual network".
Step 3: Select the Virtual Network and Subnet
* Select the virtual network: Choose VNET1.
* Select the subnet: Choose the appropriate subnet within VNET1.
* Click on "Next: Configuration".
Step 4: Configure DNS Integration (Optional)
* Configure DNS settings if needed to ensure proper name resolution within your virtual network.
* Click on "Next: Tags", add any tags if necessary, and then click on "Review + create".
* Review your settings and click on "Create".
Step 5: Restrict Public Network Access
* Navigate back to the storage account.
* Select "Networking" under the "Security + networking" section.
* Under "Firewalls and virtual networks", select "Selected networks".
* Ensure that only VNET1 is listed under the virtual networks section.
* Click on "Save".
Explanation:
* Private Endpoints: These provide secure connectivity to Azure services by assigning a private IP address from your VNet to the service, ensuring that traffic stays within the Azure backbone network12.
* Firewall and Virtual Networks: Configuring the storage account to allow access only from selected networks (VNET1) ensures that no other network can access the storage account3.
By following these steps, you can ensure that only hosts on VNET1 can access the slcnage42150372 storage account, and that all access occurs over the secure Azure backbone network.

質問**: 72**
VM1 という名前の仮想マシン、NIC1 という名前の仮想ネットワーク インターフェイス カード (NIC)、および IP1 という名前の Basic SKU パブリック IP アドレスを含む Azure サブスクリプションがあります。NIC1 は VM1 に接続され、IP1 は NIC1 に関連付けられています。

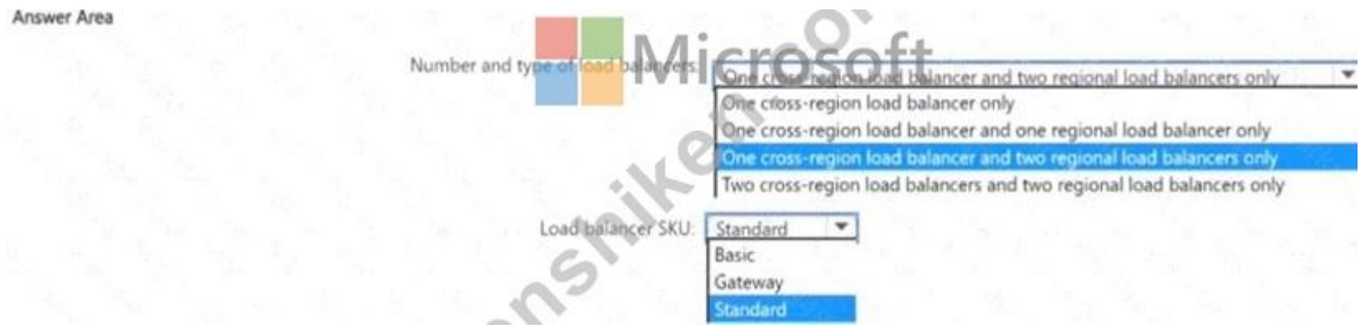
IP1 を標準 SKU にアップグレードする必要があります。
まず何をすべきでしょうか?
A. VM1 に新しい NIC を作成します。
B. VM1 を停止します。
C. IP1 と NIC1 の関連付けを解除します。
D. NIC1 を VM1 から切断します。
正解: **C** (コメントを発表する)

質問: **73**
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には、Pool1 という名前の Azure Virtual Desktop ホスト プールが含まれています。
Pool1 からのすべての送信トラフィックに対して、Azure Firewall と TLS 検査を実装する必要があります。
どの 2 つのリソースを構成する必要がありますか? それぞれの正解はソリューションの一部を示します。
注意: 正解ごとに1ポイント獲得できます
A. Azure キー コンテナー
B. プライベートエンドポイント
C. 管理されたID
D. Azure NAT ゲートウェイ
E. Microsoft Entra エンタープライズ アプリ
F. Azure プライベート DNS ゾーン
正解: (正解を表示します)

質問: **74**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
VNet1	Virtual network	In the West Europe Azure region
VNet2	Virtual network	In the East US Azure region
VM1	Virtual machine	On VNet1
VM2	Virtual machine	On VNet1
VM3	Virtual machine	On VNet2
VM4	Virtual machine	On VNet2

次の要件を満たすために、App1 という名前のアプリを展開する予定です。
* 外部ユーザーはインターネットから App1 にアクセスできる必要があります。
* App1 はすべての仮想マシン間で負荷分散されます。
* App1 は VM1、VM2、VM3、VM4 でホストされます。
* Azure リージョンに障害が発生した場合でも、App1 は使用可能である必要があります。
* コストを最小限に抑える必要があります。
アプリにグローバル ロード バランサー ソリューションを実装する必要があります。
何を設定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。注: 各正解は 1 ポイントの価値があります。



正解:

Explanation:

質問: **75**

タスク 5

VNET1 のすべてのメトリックを既存のストレージ アカウントにアーカイブする必要があります。

正解:

See the Explanation below for step by step instructions.

Explanation:

To archive all the metrics of VNET1 to an existing storage account, you can use Azure Monitor's diagnostic settings. Here's how you can do it:

Step-by-Step Solution

Step 1: Navigate to VNET1 in the Azure Portal

* Open the Azure Portal.
* Search for "Virtual networks" and select VNET1 from the list.

Step 2: Configure Diagnostic Settings

* In the VNET1 blade, select "Diagnostic settings" under the "Monitoring" section.
* Click on "Add diagnostic setting".

Step 3: Set Up the Diagnostic Setting

* Enter a name for the diagnostic setting (e.g., VNET1-Metrics-Archive).
* Select the metrics you want to archive. You can choose from various metrics like TotalBytesReceived, TotalBytesSent, etc.
* Under "Destination details", select "Archive to a storage account".

* Choose the existing storage account where you want to archive the metrics.
* Configure the retention period if needed.
Step 4: Save the Configuration
* Review your settings to ensure everything is correct.
* Click on "Save" to apply the diagnostic setting.
Explanation:
* Diagnostic Settings: These allow you to collect and route metrics and logs from your Azure resources to various destinations, including storage accounts, Log Analytics workspaces, and Event Hubs.
* Metrics: Metrics provide numerical data about the performance and health of your resources. Archiving these metrics helps in long-term analysis and compliance.
* Storage Account: Using an existing storage account ensures that the metrics are stored securely and can be accessed for future analysis.
By following these steps, you can ensure that all the metrics of VNET1 are archived to your existing storage account, enabling you to monitor and analyze the performance and health of your virtual network over time.

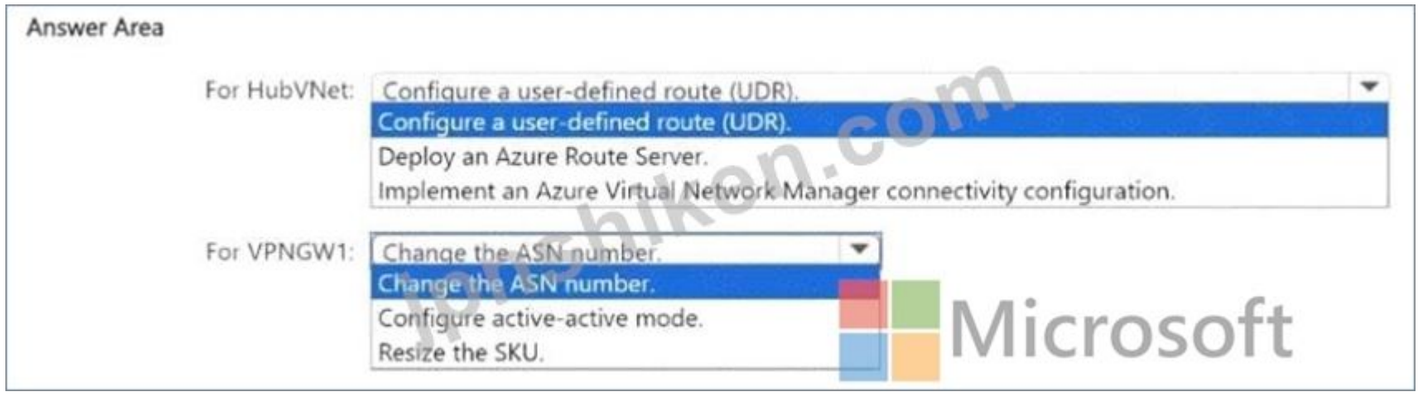
質問**: 76**
オンプレミス ネットワークには VPN デバイスが含まれています。
仮想ネットワークと仮想ネットワーク ゲートウェイを含む Azure サブスクリプションがあります。
カスタム暗号化ポリシーを持つサイト間 VPN 接続を作成する必要があります。
PowerShell スクリプトをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

質問: **77**

NYCNetとSFONet間の接続を設定する必要があります。ソリューションは接続要件を満たしている必要があります。どうすればよいでしょうか？回答するには、回答エリアで適切な選択肢を選択してください。注：正解は1つにつき1ポイントです。



正解:

Explanation:

質問: **78**

VM1 という名前の Azure 仮想マシンがあります。

Azure Network Watcher を使用して、VM1 のすべてのネットワーク トラフィックをキャプチャする必要があります。キャプチャしたデータはどの場所に書き込むことができますか？

A. VM1のみの汎用v2パス

B. 汎用 v2 標準ストレージ アカウントのみ

C. VM1のみのファイルシステムパス

D. ブロック BLOB プレミアム ストレージ アカウントのみ

E. 汎用 v2 標準ストレージ アカウントとブロック BLOB プレミアム アカウントのみ

正解: **A** (コメントを発表する)

質問: **79**

次の表に示すパブリックIPv4アドレスを含むAzureサブスクリプションがあります。

Name	SKU	IP address assignment	Location
IP1	Basic	Static	West US
IP2	Basic	Dynamic	West US
IP3	Standard	Static	West US
IP4	Basic	Static	West US 2
IP5	Standard	Static	West US 2

次の設定を持つLB1という名前のロードバランサーを作成する予定です。
*名前 :LB1
*場所：米国西部
*タイプ :パブリック
* SKU：標準
LB1で使用できるパブリックIPv4アドレスはどれですか？
A. IP1およびIP3のみ
B. IP3のみ
C. IP3およびIP5のみ
D. IP2のみ
E. IP1、IP2。IP3。IP4。およびIP5
F. IP1、IP3、IP4、および1P5のみ
正解: **C** (コメントを発表する)
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address This is because "Load balancer and the public IP address SKU must match when you use them with public IP addresses" https://docs.microsoft.com/en-us/azure/load-balancer/skus Standard SKU Load Balancer routes traffic within and across regions, and to Availability Zones for high resiliency.

質問: **80**
次の表に示すAzureリソースがあります。

Name	Type	Location	Description
storage1	Storage account	East US	Read-access geo-redundant storage (RA-GRS)
Vnet1	Virtual network	East US	Contains one subnet

サービスエンドポイントを使用して、Vnet1のサブネットへのアクセスを提供するようにstorage1を構成します。
サービスエンドポイントを使用して、ペアリングされたAzureリージョンのstorage1の読み取り専用エンドポイントに接続できることを確認する必要があります。
あなたは最初に何をすべきですか？
A. storage1をペアリングされたAzureリージョンにフェールオーバーします。
B. 別のサービスエンドポイントを作成します。
C. storage1のファイアウォール設定を構成します。
D. ペアリングされたAzureリージョンに仮想ネットワークを作成します。
正解: **C** (コメントを発表する)

質問: **81**
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。

VNet1 に、AppGw1 という名前の Azure Application Gateway v2 インスタンスをデプロイする必要があります。AppGw1 には、1 つの基本リスナーと 2 つのマルチサイト リスナーが含まれます。これらのリスナーには VNet1 からのみアクセスできます。
AppGw1 に必要な IP アドレスの最小数はいくつですか? 回答するには、回答領域で適切なオプションを選択してください。注: 正しい選択ごとに 1 ポイントが加算されます。

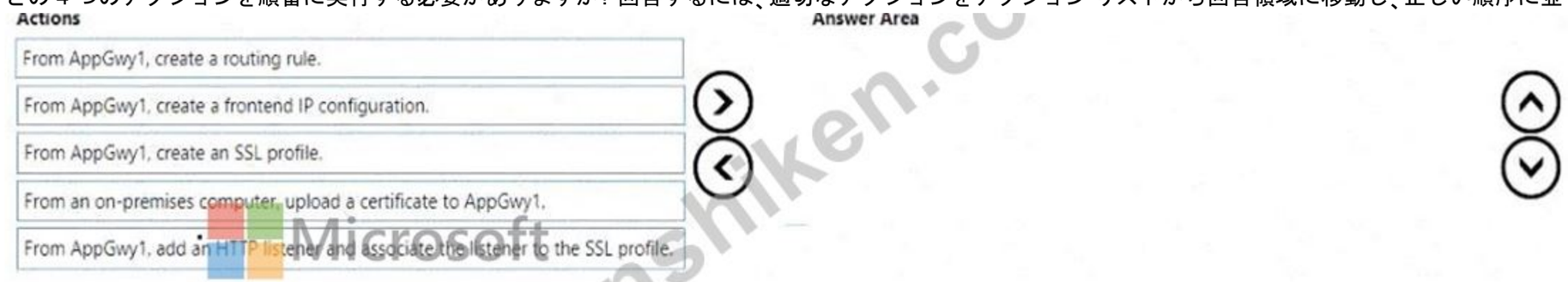
正解:

Explanation:

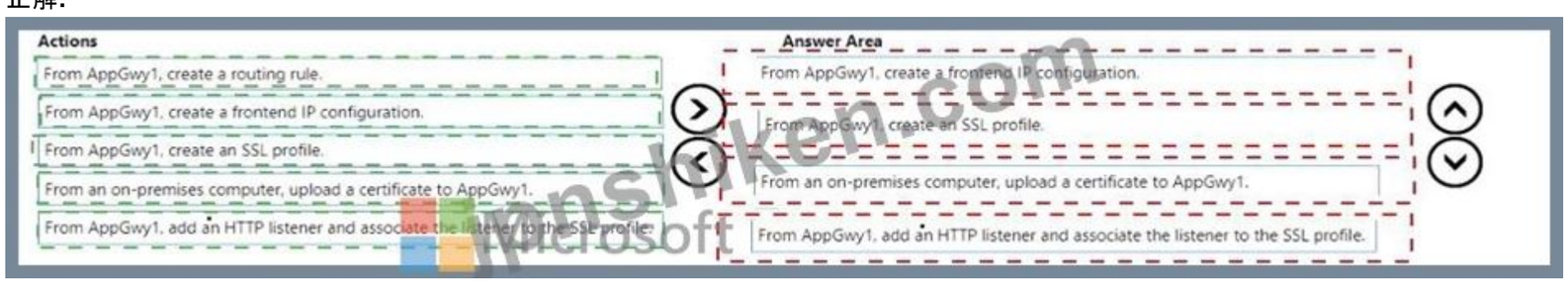
質問: **82**
オンプレミス ネットワークが 3 つあります。
Basic Azure仮想WANを含むAzureサブスクリプションがあります。この仮想WANには、1つの仮想ハブと、スループットが1Gbpsに制限された仮想ネットワークゲートウェイが含まれています。
オンプレミス ネットワークは、サイト間 (S2S) VPN 接続を使用して仮想 WAN に接続します。
仮想WANのスループットを3Gbpsに向上させる必要があります。ソリューションは管理作業を最小限に抑える必要があります。
何をすべきでしょうか?
A. 追加の仮想ハブを作成します。
B. 仮想 WAN を Standard SKU にアップグレードします。
C. AzureサブスクリプションにVPNゲートウェイを追加します。
D. ゲートウェイ スケール ユニットの数を増やします。
正解: **D** (コメントを発表する)

質問: **83**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできなくなり、これらの質問はレビュー画面に表示されなくなります。
AFD1 という名前の Azure Front Door Premium プロファイルと WAF1 という名前の Azure Web アプリケーション ファイアウォール (WAF) ポリシーを含む Azure サブスクリプションがあります。AFD1 は WAF1 に関連付けられています。
AFD1 への受信リクエストのレート制限を構成する必要があります。
解決策: WAF1 のポリシー設定を変更します。
これは目標を達成していますか?
A. いいえ
B. はい
正解: **A** (コメントを発表する)

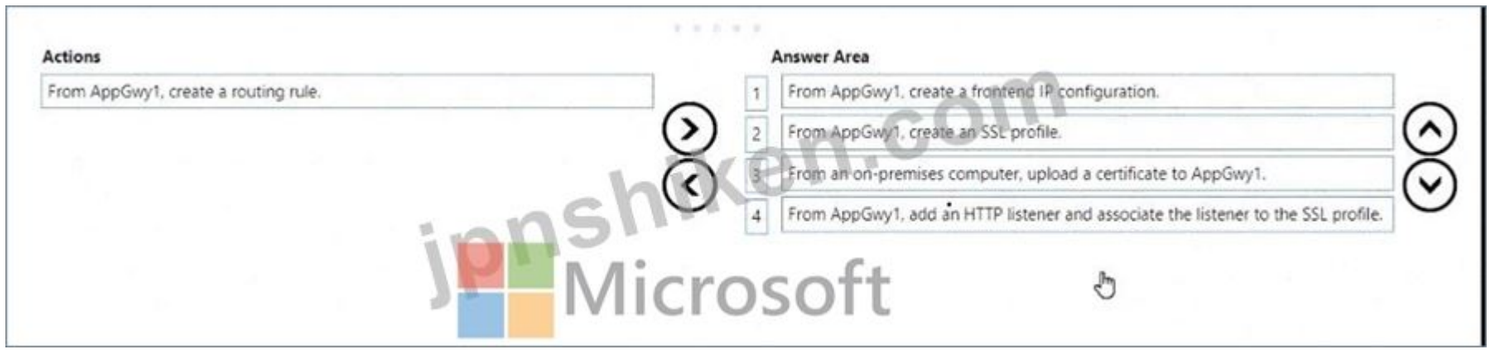
質問: **84**
オンプレミス ネットワークには、contoso という名前の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
内部証明機関 (CA) を持つ com です。
Azure サブスクリプションをお持ちです。
AppGwy1 という名前の Azure アプリケーション ゲートウェイをデプロイし、次のアクションを実行します。
* HTTP リスナーを構成します。
* ルーティング ルールをリスナーに関連付けます。
ドメインに参加しているコンピューターから contoso.com への要求に対して相互認証を実行するように AppGwy1 を構成する必要があります。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



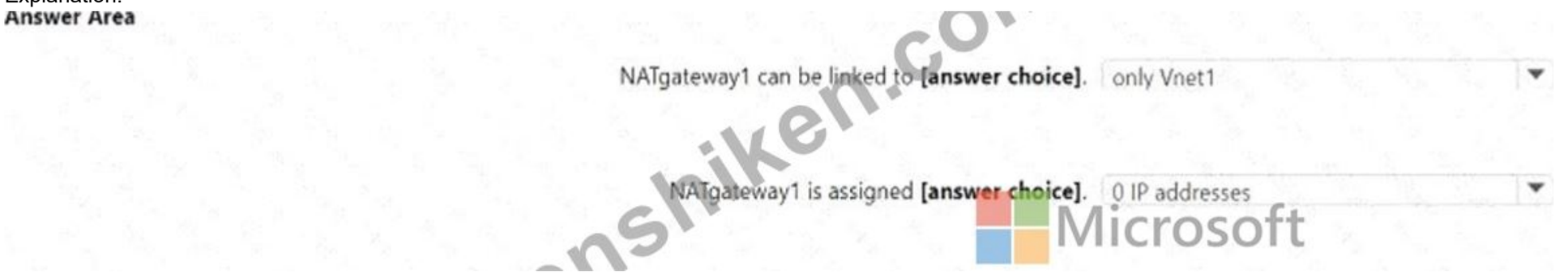
質問: **85**

Vnet1 という Azure 仮想ネットワークがあり、その中に Subnet1 と Subnet2 という 2 つのサブネットがあります。どちらのサブネットにも仮想マシンが含まれています。次の図に示すように、NATgateway1 という NAT ゲートウェイを作成します。

ドロップダウンメニューを使用して、図に示されている情報に基づいて各文を完成させる選択肢を選択してください。注: 正解は1つにつき1ポイントです。

正解:

Explanation:



質問: **86**

タスク3

米国東部 Azure リージョンに Azure アプリケーション ゲートウェイを実装する予定です。このアプリケーション ゲートウェイでは、Web アプリケーション ファイアウォール (WAF) が有効になります。
計画中のアプリケーションゲートウェイにリンクできるポリシーを作成する必要があります。このポリシーは、131.107.150.0/24 の範囲の IP アドレスからの接続をブロックする必要があります。このタスクを完了するためにアプリケーションゲートウェイをプロビジョニングする必要はありません。
正解**:**
See the Explanation below for step by step instructions.
Explanation:
Here are the steps and explanations for creating a policy that can be linked to the planned application gateway and block connections from IP addresses in the 131.107.150.0/24 range:
* To create a policy, you need to go to the Azure portal and select Create a resource. Search for WAF, select Web Application Firewall, then select Create1.
* On the Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:
* Policy for: Regional WAF (Application Gateway)
* Subscription: Select your subscription name
* Resource group: Select your resource group
* Policy name: Type a unique name for your WAF policy
* On the Custom rules tab, select Add a rule to create a custom rule that blocks connections from IP addresses in the 131.107.150.0/24 range2. Enter or select the following information for the custom rule:
* Rule name: Type a unique name for your custom rule
* Priority: Type a number that indicates the order of evaluation for this rule
* Rule type: Select Match rule
* Match variable: Select RemoteAddr
* Operator: Select IPMatch
* Match values: Type 131.107.150.0/24
* Action: Select Block
* On the Review + create tab, review your settings and select Create to create your WAF policy1.
* To link your policy to the planned application gateway, you need to go to the Application Gateway service in the Azure portal and select your application gateway3.
* On the Web application firewall tab, select your WAF policy from the drop-down list and select Save

質問**: 87**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
App1	Azure App Service	A web app
Gateway1	Azure Application Gateway	includes an SSL certificate that has a subject name of *.contoso.com

ゲートウェイ1
http://app1.contoso.com の URL を使用して App1 へのアクセスを提供します。
App2 という名前の新しい Web アプリを作成します。
管理の労力を最小限に抑えるには、Gateway1 を構成する必要があります。
Gateway1 では何を設定する必要がありますか?
A. リスナーとバックエンドプール
B. バックエンドプールとルーティング

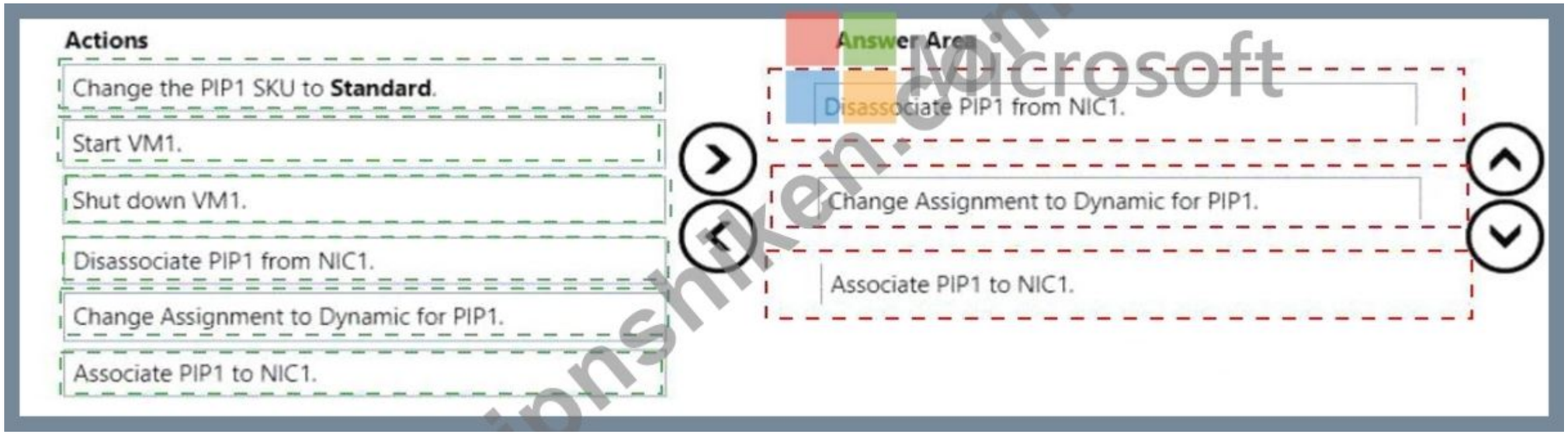
C. リスナーとルーティングルール
D. リスナー、バックエンドプール、ルール
正解: (正解を表示します)

質問: **88**
次の表に示すリソースを含む Azure サブスクリプションがあります。

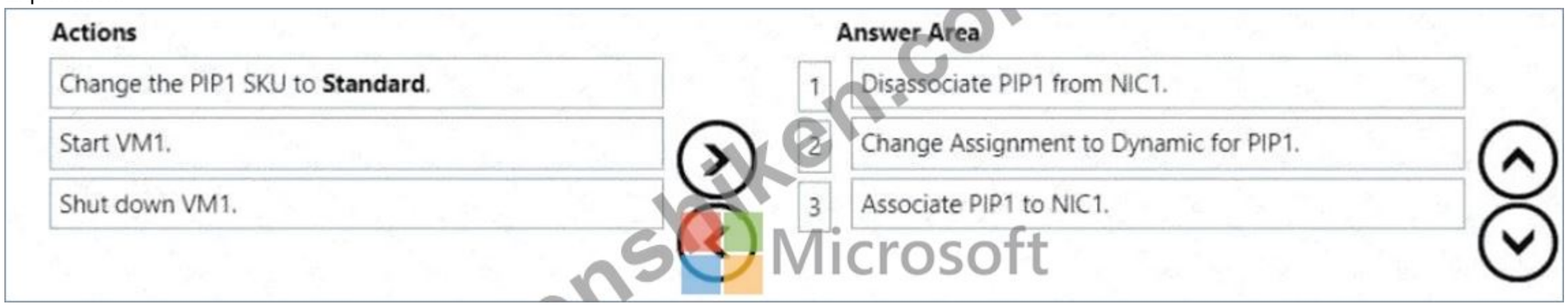
Name	Type	Description
Gateway1	NAT gateway	Unconfigured
NIC1	Network interface	A network interface with a statically assigned public IP address named PIP1
PIP1	Public IP address	A Basic SKU public IP address
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
VM1	Virtual machine	Connected to Subnet1 via NIC1

ゲートウェイ1をサブネット1に関連付ける必要があります。このソリューションでは、VM1のダウンタイムを最小限に抑える必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

正解:



Explanation:



質問: **89**
オンプレミス ネットワークでは、10.1.0.0 ～ 10.1.255.255 の IP アドレス範囲が使用されます。
次の要素を含む新しい Azure 仮想ネットワーク ソリューションを展開する予定です。
* VNet1という名前の仮想ネットワーク
* VNet1 とオンプレミス ネットワーク間のサイト間 (S2S) VPN 接続
* VNet1 の GatewaySubnet（ルートベースの仮想ネットワークゲートウェイとして使用）VNet1 と GatewaySubnet に割り当てるサブネットマスクを推奨する必要があります。ソリューションは以下の要件を満たす必要があります。
* VNet1 で使用可能な IP アドレスの数を最大化します。
* GatewaySubnetで利用可能なIPアドレスの数を最小限に抑える
VNet1 と GatewaySubnet に割り当てるアドレス空間はどれですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

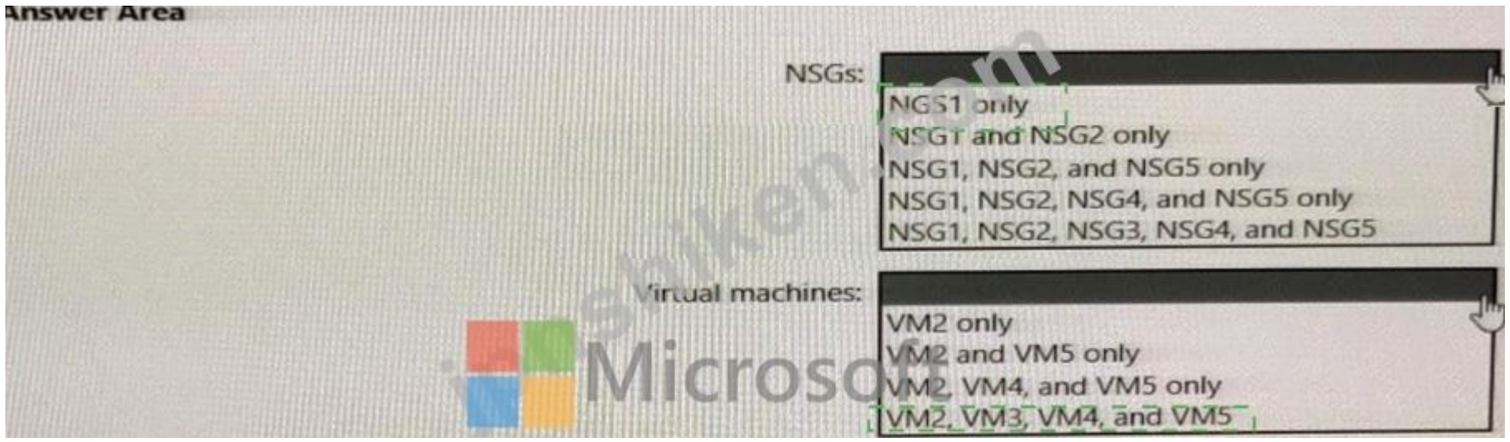
質問: **90**

ASG1 はどの NSG で使用できますか? また、どの仮想マシン ネットワーク インターフェイスに ASG1 を関連付けることができますか?

回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:



Explanation:

NGS1 only

VM2, VM3, VM4 and VM5

質問: **91**

タスク 9

サブネット4-3が507台のホストを収容できることを確認する必要があります。

正解:

See the Explanation below for step by step instructions.

Explanation:

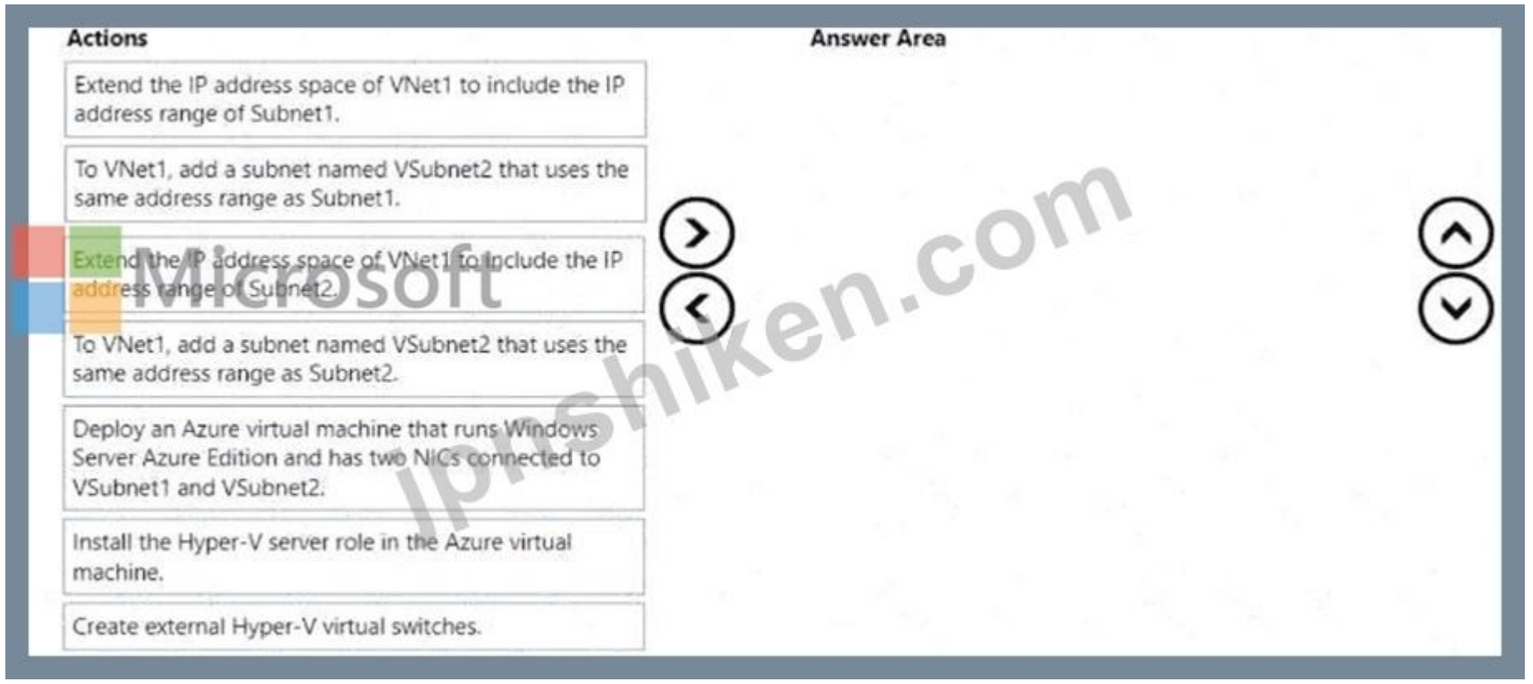
Here are the steps and explanations for ensuring that subnet4-3 can accommodate 507 hosts:

* To determine the subnet size that can accommodate 507 hosts, you need to use the formula: number of hosts = 2^(32 - n) - 2, where n is the number of bits in the subnet mask1. You need to find the value of n that satisfies this equation for 507 hosts.
* To solve this equation, you can use trial and error or a binary search method. For example, you can start with n = 24, which is the default subnet mask for Class C networks. Then, plug in the value of n into the formula and see if it is too big or too small for 507 hosts.
* If you try n = 24, you get number of hosts = 2^(32 - 24) - 2 = 254, which is too small. You need to increase the value of n to get a larger number of hosts.
* If you try n = 25, you get number of hosts = 2^(32 - 25) - 2 = 510, which is just enough to accommodate 507 hosts. You can stop here or try a smaller value of n to see if it still works.

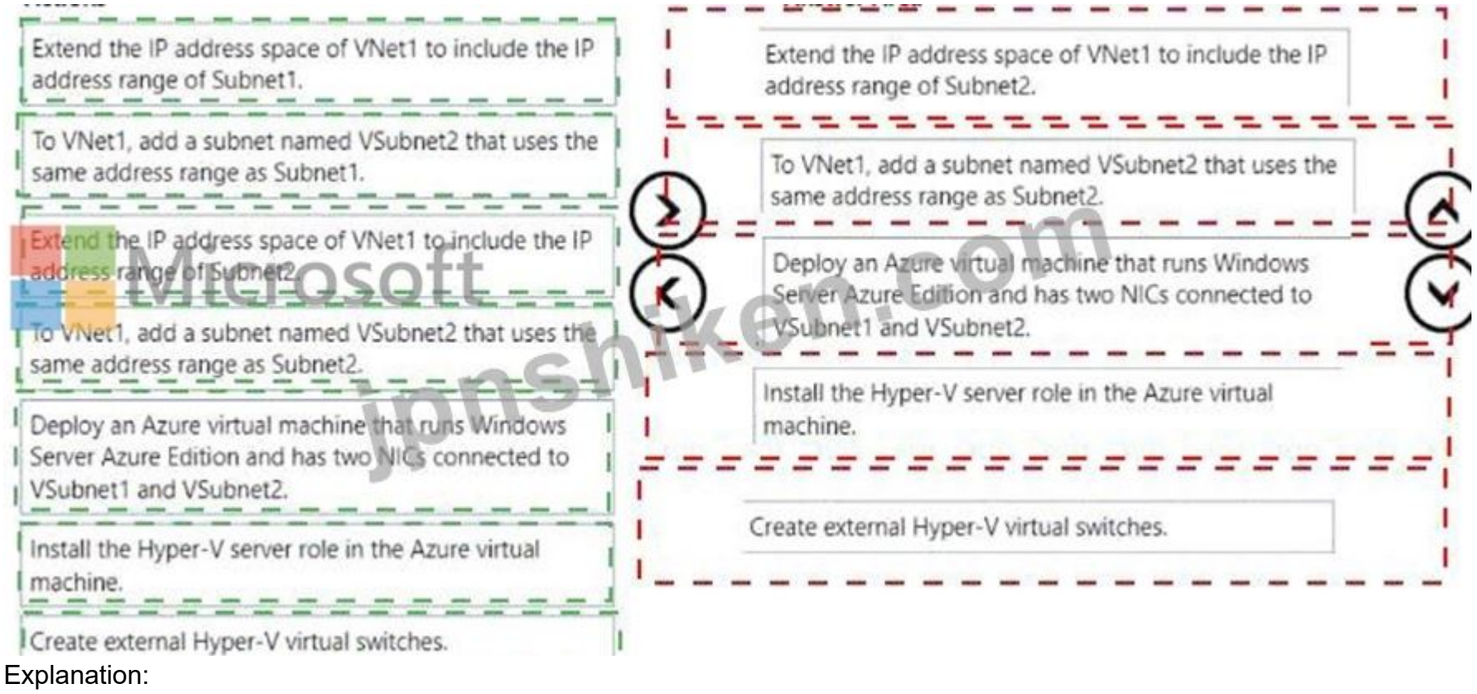
* If you try n = 26, you get number of hosts = 2^(32 - 26) - 2 = 254, which is too small again. You need to decrease the value of n to get a larger number of hosts.
* Therefore, the smallest value of n that can accommodate 507 hosts is n = 25. This means that the subnet mask for subnet4-3 should be /25 or 255.255.255.128 in dot-decimal notation1.
* To change the subnet mask for subnet4-3, you need to go to the Azure portal and select your virtual network. Then select Subnets under Settings and select subnet4-3 from the list2.
* On the Edit subnet page, under Address range (CIDR block), change the value from /24 to /25. Then select Save2.

質問: **92**
あなたの会社には 5 つのオフィスがあります。各オフィスには、ファイアウォール デバイスとローカル インターネット接続があります。オフィスはサードパーティの SD-WAN に接続します。
Vnet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。Vnet1 には、Gateway1 という名前の仮想ネットワーク ゲートウェイが含まれています。各オフィスは、サイト間 VPN 接続を使用して Gateway1 に接続します。
サードパーティの SD-WAN を Azure Virtual WAN に置き換える必要があります。ソリューションには何を含める必要がありますか?
A. Gateway1 を削除します。
B. Azure Traffic Manager プロファイルを作成します。
C. ファイアウォール デバイスで新しいポイント ツー サイト (P2S) VPN 接続を作成します。
D. Gateway1 でアクティブアクティブ モードを有効にします。
正解: **(**正解を表示します**)**

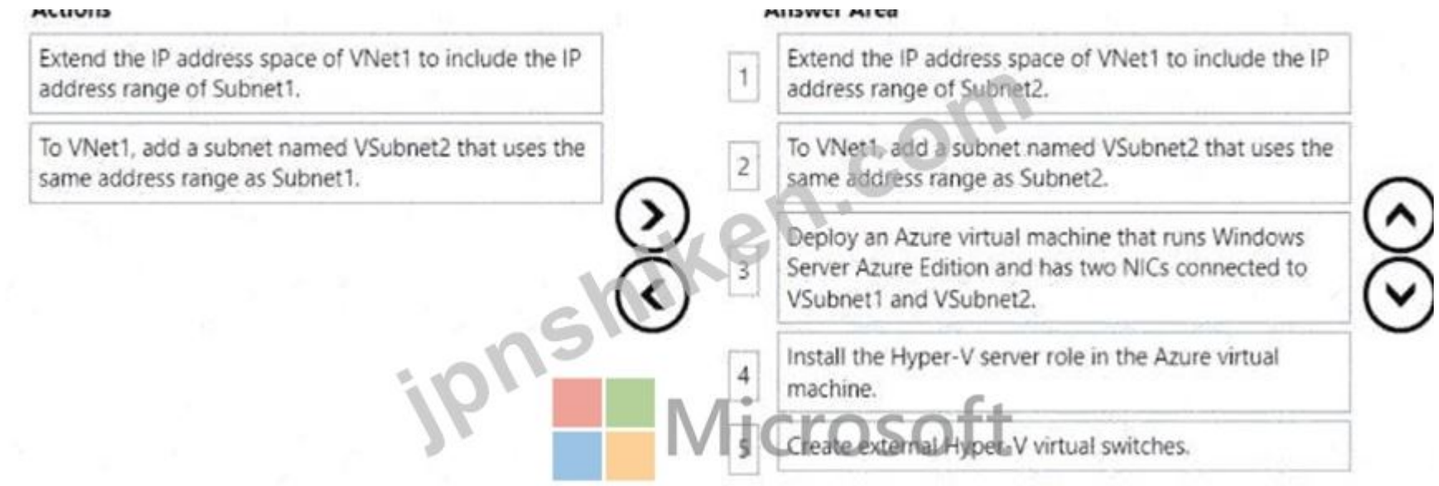
質問: **93**
オンプレミスネットワークには、Subnet1 と Subnet2 という 2 つのサブネットがあります。Subnet2 には、VM1 と VM2 という 2 つの仮想マシンを含む Hyper-V ホストが含まれています。VM1 と VM2 は Subnet2 に接続されています。
VNet1 という名前の Azure 仮想ネットワークがあり、そこには GatewaySubnet と VSubnet1 という名前のサブネットが含まれています。VNet1 は、サイト間 (S2S) VPN 接続を使用してオンプレミス ネットワークに接続されています。
VM1 を VNet1 に移行し、VM1 の既存の IP アドレスを維持する予定です。VM2 は Subnet2 に残ります。
移行が完了したら VM1 が VM2 と通信できるように環境を準備する必要があります。
どの 5 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序に並べます。



正解:

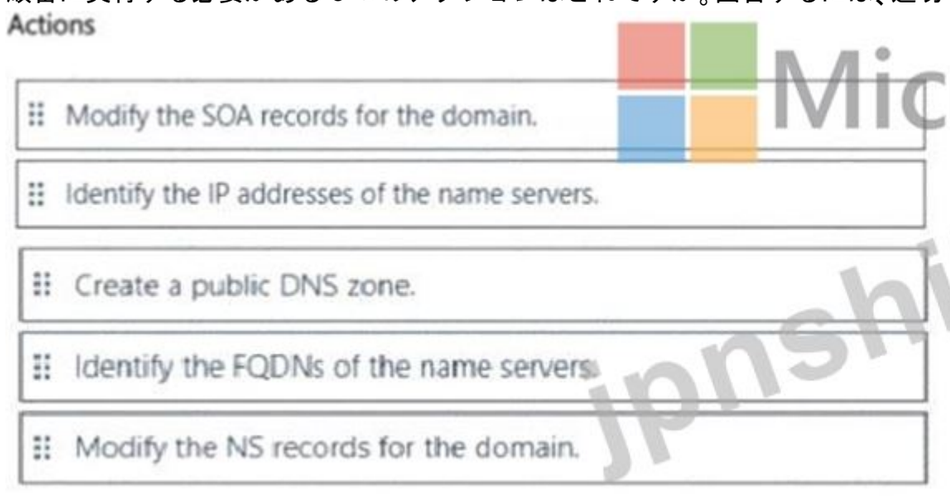


Explanation:

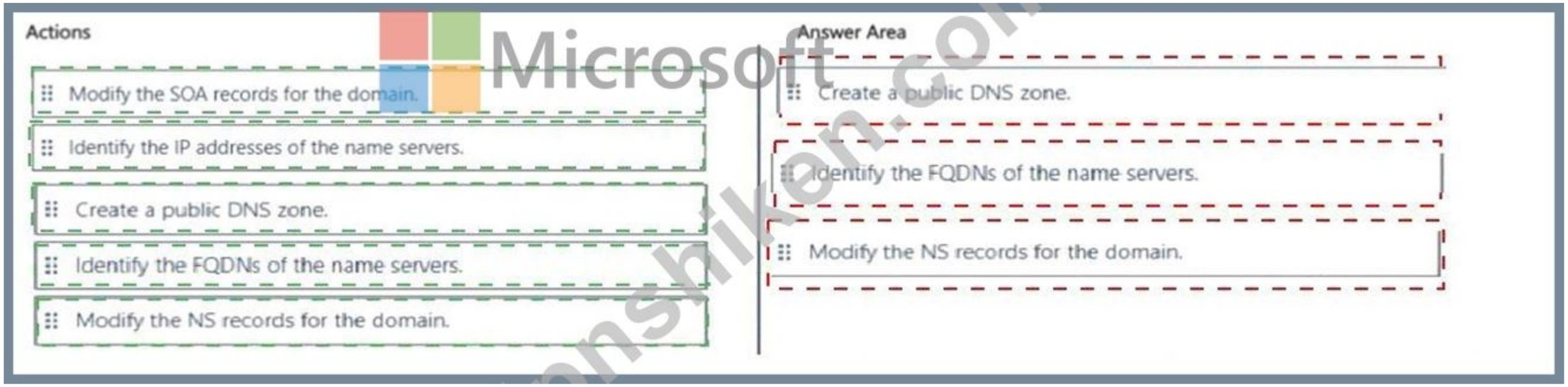


質問: **94**
Azure 仮想ネットワーク内のサブネットの IP アドレス指定を計画しています。
サブネット内の IP アドレスを必要とするリソースの種類はどれですか?
A. 内部ロードバランサー
B. ストレージアカウント
C. サービスエンドポイント
D. サービスエンドポイントポリシー
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

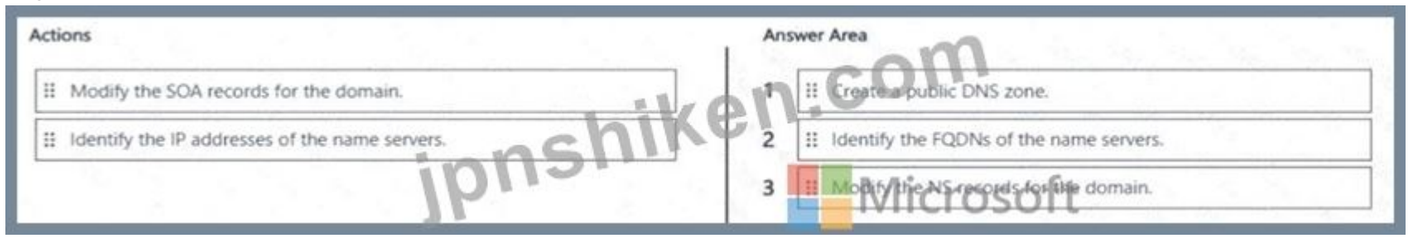
質問: **95**
DNS ドメインをサードパーティのレジストラに登録します。
DNS ゾーンを Azure でホストする必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:

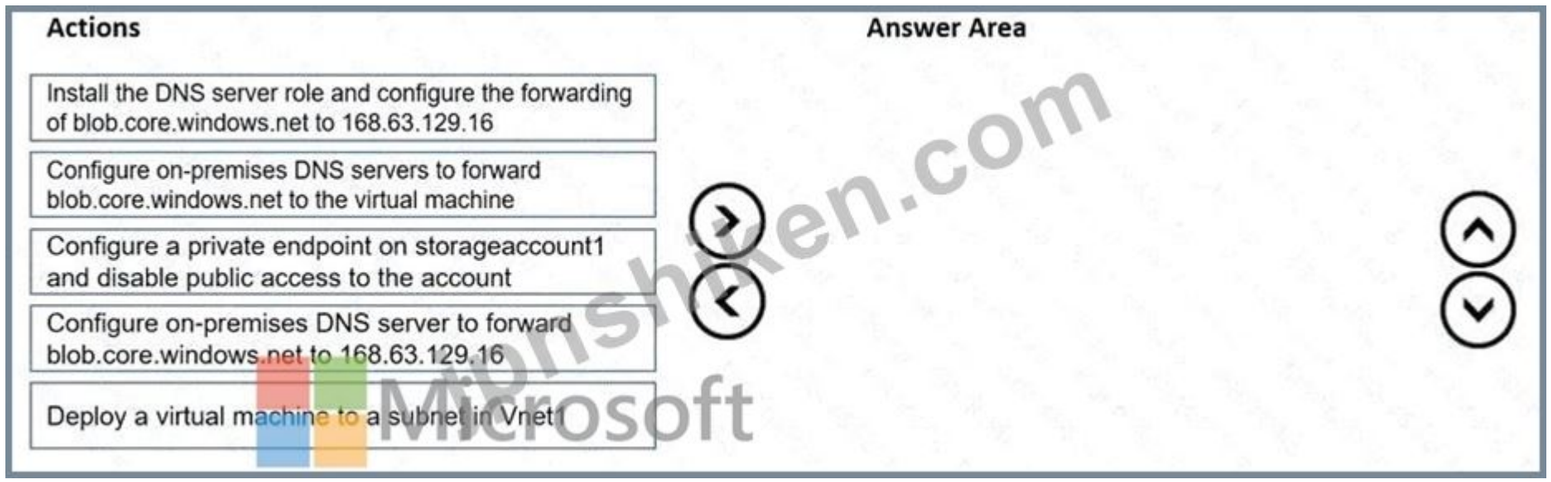


Explanation:

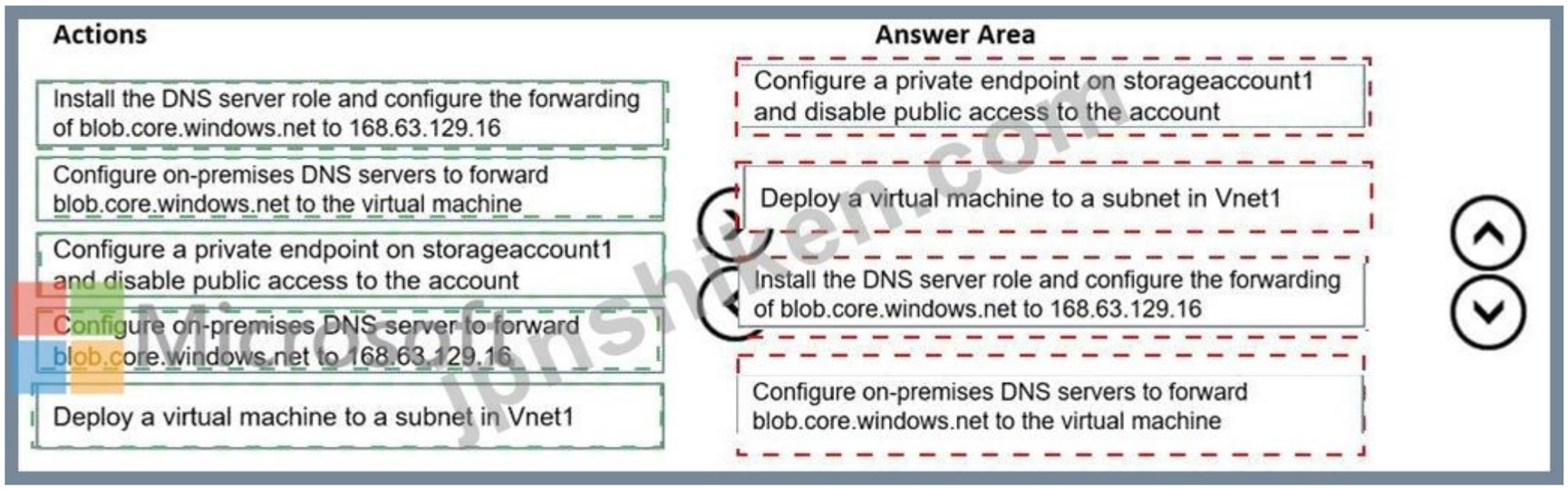


質問: **96**
Vnet2とVnet3を接続する必要があります。ソリューションは、仮想ネットワーク要件とビジネス要件を満たす必要があります。
解決策に含めるべき 2 つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. Vnet2 および Vnet3 からのピアリングで、ゲートウェイ トランジットを許可するを選択します。
B. Vnet1 からのピアリングで、転送されたトラフィックを許可するを選択します。
C. Vnet1 からのピアリングで、[ゲートウェイ トランジットを許可する] を選択します。
D. Vnet2 および Vnet3 からのピアリングで、[リモート ゲートウェイを使用する] を選択します。
E. Vnet1 からのピアリングで、[リモート ゲートウェイを使用する] を選択します。
正解: **(**正解を表示します**)**

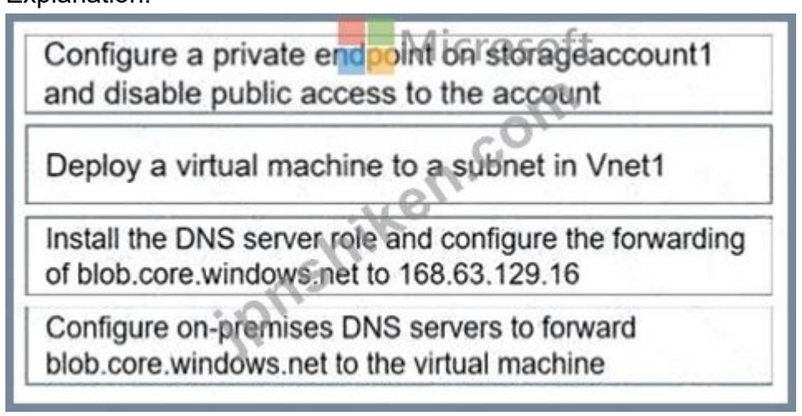
質問: **97**
オンプレミス ネットワークに接続する Vnet1 という名前の Azure 仮想ネットワークがあります。
BLOB ストレージを含む storageaccount1 という名前の Azure ストレージ アカウントがあります。
BLOB ストレージのプライベートエンドポイントを構成する必要があります。ソリューションは以下の要件を満たしている必要があります。
* すべてのオンプレミス ユーザーがプライベート エンドポイントを介して storageaccount1 にアクセスできることを確認します。
* storageaccount1 へのアクセスが中断されないようにします。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



168.63.129.16 is the IP address of Azure DNS which hosts Azure Private DNS zones. It is only accessible from within a VNet which is why we need to forward on-prem DNS requests to the VM running DNS in the VNet. The VM will then forward the request to Azure DNS for the IP of the storage account private endpoint.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

質問: **98**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、定められた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
次のリソースを含むAzureサブスクリプションがあります。
* Vnet1という名前の仮想ネットワーク
* Vnet1のSubnet1という名前のサブネット
* Subnet1に接続するVM1という名前の仮想マシン
* storage1、storage2という名前の3つのストレージアカウント。およびストレージ3
VM1がstorage1にアクセスできることを確認する必要があります。VM1は他のストレージアカウントにアクセスできないようにする必要があります。
解決策 :ネットワークセキュリティグループ (NSG) を作成します。MicrosoftStorageのサービスタグを構成し、そのタグをSubnet1にリンクします。
これは目標を達成していますか？
A. いいえ
B. はい
正解: **(**正解を表示します**)**

質問: **99**
Azure サブスクリプションをお持ちです。
次の表に示すオンプレミス サイトがあります。

Name	Number of users	Connection type to Azure
Site1	500	ExpressRoute
Site2	100	Site-to-Site VPN
Site3	1	Point-to-Site (P2S) VPN

Azure Virtual WAN をデプロイする予定です。
Virtual WAN Basic と Virtual WAN Standard を評価しています。
各サイトで使用できる仮想 WAN の種類はどれですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

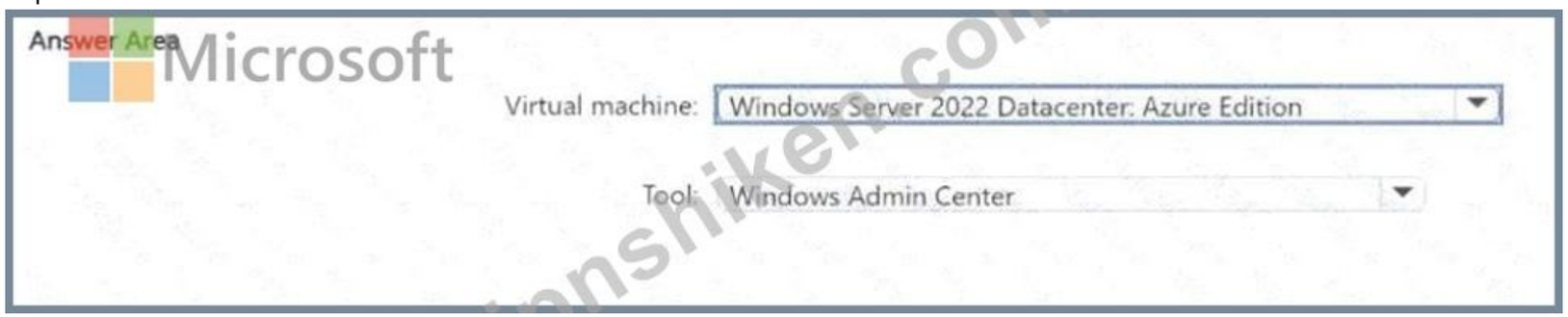
Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

質問: **100**
オンプレミス ネットワークと、VNet1 という名前の Azure 仮想ネットワークがあります。
Azure Extended Network を実装する必要があります。ソリューションはコストを最小限に抑える必要があります。
VNet1 にデプロイする仮想マシンの種類と、Azure 拡張ネットワークを構成するために使用するツールはどれですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:



質問: **101**

タスク10

サブネット 1-2 に複数の仮想マシンを展開する予定です。

サブネット1-2外のすべてのAzureホストがサブネット1-2上のホストのTCPポート5585に接続できないようにする必要があります。このソリューションは、管理作業を最小限に抑える必要があります。

正解:

See the Explanation below for step by step instructions.

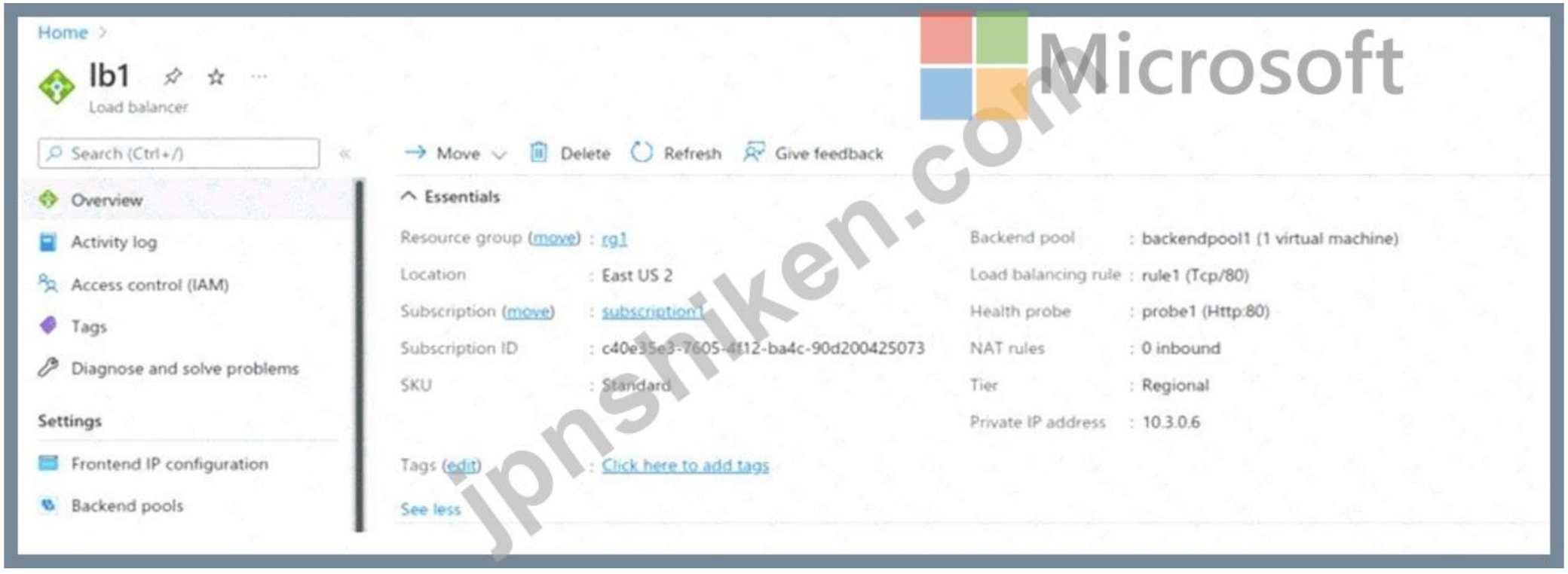
Explanation:

To prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts within subnet1-2, you can use a Network Security Group (NSG). This solution is straightforward and minimizes administrative effort.

Step-by-Step Solution
Step 1: Create a Network Security Group (NSG)
* Navigate to the Azure Portal.
* Search for "Network security groups" and select it.
* Click on "Create".
* Enter the following details:
* Subscription: Select your subscription.
* Resource Group: Select an existing resource group or create a new one.
* Name: Enter a name for the NSG (e.g., NSG-Subnet1-2).
* Region: Select the region where your virtual network is located.
* Click on "Review + create" and then "Create".
Step 2: Create an Inbound Security Rule
* Navigate to the newly created NSG.
* Select "Inbound security rules" from the left-hand menu.
* Click on "Add" to create a new rule.
* Enter the following details:
* Source: Select Service Tag.
* Source Service Tag: Select VirtualNetwork.
* Source port ranges: Leave as *.
* Destination: Select IP Addresses.
* Destination IP addresses/CIDR ranges: Enter the IP range of subnet1-2 (e.g., 10.1.2.0/24).
* Destination port ranges: Enter 5585.
* Protocol: Select TCP.
* Action: Select Deny.
* Priority: Enter a priority value (e.g., 100).
* Name: Enter a name for the rule (e.g., Deny-TCP-5585).
* Click on "Add" to create the rule.
Step 3: Associate the NSG with Subnet1-2
* Navigate to the virtual network that contains subnet1-2.
* Select "Subnets" from the left-hand menu.
* Select subnet1-2 from the list of subnets.
* Click on "Network security group".
* Select the NSG you created (NSG-Subnet1-2).
* Click on "Save".
Explanation:
* Network Security Group (NSG): NSGs are used to filter network traffic to and from Azure resources in an Azure virtual network. They contain security rules that allow or deny inbound and outbound traffic based on source and destination IP addresses, port, and protocol1.
* Inbound Security Rule: By creating a rule that denies traffic on TCP port 5585 from any source outside of subnet1-2, you ensure that only hosts within subnet1-2 can connect to this port.
* Association with Subnet: Associating the NSG with subnet1-2 ensures that the security rules are applied to all resources within this subnet.
By following these steps, you can effectively prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts within subnet1-2, while minimizing administrative effort.

質問: **102**
Subscription1 と Subscription2 という名前の 2 つの Azure サブスクリプションがあります。
2 つのサブスクリプション内の仮想ネットワーク間に接続はありません。
プライベート リンク サービスは、privatelinkservice1 の図に示すように構成します。(privatelinkservice1 タブをクリックします。)

Subscription1 にロード バランサー名を作成し、lb1 の図に示されているバックエンド プールを構成します。
(tie 1b1 タブをクリックします。)



図示の privateendpoint4 のように、Subscription2 にプライベートエンドポイントを作成します。(privateendpoint4 をクリックします)

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

正解:

Explanation:
Yes, Yes, No

質問: **103**
エンドツーエンド暗号化をサポートするには、APPGW1 を設定する必要があります。ソリューションはセキュリティ要件を満たす必要があります。どうすればよいでしょうか？
A. バックエンド設定から、内部ルートCAによって発行された秘密鍵を持つワイルドカードTLS証明書をアップロードします。
B. SSL 設定から、内部ルート CA によって発行され、完全な証明書チェーンが含まれる TLS クライアント証明書をアップロードします。
C. SSL 設定から、内部ルート CA によって発行された TLS クライアント証明書をアップロードします。
D. バックエンド設定から、内部ルート CA 証明書をアップロードします。
正解: (正解を表示します)

質問: **104**

Vnet4 および Vnet5 に接続する仮想マシンの仮想ネットワーク要件を満たすには、何を実装する必要がありますか?

A. プライベートエンドポイント
B. 仮想ネットワークピアリング
C. プライベートリンクサービス
D. ルーティングテーブル
E. サービスエンドポイント

正解: **(**正解を表示します**)**

There is no virtual network peering between VM4's VNet (VNet3) and VM5's VNet (VNet4). To enable the VMs to communicate over the Microsoft backbone network a VNet peering is required between VNet3 and VNet4.

Topic 3, Proseware. Inc

Overview

Existing Environment

Proseware. Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.

Hybrid Environment

Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.

Proseware has an Azure subscription that is linked to proseware.com.

Proseware has an internal certification authority (CA).

Network infrashtructure

The offices contain the resources shown in the following table.

NYCNet connects to Azure by using an ExptessRoute circuit.

SFONet connects to Azure by using a Site to-Site (S2S) VPN.

The Azure subscriotion contains the virtual networks and subnets shown in the followina table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet

The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

The subscription contains an Azure Private DNS zone named DNSZonel in the East US region. DNSZonel hosts a namespace of azure.piosewaie.com and is linked to HubVNet The subscription contains a Standard Azure load balancer named LBS1 in the East US region. LBS1 contains a backend pool that hosts VM1 and VM2.

Planned Changes

Proseware plans to implement the following changes:

* Deploy an Azure Private DNS Resolver named PRDNSl to HubVNet and link PRDNS1 to SpokeVNet.
* Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNSl
* Deploy Azure Virtual Network Manager and implement the following rules:

o Allow inbound connections on TCP port 3389 from the on-premises networks to SU8NET-JUMPHOSTS. o Block inbound connections on TCP poit 80 from the internet to SpokeVNet.

* Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
* Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
* Deploy a gateway load balancer named L8GW1 to HubVNet.
* Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
* Ensure that all the traffic to App2 is processed by using FD1.

Connectivity Requirements

Proseware identifies the following connectivity requirements:

* Minimize the complexity of the Azure Virtual Network Manager deployment.
* Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN
* Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to-Site (P2S) VP and their proseware.com credentials.

Security Requirements

Proseware identifies the following general requirements:

* Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
* From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.

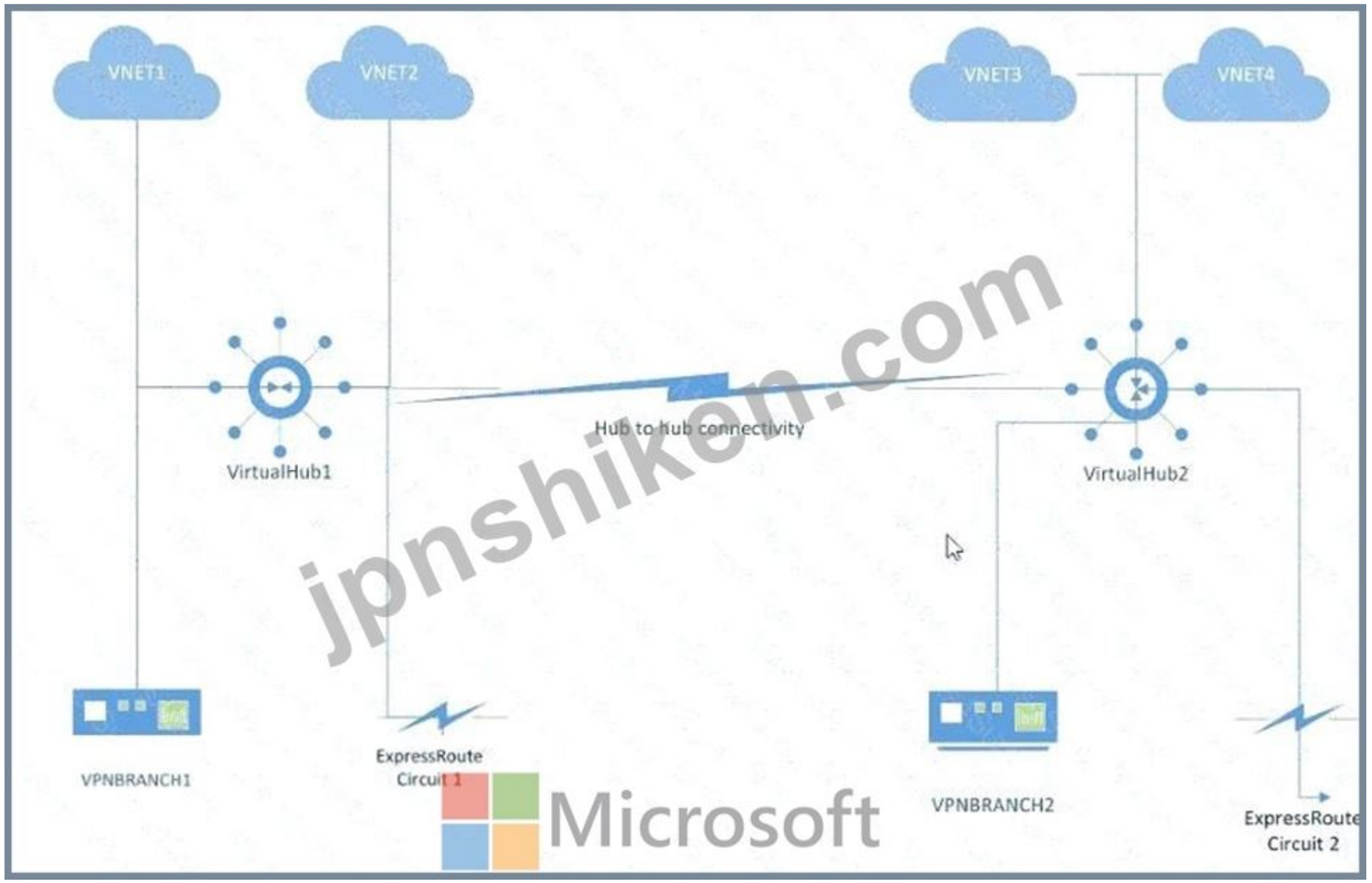
proseware.com namespace by using PRDNS1.

* Whenever possible, minimize administrative effort.

質問: 105

Azure サブスクリプションをお持ちです。

次の図に示すように、Azure Virtual WAN を実装する予定です。



作成する必要があるルート テーブルの最小数はいくつですか?

A. 4

B. 6

C. 2

D. 1

正解: **(**正解を表示します**)**

質問: **106**

次の表に示すAzureTrafficManagerプロファイルがあります。

Name	Routing method
Profile1	Performance
Profile2	Multivalue

次の表に示すエンドポイントを追加する予定です。

Name	Type	Additional settings
Endpoint1	Azure endpoint	Target resource type: App Service
Endpoint2	External endpoint	FQDN or IP: www.contoso.com
Endpoint3	External endpoint	FQDN or IP: 131.107.10.15
Endpoint4	Nested endpoint	Target resource: Profile1

Profile2に追加できるエンドポイントはどれですか？

A. Endpoint1およびEndpoint4のみ

B. Endpoint1、Endpoint2、Endpoint3、およびEndpoint4

C. Endpoint1のみ

D. Endpoint3のみ

E. Endpoint2およびEndpoint3のみ

正解: **(**正解を表示します**)**

質問: **107**

オンプレミス ネットワークがあります。

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
Vnet1	Virtual network	*None*
VM1	Virtual machine	Connected to Vnet1
VM2	Virtual machine	Connected to Vnet1
SQL1	Azure SQL Database	Internet accessible

サブスクリプション内のリソースにアクセスするには、ExpressRoute 回線を実装する必要があります。ソリューションでは、オンプレミス ネットワークが ExpressRoute 回線を使用して Azure リソースに接続できるようにする必要があります。

各接続にはどのタイプのピアリングを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

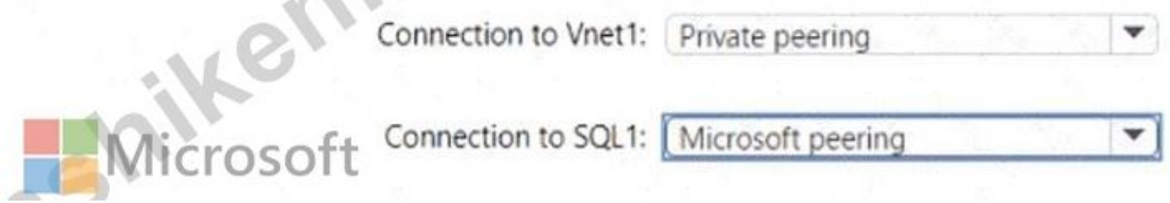
Answer Area

正解:

Answer Area

Explanation:

Answer Area



質問: 108

次の表に示す Web アプリをホストする 2 つの Azure App Service インスタンスがあります。

Name	Web app URLs
As1.contoso.com	https://app1.contoso.com/ https://app2.contoso.com/
As2.contoso.com	https://app3.contoso.com/ https://app4.contoso.com/

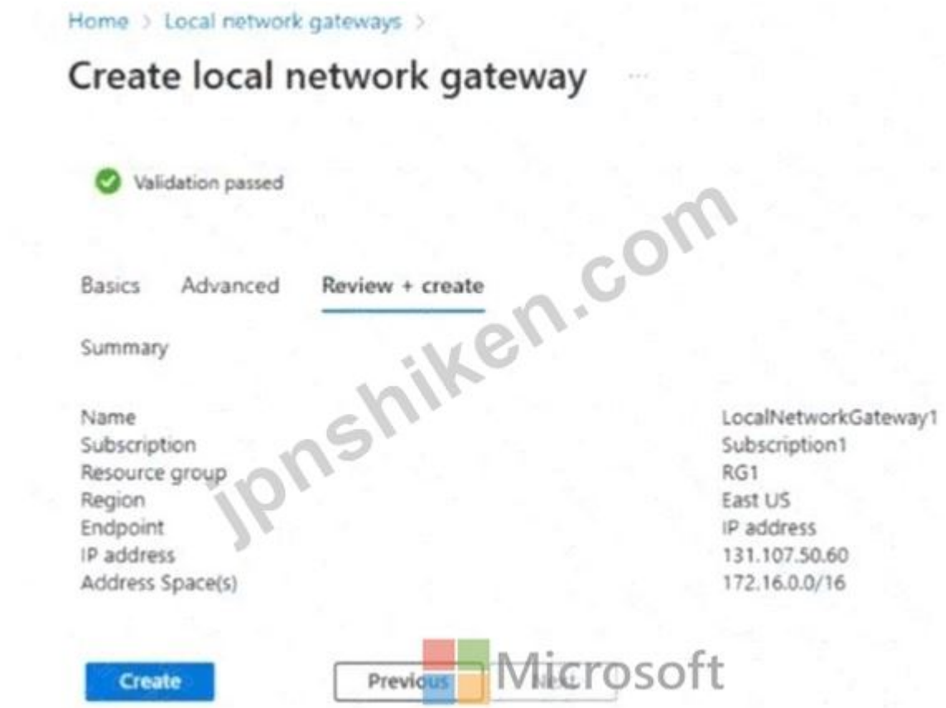
1 つのパブリック フロントエンド IP アドレスと 2 つのバックエンド プールを持つ Azure アプリケーション ゲートウェイをデプロイします。
すべてのWebアプリをアプリケーションゲートウェイに公開する必要があります。リクエストはHTTPホストヘッダーに基づいてルーティングする必要があります。
設定する必要があるリスナーとルーティング ルールの最小数はいくつですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:
1, 2

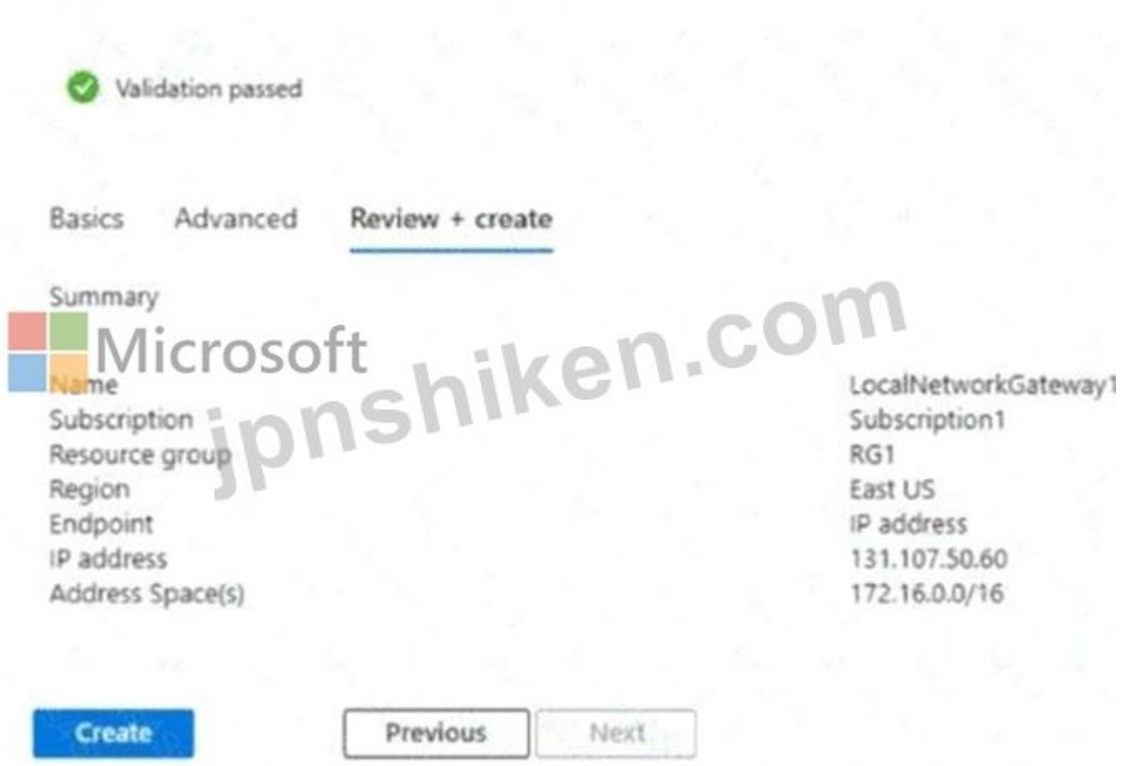
質問: **109**
次の表に示すサイトを含むオンプレミス ネットワークがあります。

Site	Site Address space	Firewall private IP	Firewall public IP address
Paris	172.16.0.0/24	172.16.0.1	131.107.50.60
Amsterdam	172.16.1.0/24	172.16.1.1	131.107.70.80
Berlin	172.16.2.0/24	172.16.2.1	131.107.90.100

各サイトはファイアウォールを介してインターネットに接続されています。すべてのサイトはSD-WANに接続されています。各サイトはBGPを使用してルートを伝播するように構成されています。
Gateway 1 という名前の仮想ネットワーク ゲートウェイが含まれる Vnet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。
ゲートウェイの図に示されている構成を使用して、ローカル ネットワーク ゲートウェイを作成します ([ゲートウェイ] タブをクリックします)。

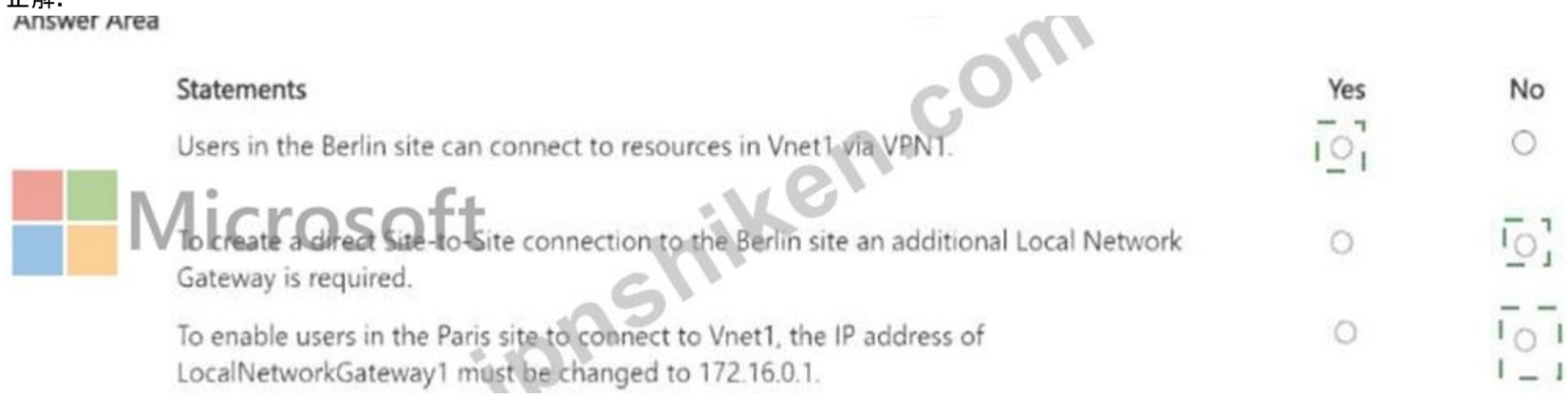


接続図に示す構成で、サイト間（S2S）接続を作成します。（接続」タブをクリックします）



次の各文について、正しい場合は「はい」を選択し、そうでない場合は「いいえ」を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:



Explanation:

質問: **110**
タスク2
Azure仮想マシンをフランス中部Azureリージョンにデプロイできることを確認する必要があります。ソリューションでは、フランス中部リージョンの仮想マシンが、IPアドレス範囲が10.5.1.0/24のネットワークセグメントに配置されていることを確認する必要があります。
正解:
See the Explanation below for step by step instructions.
Explanation:
To deploy Azure virtual machines to the France Central region and ensure they are in a network segment with an IP address range of 10.5.1.0/24, follow these steps:
Step-by-Step Solution

Step 1: Create a Virtual Network in France Central
* Navigate to the Azure Portal.
* Search for "Virtual networks" in the search bar and select it.
* Click on "Create".
* Enter the following details:
* Subscription: Select your subscription.
* Resource Group: Select an existing resource group or create a new one.
* Name: Enter a name for the virtual network (e.g., VNet-FranceCentral).
* Region: Select France Central.
* Click on "Next: IP Addresses".
Step 2: Configure the Address Space and Subnet
* In the IP Addresses tab, enter the address space as 10.5.1.0/24.
* Click on "Add subnet".
* Enter the following details:
* Subnet name: Enter a name for the subnet (e.g., Subnet-1).
* Subnet address range: Enter 10.5.1.0/24.
* Click on "Add".
* Click on "Review + create" and then "Create".
Step 3: Deploy Virtual Machines to the Virtual Network
* Navigate to the Azure Portal.
* Search for "Virtual machines" in the search bar and select it.
* Click on "Create" and then "Azure virtual machine".
* Enter the following details:
* Subscription: Select your subscription.
* Resource Group: Select the same resource group used for the virtual network.
* Virtual machine name: Enter a name for the VM.
* Region: Select France Central.
* Image: Select the desired OS image.
* Size: Select the appropriate VM size.
* Click on "Next: Disks", configure the disks as needed, and then click on "Next: Networking".
* In the Networking tab, select the virtual network (VNet-FranceCentral) and subnet (Subnet-1) created earlier.
* Complete the remaining configuration steps and click on "Review + create" and then "Create".
Explanation:
* Virtual Network: A virtual network in Azure allows you to create a logically isolated network that can host your Azure resources.
* Address Space: The address space 10.5.1.0/24 ensures that the VMs are in a specific network segment.
* Subnet: Subnets allow you to segment the virtual network into smaller, manageable sections.
* Region: Deploying the virtual network and VMs in the France Central region ensures that the resources are physically located in that region.
By following these steps, you can ensure that your Azure virtual machines in the France Central region are deployed within the specified IP address range of 10.5.1.0/24.

質問: 111
Azure Front Door に Azure Web アプリケーション ファイアウォール (WAF) のインスタンスがあります。

単一の IP アドレスからの高レートのリクエストをブロックする WAF ルールを作成する予定です。
ルールの最適なしきい値を特定するには、Log Analytics にクエリを実行する必要があります。
Log Analytics でクエリを実行する必要があるテーブルはどれですか?
A. AGWファイアウォールログ
B. セキュリティ検出
C. AzureDiagnostics
D. AZFWThreatInte1
正解: **C** (コメントを発表する)

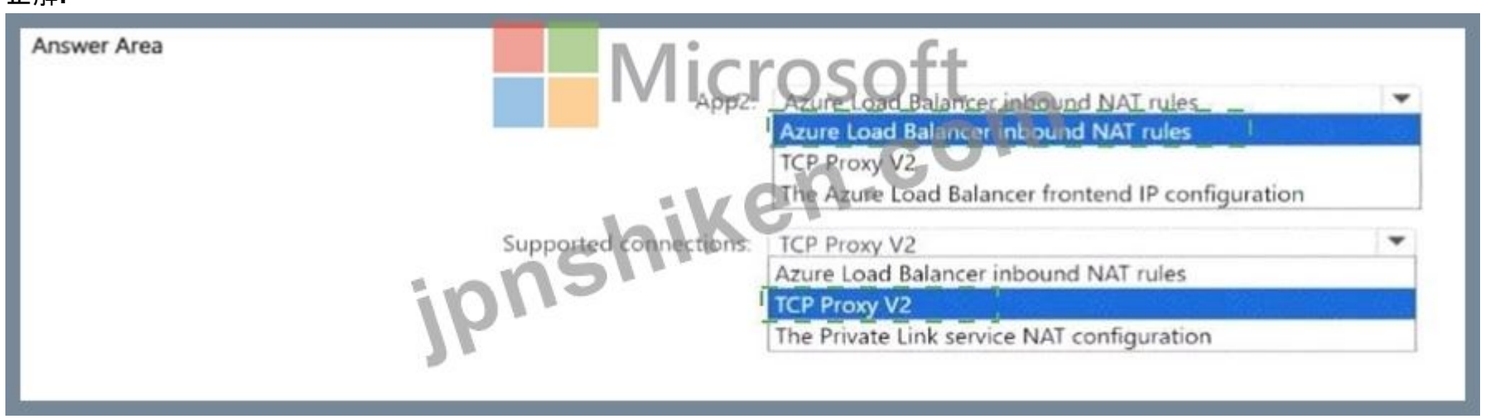
質問: **112**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Description
VNet1	Virtual network that contains a subnet named Subnet1
Endpoint1	Private endpoint that is connected to Subnet1 and linked to an Azure App Service web app named App1
storage1	Storage account that can only be accessed via Endpoint1
NSG1	Network security group (NSG) that is linked to Subnet1

NSG1 を使用して storage1 へのアクセスを制御する必要があります。最初に何を構成する必要がありますか?
A. サービスエンドポイント
B. Azure Private Link サービス
C. プライベートエンドポイントネットワークポリシー
D. アプリケーションセキュリティグループ
正解: (正解を表示します)

質問: **113**
Azureサブスクリプションをお持ちです。このサブスクリプションには、App1とApp2という2つのアプリをホストする2つの仮想マシンスケールセット、PLS1というAzure Private Linkサービス、そしてLB1というAzureロードバランサーが含まれています。
PLS1 は LB1 を使用し、TCP Proxy V2 は無効になっています。PLS1 は App1 へのアクセスのみを提供します。
次のアクションを実行する必要があります。
* App1 と App2 へのアクセスを提供します。
* サポートされるプライベート エンドポイント接続の数を増やします。
App2 へのアクセスを提供するには何を変更する必要がありますか。また、サポートされる接続の数を増やすには何を変更する必要がありますか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:



Explanation:

質問: **114**

FWPolicy1 という Azure Firewall ポリシーを含む Azure サブスクリプションがあります。以下の要件を満たすように FWPolicy1 を構成する必要があります。

* 宛先の FQDN に基づいてトラフィックを許可します。
* ソースに基づいて TCP トラフィックを許可します。

各要件にはどのようなタイプのルールを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

正解:

Answer Area

Explanation:

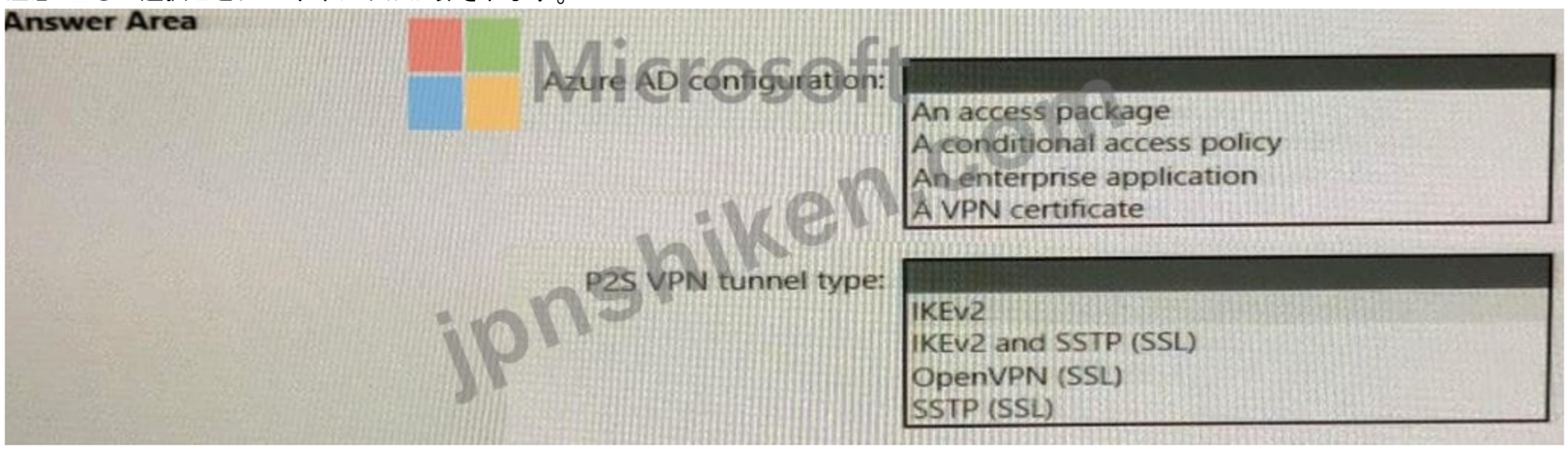
質問: **115**

単一の仮想ネットワークと仮想ネットワーク ゲートウェイを含む Azure サブスクリプションがあります。

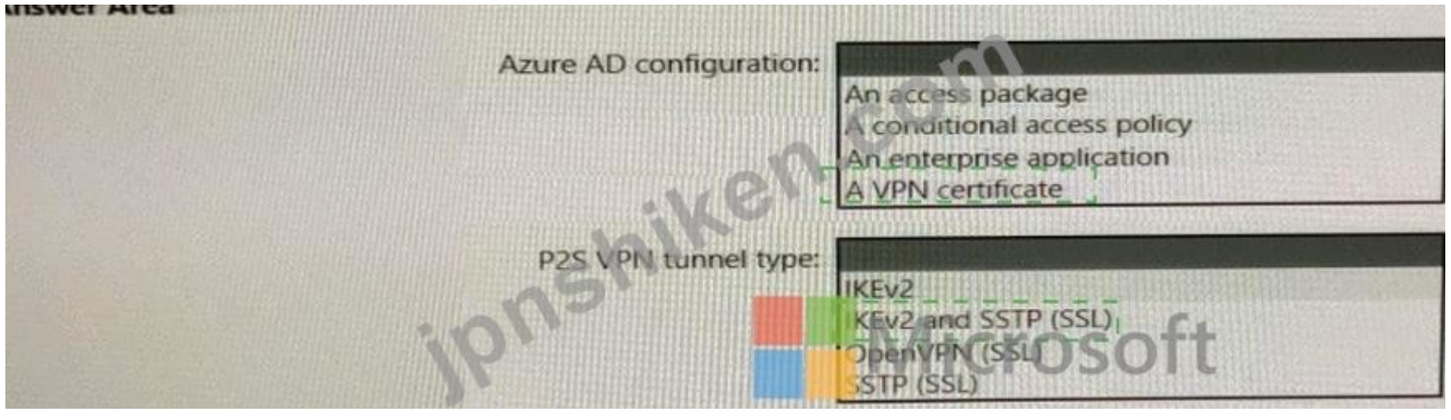
管理者がポイント対サイト (P2S) VPN 接続を使用して仮想ネットワーク内のリソースにアクセスできるようにする必要があります。接続は Azure Active Directory (Azure AD) によって認証される必要があります。

何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



質問: **116**

会社はアムステルダムとロンドンにオフィスを構えています。Azureサブスクリプションを保有しており、両オフィスともサイト間VPN接続を使用してAzureに接続しています。

アムステルダムのオフィスは北ヨーロッパのAzureリージョンのリソースを使用しています。ニューヨークのオフィスは米国東部のAzureリージョンのリソースを使用しています。

各オフィスを最寄りのAzureリージョンに接続するには、ExpressRoute回線を実装する必要があります。ExpressRoute回線が接続されると、アムステルダムオフィスのオンプレミスコンピューターは、ExpressRoute回線を使用してニューヨークオフィスのオンプレミスサーバーに接続できるようになります。
どの ExpressRoute オプションを使用すればよいですか?
A. ExpressRoute ローカル
B. ExpressRoute ファストパス
C. エクスプレスルートダイレクト
D. ExpressRoute グローバルリーチ
正解**: D (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

質問**: 117**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Vnet1とVnet2という名前の2つのAzure仮想ネットワークがあります。
ポイントツーサイト（P2S）IKEv2VPNを使用してVnet1に接続するClient1という名前のWindows10デバイスがあります。
Vnet1とVnet2の間に仮想ネットワークピアリングを実装します。Vnet1はゲートウェイトランジットを許可します。Vnet2はリモートゲートウェイを使用できます。
Client1がVnet2と通信できないことがわかりました。
Client1がVnet2と通信できることを確認する必要があります。
解決策 :VPNクライアント構成をダウンロードして再インストールします。
これは目標を達成していますか？
A. はい
B. いいえ
正解**: (**正解を表示します**)**
The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

質問**: 118**
次の表に示す Azure サブスクリプションがあります。

Name	Microsoft Entra ID tenant	Contains resources in Azure region	Virtual network
Sub1	contoso.com	East US, West US	VNet1, VNet2
Sub2	contoso.com	Europe North, Europe West	VNet3, VNet4
Sub3	fabrikam.com	Europe North, West US	VNet5, VNet6

各仮想ネットワークには、パブリック IP アドレスが割り当てられたインターネット アクセス可能なリソースが 20 個含まれています。
リソースを保護するには、Azure DDoS ネットワーク保護を実装する必要があります。ソリューションではコストを最小限に抑える必要があります。
導入する必要がある DDoS ネットワーク保護プランの最小数はいくつですか?
A. 1

B. 2
C. 6
D. 3
正解: (正解を表示します)

質問: **119**
Vnet1 という名前の Azure 仮想ネットワークがあり、そこには Subnet1 と Subnet2 という名前の 2 つのサブネットが含まれています。
NATgateway1 の図に示されている NAT ゲートウェイがあります。

VM1 の図に示すような仮想マシンがあります。

Subnet1 は、Subnet1 の図に示すように構成されています。

Subnet1

Vnet1

Name

Subnet1

Subnet address range * ⓘ

10.100.1.0/24

10.100.1.0 – 10.100.1.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space ⓘ

NAT gateway ⓘ

NATgateway1

Network security group

None

Route table

RouteTable1

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services ⓘ

Microsoft.Storage

Service	Status
Microsoft.Storage	Succeeded

Service endpoint policies

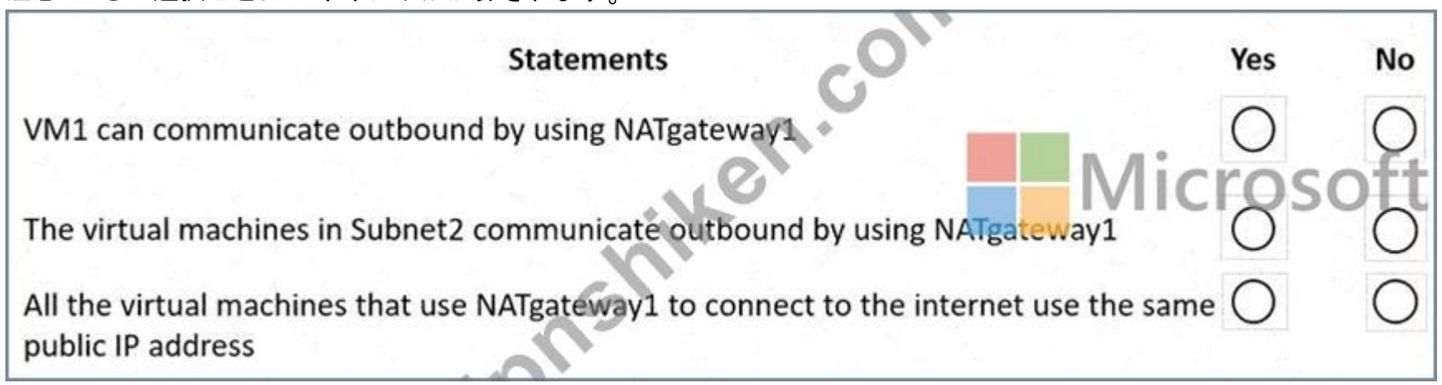
0 selected

SUBNET DELEGATION

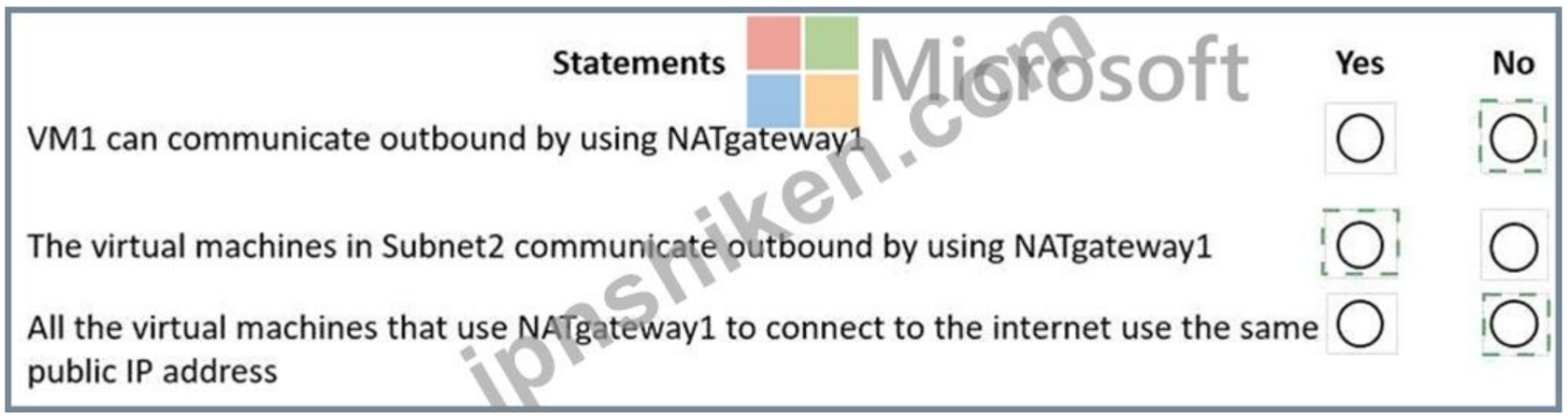
Delegate subnets to a service ⓘ

None

以下の各文について、該当する場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Box 1: No
VM1 is in Zone2 whereas the NAT Gateway is in Zone1. The VM would need to be in the same zone as the NAT Gateway to be able to use it. Therefore, VM1 cannot use the NAT gateway.
Box 2: Yes
NATgateway1 is configured in the settings for Subnet2.
Box 3: No
The NAT gateway does not have a single public IP address, it has an IP prefix which means more than one IP address. The VMs the use the NAT Gateway can use different public IP addresses contained within the IP prefix.
Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

質問: **120**
Vnet2とVnet3にデフォルトルートを設定する必要があります。ソリューションは仮想ネットワークの要件を満たしている必要があります。
デフォルトルートを構成するには何を使用すればよいですか?
A. ルートフィルター
B. BGPルート交換
C. Vnet1 の GatewaySubnet に割り当てられたユーザー定義ルート
D. Vnet2 および Vnet3 の GatewaySubnet に割り当てられたユーザー定義ルート
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

質問: **121**
会社の本社とAzure仮想ネットワークの間にサイト間VPN接続を確立できません。
IPsecトンネルを確立できない原因をトラブルシューティングする必要があります。
どの診断ログを確認する必要がありますか？
A. IKEDiagnosticLog
B. GatewayDiagnosticLog
C. TunnelDiagnosticLog
D. RouteDiagnosticLog
正解: **A (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics IKEDiagnosticLog = The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.
GatewayDiagnosticLog = Configuration changes are audited in the GatewayDiagnosticLog table.
TunnelDiagnosticLog = The TunnelDiagnosticLog table is very useful to inspect the historical connectivity statuses of the tunnel.
RouteDiagnosticLog = The RouteDiagnosticLog table traces the activity for statically modified routes or routes received via BGP.
P2SDiagnosticLog = The last available table for VPN diagnostics is P2SDiagnosticLog. This table traces the activity for Point to Site.
https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

質問: **122**
Azure仮想ネットワークに2つのネットワーク仮想アプライアンス（NVA）を構成します。これらのNVAは、仮想ネットワーク内のすべてのトラフィックを検査するために使用されます。
NVAに高可用性を提供する必要があります。ソリューションは管理作業を最小限に抑える必要があります。ソリューションにはどのようなトラフィックを含める予定ですか？

A. Azure 標準ロードバランサー
B. Azure トラフィック マネージャー
C. Azure アプリケーション ゲートウェイ
D. 青い玄関
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli

質問: **123**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Location	Description
VNet1	Virtual network	East US	Contains a subnet named Subnet1
storage1	Storage account	East US	Uses read-access geo-redundant storage (RA-GRS) redundancy
sql1	Azure SQL server	East US	Hosts a database named SQLDB1

サービスエンドポイントを使用して、storage1 と sql1 へのアクセスを制限する必要があります。ソリューションは以下の要件を満たす必要があります。
* Subnet1からSQIDB1へのアクセスを許可する
* サポートされているリソースへのアクセスを制限するために、サービス エンドポイント ポリシーを実装します。
* Subnet1 から、ペアになっている Azure リージョン内の storage1 および storage1 の読み取り専用レプリカへのアクセスを許可します。
作成する必要があるサービス エンドポイントとサービス エンドポイント ポリシーの最小数はいくつですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

質問: 124

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
VNet1	Virtual network	Has an IP address space of 192.168.0.0/23
VNet2	Virtual network	Has an IP address space of 192.168.2.0/23
VNet3	Virtual network	Has an IP address space of 10.0.0.0/20
Peering12	Virtual network peering	Peered between VNet1 and VNet2
Peering21	Virtual network peering	Peered between VNet2 and VNet1

各仮想ネットワークには、20 台の仮想マシンと、IP アドレス空間が /24 のサブネットが含まれます。

Azure Bastion を使用して、インターネットから仮想マシンにアクセスできることを確認する必要があります。

展開する必要がある要塞サブネットの最小数と、各要塞サブネットでサポートされる最小の IP アドレス空間はどれくらいですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

質問: **125**

注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。

Vnet1とVnet2という名前の2つのAzure仮想ネットワークがあります。

ポイントツーサイト（P2S）IKEv2VPNを使用してVnet1に接続するClient1という名前のWindows10デバイスがあります。

Vnet1とVnet2の間に仮想ネットワークピアリングを実装します。Vnet1はゲートウェイトランジットを許可します。Vnet2はリモートゲートウェイを使用できます。

Client1がVnet2と通信できないことがわかりました。

Client1がVnet2と通信できることを確認する必要があります。

解決策 :Vnet1のゲートウェイでBGPを有効にします。

これは目標を達成していますか？

A. はい

B. いいえ

正解: **(**正解を表示します**)**

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

質問: **126**

VM1 という名前の Azure 仮想マシンがあります。

Azure Network Watcher を使用して、VM1 のすべてのネットワーク トラフィックをキャプチャする必要があります。

キャプチャはどの場所に書き込むことができますか?

A. BLOB ストレージのみ

B. VM1 のみのファイルパス

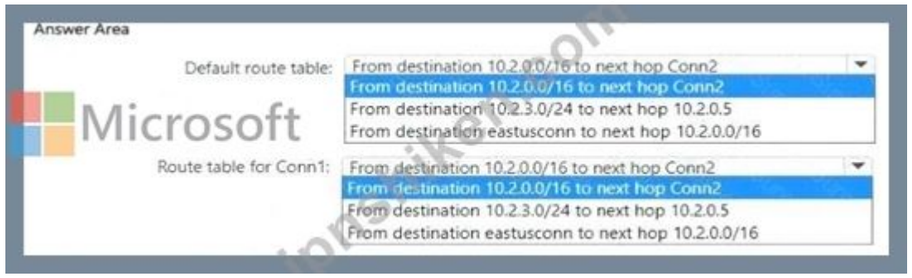
C. プレミアムストレージアカウントのみ

D. BLOB ストレージとプレミアム ストレージ アカウントのみ
E. VM1 のみの BLOB ストレージとファイル パス
F. BLOB ストレージ、VM1 上のファイル パス、およびプレミアム ストレージ アカウント
正解: (正解を表示します)

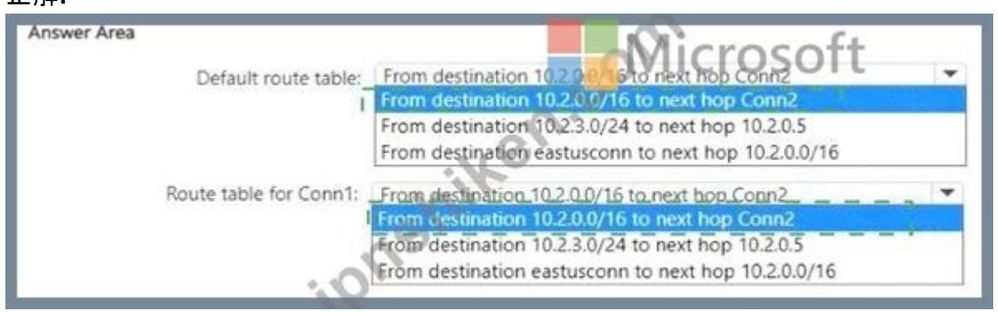
質問: **127**
Hub1 という名前のハブを含む、VWAN1 という名前の Azure Virtual WAN を実装する予定です。
VWAN1 には、次の表に示す仮想ネットワークが含まれます。

Name	IP address space	Description
VNet1	10.1.0.0/24	Connected directly to Hub1 by using a connection named Conn1
VNet2	10.2.0.0/24	Connected directly to Hub1 by using a connection named Conn2 and hosting a Network Virtual Appliance (NVA) named NVA2 that has an IP address of 10.2.0.5
VNet3	10.2.3.0/24	Connected to VNet2 by using a virtual network peering named Peering1

VNet1 に接続されたホストが VNet3 に接続されたホストと通信できることを確認する必要があります。
VWAN1 のルーティング テーブルをどのように設定すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

質問: **128**
1つのサブネットを持つVnet1という名前のAzure仮想ネットワークがあります。Vnet1は西ヨーロッパのAzureリージョンにあります。
App1という名前のAzureAppServiceアプリを西ヨーロッパリージョンにデプロイします。
App1にVnet1のリソースへのアクセスを提供する必要があります。ソリューションはコストを最小限に抑える必要があります。
あなたは最初に何をすべきですか？
A. プライベートリンクを作成します。
B. 新しいサブネットを作成します。
C. NATゲートウェイを作成します。
D. ゲートウェイサブネットを作成し、仮想ネットワークゲートウェイを展開します。
正解: **D** (コメントを発表する)
Virtual network integration depends on a dedicated subnet.
https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration For outgoing traffic from Web App to vnet, it will go through Internet, so the cost not the minimum.
The connection between the Private Endpoint and the Web App uses a secure Private Link. Private Endpoint is only used for incoming flows to your Web App. Outgoing flows will not use this Private Endpoint, but you can inject outgoing flows to your network in a different subnet through the VNet integration feature.
https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint#conceptual-overview

質問: **129**
次の表に示す仮想ネットワークを含むAzureサブスクリプションがあります。

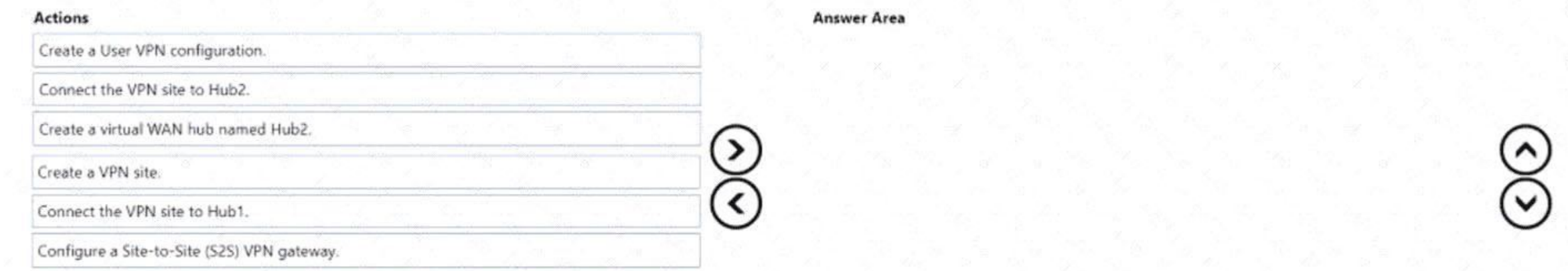
Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

米国西部のAzureリージョンで、AF1という名前のAzureファイアウォールをRG1に展開することを計画しています。
AF1を展開できる仮想ネットワークはどれですか？
A. Vnet1のみ
B. Vnet1、Vnet2、およびVnet4のみ
C. Vnet1およびVnet4のみ
D. Vnet1、Vnet2。Vnet3、およびVnet4
E. Vnet1およびVnet2のみ
正解: (正解を表示します)

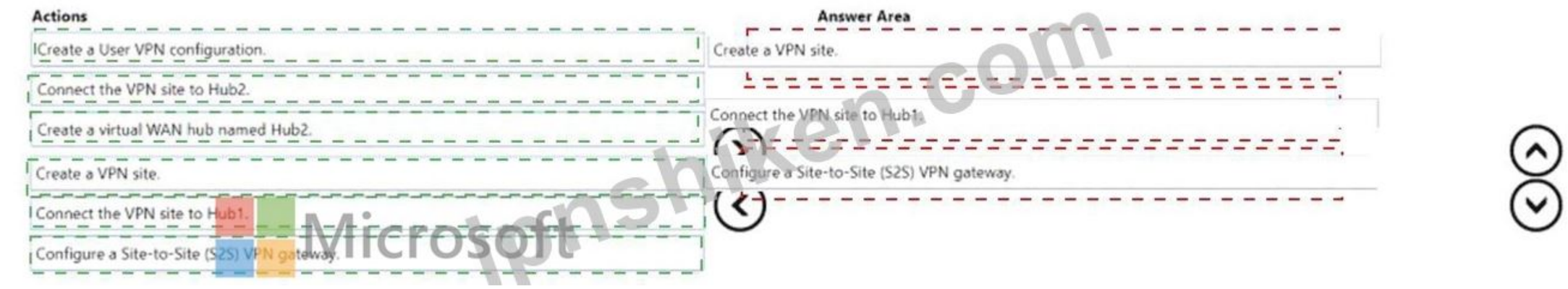
質問: **130**
Azure 仮想ネットワークとオンプレミスのデータセンターがあります。
データセンターと仮想ネットワークの間にサイト間 VPN 接続を実装する必要があります。
どの2つのリソースを作成する必要がありますか？ 正解はそれぞれソリューションの一部を示しています。注：正解を選択するごとに1ポイント獲得できます。
A. ローカルネットワークゲートウェイ

B. 仮想ネットワークゲートウェイ
C. ユーザー定義のルート
D. Azure アプリケーション ゲートウェイ
E. オンプレミスのデータゲートウェイ
F. Azure Web アプリケーション ファイアウォール (WAF)
G. Azure ファイアウォール
正解: **A,B (**コメントを発表する**)**

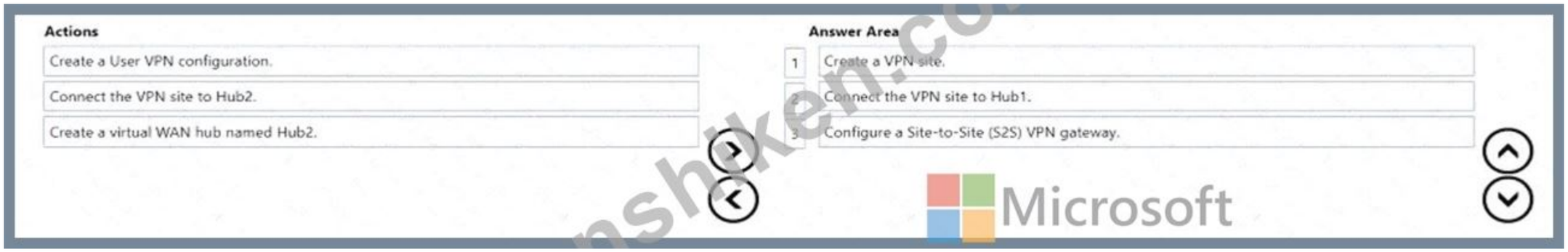
質問: **131**
オンプレミス ネットワークがあります。
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 は、Hub1 という名前の Azure Virtual WAN ハブに接続されています。
Hub1 を使用して、オンプレミス ネットワークと VNet1 間の接続を有効にする必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



質問: **132**

次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Location	Description
VNet1	Virtual network	East US	Contains a subnet named Subnet1
storage1	Storage account	East US	Has read-access geo-replicated storage (RA-GRS) redundancy to the paired region
storage2	Storage account	East US	Has read-access geo-replicated storage (RA-GRS) redundancy to the paired region
VM1	Virtual machine	East US	Connected to Subnet1

次の設定を持つサービス エンドポイント ポリシーを作成します。

* 関連サブネット: サブネット 1
* サービス: Microsoft.Storage
* 範囲: 単一アカウント
* リソース: ストレージ1

VM1 はどのリソースにアクセスできますか?

A. 米国東部 Azure リージョンの storage1 と、ペアになっているリージョンのレプリカ
B. 米国東部 Azure リージョンの storage1 と storage2 およびペアのリージョンのレプリカ
C. 米国東部 Azure リージョンの storage1 と storage2 のみ
D. 米国東部 Azure リージョンの storage1 のみ

正解: **(**正解を表示します**)**

質問: **133**

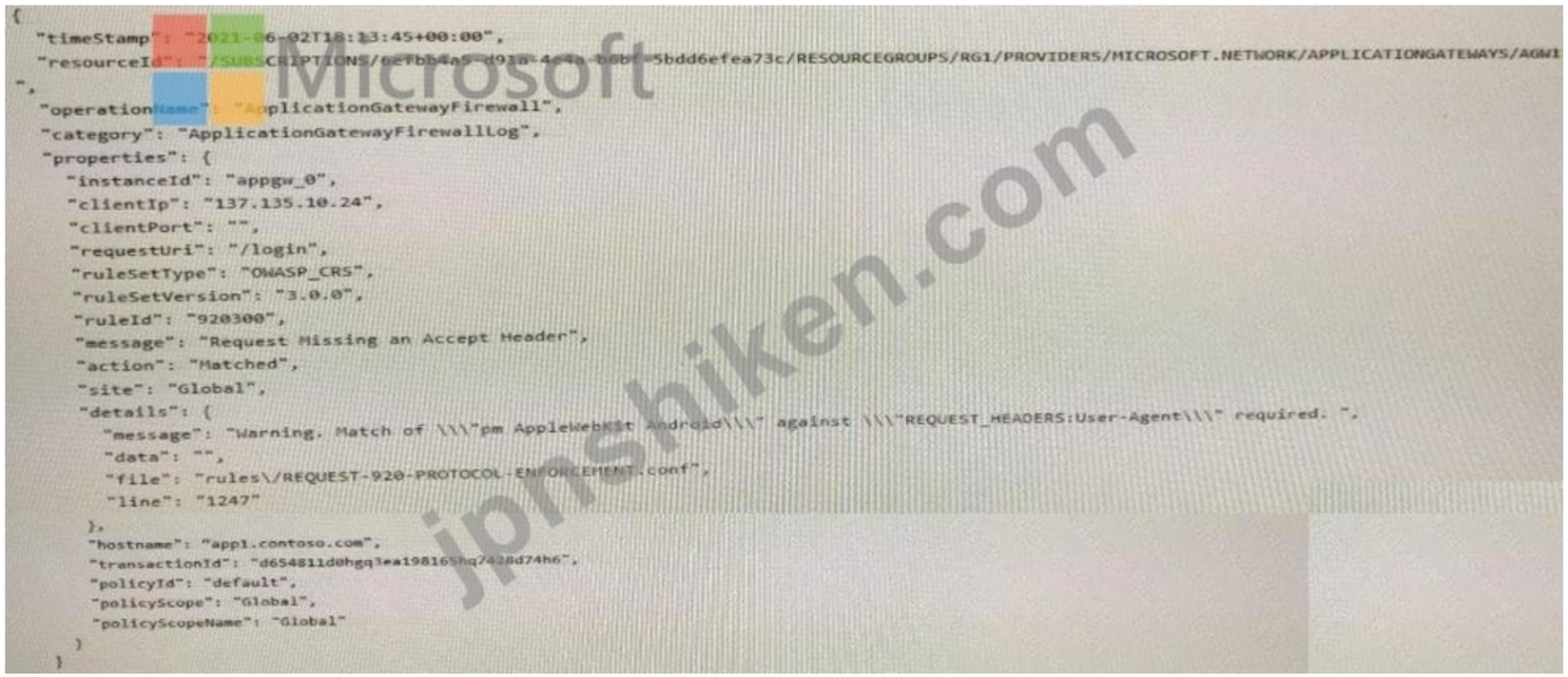
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。

Azure Web Application Firewall（WAF）が有効になっているAzureアプリケーションゲートウェイがあります。

トラフィックをアプリケーションゲートウェイのURLに転送するようにアプリケーションゲートウェイを構成します。

URLにアクセスしようとすると、HTTP403エラーが発生します。診断ログを表示して、次のエラーを発見します。



URLがアプリケーションゲートウェイを介してアクセス可能であることを確認する必要があります。
解決策 :ルールドが920300のWAFルールを無効にします。
これは目標を達成していますか？

A. いいえ
B. はい
正解: **(**正解を表示します**)**

質問: **134**
Vnet1 という Azure 仮想ネットワークがあり、FW1 という Azure ファイアウォールと 150 台の仮想マシンをホストしています。Vnet1 は contoso.com というプライベート DNS ゾーンにリンクされています。すべての仮想マシンの名前は contoso.com ゾーンに登録されています。
Vnet1 は、ExpressRoute を使用してオンプレミスのデータセンターに接続します。
オンプレミスの DNS サーバーが contoso.com ゾーン内の名前を解決できることを確認する必要があります。
実行すべき 2 つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. オンプレミスの DNS サーバーで、FW1 のフロントエンド IP アドレスを指すフォワーダーを構成します。
B. オンプレミスのDNSサーバーで、Azureが提供するDNSサービスを指すフォワーダーを構成します。
168.63.129.16.
C. Vnet1 の DNS サーバー設定を変更します。
D. FW1 の場合、DNS プロキシを有効にします。
E. FW1 の場合、カスタム DNS サーバーを構成します。
正解: **A,D (**コメントを発表する**)**
Reference:

https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns- forwarder
https://azure.microsoft.com/en-gb/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/

質問: **135**
次の表に示すリソースがあります。

Name	Type	Description
Group1	Microsoft Entra group	*None*
Group2	Microsoft Entra group	*None*
VPNGW1	Azure VPN Gateway	Supports Point-to-Site (P2S) VPN connections
VPNGW2	Azure VPN Gateway	Supports Point-to-Site (P2S) VPN connections

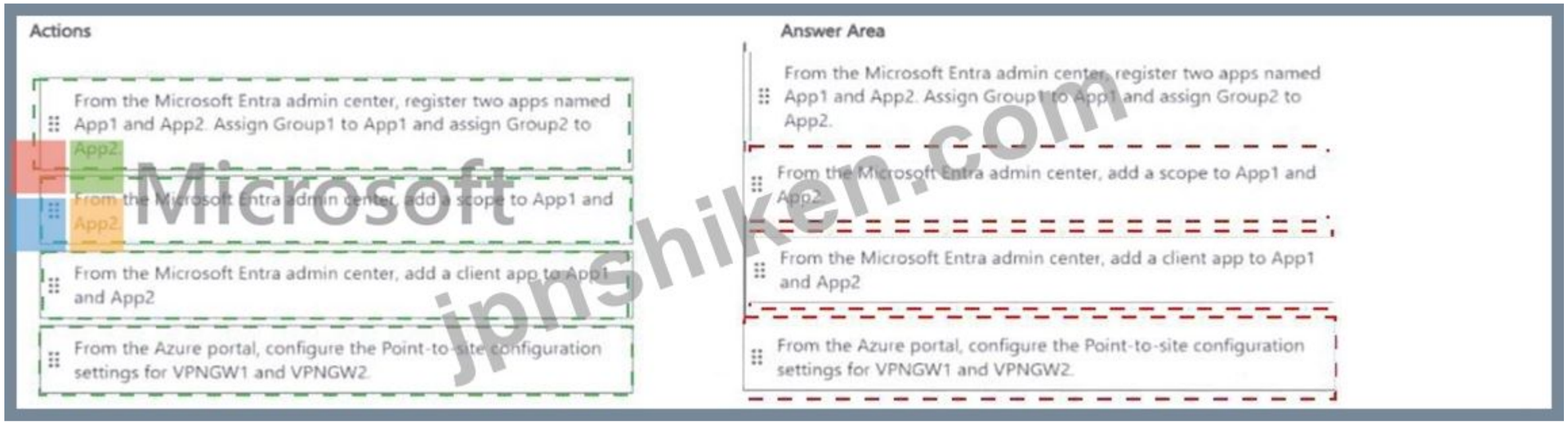
Microsoft Entra 管理センターから、Azure VPN アプリケーションをエンタープライズ アプリケーションとして登録します。
P2S VPN接続にはMicrosoft Entra認証を有効にする必要があります。ソリューションは以下の要件を満たす必要があります。
* Group1 のメンバーのみが VPNGW1 への VPN 接続を確立できることを確認します。
* Group2 のメンバーのみが VPNGW2 への VPN 接続を確立できることを確認します。
どの順序でアクションを実行すればよいですか? 回答するには、すべてのアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

Actions

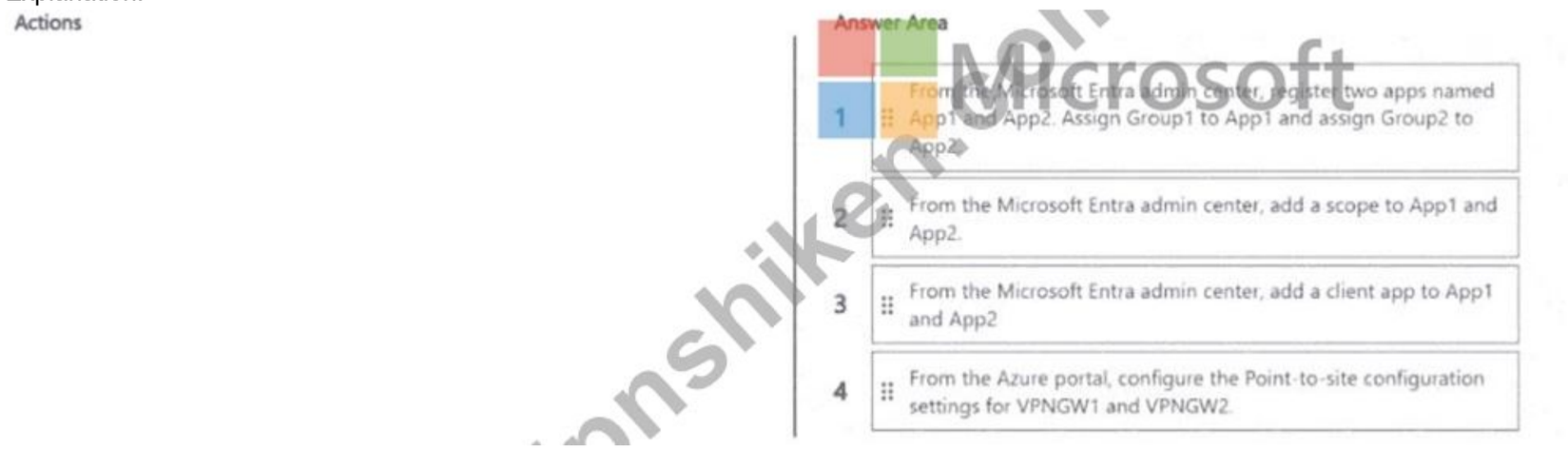
- From the Microsoft Entra admin center, register two apps named App1 and App2. Assign Group1 to App1 and assign Group2 to App2.
- From the Microsoft Entra admin center, add a scope to App1 and App2.
- From the Microsoft Entra admin center, add a client app to App1 and App2.
- From the Azure portal, configure the Point-to-site configuration settings for VPNGW1 and VPNGW2.

Answer Area

正解:



Explanation:



質問: **136**

相互にピアリングされた VNet1 と VNet2 という 2 つの Azure 仮想ネットワークがあります。VNet1 は、Web サーバーを含む 10 台の仮想マシンをホストします。VNet2 は、データベース サーバーを含む 5 台の仮想マシンをホストします。

次の要件を満たすセキュリティ ソリューションを構成する必要があります。

* データベースサーバーがWebサーバーからの接続のみを受け入れることを保証します
* Webサーバーがデータベースサーバーにのみ接続を開始できるようにします
* すべてのネットワーク セキュリティ グループ (NSG) がサブネットにのみ関連付けられていることを確認します。
* アプリケーションセキュリティグループを使用してソリューションを実装する

必要なアプリケーション セキュリティ グループの最小数はいくつですか?

A. 8
B. 4
C. 1
D. 2

正解: **D** (コメントを発表する)

質問: **137**
次の表に示すオンプレミス ネットワークがあります。

Name	ASN	IP address space	Connection type	Description
Branch1	64551	10.50.0.0/24,10.61.0.0/16	VPN	Is an on-premises datacenter
Branch2	64551	10.50.0.0/16,10.61.0.0/16	VPN and ExpressRoute	AS Path has a prefix of 64551,64551,64551
Branch3	64551	10.50.20.0/24,10.61.0.0/16	ExpressRoute	*None*

Azureサブスクリプションには、VWAN1というAzure仮想WANとVNet1という仮想ネットワークが含まれています。VWAN1は、オンプレミスネットワークとVNet1にフルメッシュトポロジで接続されています。VWAN1の仮想ハブルーティング設定はASパスです。
VNet1 から 10.61.1.5 にトラフィックをルーティングする必要があります。
どのパスが使用されますか?
A. Branch3へのExpressRoute接続
B. Branch2へのVPN接続
C. Branch1へのVPN接続
D. Branch2へのExpressRoute接続
正解: **(**正解を表示します**)**

質問: **138**
P2S VPN ユーザーのネットワーク セキュリティ要件を満たすように GW1 を構成する必要があります。
GW1 のポイントツーサイト構成設定ではどのトンネル タイプを選択する必要がありますか?
A. IKEv2 と OpenVPN (SSL)
B. IKEv2
C. IKEv2 と SSTP (SSL)
D. OpenVPN (SSL)
E. SSTP (SSL)
正解: **D (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant

質問: **139**
Vnet6 の仮想ネットワーク要件を実装しています。

作成する必要があるサブネットとサービス エンドポイントの最小数はいくつですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:
2, 4

質問: **140**
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Description
FW1	Azure Firewall Premium	Has a network intrusion detection and prevention system (IDPS) enabled
HP1	Azure Virtual Desktop host pool	All outbound traffic from HP1 to the subscription's resources route through FW1
Server1	Virtual machine	Hosts an application named App1
KV1	Azure Key Vault	*None*

HP1 のユーザーは、https://app1 .comoso.com という URL を使用して App1 に接続します。
FW1 上の IDPS が HP1 から Server1 への接続におけるセキュリティ脅威を識別できることを確認する必要があります。
実行すべき 2 つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. サーバー証明書を KV1 にインポートします。
B. FW1 の脅威インテリジェンスを有効にします。
C. HP1 にアプリケーション グループを追加します。
D. セキュリティで保護された仮想ネットワークを FW1 に追加します。
E. FW1 の TLS 検査を有効にします。
正解: **(**正解を表示します**)**

質問: **141**
あなたの会社はモントリオール、シアトル、パリにオフィスを構えています。各オフィスからの送信トラフィックは、特定のパブリックIPアドレスから発信されています。
Azure Web アプリケーション ファイアウォール (WAF) が有効になっている FD1 という Azure Front Door インスタンスを作成します。Policy! という WAF ポリシーを構成し、Rule1 というルールを設定します。Rule1 は、モントリオールのオフィスから発信されるトラフィックに対して、100 リクエストのレート制限を適用します。
各オフィスから発信されるトラフィックに対して、100 リクエストのレート制限を適用する必要があります。
何をすべきでしょうか?
A. Rule1 の条件を変更します。
B. 追加の関連付けを 2 つ作成します。
C. Rule1 のルール タイプを変更します。

D. Rule1 のレート制限しきい値を変更します。
正解: (正解を表示します)
https://techcommunity.microsoft.com/t5/azure-network-security-blog/rate-limiting-feature-for-azure-waf-on- application-gateway-now/ba-p/3934957#:~:text=Rate%20limiting%20is%20configured%20using,and%20a%
20group%20by%20variable.

質問: **142**
タスク 4
10.1.1.0/24 の範囲の IP アドレスと storage34280945.pnvatelinlcblob.core.windows.net という名前を使用して、storage34280945 ストレージ アカウントへの接続が可能であることを確認する必要があります。
正解:
See the Explanation below for step by step instructions.
Explanation:
Here are the steps and explanations for ensuring that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name stor-age34280945.pnvatelinlcblob.core.
windows.net:
* To allow access from a specific IP address range, you need to configure the Azure Storage firewall and virtual network settings for your storage account. You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings1.
* On the Networking page, select Firewalls and virtual networks, and then select Selected networks under Allow access from1. This will block all access to your storage account except from the networks or resources that you specify.
* Under Firewall, select Add rule, and then enter 10.1.1.0/24 as the IP address or range. You can also enter an optional rule name and description1. This will allow access from any IP address in the 10.1.1.0
/24 range.
* Select Save to apply your changes1.
* To map a custom domain name to your storage account, you need to create a CNAME record with your domain provider that points to your storage account endpoint2. A CNAME record is a type of DNS record that maps a source domain name to a destination domain name.
* Sign in to your domain registrar's website, and then go to the page for managing DNS settings2.
* Create a CNAME record with the following information2:
* Source domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
* Destination domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
* Save your changes and wait for the DNS propagation to take effect2.
* To register the custom domain name with Azure, you need to go back to the Azure portal and select your storage account. Then select Custom domain under Blob service2.
* On the Custom domain page, enter stor-age34280945.pnvatelinlcblob.core.windows.net as the custom domain name and select Save2.

質問: **143**
複数の仮想マシン スケール セットと複数の Azure ロード バランサーを含む Azure サブスクリプションがあります。ロード バランサーは、スケール セット間でトラフィックを分散します。
ロード バランサー間でトラフィックの負荷を分散するために、Azure Front Door をデプロイする予定です。
どのFront Door SKUを構成するか、そしてロードバランサーへのトラフィックのルーティングに何を使用するかを特定する必要があります。ソリューションはコストを最小限に抑える必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

Explanation:

質問: **144**

米国西部 Azure リージョンに複数の仮想マシンが含まれる Azure サブスクリプションがあります。

トラフィック分析を使用する必要があります。

作成すべきリソースは 2 つあります。それぞれの正解はソリューションの一部を示しています。(2 つ選択してください。) 注: 正解の選択ごとに 1 ポイントが加算されます。

A. Azure Monitor ワークブック

B. Log Analytics ワークスペース

C ストレージアカウント

C. Azure Sentinel ワークスペース

D. Azure Monitor データ収集ルール

正解: (正解を表示します)

Reference:

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics A storage acccount is used to store network security group flow logs.
A Log Analytics workspace is used by Traffic Analytics to store the aggregated and indexed data that is then used to generate the analytics.
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#enable-flow-log-settings

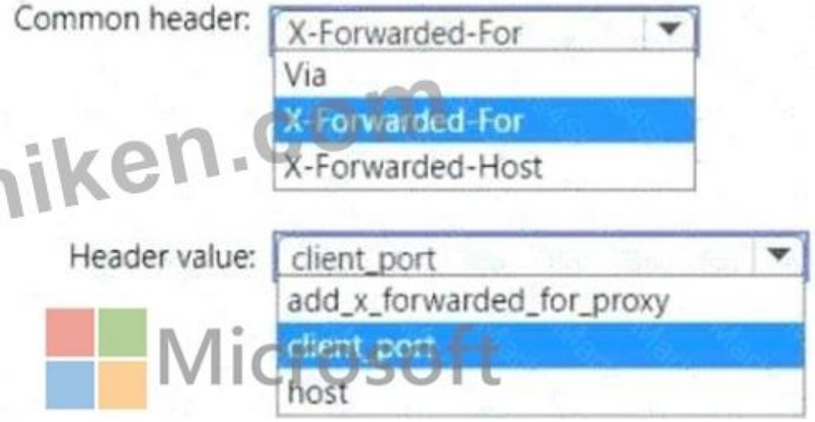
質問: **145**
LBGW1の導入計画を立てる必要があります。ソリューションは計画された変更をサポートする必要があります。
解決策には何を含めるべきですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

正解:

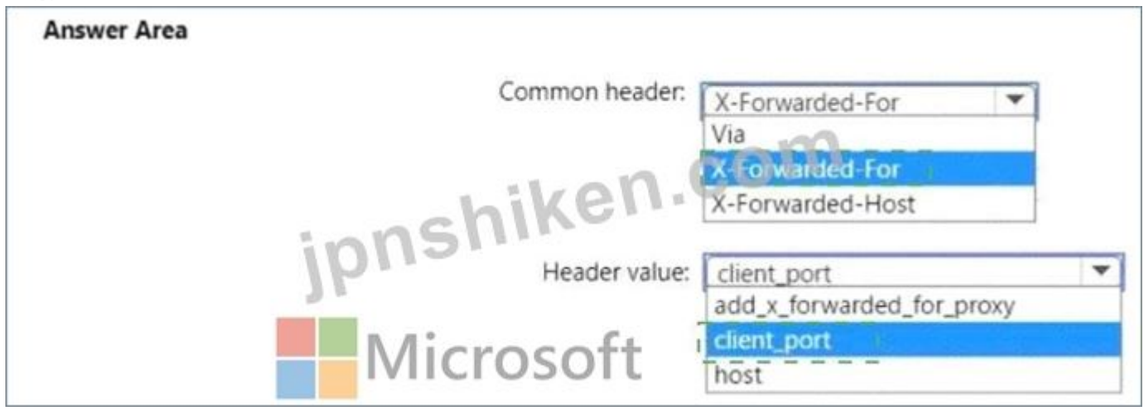
Explanation:

質問: **146**
Azure アプリケーション ゲートウェイがあります。
バックエンド プールに転送される受信リクエストの HTTP ヘッダーから元のポートを削除する書き換えルールを作成する必要があります。
各設定をどのように構成すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:



Explanation:

質問: **147**

NYCNet からプライベートエンドポイントを使用する Azure サービスへの接続を管理する必要があります。ソリューションはセキュリティ要件を満たす必要があります。まず何をすべきでしょうか？

A. SUBNET-PE のネットワーク ポリシーを有効にします。

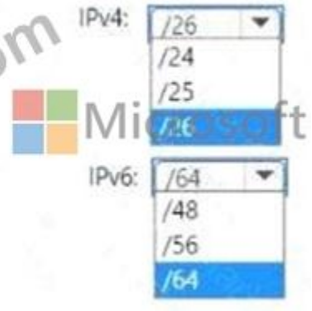
B. Azure Virtual Network Manager から、セキュリティ管理構成を作成します。

C. SUBNET-PLにルートテーブルを追加する

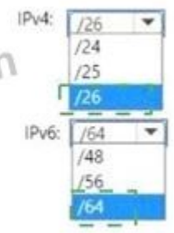
D. Azure仮想ネットワークマネージャーから、メンバーの種類がサブネットに設定されたネットワークグループを作成します。

正解: **A** (コメントを発表する)

質問: **148**
VNet1 という名前のデュアルスタック仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には次の IP アドレス空間があります。
* IPv4:192.168.0.0/24
* IPv6: fd0adbftdeca:deed:y48
Azure VPN ゲートウェイと複数の仮想マシンを VNet1 にデプロイする予定です。
VNet1のサブネットマスクを設定する必要があります。ソリューションは以下の要件を満たす必要があります。
* 使用可能な IP アドレスの数を最大化します。
* VPN ゲートウェイと仮想マシンの展開をサポートします。
各アドレス空間にはどのサブネット マスクを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area



正解:
Answer Area



Explanation:

質問: **149**
Azure AppServiceアプリを含むAzureサブスクリプションがあります。アプリはhttps://www.contoso.comのURLを使用します。
www.contoso.comのAzureFrontDoorでカスタムドメインを使用する必要があります。カスタムドメインは、許可された認証局（CA）からの証明書を使用する必要があります。
ソリューションに何を含める必要がありますか？
A. Azure Active Directory（Azure AD）のエンタープライズアプリケーション
B. Active Directory Certificate Services (AD CS)
C. Azure Key Vault

D. Azure Application Gateway
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https