AZ-500-free-Exam#02

# Q.1

Azure Container Registryに接続するAzure Kubernetes Service（AKS）クラスターがあります。

Azure Container Registryに対して認証するには、AKSクラスター用に自動生成されたサービスプリンシパルを使用する必要があります。

何を作成する必要がありますか？

1. Azure Key Vaultの秘密
2. 役割の割り当て
3. Azure Active Directory（Azure AD）ユーザー
4. Azure Active Directory（Azure AD）グループ

正解： B

参照：

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

# Q.2

Windows Server 2019を実行するVM1とVM2という名前の2つの仮想マシンを含むAzureサブスクリプションがあります。Azure Automationに更新管理を実装しています。

Update1という名前の新しい更新デプロイメントを作成することを計画しています。Update1が次の要件を満たしていることを確認する必要があります。

* VM1とVM2に更新を自動的に適用します。
* 新しいWindows Server 2019仮想マシンをUpdate1に自動的に追加します。

Update1には何を含める必要がありますか？

1. メンバーシップタイプが割り当てられているセキュリティグループ
2. メンバーシップタイプがダイナミックデバイスであるセキュリティグループ
3. 動的グループクエリ
4. Kustoクエリ言語クエリ

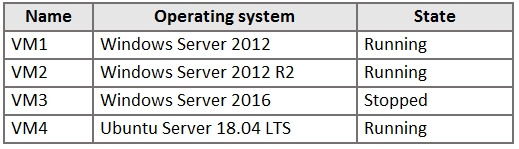
正解： C

リファレンス：

<https://docs.microsoft.com/en-us/azure/automation/update-management/configure-groups>

# Q.3

次の表に示すAzure仮想マシンがあります。



どの仮想マシンに対して更新管理を有効にできますか？

1. VM2とVM3のみ
2. VM2、VM3、およびVM4のみ
3. VM1、VM2、およびVM4のみ
4. VM1、VM2、VM3、およびVM4
5. VM1、VM2、およびVM3のみ

正解： *C*

参照：404

[https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=％2Fazure％2Fautomation％2Ftoc.json](https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%EF%BC%852Fazure%EF%BC%852Fautomation%EF%BC%852Ftoc.json)

# Q.4

DRAGDROP-

Sub1という名前のAzureサブスクリプションがあります。

ITチームのすべてのメンバーを含むGroup1という名前のAzure Active Directory（Azure AD）グループがあります。

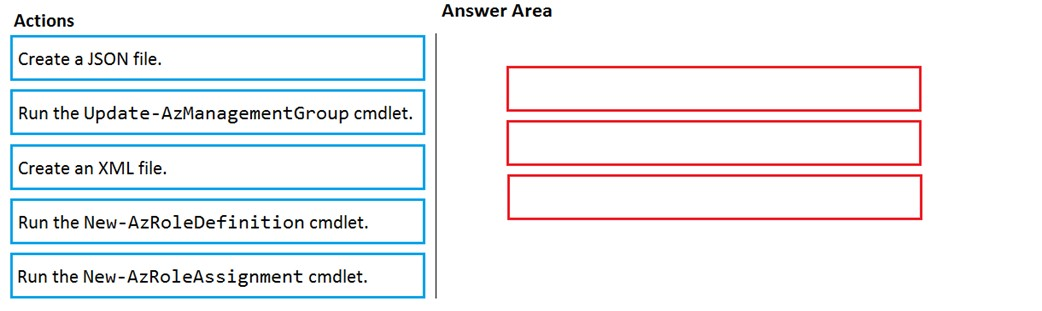
Group1のメンバーがSub1のAzure仮想マシンを停止、開始、および再起動できることを確認する必要があります。

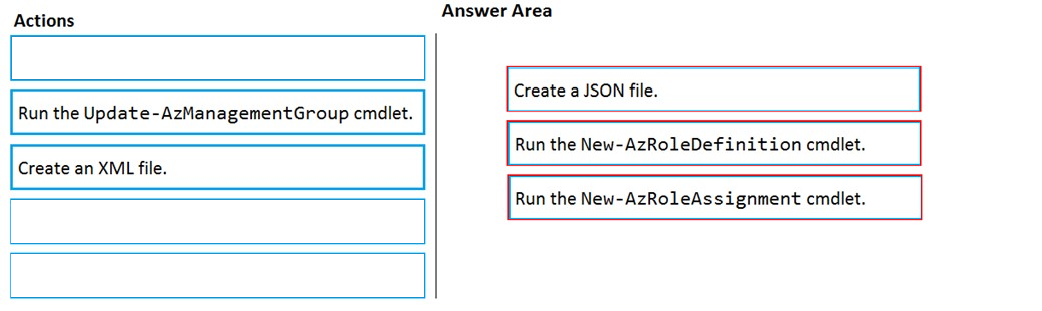
ソリューションは、最小特権の原則を使用する必要があります。

どの3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のリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解： 

参照：

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

# Q.5

DRAGのDROP -

あなたは、次のリソースが含まれているAzureのサブスクリプションを持っている

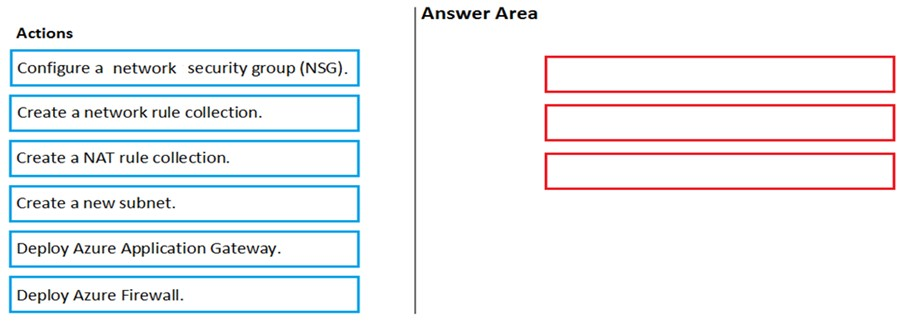
* Subnet1とSubnet2という名前の2つのサブネットが含まれていVNET1という名前の仮想ネットワーク。
* プライベートIPアドレスのみを持ち、Subnet1に接続するVM1という名前の仮想マシン。

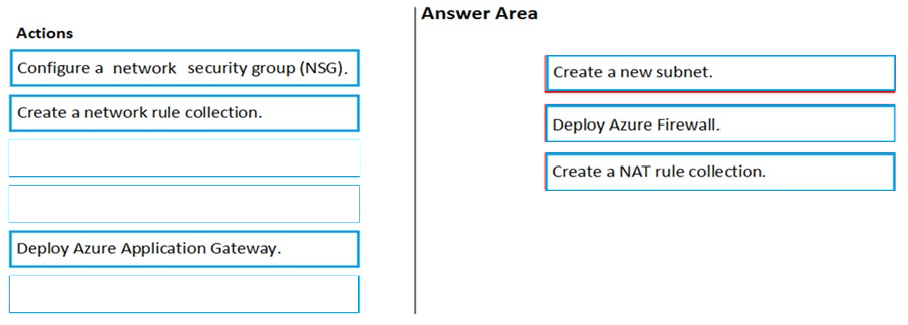
インターネットからVM1へのリモートデスクトップ接続を確立できることを確認する必要があります。

どの3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のリストから回答領域に移動し、正しい順序で配置します。

選択して配置：



正解： 

# Q.6

User1という名前のユーザーとConReg1という名前のAzure Container Registryを含むAzureサブスクリプションがあります。

ContReg1のコンテンツ信頼を有効にします。

User1がContReg1で信頼できるイメージを作成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、最小特権の原則を使用する必要があります。

User1に割り当てる必要がある2つの役割はどれですか？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。

1. AcrQuarantineReader
2. Contributor
3. AcrPush
4. AcrImageSigner
5. AcrQuarantineWriter

正解： *CD*

リファレンス：

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

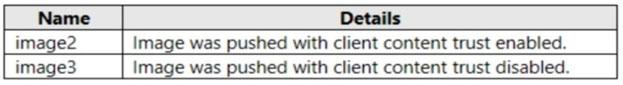
<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

# Q.7

image1という名前のコンテナーイメージを含むContReg1という名前のAzureコンテナーレジストリがあります。

ContReg1のコンテンツ信頼を有効にします。

コンテンツの信頼を有効にした後、次の表に示すように、2つのイメージをContReg1にプッシュします。



どのimageが信頼できるimageですか？

1. image1とimage2のみ
2. image2のみ
3. image1、image2、およびimage3

正解： *B*

Azure Container RegistryはDockerのコンテンツ信頼モデルを実装し、署名されたイメージのプッシュとプルを可能にします。

信頼できるイメージタグをコンテナレジストリにプッシュするには、コンテンツの信頼を有効にして、Dockerプッシュでイメージをプッシュします。

信頼できるイメージを操作するには、イメージの発行者とコンシューマーの両方がDockerクライアントのコンテンツの信頼を有効にする必要があります。パブリッシャーは、コンテンツの信頼が有効なレジストリにプッシュする画像に署名できます。

参照：

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

# Q.8シミュレーション-

インターネットからVM1という名前の仮想マシンへのRDP接続を許可するようにAzureを構成する必要があります。このソリューションでは、VM1の攻撃対象領域を最小限に抑える必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

NSGでRDPポートを有効にするには、次の手順に従います。

1.Azureポータルにサインインします。

2.仮想マシンでVM1を選択します。

3.設定でネットワークを選択します。

4.インバウンドポートルールで、RDPのポートが正しく設定されているかどうかを確認します。構成の例を次に示します。

優先度：300-

名前：Port\_3389-

ポート（宛先）：3389-

プロトコル：TCP-

ソース：任意-

宛先：任意-

アクション：許可-

参照：

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem>

# Q.9シミュレーション-

あなたはASG1という名前のアプリケーション・セキュリティ・グループにVM1という名前の仮想マシンのネットワーク・インターフェースを追加する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

1.ポータルの上部にある[リソース、サービス、およびドキュメントの検索]ボックスで、アプリケーションセキュリティグループに追加または削除するネットワークインターフェイスを持つ仮想マシンVM1の名前の入力を開始します。

2.検索結果にVMの名前が表示されたら、それを選択します。

3. [設定]で、[ネットワーク]を選択します。[アプリケーションセキュリティグループの構成]を選択するか、ネットワークインターフェイスを追加するアプリケーションセキュリティグループを選択するか、ネットワークインターフェイスを削除するアプリケーションセキュリティグループの選択を解除して、[保存]を選択します。

参照：

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

# Q.10シミュレーション

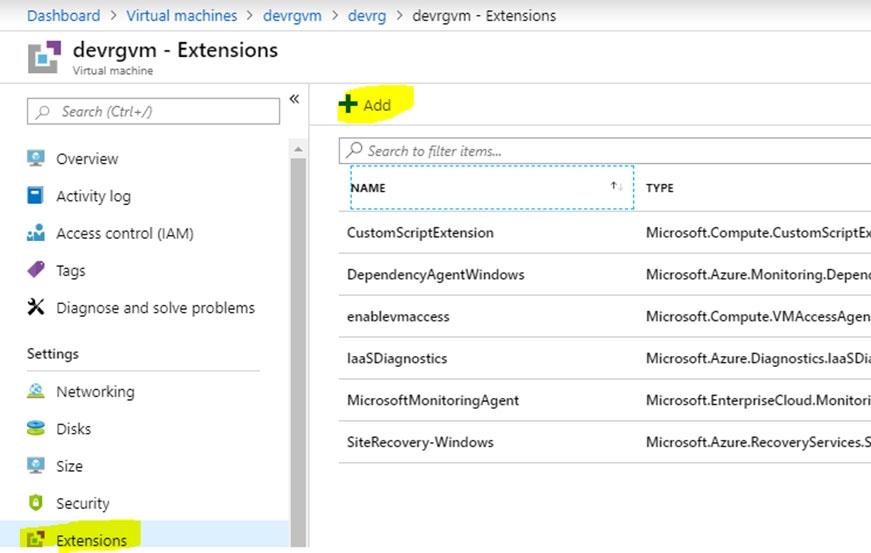
-MicrosoftAntimalware for Virtual Machinesを使用して、VM1という名前の仮想マシンで毎週日曜日の02:00に完全なマルウェアスキャンを実行する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

単一VMの展開にAzurePortalを使用してMicrosoftAntimalwareExtensionを展開する1.Azure

Portalで、Azure VM1のブレードに移動し、[拡張機能]セクションに移動して、[追加]を押します。



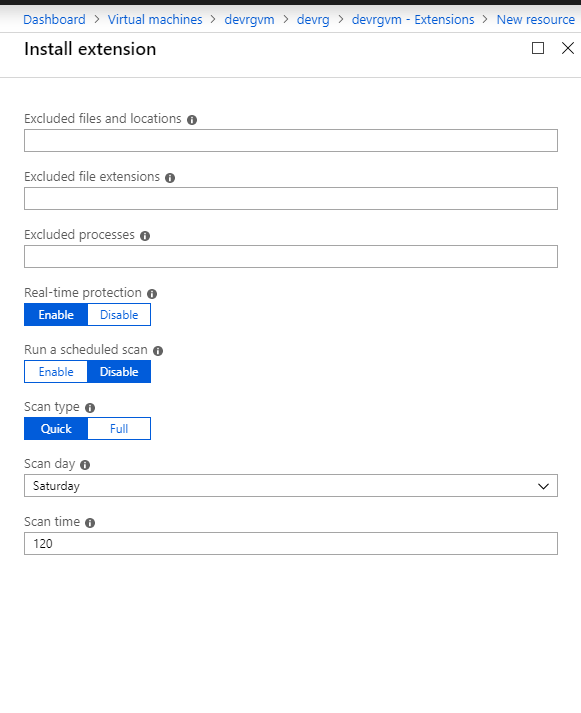
2. Microsoft Antimalware拡張機能を選択し、[作成]を押します。

3.必要に応じて、「拡張機能のインストール」フォームに入力し、「OK」を押します。

スケジュール：有効-

スキャンの種類：フル-

スキャン日：日曜日-



参照：

<https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/>

# Q.11シミュレーション-

管理ユーザーがVNET1という名前の仮想ネットワークを誤って削除しないようにする必要があります。管理ユーザーは、VNET1の設定を変更できるようにする必要があります。

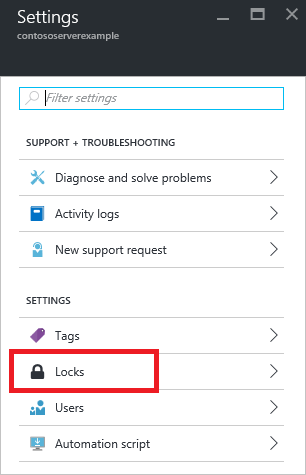
このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

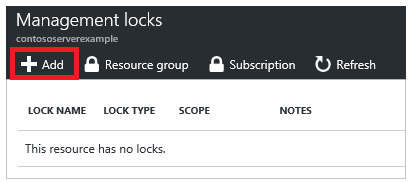
ロックすると、組織内の他のユーザーが、Azureサブスクリプション、リソースグループ、リソースなどの重要なリソースを誤って削除または変更するのを防ぐことができます。

注：Azureでは、リソースという用語はAzureによって管理されるエンティティを指します。たとえば、仮想マシン、仮想ネットワーク、およびストレージアカウントはすべてAzureリソースと呼ばれます。

1.仮想ネットワークVNETの[設定]ブレードで、[ロック]を選択します。



2.ロックを追加するには、[追加]を選択します。



3. [ロックの種類]で[ロックの削除]を選択し、[OK]をクリックします。

参照：

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

# Q.12シミュレーション-

あなたはRG1lod11641655リソースグループに仮想ネットワークを管理するためにUser211641655という名前のユーザーに必要な権限を付与する必要があります。ソリューションは、最小特権の原則を使用する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

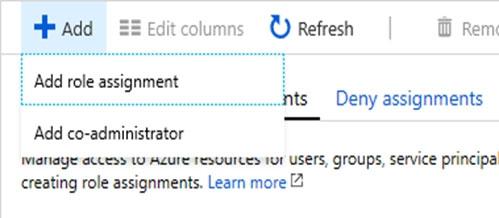
正解： *以下の説明を参照してください。*

1. Azureポータルで、RG1lod10598168リソースグループを見つけて選択します。

2. [アクセス制御（IAM）]をクリックします。

3. [役割の割り当て]タブをクリックして、このスコープのすべての役割の割り当てを表示します。

4. [追加]> [役割の割り当ての追加]をクリックして、[役割の割り当ての追加]ペインを開きます。



5. [役割]ドロップダウンリストで、仮想マシンコントリビューターの役割を選択します。

Virtual Machine Contributorを使用すると、仮想マシンを管理できますが、仮想マシンにアクセスすることはできません。また、仮想マシンが接続されている仮想ネットワークやストレージアカウントも管理できません。

6. [選択]リストで、ユーザーuser21059868を選択します。

7.[保存]をクリックして役割を割り当てます。

参照：

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

# Q.13シミュレーション-

あなたは131.107.0.0/16サブネットに接続されたデバイスのみがrg1lod10598168 Azureストレージアカウント内のデータにアクセスできることを確認する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： 以下の説明を参照してください。

手順1：

1.Azureポータルで、保護するストレージアカウントに移動します。

ここで：rg1lod105981682。ファイアウォールと仮想ネットワークと呼ばれる設定メニューをクリックします。

3.デフォルトでアクセスを拒否するには、選択したネットワークからのアクセスを許可することを選択します。すべてのネットワークからのトラフィックを許可するには、すべてのネットワークからのアクセスを許可することを選択します。

4. [保存]をクリックして変更を適用します。

手順2：

1.保護するストレージアカウントに移動します。ここで：rg1lod105981682。ファイアウォールと仮想ネットワークと呼ばれる設定メニューをクリックします。

3.選択したネットワークからのアクセスを許可することを選択したことを確認します。

4.新しいネットワークルールを使用して仮想ネットワークへのアクセスを許可するには、[仮想ネットワーク]で[既存の仮想ネットワークの追加]をクリックし、[仮想ネットワークとサブネット]オプションを選択します。131.107.0.0/16サブネットを入力し、[追加]をクリックします。

注：ネットワークルールが構成されている場合、指定されたネットワークのセットを介してデータを要求するアプリケーションのみがストレージアカウントにアクセスできます。ストレージアカウントへのアクセスを、指定されたIPアドレス、IP範囲、またはAzure Virtual Network（VNet）内のサブネットのリストから発信された要求に制限できます。

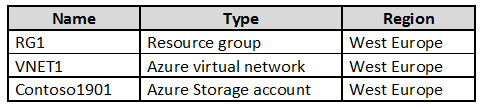
参照：

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

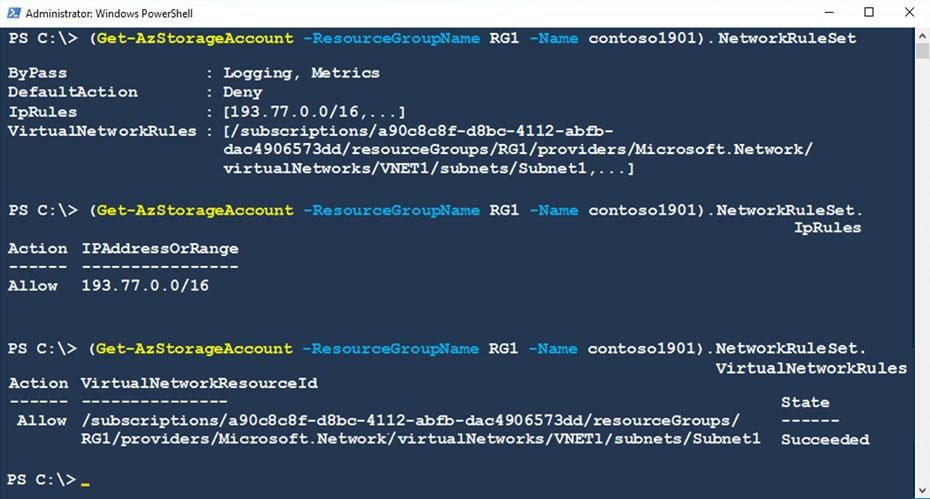
# Q.14

HOTSPOT-

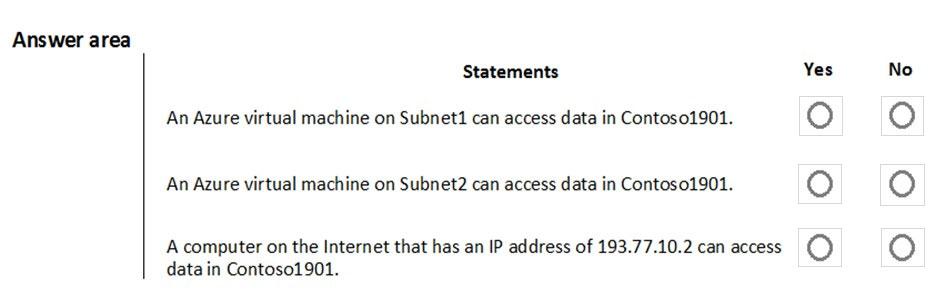
次の表に示すように、Azureサブスクリプションでリソースを作成します。



VNET1には、Subnet1およびSubnet2という名前の2つのサブネットが含まれています。Subnet1のネットワークIDは10.0.0.0/24です。Subnet2のネットワークIDは10.1.1.0/ 24です。Contoso1901は、展示に示されているように構成されています。（[展示]タブをクリックします。）



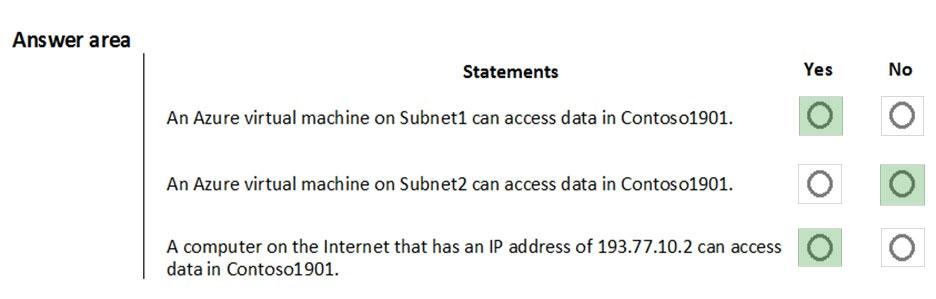
次の各ステートメントについて、ステートメントが真の場合は[はい]を選択します。それ以外の場合は、[いいえ]を選択します。



Subnet1上のAzure仮想マシンは、Contoso1901のデータにアクセスできます。

Subnet2上のAzure仮想マシンは、Contso1901のデータにアクセスできます。

IPアドレスが193.77.10.2のインターネット上のコンピューターは、Contoso1901のデータにアクセスできます。

正解： 

ボックス1：はい

-Subnet1からのアクセスが許可されます。

ボックス2：いいえ

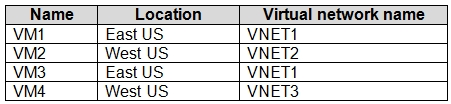
-Subnet2からのアクセスは許可されていません。

ボックス3：はい

-IPアドレス193.77.10.2からのアクセスが許可されます。

# Q.15

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。



すべての仮想ネットワークがピアリングされます。

Azure BastionをVNET2にデプロイします。

Azure Bastion ホストで保護できる仮想マシンはどれですか？

1. VM1、VM2、VM3、およびVM4
2. VM1、VM2、およびVM3のみ
3. VM2とVM4のみ
4. VM2のみ

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

# Q.16

Azure仮想マシンのデプロイに使用するAzure Resource Managerテンプレートがあります。

仮想マシンのインスタンスがプロビジョニングされるため、未使用のWindows機能を自動的に無効にする必要があります。

何を使うべきですか？

1. Microsoft Intune のデバイス構成ポリシー
2. Azure Automation の状態構成
3. Azure Security Centerのセキュリティポリシー
4. Microsoft Intuneのデバイスコンプライアンスポリシー

正解： *B*

Azure Automation State Configurationを使用して、Azure VM（ClassicとResource Managerの両方）、オンプレミスVM、Linuxマシン、AWS VM、およびオンプレミス物理マシンを管理できます。

注：Azure Automation State Configurationは、Windows機能**DSC**-Serviceと同様のDSCプルサーバーを提供します。これにより、ターゲットノードは自動的に構成を受け取り、目的の状態に準拠しレポートします。Azure Automationに組み込まれているプルサーバーを使用すると、独自のプルサーバーをセットアップして維持する必要がなくなります。Azure Automationは、クラウドまたはオンプレミスの仮想または物理のWindowsまたはLinuxマシンをターゲットにできます。

参照：

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

# Q.17

Sub1という名前のAzureサブスクリプションがあります。Sub1には、Subnet1という名前のサブネットを1つ含むVNet1という名前の仮想ネットワークが含まれています。

Subnet1には、Ubuntu Server18.04を実行するVM1という名前のAzure仮想マシンが含まれています。

Subnet1でMicrosoft Storageのサービスエンドポイントを作成します。

DockerコンテナーをVM1にデプロイするときに、コンテナーがサービスエンドポイントを使用してAzure Storageリソースにアクセスできることを確認する必要があります。

コンテナをデプロイする前に、VM1で何をする必要がありますか？

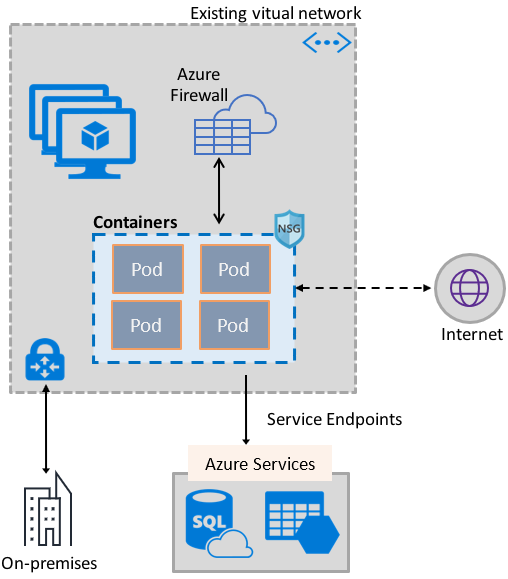
1. アプリケーションセキュリティグループとネットワークセキュリティグループ（NSG）を作成します。
2. 編集ドッキングウィンドウ-compose.ymlファイル。
3. コンテナネットワークインターフェイス（CNI）プラグインをインストールします。

正解： C

Azure仮想ネットワークコンテナーネットワークインターフェイス（CNI）プラグインは、Azure仮想マシンにインストールされます。プラグインは、LinuxとWindowsの両方のプラットフォームをサポートします。

プラグインは、仮想ネットワークから仮想マシンで起動されたコンテナにIPアドレスを割り当て、それらを仮想ネットワークに接続し、他のコンテナや仮想ネットワークリソースに直接接続します。プラグインは、接続のためにオーバーレイネットワークまたはルートに依存せず、仮想マシンと同じパフォーマンスを提供します。

次の図は、プラグインがポッドにAzure仮想ネットワーク機能を提供する方法を示しています。



<https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview>

# Q.18

Azure仮想マシンのデプロイに使用するAzure Resource Managerテンプレートがあります。

仮想マシンのインスタンスがプロビジョニングされるため、未使用のWindows機能を自動的に無効にする必要があります。

何を使うべきですか？

1. Microsoft Intuneのデバイス構成ポリシー
2. Azure Desired State Configuration（DSC）仮想マシンの拡張機能
3. アプリケーションセキュリティグループ
4. Microsoft Intuneのデバイスコンプライアンスポリシー

正解： B

Azure Desired State Configuration（DSC）拡張機能の主な使用例は、VMをAzure Automation State Configuration（DSC）サービスにブートストラップすることです。

このサービスは、VM構成の継続的な管理や、AzureMonitoringなどの他の運用ツールとの統合などの利点を提供します。

拡張機能を使用してVMをサービスに登録すると、Azureサブスクリプション間でも機能する柔軟なソリューションが提供されます。

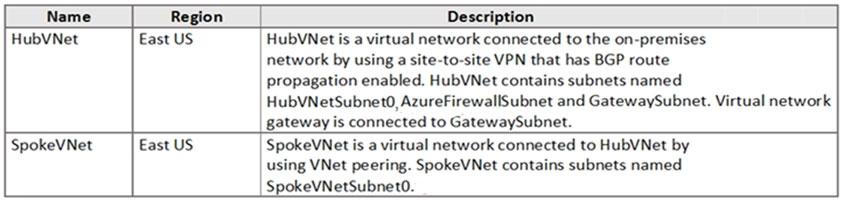
参照：

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

# Q.19

DRAGDROP-

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。



SpokeVNetSubnet0上のAzure仮想マシンは、オンプレミスネットワーク上のコンピューターと通信できます。

AzureファイアウォールをHubVNetにデプロイすることを計画しています。

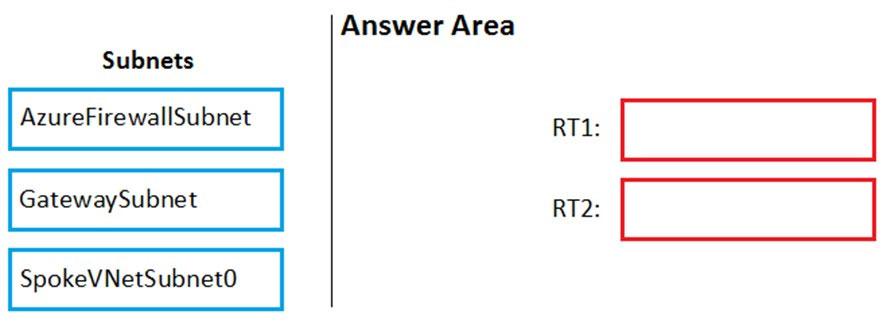
次の2つのルーティングテーブルを作成します。

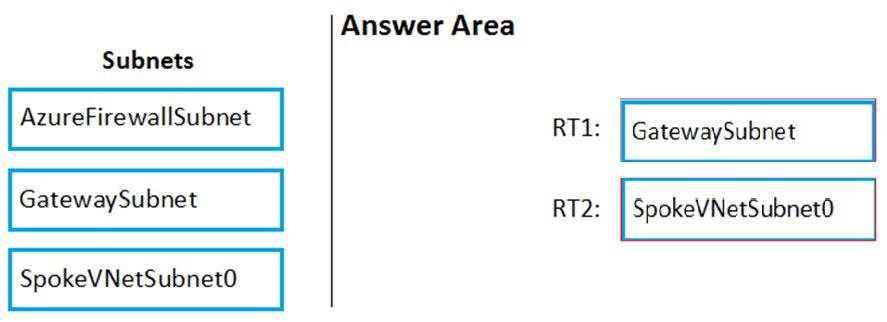
* RT1：AzureファイアウォールのプライベートIPアドレスをネクストホップアドレスとして指すユーザー定義ルートを含めます
* RT2：BGPルート伝播を無効にし、AzureファイアウォールのプライベートIPアドレスをデフォルトゲートウェイとして定義します

Spoke VNet Subnet0とオンプレミスネットワーク間のトラフィックがAzureファイアウォールを通過することを確認する必要があります。

各ルートテーブルをどのサブネットに関連付ける必要がありますか？

答えるには、適切なサブネットを正しいルートテーブルにドラッグします。各サブネットは、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、分割バーをペイン間でドラッグするか、スクロールする必要がある場合があります。



正解： 

参照：

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal#create-the-routes>

# Q.20

HOTSPOT-

Azureサブスクリプションがあります。サブスクリプションには、Windows Server 2016を実行するAzure仮想マシンが含まれています。

各仮想マシンにカスタムのマルウェア対策仮想マシン拡張機能がインストールされていることを確認するためのポリシーを実装する必要があります。

ポリシーをどのように完了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。



正解： 

ボックス1：DeployIfNotExists

DeployIfNotExistsは、条件が満たされたときにテンプレートの展開を実行します。

ボックス2：template

DeployIfNotExistsエフェクトのdetailsプロパティには、一致する関連リソースと実行するテンプレート展開を定義するすべてのサブプロパティがあります。

展開[必須]

このプロパティには、Microsoftに渡される完全なテンプレート展開が含まれている必要があります。

リソース/展開

参照：<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

# Q.21

Azure Container Registryに接続するAzure Kubernetes Service（AKS）クラスターを構成しています。

自動生成されたサービスプリンシパルを使用して、Azure Container Registryへの認証を行う必要があります。

何を作成する必要がありますか？

1. Azure Active Directory（Azure AD）グループ
2. Azure Active Directory（Azure AD）の役割の割り当て
3. Azure Active Directory（Azure AD）ユーザー
4. Azure Key Vaultの秘密

正解： *B*

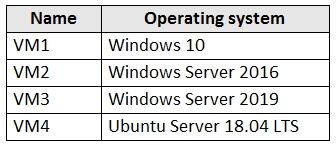
AKSクラスターを作成すると、Azureは、他のAzureリソースとのクラスター操作性をサポートするサービスプリンシパルも作成します。この自動生成されたサービスプリンシパルを使用して、ACRレジストリでの認証を行うことができます。これを行うには、クラスターのサービスプリンシパルにコンテナーレジストリへのアクセスを許可するAzureADロール割り当てを作成する必要があります。

参照：

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks>

# Q.22

次の表に示すAzure仮想マシンを含むAzureサブスクリプションがあります。



Profile1という名前のMDMセキュリティベースラインプロファイルを作成します。

Profile1を適用できる仮想マシンを特定する必要があります。

どの仮想マシンを特定する必要がありますか？

1. VM1だけ
2. VM1、VM2、およびVM3のみ
3. VM1とVM3のみ
4. VM1、VM2、VM3、およびVM4

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

# Q.23シミュレーション-

インターネットからVNET1 \ subnet0への接続がTCPポート7777経由でのみ許可されていることを確認する必要があります。ソリューションは現在展開されているリソースのみを使用する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

subnet0に関連付けられているネットワークセキュリティグループを構成する必要があります。

1. Azureポータルで、検索ボックスに「仮想ネットワーク」と入力し、検索結果から[仮想ネットワーク]を選択してから、[VNET1]を選択します。または、左側のナビゲーションペインで[仮想ネットワーク]を参照します。
2. VNET1のプロパティで、[サブネット]をクリックします。これにより、VNET1のサブネットと、各サブネットに関連付けられているネットワークセキュリティグループが表示されます。Subnet0に関連付けられているネットワークセキュリティグループの名前に注意してください。
3. 検索ボックスに「ネットワークセキュリティグループ」と入力し、Subnet0に関連付けられているネットワークセキュリティグループを選択します。
4. ネットワークセキュリティグループのプロパティで、[受信セキュリティルール]をクリックします。
5. [追加]ボタンをクリックして、新しいルールを追加します。
6. [ソース]フィールドで、[サービスタグ]を選択します。
7. [ソースサービスタグ]フィールドで、[インターネット]を選択します。
8. [送信元ポート範囲]と[宛先]フィールドをデフォルト値（\*および[すべて]）のままにします。
9. [宛先ポート範囲]フィールドに7777と入力します。
10. プロトコルをTCPに変更します。
11. [アクション]オプションを[許可]のままにします。
12. 優先度を100に変更します。
13. 名前をデフォルトのPort\_8080からAllow\_TCP\_7777\_from\_Internetなどのよりわかりやすい名前に変更します。名前にスペースを含めることはできません。
14. [追加]ボタンをクリックして、新しいルールを保存します。

# Q.24シミュレーション-

管理者がホームページアプリのサービスプランに誤って変更を加えないようにする必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

アプリサービスプランの「ロック」を構成する必要があります。読み取り専用ロックは、最初にロックを削除せずにアプリサービスプランを変更できないようにします。

1. Azureポータルで、検索ボックスに「App Service Plans」と入力し、検索結果から[App Service Plans]を選択して、[ホームページ]を選択します。または、左側のナビゲーションペインで[App ServicePlans]を参照します。
2. アプリサービスプランのプロパティで、[ロック]をクリックします。
3. [追加]ボタンをクリックして、新しいロックを追加します。
4. [ロック名]フィールドに名前を入力します。試験にどのような名前を付けてもかまいません。
5. [ロックの種類]で、[読み取り専用]を選択します。
6. [OK]をクリックして変更を保存します。

# Q.25シミュレーション-

あなたはDanny11597200という名前のユーザーがSQL Serverの使用によりweb11597200という名前のMicrosoft SQLサーバー上の任意のSQLデータベースにサインインできることを確認する必要があります

管理Studio（SSMS）とAzureのActive Directoryの（アズールAD）の資格情報を。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

SQLServer用にAzureADAdminをプロビジョニングする必要があります。

1. Azureポータルで、検索ボックスに「SQL Server」と入力し、検索結果から[SQL Server]を選択してから、web11597200という名前のサーバーを選択します。または、左側のナビゲーションペインでSQLServerを参照します。

2. [SQL Serverのプロパティ]ページで、[ActiveDirectory管理者]をクリックします。

3. [管理者の設定]ボタンをクリックします。

4. [管理者の追加]ウィンドウで、Danny11597200を検索して選択します。

5. [選択]ボタンをクリックして、Danny11597200を追加します。

6. [保存]ボタンをクリックして、変更を保存します。

参照：

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell>

# Q.26シミュレーション-

あなただけVNET01仮想ネットワーク上のSubnet0サブネットからの接続を受け入れるようにWeb11597200という名前のMicrosoft SQLサーバーを設定する必要があります。

このタスクを完了するには、Azureポータルにサインインします。

正解： *以下の説明を参照してください。*

Azureサービスへのアクセスを許可し、SQLServerの仮想ネットワークルールを構成する必要があります。

1. Azureポータルで、検索ボックスに「SQL Server」と入力し、検索結果から[SQL Server]を選択してから、web11597200という名前のサーバーを選択します。または、左側のナビゲーションペインでSQLServerを参照します。

2. SQL Serverのプロパティで、[ファイアウォールと仮想ネットワーク]をクリックします。

3. [仮想ネットワーク]セクションで、[既存のものを追加]をクリックします。これにより、[仮想ネットワークの作成/更新]ルールウィンドウが開きます。

4.ルールにAllow\_VNET01-Subnet0などの名前を付けます（試験に入力する名前は関係ありません）。

5. [仮想ネットワーク]ボックスで、[VNET01]を選択します。

6. [サブネット名]ボックスで、[サブネット0]を選択します。

7. [OK]ボタンをクリックして、ルールを保存します。

8. [ファイアウォール/仮想ネットワーク]ウィンドウに戻り、[Azureサービスへのアクセスを許可する]オプションを[オン]に設定します。

# Q.27

Azure仮想マシンのデプロイに使用するAzure Resource Managerテンプレートがあります。

仮想マシンのインスタンスがプロビジョニングされるため、未使用のWindows機能を自動的に無効にする必要があります。

何を使うべきですか？

1. Microsoft Intuneのデバイス構成ポリシー
2. Azure Desired State Configuration（DSC）仮想マシンの拡張機能
3. Azure Security Centerのセキュリティポリシー
4. Azure Logicアプリ

正解： *B*

Azure Desired State Configuration（DSC）拡張機能の主な使用例は、VMをAzure Automation State Configuration（DSC）サービスにブートストラップすることです。

このサービスは、VM構成の継続的な管理や、AzureMonitoringなどの他の運用ツールとの統合などの利点を提供します。

拡張機能を使用してVMをサービスに登録すると、Azureサブスクリプション間でも機能する柔軟なソリューションが提供されます。

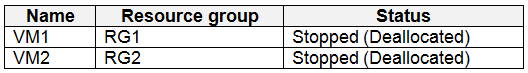
参照：

<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview>

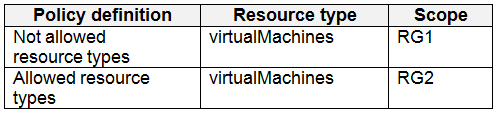
# Q.28

HOTSPOT-

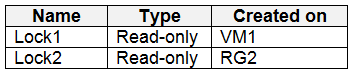
次の表に示す仮想マシンを含むAzureサブスクリプションがあります。



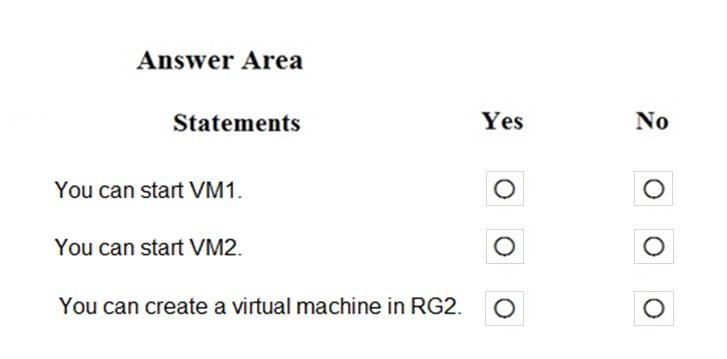
次の表に示すAzureポリシーを作成します。

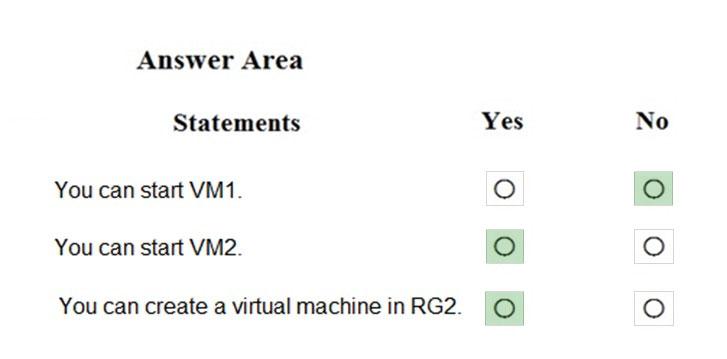


次の表に示すリソースロックを作成します。



次の各ステートメントで、ステートメントがtrueの場合は[はい]を選択します。それ以外の場合は、[いいえ]を選択します。



正解： 

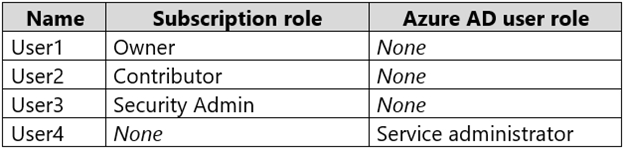
参照：

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

# Q.29

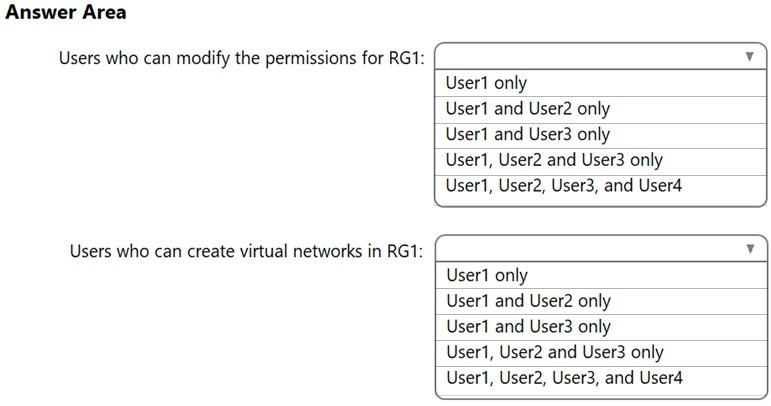
HOTSPOT-

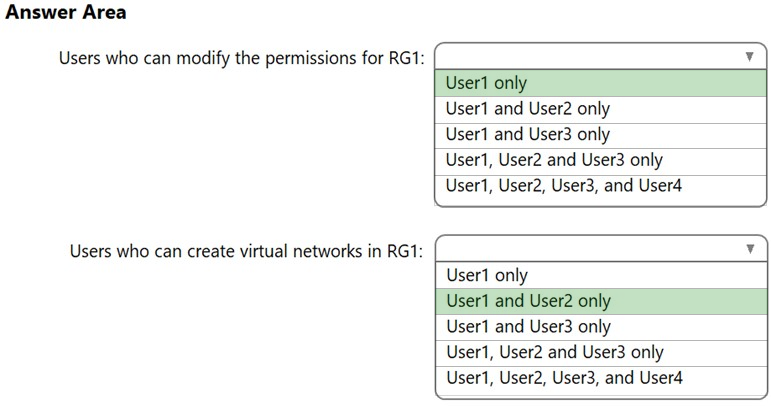
contoso.comという名前のAzure Active Directory（Azure AD）テナントを含むAzureサブスクリプションがあります。テナントには、次の表に示すユーザーが含まれています。



RG1という名前のリソースグループを作成します。

どのユーザーがRG1のアクセス許可を変更でき、どのユーザーがRG1で仮想ネットワークを作成できますか？回答するには、回答領域で適切なオプションを選択します。



正解： 

ボックス1：リソースの権限を変更できるのは所有者のみです。

ボックス2：コントリビューターはサブスクリプション内のすべてのものを作成/変更/削除できますが、アクセス許可を変更することはできません。

# Q.30シミュレーション-

あなたはVNET1という名前の仮想ネットワークとVNET2という名前の仮想ネットワーク間のネットワーク接続を構成してする必要があります。このソリューションでは、VNET1に接続された仮想マシンがVNET2に接続された仮想マシンと通信できるようにする必要があります。

このタスクを完了するには、Azureポータルにサインインし、Azureリソースを変更します。

正解： *以下の説明を参照してください。*

2つのネットワーク間でVNetピアリングを構成する必要があります。質問には、「ソリューションは、VNET1に接続された仮想マシンがVNET2に接続された仮想マシンと通信できることを保証する必要があります」と述べています。VNET2上のVMがVNET1上のVMと通信できる必要があるとは言っていません。したがって、一方向の通信のみを許可するようにピアリングを構成する必要があります。

1. Azureポータルで、検索ボックスに「仮想ネットワーク」と入力し、検索結果から[仮想ネットワーク]を選択してから、[VNET1]を選択します。または、

左側のナビゲーションペインで[仮想ネットワーク]を参照します。

2. VNET1のプロパティで、[ピアリング]をクリックします。

3. [ピアリング]ブレードで、[追加]をクリックして新しいピアリングを追加します。

4. [VNET1からリモート仮想ネットワークへのピアリングの名前]ボックスに、VNET1-VNET2などの名前を入力します（これは、VNET1のようにピアリングが表示される名前です）。

5.[仮想ネットワーク]ボックスで、[VNET2]を選択します。

6. [リモート仮想ネットワークからVNET1へのピアリングの名前]ボックスに、VNET2-VNET1などの名前を入力します（これは、VNET2のようにピアリングが表示される名前です）。

VNETからリモート仮想ネットワークへの仮想ネットワークアクセスを許可するオプションがあります。これは有効のままにしておく必要があります。

7. [リモートネットワークからVNET1への仮想ネットワークアクセスを許可する]オプションで、スライダーボタンをクリックして[無効]にします。

8. [OK]ボタンをクリックして、変更を保存します。

参照：

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

# Q.31シミュレーション-

あなたはVNET3という名前の仮想ネットワークにAzureのファイアウォールを展開する必要があります。

このタスクを完了するには、Azureポータルにサインインし、Azureリソースを変更します。

このタスクは、完了するまでに数分かかる場合があります。タスクの完了中に他のタスクを実行できます。

正解： *以下の説明を参照してください。*

AzureファイアウォールをVNETに追加するには、最初にAzureFirewallSubnetという名前のサブネットでVNETを構成する必要があります（まだ存在しない場合）。

VNET3を構成します。

1. Azureポータルで、検索ボックスに「仮想ネットワーク」と入力し、検索結果から[仮想ネットワーク]を選択してから、[VNET3]を選択します。または、

左側のナビゲーションペインで[仮想ネットワーク]を参照します。

2. [概要]セクションで、仮想ネットワークの場所（地域）とリソースグループに注意してください。ファイアウォールを追加するときにこれらが必要になります。

3.サブネットをクリックします。

4. [+サブネット]をクリックして、新しいサブネットを追加します。

5. [名前]ボックスに「AzureFirewallSubnet」と入力します。サブネットの名前はAzureFirewallSubnetである必要があります。

6. [アドレス範囲]ボックスにサブネットの適切なIP範囲を入力します。

7. [OK]ボタンをクリックして、サブネットを作成します。

Azureファイアウォールを追加します。

1. VNET3の設定で、ファイアウォールをクリックします。

2.ここをクリックして、新しいファイアウォールリンクを追加します。

3.リソースグループはデフォルトでVNET3リソースグループになります。このデフォルトのままにします。

4. [名前]ボックスにファイアウォールの名前を入力します。

5. [地域]ボックスで、VNET3と同じ地域を選択します。

6. [パブリックIPアドレス]ボックスで、使用可能なパブリックIPアドレスが存在する場合はそれを選択するか、[新規追加]をクリックして新しいパブリックIPアドレスを追加します。

7. [レビュー+作成]ボタンをクリックします。

8.設定を確認し、[作成]ボタンをクリックしてファイアウォールを作成します。

参照：

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

# Q.32シミュレーション

あなたは、次の要件を満たすためにVNET2という名前の仮想ネットワークを構成する必要があります。

* 管理者が誤ってVNET2を削除することを防止しなければなりません。
* 管理者は、サブネットをVNET2に定期的に追加できる必要があります。

このタスクを完了するには、Azureポータルにサインインし、Azureリソースを変更します。

正解： *以下の説明を参照してください。*

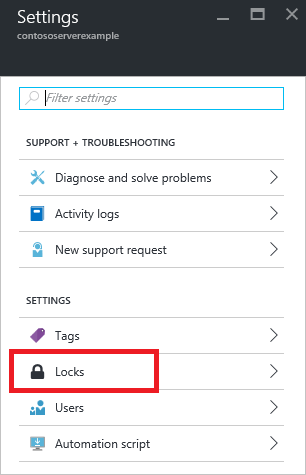
ロックすると、組織内の他のユーザーが、Azureサブスクリプション、リソースグループ、リソースなどの重要なリソースを誤って削除または変更するのを防ぐことができます。

注：Azureでは、リソースという用語はAzureによって管理されるエンティティを指します。たとえば、仮想マシン、仮想ネットワーク、およびストレージアカウントはすべてAzureリソースと呼ばれます。

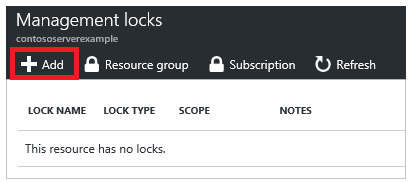
1. Azureポータルで、検索ボックスに「仮想ネットワーク」と入力し、検索結果から[仮想ネットワーク]を選択してから、[VNET2]を選択します。または、

左側のナビゲーションペインで[仮想ネットワーク]を参照します。

2.仮想ネットワークVNET2の[設定]ブレードで、[ロック]を選択します。



3.ロックを追加するには、[追加]を選択します。



4. [ロックの種類]で[ロックの削除]を選択し、[OK]をクリックします。

参照：

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

# Q.33

VM1という名前のAzure仮想マシンがあります。

Azure Security Centerから、次の重大度の高い推奨事項が得られます。「仮想マシンにエンドポイント保護ソリューションをインストールする」。

重大度の高い推奨事項の原因となっている問題を解決する必要があります。

あなたは何をするべきか？

1. VM1にマイクロソフトマルウェアの拡張を追加します。
2. VM1上のエンドポイント保護のために、Microsoft System Centerのセキュリティ管理パックをインストールします。
3. Network Watcher Agent for Windows拡張機能をVM1に追加します。
4. マイクロソフトディフェンダー高度な脅威防止にオンボードVM1（マイクロソフトディフェンダーATP）。

正解： *A*

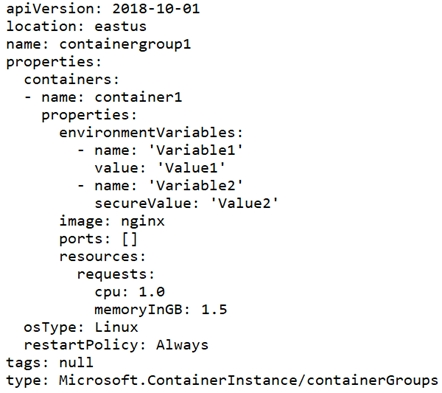
リファレンス：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection>

# Q.34

HOTSPOT -

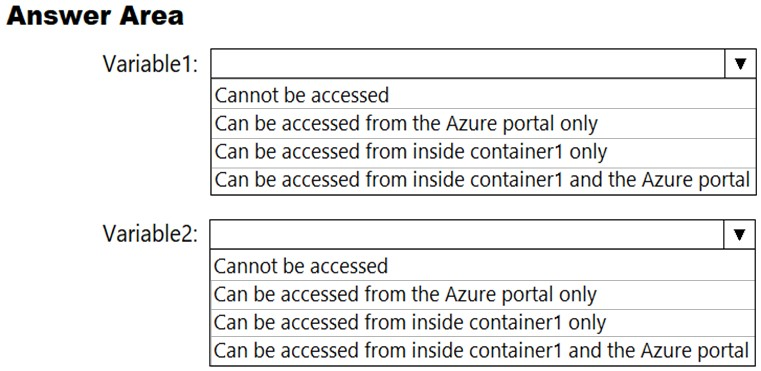
あなたは以下の内容が含まれていFile1.yamlという名前のファイルを持っています。

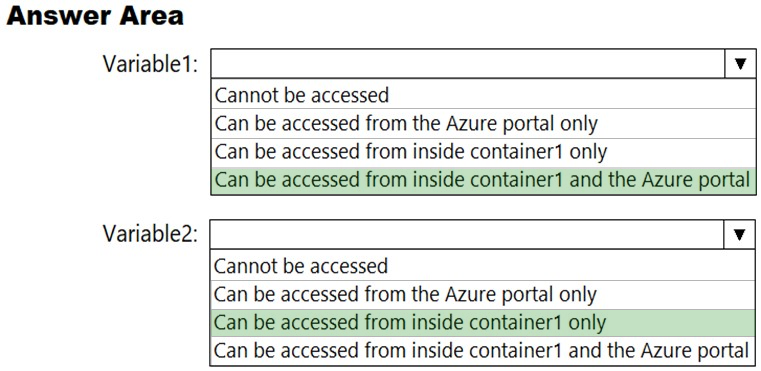


File1.yamlを使用して、container1という名前のAzureコンテナーインスタンスを作成します。

Variable1とVariable2の値にアクセスできる場所を特定する必要があります。

何を特定する必要がありますか？



正解： 

参照：

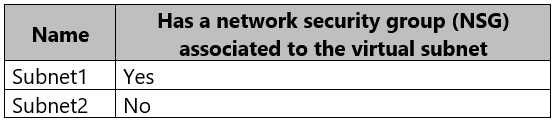
<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables>

Environment variables with secure values aren't visible in your container's properties--their values can be accessed only from within the container. For example, container properties viewed in the Azure portal or Azure CLI display only a secure variable's name, not its value.

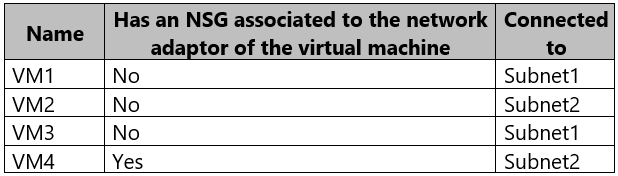
意訳：シークレット値は、コンテナ内からのみアクセスできます。

# Q.35

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。仮想ネットワークには、次の表に示すサブネットが含まれています。



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。



すべての仮想マシンに対してジャストインタイム（JIT）VMアクセスを有効にします。

JITによって保護されている仮想マシンを特定する必要があります。

どの仮想マシンを特定する必要がありますか？

1. VM4だけ
2. VM1とVM3のみ
3. VM1、VM3、およびVM4のみ
4. VM1、VM2、VM3、およびVM4

正解： *C*

NSGは、いずれかのVMレベルまたはサブネットレベルで、有効にする必要があります。

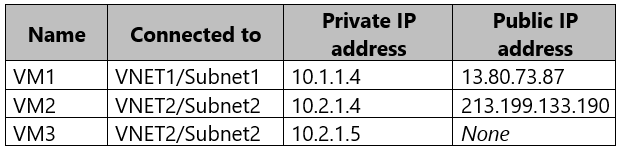
参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

# Q.36

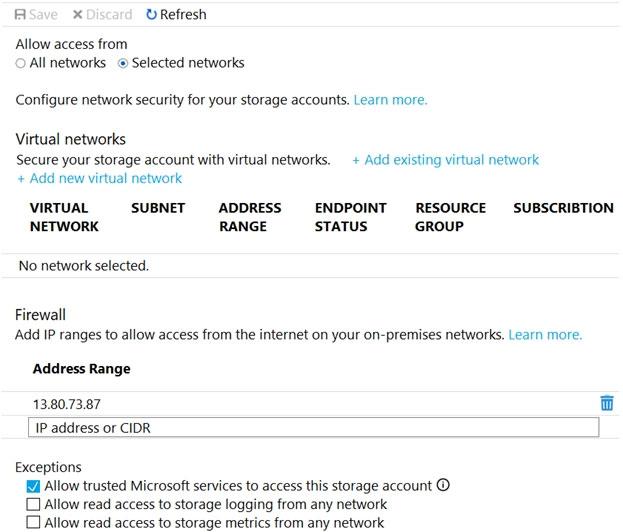
HOTSPOT-

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。

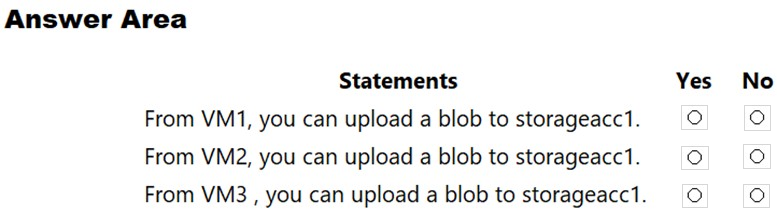


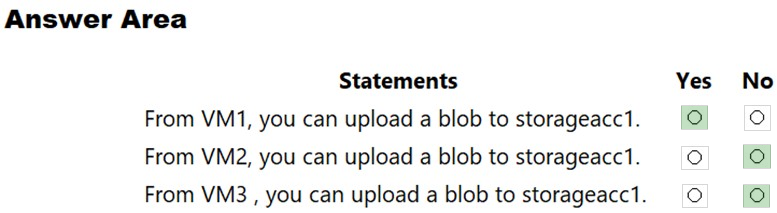
Subnet1とSubnet2には、Microsoft.Storageサービスエンドポイントが構成されています。

次の展示に示すように構成されたstorageacc1という名前のAzure Storageアカウントがあります。



次の各ステートメントで、ステートメントがtrueの場合は[はい]を選択します。それ以外の場合は、[いいえ]を選択します。



正解： 

ボックス1：はい

VM1のパブリックIPはファイアウォールの通過を許可されています。

ボックス2：いいえ-

許可された仮想ネットワークリストが空であるため、VM2はstorageacc1に直接アクセスできません。VM2のパブリックIPアドレスが許可されたIPリストにないため、VM2はインターネット経由でstorageacc1にアクセスできません。

ボックス3：いいえ-

許可された仮想ネットワークリストが空であるため、VM3はstorageacc1に直接アクセスできません。VM3にはパブリックIPアドレスがないため、インターネット経由でstorageacc1にアクセスできません。

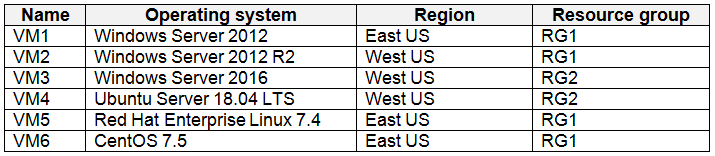
参照：

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

# Q.37

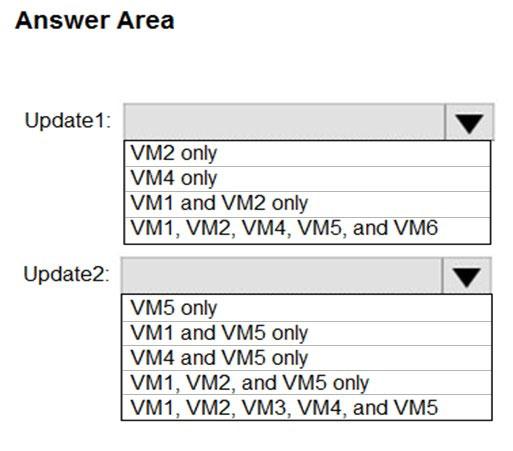
HOTSPOT-

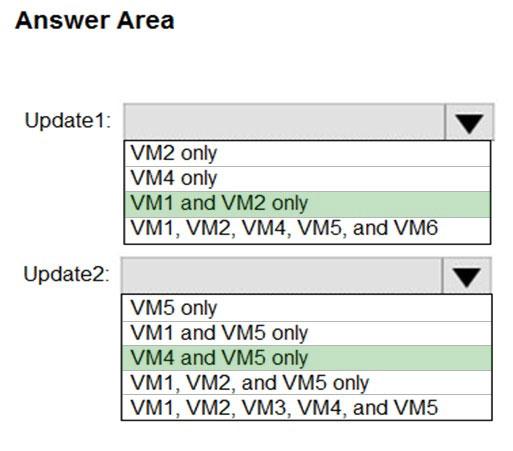
更新管理が有効になっているAzure仮想マシンがあります。仮想マシンは、次の表に示すように構成されています。



Update1とUpdate2という名前の2つの更新デプロイメントをスケジュールします。Update1はVM3を更新します。Update2はVM6を更新します。

Update1とUpdate2を使用して更新できる追加の仮想マシンはどれですか？回答するには、回答領域で適切なオプションを選択します。



正解： 

更新の展開は、WindowsVMまたはLinuxVMに適用できますが、両方に適用することはできません。VMは、さまざまなリージョン、さまざまなサブスクリプション、さまざまなリソースグループに配置できます。

アップデート1：VM1とVM2のみ-

VM3：Windows Serverの2016年

アップデート2：VM4及びVM5のみ-

VM6：CentOSの7.5。

Linuxの場合、マシンは更新リポジトリにアクセスできる必要があります。更新リポジトリはプライベートまたはパブリックにすることができます。

参照：

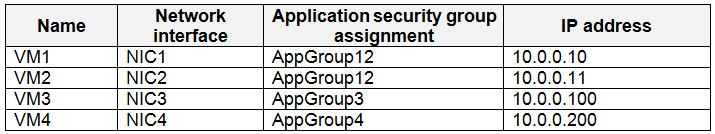
<https://docs.microsoft.com/en-us/azure/automation/update-management/overview>

# Q.38

HOTSPOT-

Sub1という名前のAzureサブスクリプションがあります。

1つのサブネットを含む仮想ネットワークを作成します。サブネット上で、次の表に示す仮想マシンをプロビジョニングします。



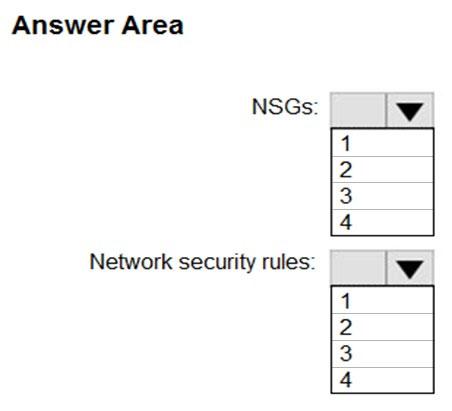
現在、ネットワークセキュリティグループ（NSG）はプロビジョニングされていません。

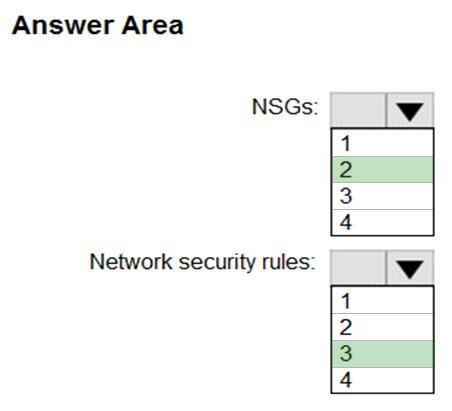
次の要件を満たすには、ネットワークセキュリティを実装する必要があります。

* VM3からVM4へのトラフィックのみを許可します。
* インターネットからVM1およびVM2へのトラフィックのみを許可します。
* NSGとネットワークセキュリティルールの数を最小限に抑えます。

NSGとネットワークセキュリティルールをいくつ作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。



正解： 

NSG：2

ネットワークセキュリティルール：3

2ではないセキュリティルールで複数のサービスタグまたはアプリケーショングループを指定することはできません。

参照：

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

# Q.39

HOTSPOT-

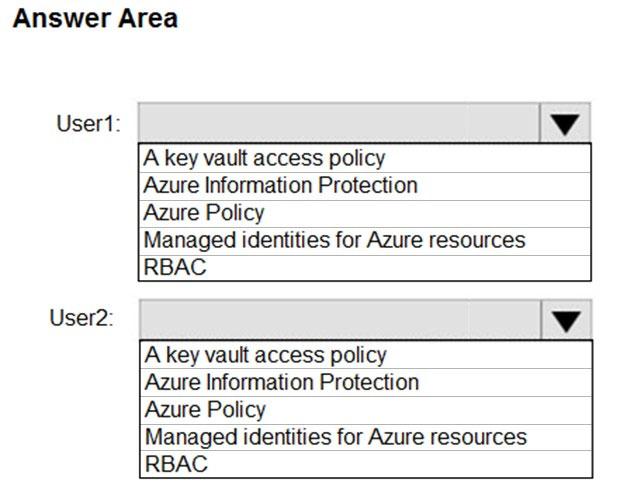
Azureキーボールトがあります。

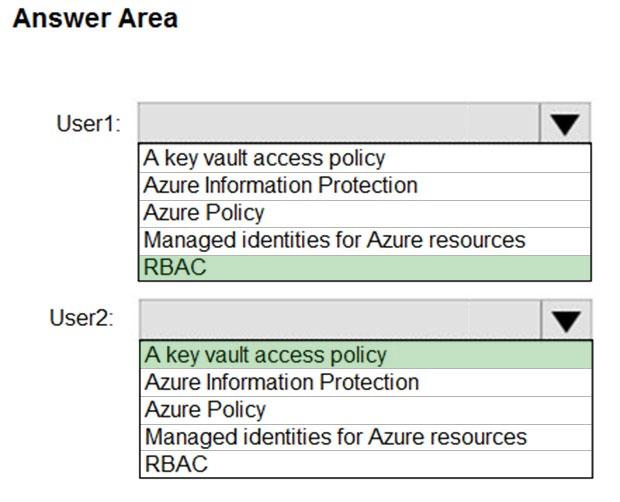
次の要件を満たすには、キーボールトへの管理アクセスを委任する必要があります。

* User1という名前のユーザーに、キーボールトの高度なアクセスポリシーを設定する機能を提供します。
* User2という名前のユーザーに、キーボールトで証明書を追加および削除する機能を提供します。
* 最小特権の原則を使用します。

各ユーザーにアクセス権を割り当てるには、何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ます。



正解： 

ユーザー1 ：RBAC

RBACは、管理プレーンのKeyVaultアクセス制御メカニズムとして使用されます。これにより、適切なIDを持つユーザーは次のことができるようになります。

* KeyVaultアクセスポリシーの設定
* KeyVaultの作成、読み取り、更新、削除
* KeyVaultタグの設定

注：ロールベースのアクセス制御（RBAC）は、詳細な機能を提供するシステムです。 Azureリソースのきめ細かいアクセス管理。RBACを使用すると、チーム内の職務を分離し、ユーザーがジョブを実行するために必要なアクセス量のみをユーザーに許可できます。

User2：Key Vault Access Policy

キーボールトアクセスポリシーは、キーボールトデータプレーンへのアクセスを取得するためのアクセス制御メカニズムです。Key Vaultアクセスポリシーは、キー、シークレット、および証明書に個別にアクセス許可を付与します。

参照：

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

# Q.40

Azure仮想マシンのデプロイに使用するAzure Resource Managerテンプレートがあります。

仮想マシンのインスタンスがプロビジョニングされるため、未使用のWindows機能を自動的に無効にする必要があります。

何を使うべきですか？

1. Microsoft Intuneのデバイスコンプライアンスポリシー
2. Azure Automationの状態構成
3. アプリケーションセキュリティグループ
4. Azure Advisor

正解： *B*

**Azure Automation State Configurationを使用して、Azure VM（ClassicとResource Managerの両方）、オンプレミスVM、Linuxマシン、AWS VM、およびオンプレミス物理マシンを管理できます。**

注：Azure Automation State Configurationは、Windows Feature DSCサービスと同様のDSCプルサーバーを提供するため、ターゲットノードは自動的に構成を受け取り、目的の状態に準拠しレポートします。

Azure Automationに組み込まれているプルサーバーを使用すると、独自のプルサーバーをセットアップして維持する必要がなくなります。

Azure Automationは、クラウドまたはオンプレミスの仮想または物理のWindowsまたはLinuxマシンをターゲットにできます。

# Q.41

Azure Security Centerから、Registry1のイメージのAzure Container Registry脆弱性スキャンを有効にします。

次のアクションを実行します。

* Image1という名前のWindowsイメージをRegistry1にプッシュします。
* Image2という名前のLinuxイメージをRegistry1にプッシュします。
* Image3という名前のWindowsイメージをRegistry1にプッシュします。
* Image1を変更し、新しいイメージをImage4としてRegistry1にプッシュします。
* Image2を変更し、新しいイメージをImage5としてRegistry1にプッシュします。

脆弱性についてスキャンされる2つの画像はどれですか？

それぞれの正解は完全な解決策を提示します。

1. Image4
2. Image2
3. Image1
4. Image3
5. Image5

正解： *B, E*

Linuxイメージのみがスキャンされます。Windowsイメージはスキャンされません。

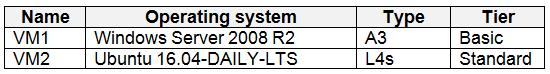
参照：

<https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration>

# Q.42 質問が不完全で正しくない

HOTSPOT-

次の表に示すように、米国東部2リージョンに2台のAzure仮想マシンがあります。

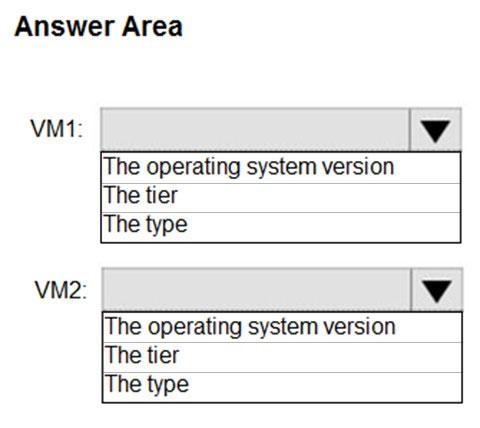


Azure Key ボールトをデプロイして構成します。

VM1とVM2でAzure Disk Encryptionを有効にできることを確認する必要があります。

各仮想マシンで何を変更する必要がありますか？

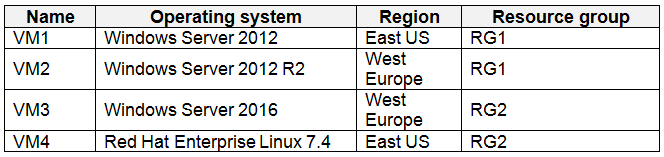
回答するには、回答領域で適切なオプションを選択します。



VM1は type:A3、Tier:Basicで両方ともsupportされていない。

# Q.43

次の表に示すAzure仮想マシンがあります。



米国東部リージョンのRG1にAnalytics1という名前のAzure Log Analyticsワークスペースを作成します。

Analytics1に登録できる仮想マシンはどれですか？

1. VM1だけ
2. VM1、VM2、およびVM3のみ
3. VM1、VM2、VM3、およびVM4
4. VM1とVM4のみ

正解： *A*

注：ワークスペースを作成する

* Azureポータルで、[すべてのサービス]をクリックします。リソースのリストに、「Log Analytics」と入力します。入力を開始すると、入力に基づいてリストがフィルタリングされます。Log Analyticsを選択します。

[作成]をクリックして、次の項目の選択肢を選択します。

Default LA Workspaceなどの新しいLog Analyticsワークスペースの名前を指定します。OMSワークスペースは、Log Analyticsワークスペースと呼ばれるようになりました。

選択したデフォルトが適切でない場合は、ドロップダウンリストから選択して、リンクするサブスクリプションを選択します。

[リソースグループ]で、1つ以上のAzure仮想マシンを含む既存のリソースグループを選択します。

VMがデプロイされている場所を選択します。詳細については、Log Analyticsが利用可能な地域を参照してください。

不正解：

B、C：Log Analyticsワークスペースは、データストレージの地理的な場所を提供します。VM2とVM3は別の場所にあります。

D：VM4は別のリソースグループです。

参照：

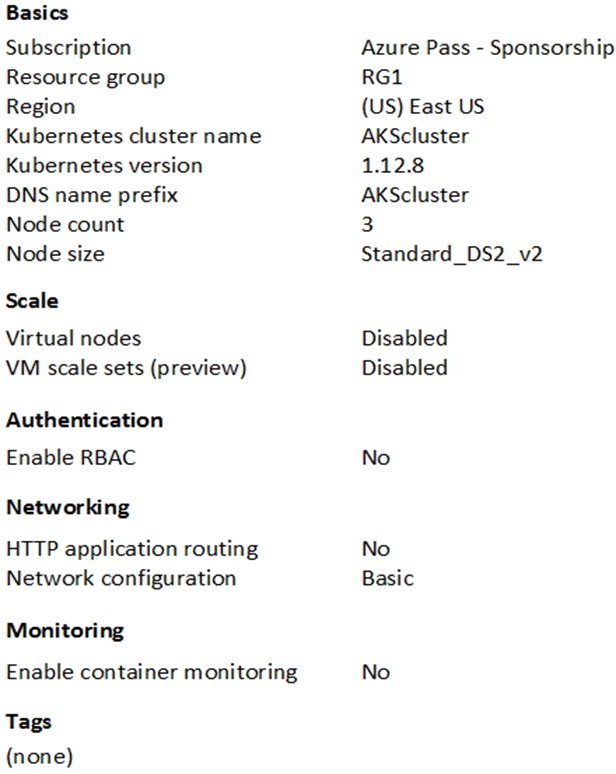
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

議論

全てのVMが対象との考えもあり、私もそこに賛成する。

# Q.44

Azure Kubernetes Service（AKS）クラスターをテストしています。クラスターは、展示に示されているように構成されています。（[Exhibit]タブをクリックします。）



クラスターを実稼働環境にデプロイすることを計画しています。

HTTPアプリケーションルーティングを無効にします。

単一のIPアドレスを使用して、AKSサービスにリバースプロキシとTLSターミネーションを提供するアプリケーションルーティングを実装する必要があります。

あなたは何をするべきか？

1. AKS Ingressコントローラーを作成します。
2. コンテナネットワークインターフェイス（CNI）プラグインをインストールします。
3. Azureの標準的なロードバランサを作成します。
4. Azure Basic Load Balancerを作成します。

正解： *A*

入力コントローラはKubernetesサービスのリバースプロキシ、設定トラフィックルーティング、およびTLS終端を提供するソフトウェアの一部です。

参照：

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

# Q.45

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サブスクリプションがあります。サブスクリプションには、Windows Server 2012 R2または Windows Server 2016 を実行する50台の仮想マシンが含まれています。仮想マシンにMicrosoft Antimalwareを展開する必要があります。

解決策：各仮想マシンに拡張機能を追加します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *A*

Visual Studioを使用して、Microsoft Antimalwareサービスを有効にして構成できます。これには、[インストールされている拡張機能]の下のドロップダウンリストからMicrosoft Antimalware拡張機能を選択し、[追加]をクリックしてデフォルトのマルウェア対策構成で構成する必要があります。

参照：

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

# Q.46

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サブスクリプションがあります。サブスクリプションには、Windows Server 2012R2または

WindowsServer2016を実行する50台の仮想マシンが含まれています。仮想マシンにMicrosoftAntimalwareを展開する必要があります。

解決策：各仮想マシンに接続し、Windows機能を追加します。

これは目標を達成していますか？

1. はい
2. いいえ

正解： *B*

Microsoft Antimalwareは、**機能ではなく拡張機能**として展開されます。

参照：

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

# Q.47

Contoso.comという名前のAzureActive Directory（Azure AD）テナントとAzure Kubernetes Service（AKS）クラスターAKS1があります。

Contoso.comのアカウントを使用してAKS1にアクセスできないことがわかりました。

Contoso.comのアカウントを使用してAKS1にアクセス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、管理作業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？

1. AKS1 を再作成する。
2. AKS1 から、Kubernetesのバージョンをアップグレードします。
3. Azure ADから、Azure AD Premiumを実装します。
4. Azure ADから、ユーザー設定を構成します。

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

# Q.48

Registry1という名前のAzure Container Registry を含むAzureサブスクリプションがあります。サブスクリプションは、Azure Security Centerの標準使用層を使用します。

複数のコンテナイメージをRegister1にアップロードします。

脆弱性セキュリティスキャンが実行されなかったことがわかりました。

Registry1にアップロードするときに、imageの脆弱性がスキャンされてい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？

1. Azureポータルから、料金階層の設定を変更します。
2. Azure CLIから、コンテナーイメージをロックします。
3. AzCopyを使用して、コンテナイメージをアップロードする。
4. ドッカーを使用してRegistry1にコンテナイメージをプッシュ

正解： *A*

リファレンス：

<https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/>

# Q.49

Azure Security Centerから、カスタムアラートルールを作成します。

アラートがトリガーされたときに電子メールメッセージを受信するユーザーを構成する必要があります。

あなたは何をするべきか？

1. Azure Monitorから、アクショングループを作成します。
2. セキュリティセンターから、Azureサブスクリプションのセキュリティポリシー設定を変更します。
3. Azure Active Directory（Azure AD）から、セキュリティリーダーロールグループのメンバーを変更します。
4. セキュリティセンターから、アラートルールを変更します。

正解： *A*

リファレンス：

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

# Q.50

ネットワーク環境を構成して保護しています。

ネットワークトラフィックを分析するように構成されたVM1という名前のAzure仮想マシンをデプロイします。

すべてのネットワークトラフィックがVM1を介してルーティングされていることを確認する必要があります。

何を設定する必要がありますか？

1. システムルート
2. ネットワークセキュリティグループ（NSG）
3. ユーザー定義のルート

正解： *C*

システムルートを使用すると、展開のトラフィックが自動的に促進されますが、仮想アプライアンスを介したパケットのルーティングを制御したい場合があります。これを行うには、特定のサブネットに流れるパケットが代わりに仮想アプライアンスに送られるネクストホップを指定するユーザー定義ルートを作成し、仮想アプライアンスとして実行されているVMのIP転送を有効にします。

ユーザー定義ルート

ほとんどの環境では、Azureによって既に定義されているシステムルートのみが必要です。ただし、次のような特定の場合には、ルートテーブルを作成し、1つ以上のルートを追加する必要がある場合があります。

* オンプレミスネットワークを介してインターネットへのトンネリングを強制します。
* Azure環境での仮想アプライアンスの使用。
* 上記のシナリオでは、ルートテーブルを作成し、それにユーザー定義のルートを追加する必要があります。

参照：

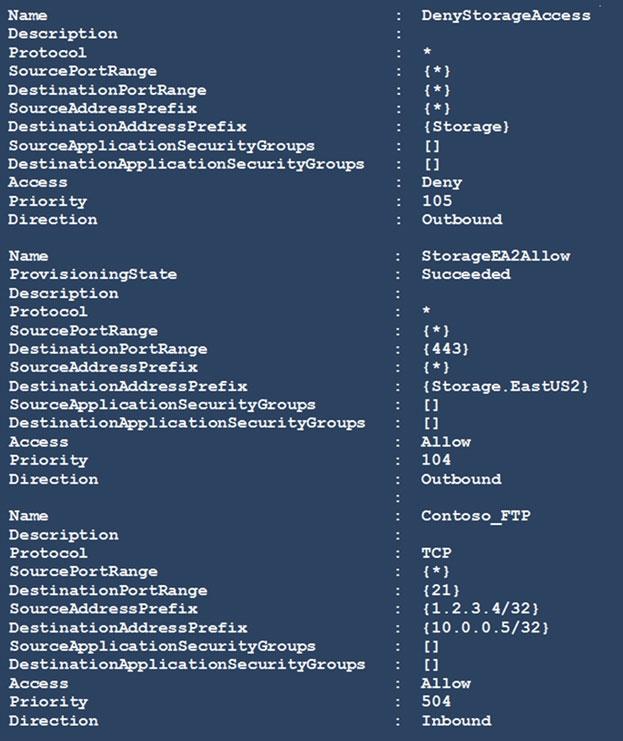
<https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md>

# Q.51

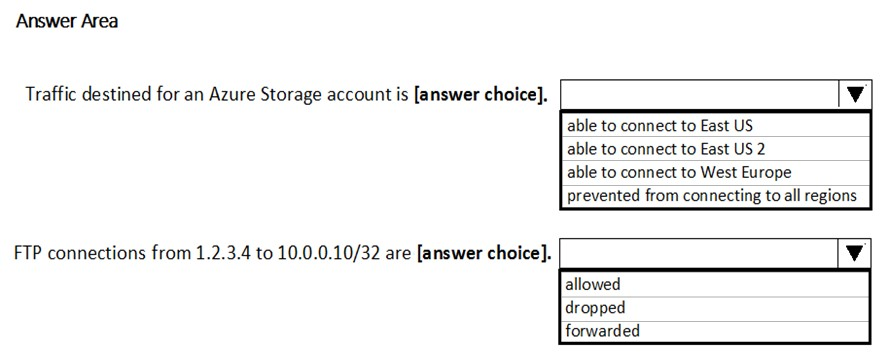
HOTSPOT-

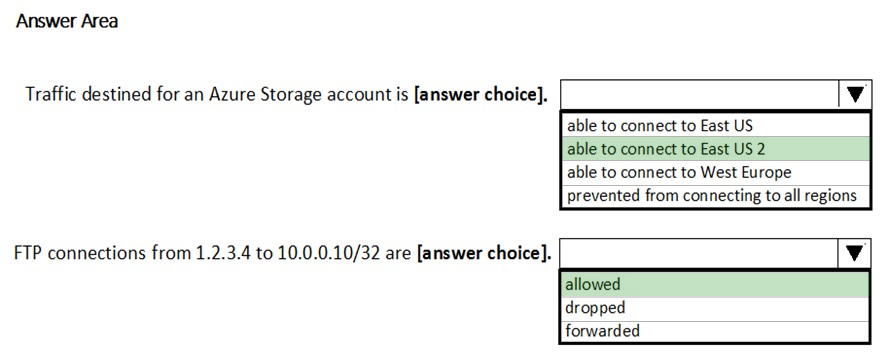
Azureサブネットにバインドされたネットワークセキュリティグループ（NSG）があります。

Get-AzNetworkSecurityRuleConfigを実行すると、次の展示に示す出力が表示されます。



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ステートメントを完了する回答の選択肢を選択します。



正解： 

ボックス1：East US 2

US2に接続可能StorageEA2AllowにはDestination Address Prefix {Storage / EastUS2}があります

ボックス2：allowed

ポート21がFTPセッションを制御します。Contoso\_FTPにはSourceAddressPrefix {1.2.3.4/32}とDestinationAddressPrefix {10.0.0.5/32}があ​​ります。

注：

Get-AzureRmNetworkSecurityRuleConfigコマンドレットは、Azureネットワークセキュリティグループのネットワークセキュリティルール構成を取得します。

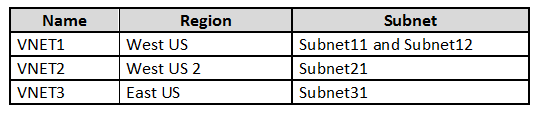
ネットワークセキュリティグループのセキュリティルールを使用すると、仮想ネットワークサブネットおよびネットワークインターフェイスに出入りできるネットワークトラフィックの種類をフィルタリングできます。

参照：

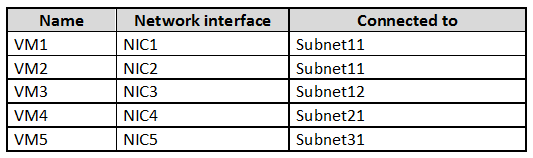
<https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group>

# Q.52

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。



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。



NIC1では、ASG1という名前のアプリケーションセキュリティグループを構成します。

他のどのネットワークインターフェイスでASG1を構成できますか？

1. NIC2のみ
2. NIC2、NIC3、NIC4、およびNIC5
3. NIC2とNIC3のみ
4. NIC2、NIC3、およびNIC4のみ

正解： *C*

アプリケーションセキュリティグループに割り当てられたすべてのネットワークインターフェイスは、アプリケーションに割り当てられた最初のネットワークインターフェイスと同じ仮想ネットワークに存在する必要があるため、Subnet11とSubnet12で構成されるNVET1のネットワークインターフェイスのみをASG1で構成できます。セキュリティグループが参加しています。

参照：

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

# Q.53

RG1という名前のリソースグループに15台のAzure仮想マシンがあります。

すべての仮想マシンは同一のアプリケーションを実行します。

許可されていないアプリケーションやマルウェアが仮想マシンで実行されないようにする必要があります。

あなたは何をするべきか？

1. RG1にAzureのポリシーを適用します。
2. Azure Security Centerから、アダプティブアプリケーションコントロールを構成します。
3. Azure Active Directory（Azure AD）ID保護を構成します。
4. RG1にリソースロックを適用します。

正解： *B*

**アダプティブアプリケーション制御は、Azure Security Centerのインテリジェントな自動化されたエンドツーエンドのアプリケーションホワイトリストソリューションです。**これは、AzureおよびAzure以外のVM（WindowsおよびLinux）で実行できるアプリケーションを制御するのに役立ちます。これは、他の利点の中でも、マルウェアに対してVMを強化するのに役立ちます。

Security Centerは、機械学習を使用してVMで実行されているアプリケーションを分析し、このインテリジェンスを使用して特定のホワイトリストルールを適用するのに役立ちます。

参照：

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application>

# Q.54

https://www.contoso.comのURLを使用してアクセスされるオンプレミスサーバーでホストされているWebアプリがあります。

WebアプリをAzureに移行することを計画しています。引き続きhttps://www.contoso.comを使用します。

Azure WebアプリでHTTPSを有効にする必要があります。

あなたは最初に何をすべきですか？

1. オンプレミスサーバーから公開鍵をエクスポートし、その鍵をP7bファイルとして保存します。
2. オンプレミスサーバーから秘密鍵をエクスポートし、TripleDESを使用して暗号化されたPFXファイルとして鍵を保存します。
3. オンプレミスサーバーから公開鍵をエクスポートし、CERファイルとして保存します。
4. オンプレミスサーバーから秘密鍵をエクスポートし、AES256を使用して暗号化されたPFXファイルとして鍵を保存します。

正解： *B*

リファレンス：

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements>

# Q.55

Azureコンテナインスタンスをデプロイすることを計画しています。

クレジットカードを検証するコンテナ化されたアプリケーションがあります。アプリケーションは、アプリケーションコンテナと検証コンテナの2つのコンテナで構成されています。

アプリケーションコンテナは、検証コンテナによって監視されます。検証コンテナは、アプリケーションコンテナにリクエストを送信し、トランザクションごとに応答を待つことで、セキュリティチェックを実行します。

アプリケーションコンテナと検証コンテナが一緒にデプロイされるようにスケジュールされていることを確認する必要があります。コンテナは、外部に公開されていないポートでのみ相互に通信する必要があります。

展開には何を含める必要がありますか？

1. アプリケーションセキュリティグループ
2. ネットワークセキュリティグループ（NSG）
3. 管理グループ
4. コンテナグループ

正解： *D*

Azure Container Instancesは、**コンテナーグループを使用した単一のホストへの複数のコンテナーのデプロイをサポート**しています。コンテナグループは、ログ記録、監視、またはサービスに2番目の接続プロセスが必要なその他の構成用のアプリケーションサイドカーを構築するときに役立ちます。

参照：

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

# Q.56

DRAGのDROP -

あなたがVNET1とVNET2という名前の2つのAzure仮想ネットワークのためのネットワーク接続を構成しています。

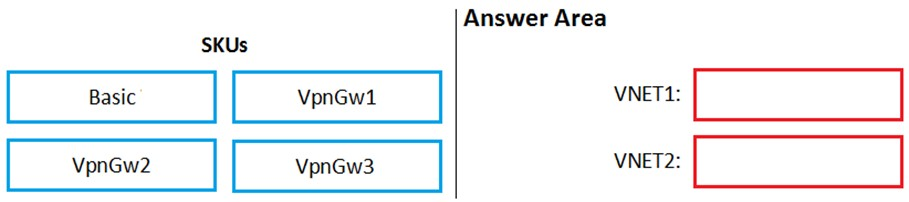
次の要件を満たすには、仮想ネットワークにVPNゲートウェイを実装する必要があります。

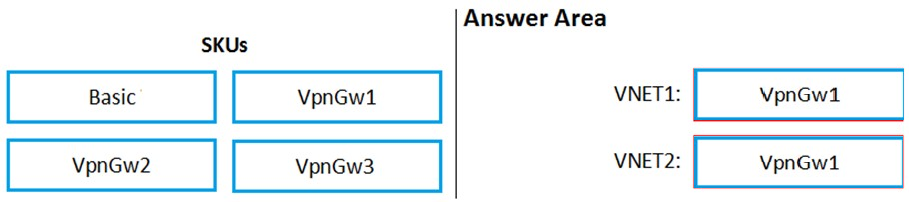
* VNET1には、BGPを使用する6つのサイト間接続が必要です。
* VNET2には、BGPを使用する12のサイト間接続が必要です。
* コストを最小限に抑える必要があります。

仮想ネットワークごとにどのVPNゲートウェイSKUを使用する必要がありますか？回答するには、適切なSKUを正しいネットワークにドラッグします。

各SKU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、分割バーをペイン間でドラッグするか、スクロールする必要がある場合があります。

選択して配置：



正解： 

参照：

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

# Q.57

Azureサブスクリプションのリソースへのアクセスを保護しています。

新しい会社のポリシーでは、サブスクリプション内のすべてのAzure仮想マシンはマネージドディスクを使用する必要があると規定されています。

ユーザーがアンマネージディスクを使用する仮想マシンを作成できないようにする必要があります。

何を使うべきですか？

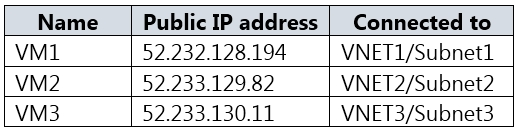
1. Azure Monitor
2. Azure policy
3. Azure Security Center
4. Azure Service Health

正解：B　Azure Policy

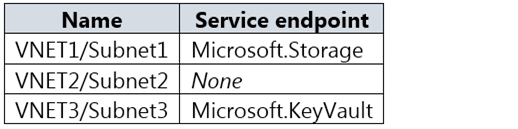
# Q.58

HOTSPOT-

storage1という名前のストレージアカウントと複数の仮想マシンを含むAzureサブスクリプションがあります。ストレージアカウントと仮想マシンは同じAzureリージョンにあります。次の表に、仮想マシンのネットワーク構成を示します。



仮想ネットワークサブネットには、次の表に示すように定義されたサービスエンドポイントがあります。

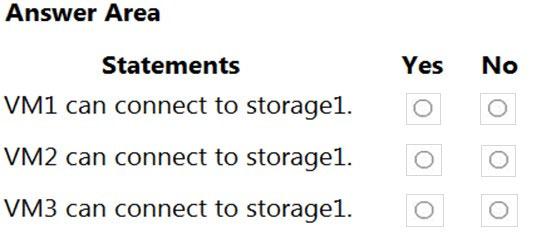


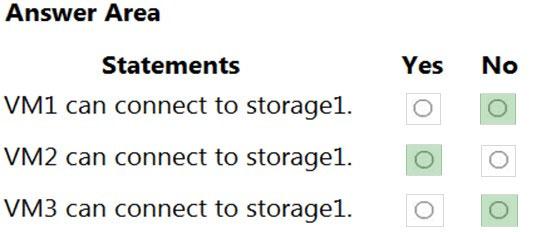
storage1に対して、次のファイアウォールと仮想ネットワークの設定を構成します。

* アクセスを許可する場所：選択したネットワーク
* 仮想ネットワーク：VNET3 \サブネット3
* ファイアウォール"アドレス範囲：52.233.129.0/24

次の各ステートメントで、ステートメントの場合は[はい]を選択します。

それ以外の場合は、[いいえ]を選択します。



正解： 

ボックス1：No

VNet1には、AzureStorage用に構成されたサービスエンドポイントがあります。ただし、Azureストレージは、VNet1またはVM1のパブリックIPアドレスからのアクセスを許可しません。

ボックス2：Yes

-VNet2にはサービスエンドポイントが構成されていません。ただし、Azureストレージでは、VM2のパブリックIPアドレスからのアクセスが許可されます。

ボックス3：No

-AzureストレージはVNet3からのアクセスを許可します。ただし、VNet3にはAzureストレージ用のサービスエンドポイントがありません。Azureストレージは、VM3のパブリックIPからのアクセスも許可しません。

# Q.59

AzureサブスクリプションでAzure Kubernetes Service（AKS）クラスターを作成することを計画しています。

登録サーバーアプリケーションのマニフェストを以下の展示に示します。



AKSクラスターとAzure Active Directory（Azure AD）が統合されていることを確認する必要があります。

マニフェストでどのプロパティを変更する必要がありますか？

1. accessTokenAcceptedVersion
2. keyCredentials
3. groupMembershipClaims
4. acceptMappedClaims

正解： *C*

Reference:

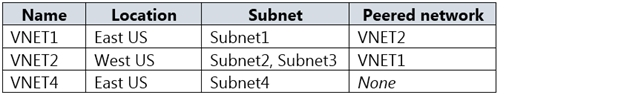
<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

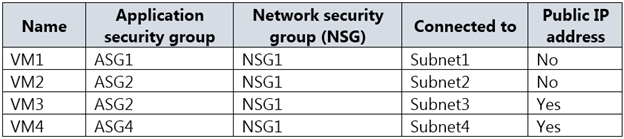
# Q.60

HOTSPOT-

次の表に示すAzure仮想ネットワークがあります。



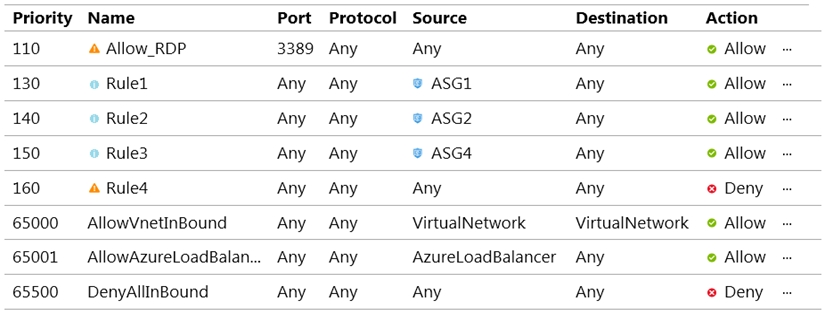
次の表に示すAzure仮想マシンがあります。



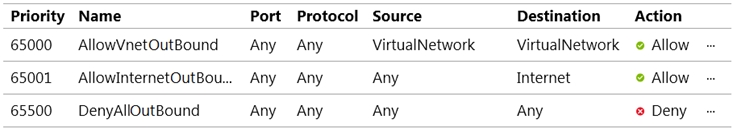
すべての仮想マシンのファイアウォールは、pingトラフィックを許可します。

NSG1は、次の展示に示すように構成されています。

インバウンドセキュリティルール-

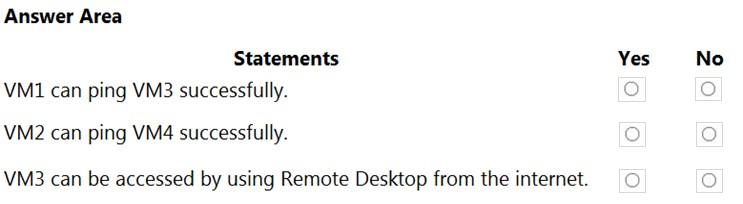


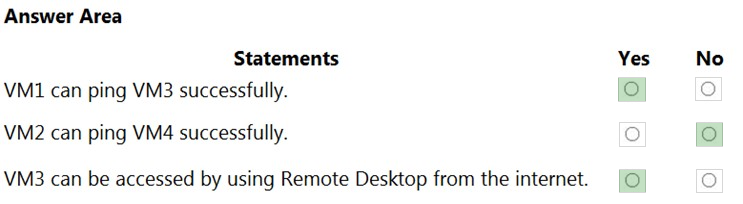
アウトバウンドセキュリティルール-



次の各ステートメントで、ステートメントがtrueの場合は[はい]を選択します。

それ以外の場合は、[いいえ]を選択します。



正解： 

ボックス1：Yes

-VM1とVM3はピアリングされたVNet上にあります。

ASG1およびASG2のソースを持つファイアウォールルールは、「任意の」プロトコルで「任意の」トラフィックを許可するため、VM1とVM3の間でpingが許可されます。

ボックス2：No

-VM2とVM4は別々のVNet上にあり、VNetはピアリングされていません。

したがって、pingはインターネット経由で送信する必要があります。

VM4にはパブリックIPがあり、ファイアウォールはpingを許可します。ただし、VM2がVM4にpingを実行できるようにするには、VM2にもパブリックIPアドレスが必要です。**Azureでは、pingは物理ネットワークの場合のようにデフォルトゲートウェイを経由しません。**Azure VMが外部IPにpingを実行するには、VMにパブリックIPアドレスが割り当てられている必要があります。

ボックス3：No

-VM3にはパブリックIPアドレスがあり、ファイアウォールはポート3389でのトラフィックを許可します。

セキュリティ操作を管理します