NO.1Azureサブスクリプションがあります。
100台のAzure仮想マシンがあります。
より安価な製品に変更できる、十分に活用されていない仮想マシンをすばやく特定する必要があります。

どのウェイドを使うべきですか？
A.カスタマーインサイトB.アド
バイザー
C.モニター
D.メトリクス
回答： Bリファレ
ンス :https：//
docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations

NO.2aks1という名前のAzureKubernetes Service（AKS)クラスターがあります。
aks1でクラスターオートスケーラーを有効にする必要があります。
Azure CLIで実行する必要があるコマンドはどれですか？
A.kubecclオートスケール
B.kubectlが適用されます
C. azaksスケール
D. az ales update回
答： D
リファレンス：
https://docs.microsoft.com/en-us/azure/aks/cluster-autoscaler#create-an-aks-cluster-and-enable the-cluster-autoscaler

NO.3Subnet1という名前のサブネットを含むAzure仮想ネットワークがあります。 Subnet1には50台の仮想マシンが含まれています。 25台の仮想マシンはWebサーバーであり、他の25台はアプリケーションサーバーです。

アプリケーションセキュリティを使用して、Webサーバーとアプリケーションサーバーのトラフィックをフィルタリングする必要があります
グループ。
どの追加リソースをプロビジョニングする必要がありますか？
A.Azureプライベートリンク
B.ネットワークセキュリティグループ（NSG）
C.Azure-ファイアウォール
D.ユーザー定義のルート
回答： B
説明 :アプリケー
ションセキュリティグループを使用すると、ネットワークセキュリティをアプリケーションの構造の自然な拡張として構成できるため、仮想マシンをグループ化し、それらのグループに基づいてネットワークセキュリティポリシーを定義できます。

ネットワークセキュリティグループを使用して、仮想ネットワークサブネットとの間で送受信されるネットワークトラフィックをフィルタリングできます。

リファレンス：
https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic

NO.4あなたは中国語で音声をテキストに書き写すアプリを作成しています。アプリはAzureのSpeechサービスを使用し、サービスプリンシパルを使用して認証します。サービスプリンシパルのアプリケーションIDとクライアントシークレットを使用するようにアプリを構成します。Speechサービスに対して認証するために、他にどの値をアプリに追加する必要がありますか？

A.サブスクリプション

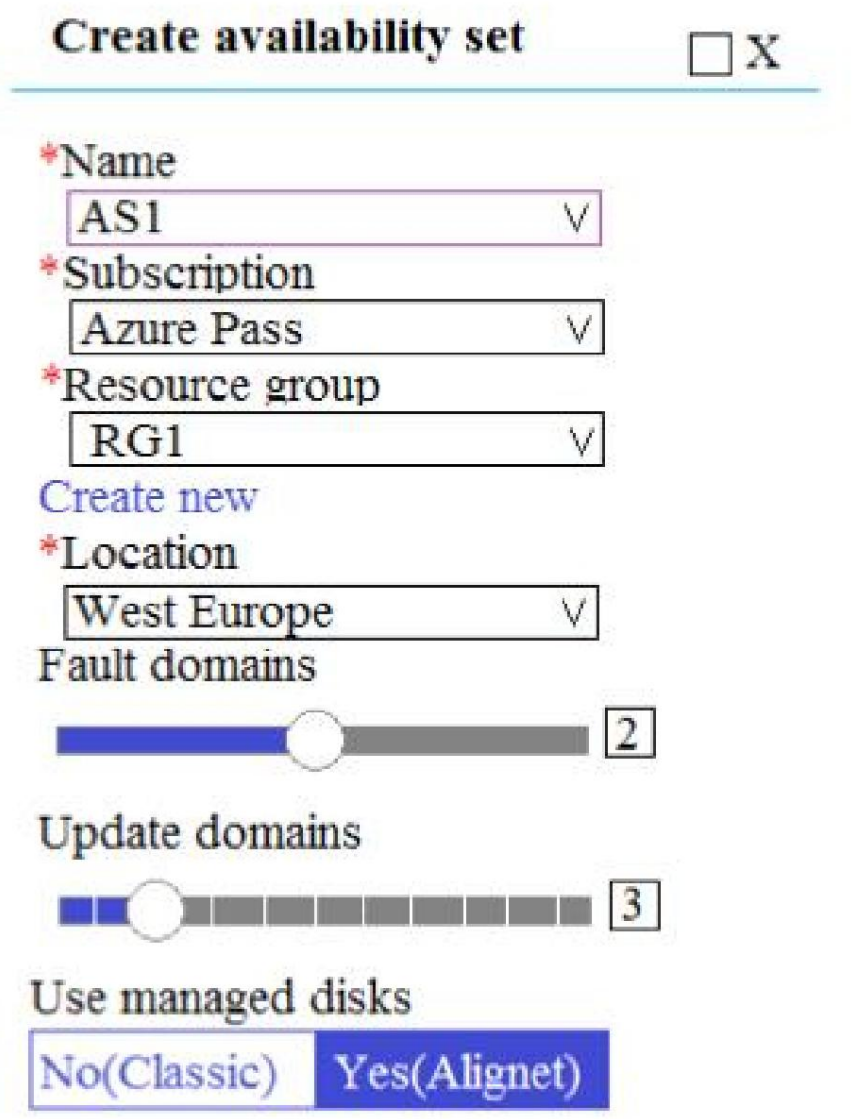
IDB 。リソースグループIDC 。

テナントID

D.アプリケーション名回

答： B

NO.5複数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。次の展示に示すように、可用性セットを作成します。



AS1に10台の仮想マシンをデプロイします。

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ステートメントを完了する回答の選択肢を選択します。

注 :正しい選択はそれぞれ1ポイントの価値があります。

During planned maintenance, at least **[answer choice]** [4 / 5 / 6 / 8] virtual machines will be available.

To add another virtual machines to AS1, the virtual machines must'be added to **[answer choice].** [any region and the RG1 resource group / the West Europe region and any resource group / the West Europe region and the RG1 resource group]

答え：

During planned maintenance, at least **[answer choice]** [4 / 5 / **6** / 8] virtual machines will be available.

To add another virtual machines to AS1, the virtual machines must'be added to **[answer choice].** [any region and the RG1 resource group / the West Europe region and any resource group / **the West Europe region and the RG1 resource group**]

リファレンス：

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/regions-and-availability

NO.6Subscription1という名前のAzureサブスクリプションがあります。

Subscription1には、次の表の仮想マシンが含まれています。

Name	IP address
VM1	10.0.1.4
VM2	10.0.2.4
VM3	10.0.3.4

Subscription1には、次の表のサブネットを持つVNet1という名前の仮想ネットワークが含まれています。

Name	Address space	Connected virtual machine
Subnet1	10.0.1.0/24	VM1
Subnet2	10.0.2.0/24	VM2
Subnet3	10.0.3.0/24	VM3

VM3には、NIC3という名前のネットワークアダプタを含む複数のネットワークアダプタがあります。 NIC3でIP転送が有効になっています。ルーティングはVM3で有効になっています。

次のテーブルのルーターを含むRT1という名前のルートテーブルを作成します。

Address prefix	Next hop type	Next hop address
10.0.1.0/24	Virtual appliance	10.0.3.4
10.0.2.0/24	Virtual appliance	10.0.3.4

RT1をSubnet1とSubnet2に適用します。

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。

注 :正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
VM3 can establish a network connection to VM1.	○	○
If VM3 is turned off, VM2 can establish a network connection to VM1.	○	○
VM1 can establish a network connection to VM2.	○	○

答え：

Statements	Yes	No
VM3 can establish a network connection to VM1.	○	○
If VM3 is turned off, VM2 can establish a network connection to VM1.	○	○
VM1 can establish a network connection to VM2.	○	○

参照 :https：//

docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview https://www.quora.com/What-is-IP-forwarding

NO.7

Name	IP address range
Subnet0	10.0.0.0/24
Subnet1	10.0.1.0/24
Subnet2	10.0.2.0/24
GatewaySubnet	10.0.254.0/24

Subnet1には、ルーターとして動作するVM1という名前の仮想アプライアンスが含まれています。

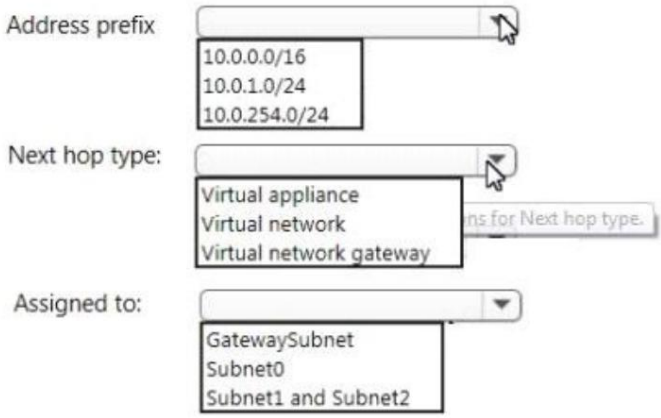
RT1という名前のルーティングテーブルを作成します。

すべてのインバウンドトラフィックをVM1を介してVNet1にルーティングする必要があります。

RT1をどのように構成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。

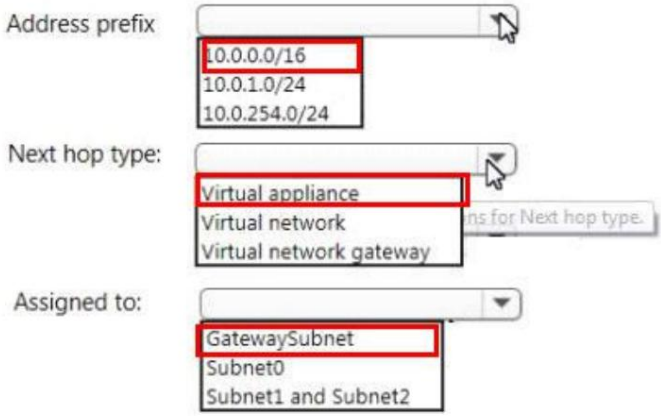
VNet1という名前の仮想ネットワークを含むAzureサブスクリプションがあります。 VNet1は10.0.0.0/16のIPアドレス空間を使用し、次の表のサブネットを含みます。

Answer Area

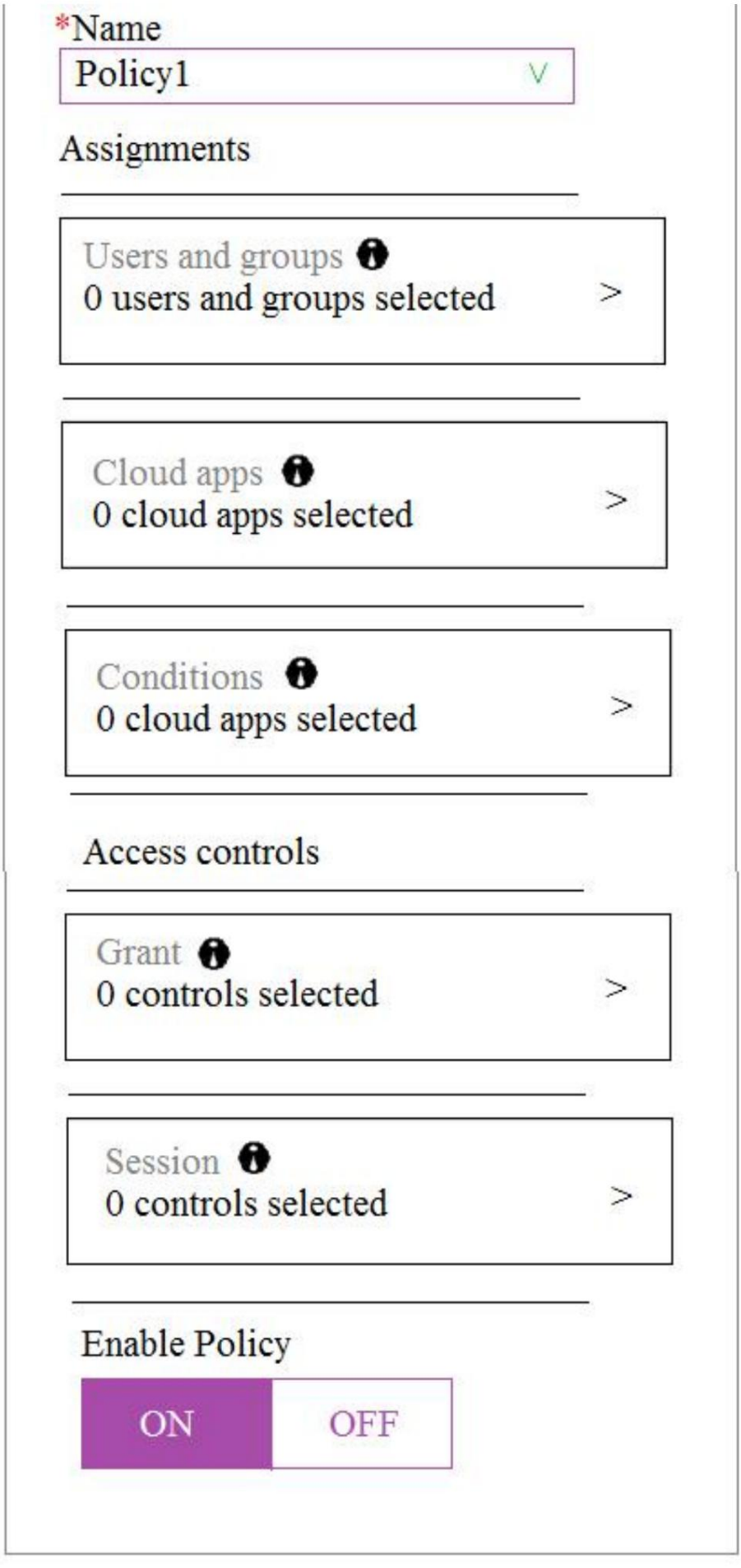


答え：

Answer Area



NO.8 Azure Active Directory（Azure AD)テナントがあります。
すべてのユーザーがAzureポータルにアクセスするときに多要素認証を使用することを要求する条件付きアクセスポリシーを作成する必要があります。
どの3つの設定を構成する必要がありますか ?答えるには、答えに適切な設定を選択してください
範囲。
注 :正しい選択はそれぞれ1ポイントの価値があります。



答え：

NO.9 AzureMonitorを使用してAzure仮想マシンを監視します。
CPU使用率が30分を超えて95％を超えたときに、仮想マシンを再起動することを計画しています。

仮想マシンを再起動するには、AzureMonitorでアラートを作成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ます。

アラートではどのタイプのアクションを使用する必要がありますか？
A. Webhook

B.ロジックアプリ
C.ITSM
D.自動化ランブック
回答： D
説明：自動化
Runbookを使用すると、VMの再起動や停止など、VMアラートに応答して標準の修復を自動的に実行できます。

以前は、VMアラートルールの作成中に、アラートがトリガーされるたびにRunbookを実行するために、Runbookに
AutomationWebhookを指定できました。ただし、これには、Runbookを作成し、RunbookのWebhookを作成してから、アラートルール
の作成中にWebhookをコピーして貼り付ける作業を行う必要がありました。この新しいリリースでは、アラートルールの作成時にリストか
らRunbookを直接選択でき、Runbookを実行する自動化アカウントを選択したり、アカウントを簡単に作成したりできるため、プロセスが
はるかに簡単になります。

参照：https：//
azure.microsoft.com/en-us/blog/automatically-remediate-azure-vm-alerts-with-automation runbooks /

NO.10次のものを含むRG1という名前のリソースグループがあります。

* Subnet1とAzureFirewallSubnetという名前の2つのサブネットを含む仮想ネットワーク
* contososa1という名前のAzureストレージアカウント
* AzureFirewallSubnetにデプロイされたAzureファイアウォール

contososa1がAzureバックボーンネットワークを介してサブネット1からアクセス可能であることを確認する必要があります。

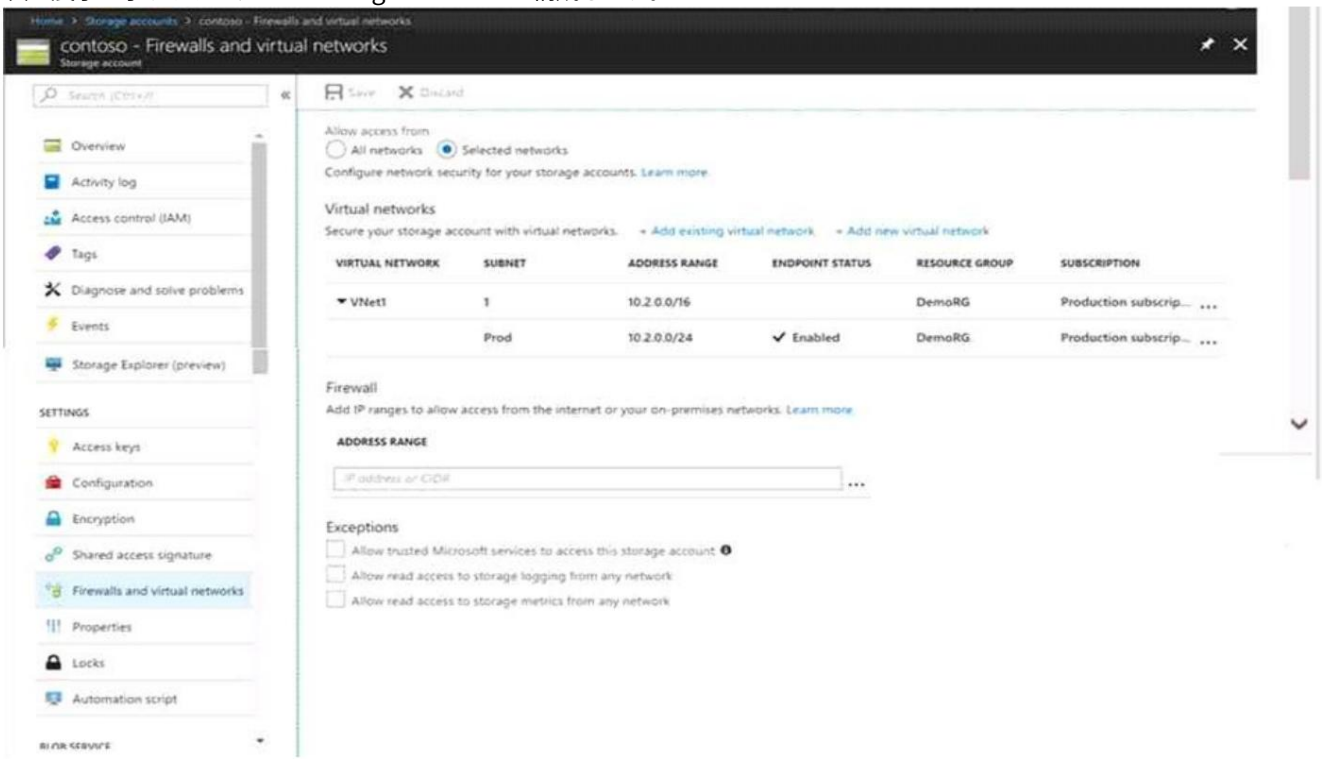
あなたは何をするべきか？
A.Azureファイアウォールを削除します

B.contososa1のファイアウォールと仮想ネットワークの設定を変更します。
C.仮想ネットワークサービスエンドポイントを実装します。
D.contososa1の保存されたアクセスポリシーを作成します。
回答： C

説明：仮想ネット
ワーク（VNet）サービスエンドポイントは、直接接続を介して、仮想ネットワークのプライベートアドレス空間とVNetのIDをAzureサービ
スに拡張します。エンドポイントを使用すると、重要なAzureサービスリソースを仮想ネットワークのみに保護できます。 VNetからAzure
サービスへのトラフィックは、常にMicrosoftAzureバックボーンネットワークに残ります。参照：https：//docs.microsoft.com/en-us/
azure/virtual-network/virtual-network-service-endpointsの概要

NO.11VNet1という名前の仮想ネットワーク上に複数のAzure仮想マシンがあります。

次の展示に示すように、AzureStorageアカウントを構成します。



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ステートメントを完了する回答の選択肢を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account **[answer choice]**.

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account **[answer choice]**.

always
during a backup
never

答え：

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account **[answer choice]**.

always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account **[answer choice]**.

always
during a backup
never

参照：

https：//docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows https://azure.microsoft.com/en-us/blog/azure -backup-now-supports-storage-accounts-secured with-azure-storage-firewalls-and-virtual-networks /

NO.12ネットワークにcontoso.comという名前のオンプレミスActiveDirectoryドメインが含まれています。ドメインには、次の表に示すユーザーが含まれています。

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	ADSyncAdmins
User4	Account Operators

Azure AD Connectをインストールし、SSOを有効にする予定です。
SSOを有効にするために使用するユーザーを指定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。

どのユーザーを指定する必要がありますか？

A. User2

B.ユーザー4

C.ユーザー1

D.ユーザー3

回答： C

説明：Active
Directoryフォレストごとに、次のようなドメイン管理者の資格情報が必要です。AzureADConnectを介してAzureADに同期します。
シームレスSSOを有効にするユーザーが含まれます。
注：ドメイン管理者の資格情報は、Azure ADConnectまたはAzureADには保存されません。
これらは、Azure ADConnectを介してシームレスSSOを有効にするためにのみ使用されます。
参照：https：//
docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

NO.13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。

Container1という名前のコンテナを含むAzureCosmosDBデータベースがあります。 Container1のパーティションキーは/ dayに設定されています。 Container1には、次の表に示すアイテムが含まれています。

Name	Content
Item1	{ "id": "1", "day": "Mon", "value" : "10" }
Item2	{ "id": "2", "day": "Mon", "value" : "15" }
Item3	{ "id": "3", "day": "True", "value" : "10" }
Item4	{ "id": "4", "day": "Wed", "value" : "15" }

プログラムでAzureCosmos DBにクエリを実行し、item1とitem2のみを取得する必要があります。

解決策：次のクエリを実行します。

```
SELECT day FROM c
   WHERE c.value = "10" OR c.value = "15"
```

EnableCrossPartitionQueryプロパティをTrueに設定します。

これは目標を達成していますか？

A.いいえ

B.はい

回答： A

説明：Item1、

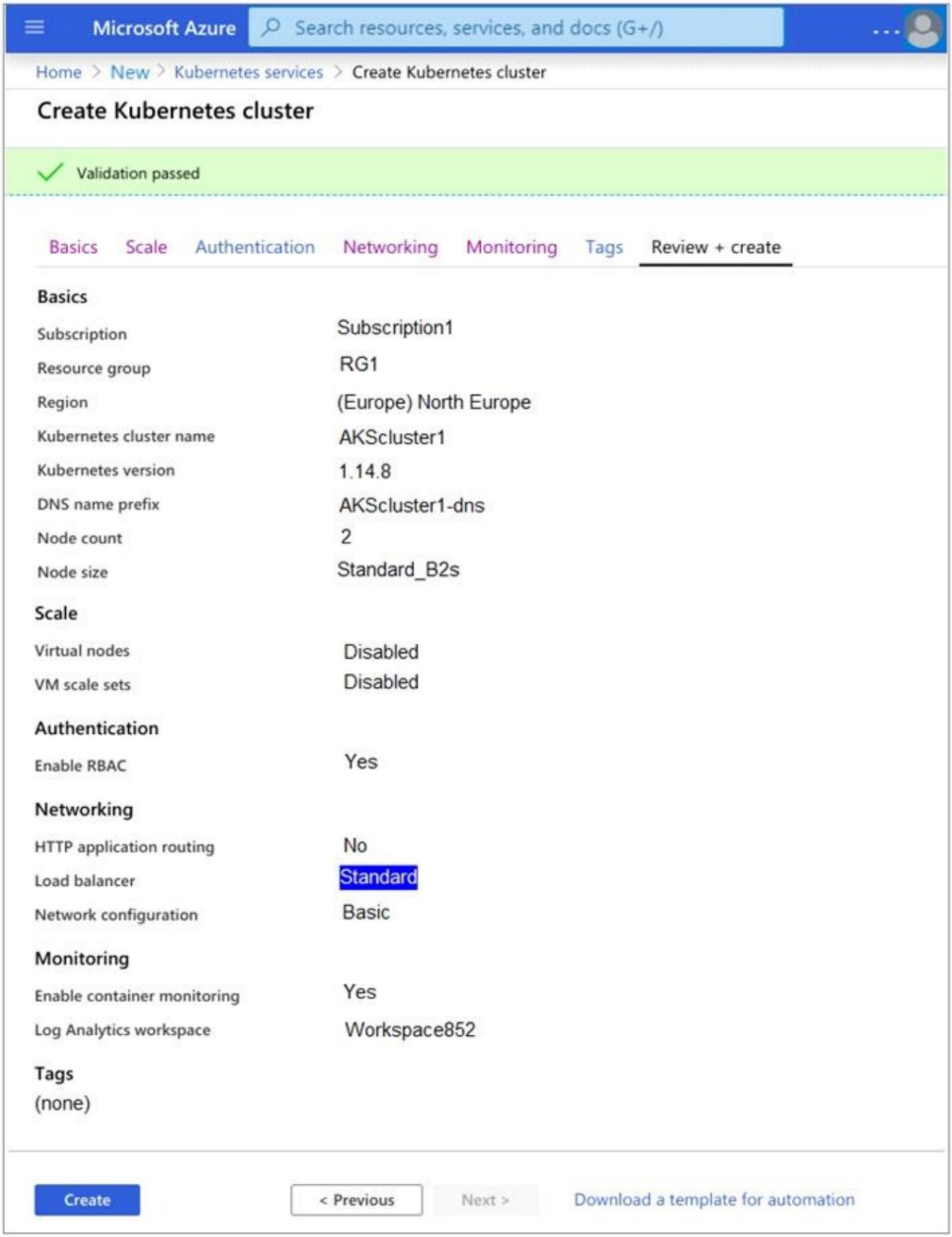
Item2、Item3、およびItem4を返します。

リファレンス：

https://docs.microsoft.com/en-us/azure/cosmos-db/sql-query-where

NO.14展示に示すように構成されたAzureKubernetes Service（AKS）クラスターを作成します。

（[展示]タブをクリックします。）



App1という名前のコンテナ化されたアプリケーションをagentPoolノードプールにデプロイします。

サイズDS3v2の4つのノードで実行されるApp2という名前のコンテナー化されたアプリケーションを作成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.AKSクラスターをアップグレードします。

B.AKSクラスターの仮想ノードを有効にします。

C.agentPoolノードの自動スケーリング設定を変更します。

D.新しいノードプールを作成します。

回答： D

説明：エージェン
トのサイズを変更することは許可されていません。将来、Microsftは、さまざまなVMサイズでさまざまなプールを作成できる複数のノードプー
ルをサポートする予定です。

参照：https：//
github.com/Azure/AKS/issues/132

NO.15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。

contoso.comという名前のAzureActive Directory（Azure AD)テナントがあります。
Admin1という名前のユーザーが、Azure Active Directory管理センターからアクセスレビューを作成しようとすると、アクセスレビュー設定
が使用できないことがわかります。 Admin1は、他のすべてのIdentityGovernance設定が使用可能であることを検出します。

Admin1には、ユーザー管理者、コンプライアンス管理者、およびセキュリティ管理者の役割が割り当てられています。

Admin1がcontoso.comでアクセスレビューを作成できることを確認する必要があります。

解決策：contoso.comのAzure Directory PremiumP2ライセンスを購入します。

これは目標を達成していますか？

A.いいえ

B.はい

回答： A

説明：代わりに、
AzureAD特権ID管理を使用してください。
注：PIMは基本的に、関心のあるリソースの誰が、何を、いつ、どこで、なぜ行うかを管理するのに役立ちます。 PIMの主な機能は次のとおりです。ア
クセスレビューを実施して、ユーザーが引き続き役割を必要としていることを確認します

参照：https：//
docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim configure

NO.16Account1という名前のAzureCosmosDBアカウントがあります。 Account1には、Container1という名前のコンテナーを含む
DB1という名前のデータベースが含まれています。 Container1のパーティションキーは/ cityに設定されています。

Container1のパーティションキーを変更する予定です。

あなたは最初に何をすべきですか？

A.新しいAzureCosmosDBアカウントを作成します。

B. Azure CosmosDB.NET.SDKを実装します。

C.Container1を削除します。

D.Account1のキーを再生成します。

回答： A

説明：Azure
CosmosDBのChangeFeedProcessorとBulkExecutor Libraryを利用して、あるコンテナーから別のコンテナーへのデータのライブマイグレーションを実現できます。これにより、データを再配布して目的の新しいパーティションキースキームに一致させ、後で関連するアプリケーションを変更して、「パーティションキーを更新する」効果を実現できます。

不正解：
A：既存のコンテナのパーティションキーを「更新」することはできません。
リファレンス：
https://devblogs.microsoft.com/cosmosdb/how-to-change-your-partition-key/

NO.17KV1という名前のAzureキーボールトがあります。
アプリケーションがKV1を使用して、外部の証明機関（CA）から証明書を自動的にプロビジョニングでき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. KV1から、証明書署名要求（CSR）を作成します。
B.CAアカウントの資格情報を取得します。
C. KV1から、証明書発行者リソースを作成します。
D.ルートCA証明書を取得します。
E. KV1から、秘密鍵を作成します。回答：
A、D説明：C：ルートCA証明書を取得します
（下の図のステップ4）

D：KV1から、証明書署名要求（CSR）を作成します（下の図のステップ2）注：Key Vaultと提携していないCAで証明書を作成するこの方法では、Key Vaultの提携プロバイダー以外のCA、つまり組織と連携できます。選択したCAで動作できます。

次の手順の説明は、前の図の緑色の文字の手順に対応しています。
上の図では、アプリケーションが証明書を作成しています。証明書は、キーボールトにキーを作成することから内部的に開始されます。

Key Vaultは、証明書署名要求（CSR)をアプリケーションに返します。
アプリケーションはCSRを選択したCAに渡します。
選択したCAはX509証明書で応答します。
アプリケーションは、CAからのX509証明書をマージして、新しい証明書の作成を完了します。

参照 :https：//
docs.microsoft.com/en-us/azure/key-vault/certificates/certificate-scenarios

NO.18KeyVault1という名前のAzureキーボールトと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

KeyVault1には、複数のユーザーにキーの作成権限を与えるアクセスポリシーがあります。
ユーザーがVM1からKeyVault1にのみシークレットを登録できるようにする必要があります。
あなたは何をするべきか？
A.KeyVault1のアクセスポリシーを変更します。
B. Subnet1にリンクされているネットワークセキュリティグループ（NSG)を作成します。
C.ハードウェアセキュリティモジュール（HSM)を使用するようにKeyVault1を構成します。
D.KeyVault1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。
回答： A
説明 :キーボール
トにキーボールトアクセスポリシーを設定することにより、データプレーンアクセスを許可します。
注1 :VMのシステム割り当てのマネージドIDアクセスにKeyVaultへのアクセスを許可します。
[アクセスポリシー]を選択し、[新規追加]をクリックします。
[テンプレートから構成]で、[シークレット管理]を選択します。
[プリンシパルの選択]を選択し、検索フィールドに前に作成したVMの名前を入力します。結果リストでVMを選択し、[選択]をクリックします。

[OK]をクリックして新しいアクセスポリシーの追加を終了し、[OK]をクリックしてアクセスポリシーの選択を終了します。
注2 :キーボールトへのアクセスは、管理プレーンとデータプレーンの2つのインターフェースを介して制御されます。管理プレーンは、
KeyVault自体を管理する場所です。このプレーンでの操作には、キーボールトの作成と削除、キーボールトプロパティの取得、およびアクセスポリシーの更新が含まれます。
データプレーンは、キーボールトに保存されているデータを操作する場所です。キー、シークレット、および証明書を追加、削除、および変更できます。
リファレンス：
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure resources / tutorial-windows-vm-access-nonaad https://docs.microsoft.com/en-us/ azure / key-vault / general / secure-your-key-vault2