Microsoft.AZ-500J.v2026-08-28.q219

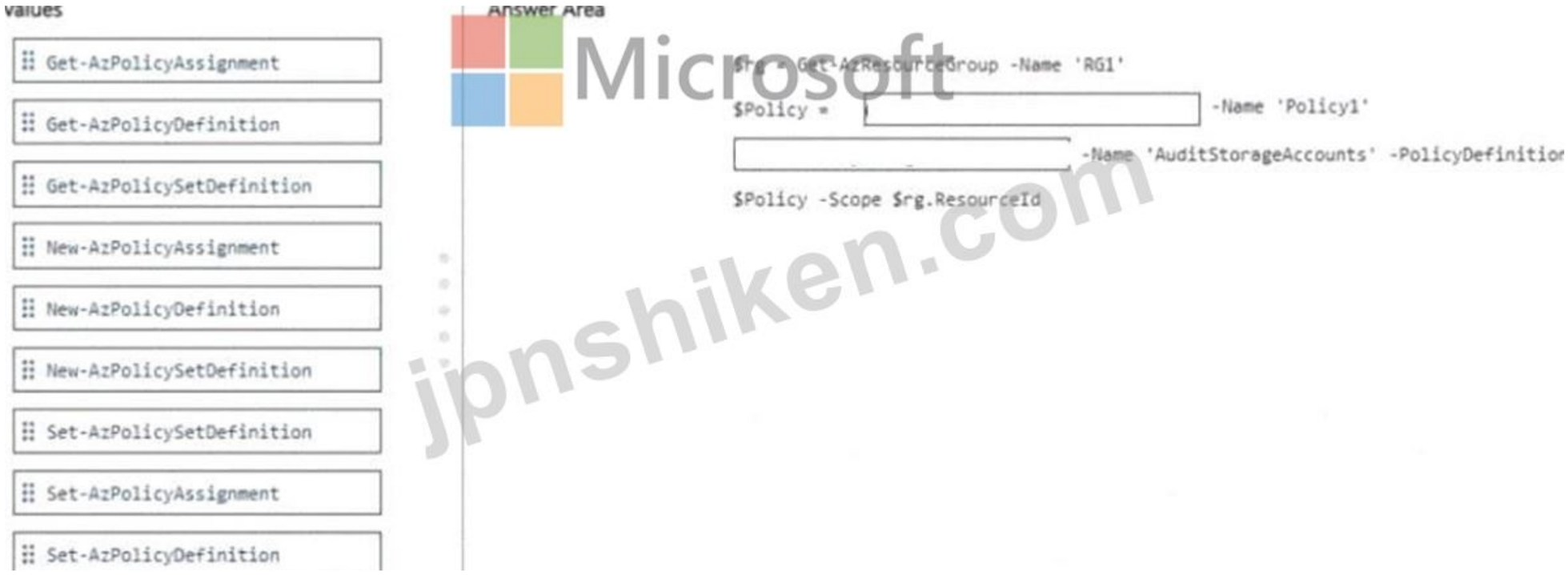
試験コード：	AZ-500J
試験名称：	Microsoft Azure Security Technologies (AZ-500日本語版)
認証ベンダー：	Microsoft
無料問題の数：	219
バージョン：	v2026-08-28
ページの閲覧量：	102
問題集の閲覧量：	2233

https://www.jpnshiken.com/shiken/Microsoft.AZ-500J.v2026-08-28.q219.html

質問: **1**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Defender for Cloud を使用する Azure サブスクリプションがあります。
次の表に示すサーバーを含むオンプレミス データセンターがあります。
Microsoft Defender for Cloud への直接オンボーディングを有効にします。
どのサーバーが Defender for Cloud にオンボードされますか?
A. Server1 と Server3
B. サーバー1、サーバー2、サーバー3
C. Servei2 と Servet3
D. サーバー2のみ
E. サーバー1のみ
F. サーバー3のみ
正解: **(**正解を表示します**)**

質問: **2**
キー コンテナーに対して計画された変更を実装します。
AKV1 バックアップをどのキー コンテナーに復元できますか?
A. AKV4とAKV5のみ
B. AKV2、AKV3、AKV4、およびAKV5
C. AKV4のみ
D. AKV3とAKV4のみ
E. AKV2、AKV3、AKV4のみ
正解: **(**正解を表示します**)**

質問: **3**
RG1 という名前のリソース グループと Policy1 という名前の Azure ポリシーを含む Azure サブスクリプションがあります。
Policy1 を RG1 に割り当てる必要があります。
スクリプトをどのように完成させるべきですか？ 回答するには、適切な値を正しいターゲットにドラッグしてください。各値は1回、複数回、または全く使用されない場合があります。内容を確認するには、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：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: 4

RG1 という名前のリソース グループと、次の表に示す ID を含む Azure サブスクリプションがあります。

User1	User	*Not applicable*
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

Group4 に RG1 の共同作成者ロールを割り当てます。

どの ID をメンバーとして Group4 に追加できますか?

A. User1、Group1、Group3 のみ

B. User1 と Group3 のみ

C. ユーザー 1、グループ 2、およびグループ 3 のみ

D. User1 のみ

E. ユーザー 1、グループ 1、グループ 2、およびグループ 3

正解: **(**正解を表示します**)**

質問: 5

注：質問は、同じ設定を表すいくつかの質問に含まれています。ただし、すべての質問には独特の結果があります。ソリューションが要件を満たしているかどうかを確認します。

あなたの会社には、weylandindustries.comという名前の単一ドメインを持つActiveDirectoryフォレストがあります。また、同じ名前のAzure Active Directory（Azure AD）テナントもあります。

ActiveDirectoryとAzureADテナントの統合を担当しました。Azure ADConnectをデプロイする予定です。

統合の戦略では、パスワードポリシーとユーザーログオンの制限が、Azure ADテナントに同期されるユーザーアカウントに影響を与え、必要なサーバーの数が削減されるようにする必要があります。

解決策：パススルー認証とパスワードハッシュ同期を使用したシームレスSSOの使用をお勧めします。

ソリューション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**)**
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

質問: **6**
次の表に示すリソースを含む Azure 480z サブスクリプションがあります。

Name	Type
Group1	Security group
Group2	Microsoft 365 group
App1	App registration
MI1	User-assigned managed identity

次の表に示すユーザーがいます。

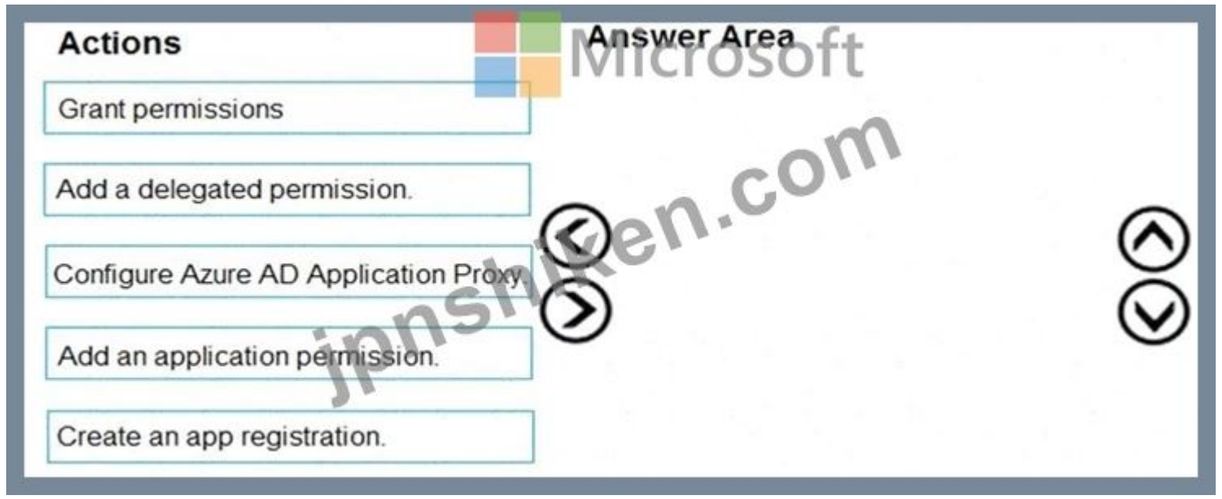
Name	Description
User1	• Member of Group1 and Group2 • Assigned Owner role for App1 and MI1
User2	• Member of Group1 and Group2 • Assigned Owner role for App1 and MI1

SQL! という名前の Azure SQL マネージド インスタンスを作成し、Microsoft Entra のみの認証を有効にします。
User! と User2 の両方が SQL1 の Microsoft Entra 管理者として設定されていることを確認する必要があります。
解決策: Group2 を SQL1 の Microsoft Entra 管理者として設定します。
これは目標を満たしていますか?
A. いいえ
B. はい
正解: **(**正解を表示します**)**

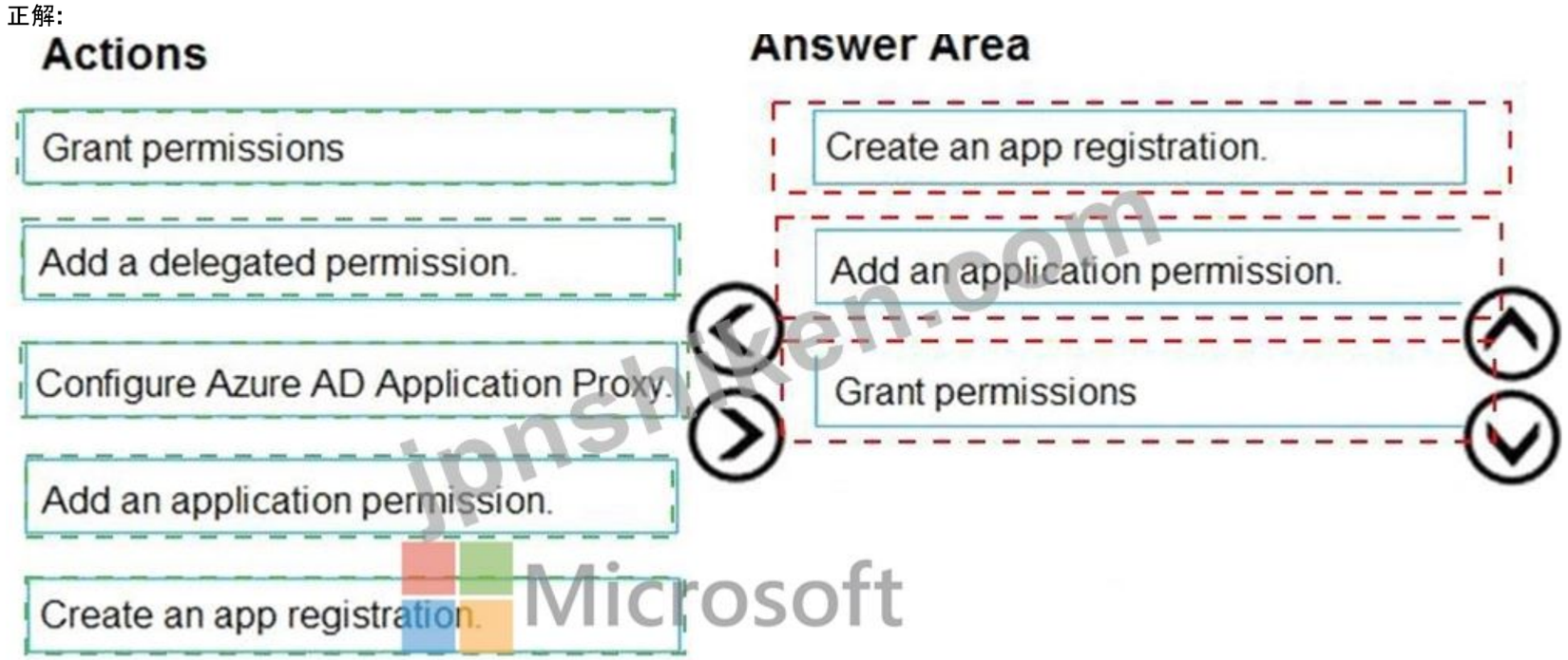
質問: **7**
お客様の環境には、Windows Serverが稼働しているオンプレミスサーバーが10台あります。
サーバーにMicrosoft Defender for Cloudの脆弱性スキャンを導入する予定です。最初にサーバーにインストールすべきものは何ですか？
A. Microsoft Defender for Endpoint エージェント
B. Azure Arc Connected Machine エージェント
C. Microsoft Configuration Manager クライアント
D. Microsoft Sentinel のセキュリティ イベント データ コネクタ
正解: **(**正解を表示します**)**

質問: **8**
会社には、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。
同社はApp1という名前のアプリケーションを開発しています。App1は、Windows Server 2016を実行するサーバー上でサービスとして実行されます。App1は、contoso.comに対して認証を行い、Microsoft Graphにアクセスしてディレクトリデータを読み取ります。

App1に最低限必要な権限を委任する必要があります。
Azureポータルから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のリストから回答エリアに移動し、正しい順序に並べます。



正解:



Explanation:

Step 1: Create an app registration
First the application must be created/registered.
Step 2: Add an application permission
Application permissions are used by apps that run without a signed-in user present.
Step 3: Grant permissions
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent

質問: **9**
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	Location	Peered with
VNet1	East US	VNet2
VNet2	West US	VNet1

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	IP address space	Virtual network	Description
Subnet11	10.1.1.0/24	VNet1	Contains a virtual machine named VM1
Subnet12	172.16.1.0/27	VNet1	Contains no resources
Subnet21	192.168.10.0/24	VNet2	Contains an integrated Azure web app named WebApp1

次の構成を持つ WebApp2 という名前の Azure Web アプリを作成する予定です。
* 地域: 米国東部
* VNet統合: 有効
* スケールアウト; 最大 10 インスタンスまで自動スケール
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 ポイントが付与されます。

Answer Area

Statements	Yes	No
WebApp2 can be integrated with Subnet11.	○	○
WebApp2 can be integrated with Subnet12.	○	○
WebApp2 can be integrated with Subnet21.	○	○

正解:

Answer Area

Statements	Yes	No
WebApp2 can be integrated with Subnet11.	○	○
WebApp2 can be integrated with Subnet12.	○	○
WebApp2 can be integrated with Subnet21.	○	○

Explanation:

Answer Area

Statements	Yes	No
WebApp2 can be integrated with Subnet11.	●	○
WebApp2 can be integrated with Subnet12.	●	○
WebApp2 can be integrated with Subnet21.	○	●

質問: **10**
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。

Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

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？
A. VM1のみ
B. VM1、VM2、およびVM3のみ
C. VM1およびVM3のみ
D. VM1、VM2、VM3、およびVM4
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

質問: **11**
Azure サブスクリプションをお持ちです。
VM1 という名前の仮想マシンを展開する予定です。
VM1 では機密ディスク暗号化を使用する必要があります。
VM1 にはどの仮想マシン シリーズを使用する必要がありますか。また、機密ディスク暗号化を使用して暗号化できるディスク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 ポイントが付与されます。

Answer Area

正解:

Explanation:

質問: **12**

VM4用にAzureDisk Encryptionを構成する予定です。暗号化キーを格納するために使用できるキーボールトはどれですか？

A. KeyVault1

B. KeyVault3

C. KeyVault2

正解: **(**正解を表示します**)**

The key vault needs to be in the same subscription and same region as the VM.

VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

Topic 4, Fabrikam, Inc.

Case Study

Overview

Existing Environment

Network Environment

Cloud Environment

Sub1 Resources

Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.

The on-premises network contains a datacenter in each office.

Fabtikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.

All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Type	Microsoft Entra role	Azure role assignment for Sub1
Admin1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admin2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admin4	User	Global Administrator	*None*
User1	User	*None*	Reader
AKS1	System-assigned managed identity	*None*	*None*
ID1	User-assigned managed identity	*None*	*None*

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune.

Sub2 Resources

Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication.

Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:

* Bot Manager 1.1
* Azure-managed Default Rule Set (DRS)

Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

* MIST SP 800-53 Rev. 4
* Microsoft cloud security benchmark (MCSB)
* System and Organization Controls (SOC) 2 Type 2

Planned Changes and Requirements

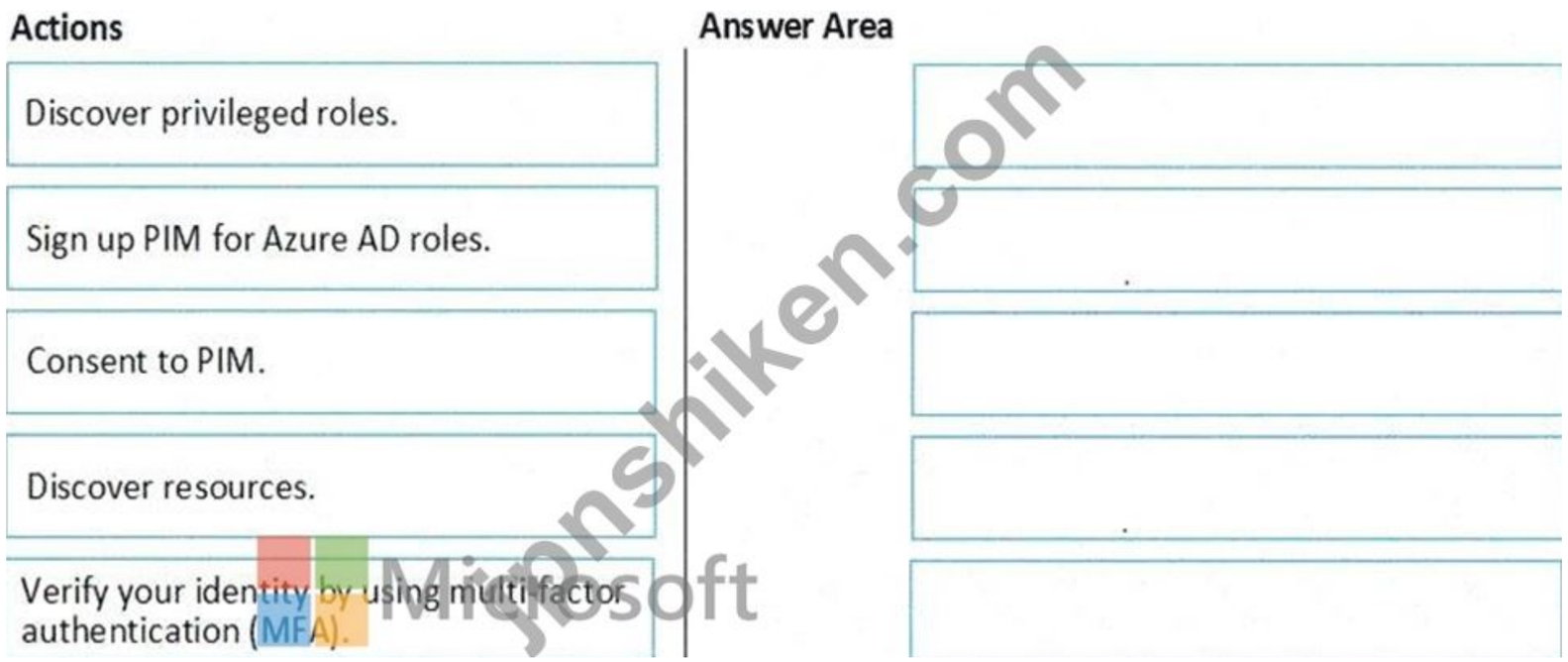
Planned Changes

Sub2 contains a resource group named RG2.
Fabtikam plans to implement the following changes:
* Deploy the following key vaults to RG1:
o AKV2 in the West Europe Azure region
o AKV3 in the Central US Azure region
o AKV4 in the East US Azure region
* Deploy the following key vaults to RG2:
o AKV5 in the East US region
* Configure VM1 to read data from storage1.
* Create function apps that have the following hosting plans:
o Fa1: Flex Consumption hosting plan
o Fa2: Consumption hosting plan
o Fa3: Dedicated hosting plan
* For WAF1, implement rate limiting rules based on the request location.
* Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud.
* Create a new storage account named storage2 that supports Azure Table storage.
* Enforce multifactor authentication (MFA) when database administrators access SQLdbl.
* Implement ExpressRoute circuits to the on-premises network as shown in the following table.

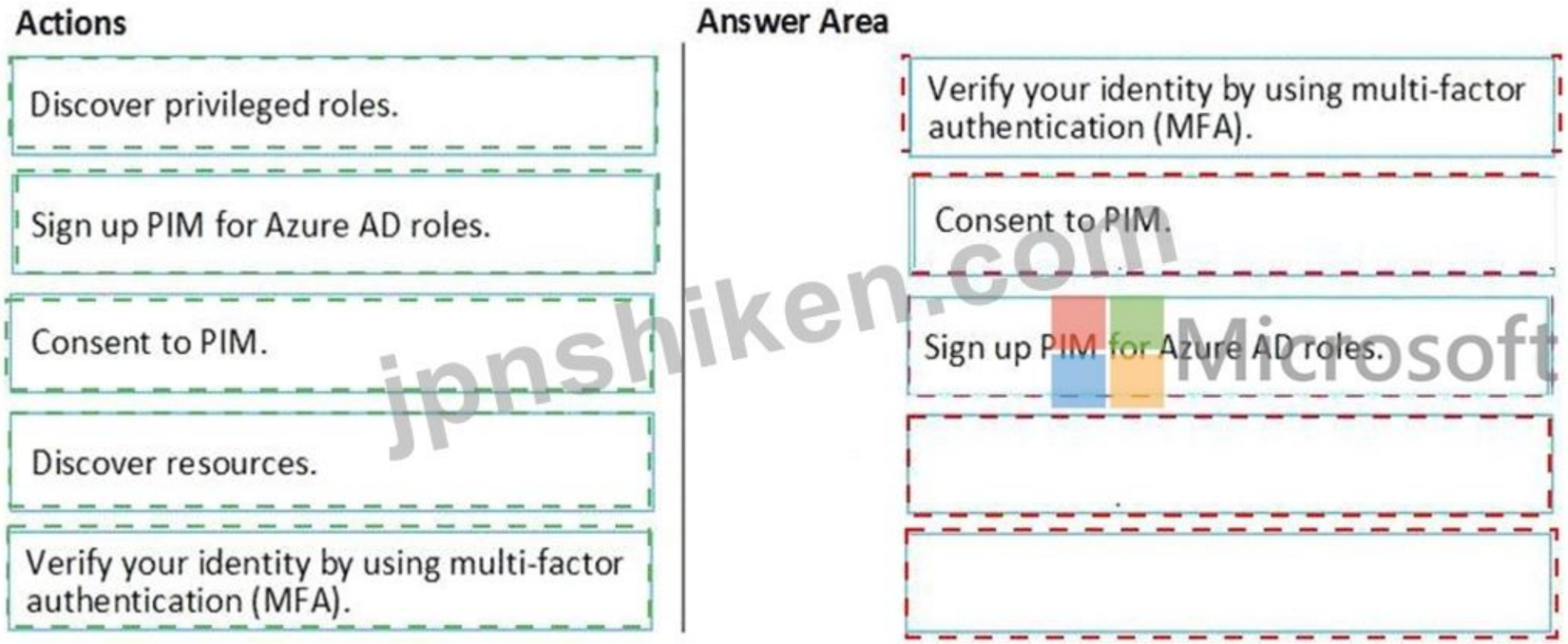
Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

* For RG1. create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.
Technical Requirements
Fabrikam has the following technical requirements:
* If VM1 is deleted, the permissions for VM1 must be removed automatically.
* The AKS1 managed identity must only be able to pull images from Registry1.
* The ID1 managed identity must be able to push images to and pull images from Registry 1.
* All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
* All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
* ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

質問**: 13**
Azure AD Premium P2でAzureサブスクリプションを作成します。
Azure Active Directory（Azure AD）Privileged Identity Management（PIM）を使用してAzureロールを保護できることを確認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のリストから回答エリアに移動し、正しい順序に並べます。



正解:



Explanation:

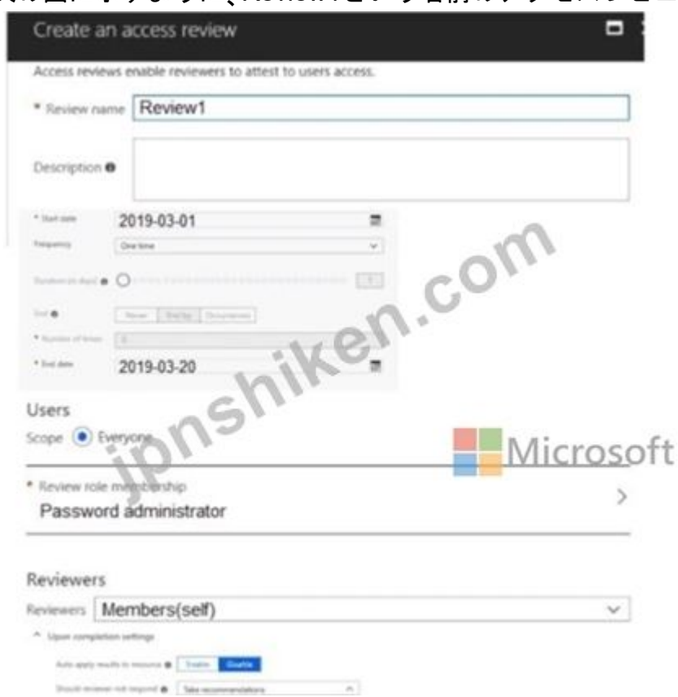
1. Verify your identity with MFA
2. Consent to PIM
3. Sign up PIM for AAD Roles

質問: 14

contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれます。

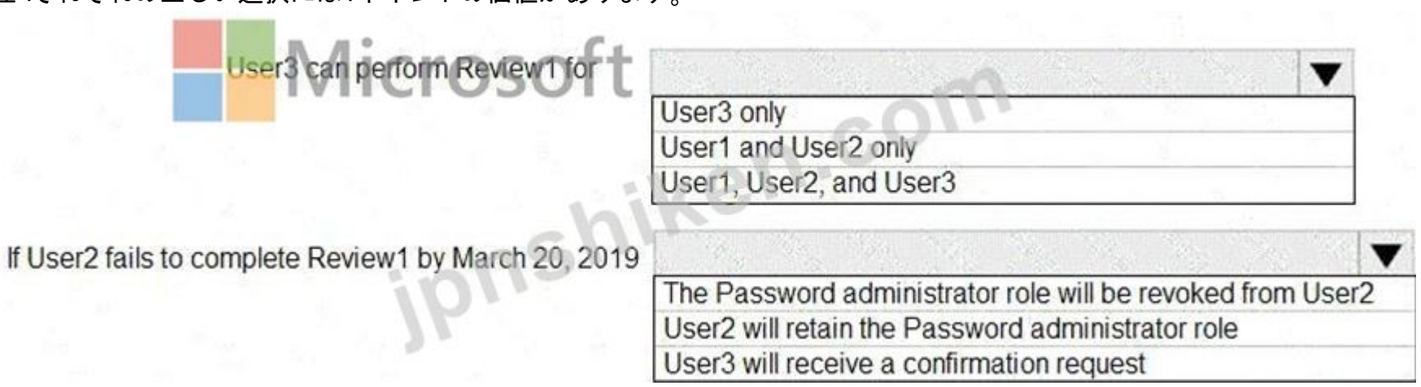
Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

次の図に示すように、Review1という名前のアクセスレビューを構成します。



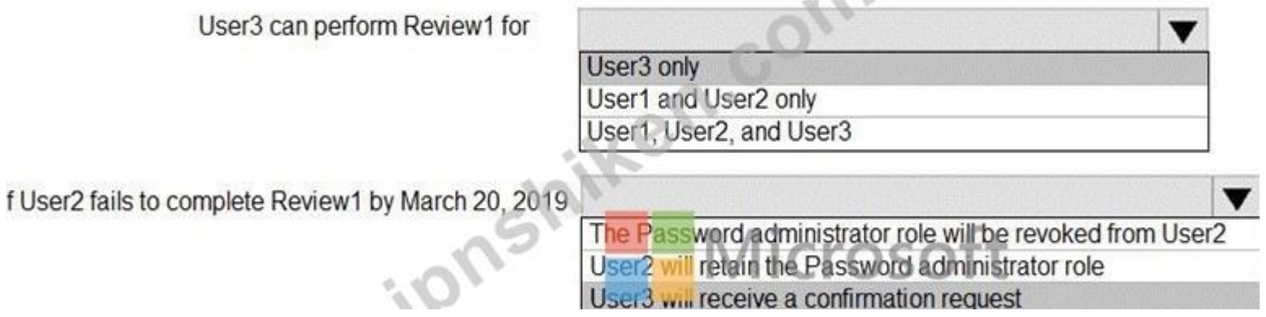
ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注 :それぞれの正しい選択には1ポイントの価値があります。



正解:

Explanation:



Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer ' s decision is Deny, then the user ' s access will be removed.

No change - Leave user ' s access unchanged

Remove access - Remove user ' s access

Approve access - Approve user ' s access

Take recommendations - Take the system ' s recommendation on denying or approving the user ' s continued access References:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to- start-security-review

質問: **15**

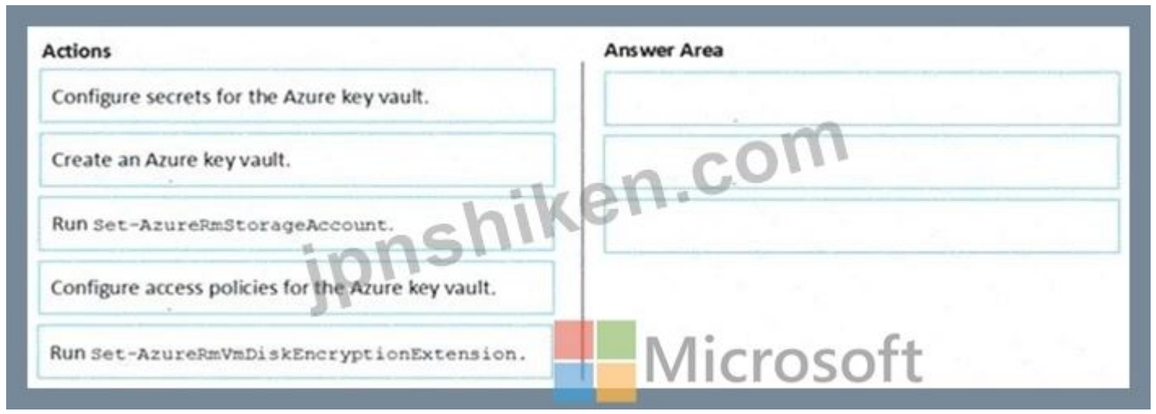
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。

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。

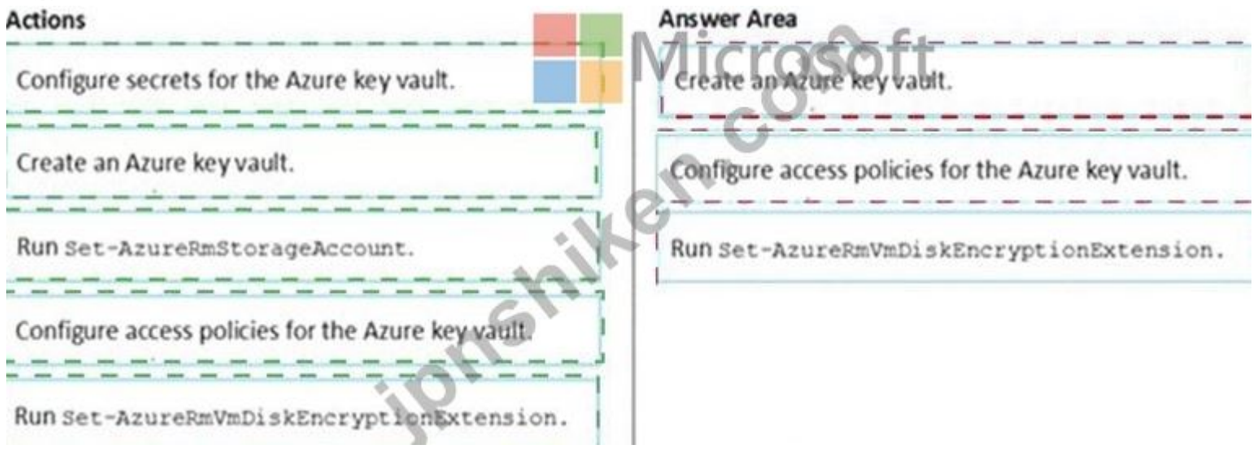
Sub1という名前のAzureサブスクリプションがあります。Sub1には、Windows Server 2016を実行するVM1という名前のAzure仮想マシンが含まれています。

Azure Disk Encryptionを使用してVM1ディスクを暗号化する必要があります。

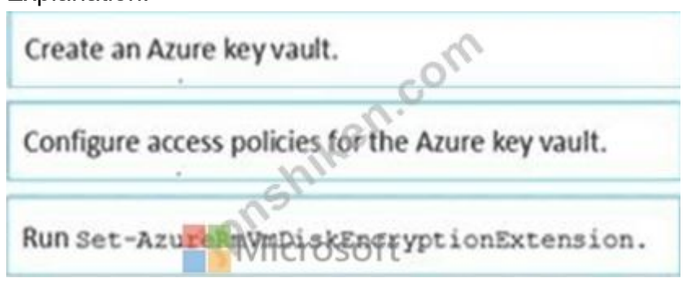
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序に並べます。



正解:

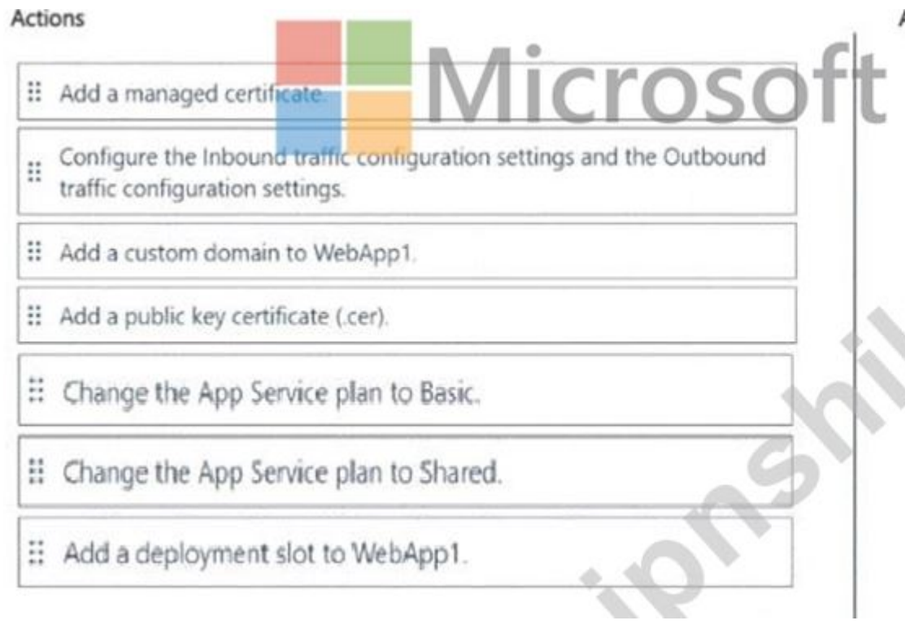


Explanation:



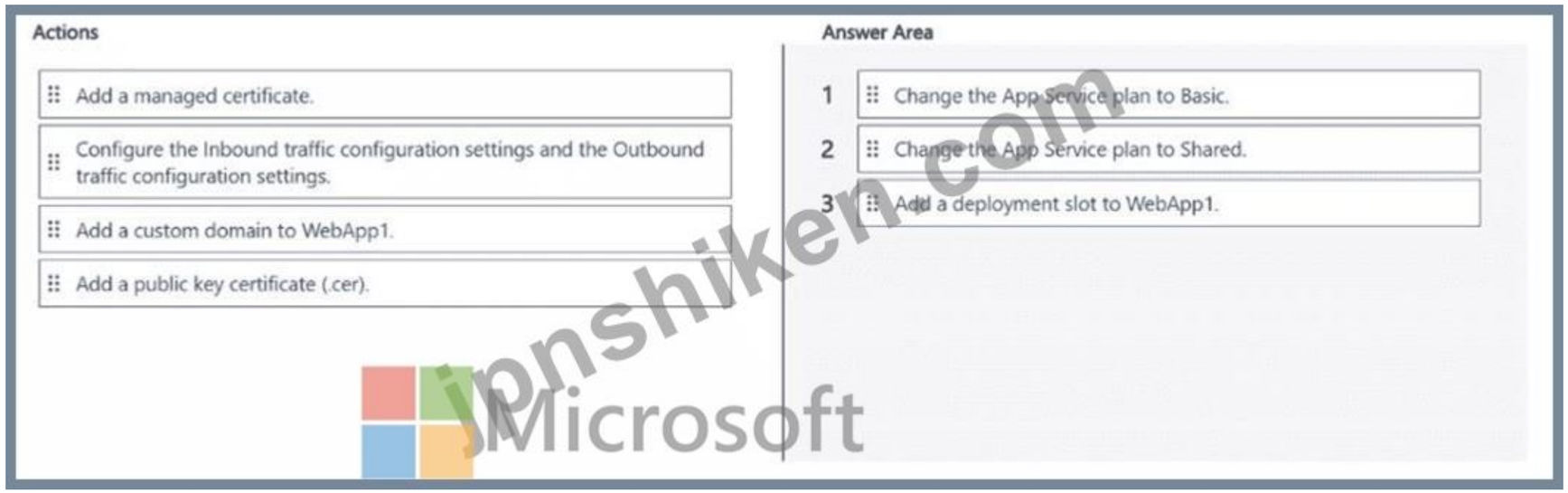
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

質問: **16**
お客様は、以下の Azure App Service Web アプリを含む Azure サブスクリプションをお持ちです。
* 名前: WebApp1
* アプリサービスプラン：無料
WebApp1でApp Service管理証明書を使用するように構成する必要があります。この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。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:

Explanation:



質問: **17**
Azure キー コンテナーを含む Azure サブスクリプションがあります。
新しいキーが有効な最大日数を構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る必要があります。
何を使うべきですか？
A. 紺碧の設計図
B. アズール パービュー
C. Azure ポリシー
D. キー コンテナーのプロパティ
正解: **(**正解を表示します**)**

質問: **18**
Azureポータルから、Azureポリシーを構成しています。
DeployIfNotExist、AuditIfNotExist、Append、Denyの各エフェクトを使用するポリシーを割り当てる予定です。
どの効果には、割り当てに管理されたIDが必要ですか？
A. AuditIfNotExist
B. Append
C. DeployIfNotExist
D. Deny
正解: **(**正解を表示します**)**
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

質問: **19**
Azure Container Registryに接続するAzure Kubernetes Service（AKS）クラスターがあります。
AKSクラスターの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を認証する必要があります。
何を作成する必要がありますか？
A. Azure Key Vaultの秘密
B. 役割の割り当て
C. Azure Active Directory（Azure AD）ユーザー
D. Azure Active Directory（Azure AD）グループ
正解: **B (**コメントを発表する**)**
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

質問: **20**
Sub2の仮想マシン間のネットワーク通信のセキュリティを評価しています。
以下の各ステートメントについて、ステートメントが真である場合は「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 :それぞれの正しい選択には1ポイントの価値があります。

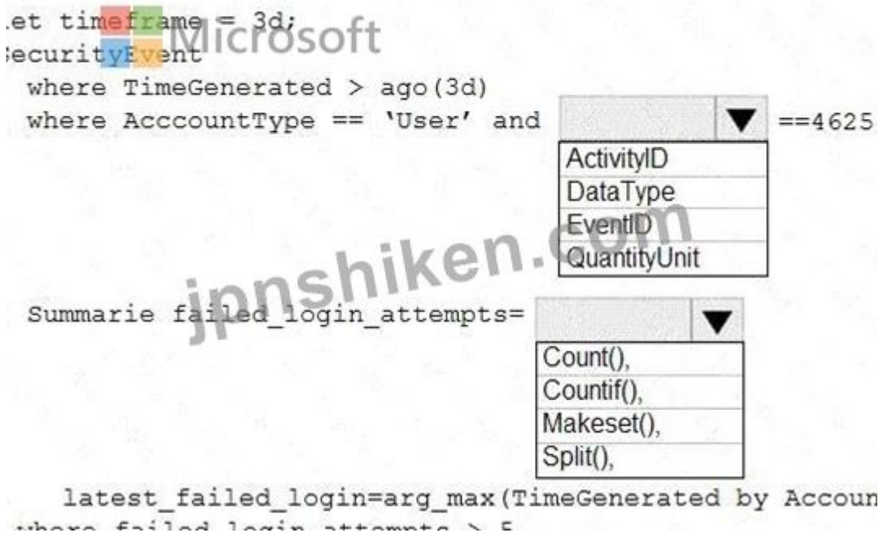
正解:

Explanation:

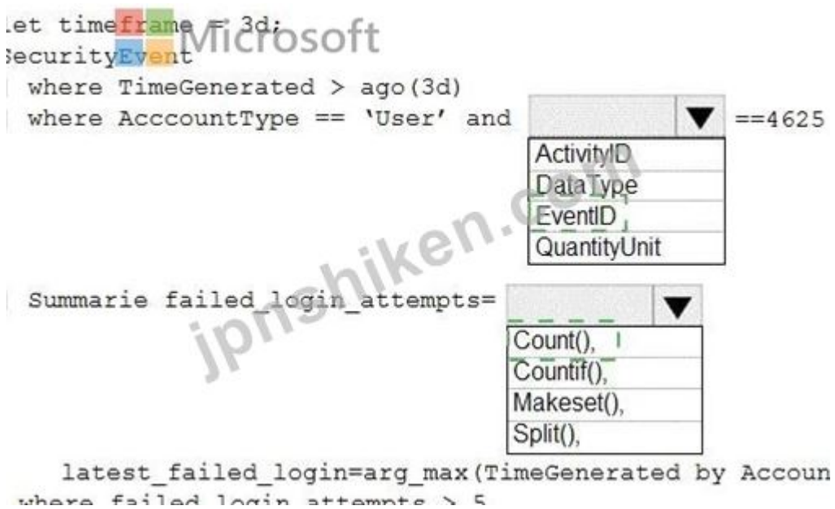
Q1: No { and it should not be allowed as only TCP 80 is allowed from the "Internet" service tag Q2: Yes {as it should be for VMs in the same local subnet pinging each other on private IP and no NSG configured} Q3: Yes {VM5 is in subnet where 1st rule of NSG allows any traffic from any source to the destination}

質問: **21**
AzFWL 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る場合、AzFW1 で次の機能を使用できるかどうかを確認する必要があります。
* TLS インスペクション
* 脅威インテリジェンス
* ネットワーク侵入検知および防止システム (IDPS)
あなたは何を使うことができますか？
A. TLS インスペクションと IDPS のみ
B. 脅威インテリジェンスのみ
C. 脅威インテリジェンスと IDPS のみ
D. TLS インスペクション、脅威インテリジェンス、および IDPS
E. TLS インスペクションのみ
正解: **(正解を表示します)**

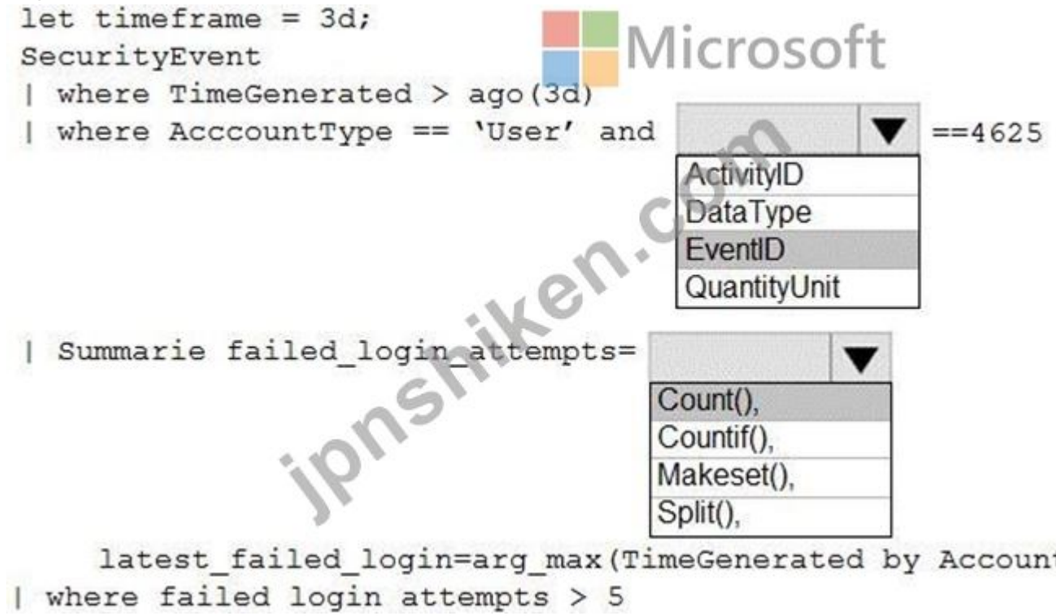
質問: **22**
ユーザーがアクセス権のないリソースにサインインしようとしていると思われます。
Azure Log Analyticsクエリを作成して、過去3日間で失敗したユーザーサインインの試行を識別する必要があります。結果には、サインインに5回以上失敗したユーザーのみが表示される必要があります。
クエリをどのように構成する必要がありますか？回答するには、回答エリアで適切なオプションを選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:



The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

let timeframe = 1d;

SecurityEvent

| where TimeGenerated > ago(1d)

| where AccountType == ' User ' and EventID == 4625 // 4625 - failed log in

| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account

| where failed_login_attempts > 5

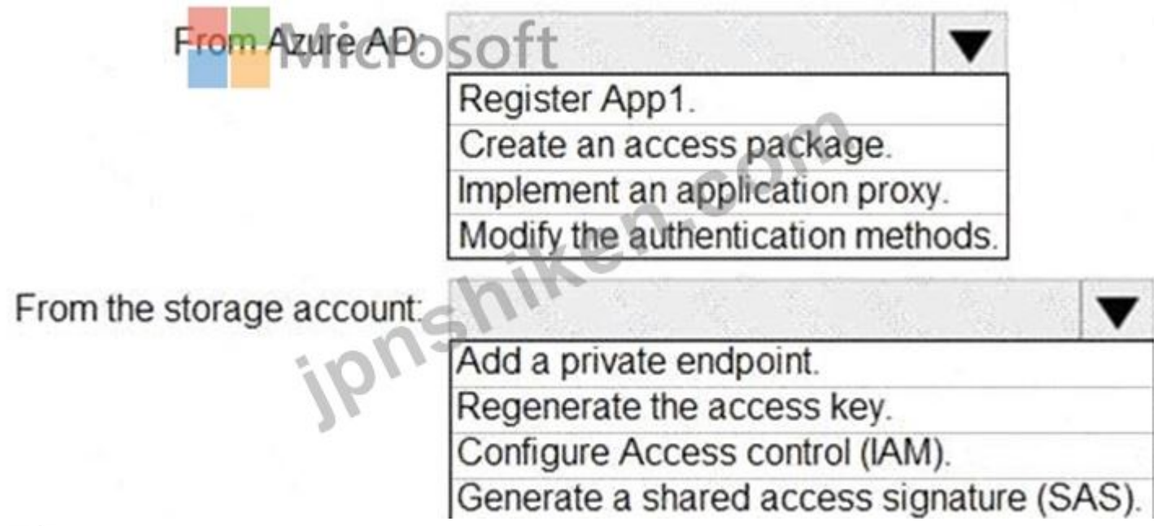
| project-away Account1

References:

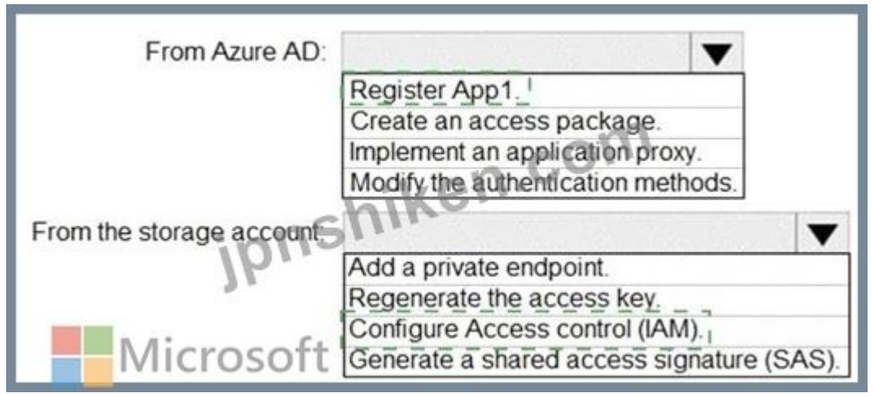
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

質問: **23**
注: この問題は、同じシナリオを提示する一連の問題の一部です。一連の問題にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
AKS1 という名前の Azure Kubernetes Service (AKS) クラスターと AZCR1 という名前の Azure コンテナー レジストリを含む Azure サブスクリプションがあります。
AKS1 が AZCR1 に保存されているコンテナー イメージをデプロイできることを確認する必要があります。
解決策: AKS1 のエージェント プールのシステム割り当てマネージド ID に Kubernetes エージェントレス オペレーター ロールを割り当てます。
これは要件を満たしていますか?
A. いいえ
B. はい
正解: **(**正解を表示します**)**

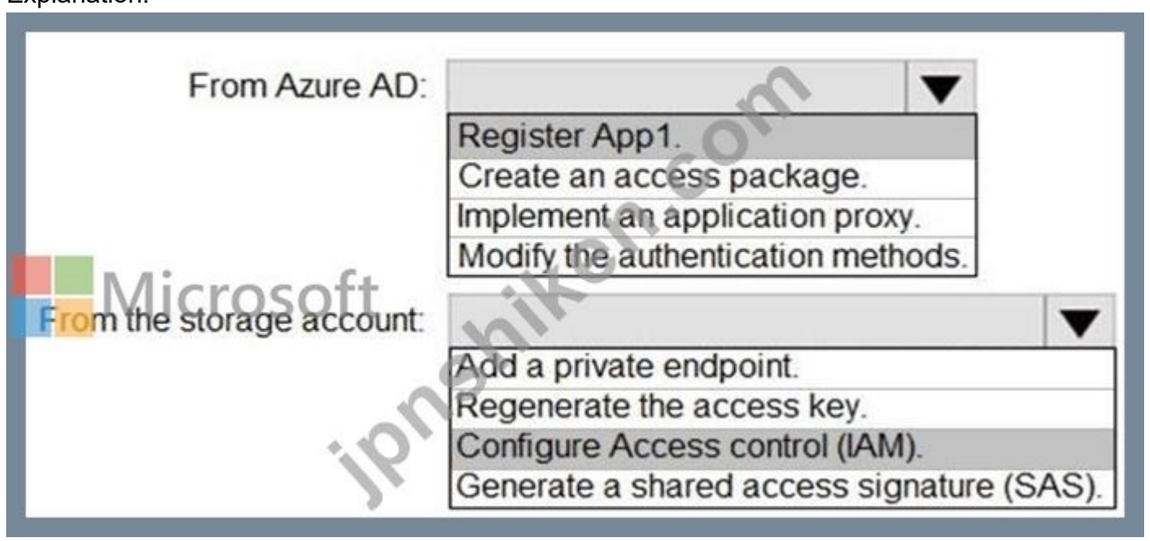
質問: **24**
container1 という名前の BLOB コンテナーと App1 という名前のクライアント アプリケーションを含む Azure ストレージ アカウントがあります。
Azure Active Directory (Azure AD) 認証を使用して、App1 から container1 へのアクセスを有効にする必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Reference:
https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac- portal.md

質問: **25**
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
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

サブスクリプションに対してMicrosoftDefenderforCloudを有効にする予定です。Microsoft Defender for Cloudを使用して保護できるリソースはどれですか？
A. VM1、VNET1、およびstorage1のみ
B. VM1.VNET1、storage1、およびVault1
C. VM1およびVNETのみ
D. VM1、storage1、およびVault1のみ
E. VM1とstorage1のみ

正解: (正解を表示します)

質問: **26**

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、次の表に示すサブネットを含む VNet1 という名前の仮想ネットワークが含まれています。

Name	Associated network security group (NSG)
Subnet1	NSG1
Subnet2	NSG1
Subnet3	NSG1
Subnet4	NSG1

サブスクリプションには、次の表に示す関数アプリが含まれています。

Name	Description
App1	Uses the Azure Functions Premium plan and has virtual network integration with VNet1/Subnet1
App2	Uses an App Service plan in the Basic pricing tier and has virtual network integration with VNet1/Subnet2
App3	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1/Subnet3
App4	Uses an App Service plan in the Isolated pricing tier and is deployed to VNet1/Subnet4

NSG1 を使用して制御されるアプリの送信トラフィックはどれですか?

A. App1、App2、App3、App4
B. App3 と App4 のみ
C. App4のみ
D. App2、App3、App4のみ

正解: (正解を表示します)

質問: **27**

Azure Active Directory (Azure AD) テナントがあります。

削除されたオブジェクトは次の表のとおりです。

Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

2020 年 5 月 4 日に、Azure Active Directory 管理センターを使用して、削除されたオブジェクトの復元を試みます。

どの 2 つのオブジェクトを復元できますか。それぞれの正解は完全な解決策を示します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

A. グループ1
B. グループ2
C. ユーザー2
D. ユーザー1

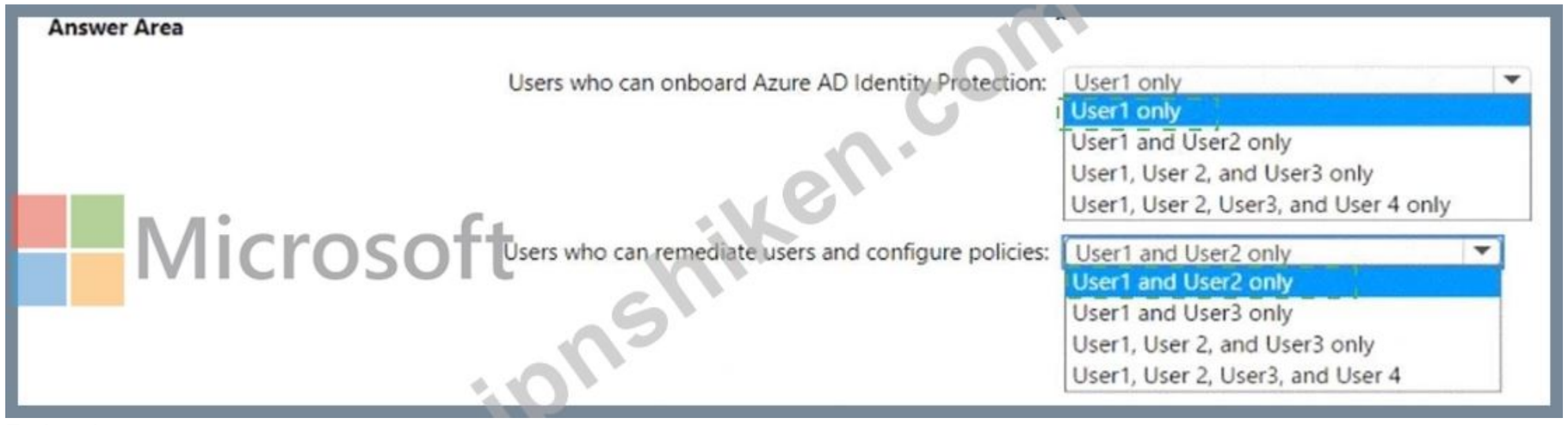
正解: (正解を表示します)
Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

質問: 28
contoso.com という名前の Azure AD テナントに関連付けられた Sub 1 という名前の 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ます。

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

各ユーザーには Azure AD Premium P2 ライセンスが割り当てられます。
Azure AD Identity Protection をオンボードして構成する予定です。
Azure AD Identity Protection をオンボードし、ユーザーを修復し、ポリシーを構成できるのはどのユーザーですか? 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 ポイントが付与されます。
Answer Area

正解:

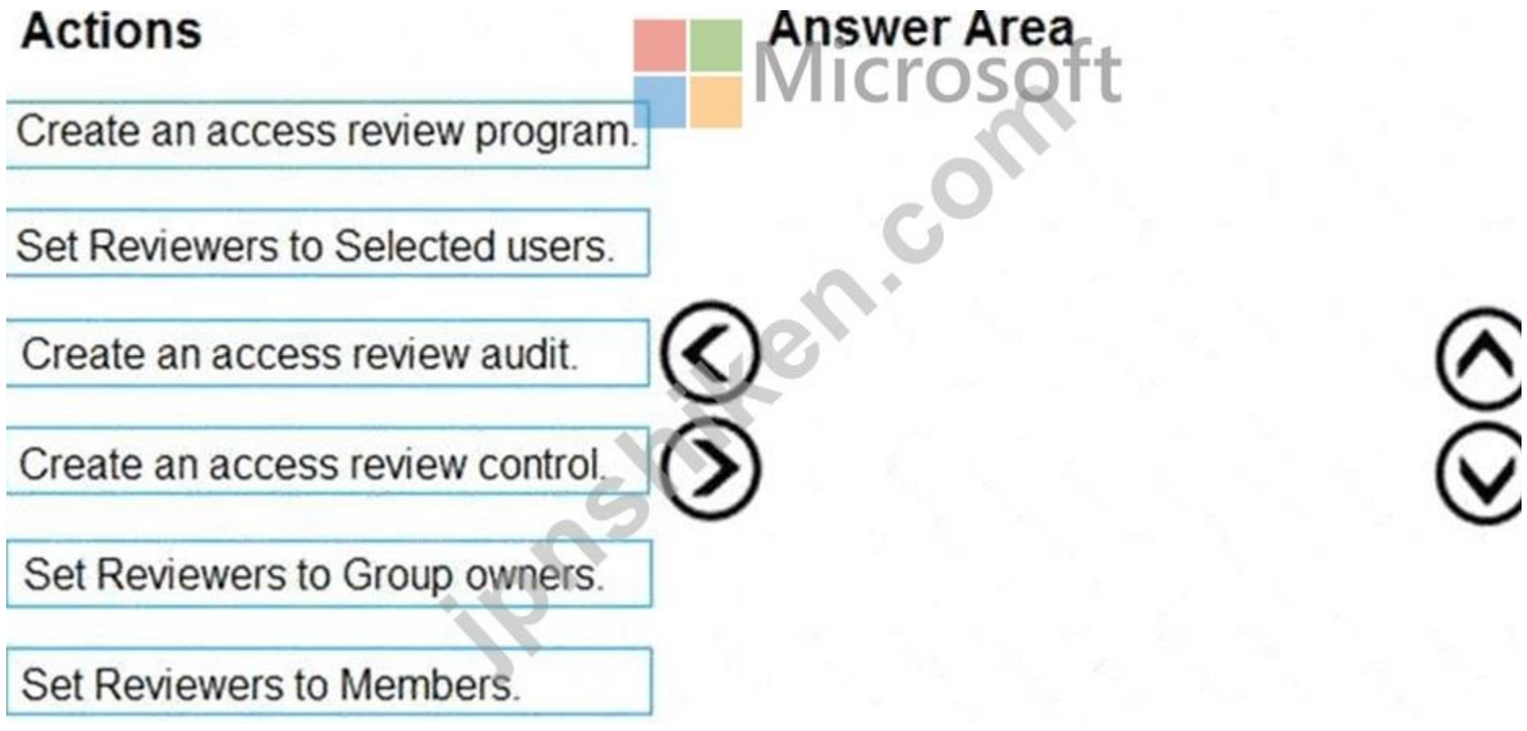


Explanation:

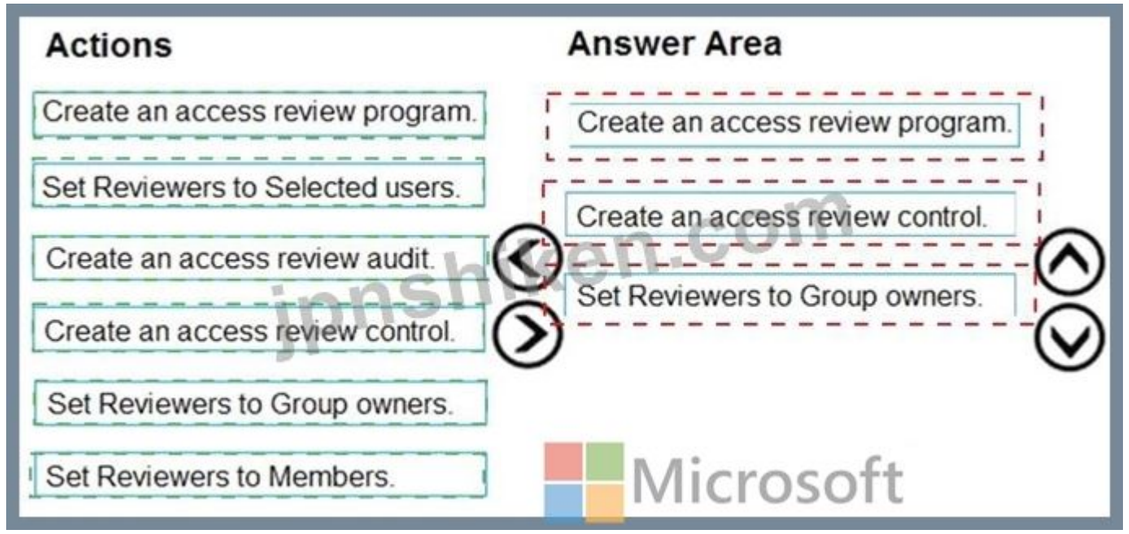
質問: **29**

アクセスレビューを設定する必要があります。レビューは新しいレビューのコレクションに割り当てられ、リソース所有者によってレビューされます。

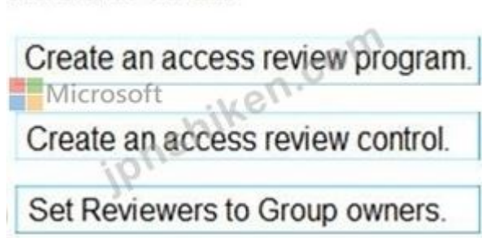
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序に並べます。



正解:



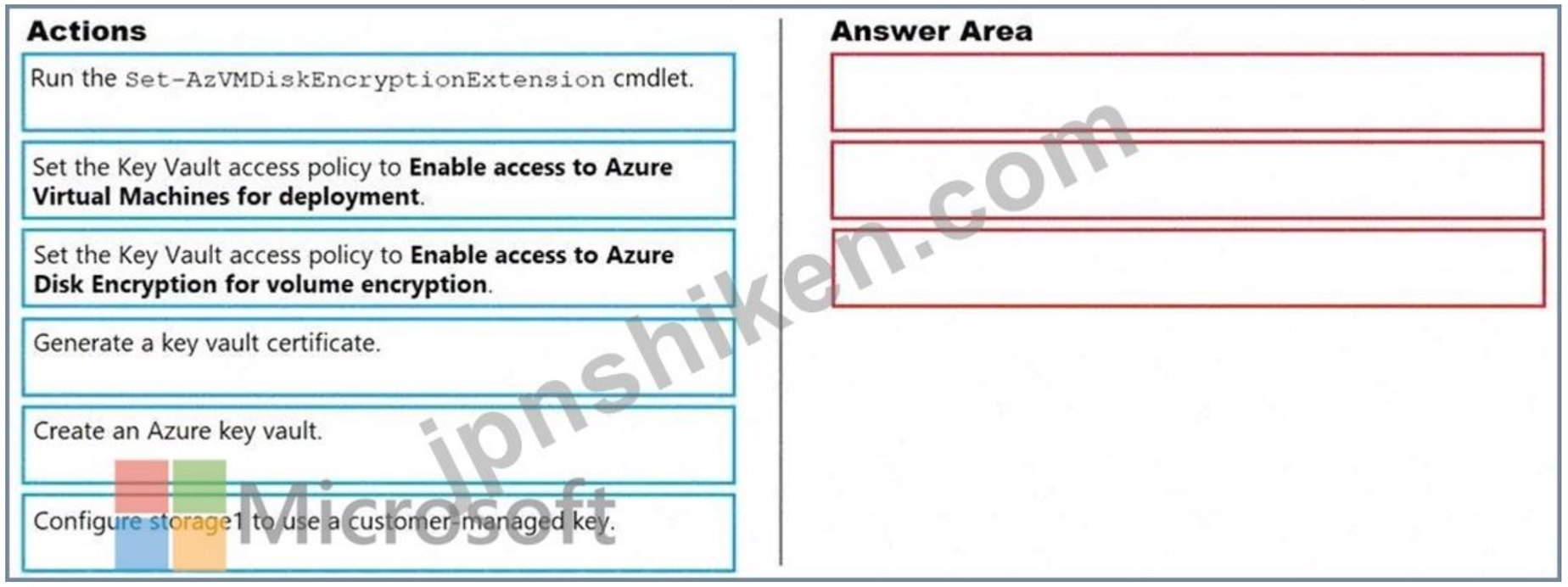
Explanation:



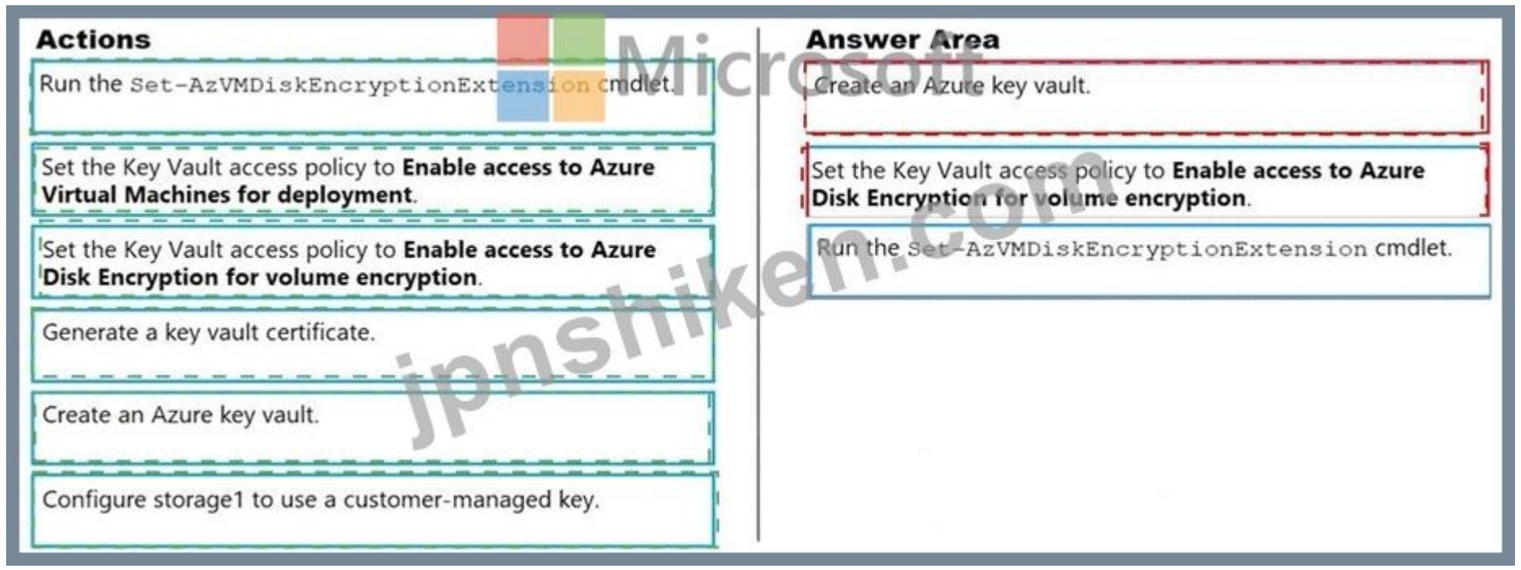
Step 1: Create an access review program
Step 2: Create an access review control
Step 3: Set Reviewers to Group owners
In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review
https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

質問: **30**
storage1という名前のAzureStorageアカウントと、VM1という名前のAzure仮想マシンがあります。VM1にはプレミアムSSDマネージドディスクがあります。
VM1に対してAzureDiskEncryptionを有効に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。



正解:



Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

質問: **31**

Azure サブスクリプションをお持ちです。

疑わしい Azure DNS アクティビティに関する通知を確実に受信する必要があります。

Cloud Workload Protection (CWP) のどの Microsoft Defender プランを有効にする必要がありますか?

A. アプリサービス

B. サーバー

C. リソースマネージャー

D. API

E. ストレージ

正解: **B (**コメントを発表する**)**

質問: **32**

Sub 1 という Azure サブスクリプションがあり、contoso.com という Azure Active Directory (Azure AD) テナントに関連付けられています。このテナントには、次の表に示すユーザーが含まれています。

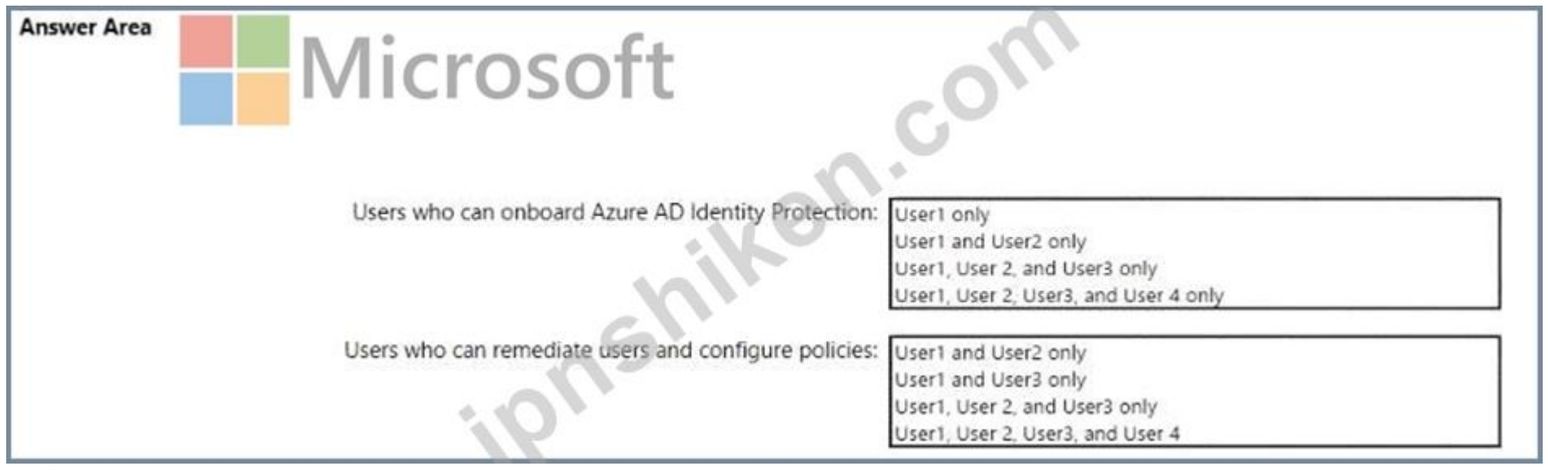
Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

各ユーザーには Azure AD Premium P2 ライセンスが割り当てられます。

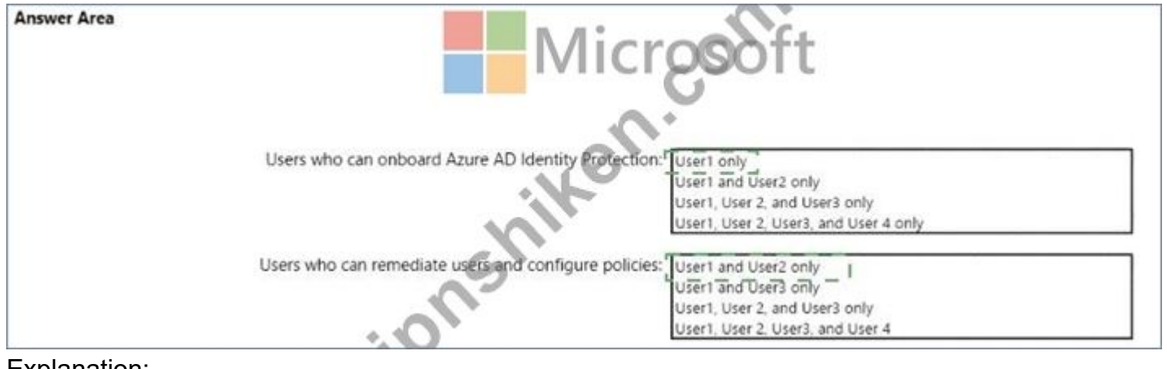
Azure AD Identity Protection のオンボードと構成を計画します。

Azure AD Identity Protection をオンボードし、ユーザーを修復し、ポリシーを構成できるのはどのユーザーですか? 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。

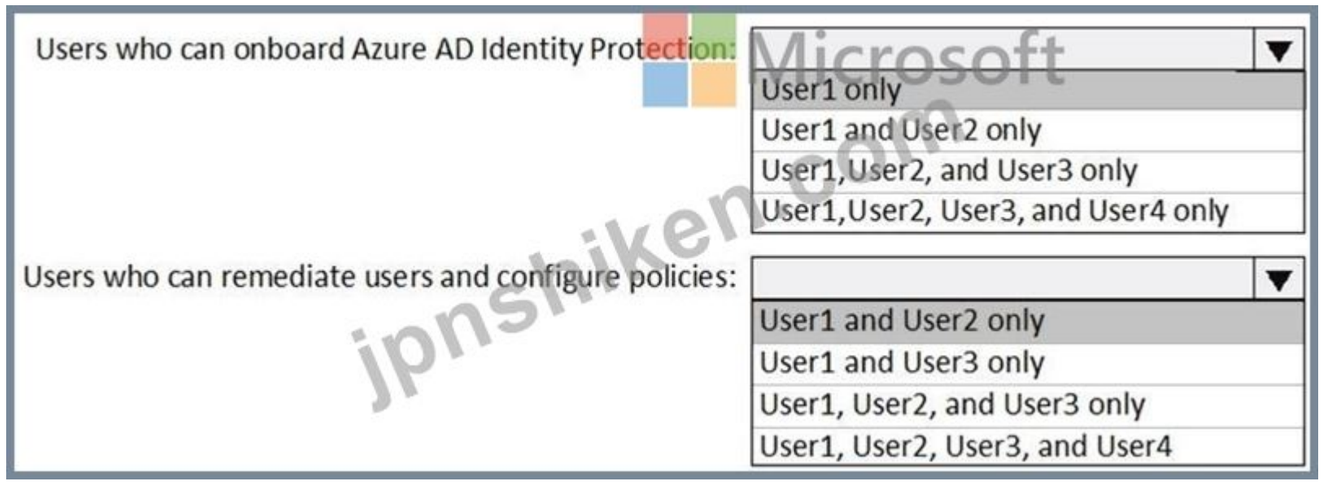
注: 正解ごとに1ポイント獲得



正解:



Explanation:



質問: **33**

あなたの会社には、weylandindustries.com という単一ドメインの Active Directory フォレストがあります。また、同じ名前の Azure Active Directory (Azure AD) テナントも存在します。

すべてのオンプレミス ID を Azure AD に同期した後、LAB で始まる givenName 属性を持つユーザーには Azure AD への同期を許可しないよう通知されます。

次のうちどのアクションを実行する必要がありますか?

A. 属性ベースのフィルタリング ルールを作成するには、同期ルール エディターを使用する必要があります。

B. ファイアウォールで DNAT ルールを構成する必要があります。

C. ファイアウォールでネットワーク トラフィック フィルタリング ルールを構成する必要があります。

D. 属性ベースのフィルタリング ルールを作成するには、Active Directory ユーザーとコンピューターを利用する必要があります。

正解: **(**正解を表示します**)**

Use the Synchronization Rules Editor and write attribute-based filtering rule.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

質問: **34**

次の表に示すストレージ アカウントを含む Azure サブスクリプションがあります。

Name	Performance	Premium account type	Redundancy	Sub-resource
storage1	Standard	*Not applicable*	Locally-redundant storage (LRS)	Two Azure Files shares
storage2	Premium	Page blobs	Locally-redundant storage (LRS)	Three containers

ストレージアカウントのターゲットサブリソースに対してプライベートエンドポイントを作成する必要があります。ソリューションでは、プライベートエンドポイントを使用してすべてのターゲットサブリソースにアクセスできるようにする必要があります。

各ストレージ アカウントに作成する必要があるプライベート 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 ポイントが付与されます。

s

正解:

Explanation:

質問: **35**

1 という名前の Azure Web アプリと VM1 という名前の仮想マシンを含む Azure サブスクリプションがあります。

VM1 は Microsoft SQL Server を実行し、VNet1 という名前の仮想ネットワークに接続します。App1、VM1、および Vent は米国中部 Azure リージョンにあります。

App1 が VM1 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コストを最小限に抑える必要があります。

A. Azure Application Gateway の統合

B. リージョン仮想ネットワーク統合

C. ゲートウェイが必要な仮想ネットワーク統合

D. アズールフロントドア

E. NAT ゲートウェイの統合

正解: **B (**コメントを発表する**)**

質問: **36**

Azure Active Directory (Azure AD) テナントがあります。テナントには、Azure AD Premium Plan 2 ライセンスが割り当てられているユーザーが含まれています。
fabrikam.com ドメインには、user' という名前のユーザーが含まれています。ユーザーのメール アドレスは userl@tabrikam.com です。
User1 にテナント内のリソースを提供する ソリューションは、次の要件を満たす必要があります。
user1 は、userl@fabrikam.com の資格情報を使用してサインインできる必要があります。テナント内のリソースへのアクセス権を User1 に付与できる必要があります。管理作業を最小限に抑える必要があります。
あなたは何をするべきか？
A. user1 のユーザー アカウントを作成します。
B. テナントに fabrikamcom をカスタム ドメインとして追加します。
C. テナントに対して [ユーザー フローによるゲスト セルフサービス サインアップを有効にする] を [はい] に設定します。
D. User1 の招待状を作成します。
正解: **(**正解を表示します**)**

質問: **37**
ネットワークに、Azure Active Directory（Azure AD）テナントと同期するオンプレミスのActive Directoryドメインが含まれています。テナントには、次の表に示すユーザーが含まれています。

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

テナントには、次の表に示すグループが含まれています。

Name	Members
Group1	User1, User2, User3
Group2	User2

次の設定を含む多要素認証（MFA）登録ポリシーを構成します。
*割り当て：
*含める：Group1
*グループ2を除外
*コントロール：Azure MFA登録が必要
*ポリシーを実施：オン
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。

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

正解:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	◉	○
User2 must configure MFA during the user's next Azure AD authentication.	○	◉
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	◉	○

Explanation:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	◉	○
User2 must configure MFA during the user's next Azure AD authentication.	○	◉
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	◉	○

質問: **38**

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、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。

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 Security Centerを使用して、3つのAzureサブスクリプションの一元化されたポリシー管理を行います。

いくつかのポリシー定義を使用して、サブスクリプションのセキュリティを管理します。
3つのサブスクリプションすべてにポリシー定義をグループとして展開する必要があります。
ソリューション：管理グループを対象とするイニシアチブと割り当てを作成します。
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**)**
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

質問: **39**
を含む Azure サブスクリプションがあります。
user1 に blob1 へのアクセスを許可する必要があります。このソリューションでは、アクセスが 6 日後に期限切れになるようにする必要があります。
何を使うべきですか？
A. 共有アクセス ポリシー
B. 共有アクセス署名 (SAS)
C. 役割ベースのアクセス制御 (RBAC)
D. マネージド ID
正解: **(**正解を表示します**)**
Depending on how you want to authorize access to blob data in the Azure portal, you'll need specific permissions. In most cases, these permissions are provided via Azure role-based access control (Azure RBAC). For more information about Azure RBAC, see What is Azure role-based access control (Azure RBAC)?.
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

質問: **40**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

テナントには、次の表に示す名前付き場所が含まれます。

Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

次の表に示すように、App1 という名前のクラウド アプリの条件付きアクセス ポリシーを作成します。

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

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 ポイントが付与されます。

正解:

Explanation:

質問: **41**

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
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

ServerAdmins が次のタスクを実行できることを確認する必要があります。

RG2 内の既存の仮想ネットワークにのみ仮想マシンを作成します。

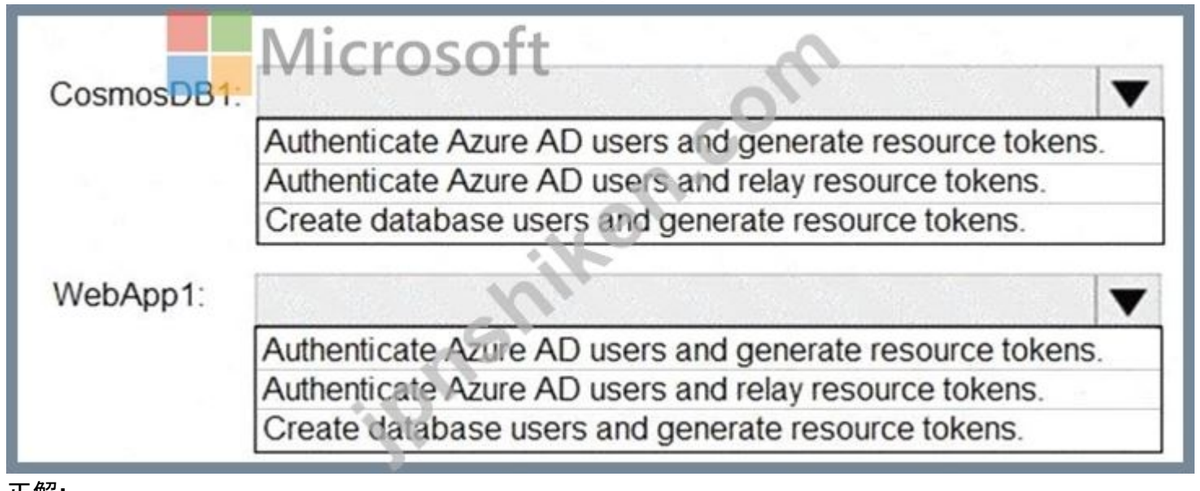
ソリューションでは最小権限の原則を使用する必要があります。

ServerAdmins に割り当てる必要がある 2 つのロールベース アクセス制御 (RBAC) ロールはどれですか。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: 正しい選択ごとに 1 ポイントが付与されます。
A. サブスクリプションの貢献者ロール
B. RG1 の仮想マシン共同作成者ロール。
C. RG1 のネットワーク コントリビューター ロール。
D. RG2のネットワーク貢献者の役割
E. RG2 のカスタム RBAC ロール
F. サブスクリプションのカスタム RBAC ロール
正解: **(**正解を表示します**)**

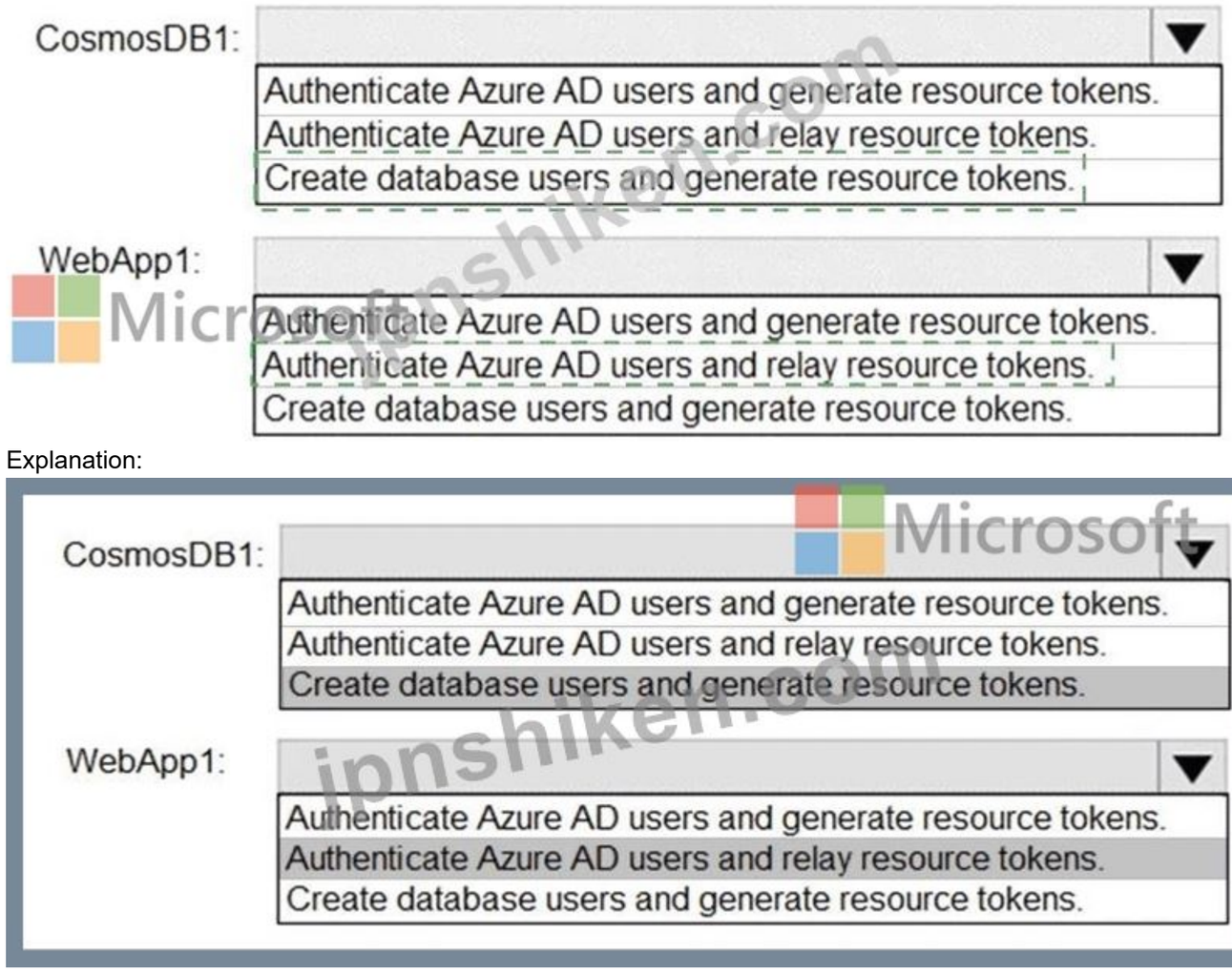
質問: **42**
contoso.com という名前の Azure Active Directory (Azure AD) テナントに関連付けられた Sub1 という名前の Azure サブスクリプションがあります。
次の表に示すリソースで構成されるアプリケーションを実装する予定です。

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

ユーザーは Azure AD ユーザー アカウントを使用して認証し、リソース トークンを使用して Cosmos DB アカウントにアクセスします。
CosmosDB1 と WebApp1 に実装されるタスクを特定する必要があります。
各リソースに対してどのタスクを特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 ポイントが付与されます。



正解:



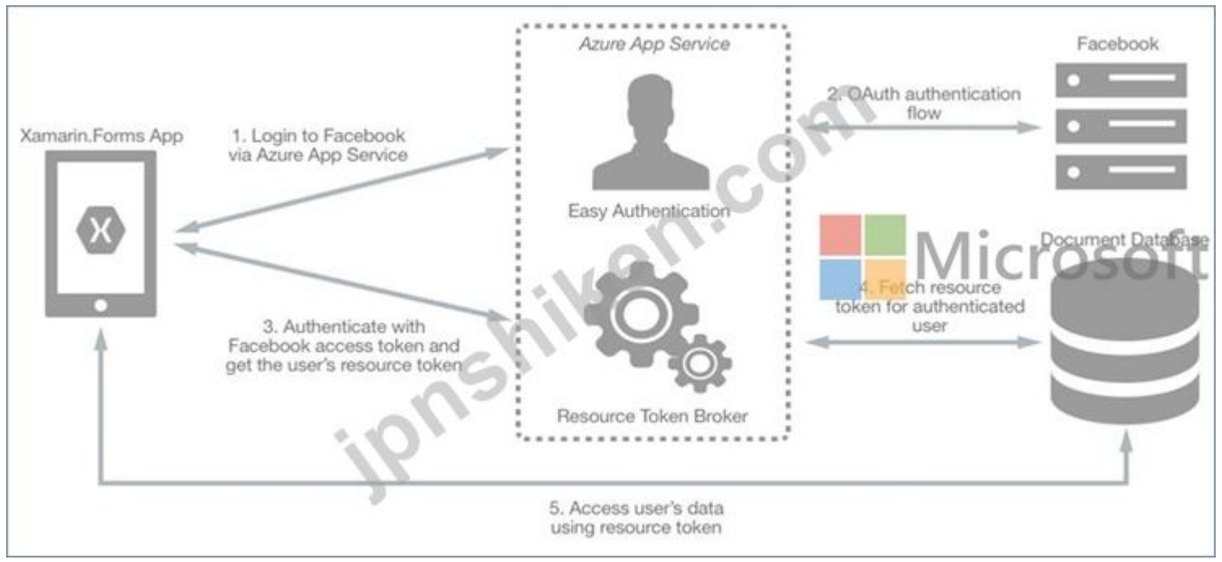
Explanation:

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

質問: 43
次の表に示すグループを含む Azure AD テナントがあります。

Name	Type	Contains members
Group1	Security	Yes
Group2	Microsoft 365	No

次の表に示すように、グループにライセンスを割り当てます。

Group	License
Group1	Azure Active Directory Premium P2
Group2	Office 365 E5
Group3	Azure Active Directory Premium P2

5 月 1 日に、Group1 を削除します。グループ2とグループ3。
次の各ステートメントについて、そのステートメントが 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: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	○	○
On May 15, you can restore Group2.	○	○
On June 3, you can restore Group3.	○	○

正解:

Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	○	○
On May 15, you can restore Group2.	○	○
On June 3, you can restore Group3.	○	○

Explanation:

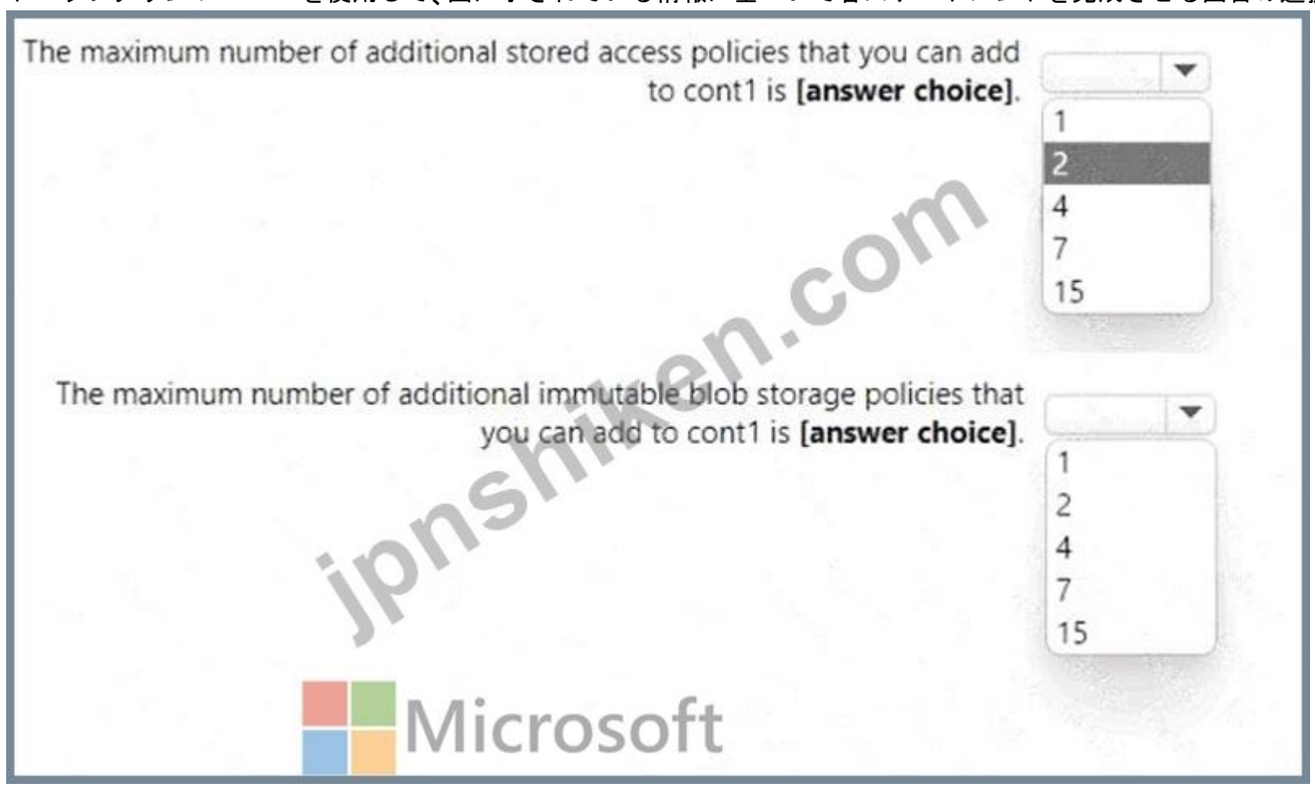
Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	◉	○
On May 15, you can restore Group2.	◉	○
On June 3, you can restore Group3.	◉	○

質問: **44**

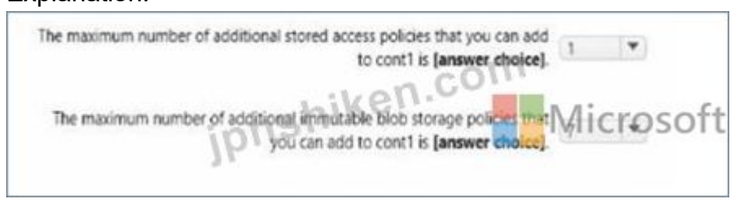
cont1 という名前の BLOB コンテナーを含む Azure サブスクリプションがあります。Cont1 には、次の資料に示すアクセス ポリシーがあります。

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ステートメントを完成させる回答の選択肢を選択します。



正解:

Explanation:



質問: **45**

Azure サブスクリプションがあります。

Role1 と Role2 という名前の 2 つのカスタム ロールを作成する予定です。

カスタム ロールは、次のタスクを実行するために使用されます。

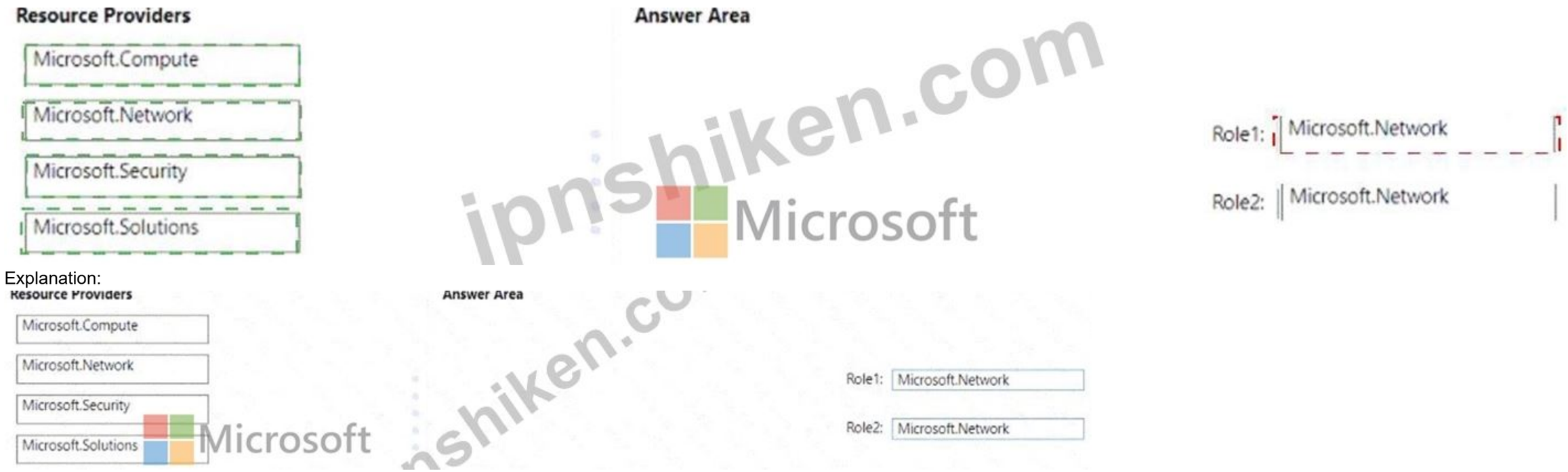
* Role1 のメンバーは、アプリケーション セキュリティ グループを管理します。

※Role2のメンバーがAzure Bastionを管理します。

カスタム ロールに権限を追加する必要があります。

各ロールにどのリソース プロバイダーを使用する必要がありますか? 答えるには、適切なリソース プロバイダーを正しいロールにドラッグします。各リソース プロバイダーは、1 回以上使用することも、まったく使用しないこともできます。ペイン間の分割バーをドラッグするか、コンテンツを表示するためにスクロールする必要がある場合があります

正解:



Explanation:

質問: **46**

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、サーバーレスRG1に10個の仮想マシン、仮想ネットワークVNET1、およびNSG1という名前のネットワークセキュリティグループ（NSG）を含むセキュリティグループがあります。ServerAdminsは、RDPを使用して仮想マシンにアクセスできます。

ServerAdminsのメンバーがアクセスを要求する場合、NSG1が最大60分間仮想へのRDP接続のみを行うようにする必要があります。

何を設定する必要がありますか？

A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.

B. a just in time (JIT) VM access policy in Azure Security Center

C. an azure policy assigned to RG1.

D. an Azure Bastion host on VNET1.

正解: **(正解を表示します)**

Reference:

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

質問: **47**

RG1という名前のリソースグループに15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。

不正なアプリケーションとマルウェアが仮想マシンで実行されるのを防ぐ必要があります。
あなたは何をするべきか？
A. AzureポリシーをRG1に適用します。
B. Azure Security Centerから、適応型アプリケーションコントロールを構成します。
C. Azure Active Directory（Azure AD）ID保護を構成します。
D. RG1にリソースロックを適用します。
正解: **B** (コメントを発表する)
Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

質問: **48**
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ます。
[展示]タブをクリックします。）

BASICS	
Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
AUTHENTICATION	
Enable RBAC	No
NETWORKING	
HTTP application routing	Yes
Network configuration	Basic
MONITORING	
Enable container monitoring	No
TAGS	

クラスターを運用環境に展開する予定です。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終了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？
A. AKS Ingressコントローラーを作成します。
B. 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。
C. Azure Standard Load Balancerを作成します。
D. Azure Basic Load Balancerを作成します。
正解: **A** (コメントを発表する)

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
References:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

質問: **49**
Azure Key Vault を含む Azure サブスクリプションをお持ちです。Key Vault のロールの割り当ては、次の図に示されています。


```
[
    {
        "RoleAssignmentId": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User2",
        "SignInName": "User2@contoso.com",
        "RoleDefinitionName": "Key Vault Crypto Officer",
        "RoleAssignmentId": "(
    `   "Scope": "/subscriptions//6c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.com",
        "RoleDefinitionName": "Key Vault Secrets Officer",
        ...
    },
    {
        "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
        "DisplayName": "User4",
        "SignInName": "User4@contoso.com",
        "RoleDefinitionName": "Key Vault Administrator",
        ...
    }
]
```


ドロップダウンメニューを使用して、図に示された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:

See the answer below at Explanation.

Explanation:

Answer is as image below.

質問: **50**

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。

Sub1という名前のAzureサブスクリプションがあります。

RG1という名前のリソースグループにsa1という名前のAzureストレージアカウントがあります。

ユーザーとアプリケーションは、いくつかの共有アクセス署名 (SAS) と保存されたアクセスポリシーを使用して、sa1のblobサービスとファイルサービスにアクセスします。

許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。

sa1へのすべてのアクセスを取り消す必要があります。

解決策 :Azureストレージアカウントのアクセスキーを再生成します。

これは目標を達成していますか？

A. はい

B. いいえ

正解: **A** (コメントを発表する)

Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

質問: **51**

VNET1およびVNET2という2つのAzure仮想ネットワーク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。
各仮想ネットワークに使用するVPNゲートウェイ SKI)はどれですか？答えるには、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、複数回、またはまったく使用できません。コンテンツを表示するには、ペイン間で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 :それぞれの正しい選択には1ポイントの価値があります

正解:

Explanation:

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

質問: **52**
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、Azure Active Directory (Azure AD) 認証を使用する VM1 という名前の仮想マシンが含まれています。
RG1 にスコープ設定された Role1 および Role2 という名前の 2 つのカスタム Azure ロールがあります。
Role1 の権限は次の JSON コードに表示されます。

```
"permissions": [
        {
            "actions": [
                "Microsoft.Compute/virtualMachines/*"
            ],
            "notActions": [
                "Microsoft.Compute/virtualMachines/delete"
            ],
            "dataActions": [],
            "notDataActions": []
        }
    ]
```

Role2 の権限は次の JSON コードに表示されます。


```
"permissions": [
        {
            "actions": [
                "Microsoft.Compute/virtualMachines/*"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
```

次の表に示すユーザーにロールを割り当てます。

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role1, Role2

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 ポイントが付与されます。

Answer Area

Statements	Yes	No
User1 can delete VM1.	○	○
User2 can delete VM1.	○	○
User3 can sign in to VM1 by using Azure AD credentials.	○	○

正解:

Answer Area

Statements	Yes	No
User1 can delete VM1.	○	○
User2 can delete VM1.	○	○
User3 can sign in to VM1 by using Azure AD credentials.	○	○

Explanation:

質問: 53

次の表に示す仮想マシンを含むSub1という名前のAzureサブスクリプションがあります。

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

承認されたユーザーがアクセスを要求するまで、RG1の仮想マシンのリモートデスクトップポートが閉じ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？

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

B. an application security group

C. Azure Active Directory (Azure AD) conditional access

D. just in time (JIT) VM access

正解: **(**正解を表示します**)**

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference:

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

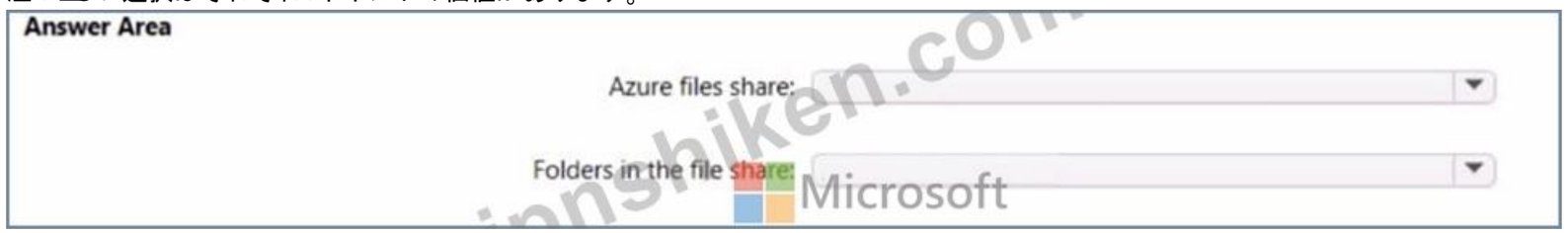
質問: **54**

Active Directoryドメインサービス（AD DS）ドメインと同期するAzureActiveDirectoryテナントがあります。

フォルダーとファイルを含むAzureファイル共有を作成する予定です。

Azureファイル共有と共有内のフォルダーにアクセス許可を割り当てるために使用できるIDストアはどれですか？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：正しい選択はそれぞれ1ポイントの価値があります。

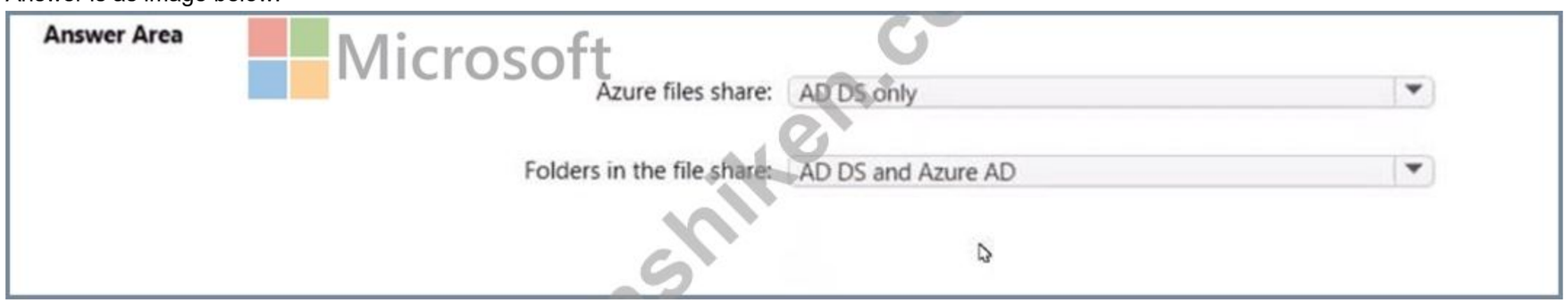


正解:

See the answer below at Explanation.

Explanation:

Answer is as image below.



質問: **55**

次の表に示すユーザーを含む Microsoft Entra テナントがあります。

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled

次の設定を持つ Microsoft Entra Identity Protection サインイン リスク ポリシーを作成して適用します。

* 割り当て: Group1 を含み、Group2 を除く

※条件 :サインインリスクレベル：低以上

* アクセス: アクセスを許可、多要素認証が必要

ユーザーが Microsoft Entra ID にサインインするときに何が起こるかを特定する必要があります。

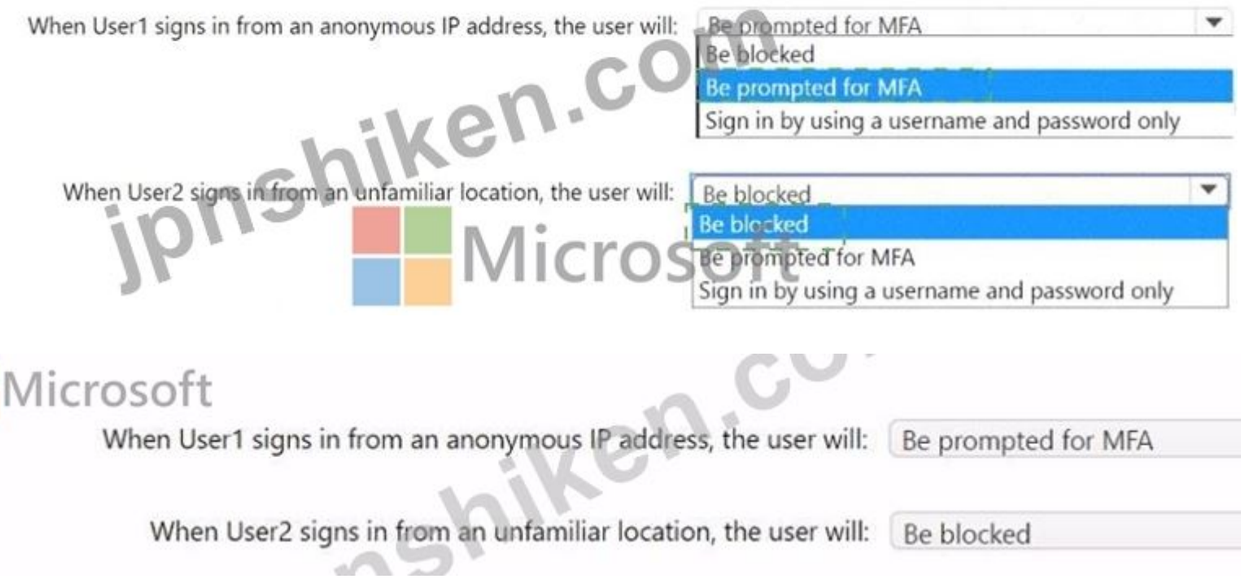
各ユーザーについて何を識別する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

正解:

Answer Area



Explanation:

Answer Area

質問: **56**

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	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

次の表に示す Azure ポリシーを作成します。

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

次の表に示すリソース ロックを作成します。

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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 ポイントが付与されます。

正解:

Explanation:

NO

NO

NO

1.) cannot perform write operation because following scope(s) are locked:

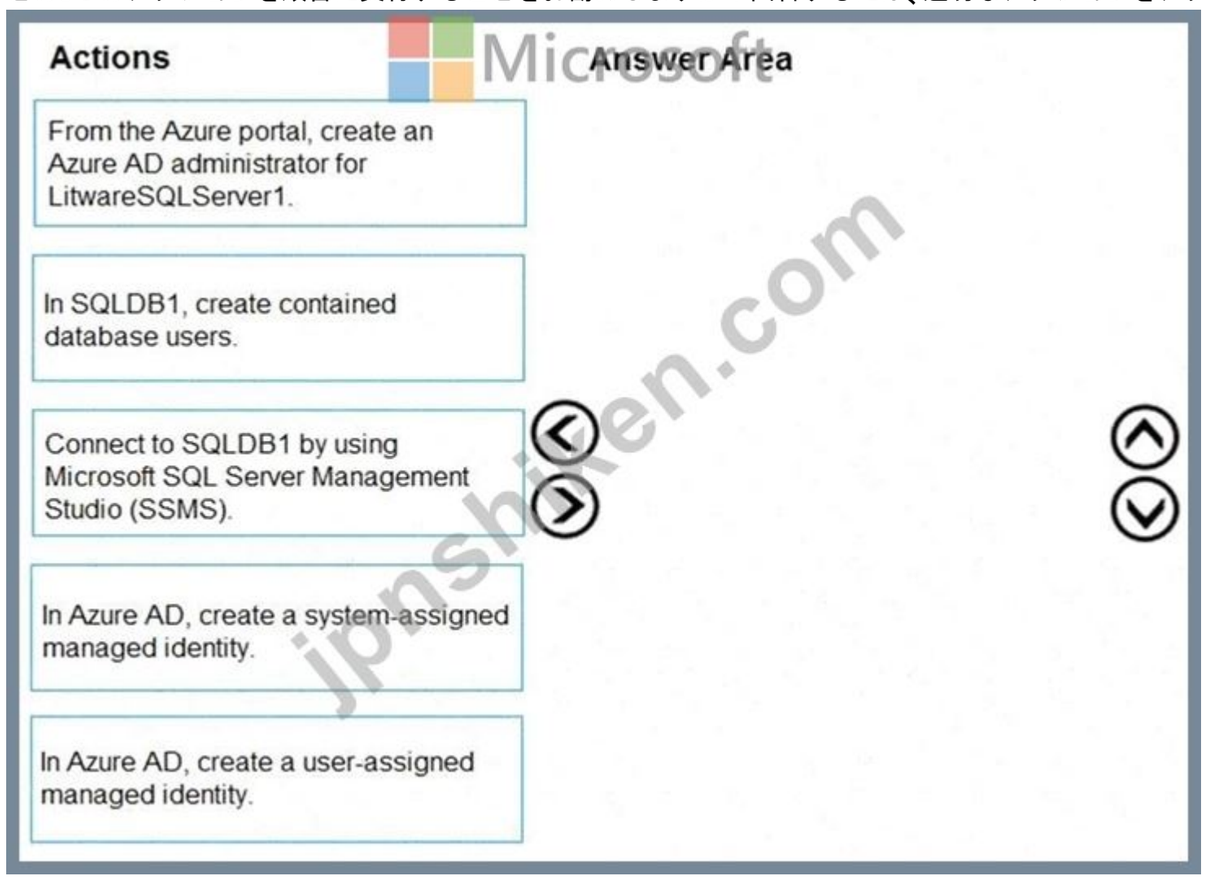
' subscriptions/xxxx/resourceGroups/xxx ' Please remove the lock and try again.

2.) When creating a VM in a resource group with a Read Only lock an error is shown:

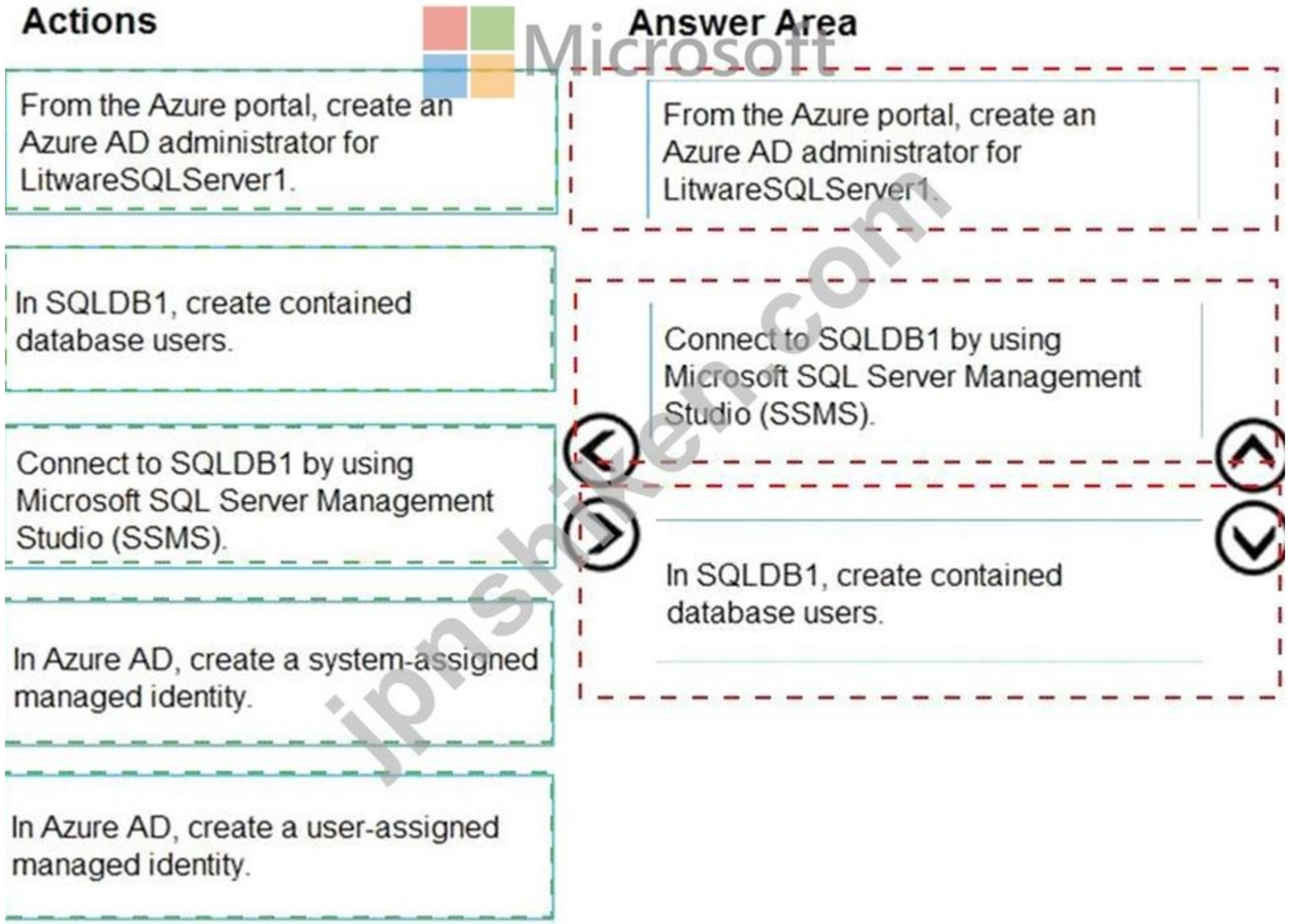
" The selected resource group is read only "

3.) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.
The article referenced in the answer states different because that is scoped to blueprints.
In the Lock Resources pages is states the following regarding starting VMs:
" A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request. "
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

質問: **57**
データとアプリケーションの要件を満たすようにSQLDB1を構成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ことをお勧めしますか？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エリアに移動し、正しい順序に並べます。



正解:



Explanation:
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS In SQLDB1, create contained database users
https://www.youtube.com/watch?v=pEPyPsGEevw

質問: **58**
Azure サブスクリプションをお持ちです。
次のカスタム ロールベース アクセス制御 (RBAC) ロール定義があります。

```
{
    "properties": {
        "roleName": "CustomRole",
        "assignableScopes": [
            "/subscriptions/<subid>"
        ],
        "permissions": [
            {
                "actions": [
                    "*"
                ],
                "notActions": [
                    "Microsoft.Authorization/*/Delete",
                    "Microsoft.Authorization/*/Write",
                    "Microsoft.Authorization/elevateAccess/Action",
                    "Microsoft.Sql/servers/administrators/write",
                    "Microsoft.Sql/servers/administrators/delete"
                ],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

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 ポイントが付与されます。

Answer Area

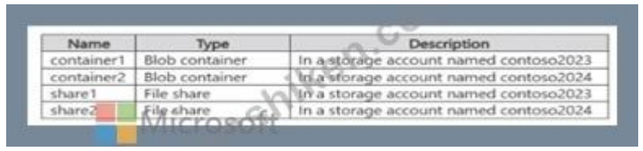
Statements	Yes	No
The custom role grants a user permission to delete Azure SQL Database resources.	○	○
The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server.	○	○
The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB.	○	○

正解:

Explanation:

質問: **59**

お客様は、以下の表に示すリソースを含む Azure サブスクリプションをお持ちです。



Name	Type	Description
container1	Blob container	In a storage account named contoso2023
container2	Blob container	In a storage account named contoso2024
share1	File share	In a storage account named contoso2023
share2	File share	In a storage account named contoso2024

次の図に示すように、共有アクセストークンを作成します。

All services > Storage accounts > contoso2023 > container1

container1 | Shared access tokens

Container

Search (Ctrl+/)

- Overview
- Diagnose and solve problems
- Access Control (IAM)

Settings

- Shared access tokens
- Access policy
- Properties
- Metadata

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage container. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. Learn more about creating an account SAS

Signing method

(•) Account key ( ) User delegation key

Signing key

Key 1

Stored access policy

None

Permissions *

7 selected

Start and expiry date/time

Start

01/01/2022 11:51:13 AM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Expiry

01/01/2030 7:51:13 PM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses

for example, 168.1.5.65 or 168.1.5.65-168.1....

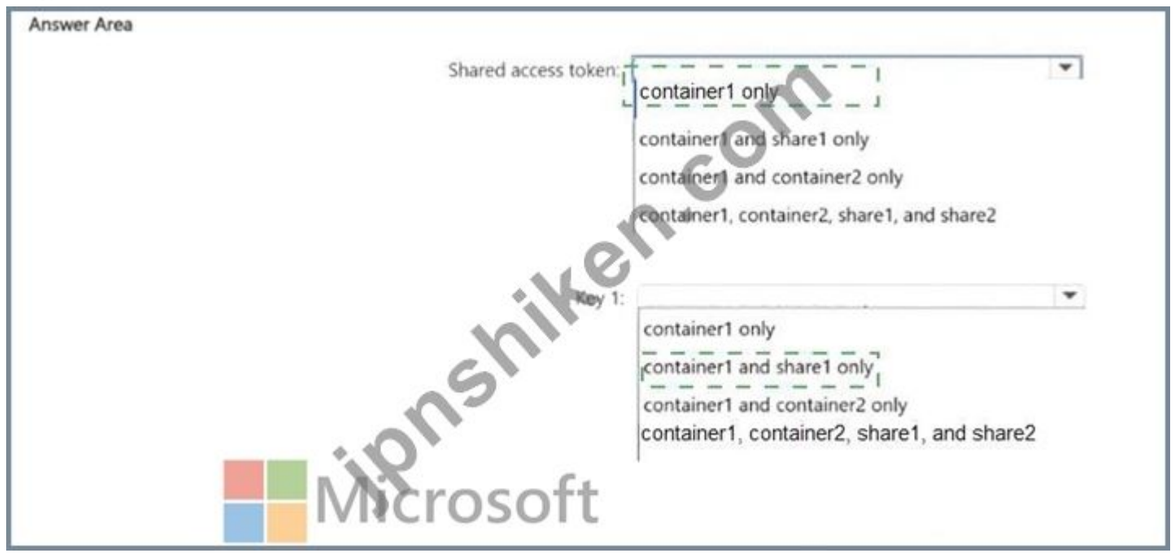
Allowed protocols

(•) HTTPS only ( ) HTTPS and HTTP

Generate SAS token and URL

共有アクセストークンとキー1を使用してアクセスできるリソースはどれですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

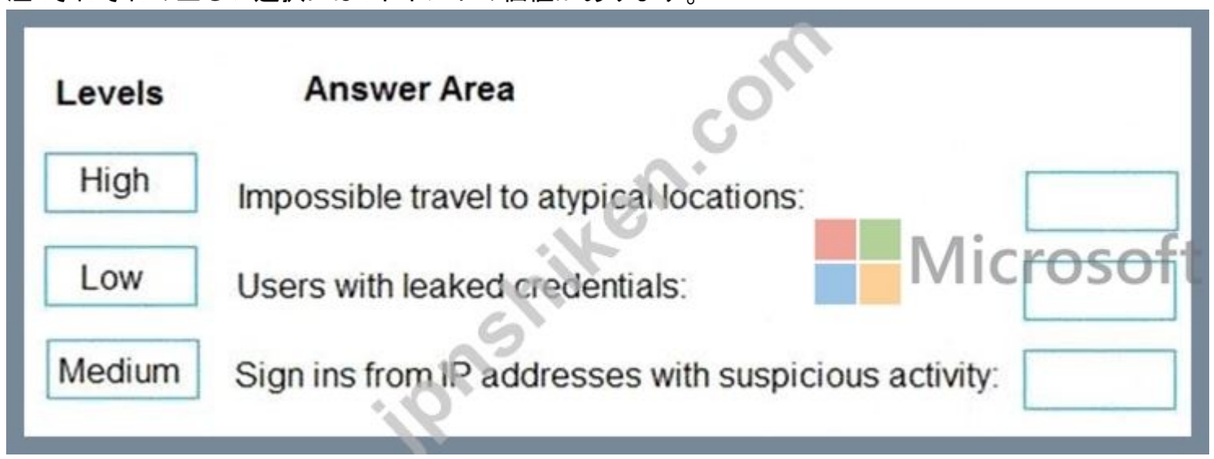
正解:



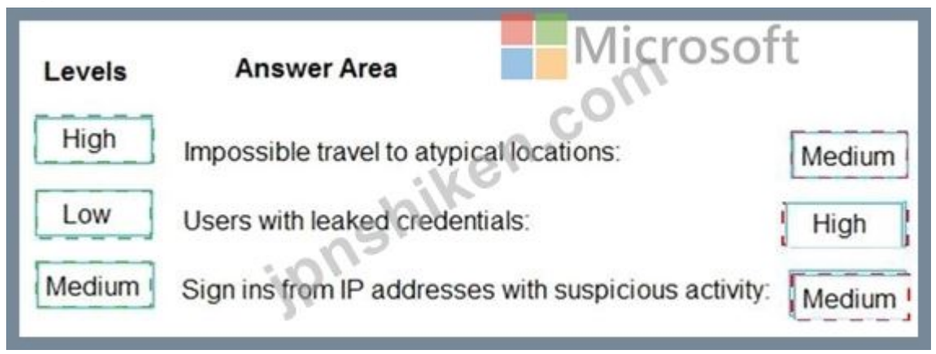
Explanation:

質問: **60**
条件付きアクセスポリシーを実装しています。

ポリシーを構成して実装するには、既存のAzure Active Directory (Azure AD)のリスクイベントとリスクレベルを評価する必要があります。
次のリスクイベントのリスクレベルを識別する必要があります。
*漏洩した資格情報を持つユーザー
*非典型的な場所への移動は不可能
*不審なアクティビティがあるIPアドレスからサインインする
リスクイベントごとにどのレベルを識別する必要がありますか？答えるには、適切なレベルを正しいリスクイベントにドラッグします。各レベルは、1回、複数回、またはまったく使用されません。コンテンツを表示するには、ペイン間で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 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:
Medium
High
Medium
Refer https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign- ins-from-ip-addresses-with-suspicious-activity

質問**: 61**
Azure Key Vaultを含むAzureサブスクリプションをお持ちです。
storage1という名前のストレージアカウントを作成します。
あなたは以下のストレージサービスにデータを保存する予定です。
* Azure Files

* Azure Blobストレージ
* Azure Table Storage
* Azure キュー ストレージ
キー保管庫に保存されているキーを使用してデータ暗号化を設定できるサービスは、どれとどれですか？正解はそれぞれ完全な解決策を示しています。
注：正解ごとに1ポイントが加算されます。
A. Azure Files
B. キューストレージ
C. テーブルストレージ
D. ブロブストレージ
正解: **(**正解を表示します**)**

質問: **62**
Contoso.com という名前のハイブリッド Microsoft Entra テナントがあり、そこには Uset1 という名前のユーザーと、次の表に示すサーバーが含まれています。

Name	Operating system	Configuration
Server1	Windows Server 2016	Domain-joined
Server2	Windows Server 2022	Domain-joined

テナントは、storage1 というストレージ アカウントを含む Azure サブスクリプションにリンクされています。storage1 アカウントには、shares1 というファイル共有が含まれています。
User1 には、storages1 のストレージ ファイル データ SMB 共有共同作成者ロールが割り当てられています。
storage1 のファイル共有のセキュリティ プロトコル設定は、次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 ポイントが付与されます。

Answer Area

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	○	○
User1 can map share1 to Server1 by using the user's credentials.	○	○
User1 can map share1 to Server2 by using the access key of storage1.	○	○

正解:

Answer Area

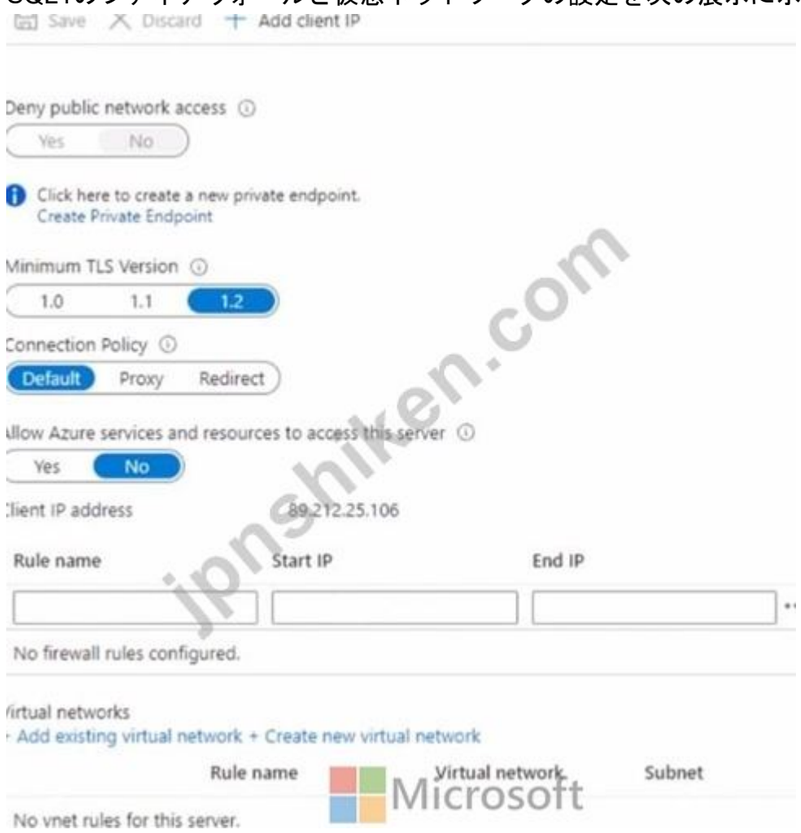
Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	○	
User1 can map share1 to Server1 by using the user's credentials.		○
User1 can map share1 to Server2 by using the access key of storage1.	○	

Explanation:

質問: 63

SQLという名前のAzureSQLデータベースロジックサーバーを含むAzureサブスクリプションがあります。VM1という名前のAzure仮想マシン。VM1はプライベートIPアドレスのみを使用します。

SQL1のファイアウォールと仮想ネットワークの設定を次の展示に示します。



VM1がSQL1に接続できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。あなたは何をするべきか？

A. 接続ポリシーをプロキシに設定します。

B. [Azureサービスとリソースにこのサーバーへのアクセスを許可する]を[はい]に設定します。

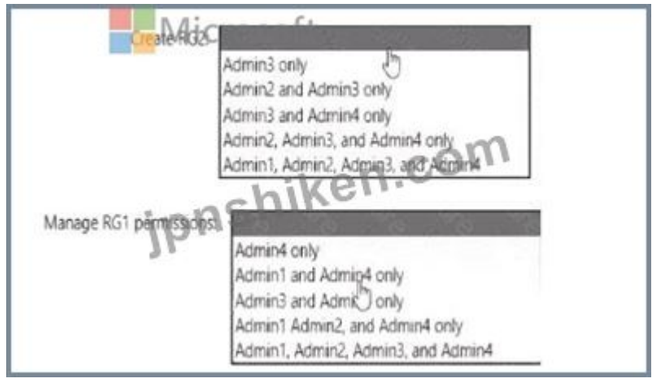
C. 新しいファイアウォールルールを作成します。

D. 既存の仮想ネットワークを追加します。

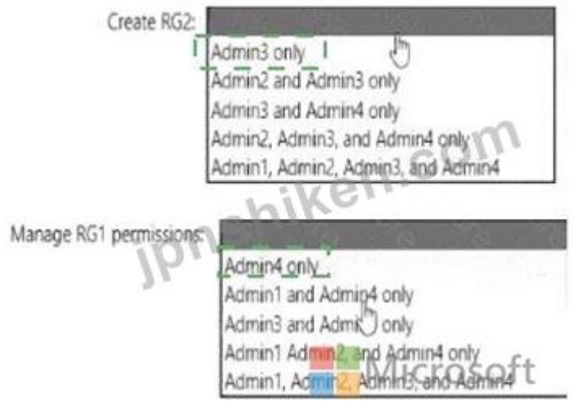
正解: **C** (コメントを発表する)

質問: 64

RG2の作成とRG1の権限の管理を委任する必要があります。どのユーザーが各タスクを実行できますか？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。注：丅しい選択はそれぞれ1ポイントの価値があります

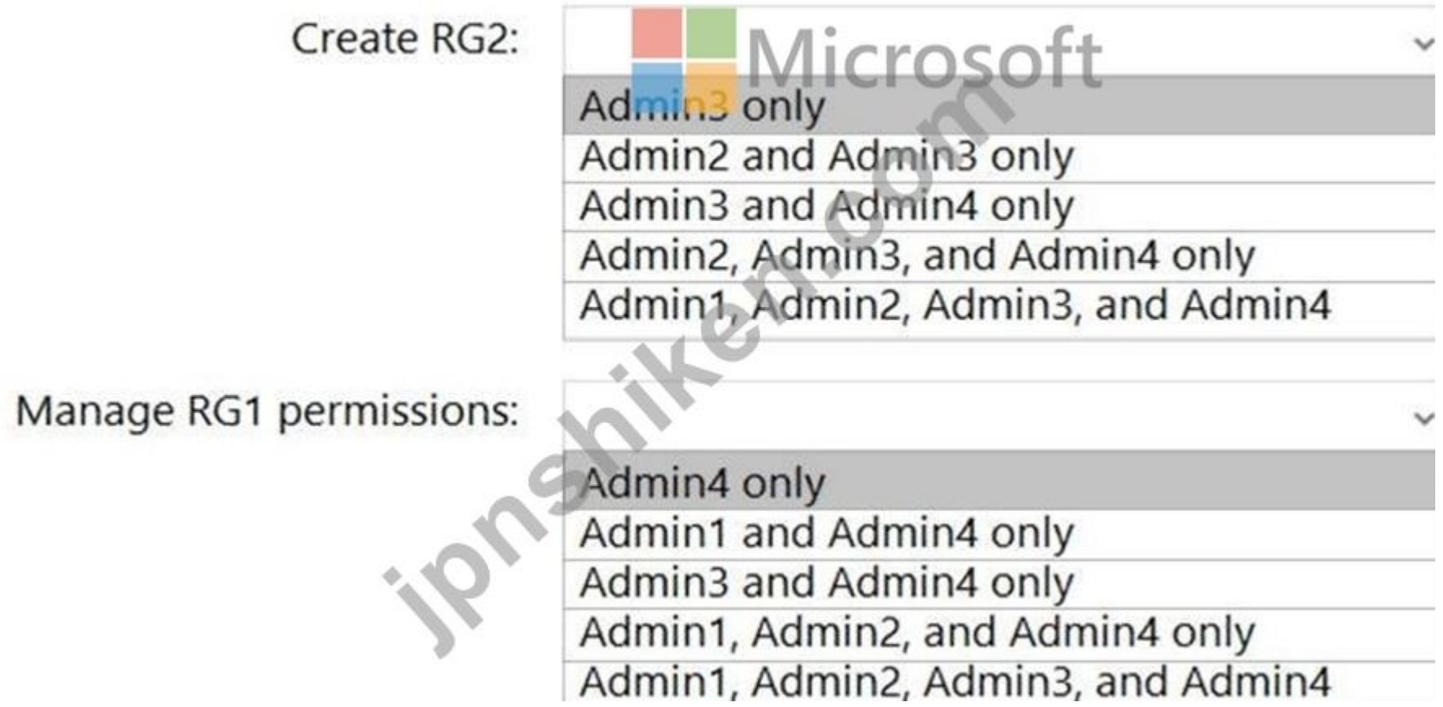


正解:



Explanation:

Graphical user interface, text, application, chat or text message Description automatically generated



Box 1: Admin3 only

The Contributor role has the necessary write permissions to create the resource group.

Box 2: Admin4 only

You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

質問: **65**

あなたは、contoso.com という名前の Microsoft Entra テナントにリンクされた Azure サブスクリプションを持っています。contoso.com に App1 という名前のアプリケーションを登録します。App1 の登録に Android アプリケーション用のプラットフォーム構成を追加する必要があります。Azure ポータルで何を構成する必要がありますか？

A. 認証

B. ブランディングとプロパティ

C. マニフェスト

D. トークン設定

正解: **A (**コメントを発表する**)**

質問: **66**

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、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。

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 Active Directory (Azure AD)のハイブリッド構成があります。

仮想ネットワーク上にAzure HDInsightクラスターがあります。

オンプレミスのActive Directory資格情報を使用して、ユーザーがクラスターに対して認証できるようにする予定です。

計画された認証をサポートするように環境を構成する必要があります。

ソリューション：Azure Active Directoryドメインサービス（Azure AD DS）をAzureサブスクリプションに展開します。
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**)**
References:
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure-adds

質問: **67**
ネットワークには、contoso.comという名前のActive Directoryフォレストが含まれています。フォレストには単一のドメインが含まれます。
contoso.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。
Azure AD Connectを展開し、Active DirectoryとAzure ADテナントを統合する予定です。
次の要件を満たす統合ソリューションを推奨する必要があります。
テナントに同期されるユーザーアカウントにパスワードポリシーとユーザーログオン制限が適用されるようにします。ソリューションに必要なサーバーの数を最小限にします。
どの認証方法を推奨事項に含める必要がありますか？
A. Active Directoryフェデレーションサービス（AD FS）とのフェデレーションID
B. シームレスシングルサインオン（SSO）によるパスワードハッシュ同期
C. シームレスシングルサインオン（SSO）を使用したパススルー認証
正解: **C (**コメントを発表する**)**
1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.
2. Minimizes the number of servers required for the solution.
>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.
>> PW Hash also require installing Azure AD Connect on your existing DC.

質問: **68**
次の表に示すユーザーを含む Azure AD テナントがあります。

Name	Description
User1	Uses app password authentication for the Mail and Calendar app in Windows 10
User2	Uses Outlook on the web

ユーザーがアプリパスワードを作成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では、ユーザー1が引き続きメールとカレンダーアプリを使用できるようにする必要があります。
何をすべきでしょうか?
A. Azure AD パスワード保護を有効にします。
B. 多要素認証 (MFA) 登録ポリシーを構成します。
C. ユーザーに認証ポリシー管理者の役割を割り当てます。
D. 新しいアプリ登録を作成します。
正解: **B (**コメントを発表する**)**

質問: **69**
次の表に示すリソースを含むSubscription1という名前のAzureサブスクリプションがあります。

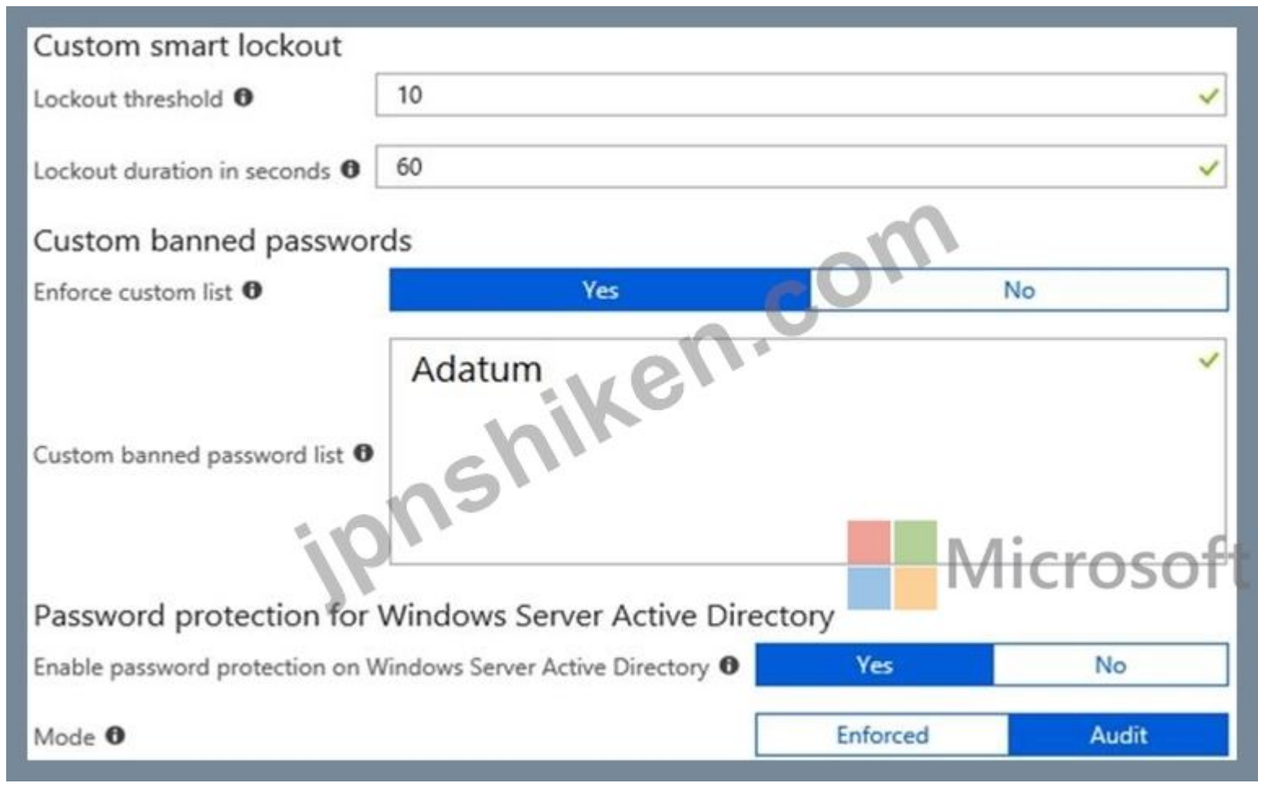
Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

Azure Security Centerを使用して、Subscription1に追加できるイニシアチブとポリシー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？
A. Policy1とPolicy2のみ
B. イニシアチブ1のみ
C. イニシアチブ1とイニシアチブ2のみ
D. イニシアチブ1、イニシアチブ2、ポリシー1、およびポリシー2
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies

質問: **70**
ネットワークには、Azure Active Directory (Azure AD) と同期する adatum.com という名前のオンプレミスの Active Directory ドメインが含まれています。
Azure AD テナントには、次の表に示すユーザーが含まれます。

Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

次の図に示すように、adatum.com の認証方法 - パスワード保護設定を構成します。



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。

注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

Text Description automatically generated

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	○	○
User2 can change the password to @d@tum_C0mpleX123.	○	○
User3 can change the password to Adatum123!.	○	○

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises- deploy
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

質問: **71**
4つのAzureSQLマネージドインスタンスを含むAzureサブスクリプションがあります。
SQLインジェクション攻撃に対するマネージドインスタンスの脆弱性を評価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. SQLヘルスチェックソリューションをAzureMonitorに追加します。
B. Azure Advanced Threat Protection（ATP）インスタンスを作成します。
C. 高度なデータセキュリティを有効にします。
D. AzureSentinelワークスペースを作成します。
正解: **(**正解を表示します**)**

質問: **72**
Group1のIDおよびアクセス要件を満たす必要があります。
あなたは何をするべきか？
A. メンバーシップルールをGroup1に追加します。
B. Group1を削除します。Office 365のメンバーシップタイプを持つGroup1という名前の新しいグループを作成します。グループにユーザーとデバイスを追加します。
C. Group1のメンバーシップルールを変更します。
D. Group1のメンバーシップタイプを割り当て済みに変更します。動的なメンバーシップを持つ2つのグループを作成します。新しいグループをGroup1に追加します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure- portal

質問: **73**
ネットワークには、corp.contoso.comという名前のオンプレミスActive Directoryドメインが含まれています。
contoso.comという名前のAzure Active Directory（Azure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。
すべての社内IDをAzure ADに同期します。
TESTで始まるgivenName属性を持つユーザーがAzure ADに同期されないように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。
何を使うべきですか？
A. 同期ルールエディター
B. Webサービス構成ツール
C. Azure AD Connectウィザード
D. Active Directoryユーザーとコンピューター
正解: **(**正解を表示します**)**
Use the Synchronization Rules Editor and write attribute-based filtering rule.
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

質問: **74**
新しいAzureサブスクリプションを作成します。
Azure Security Centerでカスタムアラートルールを作成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？それぞれの正解はソリューションの一部を示しています。
注 :それぞれの正しい選択には1ポイントの価値があります。
A. オンボードAzure Active Directory（Azure AD）ID保護。
B. Azureストレージアカウントを作成します。
C. Azure Advisorの推奨事項を実装します。
D. Azure Log Analyticsワークスペースを作成します。
E. Security Centerの価格帯をStandardにアップグレードします。
正解: **D,E (**コメントを発表する**)**
D: You need write permission in the workspace that you select to store your custom alert.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

質問: **75**
プラットフォーム保護要件を満たすには、Role1 を作成する必要があります。
Role1 のロール定義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てください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

```
{
  "Name":  "Role1",
  "Id":  "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
        [ "Microsoft.Compute/" | "Microsoft.Resources/" | "Microsoft.Storage/" ] [ "disks/*" | "storageAccounts/*" | "virtualMachines/disks/*" ]
        ],
  "NotActions":  [
                 ],
  "AssignableScopes" :  [
        [ "/" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4" ]
                      ]
}
```

正解:

```
{
  "Name":  "Role1",
  "Id":  "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
        [ "Microsoft.Compute/" | "Microsoft.Resources/" | "Microsoft.Storage/" ] [ "disks/*" | "storageAccounts/*" | "virtualMachines/disks/*" ]
        ],
  "NotActions":  [
                 ],
  "AssignableScopes" :  [
        [ "/" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1" | "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4" ]
                      ]
}
```

Explanation:
1) Microsoft.Compute/
2) disks
3) /subscrption/{subscriptionId}/resourceGroups/{Resource Group Id}
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.
Topic 1, Litware, inc
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 question on 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 sections 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 on 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.
Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.
Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.
The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subent0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com.
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:

* All San Francisco users and their devices must be members of Group1.
* The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
* Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

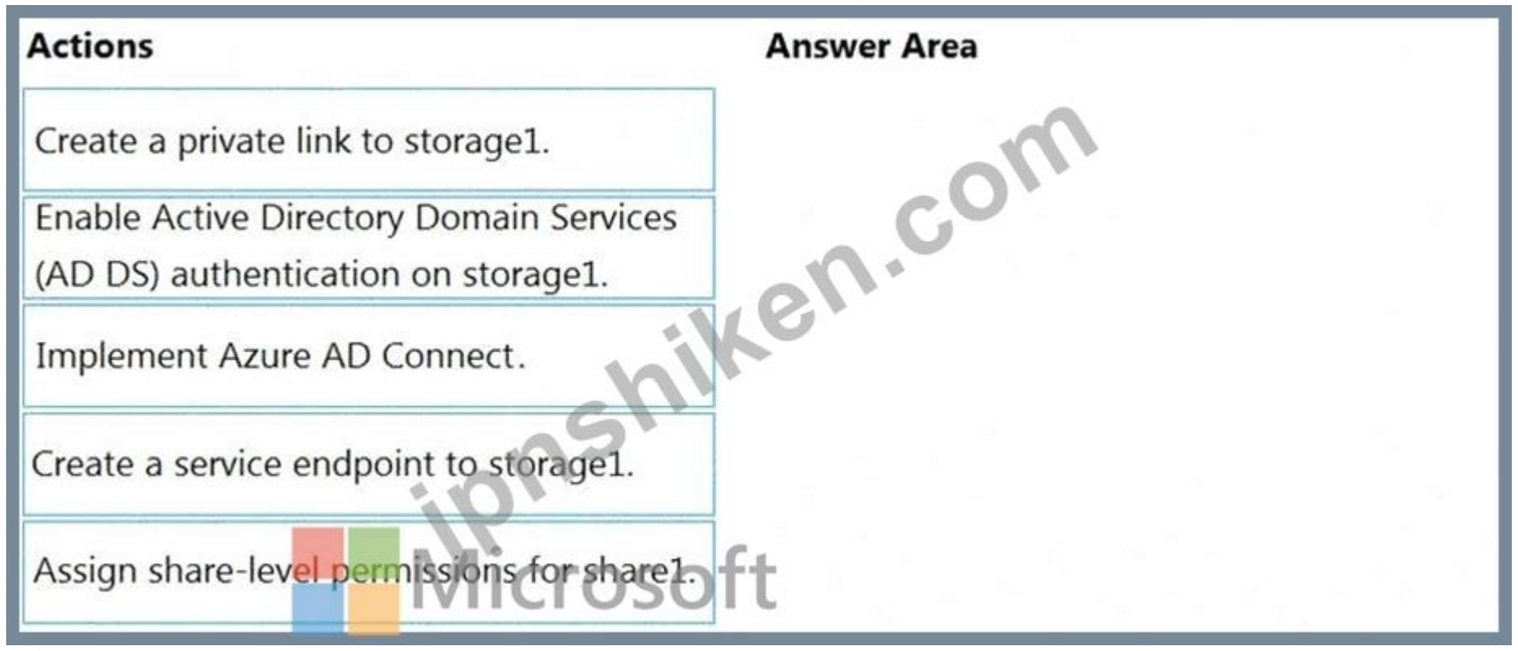
* Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
* The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
* Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
* Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
* A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements

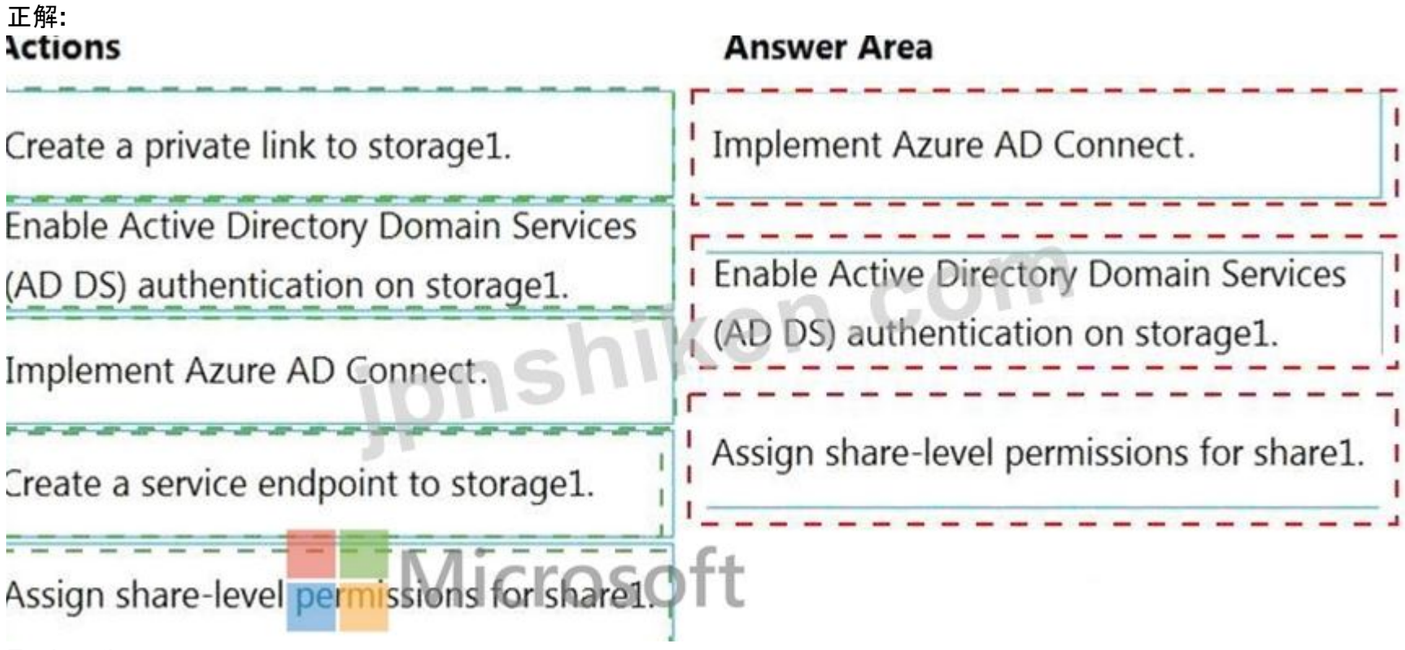
Litware must be able to customize the operating system security configurations in Azure Security Center.

質問: 76

ネットワークには、contoso.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。ドメインには、User1という名前のユーザーが含まれています。
contoso.comという名前のAzureActive Directory（Azure AD）テナントにリンクされているAzureサブスクリプションがあります。テナントには、storage1という名前のAzureStorageアカウントが含まれています。Storage1には、share1という名前のAzureファイル共有が含まれています。
現在、ドメインとテナントは統合されていません。
User1がドメイン資格情報を使用してshare1にアクセス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。



正解:

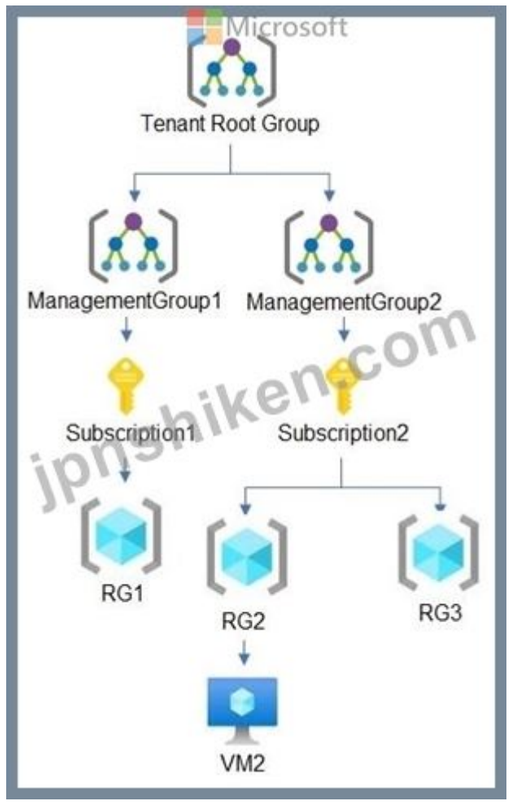


Explanation:

Implement Azure AD Connect.
Enable Active Directory Domain Services (AD DS) authentication on storage1.
Assign share-level permissions for share1.

Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

質問: **77**
次の展示に示すAzureリソースの階層があります。



RG1、RG2、およびRG3はリソースグループです。
RG2には、VM1という名前の仮想マシンが含まれています。

次の表に示すユーザーに、役割ベースのアクセス制御 RBAC)の役割を割り当てます。

Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

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
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○

正解:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○

Explanation:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○

質問: **78**
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。仮想マシンのネットワーク構成は次の表のとおりです。

Name	Public IP address	Connected to
VM1	52.232.128.194	VNET1/Subnet1
VM2	52.233.129.82	VNET2/Subnet2
VM3	52.233.130.11	VNET3/Subnet3

仮想ネットワーク サブネットには、次の表に示すようにサービス エンドポイントが定義されています。

Name	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET2/Subnet2	None
VNET3/Subnet3	Microsoft.KeyVault

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

* アクセスを許可するネットワーク: 選択したネットワーク
* 仮想ネットワーク: VNET3\Subnet3
* ファイアウォール - アドレス範囲: 52.233.129.0/24

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。

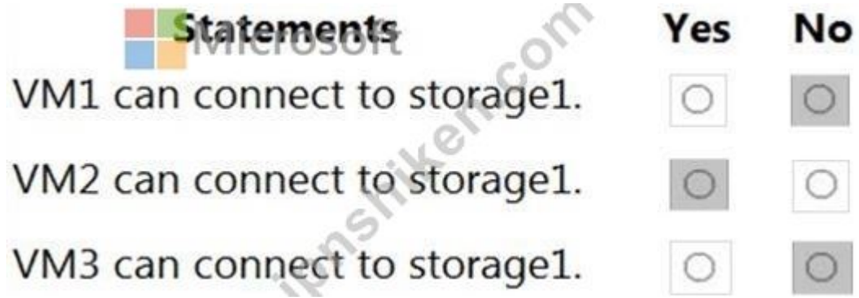
注意: 正しい選択ごとに 1 ポイントが付与されます。

Statements	Yes	No
VM1 can connect to storage1.	○	○
VM2 can connect to storage1.	○	○
VM3 can connect to storage1.	○	○

正解:

Statements	Yes	No
VM1 can connect to storage1.	○	○
VM2 can connect to storage1.	○	○
VM3 can connect to storage1.	○	○

Explanation:



Box 1: No

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

Box 3: No

Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

質問**: 79**

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

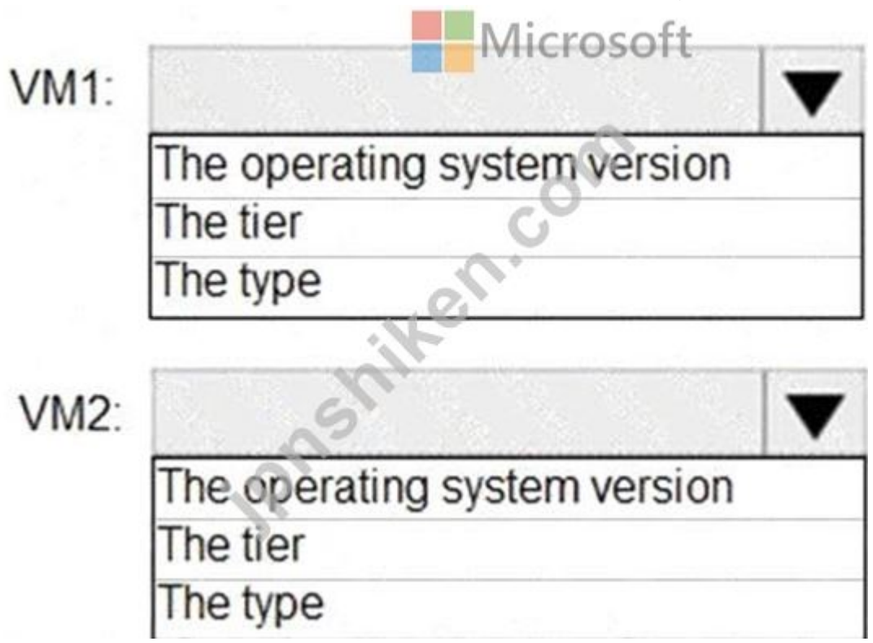
Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

Azure Key Vaultをデプロイして構成します。

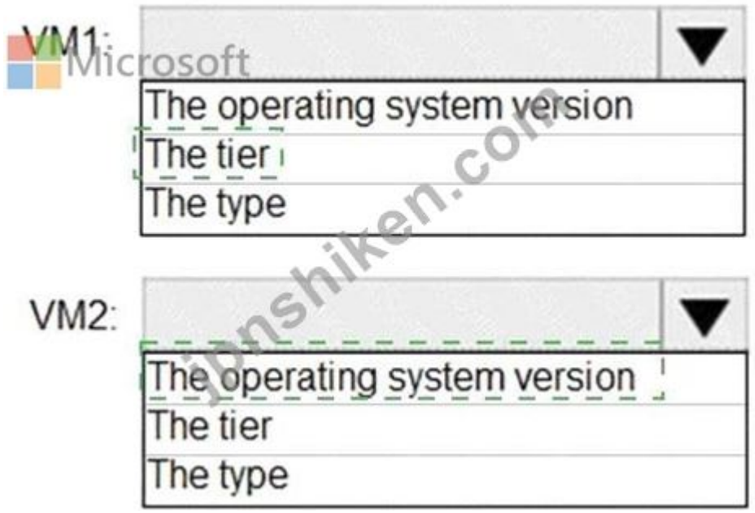
VM1およびVM2でAzure Disk Encryptionを有効にできることを確認する必要があります。

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、回答エリアで適切なオプションを選択します。

注 :それぞれの正しい選択には1ポイントの価値があります。



正解:

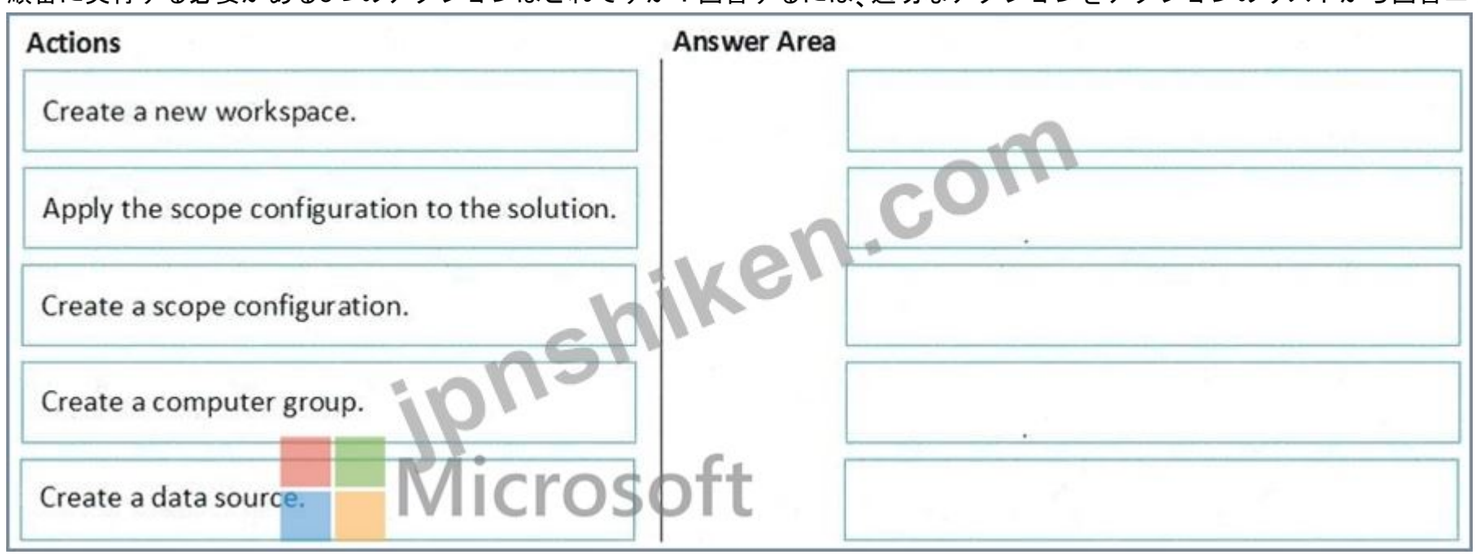


Explanation:
VM1: The Tier
The Tier needs to be upgraded to standard.
Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.
VM2: the operating system
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2- capabilities

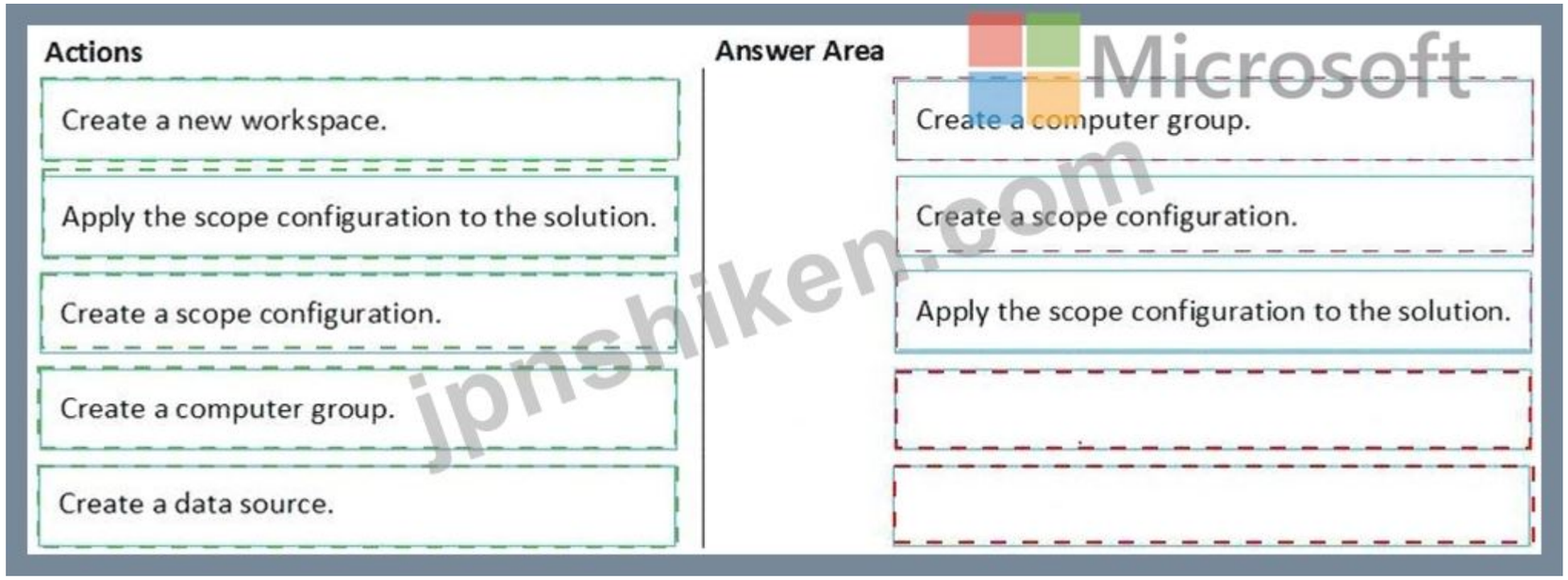
質問: **80**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。
このセクションの質問に回答すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Security Centerを使用して、3つのAzureサブスクリプションの一元化されたポリシー管理を行います。
いくつかのポリシー定義を使用して、サブスクリプションのセキュリティを管理します。
3つのサブスクリプションすべてにポリシー定義をグループとして展開する必要があります。
解決策 :ポリシーイニシアチブと、リソースグループをスコープとする割り当てを作成します。
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**)**
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups/

質問: **81**

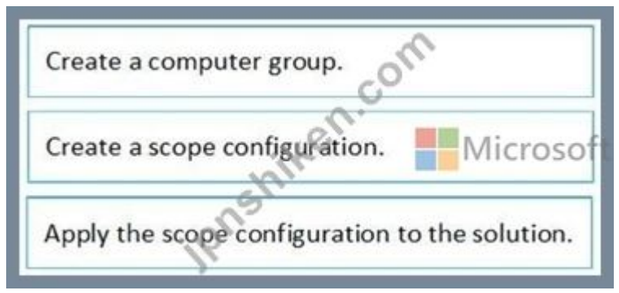
LAW1という名前のAzure Log Analyticsワークスペースを含むSub1という名前のAzureサブスクリプションがあります。
Windows Server 2016を実行し、LAW1に登録されている500個のAzure仮想マシンがあります。
システム更新評価ソリューションをLAW1に追加する予定です。
System Update Assessment関連のログは、100台の仮想マシンからのみLAW1にアップロードされるようにする必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序に並べます。



正解:

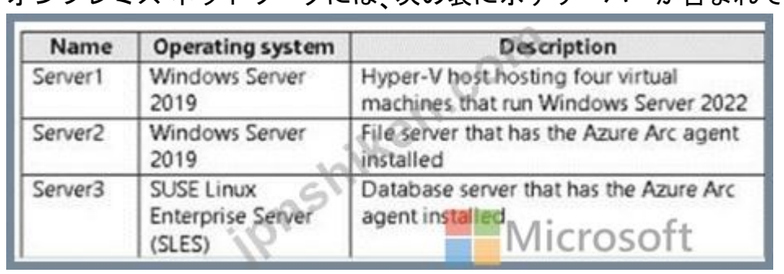


Explanation:



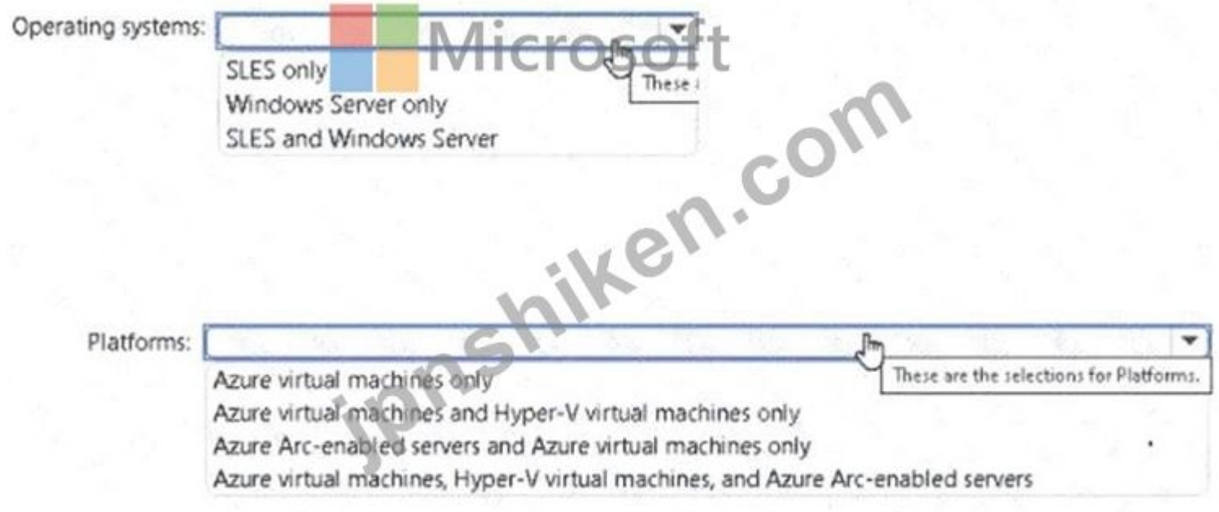
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

質問: **82**
オンプレミス ネットワークには、次の表に示すサーバーが含まれています。

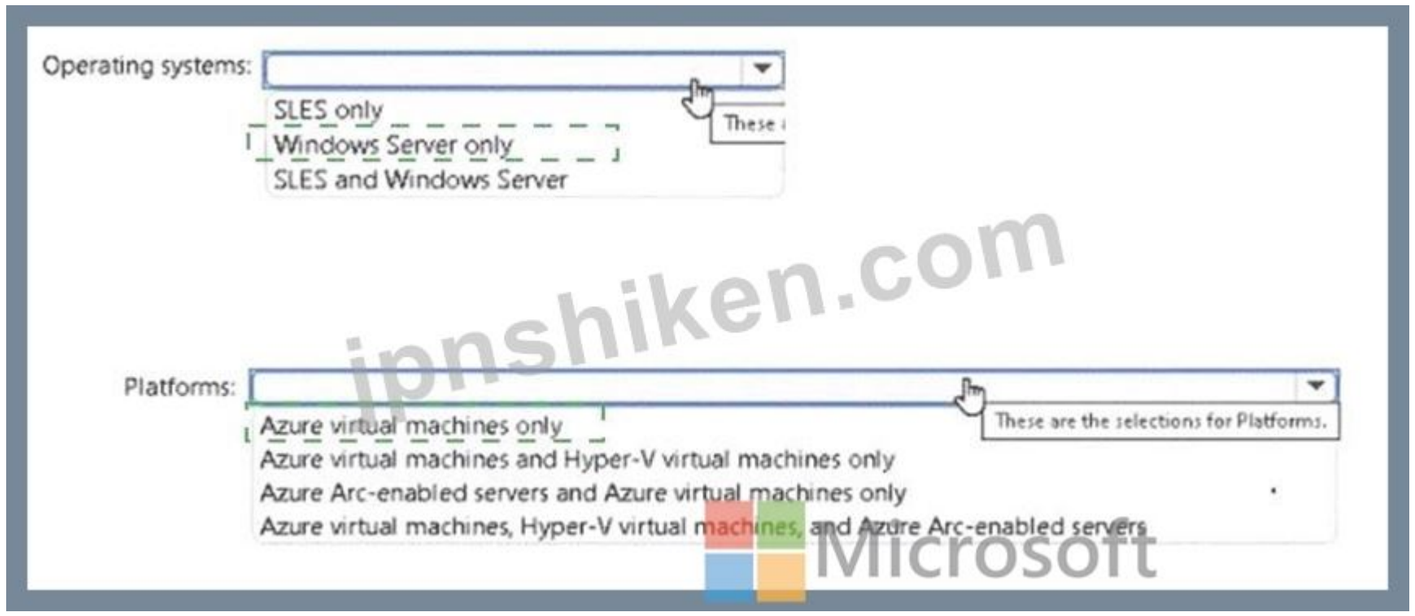


Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

Windows Server 2019 または SLES を実行する複数の仮想マシンを含む Azure サブスクリプションを所有しています。Microsoft Defender for Cloud に適応型アプリケーション制御を実装する予定です。どのオペレーティングシステムとプラットフォームを監視できますか？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。



正解:



質問: **83**
ラボのタスク
タスク6
VNET01 仮想ネットワーク上の Subnet0 サブネットからの接続のみを受け入れるように、Web3l 330471 という名前の Microsoft SQL サーバーを構成する必要があります。
正解:
see the task answer with step by step below:
* Configure the firewall settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to add a firewall rule that allows inbound traffic from the IP address range of the Subnet0 subnet. You also need to disable the option to allow Azure services and resources to access this server.
* Configure the network settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to enable service endpoints for SQL Server on the Subnet0 subnet.
You also need to add a virtual network rule that links the SQL server to the Subnet0 subnet.
* Configure the connection settings for the SQL server. You can use SQL Server Management Studio or Transact-SQL to do this. You need to enable remote server connections and specify a TCP port for listening. You also need to configure SQL Server Authentication or Azure Active Directory Authentication for connecting to the SQL server.

質問: **84**
注：質問は、同じ設定を表すいくつかの質問に含まれています。ただし、すべての質問には独特の結果があります。ソリューションが要件を満たしているかどうかを確認します。
あなたの会社には、weylandindustries.comという名前の単一ドメインを持つActiveDirectoryフォレストがあります。また、同じ名前のAzure Active Directory（Azure AD）テナントもあります。
ActiveDirectoryとAzureADテナントの統合を担当しました。Azure ADConnectをデプロイする予定です。
統合の戦略では、パスワードポリシーとユーザーログオンの制限が、Azure ADテナントに同期されるユーザーアカウントに影響を与え、必要なサーバーの数が削減されるようにする必要があります。
解決策：パスワードハッシュ同期とシームレスSSOの使用をお勧めします。
ソリューション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)**

質問: **85**
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
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

APL1 という名前の Azure Private Link サービスをデプロイする予定です。
APL1 の作成中に参照する必要があるリソースはどれですか?
A. LB1
B. VMSS1
C. VM1
D. SQL
正解: **(**正解を表示します**)**

質問: **86**
ラボのタスク
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン] ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力します。[パスワードの入力] ボックスにカーソルを置き、下のパスワードをクリックします。
Azure ユーザー名: Userl -28681041@ExamUsers.com
Azure パスワード: GpOAe4@lDg
Azure portal がブラウザーに正常に読み込まれない場合は、CTRL-K を押して、新しいブラウザー タブでポータルを再読み込みします。
次の情報は、テクニカル サポートのみを目的としています。
ラボ インスタンス: 28681041
タスク 3
会社の開発者は、App28681041 という名前の Web アプリを作成し、そのアプリを https://www.contoso.com に公開することを計画しています。次のタスクを実行する必要があります。
* App28681041 が Azure AD に登録されていることを確認します。
* App28681041 のパスワードを生成します。
正解:
Check below steps in explanation for Task.
Explanation
To register App28681041 to Azure AD and generate a password for it, you can follow these steps:
In the Azure portal, search for and select Azure Active Directory.
In the left pane, select App registrations.
Select New registration.
In the Register an application pane, enter the following information:
Name: App28681041
Supported account types: Select the appropriate account types for your scenario.

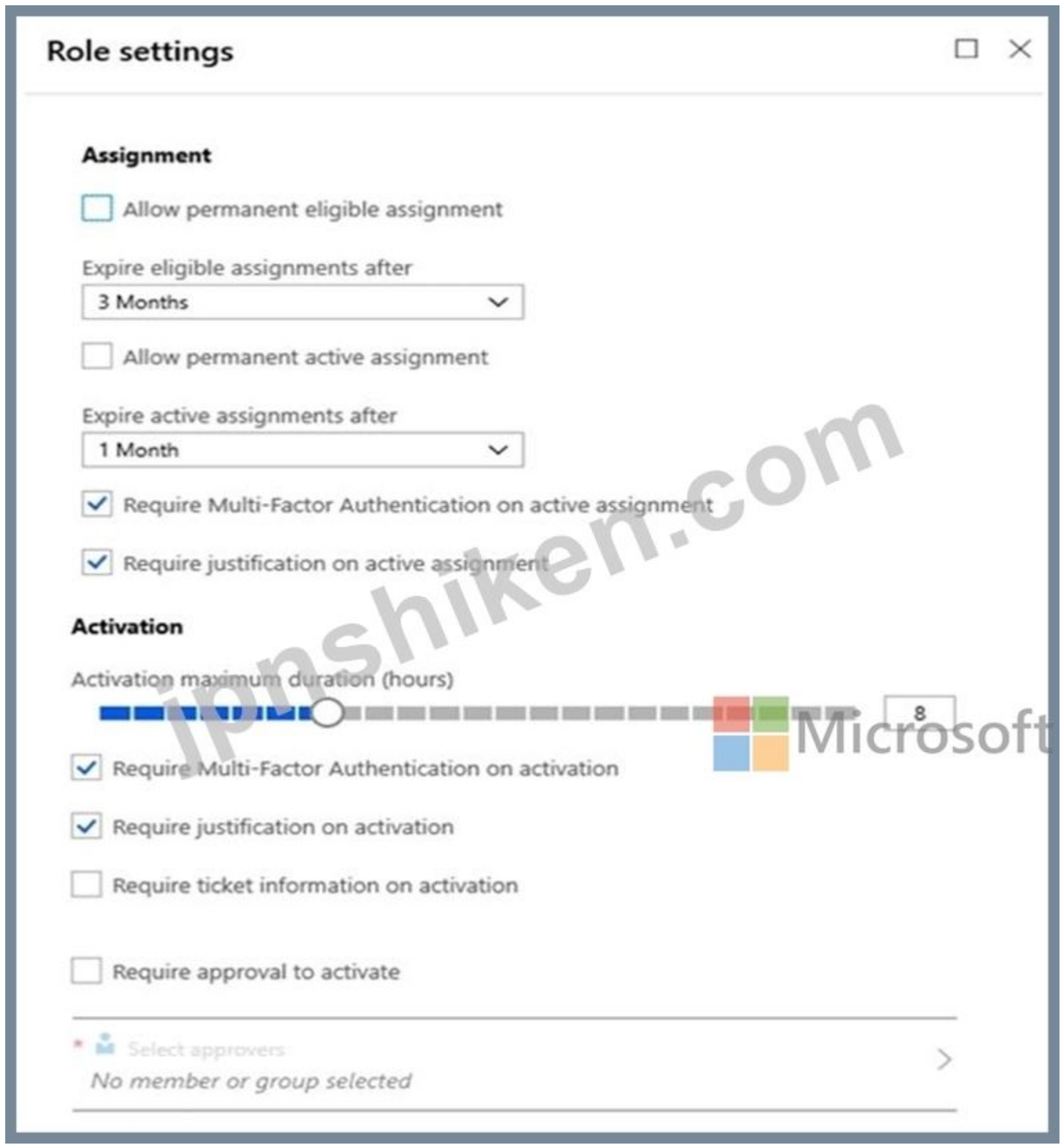
Redirect URI: Leave this field blank.
Select Register.
In the App registrations pane, select the newly created App28681041 application.
In the left pane, select Certificates & secrets.
Select New client secret.
In the Add a client secret pane, enter the following information:
Description: Enter a description for the client secret.
Expires: Select an appropriate expiration date for the client secret.
Select Add.
In the Certificates & secrets pane, copy the value of the newly created client secret.
You can find more information on this topic in the following Microsoft documentation: Quickstart: Register an application with the Microsoft identity platform.

質問**: 87**
User1 という名前のユーザーを含む Azure AD が有効になりました。
App1 という名前のアプリを購入します。
User1 は、Azure AD アプリケーション プロキシを使用して App1 を公開する必要があります。
User1 にどの役割を割り当てるべきですか?
A. Cloud App Security 管理者
B. クラウド アプリケーションの管理
C. アプリケーション管理者
D. ハイブリッド ID 管理者
正解**: (**正解を表示します**)**

質問**: 88**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

Azure AD Privileged Identity Management (PIM) では、共同作成者ロールのロール設定は図に示すように構成されています。([図] タブをクリックします。)

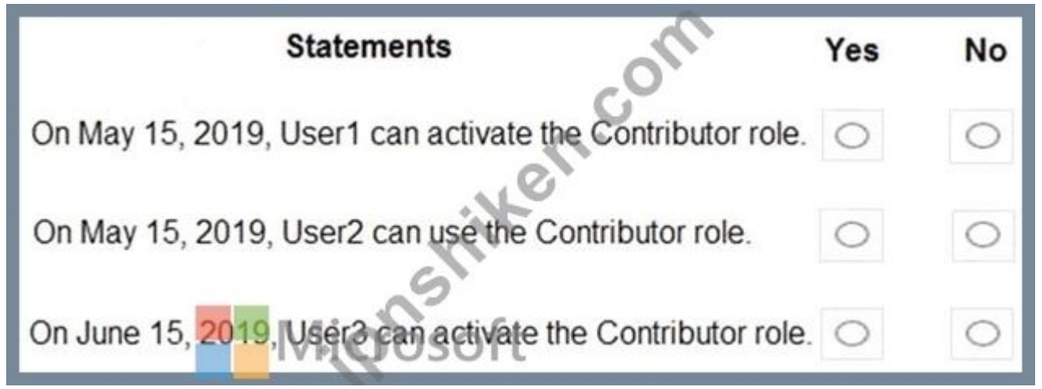


次の表に示すように、2019 年 5 月 1 日にユーザーに Contributor ロールを割り当てます。

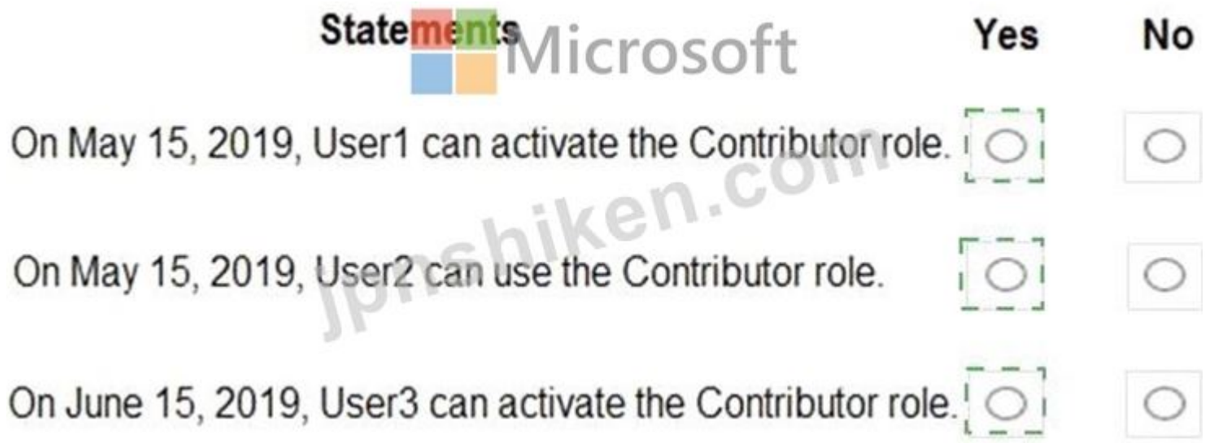
Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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。

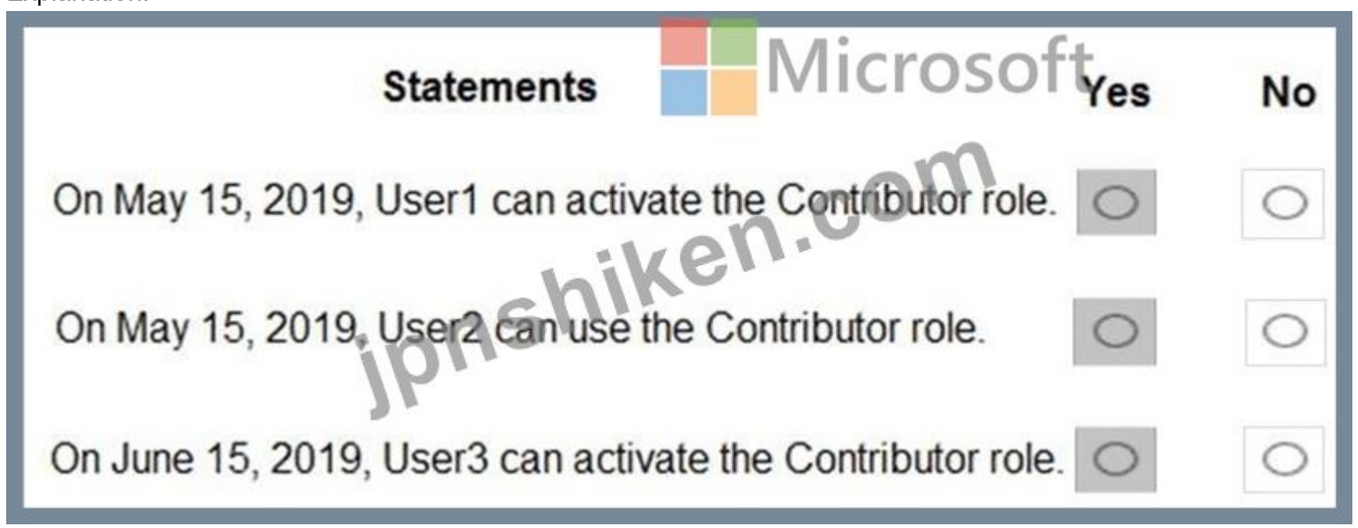
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



References:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles- assign-roles

質問: **89**
App1 という名前の Azure App Service アプリ、AC1 という名前の Azure コンテナー インスタンス、および 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。AC1 は App2 という名前のアプリをホストします。
ユーザーは、https:/app1.contoso.com/echo/resource-cache? param1 の URL を使用して App1 にリクエストを送信します。
=sample。App1 は App2 を呼び出します。App2 は storage1 からデータを取得します。
異常な IP アドレスからの接続が検出されたときに、セキュリティ アラートが生成されることを確認する必要があります。どの Microsoft Defender for Cloud サービスを使用すればよいですか?
A. ストレージ用 Microsoft Defender
B. API 用の Microsoft Defender
C. App Service 向け Microsoft Defender
D. コンテナー向け Microsoft Defender
正解: **(**正解を表示します**)**

質問: **90**
ネットワークには、contoso.comという名前のActive Directoryフォレストが含まれています。contoso.comという名前のAzure Directory（Azure AD）テナントがあります。
Azure AD Connectの高速設定インストールオプションを使用して、同期を構成する予定です。
計画された構成を実行するために必要なロールとグループを識別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2つの役割とグループを識別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ています。
注 :それぞれの正しい選択には1ポイントの価値があります。
A. Active DirectoryのDomain Adminsグループ
B. Azure ADのセキュリティ管理者の役割
C. Azure ADのグローバル管理者の役割
D. Azure ADのユーザー管理者ロール
E. Active DirectoryのEnterprise Adminsグループ
正解: **(**正解を表示します**)**
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

質問: **91**
会社はAzure DevOpsを使用しています。
コードが会社の品質基準とコードレビュー基準を満たしているかどうかを検証する方法を推奨する必要があります。
Azure DevOpsに実装することをお勧めしますか？
A. branch folders
B. branch permissions
C. branch policies
D. branch locking
正解: **(**正解を表示します**)**
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azuredevops& viewFallbackFrom=vsts

質問: **92**

オンプレミス ネットワークと Azure サブスクリプションがあります。

次の表に示す Microsoft SQL Server インスタンスがあります。

Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

Microsoft Defender for SQL を実装する予定です。

Microsoft Defender for SQL によって保護される SQL Server インスタンスはどれですか?

A. sql1、sql2、sql3のみ

B. sql1、sql2、sql3、sql4

C. sql1 と sql2 のみ

D. sql1 sql2 および so.14 のみ

正解: **(**正解を表示します**)**

質問: **93**

次の表に示すリソースを含むSubcription1という名前のAzureサブスクリプションがあります。

Name	Type	Status
EventHub1	Azure Event Hubs	*Not applicable*
Adf1	Azure Data Factory	*Not applicable*
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

次のリソースを含むSubcription2という名前のAzureサブスクリプションがあります。

AzureSentinelワークスペース

Azureイベントグリッドインスタンス

NVAからAzureSentinelにCEFメッセージを取り込む必要があります。

注：正しい選択はそれぞれ1ポイントの価値があります。

正解:

質問: **94**
セキュリティ運用要件を満たしていることを確認する必要があります。
最初に何をすべきですか？
A. セキュリティセンターで自動プロビジョニングをオンにします。
B. Security CenterとMicrosoft Cloud App Securityを統合します。
C. Security Centerの価格設定を標準にアップグレードします。
D. セキュリティセンターのワークスペース構成を変更します。
正解: **C** (コメントを発表する)
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing
Topic 2, Contoso
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 question on 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 sections 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 on 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.
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Technical requirements
Contoso identifies the following technical requirements:
* Deploy Azure Firewall to VNetWork1 in Sub2.

* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.
* Enable Azure AD Privileged Identity Management (PIM) for contoso.com

Existing Environment

Azure AD

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	*None*

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	`user.city -contains "ON"`
Group2	Dynamic user	`user.city -match "*on"`

Sub1

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networksSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Name	Subnet
VNetwork1	Subnet1.1, Subnet1.2 and Subent1.3
VNetwork2	Subnet2.1

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet1.1
VM2	NIC2	ASG2	Subnet1.1
VM3	NIC3	*None*	Subnet1.2
VM4	NIC4	ASG1	Subnet1.3
VM5	NIC5	*None*	Subnet2.1

All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet1.1
NSG3	Subnet1.3
NSG4	Subnet2.1

NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Contoso identifies the following technical requirements:

* Deploy Azure Firewall to VNetwork1 in Sub2.
* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.
* Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

質問: **95**

Microsoft Defender を使用する 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組み込まれている CIS Microsoft Azure Foundations Benchmark v2.0.0 を有効にします。

ユーザーがカスタムのロールベースアクセス制御 (RBAC) ロールを割り当てようとしたときに、社内ウェブサイトへのリンクを含むカスタムエラーメッセージが表示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、他のポリシーへの影響を最小限に抑える必要があります。

何を設定すればよいでしょうか?

A. 組み込みのデフォルトの非準拠メッセージ

B. ポリシーの修復タスク

C. ポリシー固有の非準拠メッセージ

D. ポリシーの効果

正解: **(**正解を表示します**)**

質問: **96**

Azure サブスクリプションに Azure Kubernetes Service (AKS) クラスターを作成する予定です。

登録されたサーバー アプリケーションのマニフェストを次の図に示します。

Save Discard Upload Download

The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.


```
{
   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
   "acceptMappedClaims": null,
   "accessTokenAcceptedVersion": null,
   "addIns": [],
   "allowPublicClient": null,
   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
   "appRoles": [],
   "oauth2AllowUrlPathMatching": false,
   "createdDateTime": "2019-07-15T21:09:20Z",
   "groupMembershipClaims": null,
   "identifierUris": [],
   "informationalUrls": {
       "termsOfService": null,
       "support": null,
       "privacy": null,
       "marketing": null
   },
   "keyCredentials": [],
   "knownClientApplications": [],
   "logoUrl": null,
   "logoutUrl": null,
   "name": "AKSAzureADServer",
   "oauth2AllowIdTokenImplicitFlow": false,
   "oauth2AllowImplicitFlow": false,
   "oauth2Permissions": [],
   "oauth2RequirePostResponse": false,
   "optionalClaims": null,
   "orgRestrictions": [],
   "parentalControlSettings": {
```


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?

A. アクセストークン承認バージョン
B. キー認証情報
C. グループメンバーシップクレーム
D. マップされたクレームを受け入れる

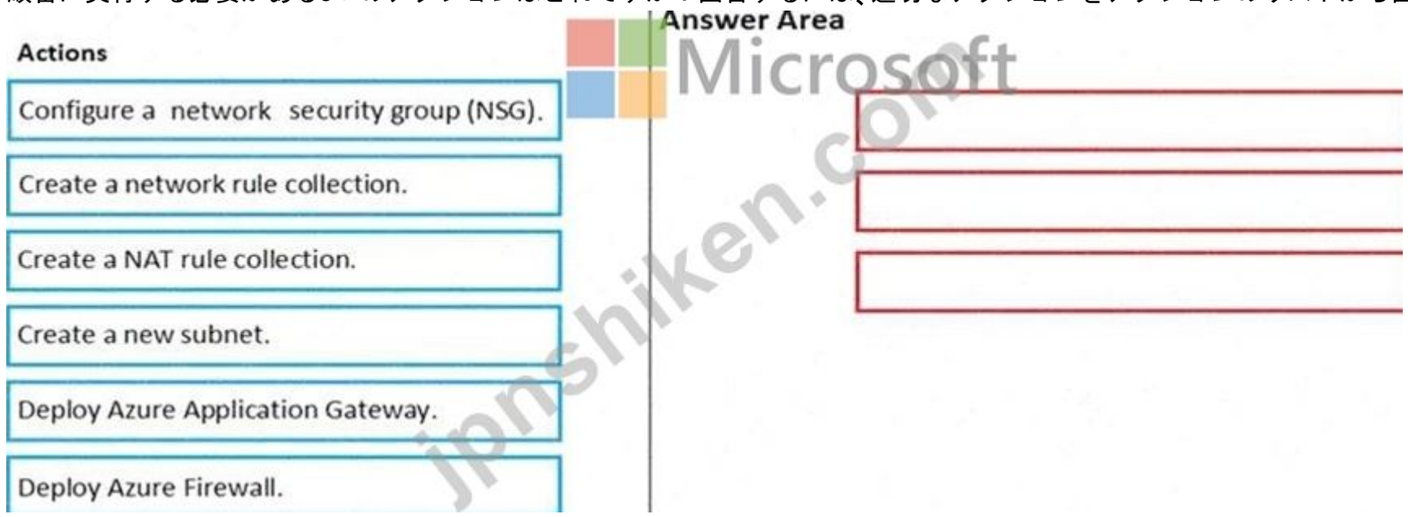
正解: **(**正解を表示します**)**

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

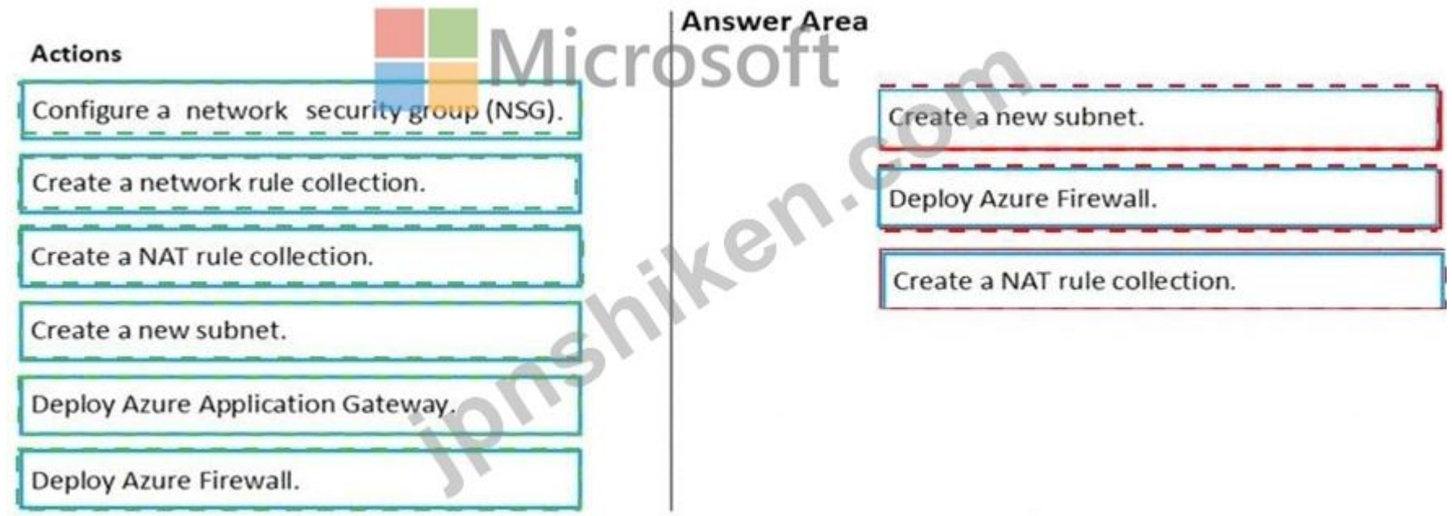
質問: **97**

次のリソースを含むAzureサブスクリプションがあります。
* Subnet1およびSubnet2という名前の2つのサブネットを含む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。

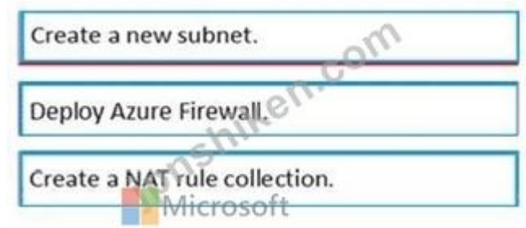
インターネットからVM1へのリモートデスクトップ接続を確立できるようにする必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序で並べます。



正解:



Explanation:



質問: **98**
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。

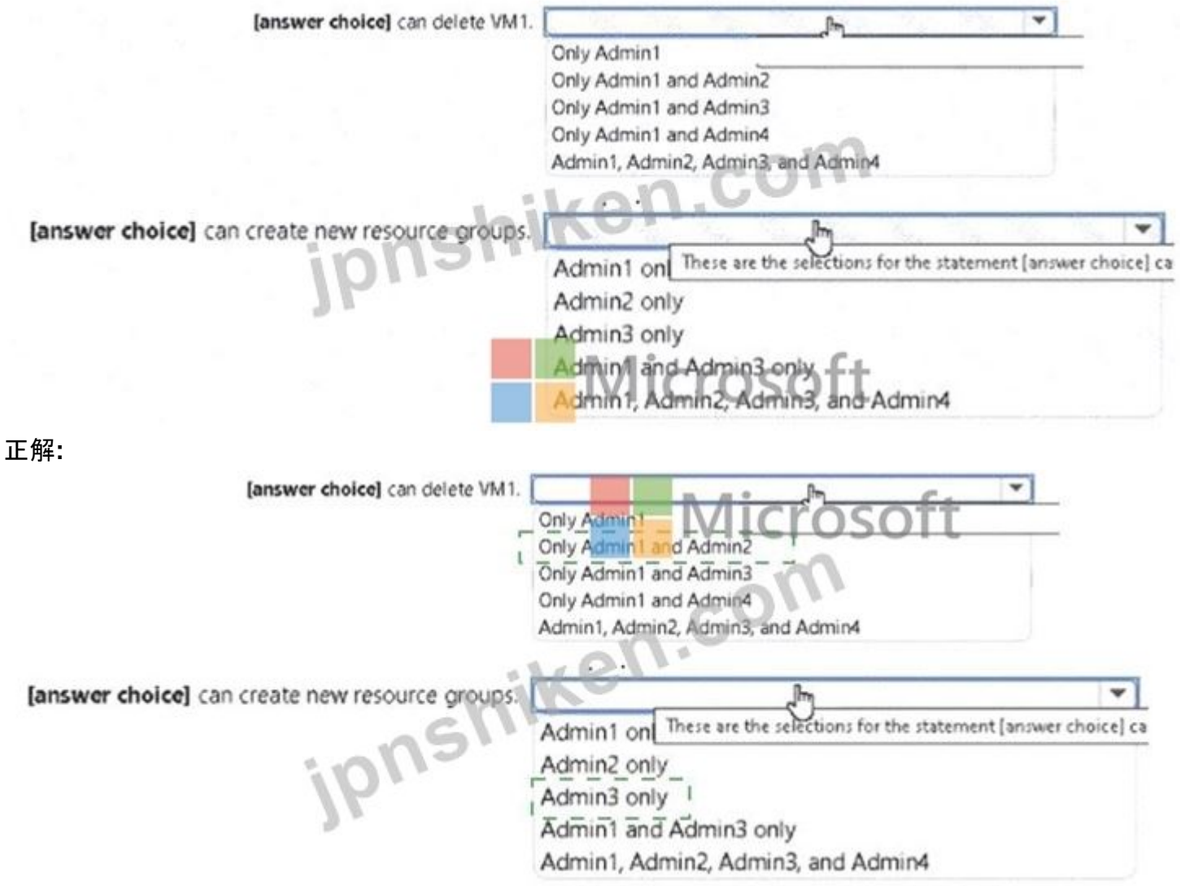
Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

VM1 と VM2 はどちらも VNET1 に接続し、NSG1 を使用するように構成されています。
VM1 と VM2 のみが DB1 にアクセスできるようにする必要があります。
何をすべきでしょうか?
A. NSG1 の場合、サービス タグを持つルールを構成します。
B. VNET1 の IP アドレス範囲を DB1 のファイアウォール設定に追加します。
C. アプリケーション セキュリティ グループを作成します。
D. DB1 を VNET1 からのアクセスのみを許可するように構成します。
正解: **(**正解を表示します**)**

質問: **99**
sa1 という名前の Azure Data Lake Storage アカウントを含む Azure サブスクリプションがあります。
sa1 にアクセスし、読み取り、一覧表示、ディレクトリの作成、ディレクトリの削除などの操作を実行する App1 という名前のアプリを展開する予定です。
プライベート エンドポイントを使用して、App1 が sa1 に安全に接続できることを確認する必要があります。sa1 に必要なプライベート エンドポイントの最小数はいくつですか。
A. 1
B. 2
C. 3
D. 4
E. 5
正解: **(**正解を表示します**)**
A private endpoint is a network interface that connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network.
You only need one private endpoint for each service that you want to access privately, such as Azure Data Lake Storage. You can create a private endpoint for your Azure Data Lake Storage account named sa1 by following the steps in this article.
References:
What is a private endpoint? - Azure Private Link
Private Endpoints for Azure Storage are now Generally Available
Step-by-Step: How to Configure a Private Endpoint to Secure Azure ...

質問: **100**
次の資料に示す役割の割り当てがあります。

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ステートメントを完成させる回答の選択肢を選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。



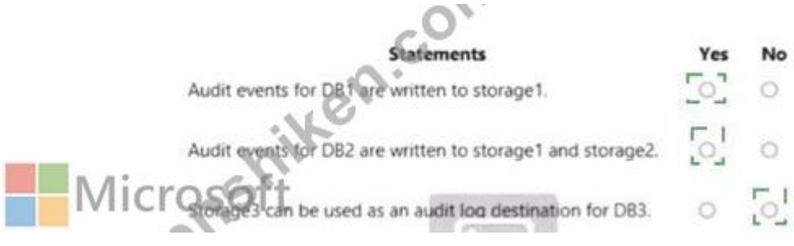
正解:

質問: **101**
あなたの会社は、部門ごとに個別のサブスクリプションを作成することを計画しています。各サブスクリプションは、同じ Azure Active Directory (Azure AD) テナントに関連付けられます。
同じロールが割り当てられるように各サブスクリプションを構成する必要があります。
何を使うべきですか？
A. Azure Security Center
B. Azure Policy
C. Azure AD Privileged Identity Management (PIM)
D. Azure Blueprints
正解: **(**正解を表示します**)**

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:
Role Assignments
Policy Assignments
Azure Resource Manager templates
Resource Groups
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

質問: **102**
3つのストレージアカウント、SQLという名前のAzure SQLマネージドインスタンス、および3つのAzureSQLデータベースを含む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は、次の表に示すように構成されます。
SQ11には次の設定があります。
*監査 :オン
*監査先 :storage1
Azure SQLデータベースは、次の表に示すように構成されています。

正解:
Answer Area



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure
https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

質問: **103**
WebApp1という名前のWebアプリがあります。
WAF1という名前の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。
WAF1を使用してWebApp1を保護する必要があります。
最初に何をすべきですか？
A. Azureフロントドアを展開します。
B. WebApp1に拡張機能を追加します。
C. Azure Firewallを展開します。
正解: **A (**コメントを発表する**)**
References:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

質問: **104**
ラボのタスク
必要に応じて、次のログイン資格情報を使用します。
ユーザー名を入力するには、[サインイン] ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力します。「パスワードを入力してください」ボックスにカーソルを置き、下のパスワードをクリックします。
Azure ユーザー名: Userl -28681041@ExamUsers.com
Azure パスワード: GpOAe4@lDg
Azure portal がブラウザーに正常に読み込まれない場合は、CTRL-K を押して、新しいブラウザー タブにポータルを再読み込みします。
次の情報は、テクニカル サポートのみを目的としています。
ラボインスタンス: 28681041
タスク6
VM1 という名前の仮想マシンの平均 CPU 使用率が 15 分間で 70% を超えた場合は、adminl@contoso.com という名前のユーザーにアラートを電子メールで送信する必要があります。
正解:
Check below steps in explanation for Task
Explanation:
To email an alert to a user named adminl@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes, you can follow these steps:
In the Azure portal, search for and select the virtual machine named VM1.
In the left pane, select Alerts.
Select New alert rule.
In the New alert rule pane, enter the following information:
Name: Enter a name for the alert rule.
Description: Enter a description for the alert rule.
Condition: Select Metric measurement.
Resource: Select the virtual machine named VM1.
Metric: Select Percentage CPU.
Operator: Select Greater than.
Threshold: Enter 70.
Aggregation type: Select Average.

Period: Select 15 minutes.
In the Actions pane, select Add action group.
In the Add action group pane, enter the following information:
Name: Enter a name for the action group.
Short name: Enter a short name for the action group.
Email recipient: Enter the email address of the user you want to receive the alert. For example, adminl@contoso.com.
Select OK.

質問**: 105**
Azure AD テナントにリンクされ、次の表に示すリソースが含まれる Azure サブスクリプションがあります。

Name	Location	Description
Group1	*Not applicable*	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	*Not applicable*	Enterprise application in Azure AD

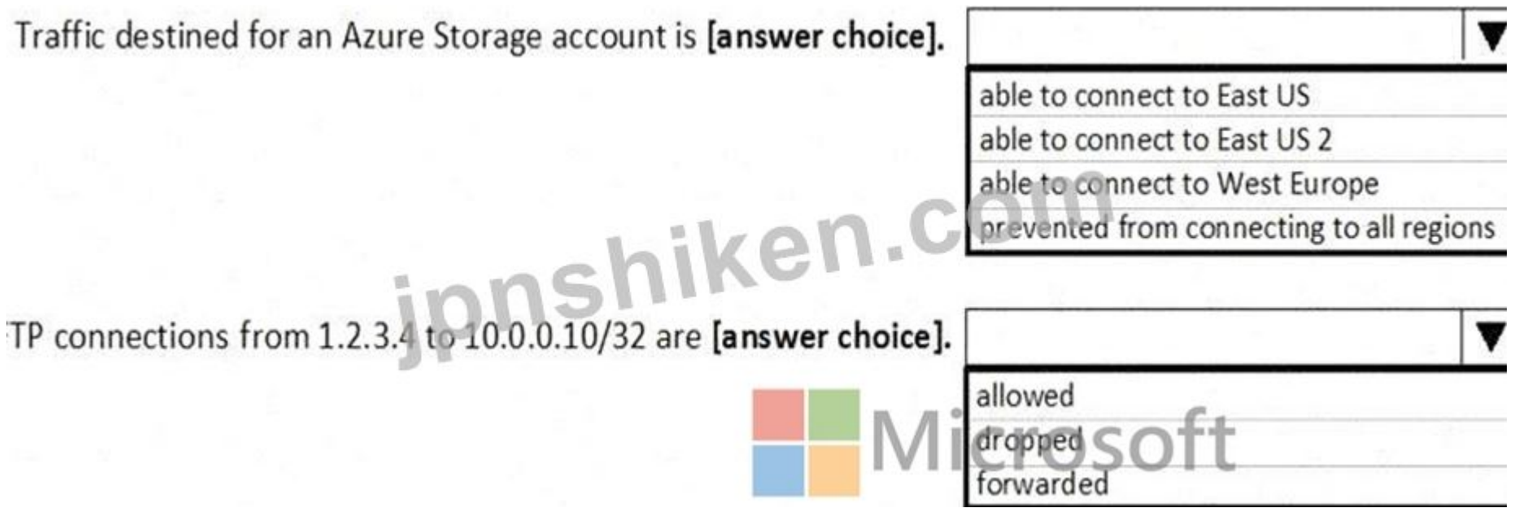
VM1 の共同作成者ロールを割り当てることができるリソースはどれですか?
A. マネージド 1 と App1 のみ
B. グループ 1、管理対象 1、VM1。およびApp1のみ
C. グループ1。マネージド 1 および VM2 のみ
D. グループ 1 と管理対象 1 のみ
正解**: A (**コメントを発表する**)**

質問**: 106**
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-AzureRmNetworkSecurityRuleConfigを実行し、次の展示に示す出力を受け取ります。

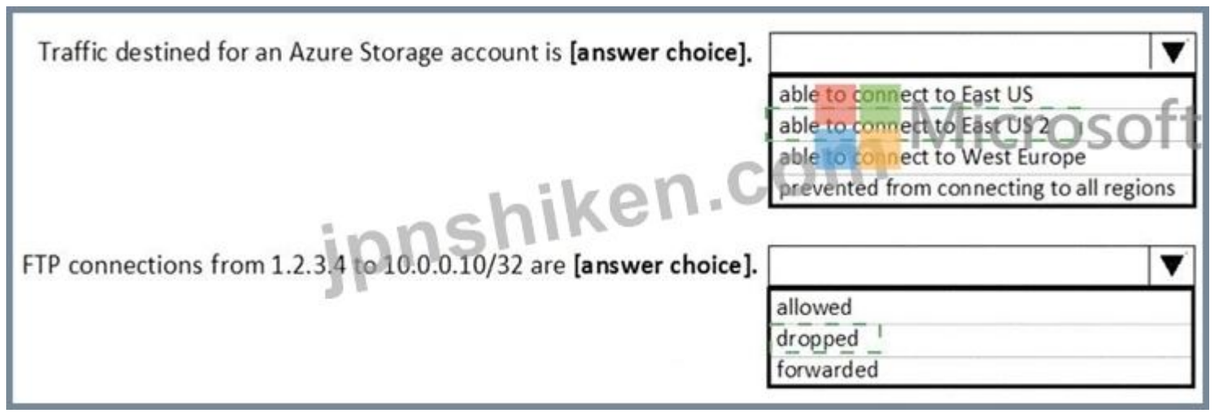
```
Name                                    :  DenyStorageAccess
Description                             :
Protocol                                :  *
SourcePortRange                         :  {*}
DestinationPortRange                    :  {*}
SourceAddressPrefix                     :  {*}
DestinationAddressPrefix                :  {Storage}
SourceApplicationSecurityGroups         :  []
DestinationApplicationSecurityGroups    :  []
Access                                  :  Deny
Priority                                :  105
Direction                               :  Outbound

Name                                    :  StorageEA2Allow
ProvisionIngState                       :  Succeeded
Description                             :
Protocol                                :  *
SourcePortRange                         :  {*}
DestinationPortRange                    :  {443}
SourceAddressPrefix                     :  {*}
DestinationAddressPrefix                :  {Storage/EastUS2}
SourceApplicationSecurityGroups         :  []
DestinationApplicationSecurityGroups    :  []
Access                                  :  Allow
Priority                                :  104
Direction                               :  Outbound
                                        :
Name                                    :  Contoso_FTP
Description                             :
Protocol                                :  TCP
SourcePortRange                         :  {*}
DestinationPortRange                    :  {21}
SourceAddressPrefix                     :  {1.2.3.4/32}
DestinationAddressPrefix                :  {10.0.0.5/32}
SourceApplicationSecurityGroups         :  []
DestinationApplicationSecurityGroups    :  []
Access                                  :  Allow
Priority                                :  504
Direction                               :  Inbound
```

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成させる回答の選択肢を選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:
Box 1: able to connect to East US 2
The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}
Box 2: dropped
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

質問: **107**
Admin1 という名前のユーザーを含む Azure Active Directory (Azure AD) テナントがあります。Admin1 には、アプリケーション開発者ロールが割り当てられています。
App1 という名前のクラウド アプリを購入し、App1 を Azure AD に登録します。

Admin1 は、App1 のトークン暗号化を有効にするオプションが利用できないことを報告しています。
Admin1 が Azure portal で App1 のトークン暗号化を有効に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. App1 の証明書をアップロードします。
B. App1 の API 権限を変更します。
C. App1 をエンタープライズ アプリケーションとして追加します。
D. Admin1 にクラウド アプリケーション管理者ロールを割り当てます。
正解**: C (**コメントを発表する**)**
This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application.
When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption

質問**: 108**
次の表に示すリソースが含まれる Subscription1 という名前の Azure サブスクリプションがあります。

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	**Not applicable**

次の JSON ファイルを使用して、Subscription1 にカスタム RBAC ロールを作成します。

```
"Name": "Role1",
"IsCustom": true,
"Description": "Role1 description",
"Actions": [
    "*/Read",
    "Microsoft.Compute/*"
],
"NotActions": [],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
  "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1
]
```

RG1 の User1 に Role1 を割り当てます。
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 ポイントが付与されます。

正解:

Explanation:
Text Description automatically generated

Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider- operations#microsoftcompute

質問: **109**
Azure Security Centerから、SecPol1をデプロイ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. AzureDefenderを有効にします。

B. Azure管理グループを作成します。
C. イニシアチブを作成します。
D. 継続的なエクスポートを構成します。
正解: **(**正解を表示します**)**
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md
https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/

質問: **110**
User1という名前のユーザーを含むcontoso.comという名前のAzureActive Din-dory（Azure AD）テナントがあります。
テナントで複数のアプリを公開する予定です。
User1が公開されたアプリの管理者同意を付与できることを確認する必要があります。
ユーザーに割り当てることができる2つの可能なユーザーロールはどれですか。この目標を達成するには？それぞれの正解は完全な解決策を提示します。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. アプリケーション開発者
B. セキュリティ管理者
C. アプリケーション管理者
D. ユーザー管理者
E. クラウドアプリケーション管理者
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

質問: **111**
RG1 という名前のリソース グループと、次の表に示すネットワーク 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。

Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

次の図に示すような Azure ポリシーを作成します。

ポリシーを RG1 に割り当てます。
NSG1 と NSG2 にポリシーを割り当てると何が起こりますか?
A. NSG1 および NSG2 のフロー ログが有効になります。
B. NSG1 および NSG2 のフロー ログは無効になります。
C. フロー ログは NSG1 に対してのみ有効になります。
D. フロー ログは NSG2 に対してのみ有効になります。
正解: **D** (コメントを発表する)

質問: **112**
Group1 という名前のグループを含む Azure Active Directory (Azure AD) テナントがあります。Group1 のメンバーがパスワードなしの認証を使用してサインインしていることを確認する必要があります。どうすればよいですか?
A. 証明書ベースの認証 (CBA) ポリシーを構成します。
B. 条件付きアクセス ポリシーを作成します。
C. サインイン リスク ポリシーを構成します。
D. Microsoft Authenticator 認証方法ポリシーを構成します。
正解: (正解を表示します)

質問: **113**

Azure Active Directory (Azure AD) コネクタ、Query1 という名前の Azure Log Analytics クエリ、および Playbook1 という名前のプレイブックを含む Azure Sentinel ワークスペースがあります。

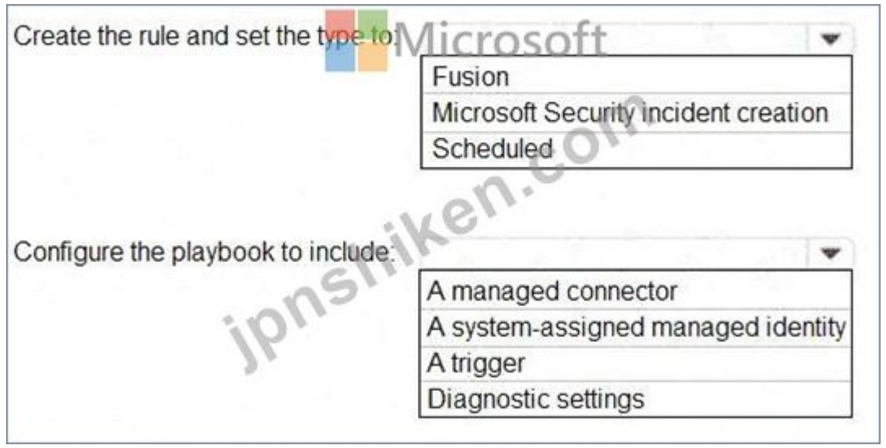
クエリ 1 は、Azure AD によって生成されたセキュリティ イベントのサブセットを返します。

Playbook1 をトリガーする Query1 に基づく Azure Sentinel 分析ルールを作成する予定です。

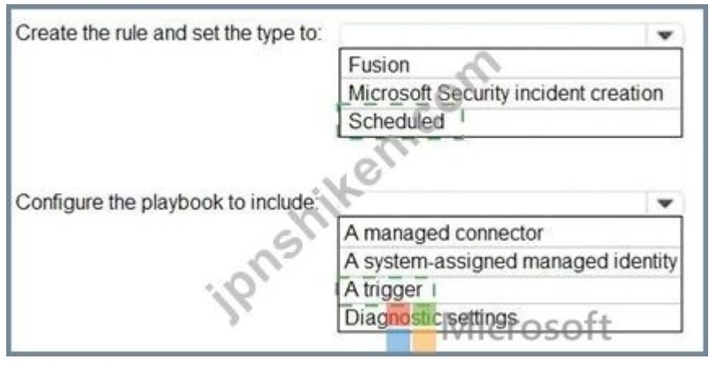
Playbook1 を新しいルールに追加できることを確認する必要があります。

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。

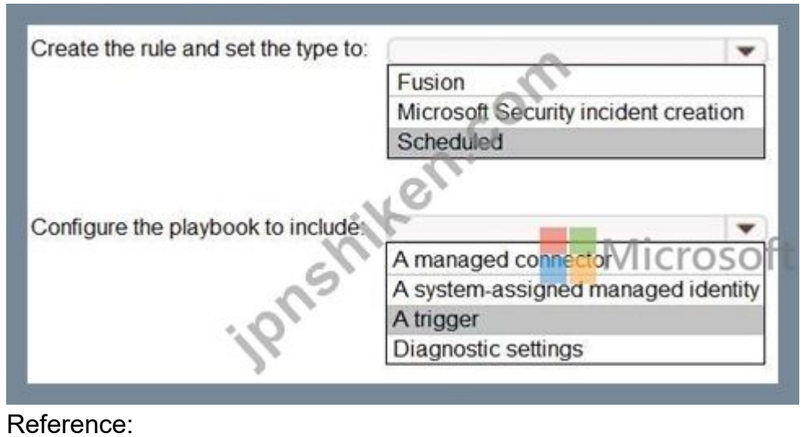
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **114**
ユーザーがVM0にアクセスできることを確認する必要があります。ソリューションはプラットフォーム保護要件を満たしている必要があります。
あなたは何をするべきか？
A. VM0をSubnet1に移動します。
B. ファイアウォールで、ネットワークトラフィックフィルタリングルールを構成します。
C. RT1をAzureFirewallSubnetに割り当てます。
D. ファイアウォールで、DNATルールを構成します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

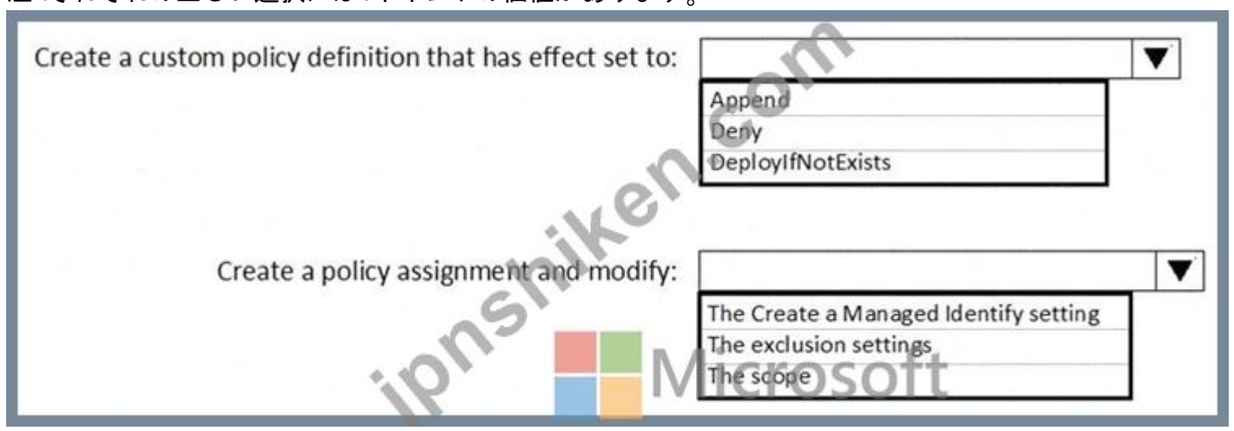
質問: **115**
Azure Container Registry に接続する Azure Kubernetes Service (AKS) クラスターがあります。
Azure Container Registry に対して認証するには、AKS クラスターの自動生成されたサービス プリンシパルを使用する必要があります。
何を作成する必要がありますか?
A. Azure Key Vault のシークレット
B. Azure AD ユーザー
C. Azure AD グループ
D. 役割の割り当て
正解: **D (**コメントを発表する**)**

質問: **116**
App1をホストするために使用する仮想マシンを推奨する必要があります。ソリューションは、KeyVault1の技術要件を満たしている必要があります。
どの仮想マシンを使用する必要がありますか？
A. VM1、VM2、VM3、およびVM4
B. VM1、VM2、およびVM4のみ
C. VM1のみ
D. VM1およびVM2のみ
正解: **(**正解を表示します**)**

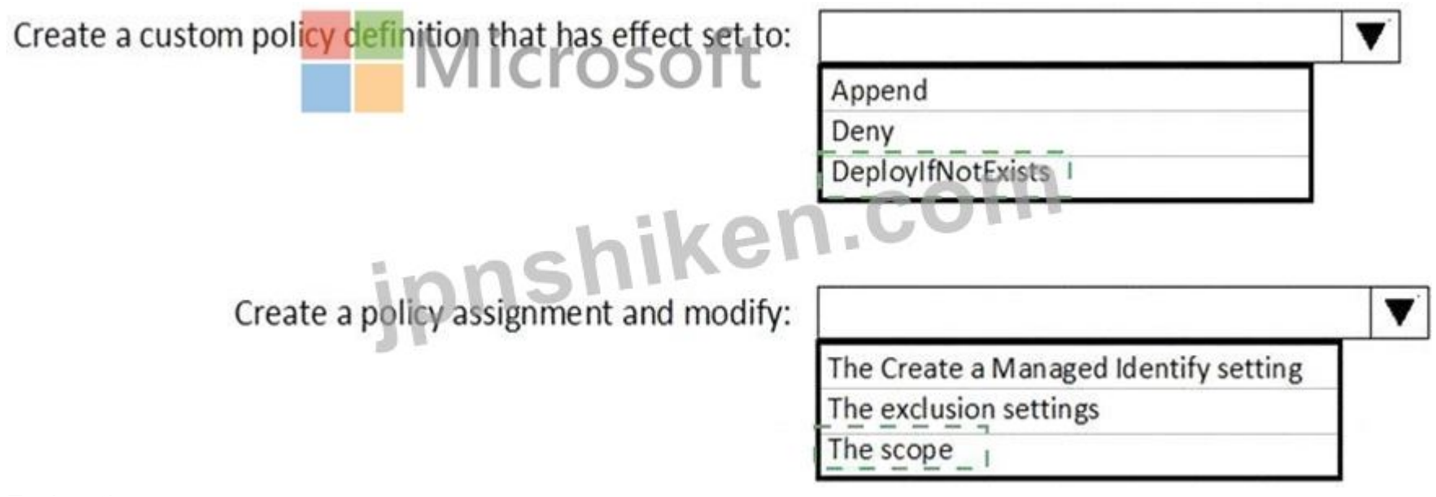
質問: **117**
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には 1 つのサブネットが含まれています。
サブスクリプションには、VNet1 に接続された VM1 という名前の仮想マシンが含まれています。
SQL1 という名前の Azure SQL マネージド インスタンスをデプロイする予定です。
VM1 が SQL1 にアクセスできることを確認する必要があります。
どの 3 つのコンポーネントを作成する必要がありますか? それぞれの正解は、解決策の一部を示します。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. ネットワーク セキュリティ グループ (NSG)

B. ルートテーブル
C. ネットワーク セキュリティ境界
D. サブネット
E. 仮想ネットワーク ゲートウェイ
正解: (正解を表示します)

質問: **118**
プラットフォーム保護の要件を満たすには、Microsoft Antimalwareを展開する必要があります。
あなたは何をするべきか？回答するには、回答エリアで適切なオプションを選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:
1. DeployifNotExists
2. Scope

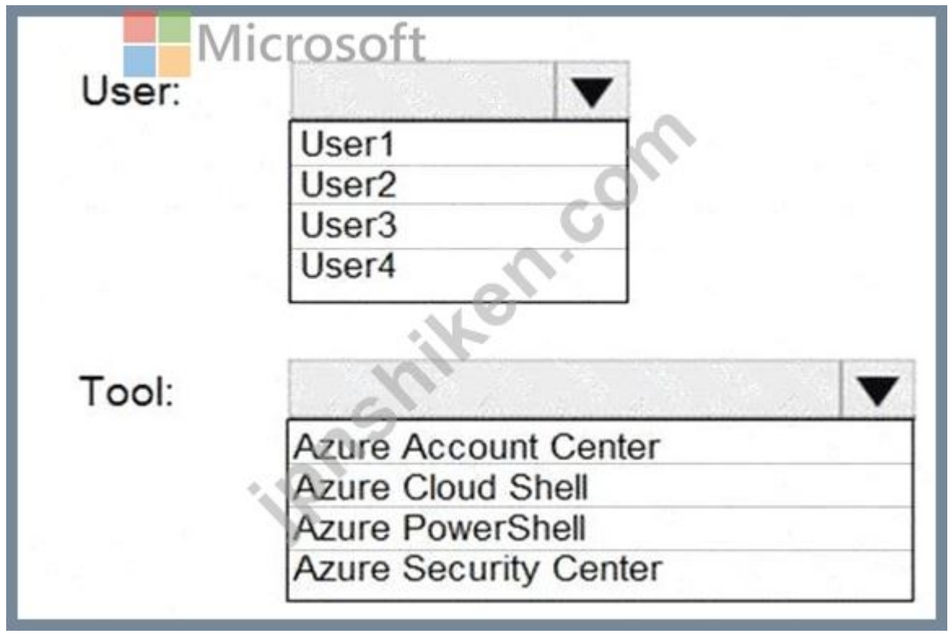
質問: **119**
会社には、contoso.comという名前のAzure Active Directory Azure Ȧzure AD）テナントに関連付けられているSub1という名前のAzureサブスクリプションがあります。

同社はApp1というモバイルアプリケーションを開発しています。App1は、OAuth 2の暗黙的な付与タイプを使用してAzure ADアクセストークンを取得します。
Azure ADにApp1を登録する必要があります。
アプリケーションを登録するには、開発者からどのような情報を取得する必要がありますか？
A. a redirect URI
B. a reply URL
C. a key
D. an application ID
正解: **(**正解を表示します**)**
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

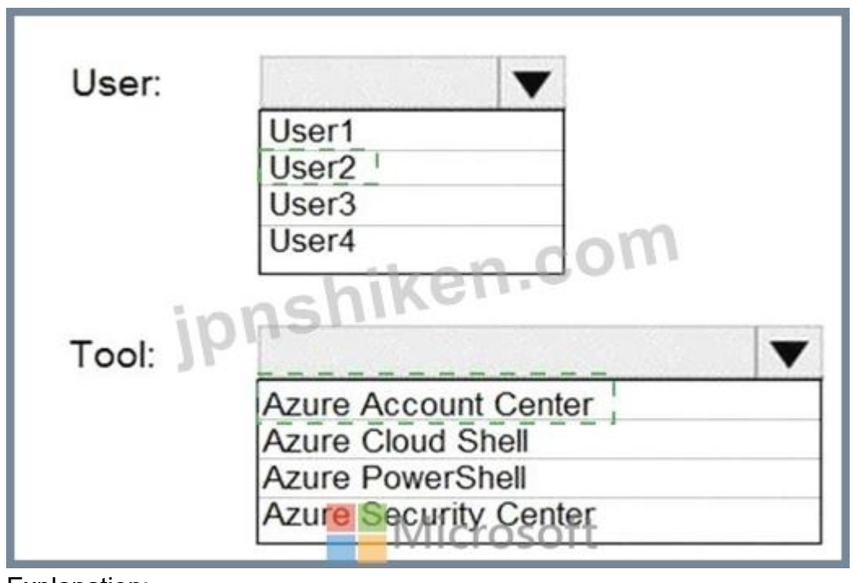
質問: **120**
会社には、次の表に示すユーザーを含むSubscription1という名前のAzureサブスクリプションがあります。

Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

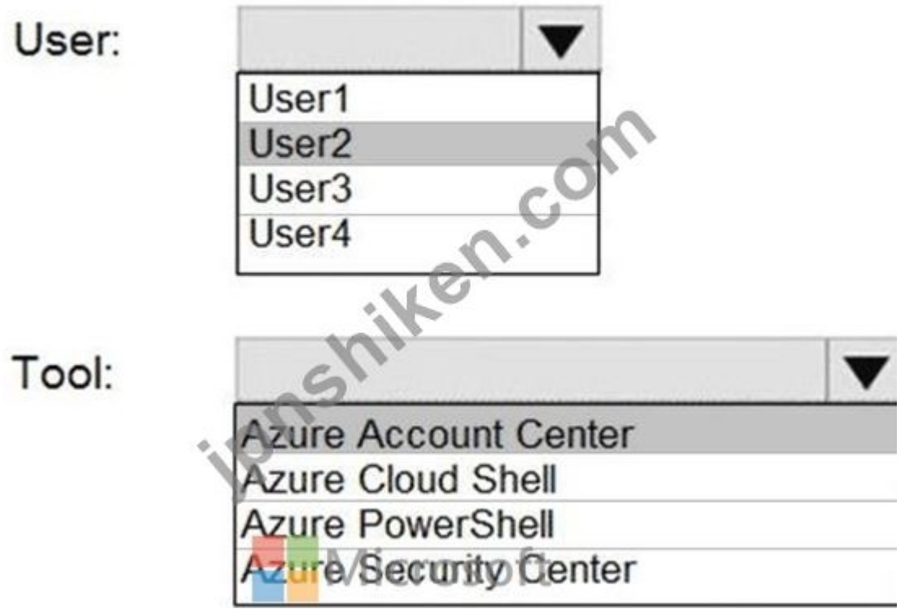
会社は新しい所有者に売却されます。
会社はSubscription1の所有権を譲渡する必要があります。
どのユーザーが所有権を譲渡でき、どのツールを使用する必要がありますか？ 回答するには、回答エリアで適切なオプションを選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:



Box 1; User2

Billing Administrator

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who ' s a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center

Azure Account Center can be used.

Reference:

https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an- azure-subscription

質問**: 121**

注: このセクションには、同じシナリオと問題を扱う1つ以上の質問セットが含まれています。各質問は、問題に対する独自の解決策を提示します。その解決策が、定められた目標を満たしているかどうかを判断してください。

セット内の複数の解決策が問題を解決できる可能性があります。また、セット内のどの解決策も問題を解決できない可能性もあります。

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

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
Group1	Security group
Group2	Microsoft 365 group
App1	App registration
MI1	User-assigned managed identity

次の表に示すユーザーがいます。

Name	Description
User1	• Member of Group1 and Group2 • Assigned Owner role for App1 and MI1
User2	• Member of Group1 and Group2 • Assigned Owner role for App1 and MI1

SQL1 という名前の Azure SQL マネージド インスタンスを作成し、Microsoft Entra のみの認証を有効にします。
User1 と User2 の両方が SQL1 の Microsoft Entra 管理者として設定されていることを確認する必要があります。
解決策: App1 を SQL1 の Microsoft Entra 管理者として設定します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**

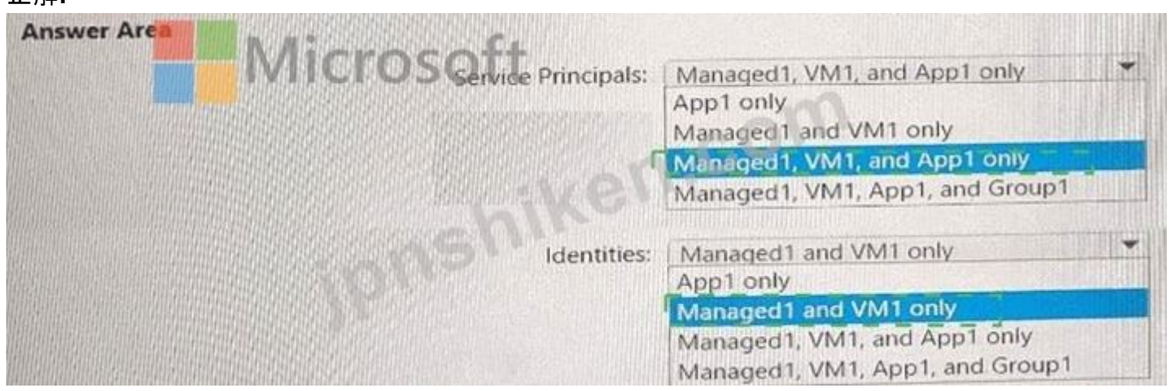
質問: **122**
ストレージ2に計画されている変更を実施する必要があります。ソリューションは、ストレージ暗号化の技術要件を満たしている必要があります。
A. アカウント暗号化キーを使用するように storage2 を構成します。
B. ストレージ2のパージ保護を有効にします。
C. storage2 に暗号化スコープを作成します。
D. storage2 に Azure ロールベースのアクセス制御 (Azure RBAC) ロールを割り当てます。
正解: **(**正解を表示します**)**

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。

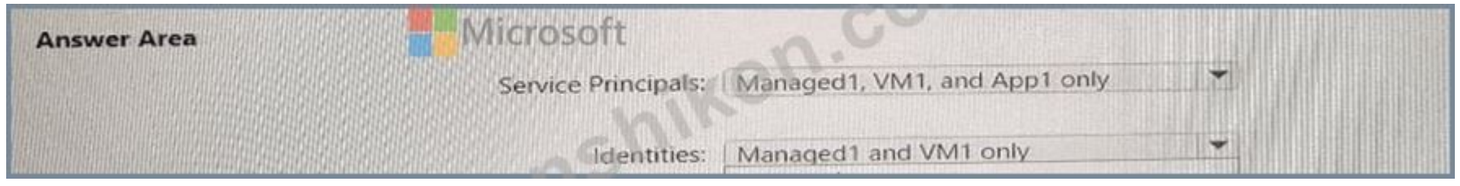
Name	Type
RG1	Resource group
VM1	Virtual machine

次のタスクを実行します。
Managed1 という名前のマネージド ID を作成します。
Group1 という名前の Microsoft 365 グループを作成します。
作成されたサービス プリンシパルと、RG1 のリーダー ロールを割り当てることができる ID 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？回答するには、回答エリアで適切なオプションを選択します。ノート：
それぞれの正しい選択は 1 ポイントの価値があります。

正解:



Explanation:



質問: **124**

Azure サブスクリプションをお持ちです。

セキュリティの脆弱性を自動的に修復するワークフロー自動化を Microsoft Defender for Cloud で作成する予定です。

最初に何を作成すればよいですか?

A. 自動化アカウント

B. アラートルール

C. Azure ロジック アプリ

D. マネージドID

E. Azure 関数アプリ

正解: **C (**コメントを発表する**)**

質問: **125**

Vault1 という名前の Azure キー コンテナーと VM1 という名前の仮想マシンを含む Azure サブスクリプションがあります。VM1 には Key Vault VM 拡張機能がインストールされています。

Vault1 では、キー、シークレット、証明書をローテーションします。

VM1 で自動的に更新されるものは何ですか?

A. キーとシークレットのみ
B. 証明書のみ
C. キーのみ
D. 秘密のみ
E. シークレットと証明書のみ
F. キー、シークレット、証明書
正解: **(**正解を表示します**)**

質問: **126**
Azure Active Directory（Azure AD）テナントを使用するMicrosoft 365テナントがあります。AzureADテナントは、Azure AD Connectのインスタンスを使用して、オンプレミスのActiveDirectoryドメインに同期します。
新しいAzureサブスクリプションを作成します
同期されたオンプレミスユーザーアカウントは、新しいサブスクリプションでロートを割り当てることができないことがわかりました。
同期されたAzureADユーザーアカウントにAzureとMicrosoft365の役割を割り当てることが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. 新しいサブスクリプションで使用されるAzureADテナントを変更します。
B. フェデレーション認証を使用するように新しいサブスクリプションで使用されるAzureADテナントを構成します。
C. パススルー認証を使用するように新しいサブスクリプションで使用されるAzureADテナントを構成します
D. Azure ADConnectの2番目のインスタンスを構成します。
正解: **(**正解を表示します**)**

質問: **127**
User2がPIMを実装できることを確認する必要があります。
最初に何をすべきですか？
A. User2にグローバル管理者ロールを割り当てます。
B. contoso.comの認証方法を構成します。
C. contoso.comのIDセキュアスコアを構成します。
D. User2の多要素認証（MFA）を有効にします。
正解: **(**正解を表示します**)**
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

質問: **128**
Azure Log Analyticsを使用して、Windows Server 2016を実行する200台のサーバーからログを収集する予定です。
Azure Resource Managerテンプレートを使用して、すべてのサーバーへのMicrosoft Monitoring Agentの展開を自動化する必要があります。
テンプレートをどのように完成させ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ます。
注 :それぞれの正しい選択には1ポイントの価値があります。

```
{
    "type" : "Microsoft.Compute/virtualMachines/extensions",
    "name" : "[concat(parameter('vmname'), /OMSExtension]",
    "apiVersion" : "[variables('apiVersion')]",
    "location" : "[resourceGroup().location]",
    "dependsOn" : [
        "[concat('Microsoft.Compute/virtualMachines/", parameters('vmName'))]"
    ],
    "properties" : {
        "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
        "type" :  "MicrosoftMonitoringAgent",
        "typeHandlerVersion" : "1.0",
        "autoUpgradeMinorVersion" : true,
        "settings" : {
            [ ▼ ] : "[variable('var1')]"
                "AzureADApplicationID"
                "WorkspaceID"
                "WorkspaceName"
                "WorkspaceURL"
    },
     "protectedSettings" : {
        [ ▼ ] : "[variable ('var2')]"
            "AzureADApplicationSecret"
            "StorageAccountKey"
            "WorkspaceID"
            "WorkspaceKey"
        }
    }
}
```


正解:

```
"type" : "Microsoft.Compute/virtualMachines/extensions",
"name" : "[concat(parameter('vmname'), /OMSExtension]",
"apiVersion" : "[variables('apiVersion')]",
"location" : "[resourceGroup().location]",
"dependsOn" : [
     "[concat('Microsoft.Compute/virtualMachines/", parameters('vmName'))]"
],
"properties" : {
     "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
     "type" :  "MicrosoftMonitoringAgent",
     "typeHandlerVersion" : "1.0",
     "autoUpgradeMinorVersion" : true,
     "settings" : {
          [                    ▼] : "[variable('var1')]"
          "AzureADApplicationID"
          "WorkspaceID"
          "WorkspaceName"
          "WorkspaceURL"
   },
    "protectedSettings" : {
          [                    ▼] : "[variable ('var2')]"
          "AzureADApplicationSecret"
          "StorageAccountKey"
          "WorkspaceID"
          "WorkspaceKey"
     }
   }
}
```

Explanation:

```
},
"properties" : {
    "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
    "type" :  "MicrosoftMonitoringAgent",
    "typeHandlerVersion" : "1.0",
    "autoUpgradeMinorVersion" : true,
    "settings" : {
        [ ▼ ] : "[variable('var1')]"
            "AzureADApplicationID"
            "WorkspaceID"
            "WorkspaceName"
            "WorkspaceURL"
    },
    "protectedSettings" : {
        [ ▼ ] : "[variable ('var2')]"
            "AzureADApplicationSecret"
            "StorageAccountKey"
            "WorkspaceID"
            "WorkspaceKey"
    }
  }
}
```

References:
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent- in-windows-json-templates/

質問: **129**

Azure Active Directory（Azure AD）にリンクされている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。

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

パージ保護が無効に設定されているVault1という名前のAzureキーボールトがあります。Vault1には、次の表に示すアクセスポリシーが含まれています。

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

次の表に示すように、Vault1の役割の割り当てを作成します。

Name	Role
User1	**None**
User2	Key Vault Reader
User3	User Access Administrator

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」、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。

正解:

Explanation:

質問: **130**

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	Location	Virtual network name
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

すべての仮想ネットワークはピアリングされています。

Azure Bastion を VNET2 にデプロイします。

要塞ホストによって保護できる仮想マシンはどれですか?

A. VM1、VM2、VM3、およびVM4

B. VM1、VM2、VM3のみ

C. VM2とVM4のみ

D. VM2のみ

正解: **(**正解を表示します**)**

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

質問: **131**
Contoso.com という名前の Microsoft Entra テナントおよび RG1 という名前のリソース グループにリンクされている Subscription1 という名前の Azure サブスクリプションがあります。
contoso.com に Role1 という名前のカスタム ロールを作成します。
権限委任に Role1 を使用できるのはどこですか?
A. contoso.com. RG1. および Subscription1
B. contoso.com とサブスクリプション 1 のみ
C. contoso.com と RG1 のみ
D. contoso.com のみ
正解: **A** (コメントを発表する)

質問: **132**
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	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	*None*
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

VNET1、VNET2、およびVNET3は相互にピアリングされます。次のアクションを実行します。
*米国西部地域にASG1とASG2という名前の2つのアプリケーションセキュリティグループを作成します。
*VM1のネットワークインターフェイスをASG1に追加します。

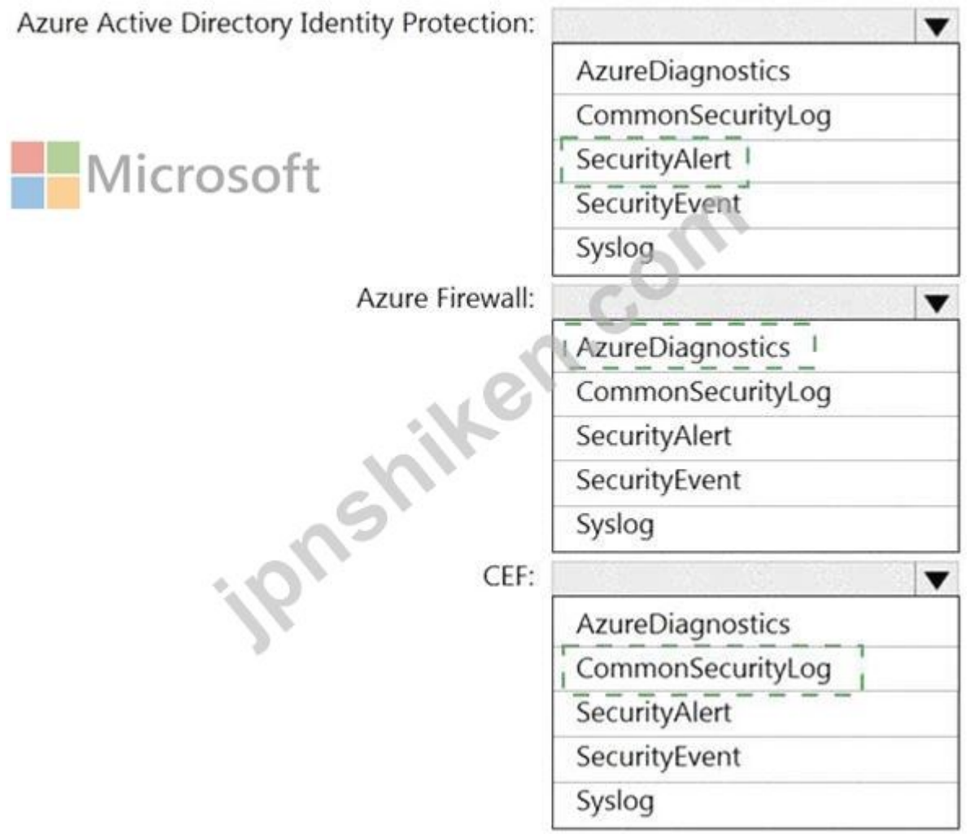
正解:
see the answer below in explanation.
Explanation:
Answer as below.

質問: **133**
Azure サブスクリプションと、AWS1 という名前の Amazon Web Services (AWS) アカウントをお持ちの場合、AWS1 を Microsoft Defender for Cloud に追加する必要があります。
AWS1 のクラウドアクセス用に Defender を構成するために使用できる 2 つのデプロイ方法は何ですか?

正解はそれぞれ完全な解答を示しています。
注：正解ごとに1ポイント獲得できます。
A. an Azure Resource Manager (ARM) template
B. an AWS CloudFormation stack
C. an Azure deployment stack
D. a Terraform template
E. AWS Systems Manager Automation
正解: **(**正解を表示します**)**

質問: **134**
次のデータコネクタを持つAzureSentinelワークスペースがあります。
Azure ActiveDirectoryID保護
共通イベント形式（CEF）
Azureファイアウォール
各コネクタからデータが取り込まれていることを確認する必要があります。
ログクエリウィンドウから、コネクタごとにどのテーブルをクエリ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：正しい選択はそれぞれ1ポイントの価値があります。

正解:



Explanation:

Graphical user interface, application, table Description automatically generated

Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Azure Firewall:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

質問: **135**

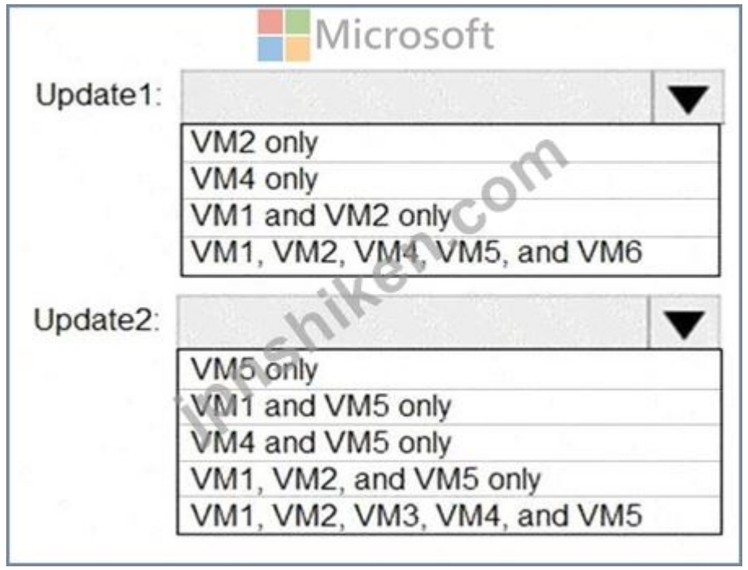
更新管理が有効になっているAzure仮想マシンがあります。仮想マシンは、次の表に示すように構成されます。

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

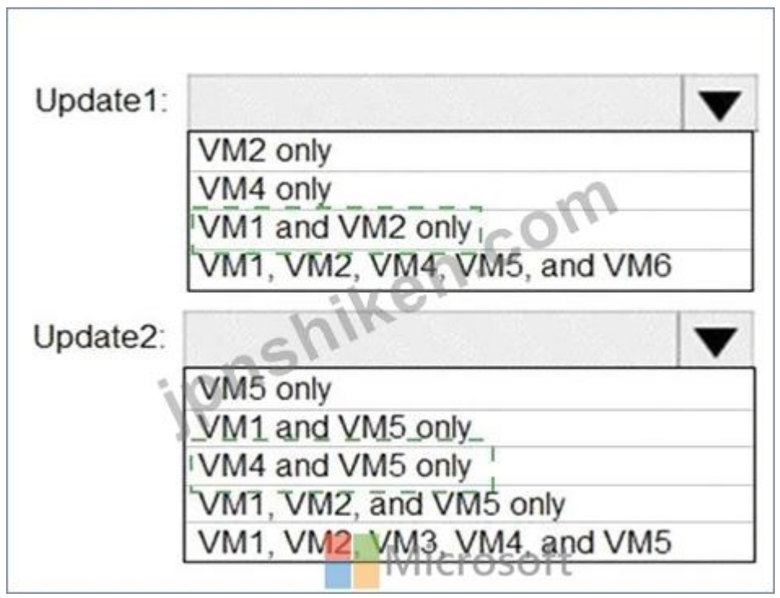
Update1とUpdate2という名前の2つの更新プログラムの展開をスケジュールします。Update1はVM3を更新します。Update2はVM6を更新します。

Update1および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、回答エリアで適切なオプションを選択します。

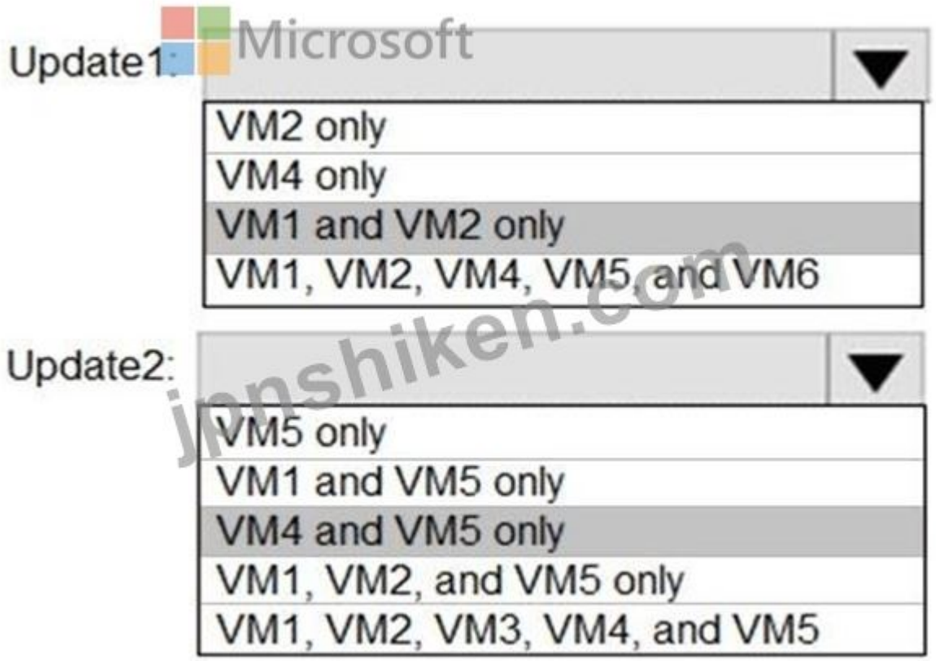
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:



Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

質問: **136**
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、次の表に示すリソースを含むStorage1という名前のAzureストレージアカウントがあります。

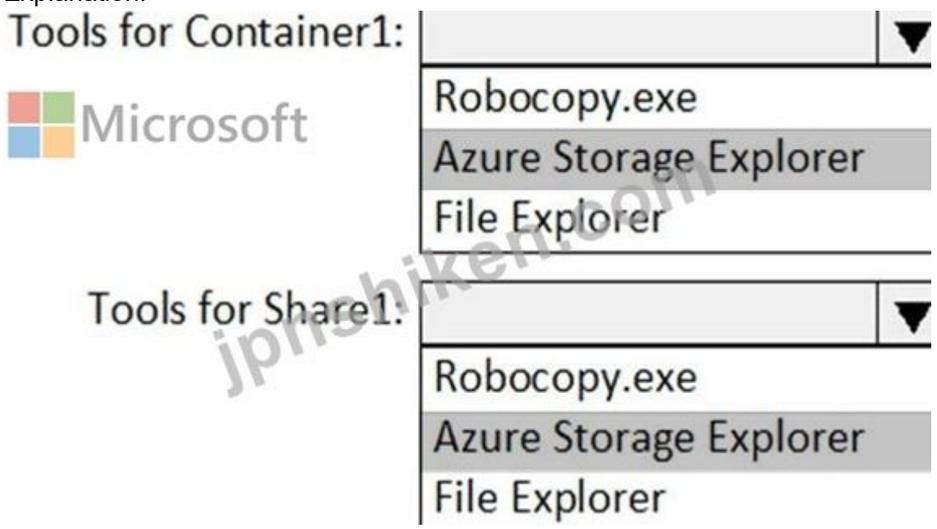
Name	Type
Container1	Blob container
Share1	File share

共有アクセス署名 $AS）を生成して、blobサービスとファイルサービスに接続します。
Container1およびShareのコンテンツにアクセスするには、どのツールを使用できますか？ SASを使用して？回答するには、回答エリアで適切なオプションを選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。
Answer Area

正解:

Answer Area

Explanation:



質問: **137**

次の表に示すユーザーを含む Microsoft Entra テナントがあります。

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

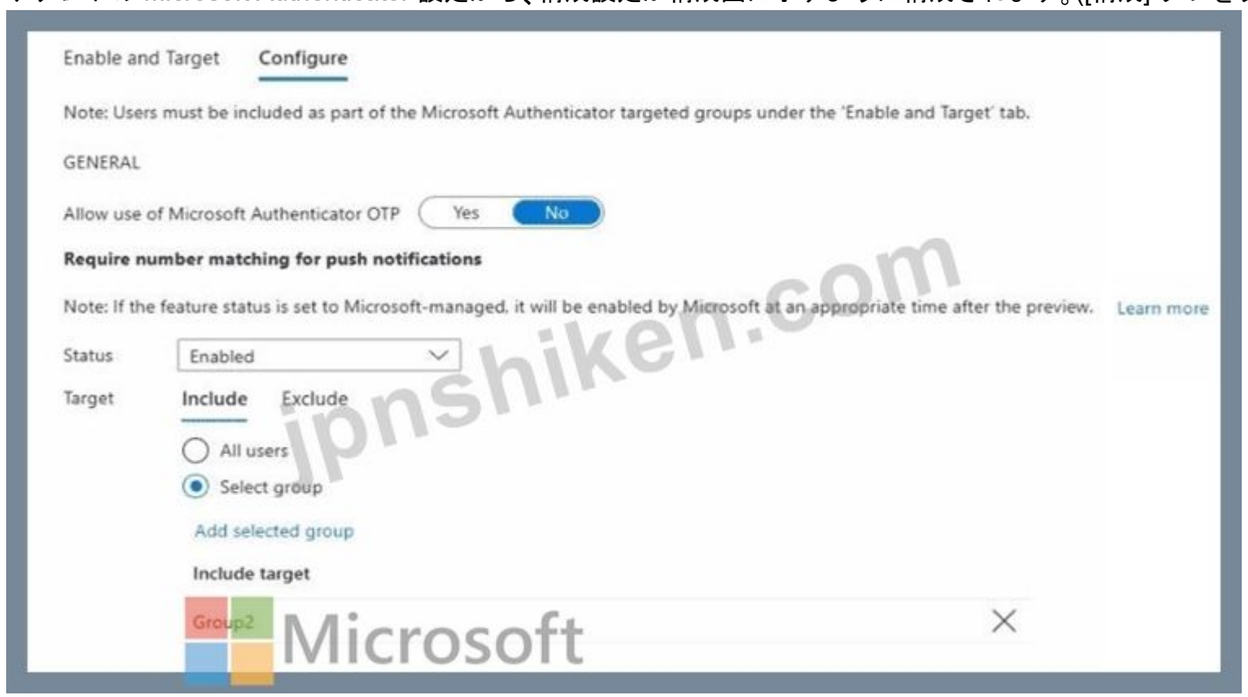
次の設定を持つ条件付きアクセス ポリシーを構成します。

* 名前: CAPolicy1
* 課題

o ユーザーまたはワークロード ID: グループ 1

o 対象リソース: すべてのクラウドアプリ
* アクセス制御
o アクセスを許可する: 多要素認証を要求する
テナントの Microsoft Authenticator 設定から、有効化とターゲットの設定が 「有効化とターゲット」の図に示すように構成されます。(「有効化とターゲット」タブをクリックします。)

テナントの Microsoft Authenticator 設定から、構成設定が構成図に示すように構成されます。([構成] タブをクリックします。)



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。
注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

質問: **138**
Subscription1という名前のAzureサブスクリプションがあります。
VM1という名前のLinux仮想マシンをSubscription1にデプロイします。
VM1のメトリックとログを監視する必要があります。
D18912E1457D5D1DDCBD40AB3BF70D5D
何を使うべきですか？
A. Azure Analysis Services
B. Linux Diagnostic Extension（LAD）3.0
C. Azure HDInsight
D. AzurePerformanceDiagnostics拡張機能
正解: **(**正解を表示します**)**

質問: **139**
Azure AD テナントがあります。

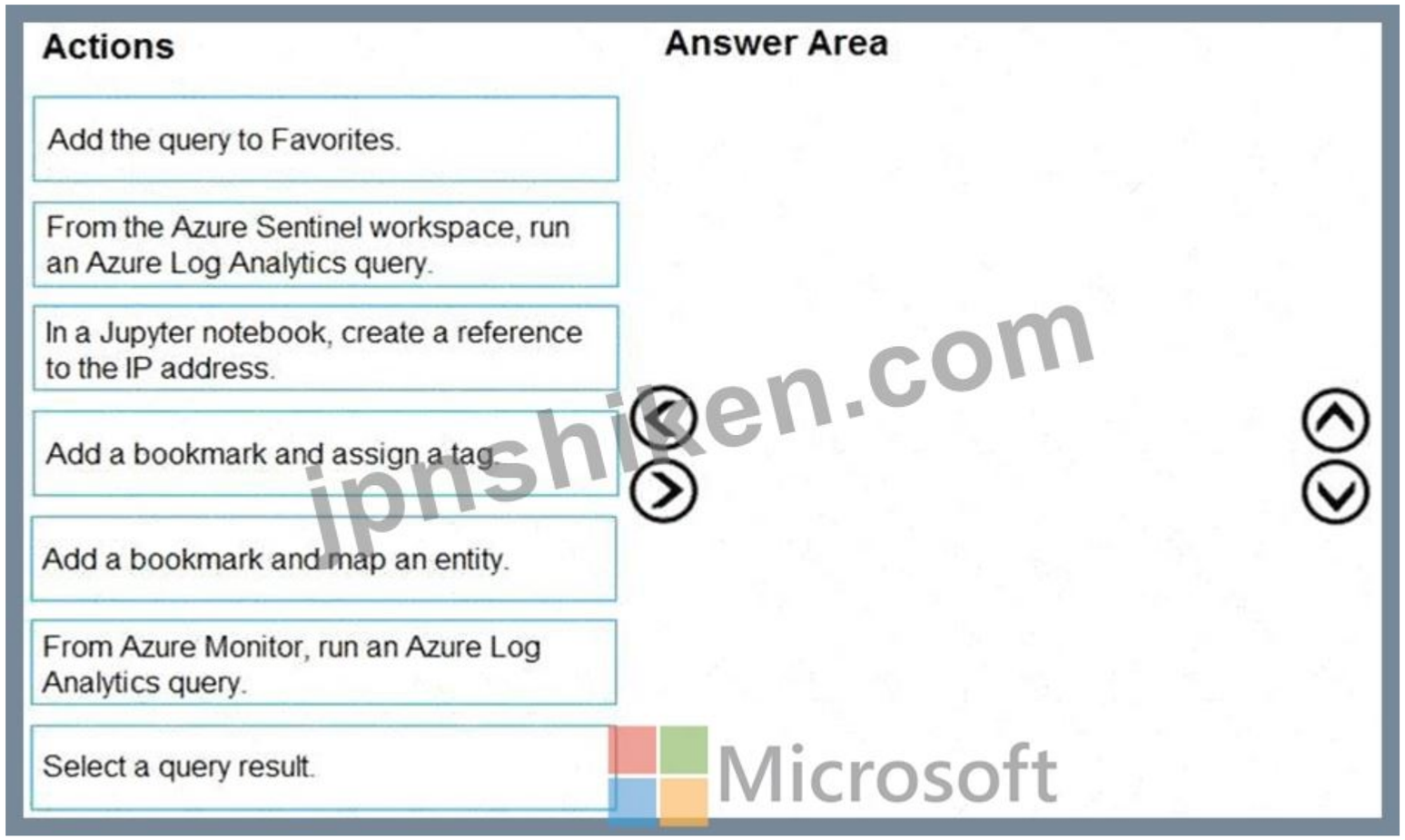
次の要件を満たす認証ソリューションを実装する予定です。
※番号合わせが必要です。
* サインイン時に地理的位置を表示します。
ソリューションにはどの認証方法を含めるべきですか?
A. SMS
B. Microsoft Authenticator
C. FID02セキュリティキー
D. 一時アクセスパス
正解: **(**正解を表示します**)**

質問: **140**
WebApp1 という名前の Azure App Services Web アプリと、Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。Vault1 には、次の表に示す証明書があります。

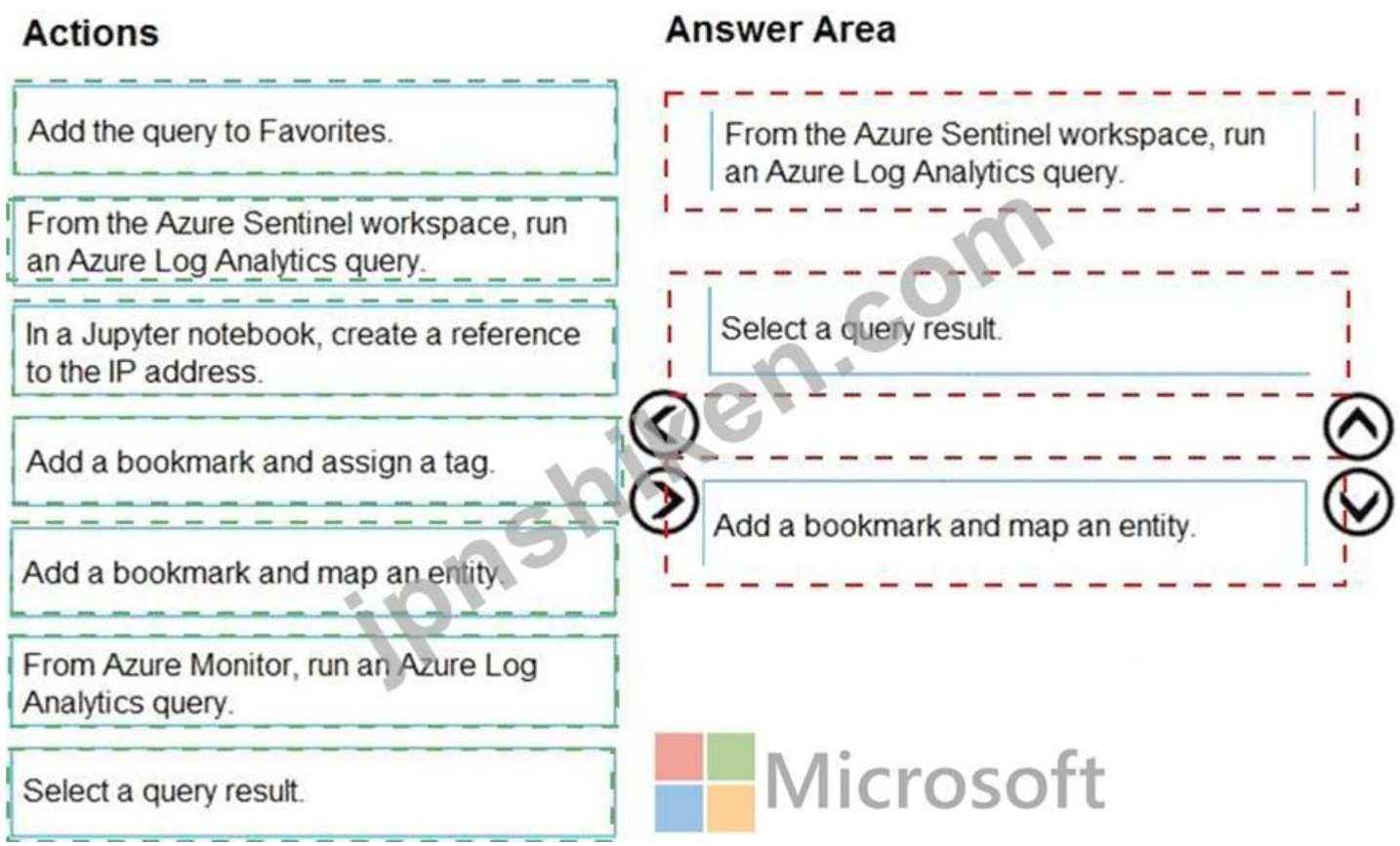
Name	Content type	Key type	Key size
Cert1	PKCS #12	RSA	2048
Cert2	PKCS #12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

WebApp1 に TLS を実装する予定です。
WebApp1 に証明書を追加する必要があります。
Vault1 のどの証明書を WebApp1 に追加できますか?
A. Cert1とCert3のみ
B. Cert3 と Cert4 のみ
C. 証明書1、証明書2、証明書3、証明書4
D. Cert1とCert2のみ
正解: **(**正解を表示します**)**

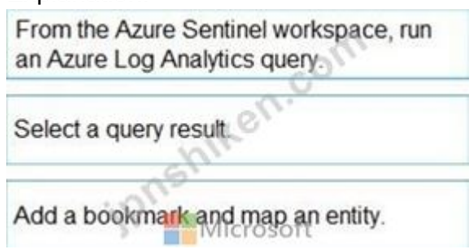
質問: **141**
Azure Active Directory (Azure AD) データ コネクタを備えた Azure Sentinel ワークスペースがあります。
特定の IP アドレスからの疑わしいトラフィックを脅威として探しています。
ワークスペースに保存されている中間イベントに注釈を付け、調査グラフ内を移動するときに IP アドレスを参照できるようにする必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

質問: **142**
Microsoft Defender for Cloud を使用する Azure サブスクリプションがあります。
アマゾン ウェブ サービス (AWS) アカウントをお持ちです。
AWS アカウントを Defender for Cloud に追加する必要があります。
まず何をすべきでしょうか?
A. Defender for Cloud から、環境設定を構成します。
B. AWS アカウントから、セキュリティ ハブを有効にします。
C. Azure portal から、AWS エンタープライズ アプリケーションを追加します。
D. Defender for Cloud から、セキュリティ ソリューション設定を構成します。

正解: (正解を表示します)

質問: **143**

次の表に示すユーザーを含む、contoso1812.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナントがあります。

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

Label1 という名前の Azure Information Protection ラベルを作成します。Label1 の保護設定は、図に示すように構成されています。(図タブをクリックします。)

Label1 は File1 という名前のファイルに適用されます。

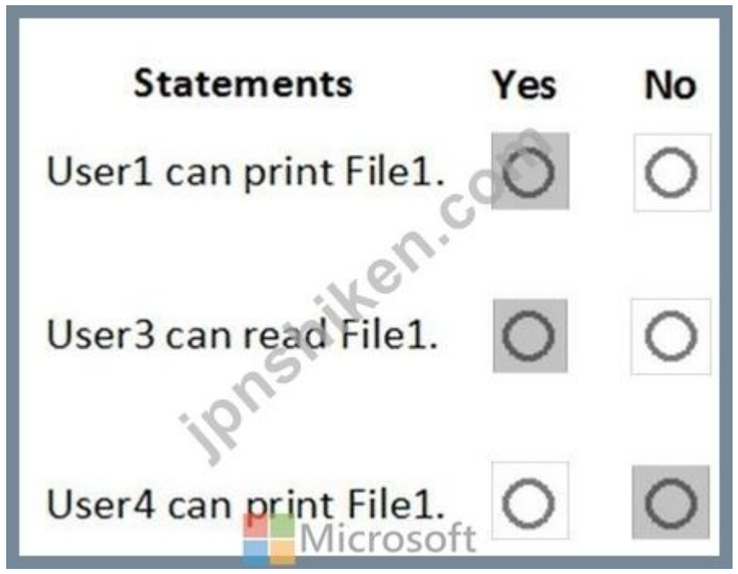
次の各文について、正しい場合は「はい」を選択し、そうでない場合は「いいえ」を選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

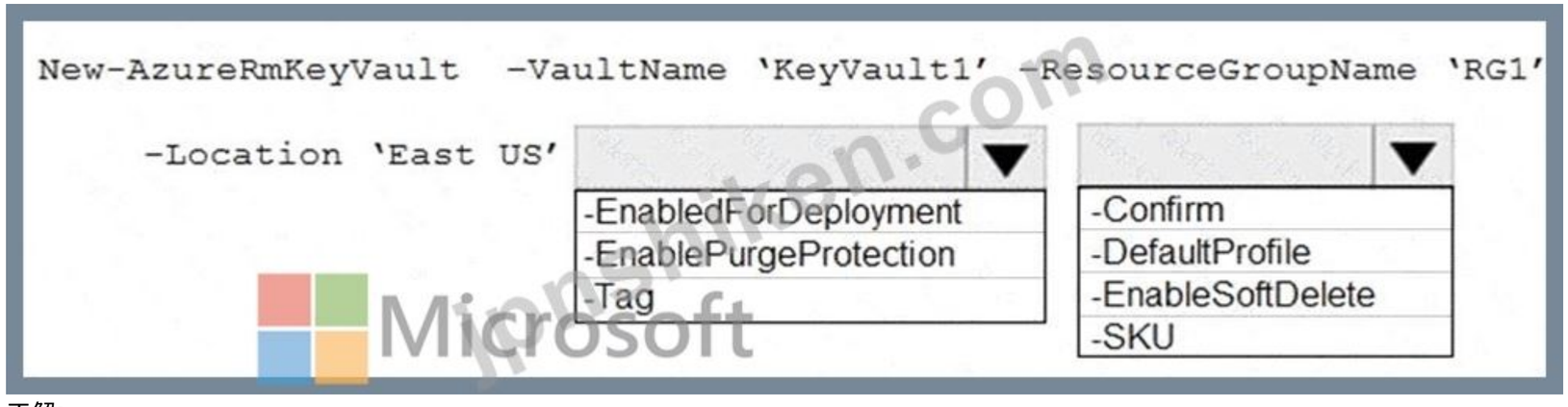
Statements	Yes	No
User1 can print File1.	○	○
User3 can read File1.	○	○
User4 can print File1.	○	○

正解:

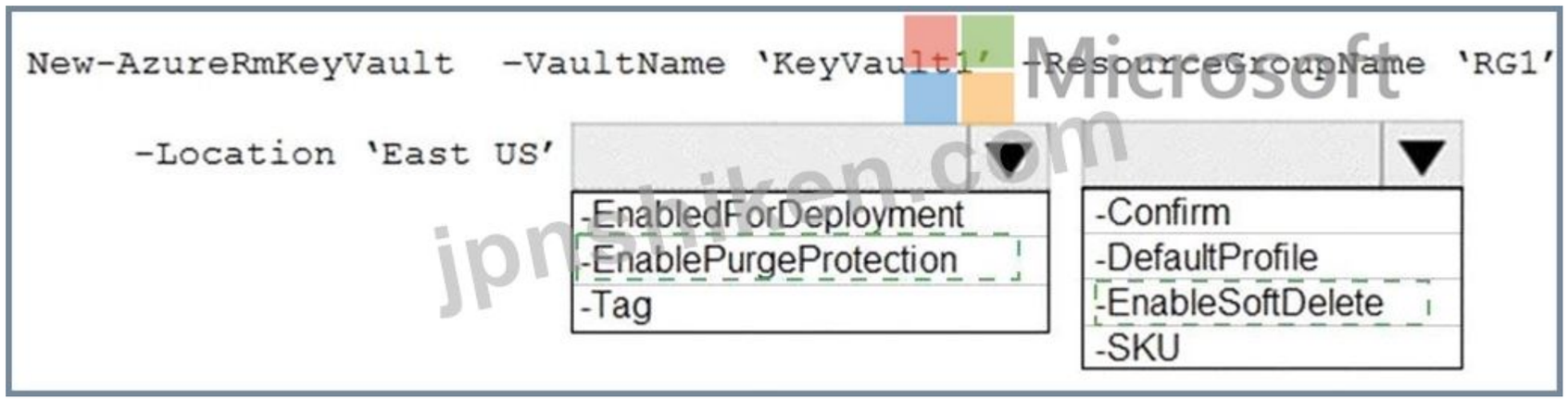
Explanation:



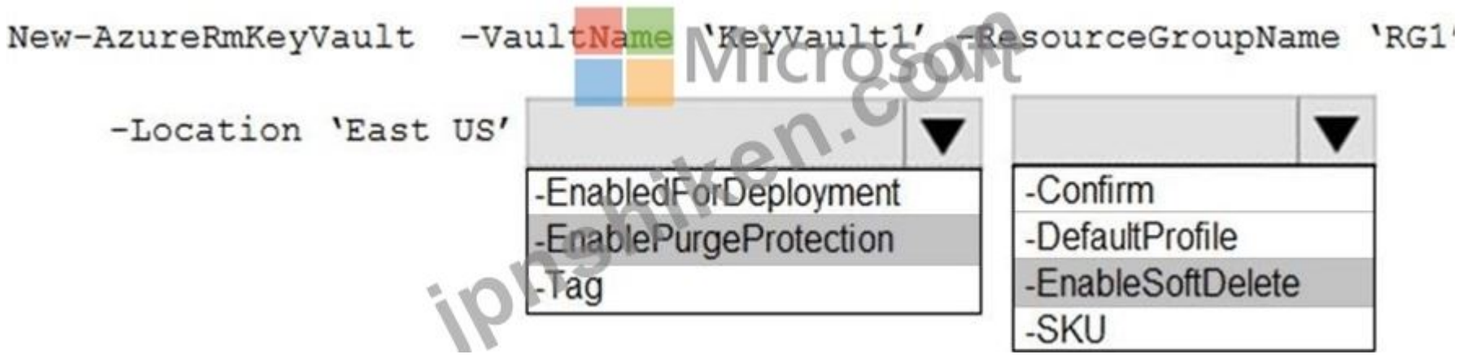
質問: **144**
Azure Key Vaultを作成する必要があります。このソリューションでは、Key Vaultから削除されたオブジェクトを90日間保持する必要があります。
コマンドをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:



Box 1: -EnablePurgeProtection

If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete

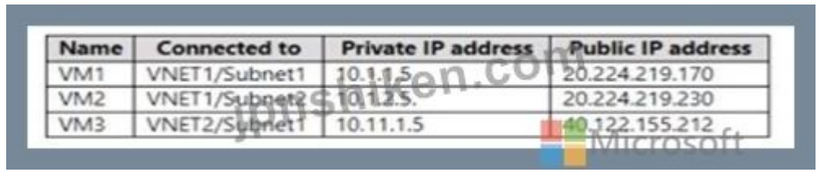
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References:

https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

質問**: 145**

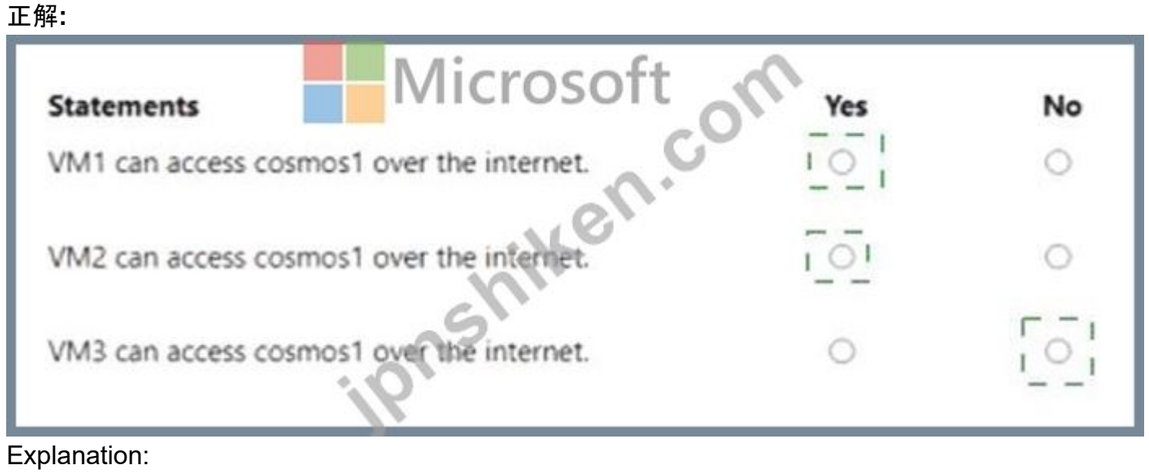
次の表に示す仮想マシンを含む Azure サブスクリプションがあります。



Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

次の図に示すように、cosmos1 という名前の Azure Cosmos DB アカウントが構成されています。

正解:



Explanation:
Yes, Yes, No

質問: **146**
Azureサブスクリプションがあります。
Azure Security Centerでワークフローの自動化を作成し、セキュリティの脆弱性を自動的に修正することを計画しています。
最初に何を作成する必要がありますか？
A. a managed identity
B. an automation account
C. an Azure function app
D. an alert rule
E. an Azure logic app
正解: **E (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

質問: **147**
Vault1という名前のAzure Key Vaultを含むAzureサブスクリプションがあります。
Vault1で、Secret1という名前のシークレットを作成します。

アプリケーション開発者は、Azure Active Directory（Azure AD）にアプリケーションを登録します。
アプリケーションがSecret1を使用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. Azure ADで、ロールを作成します。
B. Azure Key Vaultでキーを作成します。
C. Azure Key Vaultで、アクセスポリシーを作成します。
D. Azure ADで、Azure ADアプリケーションプロキシを有効にします。
正解: **C (**コメントを発表する**)**
"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token"
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

質問: **148**
ネットワークには、Azure Active Directory（Azure AD）と同期するadatum.comという名前のオンプレミスのActiveDirectoryドメインが含まれています。Azure AD Connectは、Server1という名前のドメインメンバーサーバーにインストールされます。
adatum.comドメインのドメイン管理者が同期オプションを変更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。
ドメイン管理者にどのAzureADロールを割り当てる必要がありますか？
A. セキュリティ管理者
B. グローバル管理者
C. ユーザー管理者
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

質問: **149**
100台の仮想マシンを含みAzureSecurityCentを含むAzureサブスクリプションがあります。標準階層が有効になっています。
各仮想マシンの脆弱性スキャンを実行することを計画しています。
Azure Resource Managerテンプレートを使用して、脆弱性スキャナー拡張機能を仮想マシンにデプロイする必要があります。
仮想マシンへの拡張機能の展開を自動化するには、コードでどの2つの値を指定する必要がありますか？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. ユーザーが管理IDを割り当てた
B. KeyVault管理ストレージアカウントキー
C. Azure Active Directory（Azure AD）ID
D. システムによって割り当てられたマネージドID
E. プライマリ共有キー
F. ワークスペースID
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

質問: **150**

SQL1という名前のAzure SQL Databaseサーバーがあります。
SQL1のAdvanced Threat Protectionを有効にして、すべての脅威検出タイプを検出する予定です。
Advanced Threat Protectionは脅威としてどのアクションを検出しますか？
A. A user updates more than 50 percent of the records in a table.
B. A user attempts to sign as select * from table1.
C. A user is added to the db_owner database role.
D. A user deletes more than 100 records from the same table.
正解: **(**正解を表示します**)**
Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview

質問: **151**
次の内容を含む File1.yaml という名前のファイルがあります。

```
ocation: eastus
ame: containergroup1
roperties:
 containers:
 - name: container1
   properties:
     environmentVariables:
       - name: 'Variable1'
         value: 'Value1'
       - name: 'Variable2'
         secureValue: 'Value2'
     image: nginx
     ports: []
     resources:
       requests:
         cpu: 1.0
         memoryInGB: 1.5
 osType: Linux
 restartPolicy: Always
ags: null
```


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? 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 ポイントが付与されます。

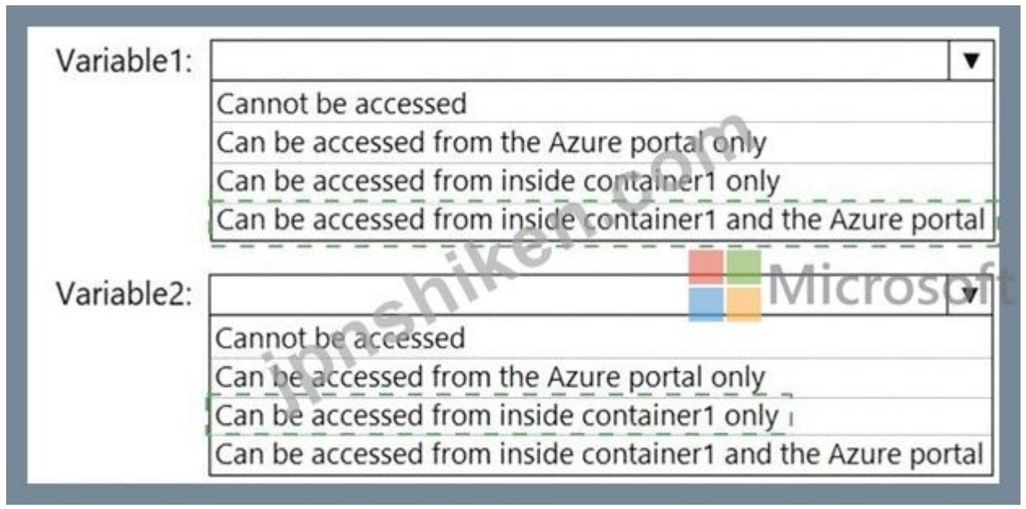
Variable1:

- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

Variable2:

- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

正解:



Explanation:

Variable1:

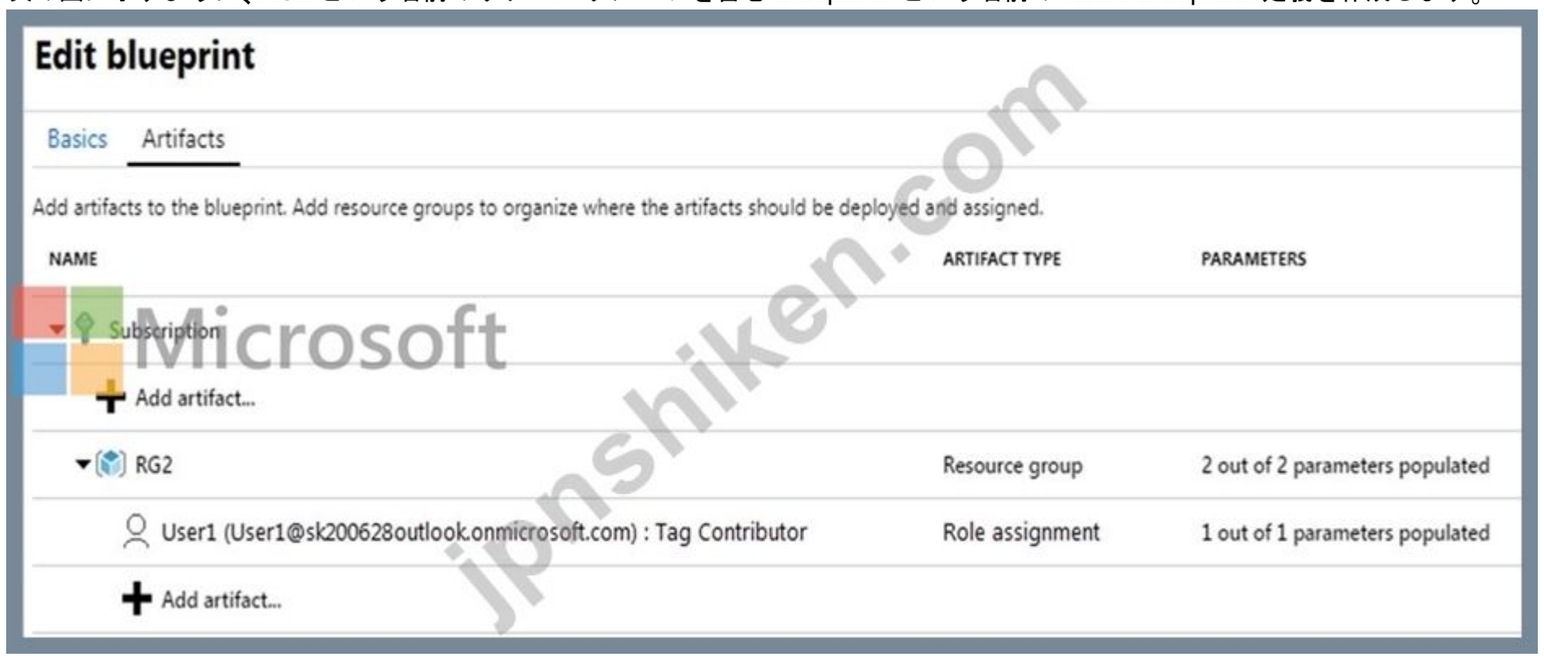
- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- **Can be accessed from inside container1 and the Azure portal**

Variable2:

- Cannot be accessed
- Can be accessed from the Azure portal only
- **Can be accessed from inside container1 only**
- Can be accessed from inside container1 and the Azure portal

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

質問: **152**
Subscription1 という名前の Azure サブスクリプションがあり、このサブスクリプションには RG1 というリソース グループと User1 というユーザーが含まれています。User1 には RG1 の所有者ロールが割り当てられています。
次の図に示すように、RG2 という名前のリソース グループを含む Blueprint1 という名前の Azure Blueprints 定義を作成します。



次の設定を使用して、Blueprint1 を Subscription1 に割り当てます。
* ロックの割り当て: 読み取り専用
* 管理対象ID: システム割り当て
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 ポイントが付与されます。

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	○	○
User1 can add tags to RG2.	○	○
You can remove User1 from the Tag Contributor role for RG2.	○	○

正解:

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	○	○
User1 can add tags to RG2.	○	○
You can remove User1 from the Tag Contributor role for RG2.	○	○

Explanation:

Graphical user interface, text, application Description automatically generated

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	○	○
User1 can add tags to RG2.	○	○
You can remove User1 from the Tag Contributor role for RG2.	○	○

Reference:

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

質問: **153**

次の表に示すストレージ アカウントを含む Sub1 という名前の Azure サブスクリプションがあります。

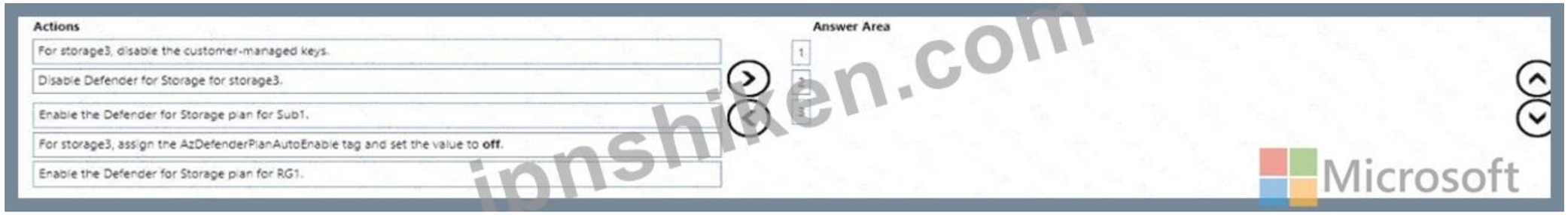
Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

storage3 ストレージ アカウントは、顧客管理キーを使用して暗号化されます。

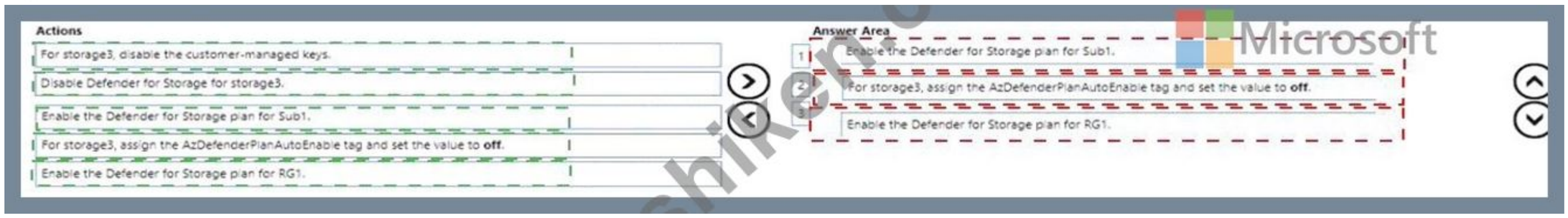
次の要件を満たすには、ストレージ用 Microsoft Defender を有効にする必要があります。

* ストレージ要件のため、storage1 および storage2 アカウントを Defender に含める必要があります。
* storage3 アカウントは、Defender for Storage の保護から除外する必要があります。

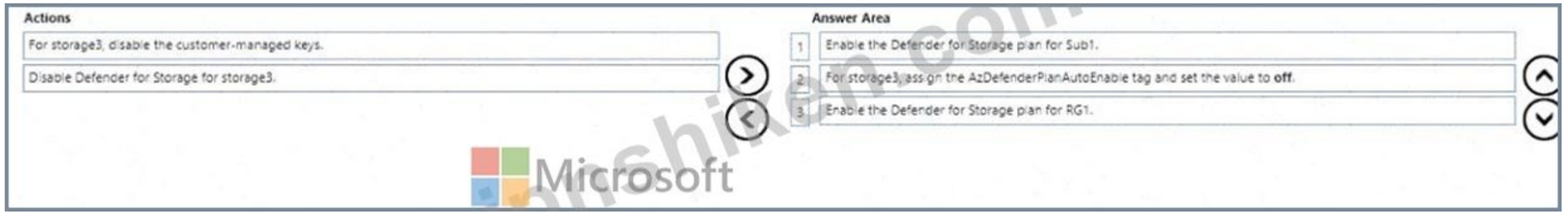
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序で実行します。



正解:



Explanation:



質問: **154**

WebApp1 という名前の Azure App Services Web アプリを含む Azure サブスクリプションがあります。WebApp1 には、複数の Azure リージョンのユーザーがアクセスします。WebApp1へのアクセスを保護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。

* 一般的な Web の脆弱性から保護します。
* さまざまな地域からのトラフィックのルーティングを最適化します。

何を使うべきでしょうか?

A. Azure コンテンツ配信ネットワーク (CDN)
B. Azure アプリケーション ゲートウェイ
C. Azure Front Door プレミアム
D. Azure ファイアウォール

正解: **(**正解を表示します**)**

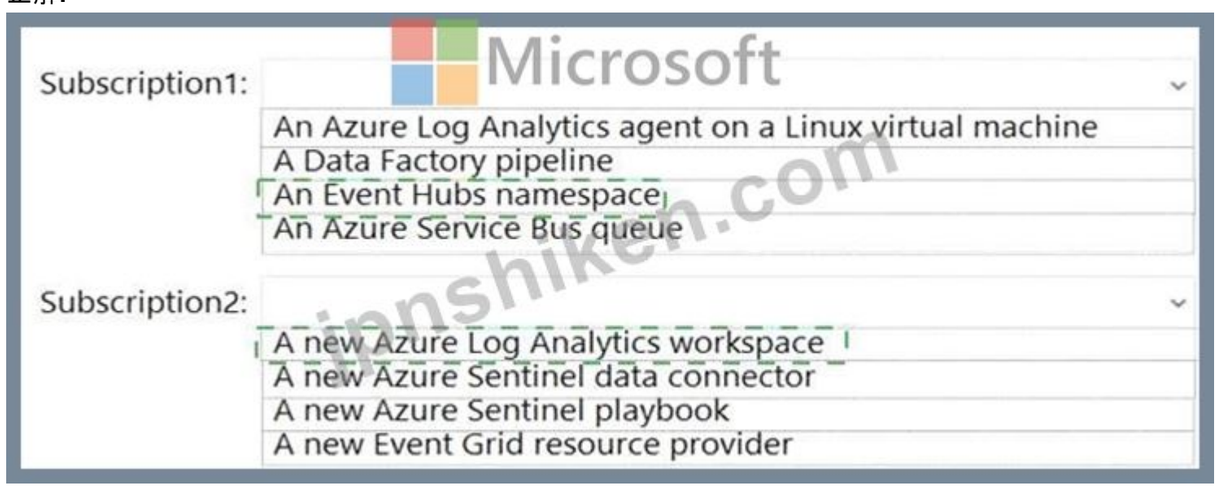
質問: **155**

次の表に示すリソースを含むSubscription1という名前のAzureサブスクリプションがあります。

Name	Type	Description
EventHub1	Azure Event Hubs	**Not applicable**
Adf1	Azure Data Factory	**Not applicable**
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

次のリソースを含むSubscription2という名前のAzureサブスクリプションがあります。
AzureSentinelワークスペース
Azureイベントグリッドインスタンス
NVAからAzureSentinelにCEFメッセージを取り込む必要があります。
サブスクリプションごとに何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：正しい選択はそれぞれ1ポイントの価値があります。

正解:



Explanation:
Graphical user interface, text, application, email Description automatically generated

質問: **156**
Microsoft Defender for Cloud を使用する Azure サブスクリプションがあります。
AWS1 という名前のアマゾン ウェブ サービス (AWS) アカウントがあり、Defender for Cloud に接続されています。
AWS の基本的なセキュリティのベストプラクティスを確実に実施する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。
Defender for Cloud では何をすべきですか?
A. 新しい顧客評価を作成します。
B. 組み込みの評価を割り当てます。
C. 新しいカスタム標準を作成します。
D. 組み込みのコンプライアンス標準を割り当てます。
正解: **(**正解を表示します**)**

質問: **157**
contoso.com という名前の Microsoft Entra テナントがあります。
fabrikam.com という名前の Microsoft Entra テナントを持つパートナー組織と共同作業を行います。Fabrikam。
com では、すべてのユーザーに対して多要素認証 (MFA) が有効になっています。
Contoso.com では、テナント間アクセス設定が テナント間アクセス設定」の図に示すように構成されています。(テナント間アクセス設定をクリックします。

Inbound access settings

Edit inbound defaults

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

Outbound access settings

Edit outbound defaults

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked

Contoso.com では、外部コラボレーション設定」の図に示すように、外部コラボレーション設定」が構成されています。(外部コラボレーション設定」タブをクリックします。)

次の設定を持つ条件付きアクセス ポリシーを作成します。

* 名前: CAPolicy1
* 課題

o ゲストまたは外部ユーザー: B2Bコラボレーションゲストユーザー
o ターゲットリソース
対象: すべてのクラウドアプリ o アクセス制御
アクセスを許可する
デバイスが準拠していることを示すマークを付ける必要がある
多要素認証を要求する
ポリシーを有効にする: オン
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」を選択してください。
注意: 正解したセクションごとに 1 ポイントが付与されます。

正解:

Explanation:

質問: **158**
ネットワーク環境を構成および保護しています。

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仮想マシンを展開します。
すべてのネットワークトラフィックがVM1経由でルーティングされるようにする必要があります。
何を設定する必要がありますか？
A. a system route
B. a network security group (NSG)
C. a user-defined route
正解**: (**正解を表示します**)**
Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.
Note: User Defined Routes
For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:
* Force tunneling to the Internet via your on-premises network.
* Use of virtual appliances in your Azure environment.
* In the scenarios above, you will have to create a route table and add user defined routes to it.
Reference:
https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.
md

質問**: 159**
SQLdb1 に対して計画された変更を実装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 ポイントが付与されます。
A. 条件付きアクセス ポリシーを作成します。
B. コンプライアンス ポリシーを作成します。
C. SQLServer1 の Microsoft Entra 認証を構成します。
D. SQLdb1 のフェデレーション クライアント ID を構成します。
E. SQLdb1 のユーザー割り当てマネージド ID を構成します。
正解**: A,C (**コメントを発表する**)**

質問**: 160**
KeyVault1 という名前の Azure キー コンテナーと、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	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

ボリューム暗号化のために、Key Vault アクセス ポリシーを Azure Disk Encryption へのアクセスを有効にするように設定します。
KeyVault1 は次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。

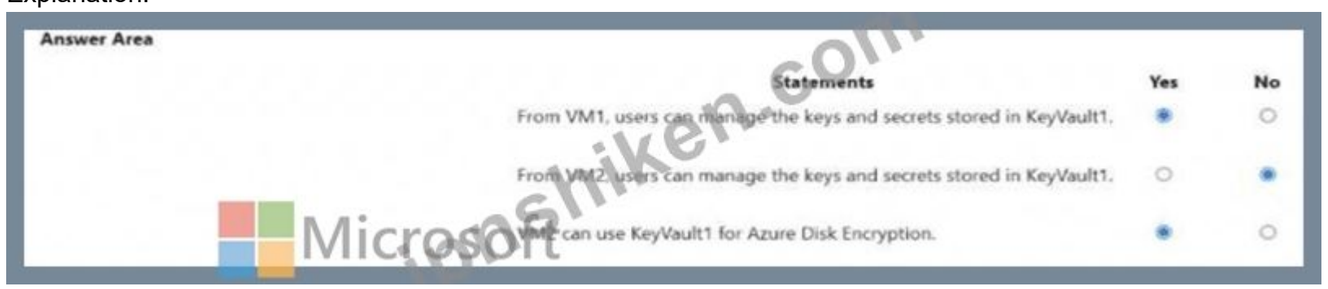
注意: 正しい選択ごとに 1 ポイントが付与されます。

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	○	○
From VM2, users can manage the keys and secrets stored in KeyVault1.	○	○
VM2 can use KeyVault for Azure Disk Encryption	○	○

正解:

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	○	○
From VM2, users can manage the keys and secrets stored in KeyVault1.	○	○
VM2 can use KeyVault for Azure Disk Encryption	○	○

Explanation:



質問: 161

Azure サブスクリプションと、次の表に示すコンピューターがあります。

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

Microsoft Defender for Cloud を使用してコンピューターの脆弱性スキャンを実行する必要があります。どのコンピューターをスキャンできますか？

A. VM1とVM2のみ

B. VM1のみ

C. VM1、VM2、および Server1 のみ

D. Server1 と VMSS1.0 のみ

E. VM1、VM2、Server1、および VMSS1.0

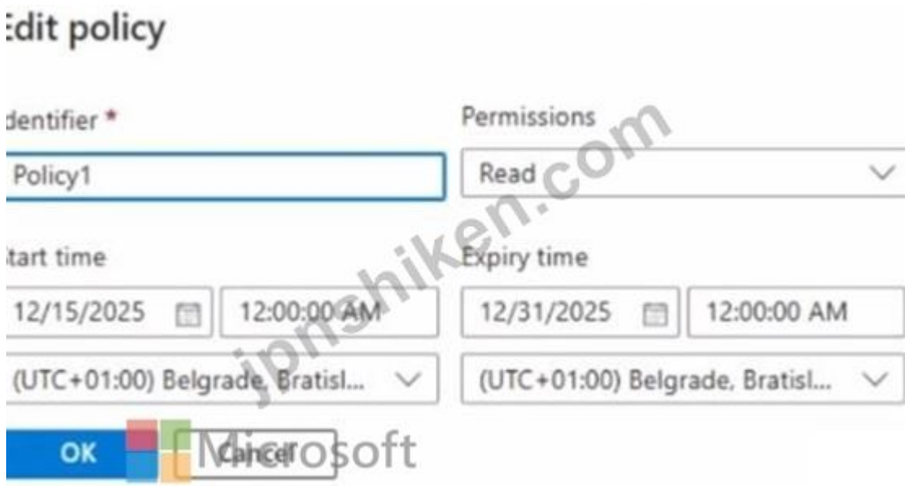
正解: **C** (コメントを発表する)

質問: 162

Azure サブスクリプションには、User1 と User2 という名前の 2 人のユーザーと、次の表に示すブロブ コンテナーが含まれています。

Name	Storage account	Access policy
container1	storage1	Policy1
container2	storage1	*None*

ポリシー1は、以下の図に示すように構成されています。



storage1アカウントには、SAS1という名前の共有アクセス署名(SAS)が付与されています。
* 許可されているサービス: Blob
* 許可されるリソースタイプ: コンテナ
* 許可される権限: 読み取り、書き込み、一覧表示、追加、作成
* Blob バージョン管理権限: バージョンの削除を有効にします
* 許可されるブロブインデックスのアクセス許可: 読み取り/書き込み
* 開始日時と終了日時 :
開始日 :2025年12月1日
終了日 :2025年12月31日
日付はMM/DD/YYYY形式で表記します。
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 : 正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
When using SAS1, User1 can write to container2 on December 5, 2025.	○	○
When using SAS1, User2 can write to container1 on December 20, 2025.	○	○
When using SAS1, User1 can read from container2 on January 10, 2025.	○	○

正解:

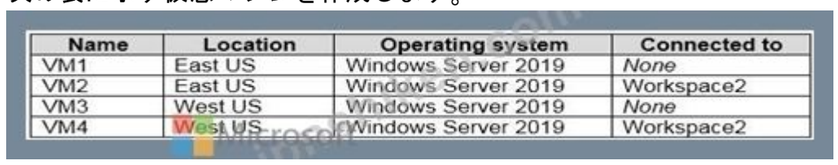
Explanation:

質問: **163**

次の表に示す Azure Log Analytics ワークスペースを含む Azure サブスクリプションがあります。

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	*Not applicable*

次の表に示す仮想マシンを作成します。



Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	*None*
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	*None*
VM4	West US	Windows Server 2019	Workspace2

Azure Sentinel を使用して仮想マシン上の Windows Defender ファイアウォールを監視する予定です。

Azure Sentinel に接続できる仮想マシンはどれですか?

A. VM1とVM3のみ

B. VM1のみ

C. VM1とVM2のみ

D. VM1、VM2、VM3、VM4

正解: **(**正解を表示します**)**

Reference:

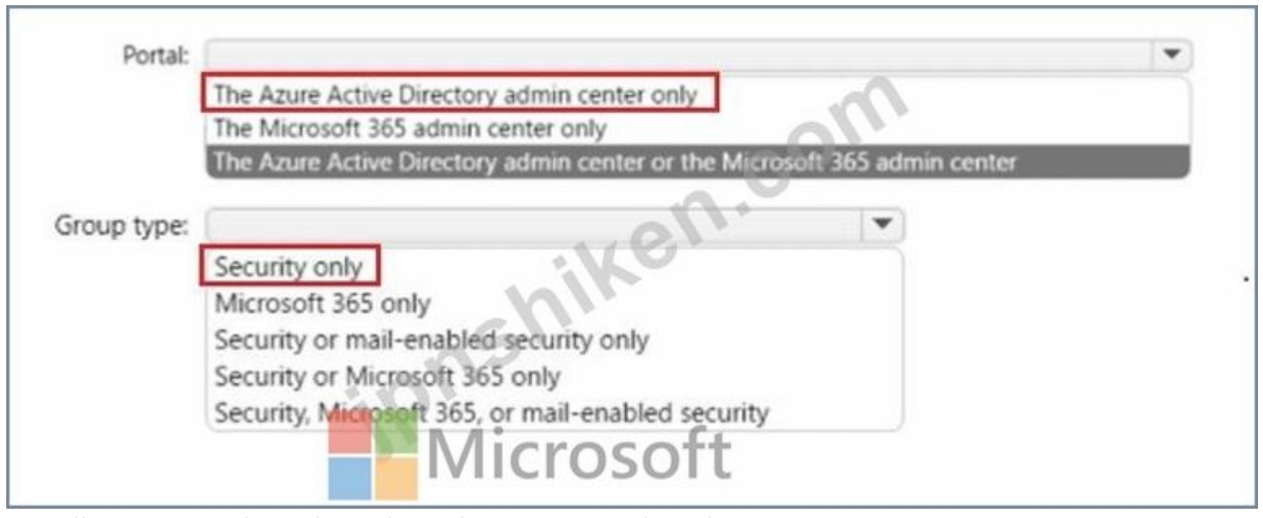
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

質問: **164**

Azure AD Premium P1 ライセンスを持つ contoso.com という名前の Azure AD テナントがあります。
グローバル リーダー ロールが割り当てられる Group1 という名前のグループを作成する必要があります。
Group1 を作成するにはどのポータルを使用する必要がありますか。また、どのようなタイプのグループを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てください。
注: 正解ごとに1ポイント獲得

正解:

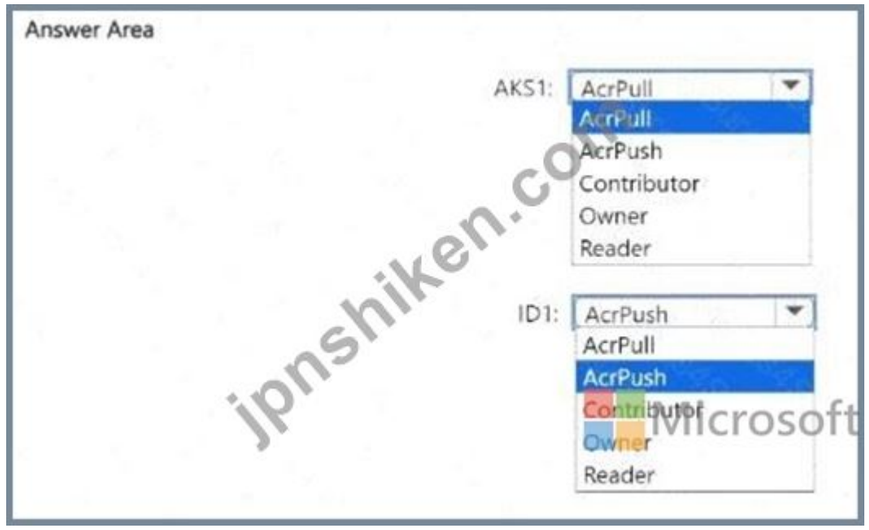
Explanation:



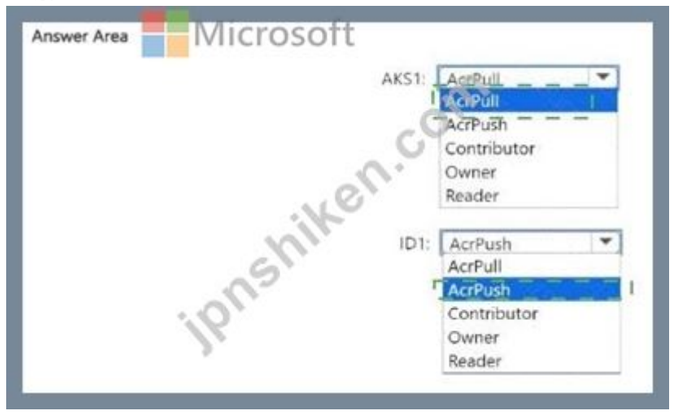
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible

質問: **165**
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。サブスクリプションには、App1 という名前の Azure App Service Web アプリが含まれています。
Azure Web アプリケーション ファイアウォール (WAF) ポリシーを持つ AFD1 という名前の Azure Front Door プロファイルがあります。
App1 へのすべての受信トラフィックが AFD1 を介してフィルタリングされるようにする必要があります。
何をすべきでしょうか?
A. Microsoft Entra アプリケーション プロキシを構成します。
B. VNet1 に対して、ネットワーク セキュリティ グループ (NSG) ルールを構成します。
C. App1 の場合、仮想ネットワーク統合を有効にします。
D. App1 に対して、HTTP ヘッダー フィルター設定を構成します。
正解: **D (**コメントを発表する**)**

質問: **166**
技術要件を満たすには、AKS1 および ID1 マネージド ID を構成する必要があります。ソリューションは、最小権限の原則に従う必要があります。
各 ID にどのロールを割り当て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 ポイントが付与されます。



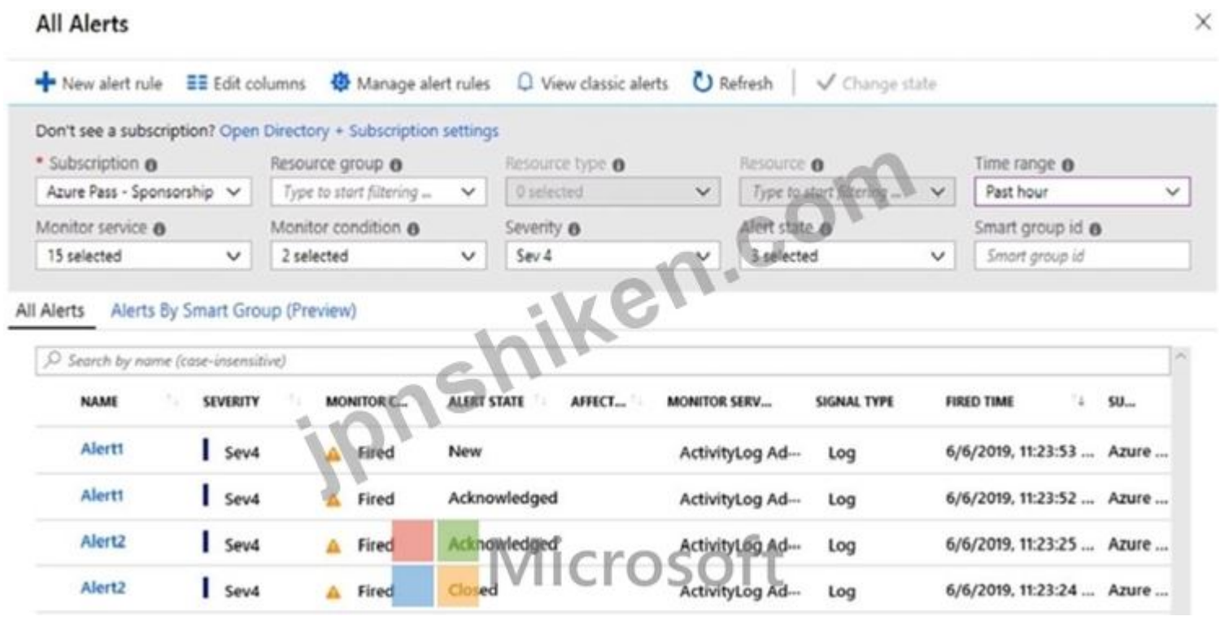
正解:



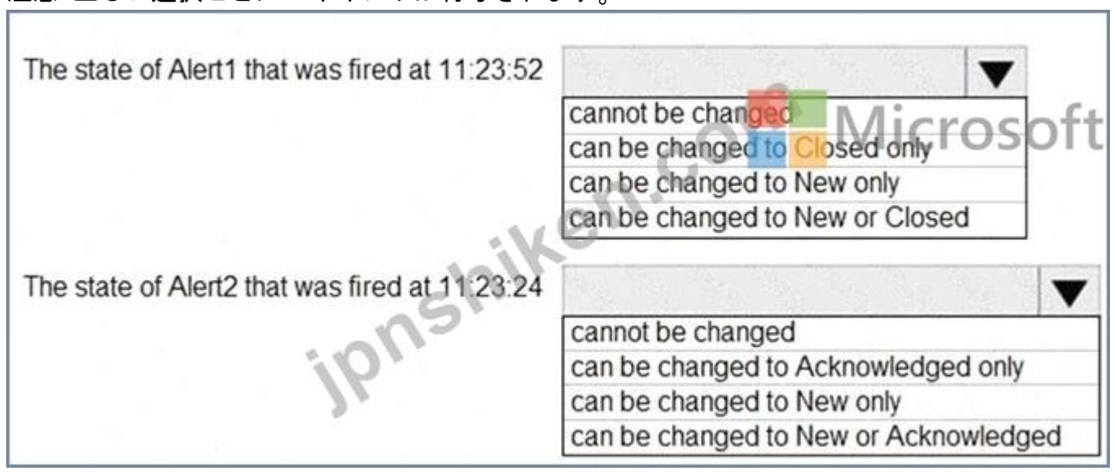
Explanation:

質問: **167**

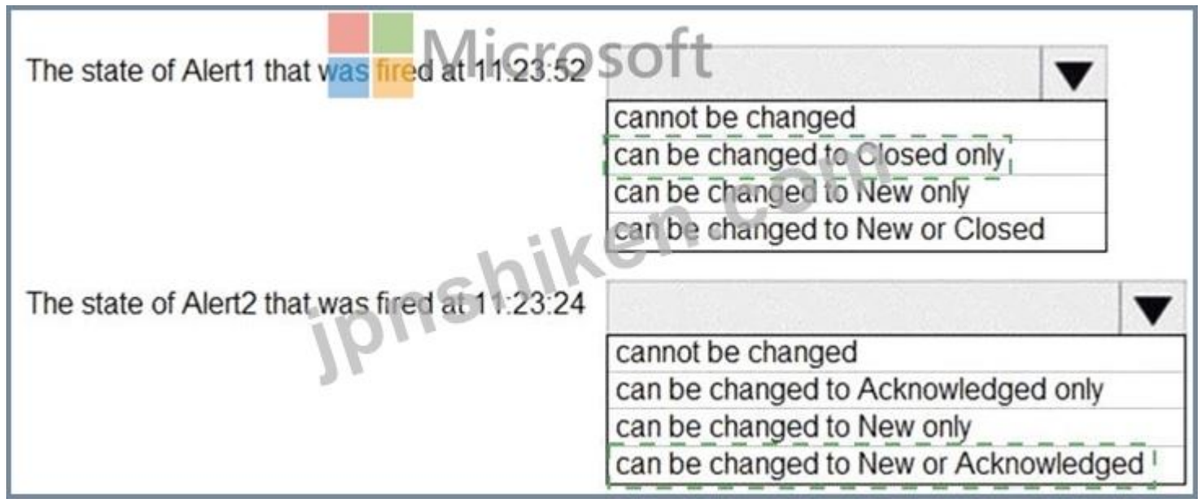
次の図に示すアラートが含まれる Azure サブスクリプションがあります。



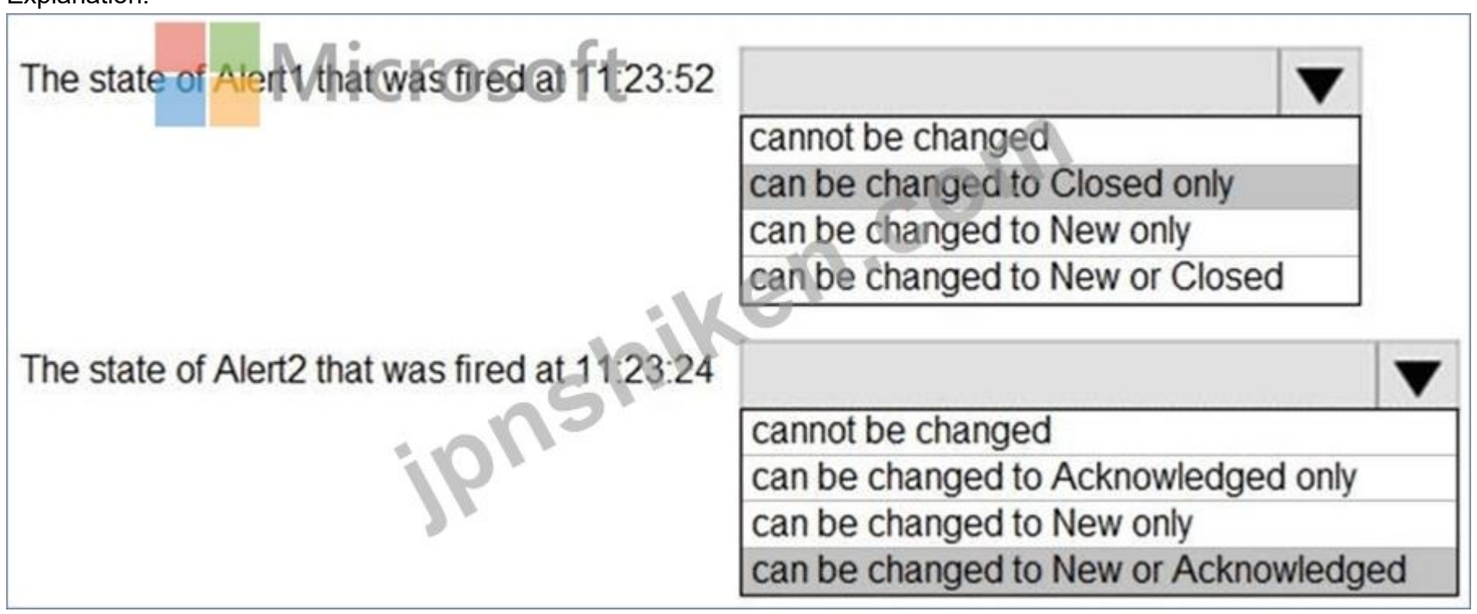
ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview

質問: **168**
次の表に示すユーザーを含むcontoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	*None*	Enabled
User3	Group1	123 555 7891	Required

次の設定を持つAzure AD Identity Protectionユーザーリスクポリシーを作成して適用します。
*割り当て :グループ1を含め、グループ2を除外します

*条件：中以上のサインインリスク
*アクセス :アクセスを許可し、パスワードの変更が必要
以下の各ステートメントについて、ステートメントが真である場合は 「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 :それぞれの正しい選択には1ポイントの価値があります。

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

正解:

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

Box 1: Yes
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.
Box 2: Yes
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.
Box 3: No
Sign-ins from IP addresses with suspicious activity is low.
Note:

Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Azure AD Identity protection can detect six types of suspicious sign-in activities:
* Users with leaked credentials
* Sign-ins from anonymous IP addresses
* Impossible travel to atypical locations
* Sign-ins from infected devices
* Sign-ins from IP addresses with suspicious activity
* Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks - High, Medium & Low:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

質問: **169**
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、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。
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 Active Directory（Azure AD）のハイブリッド構成があります。
仮想ネットワーク上にAzure HDInsightクラスターがあります。
オンプレミスのActive Directory資格情報を使用して、ユーザーがクラスターに対して認証できるようにする予定です。
計画された認証をサポートするように環境を構成する必要があります。
解決策 :Azure ADアプリケーションプロキシを展開します。
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**)**
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

質問: 170
Azure サブスクリプションには、RG1 という名前のリソース グループが含まれています。RG1 には、storage1 という名前のストレージ アカウントが含まれています。
Role1とRole2という名前の2つのカスタムAzureロールがあり、それらはRG1にスコープされています。
Role1の権限は、以下のJSONコードに示されています。

```
"permissions": [
        {
            "actions": [
                "Microsoft.Storage/storageAccounts/listKeys/action",
                "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                "Microsoft.Storage/storageAccounts/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
        }
    ]
```

Role2の権限は、以下のJSONコードに示されています。

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

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：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

正解:

Explanation:

質問: 171

Windows Server2019を実行するVM1および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。
AzureAutomation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。
あなたはそのアップデートを確実にする必要があります！次の要件を満たしています。
* VM1とVM2に更新を自動的に適用します。
*新しいWindowsServer2019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？
A. 動的グループクエリ
B. Kustoクエリ言語クエリ
C. 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
D. メンバーシップタイプがダイナミックデバイスのセキュリティグループ
正解: **(**正解を表示します**)**

質問: 172

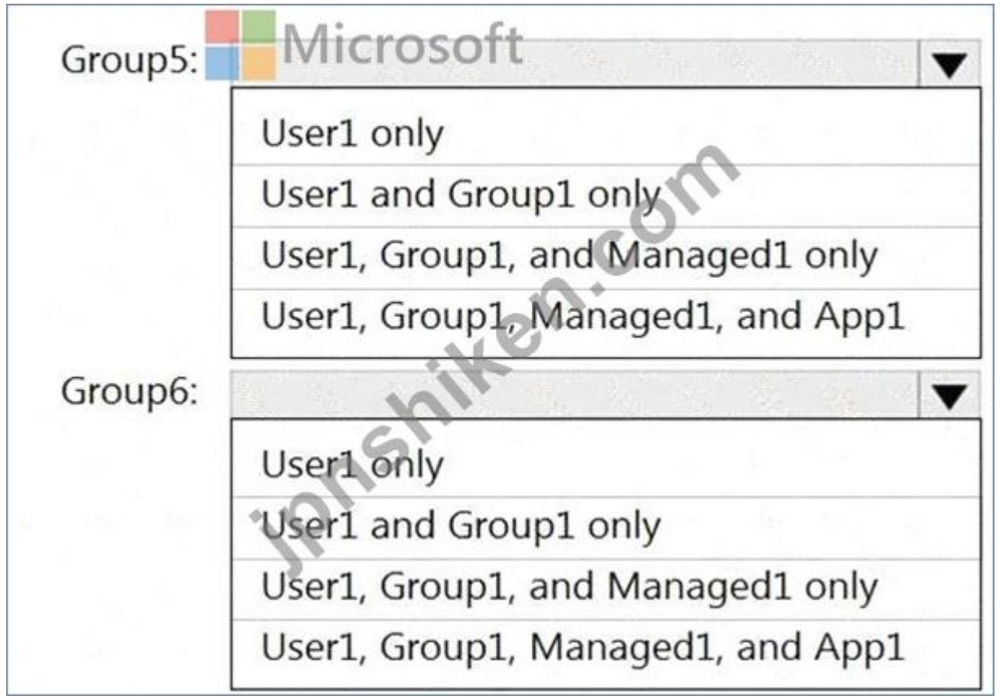
次の表に示す Azure Active Directory (Azure AD) リソースを含む Azure サブスクリプションがあります。

Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

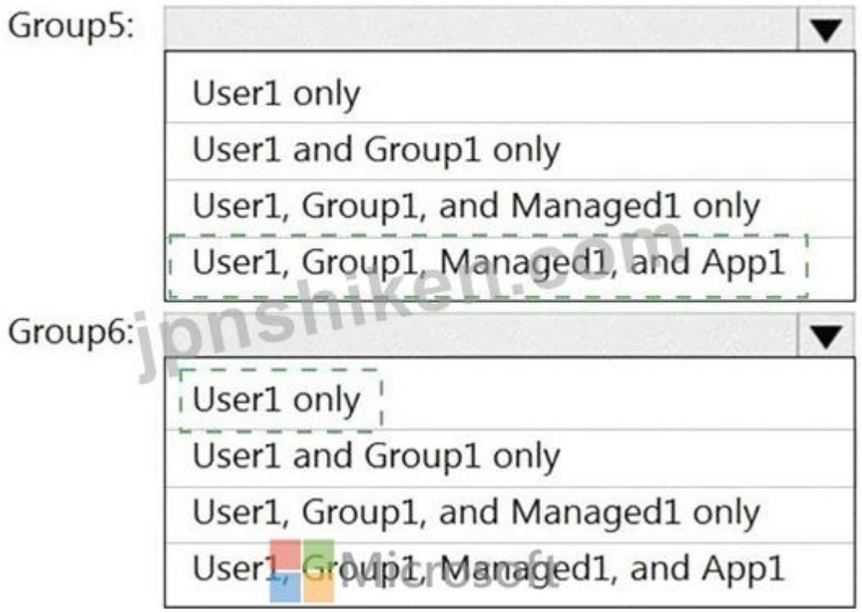
次の表に示すグループを作成します。

Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

グループ5とグループ6に追加できるリソースはどれですか? 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 ポイントが付与されます。

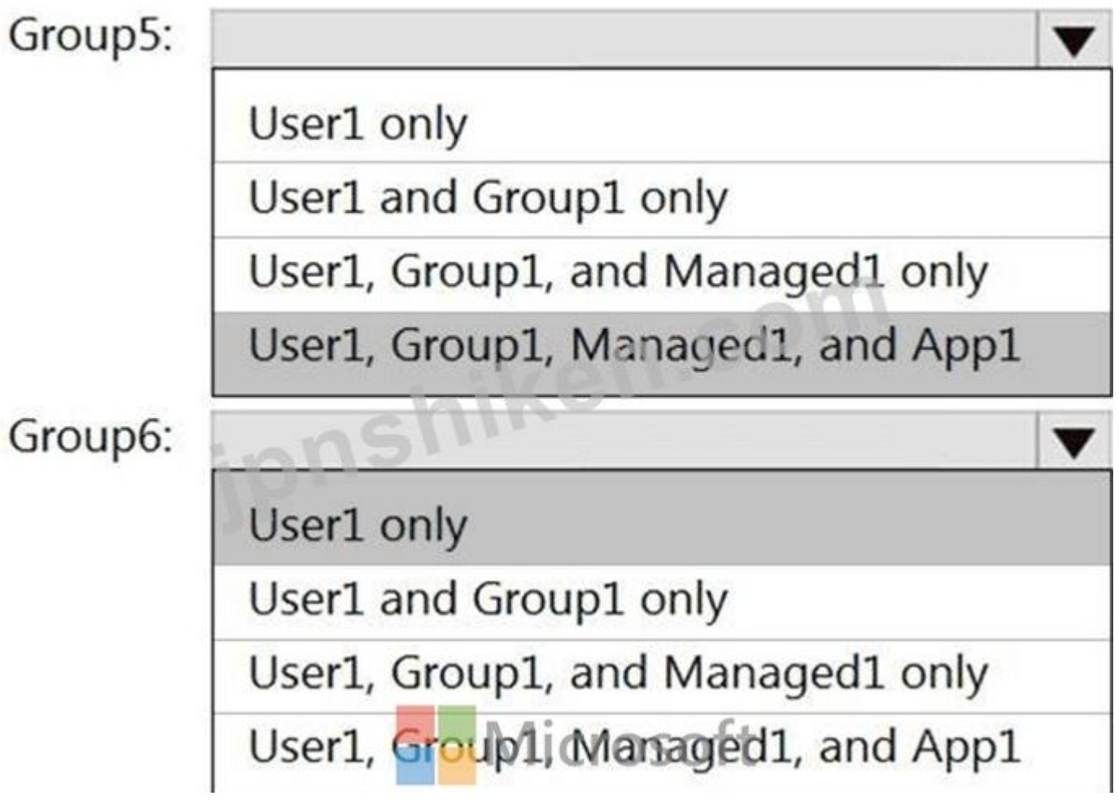


正解:



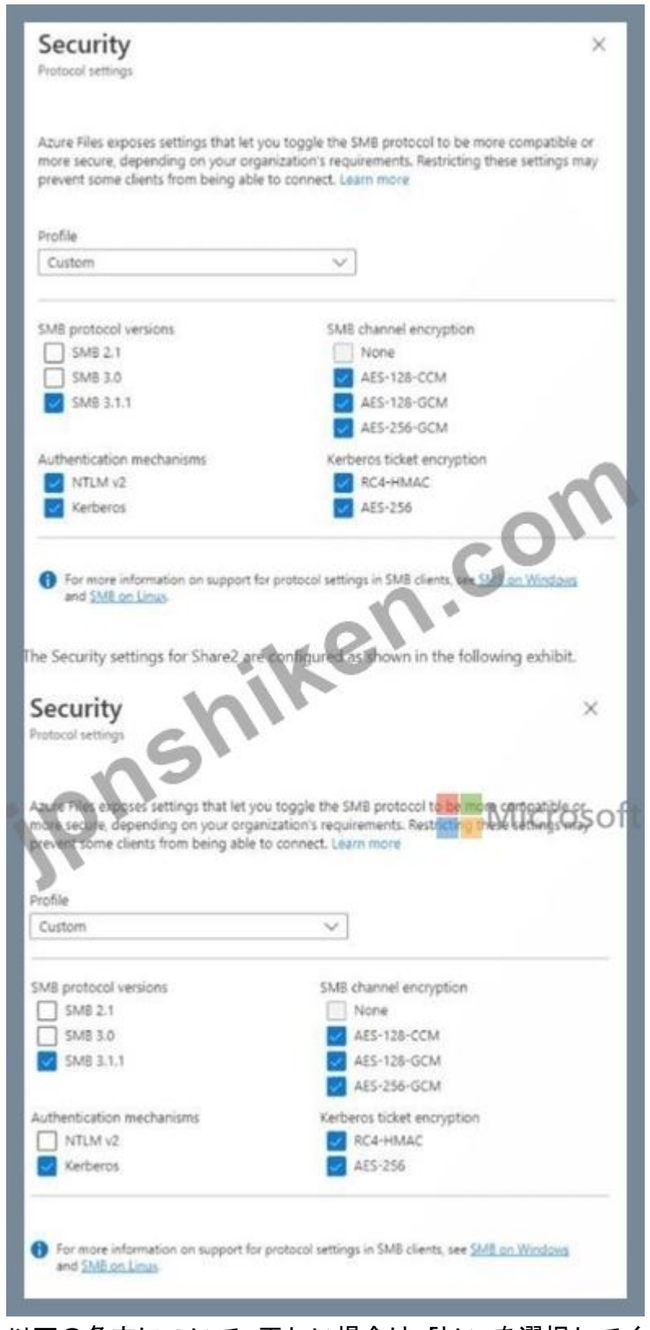
Explanation:

Graphical user interface, text, application Description automatically generated



質問: 173

オンプレミス ネットワークには、Active Directory ドメイン サービス (AD DS) ドメインと、次の表に示すデバイスが含まれています。
User1 という名前の同期されたユーザーを含むハイブリッド Microsoft Entra テナントがあります。
次の表に示す Azure Files 共有を含む Azure サブスクリプションがあります。
使用には、storage1 および storage2 にストレージ ファイル データ SMB 共有共同作成者の役割が割り当てられます。
Share! のセキュリティ設定は、次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 ポイントが付与されます。

Answer Area

Statements	Yes	No
User1 can mount share1 to Server2 by providing a storage access key.	○	○
User1 can mount share1 to Device1 by using their Microsoft Entra identity.	○	○
User1 can mount share2 to Server1 by using their AD DS identity.	○	○

正解:

Explanation:

Answer Area

Statements	Yes	No
User1 can mount share1 to Server2 by providing a storage access key.	◉	○
User1 can mount share1 to Device1 by using their Microsoft Entra identity.	◉	○
User1 can mount share2 to Server1 by using their AD DS identity.	◉	○

質問: **174**

Azure Active Directory（Azure AD）テナントがあります。

特権のないAzureADユーザーがAzureADでサービスプリンシパルを作成できないようにする必要があります。

テナントのAzureActive Directory管理センターで何をする必要がありますか？

A. [プロパティ]ブレードで、[Azureリソースのアクセス管理]を[いいえ]に設定します

B. [ユーザー設定]ブレードで、[ユーザーはアプリケーションを登録できます]を[いいえ]に設定します

C. [ユーザー設定]ブレードで、[AzureAD管理ポータルへのアクセスを制限する]を[はい]に設定します。

D. [プロパティウェイド]で、[セキュリティのデフォルトを有効にする]を[はい]に設定します。

正解: **B** (コメントを発表する)

質問: **175**

次の表に示す Azure App Service アプリを含む Azure サブスクリプションがあります。

Name	App Service plan
App1	Free
App2	Shared
App3	Basic
App4	Standard

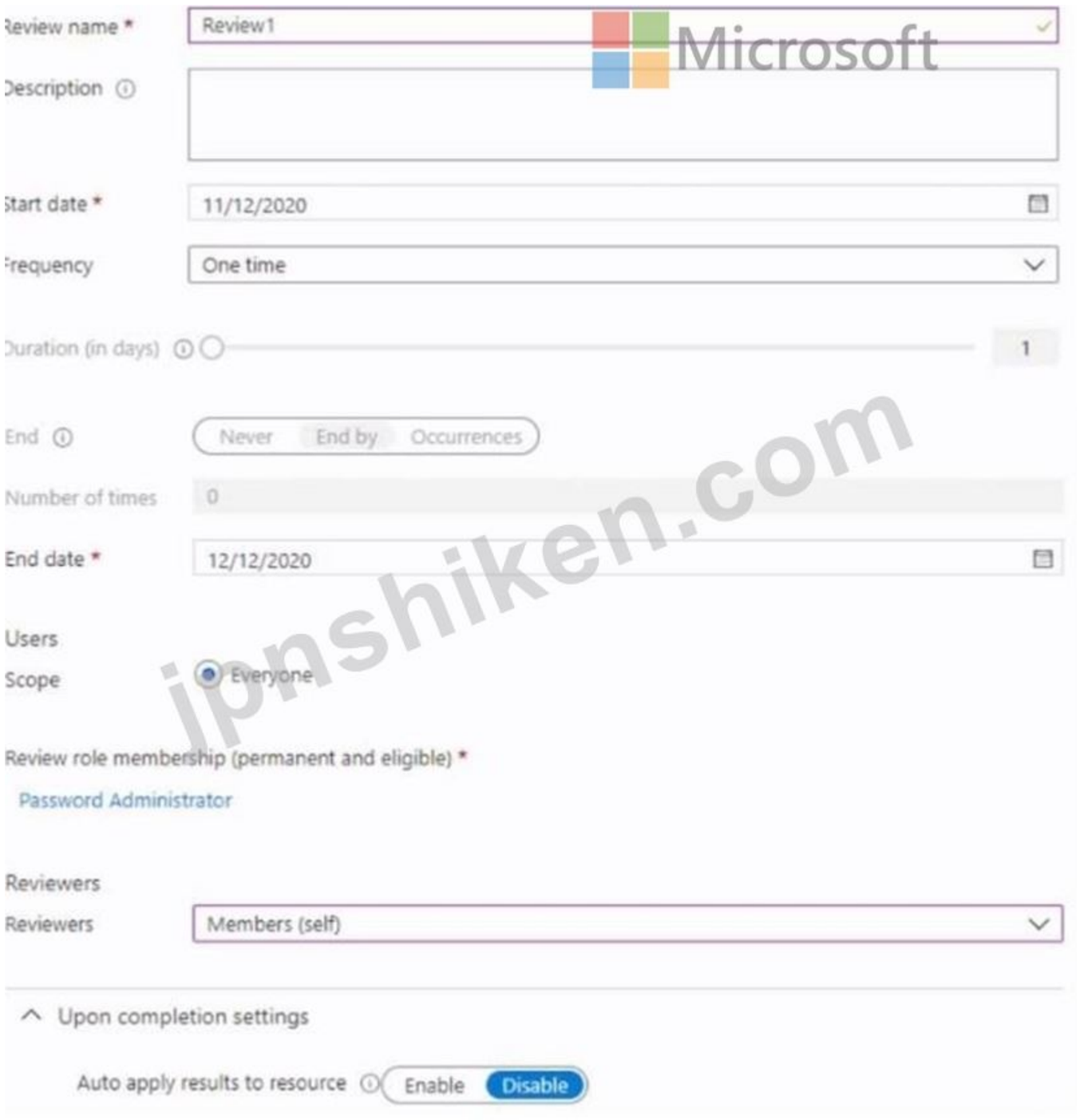
信頼できるサードパーティ機関からカスタム SSL 証明書を購入します。
カスタム SSL 証明書を割り当てることができるアプリはどれですか?
A. App4のみ
B. App3とApp4のみ
C. App2、App3、およびApp4のみ
D. App1、App2、App3、およびApp4
正解: **B** (コメントを発表する)

質問: **176**
Azureサブスクリプションがあります。
Azure Active Directory（Azure AD）特権ID（PIM）を有効にします。
管理者アカウントに対する会社のセキュリティポリシーには、次の条件があります。
*アカウントは多要素認証（MFA）を使用する必要があります。
*アカウントは20文字の複雑なパスワードを使用する必要があります。
*パスワードは180日ごとに変更する必要があります。
※アカウントはPIMで管理する必要があります。
過去90日間にパスワードを変更していない管理者に関するアラートを受け取ります。
生成されるアラートの数を最小限に抑える必要があります。
どのPIMアラートを変更する必要がありますか？
A. 役割は、アクティブ化のために多要素認証を必要としません。
B. 管理者は特権ロールを使用していません
C. 特権ID管理の外部で役割が割り当てられています
D. 特権ロールの潜在的な状態アカウント。
正解: (正解を表示します)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

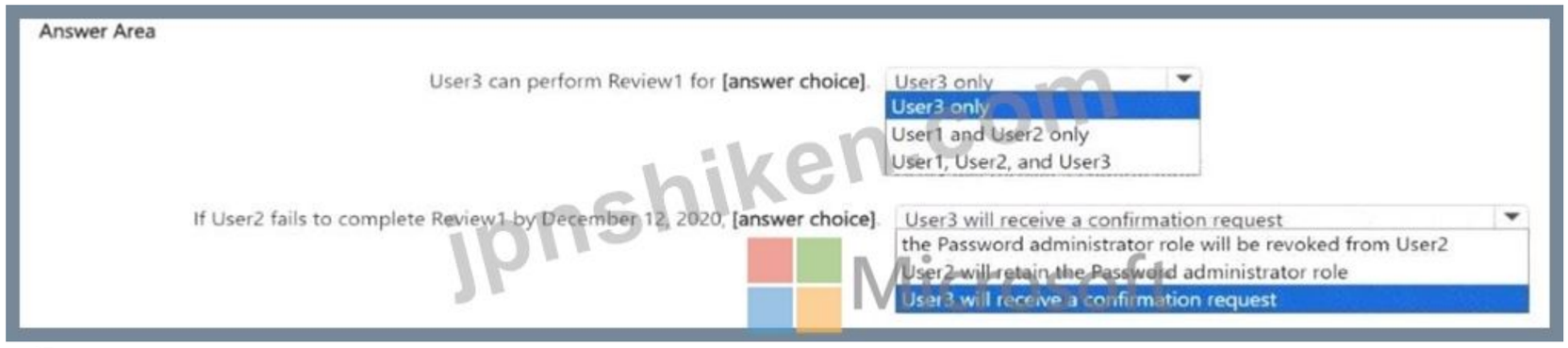
質問: **177**
contoso.com という Microsoft Entra テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

Name	Role	Sign in frequency
User1	Password Administrator	Signs in every work day
User2	Password Administrator	Signs in bi-weekly
User3	Global Administrator, Password Administrator	Signs in every month

次の図に示すように、Review1 という名前のアクセス レビューを構成します。図の日付は MM/DD/YYYY 形式です。



ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:

Explanation:

質問: **178**

Microsoft Entra テナントにリンクされた Azure サブスクリプションがあります。テナントは Microsoft Entra ID Protection を使用しています。
2,000 人のユーザーがおり、各ユーザーに Microsoft Entra ID P2 ライセンスが割り当てられています。
漏洩した資格情報を使用しているワークロード ID が検出された場合に、Azure Monitor を使用してアラートを生成する予定です。
計画されたアラートをサポートするには、診断設定を構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る必要があります。
どのログカテゴリーを収集すべきか、そして
ログはどこに送信すればよいですか? 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 ポイントが付与されます。

正解:

Explanation:

質問: **179**

User1 という名前のユーザーを含む Azure サブスクリプションがあります。User1 がマネージド ID を作成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。

あなたは何をするべきか？

A. 組織単位 (OU) を作成し、User1 にユーザー管理者の Azure AD ロールを割り当てます。

B. 管理グループを作成し、User1 にハイブリッド ID 管理者 Azure AD ロールを割り当てます。

C. リソース グループを作成し、User1 をマネージド ID 共同作成者ロールに割り当てます。

D. 管理グループを作成し、User1 にマネージド ID オペレーター ロールを割り当てます。

正解: **(**正解を表示します**)**

質問: **180**

次の表に示す Azure Firewall ポリシーが含まれる Azure サブスクリプションがあります。

Name	Type
Policy1	Standard
Policy2	Premium

サブスクリプションには、次の表に示すファイアウォールが含まれています。

Name	Tier	Policy
FW1	Premium	Policy2
FW2	Premium	Policy1

サブスクリプションには、次の表に示す仮想ネットワークが含まれています。

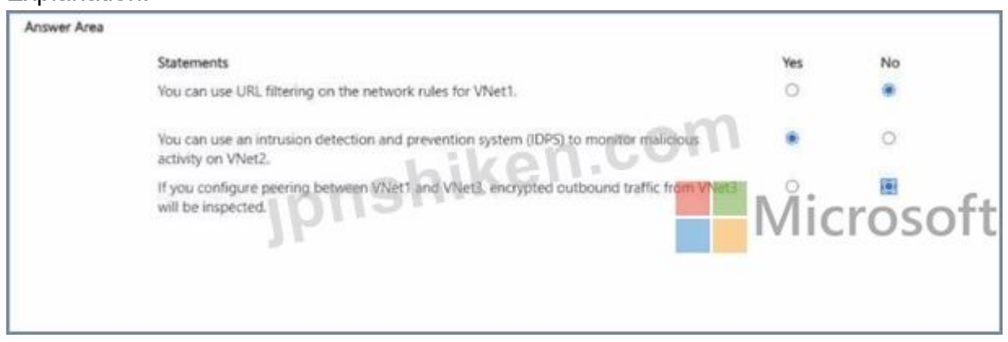
Name	Firewall
VNet1	FW1
VNet2	FW2
VNet3	*None*

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 ポイントが付与されます。

正解:

Explanation:

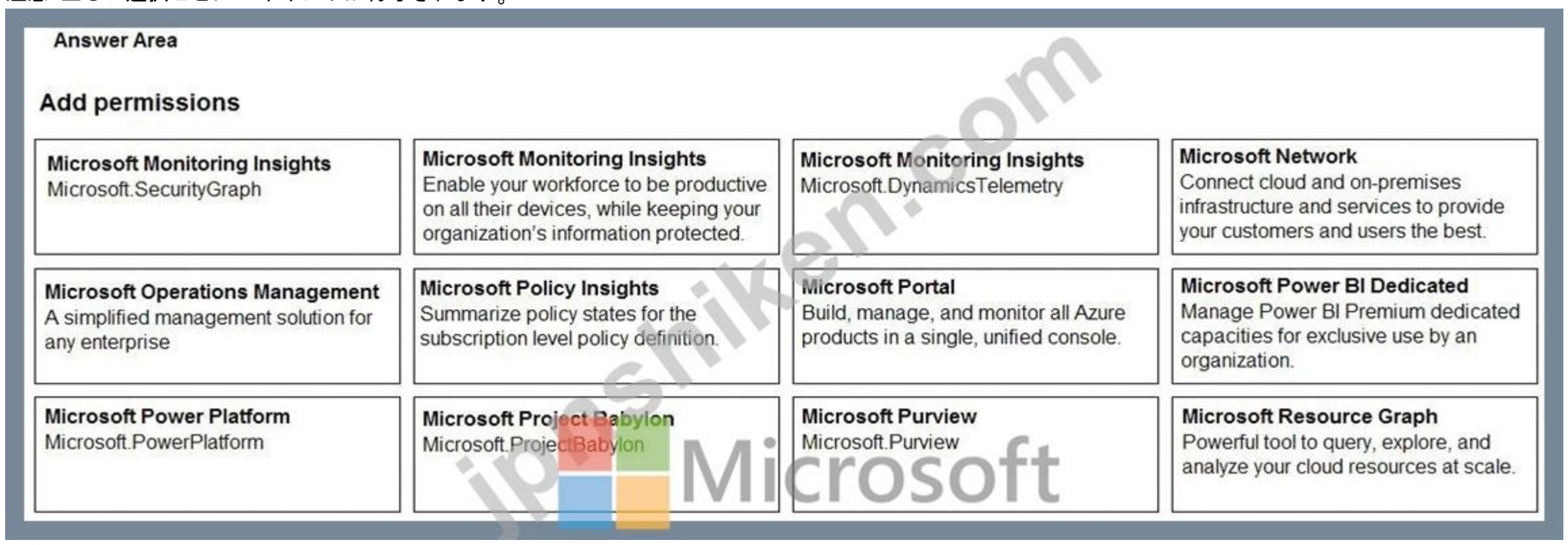


質問: 181

WebApp1という名前のAzure Webアプリがあります。

証明書をWebApp1にアップロードします。
WebApp1のアプリコードから証明書にアクセス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. ユーザー割り当ての管理対象IDをWebApp1に追加します。
B. アプリ設定をWebApp1構成に追加します。
C. WebApp1のシステム割り当ての管理対象IDを有効にします。
D. WebApp1のTLS / SSLバインディングを構成します。
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code

質問: **182**
User1 という名前のユーザーを含む Azure サブスクリプションがあります。User1 には、サブスクリプションの閲覧者ロールが割り当てられています。
Role1 という名前のカスタム ロールを作成し、Role1 を User1 に割り当てる予定です。
User1 が Azure Portal を使用してアプリケーション セキュリティ グループを作成および管理できることを確認する必要があります。
Role1 に追加する必要がある 2 つの権限はどれですか。回答するには、回答領域で適切な権限を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:

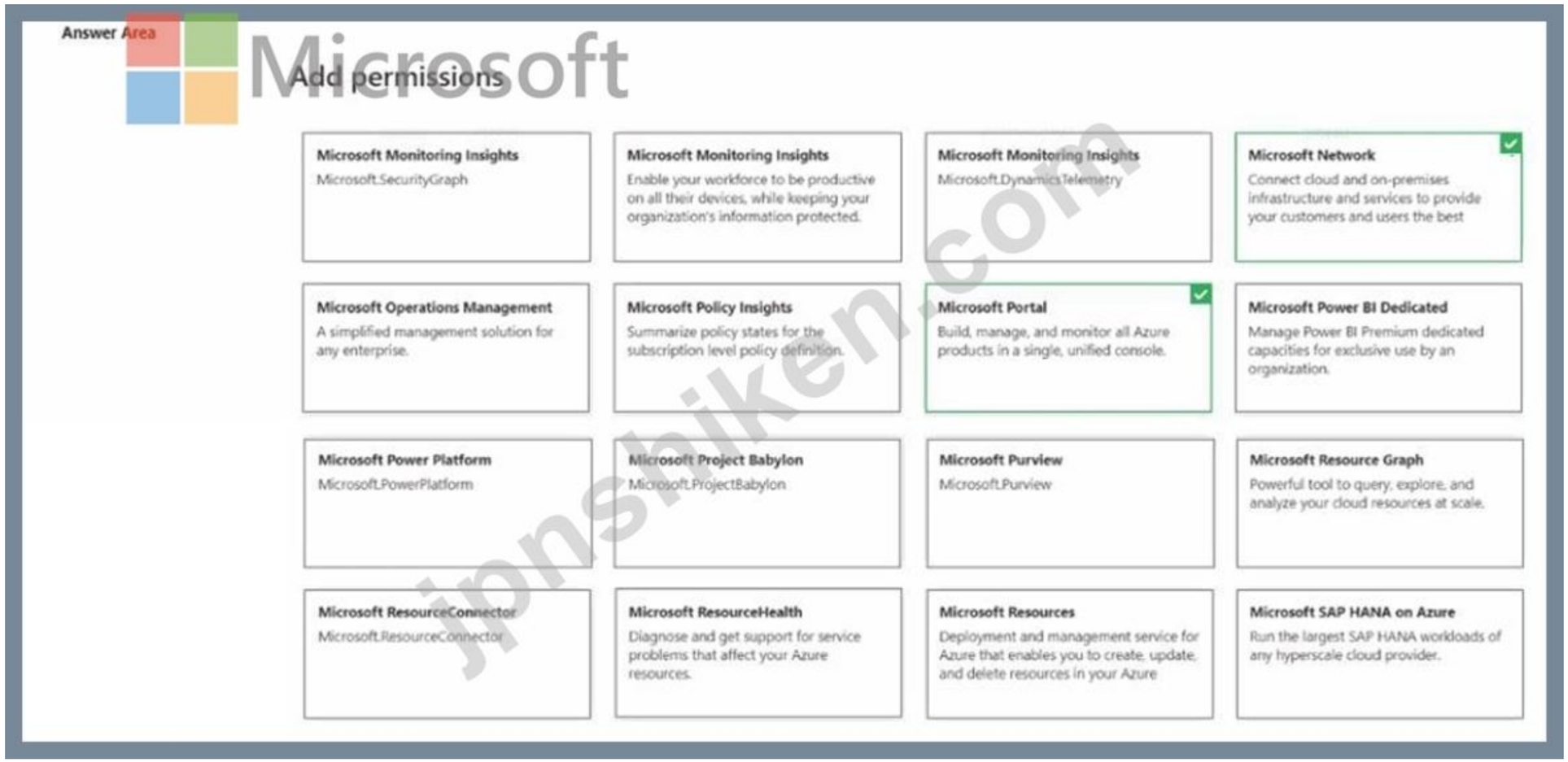
Answer Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	**Microsoft Monitoring Insights** Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	**Microsoft Monitoring Insights** Microsoft.DynamicsTelemetry	**Microsoft Network** Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	**Microsoft Policy Insights** Summarize policy states for the subscription level policy definition.	**Microsoft Portal** Build, manage, and monitor all Azure products in a single, unified console.	**Microsoft Power BI Dedicated** Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	**Microsoft Project Babylon** Microsoft.ProjectBabylon	**Microsoft Purview** Microsoft.Purview	**Microsoft Resource Graph** Powerful tool to query, explore, and analyze your cloud resources at scale.

Explanation:

Answer Area

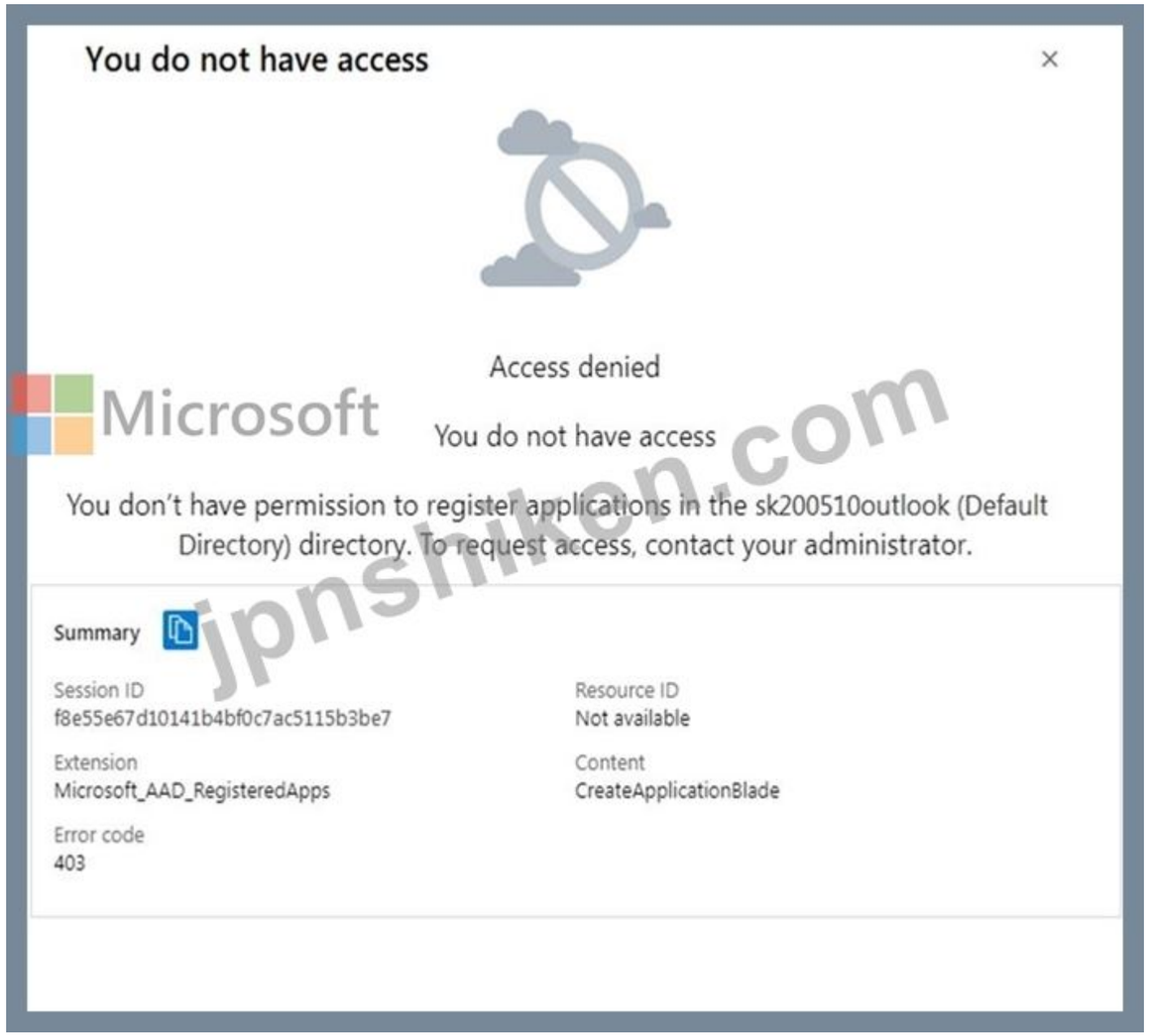


1. Microsoft Portal 2. Microsoft Network https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers

質問: 183

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。

開発者がApp1という名前のアプリをテナントに登録しようとすると、次の図に示すエラーメッセージが表示されます。

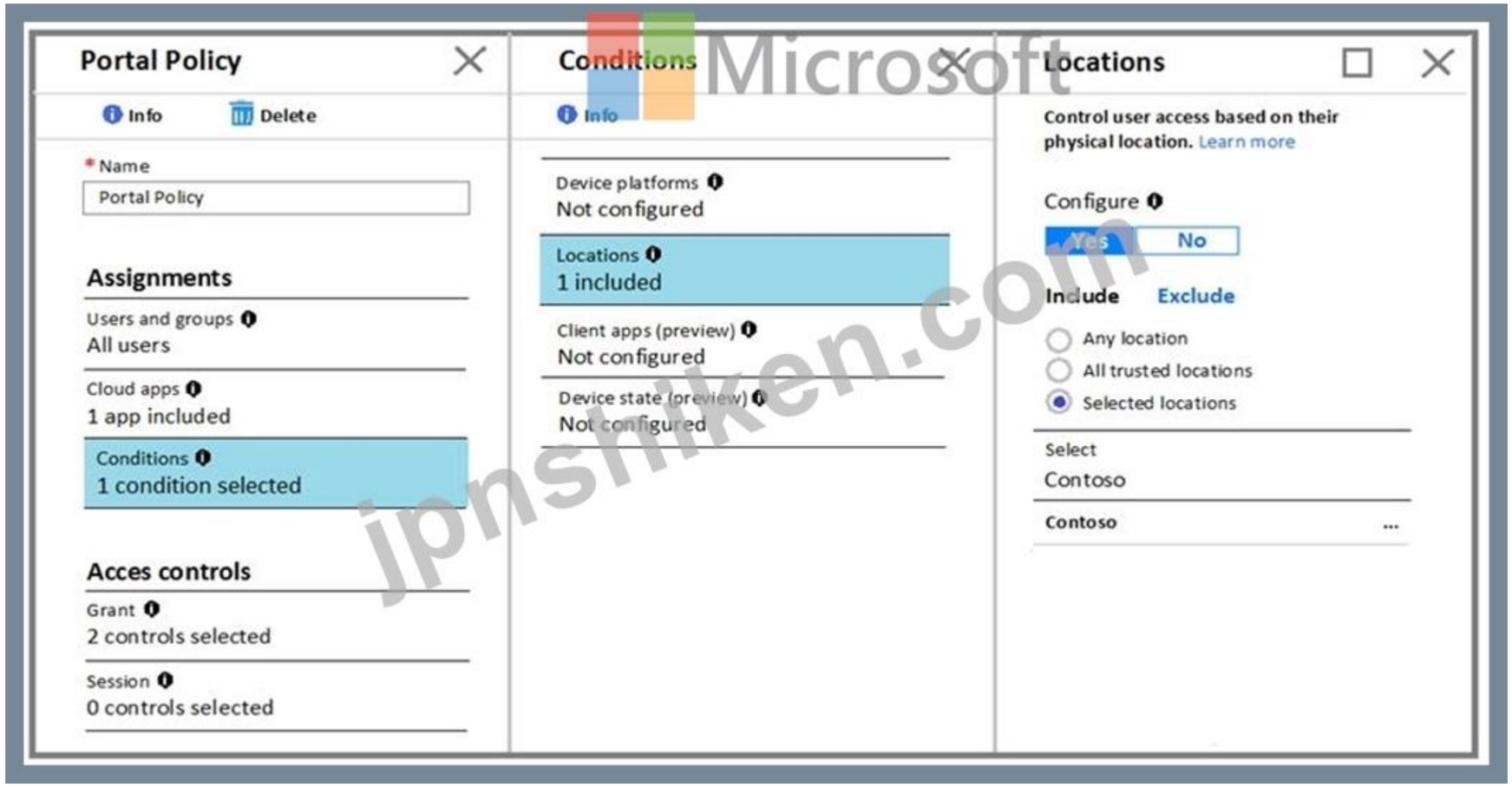


開発者がApp1をテナントに登録できることを確認する必要があります。
入居者はどうしますか？
A. ユーザー設定を変更します
B. [セキュリティを有効にする]のデフォルトを[はい]に設定します。
C. ディレクトリのプロパティを変更します。
D. エンタープライズアプリケーションの同意とアクセス許可の設定を構成します。
正解: **A (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

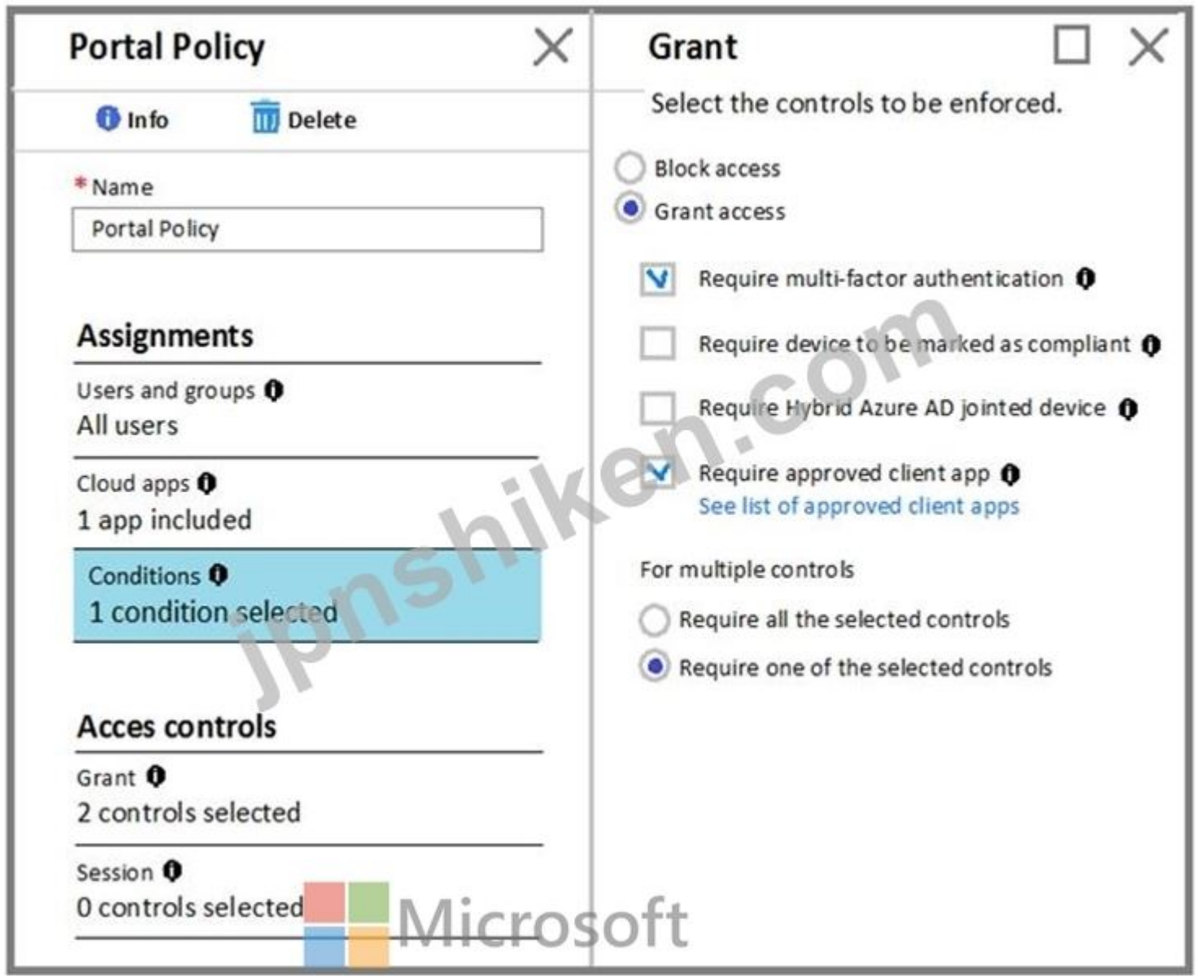
質問: **184**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。
このセクションの質問に回答すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。

Azure Active Directory（AzureAD）のハイブリッド構成があります。
仮想ネットワーク上にAzure HDInsightクラスターがあります。
オンプレミスのActive Directory資格情報を使用して、ユーザーがクラスターに対して認証できるようにする予定です。
計画された認証をサポートするように環境を構成する必要があります。
解決策 :オンプレミスデータゲートウェイをオンプレミスネットワークに展開します。
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**)**
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

質問**: 185**
新しい Azure Active Directory (Azure AD) テナントに関連付けられた新しい Azure サブスクリプションを作成します。
「ポータルポリシー」という名前のアクティブな条件付きアクセスポリシーを1つ作成します。ポータルポリシーは、Microsoft Azure管理クラウドアプリへのアクセスを提供するために使用されます。
ポータル ポリシーの条件設定は、条件の図に示すように構成されています。([条件] タブをクリックします。)



ポータル ポリシーの許可設定は、許可」の図に示すように構成されています。([許可] タブをクリックします。)



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。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

正解:

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

Explanation:
Box 1: No
The Contoso location is excluded
Box 2: NO
Box 3: NO
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

質問: 186
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.
You assign policies to the resource groups as shown in the following table.

Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	○
The deployment of SQL2 will fail.	○	○
SQL3 will be deployed and marked as noncompliant.	○	○

正解:

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	●
The deployment of SQL2 will fail.	●	○
SQL3 will be deployed and marked as noncompliant.	●	○

Explanation:
Graphical user interface, text, application Description automatically generated

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	●
The deployment of SQL2 will fail.	●	○
SQL3 will be deployed and marked as noncompliant.	●	○

Reference:

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

質問: **187**

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	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

次の表に示すAzureポリシーを作成します。

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

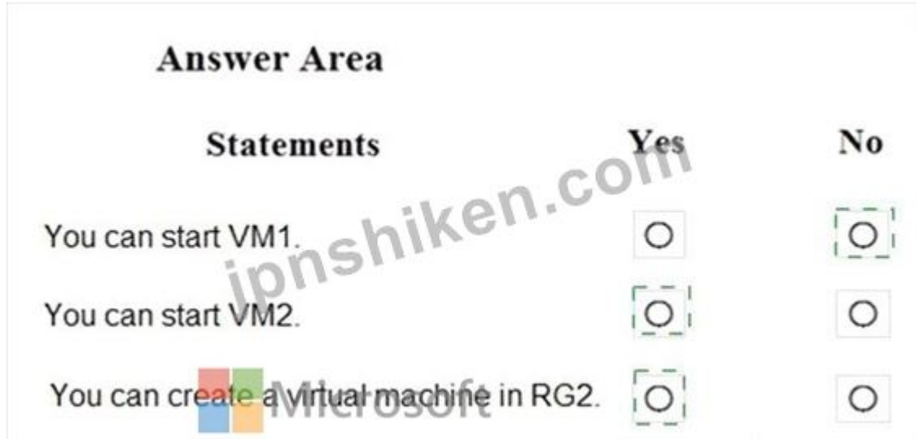
以下の各ステートメントについて、ステートメントが真である場合は「はい」を選択します。それ以外の場合は、「いいえ」を選択します。

注 :それぞれの正しい選択には1ポイントの価値があります。

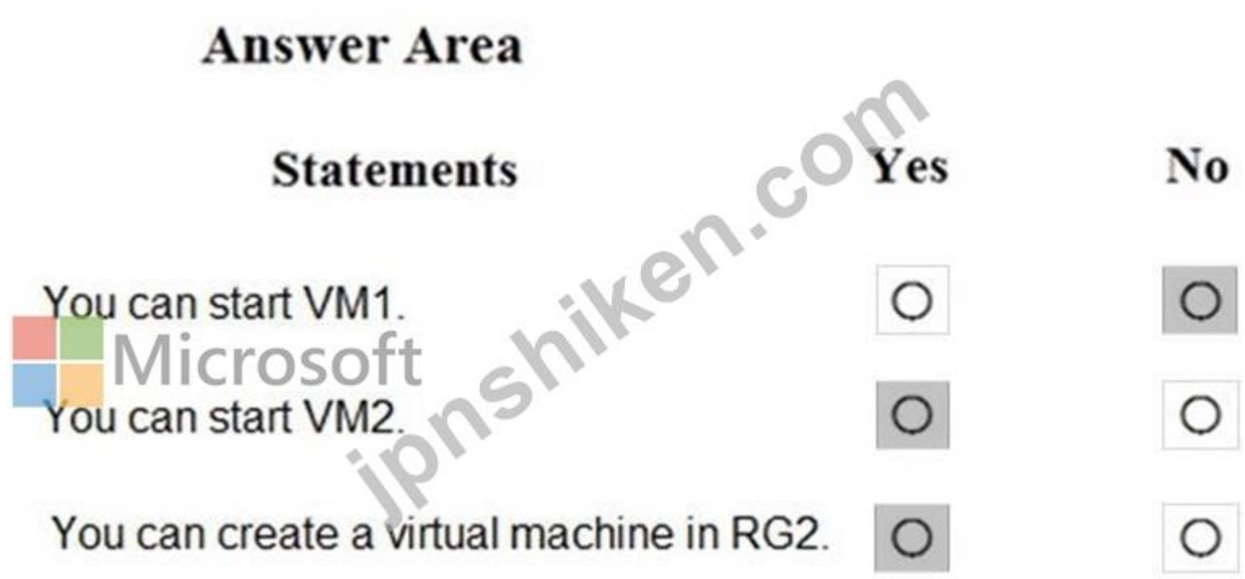
Answer Area

Statements	Yes	No
You can start VM1.	○	○
You can start VM2.	○	○
You can create a virtual machine in RG2.	○	○

正解:



Explanation:



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

質問: **188**
Azure サブスクリプションをお持ちです。
複数のデータ ソースを使用するように Microsoft Sentinel を構成します。
次の要件を満たす分析ルールを作成する必要があります。
* ルール 1: Common Event Format (CEF) ログと syslog データをドメイン、IP アドレス、および URL インジケーターと自動的に照合します。
* ルール 2: Microsoft 独自のアルゴリズムを使用します。
各ルールにはどのタイプの検出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 ポイントが付与されます。

正解:

Explanation:

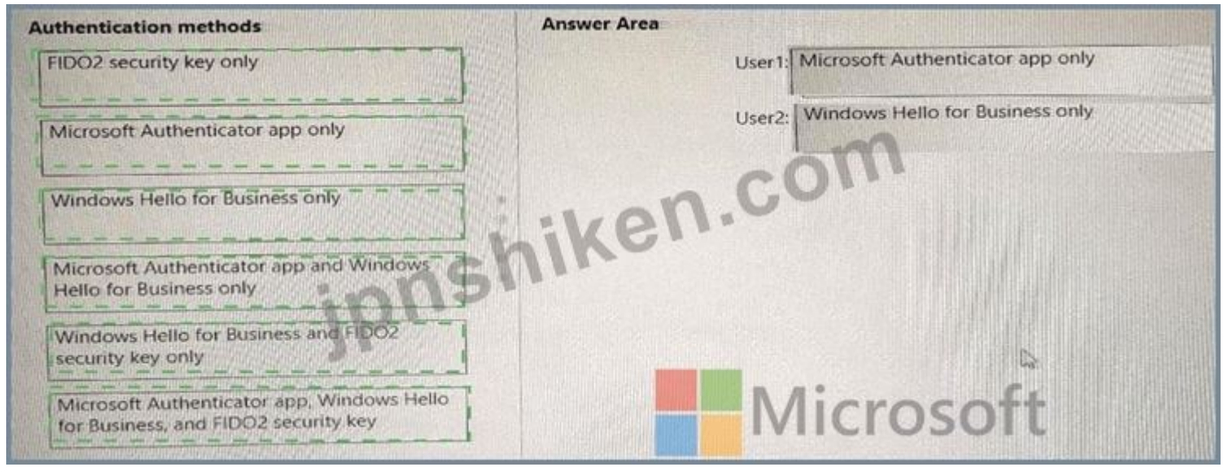
質問: **189**

次の表に示すユーザーを含む Azure AD テナントがあります。

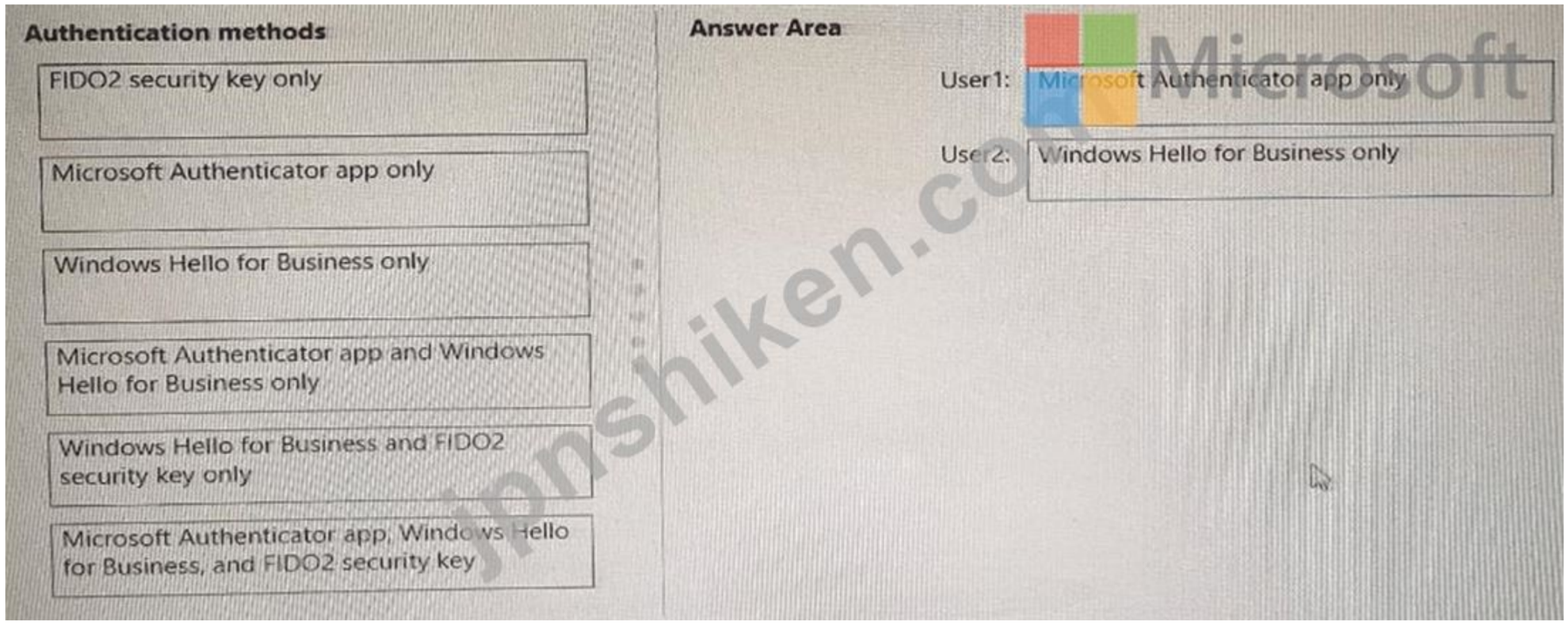
Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

テナントに対してパスワードレス認証を有効にします。
各ユーザーはパスワードレス認証にどの認証方法を使用できますか？ 適切な認証方法を適切なユーザーにドラッグしてください。各認証方法は、1回、複数回、またはまったく使用されない場合があります。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 ポイントが付与されます。

正解:



Explanation:

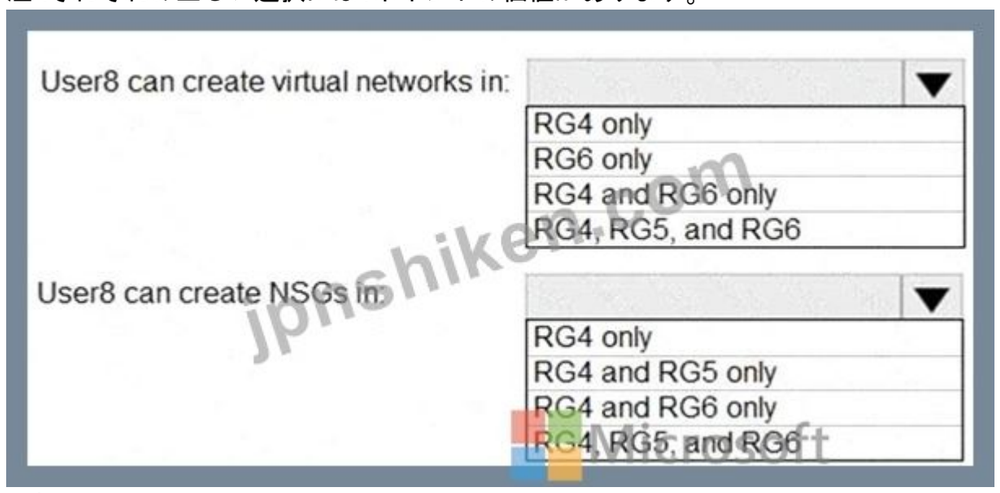


質問: 190

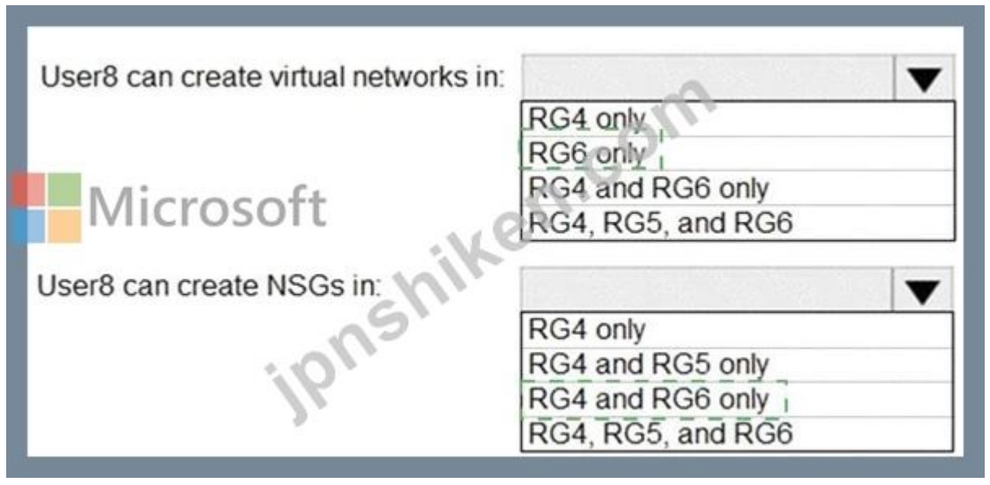
User8にRG4、RG5、およびRG6の所有者ロールを割り当てます。

User8はどのリソースグループで仮想ネットワークとNSGを作成できますか？回答するには、回答エリアで適切なオプションを選択します。

注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



Explanation:

Box1: RG6 only as there is not option for RG5 & RG6 which it should be.

Box2: RG4 & RG6

Topic 3, Fabrikam inc

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.

General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment

Network Environment

Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.

The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**Not applicable**	**None**

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	**Not applicable**
SecPol1	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected tor	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	**None**
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	**None**
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements
Planned Changes
Fabrikam plans to implement the following changes:
* Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

* Associate the network interface of VM1 to ASG1.
* Deploy SecPol1 by using Azure Security Center.
* Deploy a third-party app named App1. A version of App1 exists for all available operating systems.
* Create a resource group named RG2.
* Sync OU2 to Azure AD.
* Add User1 to Group1.
Technical Requirements
Fabrikam identifies the following technical requirements:
* The finance department users must reauthenticate after three hours when they access SharePoint Online.
* Storage1 must be encrypted by using customer-managed keys and automatic key rotation.
* From Sentinel1, you must ensure that the following notebooks can be launched:
* Entity Explorer - Account
* Entity Explorer - Windows Host
* Guided Investigation Process Alerts
VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.
Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.
App1 must use a secure connection string stored in KeyVault1.
KeyVault1 traffic must NOT travel over the internet.

質問: **191**
キー コンテナーと Azure SQL サーバーを含む Azure サブスクリプションがあります。
Transparent Data Encryption (TDE) と顧客管理キーを使用する Azure SQL データベースをデプロイする必要があります。
データベースを展開する前に何を作成する必要がありますか?
A. ユーザーが割り当てたマネージドID
B. 標準の汎用v2ストレージアカウント
C. アプリ登録
D. SQLセキュリティマネージャロールが割り当てられたユーザーアカウント
正解: **(**正解を表示します**)**

質問: **192**
ラボのタスク
タスク 7
Homepage-AGW という名前の Azure Application Gateway を介した接続が悪意のある要求について検査されていることを確認する必要があります。

正解:
see the task answer with step by step below:
* Enable Web Application Firewall (WAF) for the application gateway. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select a WAF policy and a WAF mode for the application gateway. You can choose a predefined policy or create a custom policy with your own rules and exclusions.
* Configure WAF policy settings. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the managed rulesets and rule groups that you want to enable or disable for the WAF policy. You can also configure custom rules to match specific patterns or conditions and take actions such as blocking or logging requests.
* Monitor WAF logs. You can use different types of logs in Azure to manage and troubleshoot the application gateway and the WAF policy. You can access some of these logs through the portal, such as metrics and health probes. You can also export the logs to Azure Storage, Event Hubs, or Log Analytics and view them in different tools, such as Azure Monitor, Excel, or Power BI.

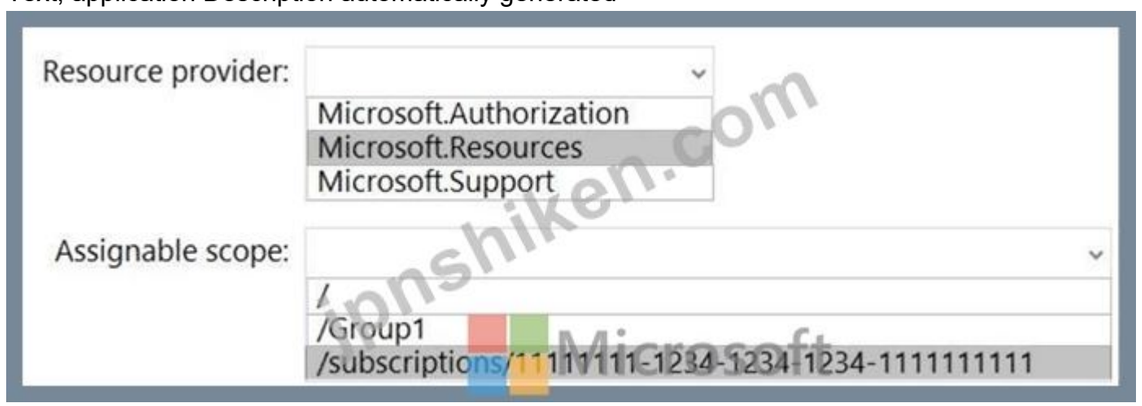
質問: **193**
Azureサブスクリプションがあります。
Azure Storageアカウントを読み取るためのアクセス許可を提供するカスタムのロールベースのアクセス制御（RBAC）ロールを作成することを計画しています。
RBACロール定義のどのプロパティを構成する必要がありますか？
A. NotActions []
B. DataActions []
C. AssignableScopes []
D. Actions []
正解: **D (コメントを発表する)**
To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission.
To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

質問: **194**
sub1という名前のAzureサブスクリプションを含むGroup1という名前の管理グループがあります。Sub1のサブスクリプションIDは11111111-1234-1234-1234-1111111111です。
Group1内のすべてのオブジェクトのタグを管理するためのアクセス許可を委任するカスタムAzureロールベースアクセス制御（RBAC）ロールを作成する必要があります。
Role1の役割定義に何を含め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：正しい選択はそれぞれ1ポイントの価値があります。

正解:

Explanation:

Text, application Description automatically generated



Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable- scopes

質問: **195**

次の表に示す Azure キー コンテナーが含まれる Sub1 という名前の Azure サブスクリプションがあります。

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

Sub1 では、次の構成を持つ仮想マシンを作成します。

* 名前:VM1
* サイズ: DS2v2
* リソースグループ: RG1
* 地域: 西ヨーロッパ
* オペレーティングシステム: Windows Server 2016

VM1 で Azure Disk Encryption を有効にする予定です。
VM1 の暗号化キーをどのキー コンテナーに保存できますか?

A. Vault1 または Vault3 のみ
B. Vault1、Vault2、Vault3、またはVault4
C. Vault1のみ
D. Vault1 または Vault2 のみ
正解: **C** (コメントを発表する)
" Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don ' t cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region. " https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

質問: **196**
container! というBLOBコンテナーとApp1というクライアントアプリケーションを含むAzureストレージアカウントがあります。Microsoft Entra認証を使用して、App1からcontainer1へのアクセスを許可する必要があります。どうすればよいでしょうか？ 回答欄から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: 197

MicrosoftSentinelを展開しています。

サードパーティのセキュリティソリューションを展開に接続する必要があります。サードパーティのソリューションは、Common Event Format（CER形式のメッセージ）を送信します。

ソリューションに何を含め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。

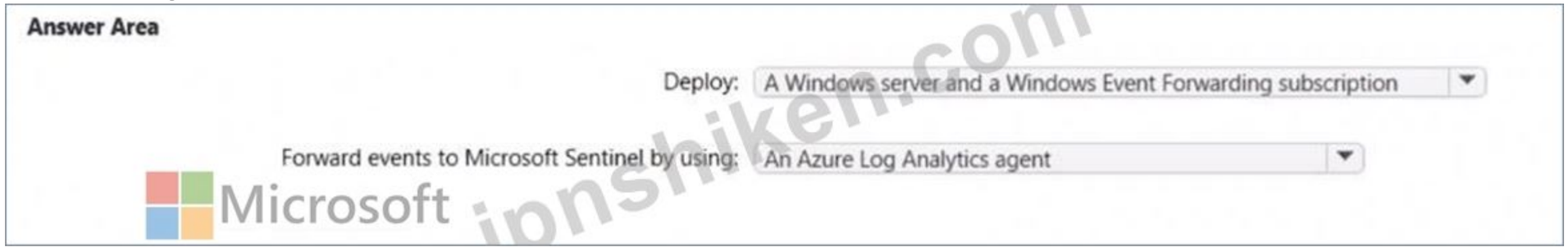
注：正しい選択はそれぞれ1ポイントの価値があります。

正解:

See the answer below at Explanation.

Explanation:

Answer is as image below.



質問: 198

100個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 Diagnosticsは、すべての仮想マシンで有効になっています。

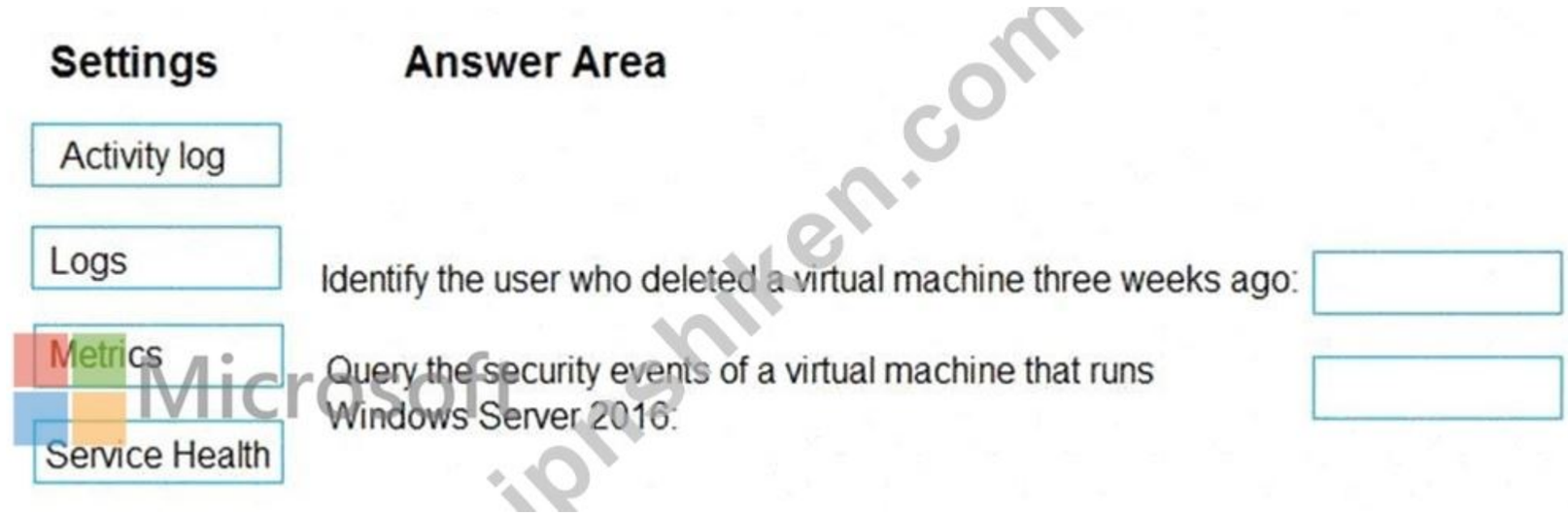
サブスクリプションでAzureサービスの監視を計画しています。

次の詳細を取得する必要があります。

* 3週間前に仮想マシンを削除したユーザーを特定します。
* Windows Server 2016を実行する仮想マシンのセキュリティイベントを照会します。

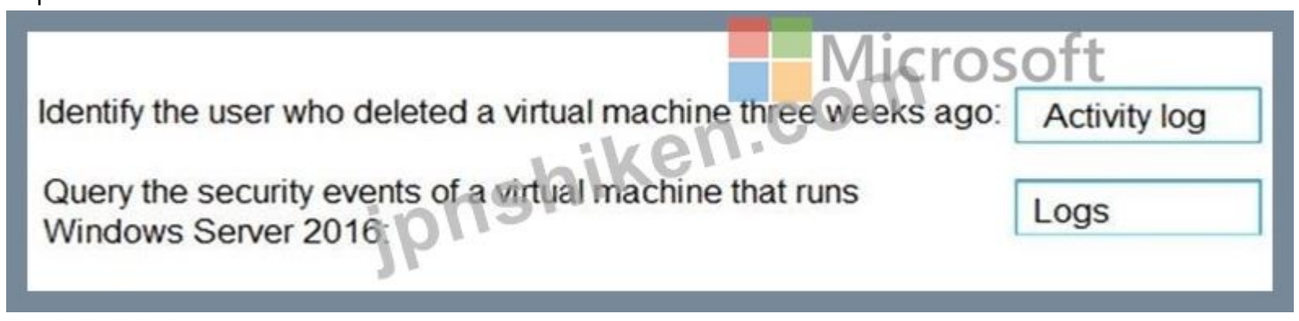
Azure Monitorで何を使用する必要がありますか？答えるには、適切な構成設定を正しい詳細にドラッグします。各構成設定は、1回、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注 :それぞれの正しい選択には1ポイントの価値があります。



正解:

Explanation:



Box1: Activity log

Azure activity logs provide insight into the operations that were performed on resources in your subscription.

Activity logs were previously known as "audit logs" or "operational logs," because they report control-plane events for your subscriptions.

Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they ' re on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

References:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

質問: **199**
User1という名前のユーザーを含むAzureActiveDirectory（Azure AD）テナントがあります。
User1が管理単位を作成および管理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にどの役割を割り当てる必要がありますか？
A. 特権ロール管理者
B. セキュリティ管理者
C. グローバル管理者
D. ヘルプデスク管理者
正解: **(**正解を表示します**)**

質問: **200**
あなたの会社は最近、Azureサブスクリプションを作成しました。
指定されたユーザーがAzureAD特権ID管理（PIM）を実装できることを確認する必要があります。
ユーザーに割り当てる必要がある役割は次のうちどれですか？
A. グローバル管理者の役割。
B. セキュリティ管理者の役割。
C. パスワード管理者の役割。
D. コンプライアンス管理者の役割。
正解: **(**正解を表示します**)**
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

質問: **201**
Azure環境があります。
ISO27001標準に準拠していないAzure構成とワークロードを特定する必要があります。何を使うべきですか？
A. Azure Sentinel
B. Azure Active Directory (Azure AD) Identity Protection
C. Azure Security Center
D. Azure Advanced Threat Protection (ATP)
正解: **C (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

質問: **202**

次の Azure ファイアウォールを含む Azure サブスクリプションがあります。
* 名前: Fw1
* Azure リージョン: 英国西部
* プライベートIPアドレス: 10.1.3.4
* パブリックIPアドレス: 23.236.62.147
サブスクリプションには、次の表に示す仮想ネットワークが含まれます。

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2

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	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

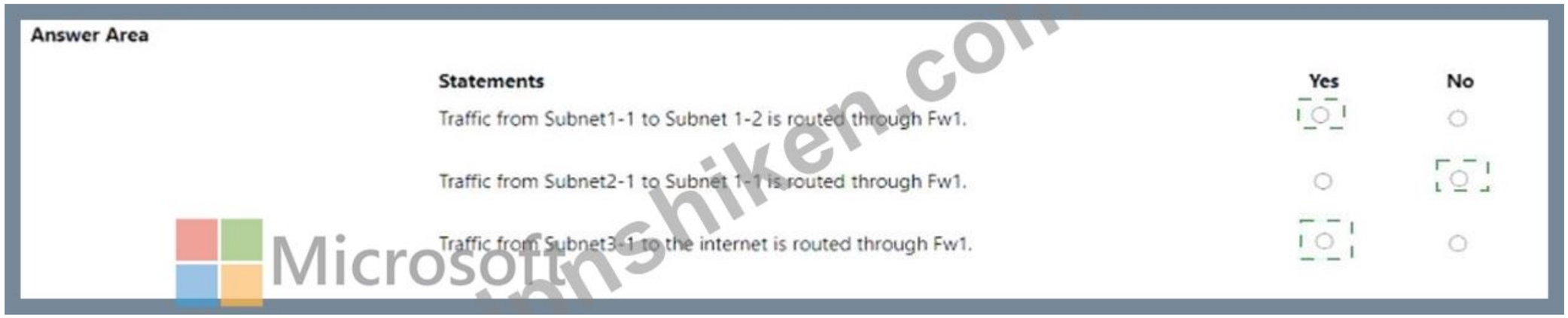
サブスクリプションには、次の表に示すルートが含まれています。

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

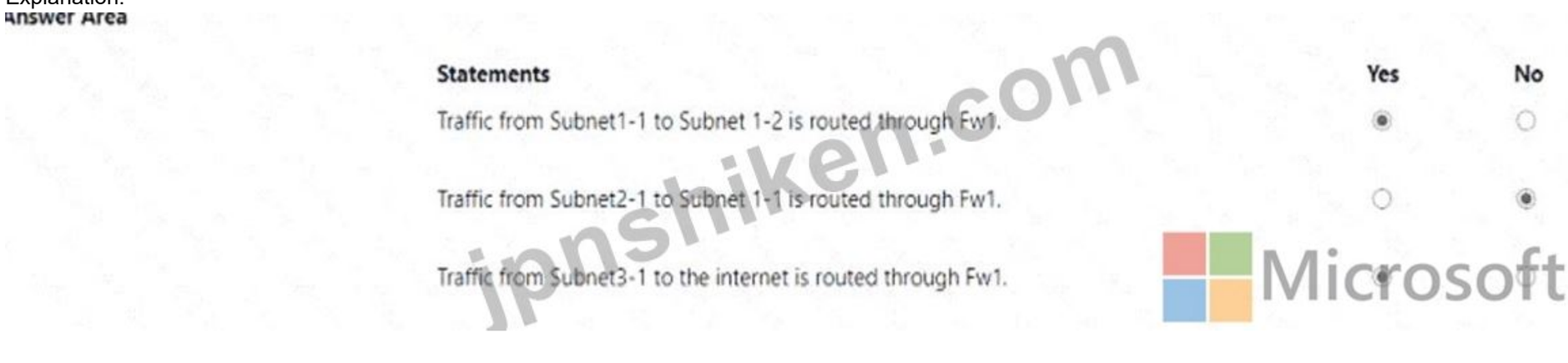
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。注：正しい選択肢は1つにつき1点です。
Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	○	○
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	○	○
Traffic from Subnet3-1 to the Internet is routed through Fw1.	○	○

正解:



Explanation:



質問: **203**

You have an Azure subscription that contains an Azure SQL database named SQL1.

You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

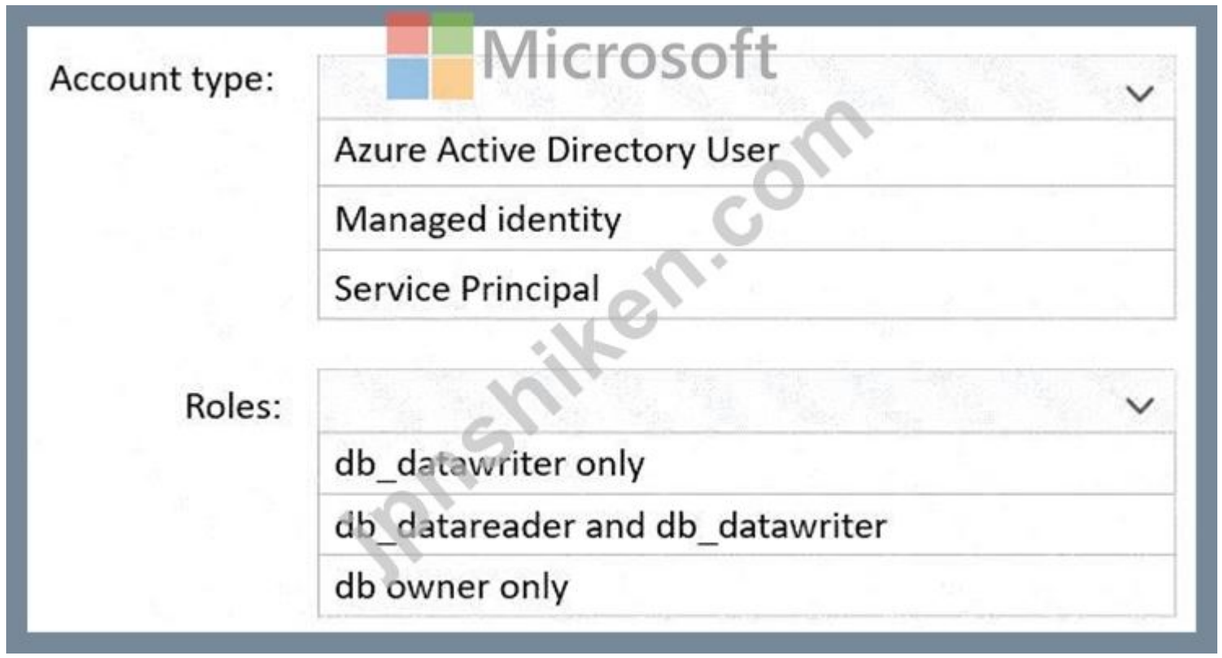
Provide App1 with access to SQL1 without storing a password.

Use the principle of least privilege.

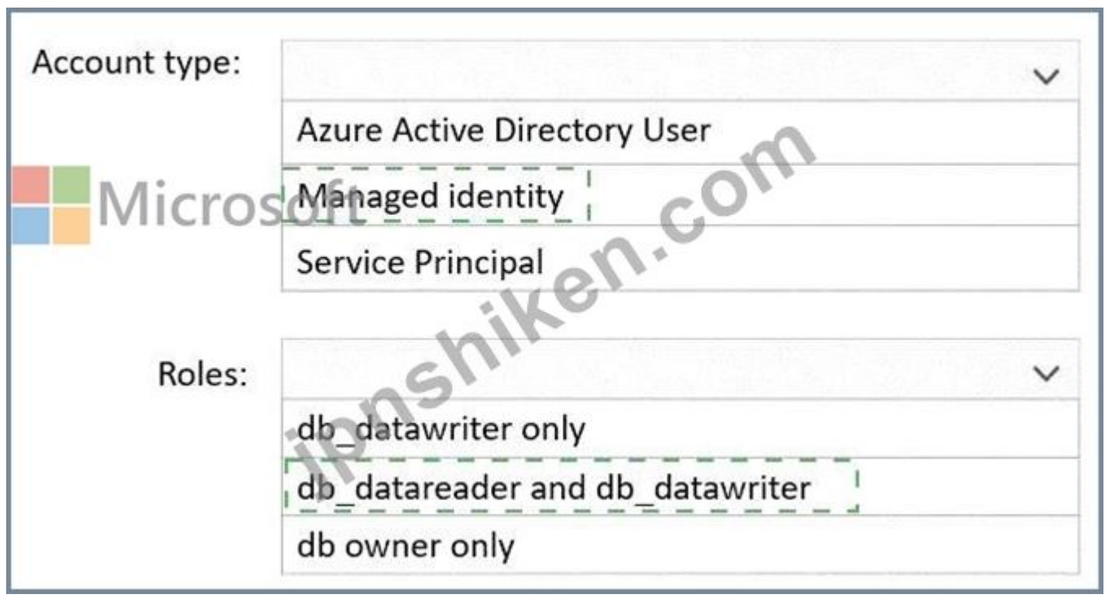
Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



正解:



Explanation:

Graphical user interface, text, application Description automatically generated

Reference:
https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet

質問: 204

App1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には、次の表に示すアプリ登録があります。

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	**None**
Microsoft.Graph	Calendars.Read	Delegated	No	**None**

App1がすべてのユーザーカレンダーを読み取り、予定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。
あなたは何をするべきか？

A. Microsoft.GraphCalendars.ReadWriteの新しい委任API権限を追加します。
B. Microsoft.GraphCalendars.ReadWriteの新しいアプリケーションAPI権限を追加します。
C. [管理者の同意を付与する]を選択します。
D. Microsoft.GraphCalendars.ReadWrite.Sharedの新しい委任API権限を追加します。
正解: **A (**コメントを発表する**)**
Reference:
https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

質問: 205

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。

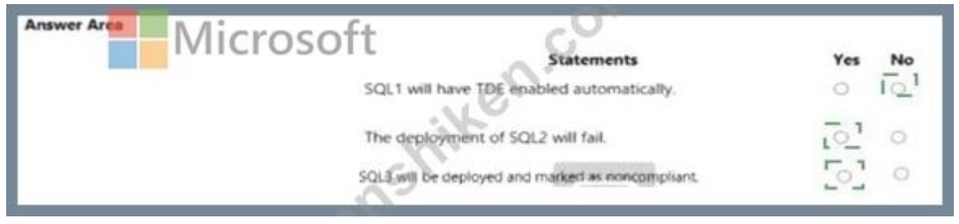
Name	Type	Resource group
RG1	Resource group	**Not applicable**
RG2	Resource group	**Not applicable**
RG3	Resource group	**Not applicable**
SQL1	Azure SQL Database	RG3

SQL1 では透過的なデータ暗号化 (TDE) が無効になっています。
次の表に示すように、リソース グループにポリシーを割り当てます。

Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

Azure Resource Manager (ARM) テンプレートを使用して Azure SQL データベースをデプロイする予定です。データベースは、次の表に示すように構成されます。
注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:



Explanation:
Graphical user interface, text, application Description automatically generated

質問: **206**
次の表に示す Azure キー コンテナーが含まれる Sub1 という名前の Azure サブスクリプションがあります。

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

Sub1 では、次の構成を持つ仮想マシンを作成します。

* 名前: VM1
* サイズ: DS2v2
* リソースグループ: RG1
* 地域: 西ヨーロッパ
* オペレーティングシステム: Windows Server 2022
VM1 で Azure Disk Encryption を有効にする予定です。
VM1 の暗号化キーをどのキー コンテナーに保存できますか?
A. Vault1 または Vault3 のみ
B. Vault1、Vault2、Vault3、またはVault4
C. Vault1のみ
D. Vault1 または Vault2 のみ
正解: **(**正解を表示します**)**
In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites

質問: **207**
User1 という名前のユーザーを含む contoso.com という名前の Microsoft Entra テナントがあります。
contoso.com に App1 という名前のアプリを登録し、Role1 という名前のアプリ ロールを作成します。
Role1 を User1 に割り当てる必要があります。
Microsoft Entra 管理センターの App1 のエンタープライズ アプリケーション ブレードでは何を構成する必要がありますか?
A. API権限
B. アプリのロール
C. 役割と管理者
D. ユーザーとグループ
正解: **(**正解を表示します**)**

質問: **208**
次の図に示すような Azure リソースの階層があります。

次の表に示す Azure Blueprints 定義を作成します。

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

Blueprint1 と Blueprint2 をどのオブジェクトに割り当てることができますか? 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 ポイントが付与されます。

Blueprint1:

- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- Subscription1 only
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

- ManagementGroup1 only
- Subscription1 and RG1 only
- Subscription1 only
- Subscription1, RG1, and VM1

正解:

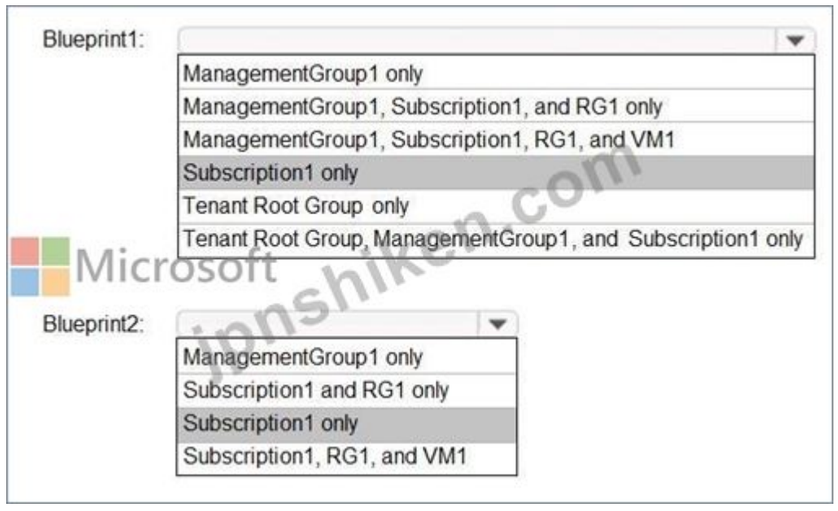
Blueprint1:

- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- Subscription1 only
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

- ManagementGroup1 only
- Subscription1 and RG1 only
- Subscription1 only
- Subscription1, RG1, and VM1

Explanation:



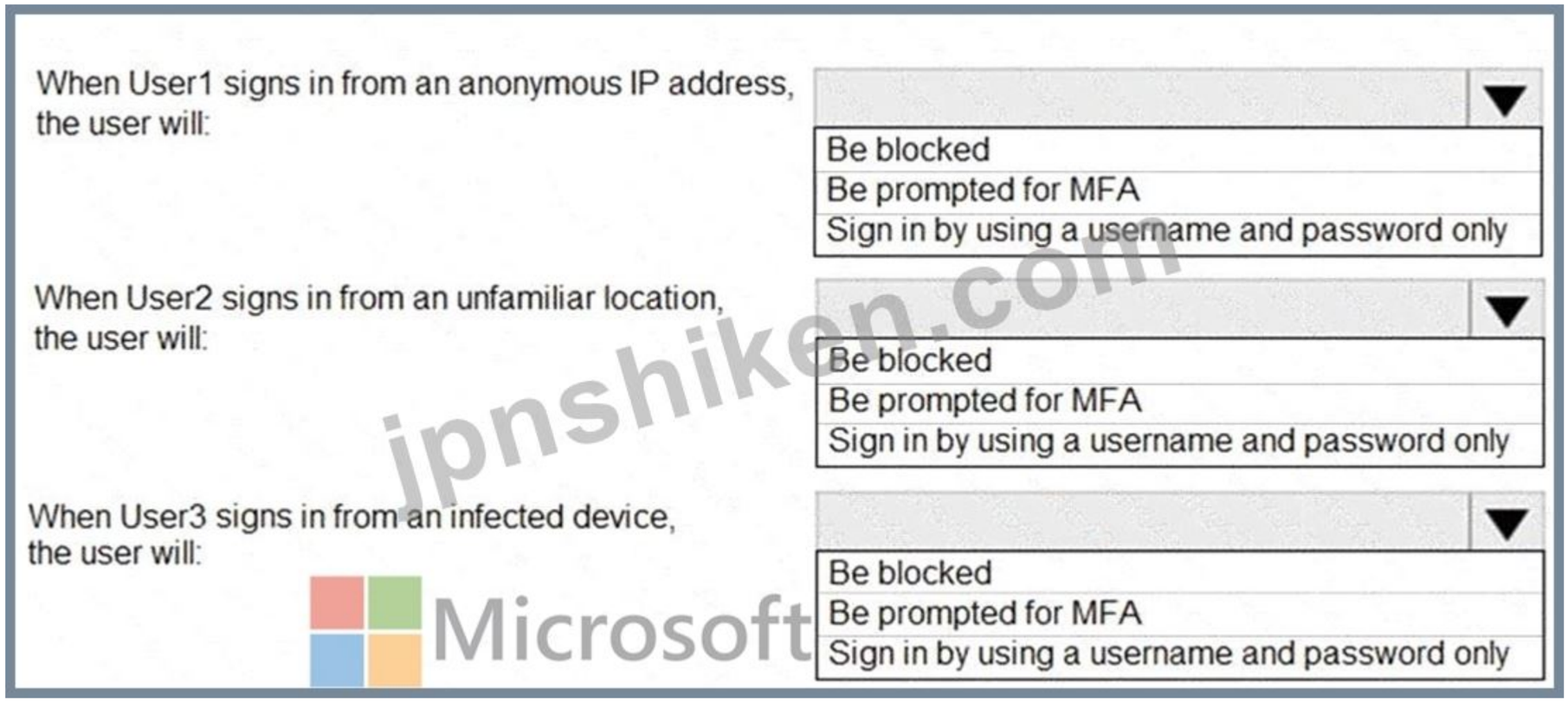
Blueprints can only be assigned to subscriptions.

質問: **209**
Azure サブスクリプションがあります。
VNet1 という名前の新しい仮想ネットワークを作成します。
VNet1 を使用し、プライベート IP アドレスを使用して到達できる App1 という名前の Azure Web アプリをデプロイする予定です。ソリューションは、インバウンドおよびアウトバウンドのネットワーク トラフィックをサポートする必要があります。
あなたは何をするべきか？
A. Azure アプリケーション ゲートウェイを作成します。
B. Azure App Service ハイブリッド接続を作成します。
C. リージョン仮想ネットワーク統合を構成します。
D. App Service 環境を作成する
正解: **D** (コメントを発表する)

質問: **210**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

次の設定を持つ Azure AD Identity Protection サインイン リスク ポリシーを作成して適用します。
* 割り当て: グループ1を含める、グループ2を除外
* 条件: サインインリスクレベル: 中以上
* アクセス アクセスを許可、多要素認証を要求する
ユーザーが Azure AD にサインインすると何が起こるかを特定する必要があります。
各ユーザーについて何を識別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 ポイントが付与されます。



正解:

When User1 signs in from an anonymous IP address, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

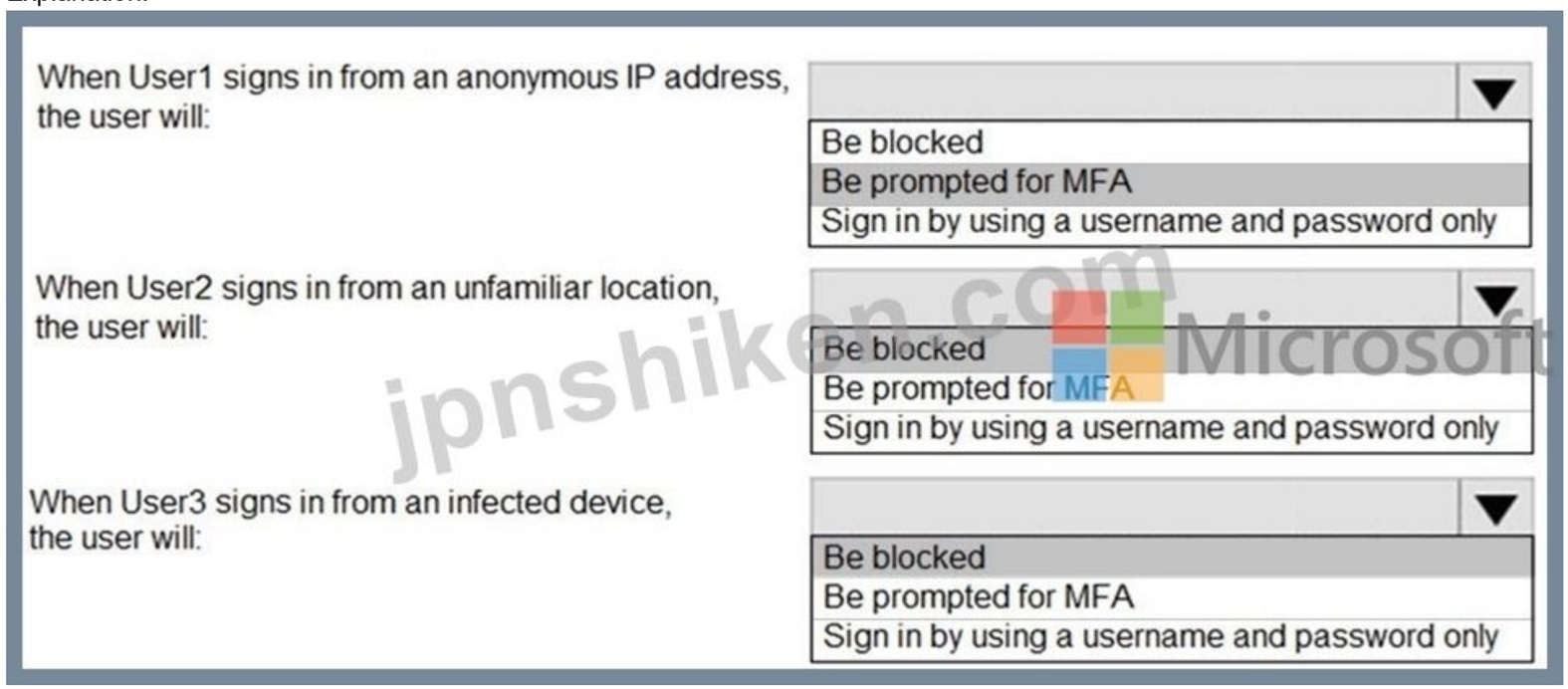
When User2 signs in from an unfamiliar location, the user will:

- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

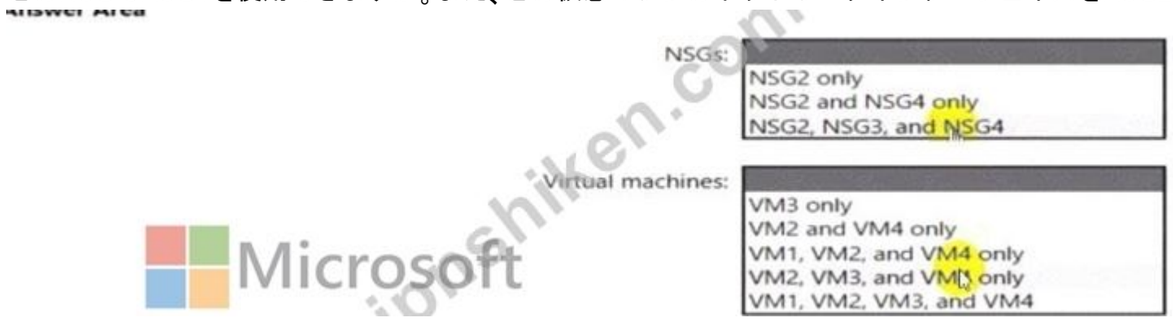
- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

Explanation:



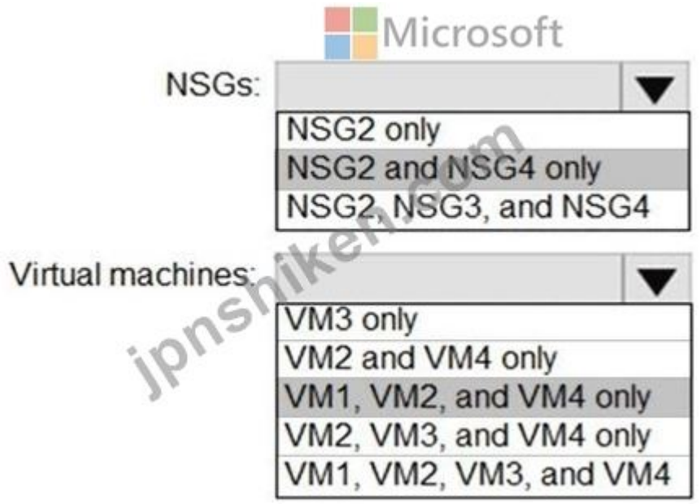
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection- policies
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

質問: **211**
ASG1およびASG2の計画された変更を実装します。
どのNSGでASG1を使用できますか。また、どの仮想マシンのネットワークインターフェイスをASG2に割り当てることができますか？



正解:

Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated



質問: **212**

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。

Sub1という名前のAzureサブスクリプションがあります。

RG1という名前のリソースグループにSa1という名前のAzureStorageアカウントがあります。

ユーザーとアプリケーションは、いくつかの共有アクセス署名 $AS）と保存されたアクセスポリシーを使用して、Sa1のblobサービスとファイルサービスにアクセスします。

許可されていないユーザーがファイルサービスとblobサービスの両方にアクセスしたことがわかりました。

Sa1へのすべてのアクセスを取り消す必要があります。

解決策：新しい保存済みアクセスポリシーを作成します。

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**)**

Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:

1. Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issused before

2. Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs liked to the Stored Access Policy.

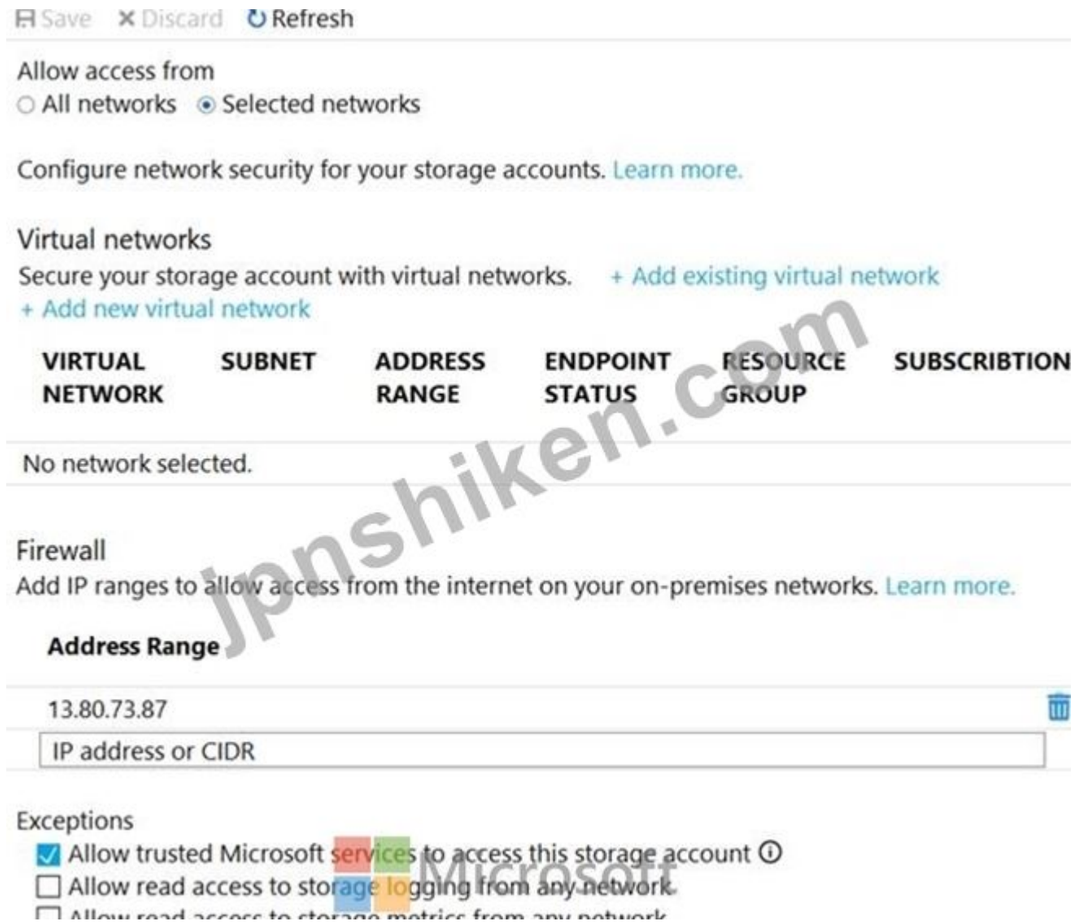
質問: **213**

お客様のAzureサブスクリプションには、Sentinel 1という名前のMicrosoft Sentinelワークスペースが含まれています。Sentinel!は、Microsoft 365の統合セキュリティ運用プラットフォームにはオンボーディングされていません。
Sentinel 1で新しいプレイブックを作成する必要があります。ソリューションは自動化ルールの使用をサポートしている必要があります。
どのようなタイプのプレイブックを作成すべきでしょうか？
A. アラートトリガーのみを含むプレイブック
B. エンティティトリガーのみを含むプレイブック
C. インシデントトリガーのみを含むプレイブック
D. インシデントトリガーまたはアラートトリガーを含むプレイブック
E. アラートトリガーまたはエンティティトリガーを含むプレイブック
正解: **(**正解を表示します**)**

質問: **214**
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	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	*None*

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。
次の図に示すように構成された、storageacc1 という名前の Azure ストレージ アカウントがあります。



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。

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

正解:

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

Explanation:

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

Box 1: Yes
The public IP of VM1 is allowed through the firewall.
Box 2: No
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No
The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.
Reference:
https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

質問: **215**
contoso.onmicrosoft.comという名前のAzure Active Directory（Azure AD）テナントがあります。
ユーザー管理者ロールは、Admin1という名前のユーザーに割り当てられます。
外部パートナーは、user1 @ outlook.comサインインを使用するMicrosoftアカウントを持っています。
Admin1は、Azure ADテナントにサインインするように外部パートナーを招待しようとし、次のエラーメッセージを受け取ります：「ユーザーuser1@outlook.comの一般的な承認の例外を招待できません。」Admin1が外部パートナーを招待してAzure ADテナントにサインイン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. [役割と管理者]ブレードで、セキュリティ管理者の役割をAdmin1に割り当てます。
B. 組織の関係ブレードから、IDプロバイダーを追加します。
C. [カスタムドメイン名]ブレードから、カスタムドメインを追加します。
D. [ユーザー]ブレードで、外部コラボレーション設定を変更します。
正解: **D** (コメントを発表する)
You need to allow guest invitations in the External collaboration settings.

質問: **216**
Vault1 という名前の Azure キー コンテナーと VM1 という名前の仮想マシンを含む Azure サブスクリプションがあります。
VM1 は、VNet1 という名前の仮想ネットワークに接続されています。
VM1 からのみ Vault1 へのアクセスを許可する必要があります。
Vault1 のネットワーク設定では何をすればよいですか?
A. [ファイアウォールと仮想ネットワーク] タブから、VM1 の IP アドレスを追加します。
B. [ファイアウォールと仮想ネットワーク] タブから、VNet1 を追加します。
C. [ファイアウォールと仮想ネットワーク] タブで、Vault1 に対して [信頼された Microsoft サービスがこのファイアウォールをバイパスすることを許可する] を [はい] に設定します。
D. [プライベート エンドポイント接続] タブから、VM1 のプライベート エンドポイントを作成します。
正解: (正解を表示します)

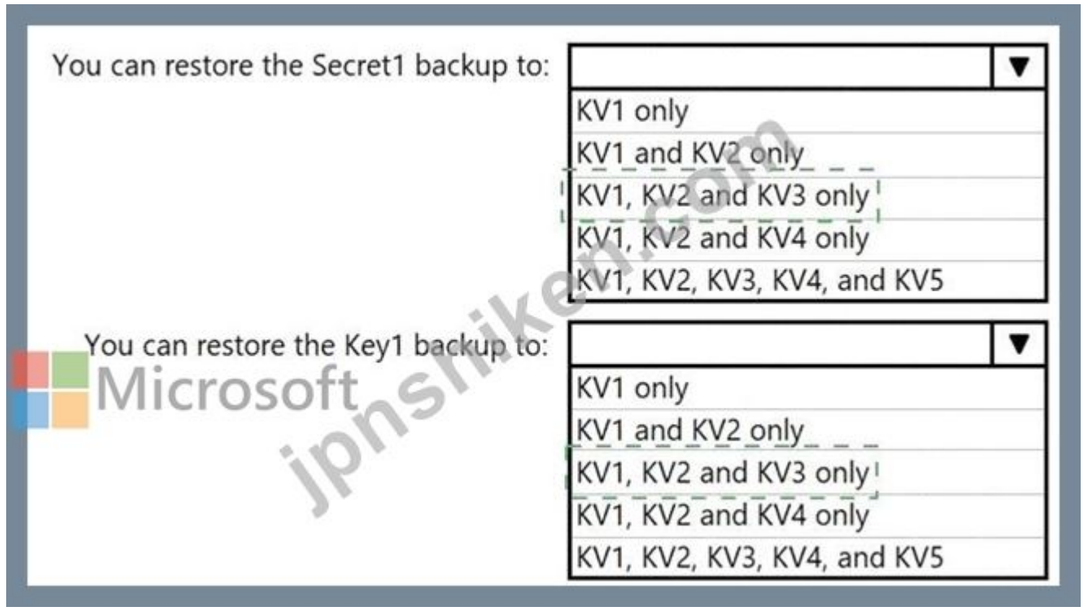
質問: **217**

次の表に示す Azure キー コンテナーがあります。

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 には、Secret1 という名前のシークレットと、Key1 という名前の管理対象ストレージ アカウントのキーが保存されます。
Secret1 と Key1 をバックアップします。
各バックアップをどのキー コンテナーに復元できますか? 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 ポイントが付与されます。

正解:



Explanation:

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.
https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli

質問: 218
次の表に示すユーザーを含むAzureサブスクリプションがあります。

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	*None*	Global administrator	Enforced
User3	*None*	Global administrator	Disabled

どのユーザーがAzureAD特権ID管理（PIM）を有効にできますか？

A. User2とUser3のみ

B. User1とUser2のみ

C. User2のみ

D. User1のみ

正解: **(**正解を表示します**)**

Reference:

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

質問: **219**

次の表に示すAzure仮想ネットワークがあります。

Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	*None*

次の表に示すAzure仮想マシンがあります。

Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

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

Priority	Name	Port	Protocol	Source	Destination	Action
110	Allow_RDP	3389	Any	Any	Any	Allow
130	Rule1	Any	Any	ASG1	Any	Allow
140	Rule2	Any	Any	ASG2	Any	Allow
150	Rule3	Any	Any	ASG4	Any	Allow
160	Rule4	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

アウトバウンドセキュリティルール

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

正解:

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Explanation:

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Box 1: Yes
VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.
Box 2: No
VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.
Box 3: Yes
VM3 has a public IP address and the firewall allows traffic on port 3389.

有効的な**AZ-500J**問題集はJPNTest.com提供され、**AZ-500J**試験に合格することに役に立ちます！JPNTest.comは今最新**AZ-500J**試験問題集を提供します。JPNTest.com AZ-500J試験問題集はもう更新されました。ここで**AZ-500J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AZ-500J-mondaishu　**520**問、３０%ディスカウント、特別な割引コード:**JPNshiken**」